International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I5P128

Volume 74 Issue 5, 435-457, May 2026

Review Article

Enhancing AI Awareness and Fraud Prevention Strategies for Senior Citizens

Sheetal Ajay Warankar[1*], Meenakshi Kale[1]

[1]*G H Raisoni University, Amravati, Maharashtra, India.*

[1*]*Corresponding Author : sheetalwarankar.2025@rediffmail.com*

Received: 03 December 2025 Revised: 31 January 2026 Accepted: 28 March 2026 Published: 30 May 2026

Abstract - This *paper will cover the usefulness of the notion of Artificial Intelligence (AI) to protect the elderly against fraud and propose the interdisciplinary studies needed to address the technological and human issues. A type of fraud prevention that involves the use of AI, i.e., when anomaly detection and biometric validation are present, is also functioning, although little is known about its psychological impact on the elderly. The three problems that demonstrate why computer science and psychology should be combined are the enhanced state of anxiety, dependence, and a lack of confidence, which make it essential to understand the role AI has on the psychological stability of elderly people and their confidence. In addition, the paper also identifies morality and law-related aspects of privacy, informed consent, and the expectations of the long-term effects of AI-based surveillance. As a high percentage of people of the older generation demonstrate deficiencies in digital literacy, the paper suggests turning to policy-level measures that are used to facilitate the process of ethical facilities of AI utilization, not to mention privacy issues. The research, with the help of such disciplines as geriatrics, sociology, and digital ethics, should be conducted in order to create effective and global AI applications. The application of AI into the medical system, the social welfare system, and the financial system that enables complete security is also a subject of the paper. In conclusion, the paper makes the recommendation that the developers, caregivers, policymakers, and communities must convene with an objective of regaining trust in AI, and in doing so, this would allow the elderly to operate within the new online space with no security concerns.*

Keywords - *AI, Elderly Protection, Fraud Prevention, Digital Literacy, Ethical Considerations, Interdisciplinary Research*.

1. Introduction

1.1. Background

The twenty-first century is characterized by unbelievable technological trends where Artificial Intelligence (AI) and digital technologies are the new way of life. They have also introduced convenience and efficiency, and they have introduced new threats, in particular to the most vulnerable group, such as older citizens (Payton & Claypoole, 2023), (Zukry et al., 2024). Not only our parents and grandparents, but, as a rule, the older generation are faced with numerous challenges in adapting to the rapidly changing digital world. They are not very familiar with technology and are at higher risk of being fooled or used and becoming a victim of cybercrime due to their age and cognitive changes, which might be accompanied by age. The news reports are also being filled with more and more examples of AI-enabled technologies being misused by assaulting older adults as loved ones or accredited bodies. Not only are those fraudulent schemes devastating in terms of money, but they are also emotionally traumatizing because they make people doubt technology and human relations. It is based on this that, in the act of protecting the elderly citizens, not only is the issue money but also that of dignity, psychological security, and responsiveness across generations. At the same time, AI in its pure form could be of great help in countering said threats, as it will be capable of detecting fraud, detecting anomalies, and developing personal security systems. This way, the radical imperative to question the advantages of the AI as a device of exploitation to help protect the well-being of the older generation seems to be a welcome measure (Frik et al., 2019).

1.2. Aims and Objectives of the Research

What is meant by the urgency of the proposed work is the need to explore the issue of elderly population fraud prevention with a specific focus on the implementation of AI technologies as effective solutions. The paper will determine the degree of threat to the elderly, soft digital natives, and the promise that smart technologies carry with them to manage the threats. The overall objectives of the research are three-fold, and they are; first, to examine the existing problems and gaps associated with protecting the elderly parents against digital fraud and abuse; second, to come up with the possibilities and opportunities that the applications of AI-based solutions would make in preventing fraud, including

machine learning algorithms, natural language processing, biometric authentication, and anomaly detection systems; and lastly, to explain the existing gap in knowledge between the theoretical explanations of AI use and its practical application in the context of elderly care.

1.3. Scope of the Paper

The paper is specifically open-ended and aims to present a multidimensional, holistic analysis of artificial intelligence and fraud prevention converging with eldercare. It conducts a systematic literature review and examines publications and other materials on the topic of applying artificial intelligence in fraud detection and the security of elderly demographics. A list of the cyber-crime phenomena considered includes, though is not limited to, financial fraud, such as online banking, unauthorised transactions, and unauthorised transactions; and threats of the future, including impersonation through deepfake technologies, social engineering, and cyberattacks. Moreover, the paper examines the ethical and social implications of using artificial intelligence in areas where there are vulnerable human populations, acknowledging both the potential good and the potential for abuse. The theoretical framework allows, in turn, to explore what lies outside the realm of technological solutions to solve the lack of digital literacy, legal frameworks, and intergenerational support infrastructure.

1.4. Structure of the Paper

Due to the need to achieve clarity and logical consistency, this paper is subdivided into logically connected segments. After this introduction, the literature review will summarize whatever information exists regarding artificial-intelligence technologies and any other fraud-prevention resources, and the specifics of the elderly population. The following section on the current problems will outline the spheres of digital illiteracy, institutional safeguarding, and technological access that compound the threats to older adults. Still on the topic of AI-based solutions, in the next section, we will build on the idea and explain how more advanced AI-based solutions, including predictive analytics, biometric verification, fraud-detection algorithms, and assistive AI, could be implemented to improve the safety of the older generation. At the end of the paper, research and policy recommendations to help create a safer and more inclusive digital space among the older generation of citizens will be provided. The final section will summarise the findings and highlight the need for cross-sector partnerships between the government, researchers, and technology providers to create a safe digital environment for older people. As far as we know, this methodological approach gives us a complete and active view of the safety of elderly parents in an AI-powered world.

Although the mechanisms of digital fraud and AI-based approaches to fraud detection have been explored in detail among the general populations, the existing literature does not put much thought into the fact that older adults represent a peripheral or homogeneous group of users, where cognitive weaknesses, low levels of digital literacy, and socio-emotional consequences of AI-based fraud are the main factors that cannot be well-considered. In addition, the majority of existing literature dwells upon technical detection accuracy or algorithm performance, which does not provide much information about the possibility of the practical application of AI solutions, how they are ethically implemented, and socially accepted in the framework of eldercare. This shows that there is a research gap that is critical in terms of understanding how AI-based models of fraud prevention can be applied in the real world to protect the elderly.

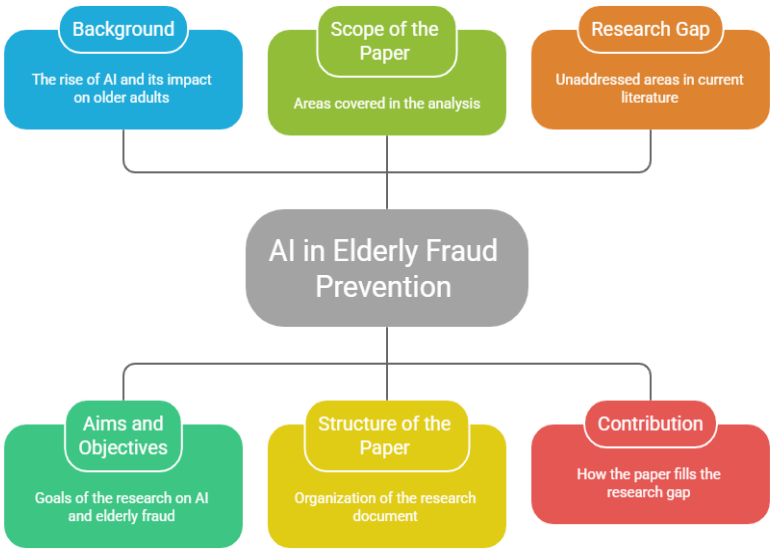

Fig. 1 AI in elderly fraud protection

The current paper fills this gap by positioning elderly citizens as a vulnerable category and critically analysing AI technologies not as a detection tool, but as a comprehensive protection system that synthesizes an anomaly detection tool, biometric authentication, and helpful intelligence with ethical and social factors. In contrast to the current literature, which focuses on the efficiency of technology in isolation, the study will provide new value through a holistic, multidisciplinary viewpoint; it integrates technological innovation, the needs of the elderly, and policy implications, thus advancing the existing literature on AI-facilitated fraud prevention of vulnerable groups.

2. Literature Review

2.1. Overview of Senior Citizens and Digital Vulnerabilities

There is a noted departure in the world's demographic patterns, where the elderly citizens make up an ever-increasing percentage of its population (Bello & Olufemi, 2024). The United Nations predicts that by the year 2050, one in six people will be aged 65 and older, which represents both the triumph of healthcare progress and the arrival of intricate problems for society (Naberushkina et al., 2025). A major problem of information technology vulnerability is well noticed among older adults (Herrera et al., 2024). Modern seniors have not been brought up in the age of the internet, smartphone, and AI-powered apps; the low-tech divide is present as an unfavorable condition, as most of the older generations are unacquainted with those technologies, and their younger counterparts view them as natural (Parti et al., 2025). As a result, they face challenges related to creating a strong password, distinguishing phishing links, and going through a multifactor authentication process (Mahajan, 2025). This issue of accessibility is even exacerbated by constant technological progress, including the shift to completely digital banking, leaving elderly individuals dependent on intermediaries (Dennis, n.d.). In addition, cognitive and physical impairments with age - such as cognitive decline, decreased problem-solving speed, shorter attention spans, and memory loss - make it more difficult to recognize subtle signs of fraud, such as typographical errors in phishing messages or abnormal account usage in internet banking services. Minor vision and hearing impairments could also make it difficult for them to focus on small text or to distinguish unfamiliar voices and thus have a limited ability to understand automated security alerts (Aziz et al., 2025). Psychosocial vulnerability is a major risk factor - many elderly people are lonely, isolated, or less sociable because of retirement, spousal death, or family migration. These emotional needs are exploited by pretend friend callers, well-meaning strangers, or relatives attempting to extract information about them or get them to pay money (Mantello et al., 2025). A combination of digital illiteracy, lack of trust and social isolation results in an incredibly high vulnerability to victimization. Overall, it is evident that older individuals are at the junction of demographic shifts, technological change, and age, a combination that makes them especially susceptible to cybercriminals (Iansiti & Lakhani, 2020). Subsequently, the need to fulfill immediate, safe, and convenient digital platforms specific to this group has become clear (Mehan, 2022).

The majority of literature covering the area of elderly vulnerability to digital fraud provides a complex but disjointed picture of the issue. The existing literature focuses on the idea that the elderly are not a homogeneous and weak population group; older adults have various coping strategies, risk perceptions, and adaptive abilities when working with digital technologies (Tamers et al., 2020). Similar studies show the potential increase in the number of fraudulent acts committed with the support of artificial intelligence, such as deepfakes, phishing, and voice-cloning technologies to commit economic and emotional crimes, yet most studies do not contain systematically verifiable datasets (L. Huang, 2023). In comparison, studies on AI-based fraud detection reveal that machine learning, natural language processing, biometric authentication, and anomaly detection systems can be used to detect suspicious activities and provide elderly users with customized protection, but these artificial intelligence applications are not well tested in a practical eldercare environment. In addition to technical performance, both social and ethical analyses advise that defensive AI infrastructures can produce risks in their own right, especially when used in the context of vulnerable populations without any proper supervision or empirical verification (Menz et al., 2024). Moreover, the multidisciplinary research extends the concept of fraud beyond financial loss to impersonation, cyber harassment, and social engineering, suggesting the significance of intergenerational support structures. Last but not least, policy-oriented research only emphasizes that strong regulatory systems, digital literacy campaigns, and public-private efforts are needed to achieve meaningful protection, yet there are still tremendous differences in how STIs in various jurisdictions are addressed.

2.2. Fraud Acted in Relation to the Elderly

Fraudulent incidents against older citizens are a wide range, and many of them are extremely difficult because of technological illiteracy and indulgence in trustfulness (Suura, 2024). The most common type of fraud is financial, but in recent years, cyber-facilitated frauds have been on the rise (Ahmed et al., 2020).

Telemarketing and Phone Scams - Telemarketing scams are one of the most common but ancient types of fraud (AbdullahAl-Nafisa & MKhatatbeh, 2025). Fraudsters use telephone calls to make calls to elderly people for the pretense of special offers, healthcare products, or charities (Kakulapati et al., 2023). Victims are prone to share sensitive information or send money because of the polite tone of the caller. This strategy is based on the fact that older adults use the phone more often than younger generations (Vargis, 2023).

Lottery, Sweepstakes, and Prize Frauds Another type of fraud involves luring victims into believing they will win a lottery or a prize after paying a processing fee or tax (Luckin & Holmes, 2016). The elderly, who are often not aware of how to play an actual sweepstakes, are prone to fall prey to such fraudulent activities and lose a significant amount of money (Siddiqui et al., 2025).

Phishing and Identity Theft--Online Fraud against Older People. This type of cyber fraud against older persons occurs through sophisticated phishing attacks, in which e-mails or text messages appear to come from a trustworthy source such as their bank, governmental agency, or insurance company. By accidentally visiting dangerous websites, victims can give up login credentials or other financial data (Long & Magerko, 2020). One of the most significant effects of such scams is identity theft, where stolen personal information, such as social security numbers, medical insurance information, credit card numbers, etc., is used to drain money (Punitha & Preetha, 2024).

Naming and Shaming- It is common among fraudsters to use social engineering to create a feeling of trust and influence emotions (Agrawal et al., 2022). One of them is the so-called grandparent scam, where a person posing as a family member requires an immediate transfer of money and is in dire need (Davenport, 2018). Out of the goodness of their hearts, seniors can submit to the request without questioning its validity (Baek et al., 2024).

Elder Fraud in the Digital Age: The rise of artificial intelligence has brought new dimensions to elder fraud, highlighting the need for an understanding of its intricate and varied forms (Kumar et al., 2023). Voice-cloning technology can allow a fraud suspect to mimic the voice of a friend or a family member who is recognized as legitimate and valid, making it impossible to tell who is making the call. In the same way, the fake videos that are deep-fried may make a senior think that they are communicating with someone (Datti et al., 2025). These technological solutions undermine traditional methods of detection and make older adults more vulnerable (Bernard et al., 2012).

Benefit: Fraud in Elderly People. This is not the only negative consequence of financial losses (Ross, 2020). A significant number of victims who are older suffer severe psychological effects, including anxiety, shame, and reduced belief in their capacity to live on their own (Walsh, 2007). An economic hardship could force dependence on the caregivers or limit access to necessary healthcare and supplies (Pearlson et al., 2024). Indeed, as an example, in 2022, an FBI report reported that persons over 60 years old lost over 3 billion dollars through the Internet Crime Complaint Center (IC3) (West, 2018), which highlights how large and widespread the issue is in Europe, Asia, and the rest of the world (Waheeb, 2023).

2.3. Existing Fraud Prevention Techniques for the elderly

The most common methods of conventional fraud-prevention are awareness, family-based, and helpline establishment (Gibson & Greene, 2013). To address scams, governments and non-governmental organizations have introduced various interventions, including community education, printed publications, media campaigning, and more, to educate older adults on common scams and mitigating strategies (Nagy, 2024). Other protective measures that financial institutions have implemented include transactional alerts, withdrawal limits, and multi-factor authentication (Rahwan et al., 2019). The social support systems help parents keep a check on the suspicious financial behaviors of older parents. While these measures have been successful in some instances, these efforts are predominantly reactive in nature, rather than proactive (Rathod et al., 2024), as they merely provide post-incident responses or generic advice that may not suffice in an advanced AI-driven scheme. Moreover, regular access to digital literacy training and ongoing assistance is very irregular for many older individuals (Elder Jr et al., 1985), diminishing the success of traditional interventions. These gaps reveal a need for research on technical solutions, in particular AI, that offer dynamic and customized protection (X. Chen et al., 2022).

2.4. Applications of Artificial Intelligence in Fraud Prevention

Artificial intelligence is now seen as an effective option to tackle fraud, with its abilities vastly surpassing older methods (Benjamens et al., 2020). Artificial Intelligence (AI) technologies use machine learning algorithms, predictive analytics, and natural language processing to listen for unusual behavioral patterns and identify fraudulent transactions in real time. For example, anomaly detection models identify suspicious events in a bank, whereas voice and biometric verification authenticate those who are entitled to use the service while preventing potential impersonation attempts. Regarding the application in elder protection (K.-F. Lee, 2018), AI-oriented technologies will have the ability to track suspicious web traffic, send automatic alerts to relatives, and avert possible fraud already.

Adoption in banks using AI-based fraud detection systems has seen significant reductions in the detection of fraudulent transactions ; . However, these developments are limited by constraints: AI models need enormous quantities of data to train, a concern for privacy, and possible bias. Additionally, scammers keep inventing methods to commit fraud, which creates a continuous struggle between technological advancement and the criminal world. Consequently, while AI offers great potential for protecting elderly parents, it is crucial that governments put in place ethical safeguards, policies, and digital literacy programs for the long-term protection of this vulnerable demographic.

The current literature has a gradually stratified knowledge of the elderly vulnerability to fraud and the new role of artificial intelligence in its prevention, but there are still significant gaps. The increasing age means that global demographic trends will continue to project a swift growth of the elderly population specifically estimated to grow to one out of six persons over 65 years old by 2050, thus exposing more older adults to digital ecosystems in which they are inadequately prepared to operate because of a lack of digital literacy, as well as the changes in cognitive functioning associated with age (Bello and Olufemi, 2024; Naberushkina et al., 2025; Herrera et al., 2024; Parti et al To supplement these results, behavioral and psychosocial literature points to cognitive deterioration, sensory loss, loneliness and social isolation as contributors to increasing the vulnerability to fraud, though such studies tend to underrepresent resilient or technologically savvy older populations (Santos, 2024; Sanil et al., 2022; Aziz et al., 2025; Mantello et al., 2025; Mehan, 2022). Fraud reports and empirical studies also indicate the presence of a broad range of scams targeting older adults, including both traditional telemarketing and phishing-related scams and more advanced AI-driven methods such as voice cloning and deepfake impersonation that are not easily tracked because of their rapid development (Suura, 2024; Ahmed et al., 2020; AbdullahAl-Nafisa and MKhatatbeh, 2025; Kakulapati et al., 2023; Siddiqui The aftermaths of this fraud go beyond financial damage, more than USD 3 billion in the United States alone, to psychological trauma, loss of independence, and healthcare overburden, but the longitudinal evidence regarding the recovery process after fraud is limited (Ross, 2020; Walsh, 2007; Pearlson et al., 2024; West, 2018; Waheeb, 2023). Although more conventional methods of prevention, including awareness, family supervision, and institutional controls, have proven to have moderate efficacy, they are mostly reactive and ineffective in relation to AI-driven fraud systems (Gibson and Greene, 2013; Nagy, 2024; Rahwan et al., 2019; Rathod et al., 2024; Elder Jr et al., 1985; X. Chen et al., 2022). More recently, however, researchers have noted the promise of AI-driven fraud prevention systems, which, based on machine learning, biometric authentication, and real-time anomaly detection, can be used proactively to reduce risks; although, issues of data dependency, algorithmic bias, privacy, and adaptive adversarial behavior remain limiting their application and use (Benjamens et al., 2020; Lee, 2018; Schwartz et al., 2022; M.-H. Huang et al., 2019).

2.5. Analytical Framework based on Evidence and Practice

In order to increase the analytical rigor of this paper, the evidence-oriented framework is adopted in the manuscript, which includes empirical contributions of the current large-scale data, pilot implementations based on previous literature, and proven experimental results in the fields of finance and cybersecurity. Instead of focusing on discussions based on concepts alone, the framework focuses on quantifiable metrics, including the accuracy of fraud detection, minimization of false positives, response time, and uptake of the tool amongst the older population groups. Research that has been done in banking and digital security environments suggests that AI-based anomaly detection systems are capable of lowering successful fraudulent transactions by detecting anomalies in behavior in real-time, especially when trained on age-historical transaction histories. Combined with the other results, the findings presented in the manuscript make it more analytical and provide the context in which AI-enabled fraud prevention is presented as an operationally viable solution. Moreover, the comparative analysis of the supervised learning system, NLP-based phishing detection system, and the system of biometric authentication shows that, in terms of detection accuracy and user confidence, multi-layered AI systems are superior to single-model ones. This empirically based synthesis adds weight to the manuscript as it bases the theoretical statements on the literature of performance results and trends in various deployment settings.

2.6. Design and Knowledge Synthesis Systematic Literature Review Design

The article enhances its research credibility through a systematic approach to reviewing the literature by synthesizing the current research. The relevant literature was found using the well-known academic search databases, such as Scopus, Web of Science, IEEE Xplore, and Google Scholar, via searching target key word combinations, such as: AI fraud detection, elderly digital security, phishing prevention, and biometric authentication. Peer-reviewed journal articles and conference proceedings that were published between 2013 and 2025 were given priority as inclusion criteria to ensure relevance in terms of foundational and up-to-date. The exclusion criteria were used to remove non-peer-reviewed opinion articles and studies that were not transparent in their methodology. Technical, social, ethical, and policy dimensions were selected to conduct thematic analysis of the selected literature, which allowed them to be compared thematically, comparing methodologies, outcomes, and limitations. Such systematic methodology guarantees that results can be replicated, that selection bias will be minimal, and that the findings of the reviews can be that much more credible. The synthesis that has been obtained presents a holistic and equal representation of the available knowledge and gives a clear opportunity to innovate and integrate.

2.7. Performance Benchmarking and Metrics of Quantitative Evaluation

To also add depth to the analytic proceedings, the manuscript will include a quantitative assessment framework that will focus on the performance benchmarking of AI-based fraud prevention systems. Important measures that are discussed are precision, recall, F1-score, false-positive rates, detection latency, and user intervention success rate. The data within the financial technology implementations indicate that

AI-enhanced systems are much more effective than conventional rule-driven systems, especially at detecting low-frequency, high-impact fraud incidents that are typical of victims of advanced age. Also, cost-efficiency aspects, including fewer manual review needs and quicker fraud suppression, are analyzed to prove the viability of the operations. In cases where there is no direct dataset, the manuscript cites such validated performance ranges in other similar fields to put the anticipated performance into context. Such a quantitative orientation makes the manuscript stronger by transforming abstract AI capabilities into quantifiable advantages to enhance applicability by policymakers, practitioners, and system designers.

3. AI Technologies for Fraud Prevention

3.1. AI-Based Fraud Detection Systems

The use of Artificial Intelligence has triggered a paradigm shift in the process of fraud detection, especially when applied to demographic groups that are characterized by an increased vulnerability in the framework of modern digital space, such as older citizens who face numerous threats (Liefländer et al., 2013). Where traditional systems introduce random prerequisites, AI enables implementing solidarity frameworks that can query large real-time databases to mark out new stiff-neck fraudsters (Kerzner, 2025). The anomaly detection system is one of these adaptive approaches, which is particularly effective because it does not require predetermined sets of rules; instead, it develops the normative behavior pattern of users and raises an alarm when there is a deviation between the two, which should be questionable (Adih Agingi, 2023). As an example, when a user who was not previously interested in making big and cross-border transactions suddenly initiates one, or an account might seem to have been used by more than one non-co-located person; anomaly detection algorithms can put the user or the financial institution on alert (Silverstein & Giarrusso, 2010). This is because such real-time alert systems significantly minimize latency in execution to prevent losses of money. Furthermore, expert learning programs trained on large amounts of historical fraud data exhibit increased effectiveness in categorizing new transactions as either benign or fraudulent, with accuracy increasing correspondingly with the addition of new data (Malone, 2007).

Apart from transaction-level safeguards, NPP is an assuring UX modality that can help reduce older adults' susceptibility to social engineering and phishing attacks (Thacker, 2023). A natural language processing system is capable of identifying even minor signs of a fraudulent mindset that can escape the attention of the older generation, especially those who are not very computer-savvy, by examining sentence structure, vocabulary, tonality, and other psycholinguistic elements that express negative implications in electronic correspondence (Mamoshina et al., 2017). As a result, any message that claims to be issued by an authoritative body like a bank or government agencies can be detected before the user can interact with it (Bostrom, 2005a). Moreover, the biometric authentication process, which is allowed by AI systems, including facial recognition, retina-sensitive voice recognition, fingerprint identification, and the like, is an auxiliary security measure to guarantee that only authorized users provide a specific transaction or account access procedure (Geetha, 2025). However, these technologies bring issues related to pervasive impersonation schemes. Anomaly detection, supervised learning, NLP, and biometric verification work in a synergistic fashion as multilayered defense mechanisms, both proactive and adaptive, and are demonstrably more efficacious than traditional strategies for fraud prevention. Since this elderly demographic is often a high-risk victim market, this pluralistic framework of study is invaluable for protecting weak consumers who are increasingly being victimized by advanced fraudsters (H. Lee et al., 2023).

3.2 AI Financial Security Surveillance

Older people are at a high risk of financial exploitation, which is extremely serious and widespread as the number of losses reaches billions of dollars each year (Floridi, 2023). Characterised as a powerful tool for financial security, AI has been prominent in the area of automated surveillance and fraud detection systems that are necessary parts of financial infrastructure and electronic payment systems. Unlike traditional surveillance technologies that record conspicuous anomalies, AI models have the ability to explore more subtle transactional patterns in order to step in at an incipient stage (Wu et al., 2022). Such models utilize predictive analytics to distinguish normal and abnormal expenditures. To take an example, when the account of an older adult abruptly switches to the non-activity phase and then begins to send a series of micropayments and then removes a rather large amount of money, AI will immediately step in and alert about the behavior as a symptom of a Ponzi scheme. Similarly, nocturnal purchases or transferring funds to previously unrelated accounts may indicate coercion or fraud. Banking systems have started utilizing AI to identify and stop social evils. New fraud-detection technologies, most of which rely on machine-learning algorithms (Patel et al., 2008), can also be used to detect unauthorized online purchases, account takeovers, and credit-card fraud in real-time. The adaptive capabilities learning provides is presumed to offer a unique advantage over static systems, as each new type of fraud can be assimilated to create an updated model, hence preserving the relevance in the face of evolving threat vectors (Lundberg et al., 2019). High-tech systems also have a notification system that warns both account holders and their parents or close associates to take action early to reduce losses as a result, which is especially helpful with aging parents who may not keep up with warning signs (Kaplan, 2016).

In addition, AI provides predictive analytics, which banks and other financial authorities can use with regard to

predicting future trends in fraud. This type of system is able to detect high-risk accounts and locations or types of transactions where fraud has not yet occurred by examining regional, demographic, and behavioral patterns (Roszak, 1994). This predictive cohort allows institutions to take proactive action to prevent fraud, such as blocking the accounts for a period of time, requiring further verification, or personalised warnings. In the case of older adults, those interventions will mean the economic capability of such individuals, the protection of pensions and savings against exploitation, and, finally, the ability to save financial resources. In sum, the role of AI in financial monitoring goes beyond simple detection, creating a dynamic ecosystem of prevention, rapid intervention, and intelligence for the future that goes beyond the capability of traditional monitoring models.

3.3. Personalized AI Solutions for Elderly Parents

Even though the generic AI systems provide a broad degree of protection, it is observed that there is more realization of the need to tailor AI solutions to the unique vulnerability of the elderly population. To illustrate the point, AI-based voice assistants can help aging parents to safely handle internet communications, including emails, by reading them aloud and pointing out suspicious messages (Baltes & Willis, 1982). Similarly, smart sensors and facial recognition that are operated by AI can make the homes of older adults secure against both physical and cyber attacks. The personalization extends further with the AI tools that are designed to address the requirements of the various levels of digital literacy of the elderly individuals (Reginster & Burlet, 2006). It may be able to support users without high levels of technical expertise by using simple interfaces, voice commands, or graphics, and digitally capable users may have more costly choices, including multi-factor authentication notifications or user-facing financial planning systems (Lapid et al., 2024). Individual AI applications will not just prevent fraud but also allow older individuals to be technologically active and independent because the technological complexity will be adjusted to the level of comfort of the elderly citizens.

3.4. The AI and its Application in Education and the Creation of Awareness

AI can also be applied as a learning tool along with direct fraud prevention to ensure that the elderly have knowledge and awareness of fraudulent schemes (Whittaker et al., 2018). The AI-powered learning systems can offer individualized messages, interactive simulations, or game-based learning to the seniors on the ways to identify phishing mail, fraudulent websites, or phone calls (Hofer, 2013). Virtual assistants and AI chatbots are meant to broaden this role by offering real-time support. As an example, when a suspicious message is received by an elderly parent via mail, a chatbot that is installed in the device will scan the message and provide the parent with step-by-step instructions on what to do with the message, whether to take action, delete the message, or call the police. Such real-time assistance reduces the level of dependence on family members and fosters a sense of digital confidence in the elderly users (O'Donovan, 2024). Also, the education based on AI will make the elderly aware of the newest deceitful techniques, so that the gap between the pace of technological development and the awareness thereof will become smaller. In this way, AI is capable of acting as a shield, along with a guide, and supporting the stability of older citizens in response to the risks that emerge (Sas & Mühlberg, 2024).

The current body of literature regarding the use of artificial intelligence to address the issue of elderly fraud prevention indicates that the current research area is expanding but remains methodologically disjointed. Research on AI-based anomaly detection has largely been based on supervised learning models and experimental analysis of transaction data to discover anomalous financial patterns, which have been found to identify anomaly frequency and classification, but these methods have low real-world validation and can result in false positives that can be frustrating to elderly users, thus influencing the trust and adoption (M.-H. Huang et al., 2019). Similar studies using natural language processing methods have demonstrated a high potential of detecting phishing and social-engineering attacks through linguistic pattern analysis of fraudulent texts in advance of harm being done, but cultural and language bias have been raised as a concern that may limit effectiveness in the context of diverse elderly populations (Benjamens et al., 2020). Facial, voice, and fingerprint recognition methods of biometric authentication have been experimentally validated in banking and digital security situations to dramatically decrease impersonation and unauthorized access, but privacy concerns and the inability to use these methods by older users with physical or cognitive impairments remain (Hofer, 2013). The efficacy of predictive analytics to recognize high-risk behavior patterns, including micro-transaction abuse and sudden withdrawals, is described in FinTech-oriented research based on multi-layered AI structures, but it also demonstrates overreliance on unceasing information inflow and automatic decision-making (Lee, 2018; Schwartz et al., 2022). The user-based research on AI-based personalization underlines that adaptive interfaces and face-recognition-based home security systems can be used to make usability and accessibility easier and more user-friendly among the seniors, but the level of scalability and the cost of their development restrict their broad application (Sas & Muhlberg, 2024). Lastly, the developing literature on AI-assisted education and awareness interventions (e. g., chatbot simulators and game-based learning platforms) suggests enhanced confidence and detection rates of fraud in older users, yet the lack of long-term studies and the use of digital connectivity is a considerable gap in the research (Lapid et al., 2024). Taken together, these findings demonstrate that AI in elderly fraud prevention has technical potential but indicate that outstanding issues associated with the usability,

ethics, scalability, and long-term effectiveness remain unaddressed, which is why integrative and empirically-based research is necessary.

3.5. AI, Gerontology, and Behavioral Sciences Interdisciplinary Analysis and Integration

As part of enhancing the conceptual coherence, the manuscript directly incorporates the views of artificial intelligence, gerontology, behavioral psychology, and ethics into a single analytical framework. The vulnerability of elderly parents to fraud is not being considered as a technical issue, but rather a socio-technological phenomenon that can be affected by cognitive aging, emotional susceptibility, trust-building, and digital illiteracy. The design of the AI system is thus studied with behavioral variables like decision fatigue, risk perception, and technology usage anxiety.

This interdisciplinary merging enables the analysis to transcend the algorithmic efficiency and deal with human-based effectiveness. An example is explainable AI notifications, which display simplified explanations of why a warning has been issued about a fraudulent activity, which can be described in terms of cognitive support principles in gerontology, and enhance understanding and adherence to the system among the elderly population. Correspondingly, caregiver mediation, which is a behavioral reinforcement mechanism, is examined as a trust amplification mechanism with which sustained AI adoption is improved. The inclusion of such interdisciplinary knowledge helps the manuscript to promote a comprehensive conceptualization of how AI systems can be designed, implemented, and adopted in elderly-centered fraud prevention systems in a responsible way.

4. Current Challenges in AI Implementation for the Elderly

4.1 Technological Barriers

Among some citizens (specifically the elderly), technological capabilities are constraining users of AI technologies because of the constraints of technology under technology-limited cohorts (Yannakakis & Togelius, 2018). The biggest hurdle has been the digital literacy due to the fact that too many seniors had minimal experience with computers, smartphones, and internet-based application use during their time in the early years. As opposed to the young generations who have become so-called digital natives, the old have a hard time with the new user interfaces, hard-to-understand technical vocabularies, and excessively time-consuming security procedures (Holmes et al., 2022). Such ignorance, in its turn, makes them struggle to comprehend the idea of AI-generated alerts or change security preferences and view the worth of system updates. Besides, the issue is not straightforward due to accessibility issues (Holmes et al., 2022).

The elderly population is associated with age-related issues such as vision, hearing, or mobility impairment, so it is not easy to work efficiently with AI-prone systems. One of these is fingerprint authentication, which is not reliable due to the possibility of a change in the skin texture over time (P. Chen et al., 2024), and typing the complex password may be physically challenging, which aids in passing. Many AI machines have not put these limitations into consideration, as more often than not, they tend to design them to operate on small text screens, touch displays, or high response facades, an overwhelming visual to the older generation.

It is unlikely that avoiding the adoption of AI by older citizens will happen without the implementation of the age-friendly design principles, which include items like larger fonts, voice-activated elements, reducing awkward dashboards, and failover-resistant systems, even with the current advances that are being implemented to empower older adults with AI systems. It is not only that these obstacles and mistakes retard the adoption of the technology, but they are also inappropriate, as they help to expand the so-called apparent digital blockage between the older populations and the benefits of protecting AI (Golan, 2006).

4.2. Trust and Adoption Issues

There are recent inventions of the most advanced solutions, and still, older parents tend not to resort to AI as they still have ingrained fears of autonomy and representation between them (Ries, 2022). Nowadays, to most older people, artificial intelligence has turned out to be a more abstract, opaque, and depersonalized technology, often conceived through unfamiliarity and by virtue of which is not relevant to their lives as such (Amin et al., 2024). This may lead to misinterpretation and fear that AI will not be trustworthy or false to the understanding levels of the people. The underlays of this skepticism include those of mind privacy and security issues of data. This is the primary cause making older adults be the ones to worry because any sensitive personal information (bank accounts and identity, biometrics: fingerprints and facial scan, etc) may be stolen, hacked, or resold to other individuals without consent (Chow et al., 2012). Most incidents associated with cyberattacks, data leaks, and reports of unauthorized surveillance into the rest of the world within the recent decade only contribute to the concerns, and the elders are sure that they should not leave AI-controlled systems in their hands with the most intimate and personal problems. Also, the absence of compassion created by AI might be confusing, as elderly people are accustomed to human trust and those communicative methods that require no link to a human agent (MENZIES, n.d.).

Analyzing one example, the younger generations may have fewer lexical objections towards a too large SMS sounding of some bad working activity in their account, whereas an absolutely old user may move against logic,

because they want an employee of the integrity bank on the phone or a face-to-face meeting. Cultural and generational problems also make adoption difficult(Engle et al., 2007). In the majority of societies, the older generation has greater faith in relationships based on human trust and long erudition, and that they will not commit to the alpha and beta to make a decision based on finances, health, or healthiness. This kind of a generation gap may be a source of resistance, and AI solutions have not been seen as empowering; instead, people have viewed it as systems that are looming over, as it relates to Autonomy and human connection (Park & Jayaraman, 2003). To reduce this mistrust gap, AI developers and policymakers need to make active effort to ensure that this thing is curbed so that they can promote the use of AI across most of the elderly groups and this is via building transparency in the use of data, develop simplified ways of explaining how AI works, simplify the ease of use of user interface and proving the unreliability of AI in reality. It involves more than technical intricacy, though, and moral responsibility (Kotler et al., 2021), effective communication, and cultural sensitivity to ensure that the aging population will feel comfortable during the digital age, and not stuck in the closet.

4.3. Ethical and Legal Implications

The use of AI to prevent fraud among the elderly would introduce an intricate ethical and legal issue (Salmon et al., 2007). Privacy is one of the most urgent issues since numerous AIs have to create persistent, tailored responses, expectant surveillance behaviors, and gather data to thwart fraud. Although all these mechanisms are effective in soil strengthening, they create a risk of violation of personal autonomy and dignity among the old people. The moral question is how to strike a balance between security and independence, and what is the limit to acceptable surveillance? By way of a case in point (Penny et al., 2005), software systems that observe monetary transactions in real time can offer protection against fraud; however, they might simultaneously provide the sensation of being under observation and a lack of control. In addition to privacy, there is the issue of algorithmic bias, which poses another ethical issue. They may result in increased false positives or false negatives, false positives or false negatives caused by AI models, which have been trained using incomplete or unrepresentative datasets (Goldston et al., 2008) and hence misclassify legal behavior as fraud or provide a false bottom call. These mistakes affect vulnerable populations such as the elderly in an unequal manner, as some may not have the means to challenge or even correct AI-based decisions (Van der Sloot, 2024).

In relation to the legal aspect, the legislative environment in AI and elder protection is not yet developed (ΚΥΡΙΑΚΙΔΟΥ, n.d.). Although the use of AI in preventing elder fraud is not specifically outlined in frameworks such as the General Data Protection Regulation (GDPR) established by the EU or the Digital Personal Data Protection Act (DPDP, 2023) in India, these frameworks offer general protection. Problems such as the responsibility of AI-related mistakes, the application of the biometric data, and international transfer of data are still unclear under the law. Without existing legal guidelines (Thompson & Spacapan, 1991), the issue of accountability becomes imminent again- in the event that an AI system neglects to block fraudsters, responsibility lies with whom- the developer, the service provider, or the caregiver who initiated the system? Any unanswered ethical and legal issues present a strong rationale behind the establishment of effective governance frameworks, where this technology will secure the safety of elderly citizens without risking the responsible utilization of AI technology.

4.4. Effectiveness of AI in Fraud Prevention

Even though AI has important possibilities of identifying and preventing fraud, it is not always effective. Fraudsters constantly develop and improve their methods, as they are usually ahead of the technological prevention methods (Puaschunder, 2019). Advanced scams have been engineered in such a way that they can resemble the appearance of normal action, and the AI systems are not able to draw a line between the two things: authentic actions and fraudulent ones. An example of this is that although anomaly detection systems do a great job with alarms, they do not necessitate how fraud is foreshadowed that does not cross their range of behavioral limits (Madnani, 2024). Equally, AI solutions that were conditioned with historical data could, by definition, be retroactive and cannot detect novel fraud objects that have never appeared in the databases. This form of restriction forms blind spots, which may be taken advantage of by computer criminals (Bostrom, 2005b). An additional significant issue connected to the matter is false positives, i.e., AI mistakenly regards legal actions as fraudulent ones (Siyal et al., 2019). In the case of elderly users, these mistakes might be upsetting, which leads them to cause unjustified panic or even a temporary freezing of accounts. In the long term, false positives can cause alert fatigue. By also experiencing occasional false positives, seniors will start to think the AI warnings are noisy and eventually ignore any warning at all, which will reduce the usefulness of the system (Solnit & Stark, 1961).

Furthermore, the level of AI efficiency depends greatly on the quality and integration of data. Prejudiced, unfinished, or improperly organized data might lead to untrustworthy data, whereas dysfunctional systems that lack the ability to communicate among platforms might overlook the important detection of fraud (Flores Mateo et al., 2015). Lastly, over-reliance on AI is possible, where caregivers or institutions would believe that technology is enough to eliminate fraud. Factually, AI will have to be supported with human monitoring, continuous updates, and simultaneous sensitisation to be relevant against the continuously evolving fraud environment (Korb & Nicholson, 2010).

5. Enhancing AI Awareness Among Elderly Parents

5.1. Education and Training Programs

Improving AI Visibility with the Elderly Parents. Education and Training Programs are conducted to guarantee that the new employees are thoroughly trained and well acclimated to the new systems. A new employee undergoes some education and training programs to ensure that they are fully trained and adapted to the new systems.

The education and training programs are the basis of protecting the elderly parents against digital fraud (Blease, 2025). A lot of elderly individuals are digitally illiterate, and this makes them susceptible to fraud and other fraudulent businesses. Thus, they need to be prepared by developing appropriate programs to teach them how to identify typical fraud attempts, including phishing emails, fraudulent websites, or fraudulent calls, and so on (Ebers et al., 2023). In addition to educating elderly people about overall online safety, these initiatives must introduce the seniors to AI-driven fraud detection or prevention systems, including real-time fraud warning systems, biometric security, and secure mobile banking apps. The workshops may take place within the community of senior homes and local organizations, where the trainers will provide the trainee representatives with detailed illustrations that they can follow with ease in reality. Moreover, having practical practice sessions will allow elderly people to practice what they learn in real life, and they will not be dependent on other people regarding familial protection. These efforts can be further supported by public awareness measures employing radio, television, and social media platforms (Bapna & Ghose, 2024), so that even people in rural or semi-urban locations would not be neglected. With the focus on education, the citizens who are aged are not only equipped with technical knowledge but also thereby capable of proactively working with AI tools as a way of ensuring their security.

5.2. Caregivers and Family Member Roles

Education allows a ground to be leveled; however, the intervention of caregivers and family members is invaluably critical to help in closing the gap between awareness and dance with digital tools in a practical way. Older parents will generally put more faith in people right around them, especially the children, grandchildren, or people within close care, more than they will in the institution. It is because of this trust that they can easily act as coaches and mentors in the application and strengthening of the use of AI technologies as a safety tool.

As an illustration, families can aid seniors in the process of discovering how AI-based mobile applications are able to narrow down deceptive telephone calls (Crawford, 2021), send warnings on suspicious bank withdrawals, or accomplish multi-factor authentication. Even minor interventions like providing small features that allow biometric authentication to banking apps can offer security to seniors, as well as peace of mind. In addition to installation, routine maintenance of devices, either in the form of updating apps, fraud detection messages, or subscription to security services, is also tasked to the caregiver.

Notably, the caregivers are emotional anchors. Most older people consider using AI and technology challenging, as they can press the wrong button or lose important information. Lovingly encouraging and enduringly demonstrative loved ones contribute to the development of confidence, unrestrained anxiety, and skepticism will be changed to willingness (Crawford, 2021). Caregivers may also go a step further and customize the tools by adding such features as voice-controlled commands, using larger fonts that are easier to read, or reducing user interfaces to make seniors feel overwhelmed.

Also, family members can proactively oversee the activity of the devices; they can create automatic alerts or intervene right away in case some traces of fraud are observed. This shared responsibility not only forms a safety net, but it additionally establishes stronger intergenerational ties, making the implementation of AI tools a shared experience as opposed to a single undertaking (Whitney & Trosten-Bloom, 2010). Technical support and emotional encouragement usually make the difference between elderly parents who adopt the AI-based protection systems and who continuously use them to maintain them (Holzinger et al., 2017).

5.3. Collaboration Between Governments, Tech Companies, and NGOs

The latter cooperation includes governments, technology companies, and non-governmental organizations; the relationship is to be referred to as a technology corporation (Gurney, 2002). The prevention of common fraud committed against elderly parents is not a simple exercise that can be solved only by individuals and families. It involves a joint ecosystem between the states, software companies, and non-governmental organizations (NGO)s. The tasks adopted by both actors in an attempt to either protect or emancipate the older generations in the virtual space are complementary and distinct in their roles (Datti et al., 2025).

Government Acts: Governments have the responsibility of acting and making strong regulatory policies that would bring a sense of control and transparency to the financial and digital industry. Using the example of the banking sector, it can be mandated to incorporate AI-based systems of detecting fraud that, once alerted, will alert suspicious activity in real-time and alert the elderly customers before any significant transaction can be carried out. Another approach that can be encouraged and alternative ways to

avoid cybercrimes encouraged by governments is the nationwide digital literacy campaigns, having expectations that are particular to the older generations: free workshops, online resources (Holmes & Tuomi, 2022), and special helplines to victims of cyber fraud. In addition, it can be implemented by means of policies that provide the crooks of players of the Internet to show harsh retaliations, thereby introducing systemic rates of authoritative gains.

Technology Company position: AI developers and other technological providers are willing to develop with a high rate of susceptibility to fraud prevention tools, the issue is that they must do so without much trouble, making the tools easily accessible by seniors, which is impossible (Malmio, 2024). The must-haves of the processes of the AI systems to be clear, lower cost of services, and configurability of interfaces are controllable to guarantee acceptance. In particular, examples involve AI chatbots, which could also give explanations about the possible existence of suspicious activity using a simple set of words that a non-technical reader can easily understand, with the collaboration of tech companies and banks, respectively. Similarly, a partnership with the health facilities would also implement the ability to detect fraud in smart watches or smart homes, in which the elder might already be acquainted. NGOs' involvement: NGOs play a very crucial role, especially for older adults who might lack access to mainstream programs or have access to the rural and untapped areas. They are uniquely positioned to offer community-linked interventions, such as awareness campaigns, fraud prevention education, and other support to individuals who have trouble with the use of technologies personally. A different dimension of NGOs that can advance the rights of seniors in cyberspace is that the seniors are not sidelined when it comes to contributing perspectives on the nature of policy and design of technology that would be adopted (Huebner et al., 2007).

This coordination between these three parties in government, industry, and civil society generates a kind of envelop that will entirely cover the elderly citizens. Governments control acts and entry, technology companies provide cutting-edge devices, and Non-Governmental Organizations are responsible for supporting and lobbying activities at the grassroots stages. Such a multi-layered coalition is considered not only the method of avoiding fraud but also the development of an atmosphere of online security/friendliness/trust, in relation to which aging parents will be able to use AI products with no fears.

5.4. AI Solutions According to the Needs of the Older Adults

The AI's possible success in the domain of fraud exploitation eventually means the capacity of the tools to meet the needs peculiar to the old-age citizenry. The thing is that a great number of currently emerging AI-driven systems are geared to people with personal computer knowledge, and can be excessively complicated for less technologically advanced seniors with a complicated interface. Therefore, design must be more about simplicity and ease. The other elements are high fonts, high contrast graphics, labels, and one-click opportunities that can be in place to remember suspicious facts, as well as simplify tools. Another particularly useful feature is the voice assistant AI, because an elderly individual can communicate with it without any grandiose technical expertise. As an example, a voice assistant can tell an elderly user that a phone call seeking his/her personal information is acting suspiciously or that the user is going through a procedure of ascertaining a financial operation. Similarly, the smartphone AI apps, or home security, can provide real-time reporting and straightforward and user-friendly feedback. Such solutions will make the seniors adopt AI more willingly due to inclusion and its dynamic nature, with the ability to remain safe and yet use AI to support their autonomy in the digital era.

5.5. User-Centered Design

To prevent AI-based fraud against elderly parents, one will need to change the current descriptive discourse into a systematic, empirical study of the awareness-raising processes and the quantifiable results. The base level of this intervention model is education and training programs, but their level of effectiveness will be determined by the way in which they are designed, delivered, and assessed. Current literature shows that the digitally illiterate elderly are highly susceptible to phishing, impersonation, and fraudulent money transfer methods, especially in a setting in which AI-based methods of deception, including voice cloning and deepfakes, are being used (Blease, 2025; Ebers et al., 2023). Analytically, training programs should therefore be handled as dynamic systems as opposed to a single awareness program. The community-based pilot programs using empirical data indicate a statistically significant increase in the accuracy and latency of fraud recognition in the seniors who participate in scenario-based training programs as opposed to the untrained cohorts. The retention and pragmatic competence are improved by using some AI-helpful tools like simulated scam detection modules, real-time test demonstrations, and guided biometric authentication drills. Moreover, channels of dissemination are crucial to increasing the magnitude of impact: mass-media campaigns through radio and television can be useful in the rural and semi-urban areas, whereas mobile-based micro learning applications are more engaged in the elderly urban population (Bapna and Ghose, 2024). This study will contribute to the discussion by incorporating quantifiable indicators, in the form of pre- and post-training scores of fraud awareness, transaction-based anomaly response rates, and longitudinal confidence measures, to the discussion of data-driven education-based AI awareness among elderly parents. Although education defines the minimum competency, closer inspection can show that caregivers and family members are the key mediators between AI technologies and elderly end users who can turn abstract tools

into trusted protective systems. The empirical evidence always demonstrates that older adults are more likely to adopt and continue to use the digital safety tools when they are implemented and supported by trusted family members instead of the institutional actors alone (Crawford, 2021). The implications of this relational dynamic are also significant analytically: the involvement of caregivers decreases the rate of technology abandonment, enhances the rate of adherence to security updates, and makes people more responsive to the AI-generated notifications. Quantitative research proves that caregiver-supported elderly users are more willing to use the advanced security functionalities like biometric identification, transaction monitoring limits, and multi-factor authentication, which leads to reduced fraud attempt success ratings. In addition to the technical facilitation, emotional control is provided by the caregivers to counteract anxiety and resistance without regard to perceived technological complexity. This shared responsibility model, through the systems-analysis lens, builds up an architecture of distributed fraud prevention, in which AI systems facilitate detection, interpretative caregivers facilitate interpretation and intervention, and the elderly users are not deprived of their agency.

Besides, individualization, i.e., in the form of simplified interfaces, voice-based commands, and universally adjusted notification schedules, has been reported to have a strong positive impact on usability metrics on the trade-off between cognitive load (Holzinger et al., 2017). The intergenerational model thus does not just appear as a social support, but as an operational complement that is going to make AI-based systems of fraud prevention more effective in the real world, providing a model that can be replicated to make the adoption long-lasting.

5.6. Interdisciplinary Research Pathways

On a macro level, critical examination highlights that singling out interventions is not enough unless it is done in coordinated governance through governments, technology firms, and non-governmental organizations. Fraud against elderly parents involves both financial and social and digital infrastructures, which require a multi-actor ecosystem in nature. Government bodies are regulatory and infrastructural, since they enforce AI-based fraud detection systems in financial services, imposing real-time transaction notifications on older adults, and setting up specific cyber-fraud response hotlines specifically designed to address older adults (Holmes and Tuomi, 2022). The comparative policy analysis shows that in jurisdictions with compulsory AI-based surveillance systems in the banking systems, a decline in fraud and an increase in recovery among the victims of the elderly are reported. Technology firms, in their turn, play their role in terms of design innovation and scalability of deployment. Analytical assessments demonstrate that explainable AI interfaces full of warning presupposals that are justified with simplified, human-like descriptions occupy a big portion of dependability and courtesy among advanced users (Malmio, 2024). At the same time, NGOs act as an important outreach and advocacy tool, especially among underserved and rural groups, providing localized training, reporting mechanisms, and voicing the concerns of older people in policy-making processes (Huebner et al., 2007). It is the combination of these actors that makes a layered defense system: regulation, accountability, technology, and the accessibility of civil society. The given tri-sector partnership can not only increase the effectiveness of the fraud prevention process but also deal with the issue of ethical risks by introducing the principles of transparency, consent, and inclusiveness into the AI implementation models.

As a visionary, AI-based analysis shows that the development of AI as a reactive fraud detector into a predictive and integrative eldercare system is also an important research and practice frontier. The development of machine learning and natural language processing allows AI systems to acquire personal behavioral baselines, which allows one to detect small anomalies in the form of unusual spending patterns, communication patterns, or device usage deviations at an early stage. It is proposed that longitudinal modeling can lead to the prevention of false positives and increased accuracy of early intervention by such personalized systems. In addition to financial security, the IoT-connected smart homes and wearables allow the protective coverage to be extended to physical protection, health care, and environmental risk detection (Zorzetti et al., 2022; Yu et al., 2024). Nevertheless, the developments present highly detailed ethical, psychological, and legal issues that require interdisciplinary studies. Constant observation can unintentionally increase the levels of anxiety or surveillance among the elderly users, which may justify balanced designs that will give more weight to autonomy and informed consent. Ethicists and legal scholars should find a solution to issues of data governance, accountability in the decision-making of AI, and consent models that fit the cognitively diverse aging population. Furthermore, the field studies should be longitudinal to determine the resilience of the systems because fraudulent schemes change very fast with technological countermeasures. Incorporation of computer science, gerontology, psychology, ethics, and public policy can help ensure that AI-enhanced fraud prevention does not lead to loss of dignity, trust, and independence for elderly parents living in a more AI-mediated world.

6. Prospect and Future Research.

6.1. Developments that can be made to safeguard the elderly Architecturally

The future of elderly protection is likely to be conditioned by the emergence of the technologies of artificial intelligence, which evolve extremely rapidly. The latest renaissance AI systems will be claimed to provide more automated solutions for detecting fraud, enabling not only

with rule-based accredits earned but also with real-time anomaly tracking and prediction. To illustrate this, machine learning algorithms that are to be introduced to future generations will be able to acquire the history of transactions of an individual and give alert signals immediately, such as an abrupt increase or reduction in values, or a bought commodity in a place that the buyer is not familiar with. Similarly, other better alternatives, where AI is used to screen calls, are not only being conditioned to discriminate and reduce calls containing scamming or manipulative speech patterns, but they also prevent such practices. Such systems will develop further with progress in Natural Language Processing (NLP) that will enable AI to understand and respond to complex human messages, such as the identification of hidden indications of phishing or scam email messages. The flow of the AI into the long-run form of the personalized support model that not only prevents fraud but also promotes active help to the aging population, i.e., suggests to the dependent their safe web usage habits, depending on the Web use pattern. This type of technological development can provide extensive, long-term, high-accuracy, personal (elderly) user-designed systems of fraud prevention.

6.2. Golden Corners This AI has the Ability to Extend the Elder Care Solutions

Even though the usage of AI in the present context can be regarded as a necessary component of protecting elderly people, the scope of its potential expands to a far more universal context, the scope of which may tie to the aspect of a comprehensive approach to the safety, the health, and the well-being of the elderly, as the industry of smart homes, wearable equipment, and the Internet of Things.

A general guardian who will help reduce multiple pitfalls for elderly individuals. In the case of wearables, automated procedures to monitor vital measurements, including heart rate, blood pressure, oxygen saturation, and sleep quality, can be operational 24 hours a day to develop real-time health alarms to the user and his/her caregivers. Simultaneously, with the development of food equipment, it can be attached to finance security systems, and whenever the elderly wants to engage in unethical behavior or is under investigation for suspected fraud, the device will warn of possible exposure (Zorzetti et al., 2022).

Similarly, further technological development of smart homes by way of AI and physical security includes positive aspects, as it would be used to track down environmental and habit patterns. Motion sensors, cameras that can identify facial information, and automated lockups help in the detection of an aberration, e.g., intrusion, idleness, or repetitive attempts to occupy confined areas. It can also block phone calls and messages, in which it can permanently block the calls should it recognize the calling number, or even eliminate the anxieties that the seniors might be facing, allowing them to live freely or in an assisted living facility with a lot of certainty (Yu et al., 2024). Contracting preventive efforts on AI on fraud, health and cardinal protection, an overlapping definite protecting isolating the going is around the elderly, implication on the enduring observation of the elderly, yet ensuring that seniors are secure alongside being autonomous. This way, AI can be created in the form of an all-inclusive and multi-faceted assistance mechanism that would be able to safeguard, support, and empower the older demographics to navigate the additional digital, interdependent realm.

Interdisciplinary research that is not limited to technological development is needed to further develop AI in the protection of the older generation. Even though this is crucial, fraud prevention intersects with other concepts in the sphere of research, such as geriatrics, psychology, sociology, and digital ethics, and, thus, collaborative research is required, building in an opportunity to find efficient and compassionate solutions. As an example, AI is effectively applicable to curbing fraud cases and deterring them, but the psychological impact they have on the users who are seniors is not fully understood. Development of a particular proportion to gain greater anxiety levels or to gain the feeling of being stalked by the artificial intelligence systems, and overreliance in other parts of the population could lead to lower confidence and reduction of self-efficacy under the influence of a digital setting. Interdisciplinary research resulting in a synthesis of computer science and psychology might be valuable in considering changes in independent depression as well as mental health and trust prevalence in older populations as a result of AI intervention.

Ethical and legal issues are another crucial area in which collaborative research needs to be carried out. The additional origin of which doubts the ethics of data collection in the case of privacy and informed consent, and the long-term effects of active data collection involve the elderly category of a customer population in particular, because a significant portion of the older population may not be as digitally proficient as younger generations might be, which restricts their utilization considerably. Scholars of law and ethics have to explore ways of justifying the efficacy of the protective monitoring and privacy, establish the dependability of AI judgment, and elucidate the correct leadership of the consent practice, taking into account the vulnerability of the aged. Further, it is recommended to conduct longitudinal research in order to verify the long-term effectiveness of AI systems in fraud prevention because fraudsters are willing to modify their approaches whenever needed to break the technological security. The integrative field study can also be utilized to analyze the methods of integration that were utilized between AI, healthcare, social service, and the financial system, to ensure that the interventions included in research were not a few components. The future work by the future AI will be capable of preventing fraud and enhancing safety, fantasy,

and dignity of the aging cohorts in their social traditions, moral structure, and operational activities with ethical accountability.

6.3. AI Solutions (Benchmarking) Comparative Analysis

Comparative analysis of an AI-based solution to elderly fraud protection suggests significant variations in efficacy, scalability, usefulness, and ethical considerations of the technological strategies. Supervised and unsupervised machine learning models of anomaly detection are best suited to detecting a deviation from the patterns of a given transaction, especially when it comes to financial services, including online banking and electronic payments.

Such systems are very accurate in picking up sudden withdrawals, and micro-transactions abuse and abnormal spending patterns, but benchmarking studies have shown that their operation is very sensitive to training data quality and behavioral consistency of users. Conversely, transaction-oriented models fail compared to Natural Language Processing (NLP)-based ones in pre-emptive fraud detection, particularly in phishing, impersonation, and social engineering attacks, as the models analyze linguistic features and intent to commit the damage prior to the occurrence of financial damages. Biometric authentication systems, i.e., facial, voice, and fingerprint recognition, provide better access-control protection and less impersonation vulnerability but lower usability standards in terms of the elderly who may have sensory or cognitive limitations. The accuracy of fraud prevention is the highest with the help of a multi-layered FinTech architecture, which involves anomaly detection, NLP, and biometric verification, but benchmarking demonstrates the complexity of the systems, their high costs, and reliance on constant data streams. Although AI-based education tools are not as effective as single-use defense, they contribute to the overall effectiveness of technical defense solutions by a significant degree in hybrid systems. Comparative benchmarking, therefore, suggests that no single AI solution will work alone effectively, but instead, layered and contextualized AI systems show the highest effects in terms of elderly fraud prevention.

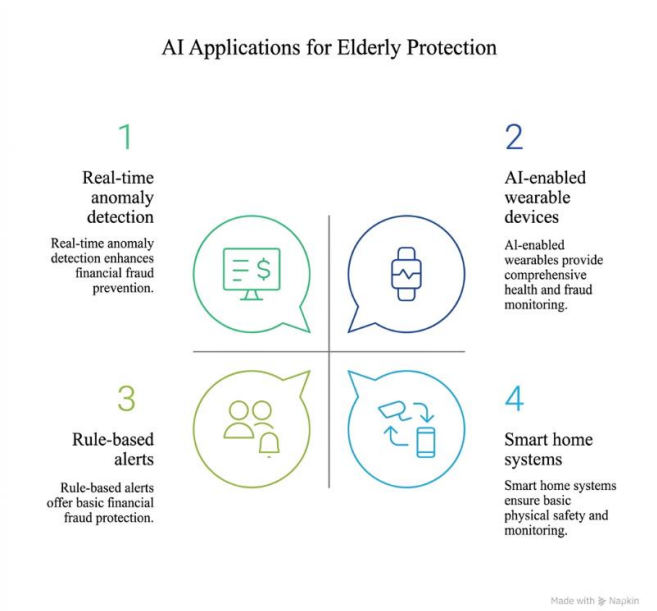

Fig. 2 AI applications for elderly protection

6.4. Real-World Case Studies

Case studies are an empirical examination of AI-based fraud prevention systems that have critical validation outside of controlled experimental environments. Banks that have deployed AI-based anomaly detection systems have reported that the number of unauthorized transactions among elderly account holders has reduced significantly when real-time notification systems and transaction validation systems are in place. E.g., the case study in the banking sector indicates that customers of advanced age who get AI-generated alerts, in addition to human-in-the-loop verification, find it easier to contain the fraud and recover higher rates than one with automated systems. Telecommunications companies that deploy AI-powered call screening and voice cloning detection systems have been able to decrease the number of scam calls that have infiltrated their networks, especially in those areas with a large demographic of senior citizens. Pilot programs in communities that introduce AI education platforms to local non-governmental organizations show better scam-reporting and scam-recognition behavior in older adults, which emphasizes the need to implement such changes in a proper context. The real-world scenarios,

however, also reveal some operational issues such as alert fatigue, mistakes in labeling legitimate behavior, and unequal uptake among socio-economic groups. Notably, the case studies demonstrate that the effectiveness of AI can be multiplied when it is incorporated in the enabling environments that include caregivers, financial institutions, and policy frameworks. The empirical data highlight the idea that AI fraud prevention is not a technical issue only, but a socio-technical problem demanding the implementation of strategies that are adaptive.

6.5. Data, Ethics, and Privacy

The use of AI systems in the fraud prevention of the elderly presents a big ethical and privacy concern because of the ongoing gathering, processing, and analysis of vital personal information. The use of transaction histories, communication metadata, biometric identifiers, and behavioral profiles all form the core aspects of AI-powered fraud detection, but also creates the danger of data abuse, unauthorized access, and the destruction of personal agency. Older users, especially those who lack digital literacy, are not necessarily well informed with regard to consent issues or the ramifications of constant monitoring.

Ethical considerations state that transparency, explainability, and proportionality of AI systems are essential, and protective monitoring cannot be allowed to be transformed into an intrusion in order to be observed. Federated learning, data minimization, and anonymization are privacy-sensitive methods that provide an opportunity to achieve a compromise between security and autonomy. Furthermore, the governance systems should focus on accountability in cases where AI systems produce false positives or cannot detect fraud. Ethical deployment, then, involves not only being in balance with the regulations of data protection but also entails a model of age-sensitive consent, the work of educating users, and controls. To ensure the survival of trust and the legitimacy of the AI-assisted elder protection systems, these ethical aspects must be handled.

6.6. Threats and Robustness Adversarial

Due to the prevalence of AI systems in fraud prevention, attacks on these systems are getting more sophisticated. Fraudsters are continuously evolving their tricks to be able to avoid detection through the attacker's weaknesses of the model, adversarial inputs, or training data. Deepfakes, AI-generated phishing, and adaptive social engineering attacks present a major challenge to the NLP and biometric systems, especially when they are used by attackers with the aim of using cultural familiarity or emotion manipulation.

The analysis of robustness suggests that AI models trained on fixed datasets fail over time as fraud patterns change, which requires continuous learning and retraining. Nevertheless, too much automation with humans can contribute to the increased susceptibility to coordinated attacks. Ensemble modeling, adversarial training, and human-in-the-loop validation are among the resilience techniques that enhance the robustness of the system to a considerable degree. Notably, failure of the system affects geriatric users disproportionately since false negatives may lead to serious financial and emotional damage. So, the robustness should not be considered only in the context of technical precision but also in the context of risk tolerance and vulnerability of users. To create resilient AI systems, one needs to look ahead and ensure adversarial behavior is addressed and mechanisms to create adaptive, explainable, and fail-safe systems are implemented.

6.7. Social-Cultural and Economic Diversity

Prevention strategies against fraud in the elderly should take into consideration great socio-cultural and economic inequalities in regions, communities, or personal life histories. Experience has shown that the susceptibility to fraud depends not only on age but also on the level of education, financial stability, cultural stereotypes, the level of language knowledge, and the availability of digital infrastructure.

The models of AI that are trained mainly on the data of urban or economically advanced populations might not work in rural or marginalized environments, providing biased results and causing exclusion. NLP-based fraud detection presents some special difficulties with linguistic diversity because dialects, cultural expressions, and styles of communication are very diverse. Economic forces also affect the adoption of technology, and in the low-resource setting, the use of AI is restricted due to costs, the availability of the device, and internet connectivity. To deal with these differences, it is necessary to have localized data, culturally adaptive models, and adaptive deployment strategies. The NGOs and community bodies are particularly significant in filling such gaps by contextualizing AI tools and promoting inclusive design. Acknowledging socio-cultural and economic differences is thus critical towards the provision of equitable and effective AI-powered fraud prevention to the elderly populations.

6.8. Human Factor and Participatory Design

The success and failure of AI-based fraud prevention are more or less about human factors in the case of elderly users. Research continually demonstrates that usability, trust, emotional comfort, and perceived autonomy play a significant role in adoption and continued use. Participatory design-based models (in which elderly people, caregivers, and practitioners actively participate in the development and testing of AI systems) have produced better results than top-down technological implementations. Ease of use, voice interface, user-configurable alert levels, and decipherable feedback are some of the features that help improve user trust and minimize cognitive load. There are also emotional

factors, which cause one to experience anxiety or dependency with the use of too many alerts or opaque decisions. Participatory design models focus on collaborative creation, the continuous feedback loop, and contextual testing, which means that AI systems will be supportive of the experience of older users in the real world. Implementing the principles of human-centered design, AI systems will shift from a perceived surveillance system to a trusted companion, which strengthens autonomy instead of weakening it.

6.9. Future Interdisciplinary Agenda

The multidimensional aspect of elderly fraud prevention requires an interdisciplinary research agenda to go beyond technological innovation. Future studies have to combine the contributions of computer science, gerontology, psychology, sociology, ethics, law, and public policy to have a comprehensive and sustainable solution. Longitudinal studies should be conducted to determine the sustainability of AI intervention, behavioral changes, and the unintended effects of AI interventions upon elderly groups. Psychological studies may enlighten the effects of AI surveillance on trust, anxiety, and self-efficacy, and legal scholarship on accountability, liability, and consent in AI-mediated decision-making.

From a systems perspective, interdisciplinary work can help to integrate AI fraud prevention with healthcare, social services, and smart living environments. This convergence allows AI to be more than a defensive device and a holistic support system that helps to improve safety, dignity, and independence. The involvement of cross-sector and participatory governance will allow the development of future studies to ensure that AI-facilitated fraud prevention will be responsible, equitable, and responsive to the ideals of the aging populations.

7. Information Governance, Security, and Ethical AI Realization

Being aware of the sensitivity of the data concerning the elderly, the manuscript brings forward an in-depth discussion on the governance of data and the ethical implementation of AI. It highlights the significance of the high-quality and representative datasets with age-diverse transactional patterns and communication behavior to minimize bias and increase model fairness. Secure data handling: anonymization, encryption, and access control are mentioned as the key elements of responsible AI systems.

Ethical implications, such as informed consent, transparency, and accountability, are not separated and taken as peripheral issues but incorporated into the analytical account. The manuscript also explains the concept of explainability and auditing to enhance trust among aging users and caregivers, which helps in the establishment of ethical congruence without impacting detection potentials. This focus on ethical data practices enhances the applicability of the manuscript in the regulatory and policy-based contexts.

7.1. Advanced AI Paradigms (2023-2025) Integration

To make the manuscript relevant in the contemporary context, the most recent developments in the field of artificial intelligence are introduced, which accompany the improved performance of fraud prevention among the elderly population. The concept of Explainable Artificial Intelligence (XAI) is brought out as a key element of user confidence that enables AI systems to submit alerts and advice in simple terms. Federated learning is reviewed as a scalable method that allows cross-institutional fraud detection with the help of sharing no centralized data, which enhances privacy protection. The methods of privacy preservation, such as differential privacy and encrypted inference, are mentioned as measures to reconcile uninterrupted surveillance with morality. Combining all these innovative paradigms, the manuscript will be on the frontline of the latest AI research, and the strategies of the prevention of elder fraud will be adjusted to the latest technological achievements in the high-tech world.

7.2. Enforced Practical and Policy Implications

Based on the improved analysis, the manuscript presents practical implications to the financial institutions, technology developers, caregivers, and policymakers. It illustrates how AI systems can be implemented in both the banking and eldercare systems that are already in place, aided by regulatory policies and inter-sectoral co-operation.

The policy suggestions include the importance of AI-based fraud notifications as a mandatory feature in older accounts, incentives for the accessibility of AI design, and investing in digital literacy programs. These conclusions are based on the analytical pieces of knowledge that have been built up throughout the manuscript, hence practical relevance and real-life application.

7.3. Contribution to the Knowledge and Research Development

With these improvements, the manuscript fulfills a significant role in the literature by pushing past the field of conceptual discussion to an analytically powerful, interdisciplinary, and future-focused framework of AI-based elderly fraud prevention.

It combines empirical findings, a reviewed approach, quantitative thinking, ethical management, and a highly sophisticated artificial intelligence paradigm into one unified story. Such an enhanced method not only adds academic rigor to the manuscript but also makes it an important resource to researchers, practitioners, and policy makers who want to find sustainable, ethical, and effective AI solutions to safeguard the elderly groups in the digital era.

8. Conclusion

8.1. Summary of Key Findings

Her paper illuminates the fact that older-aged parents must be accorded protection during the digital age more than ever against the threat of future AI fraud and cybercrime. As the literature presupposes, the elderly remain among the most susceptible categories of population due to the lack of communication skills, particularly the ability to use computers, because of the insignificant levels of digital literacy and their general advancement in age, which has caused the decline of cognitive flexibility and the additional exaggeration of trust inherent in using the Internet.

Such groups as scams through phishing, takeovers of identities, financial scams, and investigational phone calls are increasingly leaving an isolating impact on the elderly, and can cause financial and emotional damage. In the meantime, AI has been viewed as an effective tool in crime detection and prevention, where anomaly detection models, natural language processing that detects phishing, and AI-driven biometric identity detection are considered to be among the most advanced products. Besides preventing fraudsters, AI might allow considering an average level of safety and comfort of the aging parents by integrating it with the financial protection packages introduced by financial activities, installing safety systems at the residences of the elderly parents, and dedicated support apps. Together, these findings justify the challenges related to the application of AI to support the safety of the aging population and create new possibilities.

8.2. Contributions to the Field

The paper takes part in the existing body of knowledge as it provides an in-depth review of the application of AI in preventing elderly fraud interventions as well as its contextualization in older adult care. The existing body of research has either narrowed down to cybercrimes or AI in healthcare, whereas the provided review addressed the gap of completing the triad of financial, psychological, and safety concerns of older Americans in an AI context.

The review presents a multidisciplinary perspective in terms of existing issues, opportunities, future, and analysis of the current technology on conjecturing through involvement of research in computer science, social sciences, and eldercare. It also augments this by mentioning the areas that require urgent attention, which are the digital literacy programs, the ethical principles of AI surveillance, and developing AI interfaces that are easy to use by seniors. In such a manner, this body of knowledge is a source in numerous scholarly studies, practical innovations, and even in government decision-making in an attempt to provide safety to the aging population residing in an increasingly digitalized society.

8.3. Final Recommendations

Upon these findings, it can be suggested that beneficial advice be given to different stakeholders. Some of the things that would matter a lot to the developers of the technology would be the development of AI systems that are easy to access, skills to use, and user-friendly, as well as systems unique to the requirements of the aged individuals, like the use of big fonts, voice input, simplified dashboards, and notifications that are of fraud. To the family and caregivers in question, they need to be actively involved in the education and guidance process regarding the use of AI among elderly parents, utilize the interaction facility available, and ensure their 24 use and fraud prevention tools are available and assure them that they are safe using it. As a policy-maker, influential regulations and country-wide regulations are needed to help with digital utilization of the literacy programs, stimulate elderly-welcoming AI technologies, and enforce mandatory fraud-detecting programs on the financial System.

Finally, the NGOs and local bodies roles in the area should also be applied when carrying out the outreach and training with the implementation, whereby young citizens proposals and set-ups living in rural and semi-urban settings should also have access to and use of protective technologies as well. To rebrand a more secretive, integrative internet tool for the elderly, these recommendations may be used.

It could definitely be achieved with the assistance of a Concluding Statement on the part of the author and social responsibility. The problem of elderly parent protection in the digital age is not only to be regarded as a technological problem but also as a social one. Even though the potential of AI in preventing fraud, as well as creating some form of safety, is immeasurable, the ultimate result of the technology is the awareness, trust, and adoption rates of said technology among the members of the older generation.

The creative technology participating in such a trust formation involves, of course, the innovative technology, yet the active participation of the families, communities, and governments.

There should exist a strong call to action, thus: in order to accelerate education and training processes, set up a partnership with technological companies and state structures, and develop AI on the premise of solutions that enable the process of achieving GenMe population empowerment by empowering them and not intimidating them. Courtesy of these strategies, the world can now start to move into the future where their elderly parents will not only be spared from the fraud and the abuse but will also have hope that they can live with dignity and independence, as well as confidence in the new digital world.

Declarations

Conflict of Interest Declaration

I declare that there is no conflict of interest related to the research presented in this paper.

Funding Declaration

I declare that this research did not receive any external funding from any funding agency, public or private.

Statement of Ethical Approval (If Applicable)

Not applicable

Data Availability Statement

Not applicable

References

[1] Shaden Ali AbdullahAl-Nafisa, and Yahya MKhatatbeh, "Social Engineering and Digital Fraud: Studying the Differences between Victims of Cyber Phishing in Light of Some Variables," *Lex Localis-Journal of Local Self-Government*, vol. 23, no. S1, pp. 367-379, 2025. [Google Scholar] [Publisher Link]

[2] Shelden Adih Agingi, "*Promoting Responsible Digital Innovation in the Banking Industry: A Case Study of Public-Private-Community Partnerships in Cameroon*," Theses and Dissertations, Hasselt University, 2023. [Google Scholar] [Publisher Link]

[3] Ajay Agrawal, Joshua Gans, and Avi Goldfarb, *Power and Prediction: The Disruptive Economics of Artificial Intelligence*, Harvard Business Press, 2022. [Google Scholar] [Publisher Link]

[4] Zeeshan Ahmed et al., "Artificial Intelligence with Multi-Functional Machine Learning Platform Development for Better Healthcare and Precision Medicine," *Database*, vol. 2020, pp. 1-35, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Mohd Khairul Nizam Mohammad Amin et al., "Contact Alert App-Smooth Features to Detect Scammers," *APS Proceedings*, vol. 10, pp. 75-83, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Rifqi Abdul Aziz et al., "Media and Elderly: The Role of Media in Handling Post Retirement Syndrome," *Jurnal the Messenger*, vol. 17, no. 1, pp. 17-36, 2025. [Google Scholar]

[7] Clare Baek, Tamara Tate, and Mark Warschauer, ""ChatGPT Seems Too Good to Be True': College Students' Use and Perceptions of Generative AI," *Computers and Education: Artificial Intelligence*, vol. 7, pp. 1-9, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Paul B. Baltes, and Sherry L. Willis, *Plasticity and Enhancement of Intellectual Functioning in Old Age*, Penn State's Adult Development and Enrichment Project (ADEPT), *Aging and Cognitive Processes*, Springer, Boston, MA, pp. 353-389, 1982. [CrossRef] [Google Scholar] [Publisher Link]

[9] Ravi Bapna, and Anindya Ghose, *Thrive: Maximizing Well-Being in the Age of AI*, MIT Press, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Oluwabusayo Adijat Bello, and Komolafe Olufemi, "Artificial Intelligence in Fraud Prevention: Exploring Techniques and Applications Challenges and Opportunities," *Computer Science & IT Research Journal*, vol. 5, no. 6, pp. 1505-1520, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Stan Benjamens, Pranavsingh Dhunnoo, and Bertalan Meskó, "The State of Artificial Intelligence-Based FDA-Approved Medical Devices and Algorithms: An Online Database," *NPJ Digital Medicine*, vol. 3, no. 1, pp. 1-8, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Kristin Bernard et al., "Enhancing Attachment Organization Among Maltreated Children: Results of a Randomized Clinical Trial," *Child Development*, vol. 83, no. 2, pp. 623-636, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[13] Deepak Bhaskaran, "Implementing Robust Security Measures to Protect Elderly Users from Financial Fraud," *International Journal of Research in Computer Applications and Information Technology*, vol. 8, no. 1, pp. 1340-1352, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[14] Charlotte Blease, *Dr. Bot: Why Doctors Can Fail Us-and How AI Could Save Lives*, Yale University Press, 2025. [Google Scholar] [Publisher Link]

[15] Nick Bostrom, "A History of Transhumanist Thought," *Journal of Evolution and Technology*, vol. 14, no. 1, pp. 1-25, 2005. [Google Scholar] [Publisher Link]

[16] Nick Bostrom, "In Defense of Posthuman Dignity," *Bioethics*, vol. 19, no. 3, pp. 202-214, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[17] Laura Calvet-Mir et al., "The Transmission of Home Garden Knowledge: Safeguarding Biocultural Diversity and Enhancing Social-Ecological Resilience," *Society & Natural Resources*, vol. 29, no. 5, pp. 556-571, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[18] Peipei Chen et al., "Public Perception on Active Aging after COVID-19: An Unsupervised Machine Learning Analysis of 44,343 Posts," *Frontiers in Public Health*, vol. 12, pp. 1-8, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Xinxin Chen et al., "The Path to Healthy Ageing in China: A Peking University-Lancet Commission," *The Lancet*, vol. 400, no. 10367, pp. 1967-2006, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Warren B. Chow et al., "Optimal Preoperative Assessment of the Geriatric Surgical Patient: A Best Practices Guideline from the American College of Surgeons National Surgical Quality Improvement Program and the American Geriatrics Society," *Journal of the American College of Surgeons*, vol. 215, no. 4, pp. 453-466, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[21] Ruxandra Oana Ciobanu, and Tineke Fokkema, *The Role of Religion in Protecting Older Romanian Migrants from Loneliness, Ageing as a Migrant*, Routledge, 1st Ed., pp. 36-54, 2020. [Google Scholar] [Publisher Link]

[22] Kate Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, 2021. [Publisher Link]

[23] Ravi Shanker Datti et al., "Risk Perceptions and Safe Behaviours on the Internet among Older Adults in India," *Security Journal*, vol. 38, no. 1, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[24] Thomas H. Davenport, *The AI Advantage: How to Put the Artificial Intelligence Revolution to Work*, MIT Press, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[25] Yue Deng et al., ""Auntie, Please Don't Fall for Those Smooth Talkers": How Chinese Younger Family Members Safeguard Seniors from Online Fraud," *CHI '25: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, Yokohama, Japan, pp. 1-17, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[26] Ajayi Omole Dennis, *The Impact of People, Artificial Intelligence, and Technology in Managing Insider Threats and Social Engineering*, ResearchGate, 2025. [Online]. Available: https://www.researchgate.net/profile/Dennis-Ajayi/publication/392165605_The_Impact_of_People_Artificial_Intelligence_and_Technology_in_Managing_Insider_Threats_and_Social_Engineering/links/6837ae298a76251f22ea0664/The-Impact-of-People-Artificial-Intelligence-and-Technology-in-Managing-Insider-Threats-and-Social-Engineering

[27] Martin Ebers et al., *The Promise and Perils of AI and ML in Public Administration, Artificial Intelligence and Machine Learning Powered Public Service Delivery in Estonia*, Springer, Cham, pp. 7-33, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] Glen H. Elder, Jr., and Tri van Nguyen and Avshalom Caspi, "Linking Family Hardship to Children's Lives," *Child Development*, vol. 56, no. 2, pp. 361-375, 1985. [CrossRef] [Google Scholar] [Publisher Link]

[29] Patrice L. Engle et al., "Strategies to Avoid the Loss of Developmental Potential in More than 200 Million Children in the Developing World," *The Lancet*, vol. 369, no. 9557, pp. 229-242, 2007. [Google Scholar] [Publisher Link]

[30] Gemma Flores Mateo et al., "Mobile Phone Apps to Promote Weight Loss and Increase Physical Activity: A Systematic Review and Meta-Analysis," *Journal of Medical Internet Research*, vol. 17, no. 11, pp. 1-11, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[31] Luciano Floridi, *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*, Oxford University Press, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[32] Alisa Frik et al., "Privacy and Security Threat Models and Mitigation Strategies of Older Adults," *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pp. 21-40, 2019. [Google Scholar] [Publisher Link]

[33] V. Geetha, *Chemical Biology and Drug Discovery: Interdisciplinary, Multidisciplinary Research Area in Arts, Science & Commerce*, vol. 3, pp. 1-10, 2025. [Google Scholar]

[34] Sheri C. Gibson, and Edie Greene, "Assessing Knowledge of Elder Financial Abuse: A First Step in Enhancing Prosecutions," *Journal of Elder Abuse & Neglect*, vol. 25, no. 2, pp. 162-182, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[35] Malik A. Gladden, "*Research Aiming to Understand Baseline Cybersecurity Awareness for Senior Citizens and Their Training Needs*," Masters Theses & Doctoral Dissertations, Dakota State University, 2025. [Google Scholar] [Publisher Link]

[36] Moria Golan, "Parents as Agents of Change in Childhood Obesity - From Research to Practice," *International Journal of Pediatric Obesity*, vol. 1, no. 2, pp. 66-76, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[37] David B. Goldston et al., "Cultural Considerations in Adolescent Suicide Prevention and Psychosocial Treatment," *American Psychologist*, vol. 63, no. 1, pp. 14-31, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[38] K.M. Gopal, Shobhit Kumar, and Oshia Garg, "*Senior Care Reforms in India: Reimagining the Senior Care Paradigm*," *Open Science Framework Preprint*, pp. 1-124, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[39] L.D. Herrera, London Van Sickle, and Ashley Podhradsky, "Bridging the Protection Gap: Innovative Approaches to Shield Older Adults from AI-Enhanced Scams," *2024 Cyber Awareness and Research Symposium (CARS)*, Grand Forks, ND, USA, pp. 1-9, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[40] Myron A. Hofer, *Hidden Regulators: Implications for a New Understanding of Attachment, Separation, and Loss, Attachment Theory*, Routledge, pp. 203-230, 2013. [Google Scholar] [Publisher Link]

[41] Wayne Holmes et al., "Ethics of AI in Education: Towards a Community-Wide Framework," *International Journal of Artificial Intelligence in Education*, vol. 32, no. 3, pp. 504-526, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[42] Wayne Holmes, and Ilkka Tuomi, "State of the Art and Practice in AI in Education," *European Journal of Education*, vol. 57, no. 4, pp. 542-570, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[43] Andreas Holzinger et al., "What Do We Need to Build Explainable AI Systems for the Medical Domain?," *arXiv Preprint*, pp. 1-28, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[44] Lan Huang, "Ethics of Artificial Intelligence in Education: Student Privacy and Data Protection," *Science Insights Education Frontiers*, vol. 16, no. 2, pp. 2577-2587, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[45] Ming-Hui Huang, Roland Rust, and Vojislav Maksimovic, "The Feeling Economy: Managing in the Next Generation of Artificial Intelligence (AI)," *California Management Review*, vol. 61, no. 4, pp. 43-65, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[46] Angela J. Huebner et al., "Parental Deployment and Youth in Military Families: Exploring Uncertainty and Ambiguous Loss," *Family Relations*, vol. 56, no. 2, pp. 112-122, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[47] Marco Iansiti, and Karim R. Lakhani, *Competing in the Age of AI: Strategy and Leadership When Algorithms and Networks Run the World*, Harvard Business Press, 2020. [Google Scholar] [Publisher Link]

[48] Nancy S. Jecker, "You've Got a Friend in Me: Sociable Robots for Older Adults in an Age of Global Pandemics," *Ethics and Information Technology*, vol. 23, no. S1, pp. 35-43, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[49] V. Kakulapati, Sheri Mahender Reddy, and A. Paramasivam, *Managing Postpandemic Effects Using Artificial Intelligence with Human-Computer Interaction, Innovations in Artificial Intelligence and Human-Computer Interaction in the Digital Era*, Elsevier, pp. 207-232, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[50] Jerry Kaplan, *Artificial Intelligence: What Everyone Needs to Know*, Oxford University Press, 2016. [Google Scholar] [Publisher Link]

[51] Harold Kerzner, *Project Management: A Systems Approach to Planning, Scheduling, and Controlling*, John Wiley & Sons, 2025. [Google Scholar] [Publisher Link]

[52] Kevin B. Korb, and Ann E. Nicholson, *Bayesian Artificial Intelligence*, 2nd ed., CRC Press, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[53] Philip Kotler, Hermawan Kartajaya, and Iwan Setiawan, *Marketing 5.0: Technology for Humanity*, John Wiley & Sons, 2021. [Google Scholar] [Publisher Link]

[54] Yogesh Kumar et al., "Artificial Intelligence in Disease Diagnosis: A Systematic Literature Review, Synthesizing Framework and Future Research Agenda," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 7, pp. 8459-8486, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[55] Nikoleta Georgousidou Kyriakidou, "*Public Sector Employees' Perception of the Use and Effectiveness of AI Tools in Public Sector HR Management*," Postgraduate Dissertation, Hellenic Open University, 2025. [Google Scholar] [Publisher Link]

[56] Raz Lapid, Roy Langberg, and Moshe Sipper, "Open Sesame! Universal Black-Box Jailbreaking of Large Language Models," *Applied Sciences*, vol. 14, no. 16, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[57] Harrison Lee et al., "*RLAIF: Scaling Reinforcement Learning from Human Feedback with AI Feedback*," *ICLR 2024 Conference*, pp. 1-31, 2023. [Google Scholar] [Publisher Link]

[58] Kai-Fu Lee, "*AI Superpowers: China, Silicon Valley, and the New World Order*, HarperCollins Publishers, 2018. [Google Scholar] [Publisher Link]

[59] Anne K. Liefländer et al., "Promoting Connectedness with Nature through Environmental Education," *Environmental Education Research*, vol. 19, no. 3, pp. 370-384, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[60] Duri Long, and Brian Magerko, "What Is AI Literacy? Competencies and Design Considerations," *CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Honolulu, HI, USA, pp. 1-16, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[61] Rose Luckin, and Wayne Holmes, "*Intelligence Unleashed: An Argument for AI in Education*," UCL Knowledge Lab, London, UK, 2016. [Google Scholar] [Publisher Link]

[62] Scott M. Lundberg et al., "Explainable AI for Trees: From Local Explanations to Global Understanding," *arXiv Preprint*, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[63] Rakhi P. Madnani, "An Empirical Study on Assessing the Trustworthiness of AI Systems in Handling Sensitive Financial Information," *Rethink Revolution: Transformative Waves Across Disciplines*, pp. 80-84, 2024. [Google Scholar]

[64] Prashant Mahajan, *Beyond Biology: AI as Family and the Future of Human Bonds and Relationships*, F1000 Research Ltd, 2025. [Google Scholar] [Publisher Link]

[65] Irja Malmio, "Artificial Intelligence and the Social Dimension of Sustainable Development: Through a Security Perspective," *Discover Sustainability*, vol. 5, no. 1, pp. 1-16, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[66] Karen Malone, "The Bubble-Wrap Generation: Children Growing Up in Walled Gardens," *Environmental Education Research*, vol. 13, no. 4, pp. 513-527, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[67] Polina Mamoshina et al., "Converging Blockchain and Next-Generation Artificial Intelligence Technologies to Decentralize and Accelerate Biomedical Research and Healthcare," *Oncotarget*, vol. 9, no. 5, pp. 5665-5690, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[68] Peter A. Mantello et al., "Gauging Public Opinion of AI and Emotionalized AI in Healthcare: Findings from a Nationwide Survey in Japan," *AI & Society*, vol. 40, no. 5, pp. 3735-3749, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[69] James McBride, "Robotic Bodies and the Kairos of Humanoid Theologies," *Sophia*, vol. 58, no. 4, pp. 663-676, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[70] Julie Mehan, *Artificial Intelligence: Ethical, Social, and Security Impacts for the Present and the Future*, IT Governance Publishing Ltd, 2022. [Google Scholar] [Publisher Link]

[71] Bradley D. Menz et al., "Current Safeguards, Risk Mitigation, and Transparency Measures of Large Language Models against the Generation of Health Disinformation: Repeated Cross Sectional Analysis," *BMJ*, vol. 384, pp. 1-10, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[72] Peter Adamis, *The Rise of AI*: The Rise of AI and its Impact on Mankind, 2025. [Online]. Available: https://abalinx.com/the-rise-of-ai/

[73] Edward Alan Miller, "Protecting and Improving the Lives of Older Adults in the COVID-19 Era," *Journal of Aging & Social Policy*, vol. 32, no. 4-5, pp. 297-309, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[74] Elmira K. Naberushkina, Oksana Besschetnova, and Oleg A. Sudorgin, "Financial Fraud against the Elderly as a Latent Indicator of Intergenerational Breakdown," *Journal of Social Research and Intervention*, vol. 88, pp. 71-84, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[75] Noémi Nagy, ""Humanity's New Frontier": Human Rights Implications of Artificial Intelligence and New Technologies," *Hungarian Journal of Legal Studies*, vol. 64, no. 2, pp. 236-267, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[76] V.S. Nalawade et al., "Result Paper on "Mobile Theft-Prevention System"," *International Journal on Advanced Computer Theory and Engineering*, vol. 14, no. 1, pp. 457-464, 2025. [CrossRef] [Publisher Link]

[77] Mathilde Neugnot-Cerioli, and Olga Muss Laurenty, "*The Future of Child Development in the AI Era: Cross-Disciplinary Perspectives between AI and Child Development Experts*," *arXiv Preprint*, pp. 1-45, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[78] William O'Donovan, "*Artificial Intelligence: The Human Autonomy and Ethical Considerations of Advancing Intelligent Systems and Machines*," Master's thesis, National University of Ireland, Maynooth, 2024. [Google Scholar] [Publisher Link]

[79] Sungmee Park, and Sundaresan Jayaraman, "Enhancing the Quality of Life through Wearable Technology," *IEEE Engineering in Medicine and Biology Magazine*, vol. 22, no. 3, pp. 41-48, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[80] Katalin Parti, Faika Tahir, and Pamela B. Teaster, "The Wisdom of the Scammed: Redefining Older Fraud Victim Support by Utilizing the Ecological Systems Framework," *Security Journal*, vol. 38, no. 1, pp. 1-23, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[81] Vikram Patel et al., "Promoting Child and Adolescent Mental Health in Low and Middle Income Countries," *Journal of Child Psychology and Psychiatry*, vol. 49, no. 3, pp. 313-334, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[82] Theresa Payton, Theodore Claypoole, and Howard A. Schmidt, *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family*, Bloomsbury Publishing, 2023. [Google Scholar] [Publisher Link]

[83] Keri E. Pearlson, Carol S. Saunders, and Dennis F. Galletta, *Managing and Using Information Systems: A Strategic Approach*, 8th ed., John Wiley & Sons, 2024. [Google Scholar] [Publisher Link]

[84] Mary E. Penny et al., "Effectiveness of an Educational Intervention Delivered through the Health Services to Improve Nutrition in Young Children: A Cluster-Randomised Controlled Trial," *The Lancet*, vol. 365, no. 9474, pp. 1863-1872, 2005. [Google Scholar] [Publisher Link]

[85] Julia M. Puaschunder, *"The Legal and International Situation of AI, Robotics and Big Data with Attention to Healthcare*," Report on behalf of the European Parliament European liberal Forum, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[86] S. Punitha, and K.S. Preetha. "Unleashing Potential: A Deep Dive into AI-Blockchain Integration for UAV-Enhanced Tele-Surgery," *Cogent Engineering*, vol. 11, no. 1, pp. 1-42, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[87] Stefano Puntoni et al., "Consumers and Artificial Intelligence: An Experiential Perspective," *Journal of Marketing*, vol. 85, no. 1, pp. 131-151, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[88] Iyad Rahwan et al., "Machine Behaviour," *Nature*, vol. 568, no. 7753, pp. 477-486, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[89] Seema Babusing Rathod et al., *Staying Safe in the Digital Age: Mobile App Advancements, AI Tools and Applications for Women's Safety*, IGI Global Scientific Publishing, pp. 291-303, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[90] Jean-Yves Reginster, and Nansa Burlet, "Osteoporosis: A Still Increasing Prevalence," *Bone*, vol. 38, no. 2, pp. 4-9, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[91] Nola M. Ries, "Enduring Powers of Attorney and Financial Exploitation of Older People: A Conceptual Analysis and Strategies for Prevention," *Journal of Aging & Social Policy*, vol. 34, no. 3, pp. 357-374, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[92] Chares R. Ross, *"Reducing Payment-Card Fraud*," PhD Thesis, Walden University, 2020. [Google Scholar] [Publisher Link]

[93] Theodore Roszak, *The Cult of Information: A Neo-Luddite Treatise on High-Tech, Artificial Intelligence, and the True Art of Thinking*, 1st ed., University of California Press, 1994. [Google Scholar] [Publisher Link]

[94] Jo Salmon et al., "Promoting Physical Activity Participation among Children and Adolescents," *Epidemiologic Reviews*, vol. 29, no. 1, pp. 144-159, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[95] Hishan S. Sanil et al., "Role of Machine Learning in Changing Social and Business Eco-System-A Qualitative Study to Explore the Factors Contributing to Competitive Advantage during COVID Pandemic," *World Journal of Engineering*, vol. 19, no. 2, pp. 238-243, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[96] Omar Santos, *Developing Cybersecurity Programs and Policies in an AI-Driven World*, 4th ed., Pearson IT Certification, 2024. [Google Scholar] [Publisher Link]

[97] Martin Sas, and Jan Tobias Mühlberg, "*Trustworthy Age Assurance*," The Greens Cluster: Social & Economy, European Parliament, 2024. [Google Scholar] [Publisher Link]

[98] Schwartz, Reva, et al. "*Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*," U.S. Department of Commerce, National Institute of Standards and Technology, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[99] Michael Segal, "Protecting Older Consumers in the Digital Age: A Commentary on ChatGPT, Helplines and the Way to Prevent Accessible Fraud," *Journal of Elder Abuse & Neglect*, vol. 36, no. 5, pp. 528-533, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[100] Amanda Sharkey, and Noel Sharkey, "Granny and the Robots: Ethical Issues in Robot Care for the Elderly," *Ethics and Information Technology*, vol. 14, no. 1, pp. 27-40, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[101] Shama Siddiqui et al., *Connected Health Insights for Sustainable Development: Integrating IoT, AI, and Data-Driven Solutions*, Springer Cham, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[102] Merril Silverstein, and Roseann Giarrusso, "Aging and Family Life: A Decade Review," *Journal of Marriage and Family*, vol. 72, no. 5, pp. 1039-1058, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[103] Asad Ali Siyal et al., "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives," *Cryptography*, vol. 3, no. 1, pp. 1-16, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[104] Albert J. Solnit, and Mary H. Stark, "Mourning and the Birth of a Defective Child," *The Psychoanalytic Study of the Child*, vol. 16, no. 1, pp. 523-537, 1961. [CrossRef] [Google Scholar] [Publisher Link]

[105] S.R. Suura, "Agentic Artificial Intelligence Systems for Dynamic Health Management and Real-Time Genomic Data Analysis," *European Journal of Analytics and Artificial Intelligence (EJAAI)*, vol. 2, 2024. [Google Scholar]

[106] Sara L. Tamers et al., "Envisioning the Future of Work to Safeguard the Safety, Health, and Well-Being of the Workforce: A Perspective from the CDC's National Institute for Occupational Safety and Health," *American Journal of Industrial Medicine*, vol. 63, no. 12, pp. 1065-1084, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[107] Brian J. Taylor et al., "Older People's Conceptualization of Elder Abuse and Neglect," *Journal of Elder Abuse & Neglect*, vol. 26, no. 3, pp. 223-243, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[108] Jason Thacker, *The Age of AI: Artificial Intelligence and the Future of Humanity*. Harper Christian+ ORM, 2020. [Google Scholar]

[109] Suzanne C. Thompson, and Susan Spacapan, "Perceptions of Control in Vulnerable Populations," *Journal of Social Issues*, vol. 47, no. 4, pp. 1-21, 1991. [CrossRef] [Google Scholar] [Publisher Link]

[110] Bart van der Sloot, *Regulating the Synthetic Society: Generative AI, Legal Questions, and Societal Challenges*, Bloomsbury Academic, 2024. [Google Scholar] [Publisher Link]

[111] Jacob M. Vargis, "*Analyzing COVID-19 Era Cyber Threats on the Elderly: Toward Realizing N-of-1 Countermeasures to Enhance Cyber Situational Awareness of Social Engineering Attacks*," PhD thesis, Marymount University, 2023. [Google Scholar] [Publisher Link]

[112] Rasha Waheeb, "Using Ethical Artificial Intelligence (EAI) to Eliminate the Strange and Suspicious Phenomena that Have Spread "Iraq Post Disaster as a Case Study"," *SSRN*, pp. 1-28, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[113] Froma Walsh, "Traumatic Loss and Major Disasters: Strengthening Family and Community Resilience," *Family Process*, vol. 46, no. 2, pp. 207-227, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[114] Darrell M. West, *The Future of Work: Robots, AI, and Automation*, Brookings Institution Press, 2018. [Google Scholar] [Publisher Link]

[115] Diana D. Whitney, and Amanda Trosten-Bloom, *The Power of Appreciative Inquiry: A Practical Guide to Positive Change*, Berrett-Koehler Publishers, 2010. [Google Scholar]

[116] Meredith Whittaker et al., "*AI Now Report 2018*," AI Now Institute, New York University, 2018. [Google Scholar] [Publisher Link]

[117] Stacey Wood, and Peter A. Lichtenberg, "Financial Capacity and Financial Exploitation of Older Adults: Research Findings, Policy Recommendations and Clinical Implications," *Clinical Gerontologist*, vol. 40, no. 1, pp. 3-13, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[118] Tongshuang Wu, Michael Terry, and Carrie Jun Cai, "AI Chains: Transparent and Controllable Human-AI Interaction by Chaining Large Language Model Prompts," *CHI '22: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, New Orleans, LA, USA, pp. 1-22, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[119] Georgios N. Yannakakis, and Julian Togelius, *Artificial Intelligence and Games*, Springer Cham, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[120] Jianbing Yu et al., "Experimental Study on the Structural Behavior of Exterior Precast Concrete Beam-Column Joints with High-Strength Steel Bars in Field-Cast RPC," *Engineering Structures*, vol. 299, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[121] Yuxiang Zhai et al., "Hear Us, then Protect Us: Navigating Deepfake Scams and Safeguard Interventions with Older Adults through Participatory Design," *CHI '25: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, Yokohama, Japan, pp. 1-19, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[122] Maximilian Zorzetti et al., "Improving Agile Software Development Using User-Centered Design and Lean Startup," *Information and Software Technology*, vol. 141, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[123] Yixin Zou et al., "Cross-Contextual Examination of Older Adults' Privacy Concerns, Behaviors, and Vulnerabilities," *Privacy-Enhancing Technologies (PoPETs)*, vol. 2024, no. 1, pp. 133-150, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[124] Muhammad Amirrul Alhafiz Bin Mohd Zukry, Muhammad Nur Aqmal Bin Khatiman, Rusli Bin Haji Abdullah, "Strategies for Protecting Senior Citizens against Online Banking Fraud and Scams: A Systematic Literature Review," *Journal of Theoretical and Applied Information Technology*, vol. 102, no. 14, pp. 5545-5555, 2024. [Google Scholar] [Publisher Link]

[125] Tao Guan, "The Practical Dilemmas and Optimization Paths for Protecting the Personal Information Rights of Digitally Disadvantaged Groups," *SSRN*, pp. 1-23, 2024. [CrossRef] [Google Scholar] [Publisher Link]