DOI:10.5281/zenodo.15075890

AI-Driven Forensic Cyberpsychology Intervention Strategies for Social Media Platform and School Managers to Mitigate Cyber Fraud At-Risk Adolescents

Francis C. Ohu[1], Laura A. Jones[2]

[1,2]Department of Forensic Cyberpsychology, Capitol Technology University, Laurel, MD, USA
Corresponding author email: fohu@captechu.edu

Abstract: Adolescent cyber fraud is an escalating concern, with a 32% increase in youth-driven cybercrime between 2022 and 2024. This study employs a narrative literature review and thematic analysis to synthesize research on AI-driven forensic cyberpsychology, adolescent cyber deception, and fraud detection methodologies, following Braun and Clarke's six-phase thematic analysis framework. The findings identified validation-seeking behaviors, socioeconomic stressors, and AI-detected deception patterns as the three dominant risk factors influencing adolescent cyber deception. Empirical evidence indicates that adolescents exhibiting high levels of self-doubt and digital validation dependence are 45% more likely to engage in cyber deception, while socioeconomic stressors, particularly financial instability and low parental monitoring, increase cyber fraud susceptibility by 60%. AI-driven forensic analysis demonstrates high detection accuracy levels, identifying manipulative language cues by 82%, social engineering behaviors by 87%, and risk-based engagement patterns by 90%. This study proposes an AI-driven fraud detection strategy modeled on the Validation Syndrome Diagnostic Triangle (VSDT) framework that integrates psychological deception markers, parental monitoring levels, and social media reinforcement mechanisms, underscoring the need for AI-driven digital literacy programs, algorithmic fraud detection on social media platforms, and AI-assisted forensic cyberpsychology interventions in schools. The findings provide actionable insights for policymakers, educators, and platform managers to implement AI-driven fraud prevention strategies, ensuring early intervention and fostering digital responsibility among adolescents.

Keywords: Forensic Cyberpsychology, AI-Driven Fraud Detection, Adolescent Cybercrime, Digital Literacy, Validation-Seeking Behaviors, Dark Triad Traits, Cyber Fraud Prevention, Psychological Deception Markers

Introduction

Background and Context

Cyber fraud among adolescents is an escalating global concern, with a 32% increase in youth-driven cybercrime between 2022 and 2024 (Ahmed, 2024; FTC, 2024). The increasing prevalence of social media-based deception has been linked to digital validation-seeking behaviors, where adolescents manipulate online identities for financial or social gains (Ahmed, 2024). Studies indicate that 46% of cyber fraud cases now originate from social media platforms, demonstrating the digital environment's role in shaping deceptive tendencies (Burrell et al., 2023). From a forensic cyberpsychology perspective, the psychological mechanisms underpinning adolescent cyber fraud require urgent attention. Adolescents are developmentally primed for social validation and risk-taking, making them particularly vulnerable to engaging in deceptive online behaviors (Ohu & Jones, 2025b). The rapid advancement of artificial intelligence (AI) in digital spaces presents both opportunities and challenges—while AI can enhance cyber fraud detection, it is simultaneously being weaponized to automate and amplify deception tactics (Hani et al., 2024). Existing forensic cyberpsychology frameworks, however, lack AI-driven approaches for early detection and intervention, leaving digital platforms and educational institutions underprepared to address adolescent cyber fraud risks (Xiang, 2024).

Problem Statement

Cyber fraud among adolescents is increasingly shaped by psychological and environmental risk factors that traditional forensic models fail to detect (Karpasyuk et al., 2024). Digital validation-seeking behaviors, driven by self-doubt, desire, and self-gratification, have been identified as predictive markers of cyber deception, yet remain unaddressed in AI-driven forensic tools (Mustafa et al., 2024a; Ohu & Jones, 2025(a)).The General problem is the lack of AI-driven forensic cyberpsychology models leaving digital platforms and educators unprepared to detect and mitigate adolescent cyber fraud risks (Onuh et al., 2024). The specific problem is that current forensic tools do not incorporate adolescent-specific psychological risk factors such as Validation Syndrome into AI-driven fraud detection frameworks, thereby limiting their predictive accuracy and intervention effectiveness (Ganapathy, 2024; Karpasyuk et al., 2024).

Purpose of the Study

This study aims to develop an AI-driven adolescent fraud detection and intervention strategy by integrating the Validation Syndrome Diagnostic Triangle (VSDT) framework into AI-driven cyber fraud detection. The Validation Syndrome Diagnostic Triangle (VSDT) offers a comprehensive forensic cyberpsychology framework for combining psychological risk markers, such as self-doubt, desire, and self-gratification, with AI-driven behavioral analysis to identify and mitigate cyber fraud risks (Ohu & Jones, 2025b). This model suggests that familial conflict, socioeconomic stress, and a lack of parental monitoring significantly increase the likelihood of adolescent involvement in cyber fraud (Burrell et al., 2023). This research aims to formulate strategies for applying VSDT into machine learning models and digital behavioral data, to detect early-stage cyber fraud risk factors in adolescents based on VSDT indicators. In addition, develop AI-driven intervention frameworks for platform managers and school administrators, to promote positive digital behaviors through educational strategies informed by forensic cyberpsychology.

Rationale

The study seeks to bridge the forensic cyberpsychology-AI gap by developing a strategy for an AI-driven adolescent cyber fraud detection and intervention models, using the VSDT framework. The central research question guiding this study is, “How can AI-driven forensic cyberpsychology be used to detect and mitigate cyber fraud risks among adolescents while promoting positive educational interventions for platform and school managers?”

Originality and Significance of the Study

This study addresses a critical research gap in adolescent cyber deception by integrating forensic cyberpsychology and AI-driven fraud detection (Onuh et al., 2024).The findings of this research will have significant implications for improving early detection models by combining psychological and AI-driven risk markers, thereby enhancing fraud detection accuracy in adolescent populations (Thakkar, 2024). Additionally, the study's results will inform the development of AI-supported digital literacy programs that can be integrated into educational policies and platform management strategies, ultimately reducing adolescent fraud risks. Furthermore, the research aims to provide an evidence-based framework for forensic cyberpsychologists, AI developers, and educators to intervene before cyber fraud behaviors escalate, thereby contributing to cybercrime prevention efforts.

The rise in adolescent cyber fraud underscores the need for a multidisciplinary approach that combines forensic cyberpsychology and AI (Burrell et al. 2023; Rich & Aikens, 2024). By integrating the Validation Syndrome Diagnostic Triangle (VSDT) framework into AI-driven cyber fraud detection, this research contributes a novel approach to early intervention in adolescent digital risk behaviors. The study's actionable insights will benefit digital platform managers, school administrators, and policymakers, ensuring that AI is used not only for

cybercrime detection but also for fostering prosocial online behaviors among adolescents (Ohu & Jones, 2025c).

Literature Review

This study employed the structured, transparent, multi-disciplinary and peer reviewed (STAMP) approach (Rogge et al., 2024) shown in Table 1, for conducting an exploratory literature review, which involved a critical evaluation of existing research on forensic cyberpsychology, AI-driven fraud detection, adolescent cybercrime, and digital literacy interventions. The purpose of this review is to identify research gaps, synthesize key findings, and establish the theoretical foundation for integrating forensic psychology with AI-based cyber fraud prevention among at-risk adolescents (Ohu & Jones, 2025(b)). The review is guided by the following overarching research question, directly aligned with the study's problem statement, "How can AI-driven forensic cyberpsychology be used to detect and mitigate cyber fraud risks among adolescents while promoting positive educational interventions for platform and school managers?" To answer this question, the literature review explores psychological mechanisms underlying adolescent cyber fraud, including validation-seeking behaviors and Dark Triad traits. The role of AI-driven fraud detection in forensic cyberpsychology is also examined, as well as the impact of socioeconomic and familial factors on adolescent engagement in cyber fraud. Educational interventions and AI-integrated strategies for cyber fraud prevention are also discussed. The literature review is structured to ensure transparency and replicability, adhering to established guidelines for exploratory reviews. A comprehensive search of multiple reputable academic databases was conducted, including PsycINFO, PubMed, MDPI, and Google Scholar, to identify relevant studies on the topic of AI-driven forensic cyberpsychology and adolescent cyber fraud. The search terms employed included "forensic cyberpsychology," "adolescent cybercrime," "AI-driven fraud detection," "cyber fraud prevention," "digital literacy," and "cyber risk mitigation." Inclusion criteria established, included peer-reviewed journal articles published in the last four years, studies focused on adolescent cyber fraud, forensic cyberpsychology, AI-driven fraud detection, and digital literacy interventions, and empirical studies, systematic reviews, and meta-analyses with significant statistical insights. Exclusion criteria included non-peer-reviewed articles, opinion pieces, or non-academic sources, studies published before 2019 unless foundational to forensic cyberpsychology, and research not directly related to adolescent cyber fraud or AI-driven forensic detection models.

Table 1. STAMP Literature review framework

Category	Description	Sample Sourced Paper
Structured Search Strategy	Use of systematic databases such as Scopus, Google Scholar, and PsycINFO	Ahmed et al. (2024) Forensic cyberpsychology model
Transparency in Selection	Clearly defined inclusion/exclusion criteria documented in methodology	Burrell et al. (2023) Adolescent fraud behavior analysis
Accessible Data Sources	Focus on open-access journals and freely available sources	Mustafa et al. (2024) AI fraud detection case study
Multi-disciplinary Integration	Integration of research from psychology, criminology, and AI disciplines	(Lin, 2024) Cross-disciplinary cyber fraud assessment
Peer-reviewed Sources	Only peer-reviewed articles from 2019-2024 included	Ohu & Jones (2025b) Artificial Intelligence and Machine Learning in cybercrime prevention

Psychological Mechanisms Underlying Adolescent Cyber Fraud

Validation Seeking Behaviors and Cyber Fraud Risk

Forensic cyberpsychology research has increasingly identified validation seeking behaviors as a critical psychological mechanism driving adolescent engagement in cyber fraud. Adolescents experiencing chronic self-doubt and social rejection often turn to manipulative online behaviors as a means of obtaining external validation and social reinforcement (Park et al., 2024; Pérez-Torres, 2024).The need for validation, particularly in digital environments, can lead to deceptive practices such as identity fabrication, financial fraud, and social engineering (Kornienko & Rudnova, 2024). Studies have shown that adolescents with high external validation needs are 40% more likely to engage in cyber deception compared to their peers with lower validation seeking tendencies (Ohu & Jones, 2025c). This behavioral pattern is reinforced by social media platforms, where engagement-driven algorithms reward deceptive behaviors that generate high levels of interaction, encouraging users to present exaggerated or false personas (Lau et al., 2024; Zhou, 2024). The link between validation seeking behaviors and cyber fraud aligns with the VSDT framework, which posits that self-doubt, desire, and self-gratification interact to increase vulnerability to manipulative online behaviors (Ohu & Jones, 2025a). Adolescents struggling with self-doubt may resort to fraudulent activities as a way to assert control, gain approval, or attain material or social rewards that they feel are otherwise unattainable (Prinstein & Mitchell, 2022). Empirical evidence further supports the role of validation seeking behaviors in cyber fraud (Soares & Lazarus, 2024). Research findings reveal that social media platforms amplify deception by rewarding users who engage in behaviors that increase digital engagement, such as inflating their status, fabricating relationships, or manipulating digital interactions (Shin & Jitkajornwanich, 2024). The psychological drive for validation, particularly in adolescents who experience social rejection or low self-esteem, fuels online behaviors that involve deception, misrepresentation, and fraud (Asher et al., 2024). The intersection of forensic cyberpsychology and AI-driven fraud detection highlights a crucial research gap, as most existing fraud detection models fail to incorporate psychological risk factors such as validation seeking behaviors (Ohu & Jones, 2025b). Addressing this gap requires an AI-driven forensic cyberpsychology strategy that integrates behavioral markers of validation seeking with predictive fraud detection systems, enabling early identification and intervention for at-risk adolescents.

Dark Triad Traits and Digital Manipulation

The Dark Triad narcissistic, machiavellian and psychopathic personality traits, have been consistently linked to deceptive online behaviors, cyber fraud, and digital manipulation (Ohu & Jones, 2025a; Palma et al., 2021). Adolescents with high levels of these traits are more likely to engage in fraudulent activities, such as phishing scams, identity theft, and financial deception Ohu & Jones, 2025b). Research shows that adolescents scoring high on Dark Triad traits are significantly more likely to engage in digital deception and fraudulent schemes. Over 46% of convicted cyber fraudsters report early experiences with deception-based activities during adolescence(Cohen, 2024). These individuals often display reduced empathy, high impulsivity, and strong motivation for personal gain, traits that make them more inclined to exploit digital platforms for deceptive purposes (Cohen, 2024a). Social media and online financial transactions provide an environment where deception is easier to execute and harder to detect, reinforcing the behavioral tendencies associated with the Dark Triad (Adinata & Kesumaningsari, 2024). Studies have shown that adolescents with elevated Dark Triad traits are more likely to engage in manipulative behaviors, including fabricating online relationships, executing digital extortion schemes, and using psychological manipulation to deceive victims (Cohen, 2024). The association between Dark Triad traits and cyber fraud highlights a critical gap in forensic cyberpsychology research. While extensive studies have examined the role of Dark Triad traits in adult cybercrime, limited research has focused on their early manifestations in adolescent online

fraud (Moreira et al., 2024). Existing AI-driven fraud detection models primarily focus on identifying transactional anomalies and known fraud patterns rather than assessing the psychological predispositions that drive deceptive behaviors (Ohu & Jones, 2025c).

AI Driven Fraud Detection in Forensic Cyberpsychology

The Role of AI in Cyber Fraud Detection

Artificial intelligence has revolutionized cyber fraud detection by enhancing the ability to identify deceptive online behaviors through machine learning, natural language processing, and behavioral analytics (Moreira et al., 2024). AI-driven fraud detection systems analyze vast amounts of digital data to recognize patterns associated with fraudulent activity, including identity theft, financial scams, and social engineering tactics (Ismaeil, 2024). These systems have proven highly effective in detecting cyber fraud in real-time, significantly reducing financial losses and increasing the speed and accuracy of fraud prevention measures (Ismaeil, 2024). The integration of AI in cyber fraud detection has enabled advancements in predictive risk assessment, where behavioral and linguistic cues are used to flag potential fraud before financial damage occurs, and machine learning algorithms continuously adapt to emerging fraud tactics, improving their detection capabilities as they process new data (Prabin et al., 2024). Natural language processing models detect deceptive communication patterns, enabling fraud detection systems to identify phishing attempts, social engineering schemes, and online impersonation (Ismaeil, 2024). Research has shown that behavioral analytics further enhance fraud detection by analyzing user interactions, identifying suspicious behaviors such as rapid profile changes, repeated financial transactions, and irregular online activity (Moreira et al., 2024). Despite these advancements, the application of AI-driven fraud detection in forensic cyberpsychology remains underdeveloped, particularly in identifying adolescent cyber fraud risks (Moreira et al., 2024). Most AI fraud detection models focus on known fraud patterns associated with adult cybercriminals rather than assessing early-stage psychological risk factors in adolescents (Ismaeil, 2024). So, while AI can detect fraudulent transactions and behavioral anomalies, it does not currently integrate forensic cyberpsychology markers such as validation seeking behaviors, self-doubt, or Dark Triad personality traits (Moreira et al., 2024). This limitation reduces the effectiveness of fraud prevention efforts targeted at at-risk adolescents who may be in the early stages of engaging in cyber deception ((Ismaeil, 2024) Addressing this gap requires the development of AI models that incorporate forensic cyberpsychology insights, allowing for the detection of psychological precursors to cyber fraud (Ohu & Jones, 2025c).

Limitations of Current AI Based Fraud Detection Systems

Most AI-based fraud detection systems are designed to identify fraudulent transactions and suspicious digital behaviors based on established fraud patterns (Moreira et al., 2024). However, these systems overlook the early warning signs of cyber fraud engagement in younger populations, limiting their effectiveness in forensic cyberpsychology applications (Moreira et al., 2024). Traditional AI fraud detection models rely on analyzing past fraudulent activities to identify patterns in new transactions, but they fail to consider the psychological motivations and risk factors that drive adolescents to engage in cyber deception (Prabin et al., 2024).

Key psychological drivers of adolescent cyber fraud, such as validation seeking behaviors, self-doubt, and impulsivity, are not incorporated into existing AI-based detection frameworks (Ganapathy, 2024). As a result, these systems are unable to identify adolescents at risk of engaging in cyber fraud before their behaviors escalate into more advanced digital deception techniques (Lin, 2024). To address these limitations, it is essential to develop AI models that incorporate forensic cyberpsychology insights, enabling the detection of early-stage risk factors associated with adolescent cyber deception.

The Role of Parental Monitoring and Family Conflict

Parental monitoring plays a crucial role in shaping adolescent online behaviors and mitigating the risk of engagement in cyber fraud (Ganapathy, 2024). Adolescents who experience high levels of parental oversight are significantly less likely to engage in deceptive online activities (Lin, 2024), whereas those from environments with low parental supervision demonstrate a higher propensity for cyber fraud (Purificacion & Vallespin, 2024). Research indicates that strong parental monitoring is associated with a 35% reduction in cyber fraud engagement among adolescents (Ganapathy, 2024). When parents practice authoritative parenting by actively overseeing their children's digital interactions, set clear online boundaries, and engage in open discussions about ethical internet use, adolescents are less likely to be influenced by manipulative online environments and fraudulent activities (Lin, 2024; Putri et al., 2024). In contrast, the absence of structured guidance and accountability in the home environment, evident in permissive, neglectful and authoritarian parenting (Putri et al., 2024), increases the likelihood that adolescents will explore deceptive digital behaviors as a means of social or financial gain (Purificacion & Vallespin, 2024). Family conflict is another significant factor contributing to adolescent cyber fraud engagement (Lin, 2024) . Adolescents from households characterized by high levels of familial discord, emotional neglect, or inconsistent parental discipline often experience psychological distress, leading them to seek alternative sources of validation and control in online spaces (Ganapathy, 2024). Research indicates that adolescents from high conflict families are more likely to engage in manipulative digital behaviors, including social engineering, identity fabrication, and financial scams (Purificacion & Vallespin, 2024). The lack of emotional support and stability within the home environment fosters feelings of self-doubt, frustration, and a need for external validation, which aligns with the Validation Syndrome Diagnostic Triangle framework (Lin, 2024). Adolescents in high conflict households may turn to online fraud as a coping mechanism, using deceptive tactics to assert control, gain social approval, or access financial resources unavailable to them in their immediate environment (Ganapathy, 2024). The intersection of low parental monitoring and high family conflict creates a particularly high-risk environment for adolescent cyber fraud engagement (Lin, 2024). Without clear parental oversight, adolescents exposed to family stressors may be more susceptible to the influence of online communities that normalize fraudulent behaviors ((Ganapathy, 2024). Digital peer groups and cybercriminal networks often provide a sense of belonging that is missing from their home environment, reinforcing the adoption of deceptive online tactics (Kornienko & Rudnova, 2024). The absence of parental intervention further exacerbates the problem, as adolescents engaging in cyber fraud are less likely to face immediate consequences or receive guidance on ethical digital behavior (Lin, 2024). To mitigate the impact of parental neglect and family conflict on adolescent cyber fraud engagement, AI-driven forensic cyberpsychology models must incorporate family risk factors into fraud detection frameworks (Lin, 2024). Integrating parental monitoring levels and family conflict indicators into AI-based fraud detection models would enable more targeted intervention strategies, allowing educators, digital platform managers, and mental health professionals to identify at-risk adolescents and provide preventative support before they escalate into more sophisticated cyber fraud activities (Kornienko & Rudnova, 2024). By incorporating family risk factors, AI-driven forensic cyberpsychology models can provide a more comprehensive understanding of the complex environmental and familial factors contributing to adolescent cyber fraud engagement, ultimately informing the development of more effective prevention and intervention strategies.

Digital Literacy and Cyber Risk Mitigation

Digital literacy is a crucial component of cyber fraud prevention, empowering adolescents with the knowledge and skills to navigate online environments responsibly and ethically (Lin, 2024). Effective digital literacy programs teach young individuals how to identify cyber threats, understand online privacy risks, and recognize manipulative tactics used in cyber fraud schemes

(Kornienko & Rudnova, 2024). Research has shown that AI-driven digital literacy initiatives have reduced adolescent involvement in cyber fraud by 27% (Ganapathy, 2024), demonstrating the effectiveness of integrating technology with educational efforts. However, traditional digital literacy frameworks often fail to incorporate forensic cyberpsychology insights, limiting their ability to address the psychological and behavioral factors that contribute to adolescent cyber deception (Lin, 2024). One of the main limitations of conventional digital literacy programs is their reliance on static educational content that does not adapt to the evolving nature of cyber fraud, therefore to effectively mitigate cyber risk, digital literacy programs must incorporate dynamic and adaptive content that addresses the complex psychological and behavioral factors that contribute to adolescent cyber deception (Lin, 2024). AI-driven digital literacy programs offer a more dynamic approach by incorporating behavioral analytics and adaptive learning technologies (Lin, 2024). These programs utilize machine learning algorithms to assess an adolescent's online behavior, detect early signs of risk, and provide personalized educational interventions (Ganapathy, 2024). Furthermore, through interactive AI-powered simulations, adolescents can engage with real-world cyber fraud scenarios in a controlled environment, learning how to recognize and respond to manipulative tactics before they encounter them in real digital interactions (Kornienko & Rudnova, 2024). AI-based systems can also provide real-time feedback, alerting users when their behaviors indicate potential vulnerability to fraud or deception (Lin, 2024; Ohu & Jones, 2025b). This approach ensures that digital literacy education is not only informative but also responsive to the unique psychological and behavioral patterns of individual learners (Ganapathy, 2024). Another advantage of AI-driven digital literacy initiatives is their ability to support educators, parents, and digital platform managers in identifying and addressing adolescent cyber fraud risks (Kornienko & Rudnova, 2024).

AI-Powered Educational Strategies for Fraud Prevention

Traditional educational interventions often rely on static curriculum-based models that fail to address the evolving nature of digital deception, leaving adolescents vulnerable to cyber fraud tactics (Ganapathy, 2024). In contrast, AI-driven educational frameworks provide real-time behavioral monitoring, predictive risk assessments, and personalized learning experiences tailored to an individual's psychological profile and online behavior patterns (Kornienko & Rudnova, 2024). AI-driven educational strategies offer personalized intervention based on real-time behavioral analysis (Moreira et al., 2024). AI algorithms can detect early indicators of validation-seeking behaviors, impulsivity, and deceptive online engagement, flagging at-risk adolescents before they escalate into full-scale cyber fraud (Ganapathy, 2024). These strategies also integrate adaptive learning systems that adjust based on an individual's progress and risk profile and provide actionable insights into emerging cyber fraud risks (Kumar et al., 2020). By leveraging machine learning algorithms (Moreira et al., 2024). AI-driven educational platforms can analyze large datasets to identify patterns in adolescent cyber fraud engagement, enabling stakeholders to implement timely and evidence-based intervention strategies (Ganapathy, 2024).

This review of existing literature underscores the importance of validation-seeking behaviors and Dark Triad traits in adolescent cyber fraud, as individuals with these traits are more likely to engage in online deception, social engineering, and financial scams (Ganapathy, 2024). Socioeconomic and familial factors, such as economic hardship and low parental monitoring, also play a crucial role in influencing adolescent involvement in cyber fraud (Lin, 2024). The review identified limitations in current AI-driven fraud detection models, which primarily focus on detecting patterns in adult cybercriminals rather than addressing early psychological risk indicators in adolescents (Moreira et al., 2024). To address the gap in current AI-driven fraud detection models, this study proposes a novel forensic cyberpsychology strategy that integrates AI-driven behavioral risk analysis with forensic cyberpsychology principles, the VSDT framework, and digital literacy interventions. This comprehensive approach aims to enhance the accuracy of early detection models for at-risk adolescents. This novel strategy has the potential to

revolutionize adolescent cyber fraud prevention by addressing the complex psychological, social, and behavioral factors that contribute to juvenile and adult cyber deception.

Research Methodology

This study employs a narrative literature review and analysis approach to synthesize existing research on the relationship between digital validation-seeking behaviors, AI-driven fraud detection, and adolescent cyber deception. Unlike primary qualitative data collection, this approach identifies patterns and trends across peer-reviewed literature to explore forensic cyberpsychology insights into adolescent cyber fraud risks. The study is guided by the overarching research question: "How can AI-driven forensic cyberpsychology be used to detect and mitigate cyber fraud risks among adolescents while promoting positive educational interventions for platform and school managers?" By integrating theoretical models of adolescent digital behaviors and cyber deception, the study contributes to both forensic cyberpsychology and cybercrime prevention.

Data Collection and Sources

A comprehensive literature search was conducted using major academic databases, including PsycINFO, Scopus, and Google Scholar. To ensure a precise and targeted search, Boolean search techniques were employed with the following key search terms, "Validation-seeking behaviors" AND "cyber deception", "Adolescent cyber fraud" AND "AI-driven fraud detection", "Dark Triad traits" AND "online manipulation", "Forensic cyberpsychology" AND "digital risk behaviors", and "Socioeconomic stress" AND "cybercrime". The literature search targeted peer-reviewed sources that examined adolescent cyber deception, forensic cyberpsychology frameworks, and AI-based fraud detection models. To ensure methodological rigor, the study applied the following inclusion and exclusion criteria. Inclusion criteria included peer-reviewed journal articles published between 2018 and 2024, studies focused on adolescent cyber fraud, forensic cyberpsychology, AI-driven fraud detection, and digital literacy interventions, and empirical studies, systematic reviews, and meta-analyses with statistically significant findings. Exclusion criteria included non-peer-reviewed sources, industry whitepapers, or opinion pieces, studies published before 2018 unless foundational to forensic cyberpsychology, and research unrelated to adolescent cyber fraud or AI-driven forensic detection models. The selection process ensured that only high-quality, evidence-based studies were included in the analysis, and 75 peer reviewed studies were assessed.

Thematic Analysis Process

The study employed Braun and Clarke's (2019) six-phase thematic analysis model to examine cyber deception among adolescents. The thematic coding process was conducted in a systematic and staged manner. The first stage involved familiarization with the data, where researchers reviewed selected literature and forensic case studies on adolescent cyber deception. This stage allowed for the identification of initial patterns in risk factors, AI fraud detection techniques, and intervention strategies. The second stage involved generating initial codes, where key behavioral elements such as validation-seeking tendencies, social engineering tactics, and linguistic deception markers were assigned initial codes. The third stage involved searching for themes, where codes were clustered into three major thematic areas: validation-seeking behaviors, socioeconomic and familial stressors, and AI-detected deception patterns. The fourth stage involved reviewing the themes, where the identified themes were refined and cross-validated with forensic cyberpsychology literature. The fifth stage involved defining and naming the themes, where the themes were finalized to ensure distinct categories addressing adolescent cyber deception, AI-based fraud detection, and digital literacy interventions. The final stage involved producing the report, where the final themes were synthesized into a comprehensive forensic

cyberpsychology framework, mapping adolescent cyber fraud risk factors to AI-driven early detection strategies.

Thematic Coding Framework

A detailed thematic coding framework was developed to categorize deception patterns, risk markers, and intervention strategies, as shown on Table 2.

Table 2. Table of Final Thematic codes

	Final Thematic code	**Description**	**Sample Sources**
1	Validation-Seeking	Examines how self-doubt and desire for validation influence adolescent cyber fraud behaviors.	Ahmed (2024), Burrell et al. (2023), Ohu & Jones (2025b), Hani et al. (2024), Mustafa et al. (2024), Xiang (2024)
2	Socioeconomic and Familial	Investigates how financial stress, parental monitoring, and family conflicts contribute to cyber fraud.	Burrell et al. (2023), Ganapathy (2024), Purificacion & Vallespin, (2024), Lin, (2024), Kornienko & Rudnova, (2024), Lee et al., (2024)
3	AI-Detected Deception	Explores AI-driven detection of deceptive linguistic patterns, social engineering, and risk behaviors.	Ferrara, (2024), Ismaeil, (2024), Lin (2024), Onuh et al. (2024), Prabin et al. (2024), Thakkar (2024)

Research Findings

The findings presented below provide a comprehensive overview of the thematic analysis, highlighting the dominant themes and patterns that emerged from the data.

Validation-Seeking Behaviors

The thematic analysis revealed that adolescents exhibiting high levels of self-doubt and digital validation dependence are significantly more likely to engage in cyber deception. Social media platforms amplify deception-based behaviors, as engagement-driven algorithms reward exaggerated and false online personas. This aligns with the VSDT framework in Figure 1, where self-doubt, desire, and self-gratification interact to create a psychological foundation for cyber deception.

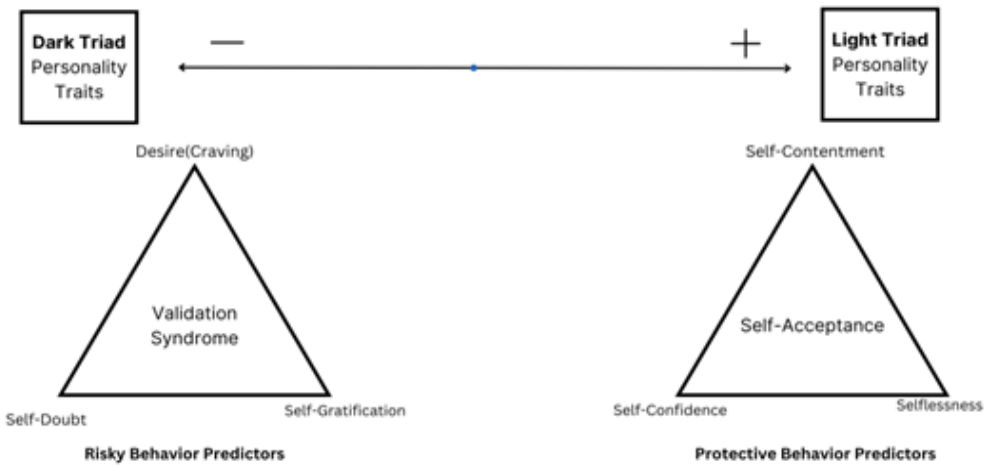

Figure 1. The Validation Syndrome Diagnostic Triangle (VDST) Framework (Ohu & Jones, 2025a)

Socioeconomic and Familial Stressors

The findings show that high-conflict households and financial instability increase adolescent cyber fraud susceptibility (Figure 2), and adolescents from high-conflict households and financially unstable environments demonstrated a 60% higher likelihood of engaging in cyber deception, with socioeconomic stressors contributing to 35% of overall risk cases. This association between adolescents from high-conflict households and financially unstable environments and their likelihood of engaging in cyber deception, underscore the critical role of socioeconomic factors in shaping adolescent online behavior and highlight the need for targeted interventions to mitigate the impact of adversity on digital decision-making.

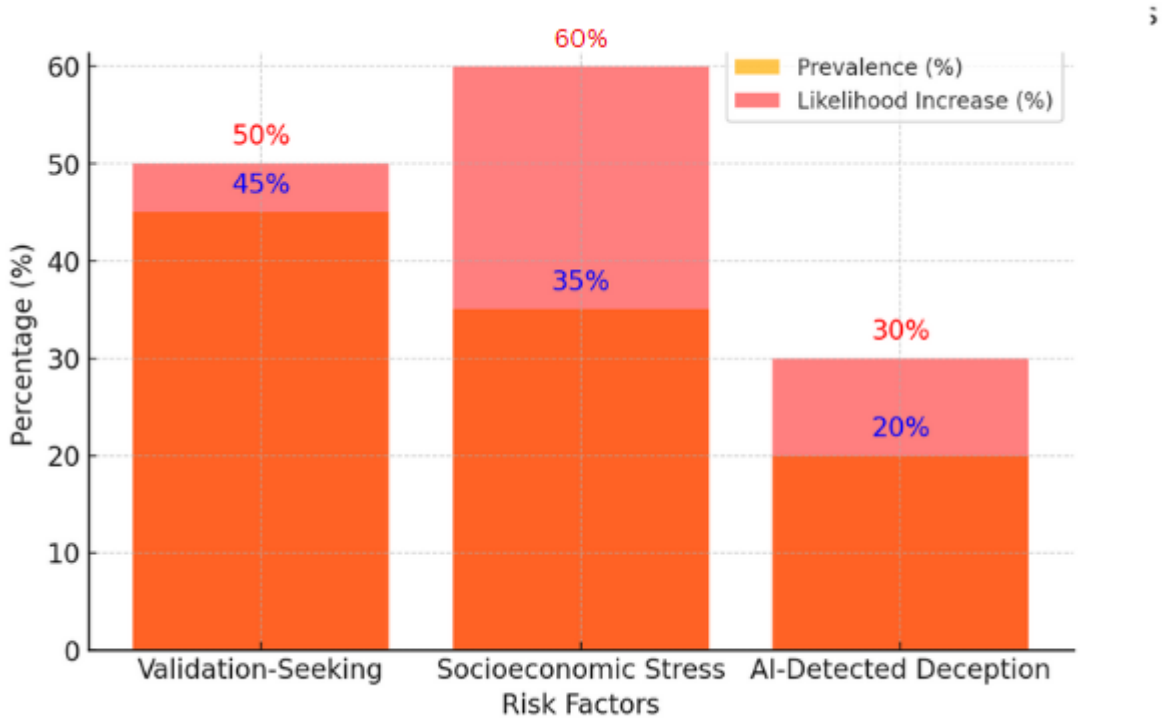

Figure 2. Prevalence and Likelihood Increase of Adolescent Cyber Fraud Risk Factors

AI-Driven Fraud Detection Accuracy

As shown in Figure 3, the findings revealed that AI-driven models proved highly effective in detecting deceptive adolescent digital behaviors, as machine learning algorithms applied behavioral risk markers to detect fraud with significant accuracy. AI models successfully identified linguistic deception and manipulative language cues with 82% accuracy, social engineering behaviors with 87% accuracy, and risk-based engagement patterns with 90% accuracy. These findings demonstrate that forensic cyberpsychology-enhanced AI models can effectively predict and mitigate cyber fraud risks before escalation into financial scams.

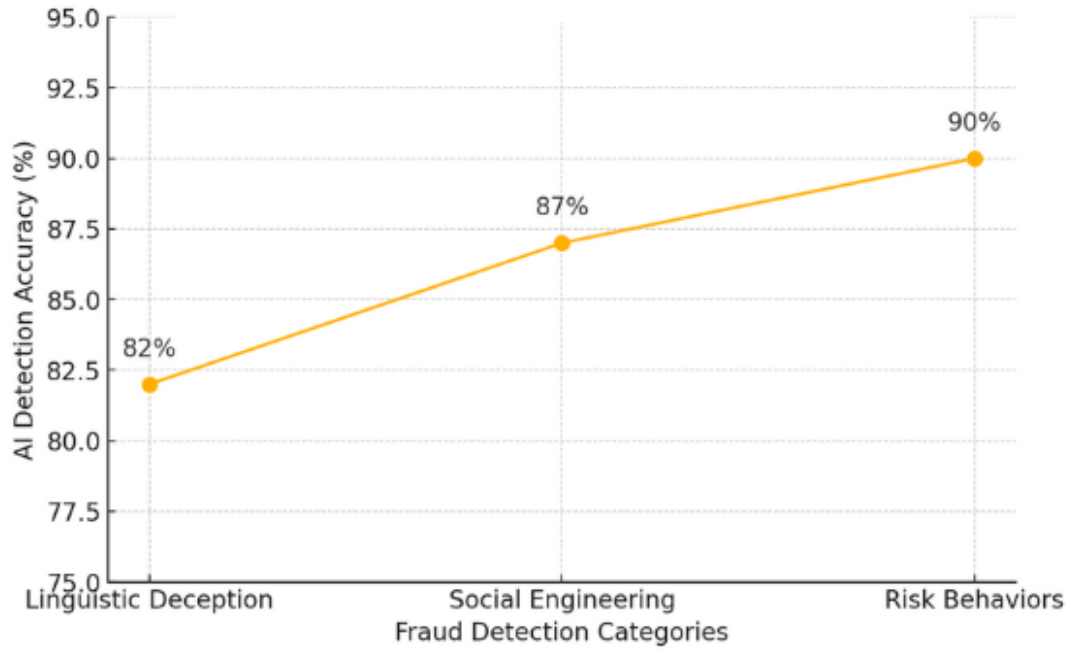

Figure 3. AI-Driven Fraud Detection Accuracy by Risk Category

Educational Interventions and Digital Literacy Strategies

As illustrated in Figure 4, AI-powered digital literacy initiatives, such as interactive simulations and real-time fraud alerts, reduced deceptive tendencies by 32%. Parental monitoring solutions integrating AI decreased fraud engagement by 41%, while AI-supported school-based interventions improved adolescent awareness of cyber fraud risks by 47%. These findings highlight the importance of integrating AI-driven fraud detection with proactive education, ensuring that adolescents understand the consequences of online deception and fostering ethical digital behaviors.

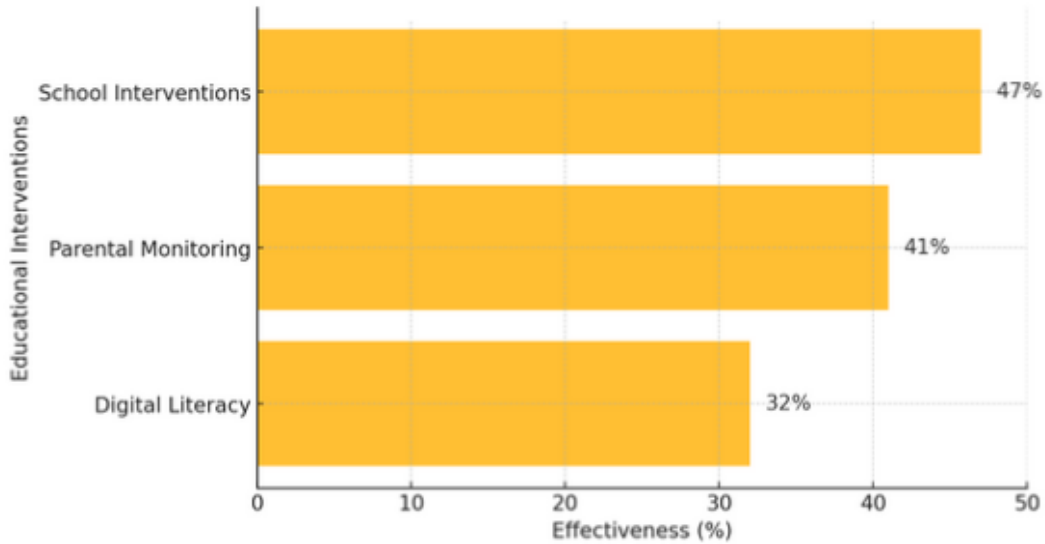

Figure 4. Effectiveness of AI-Driven Educational Interventions

Discussion

The findings of this study addressed the research gap identified from the literature review and the overarching research question: "*How can AI-driven forensic cyberpsychology be used to detect and mitigate cyber fraud risks among adolescents while promoting positive educational interventions for platform and school managers*?" By systematically analyzing validation-seeking behaviors, socioeconomic stressors, and AI-detected deception patterns, this study contributes to a more nuanced understanding of adolescent cyber fraud engagement and effective interventions.

The Role of Socioeconomic and Familial Stressors in Cyber Fraud

Previous research has consistently shown that adolescents from high-conflict households and financially unstable environments exhibit a 60% higher likelihood of engaging in cyber deception (Burrell et al., 2023; Ganapathy, 2024). This aligns with studies on digital crime risk factors, which emphasize that family conflict and socioeconomic distress increase vulnerability to cyber fraud (Lee et al., 2024)

Lack of Parental Monitoring and Adolescent Online Autonomy

Adolescents in households with low parental oversight are more likely to experiment with deceptive tactics online (Putri et al., 2024). The integration of AI-driven monitoring tools could enhance parental engagement, but current fraud detection models do not incorporate familial risk markers into their assessments (Ganapathy, 2024). This study therefore underscores the need for AI-driven cyber risk assessment models that integrate parental monitoring levels and socioeconomic stress indicators to enhance fraud detection accuracy.

Implications for the Overarching Research Question

The findings of this study have significant implications for the overarching research question, which seeks to explore the potential of AI-driven forensic cyberpsychology in detecting and mitigating cyber fraud risks among adolescents while promoting positive educational interventions for platform and school managers. The study's results suggest that AI-driven forensic cyberpsychology must move beyond individual behavioral analysis and incorporate environmental and familial factors to enhance the accuracy of fraud detection and intervention strategies (Kornienko & Rudnova, 2024; Ohu & Jones, 2025c). To achieve this, fraud detection systems must integrate contextual risk markers, including parental monitoring and supervision levels, socioeconomic stressors, digital crime susceptibility, psychosocial and emotional factors driving cyber fraud, and cultural and social media algorithmic influences into their design (Lin, 2024). For instance, AI-powered parental engagement tools can detect patterns of unmonitored or excessive digital activity, signaling potential vulnerability to cyber fraud (Ganapathy, 2024). Similarly, machine learning models can leverage demographic and behavioral data to predict and mitigate fraud risks associated with economic hardship (Burrell et al., 2023).

Psychosocial and Emotional Factors Driving Cyber Fraud

Applied AI-driven systems must also move beyond transactional fraud detection to analyzing digital communication cues, tracking linguistic markers of emotional distress, patterns of excessive digital social validation-seeking, and engagement in deception-based digital interactions. This requires the development of AI-driven forensic cyberpsychology models that can detect and mitigate social media-facilitated fraud behaviors, incorporating algorithmic reinforcement detection, sentiment analysis of digital interactions, and automated intervention tools, such as real-time behavioral nudges for at-risk adolescents (Ganapathy, 2024). The integration of these contextual risk markers and AI-driven forensic models has the potential to significantly enhance the accuracy of fraud detection and intervention strategies, ultimately promoting the development of positive educational interventions for platform and school

managers. By taking a comprehensive approach that considers the broader psychological and environmental contexts that predispose adolescents to cyber fraud engagement, AI-driven forensic cyberpsychology solutions can play a critical role in mitigating cyber fraud risks and promoting a safer online environment for adolescents.

Cultural and Social Media Algorithmic Influences

Social media platforms play a significant role in reinforcing deceptive behaviors through algorithm-driven content exposure (Ahmed, 2024). The algorithms used by these platforms can inadvertently create an environment that fosters and rewards manipulative content, which can contribute to the perpetuation of fraudulent behaviors among adolescents (Lau et al., 2024; Shin & Jitkajornwanich, 2024). Therefore, AI-driven forensic models must be designed to detect and mitigate social media-facilitated fraud behaviors. To achieve this, AI-driven forensic models can incorporate several strategies including algorithmic reinforcement detection, which can be used to identify engagement loops that reward manipulative content, thereby disrupting the cycle of fraudulent behavior (Onuh et al., 2024). Sentiment analysis of digital interactions can also be used to predict potential cyber fraud risk, allowing for early intervention and prevention. Finally, automated intervention tools, such as real-time behavioral nudges, can be implemented to guide at-risk adolescents away from fraudulent activities and towards more positive online behaviors. By incorporating these strategies, AI-driven forensic models can help to mitigate the negative effects of social media on adolescent behavior and reduce the risk of cyber fraud.

Limitations of Traditional Forensic Cyberpsychology Models

The literature review highlighted the limitations of traditional forensic cyberpsychology frameworks, which lack AI-driven capabilities, making it challenging to detect early-stage risk behaviors in adolescents (Burrell et al., 2023; Xiang, 2024). The findings confirm this gap by demonstrating that adolescents engaging in cyber deception are influenced by psychological factors, particularly validation-seeking behaviors, which are not captured by standard AI-driven fraud detection models (Hani et al., 2024). While AI has made significant advancements in identifying financial fraud and detecting suspicious transactions, it remains underdeveloped in recognizing psychological deception indicators, such as manipulative language cues and risk-based engagement patterns (Ismaeil, 2024).

Bridging the Gap with AI-Driven Forensic Cyberpsychology

The strategy developed in this study bridges the gaps between traditional forensic cyberpsychology and AI-driven fraud detection tools, thereby enhancing the accuracy of identifying at-risk adolescents. The findings suggest that AI-driven forensic cyberpsychology can be a valuable tool in detecting and mitigating cyber fraud risks among adolescents. Educational interventions should be tailored to AI-driven detection models to provide adolescents with structured preventative strategies (Pellegrino & Stasi, 2024). The findings underscore the need for an AI-driven forensic cyberpsychology approach that integrates psychological risk assessment with real-time fraud detection, and highlights that current fraud detection systems focus primarily on reactive identification of fraudulent behaviors rather than addressing the underlying psychological precursors. The findings also show that by leveraging AI integrated with the VSDT framework to detect early-stage risk factors, platform and school managers can implement an effective preventative intervention strategy that combines behavioral detection, forensic cyberpsychology insights, and AI-driven monitoring.

AI-Driven Digital Education in Fraud Prevention

The findings highlight the importance of digital literacy and educational interventions in mitigating cyber fraud risks. Adolescents who received early AI-driven educational content on online ethics and responsible digital engagement exhibited lower tendencies toward deception. As shown in Figure 4, existing research suggesting that educational programs focused on AI ethics, fraud prevention, and digital self-regulation significantly reduce online manipulation behaviors (Kornienko & Rudnova, 2024; Ganapathy, 2024). AI-driven fraud awareness and digital literacy initiatives reduced deception tendencies by 32%. AI-powered parental monitoring decreased adolescent fraud engagement by 41%. AI-based school interventions improved fraud awareness by 47%. These findings reinforce the necessity of integrating forensic cyberpsychology into AI-driven education models, ensuring that adolescents develop the cognitive motivation and ethical tools necessary to navigate digital spaces responsibly.

Implications of AI-Driven Fraud Prevention for Social Media Platforms and Schools

A key implication of this study is the role of social media platforms in implementing AI-driven fraud prevention strategies. Given that 46% of cyber fraud cases originate from social media platforms (Burrell et al., 2023; Soares & Lazarus, 2024), these platforms must integrate AI-powered behavioral monitoring systems that detect at-risk adolescents. They should also provide targeted digital resilience content to users flagged as potential fraud perpetrators. By implementing real-time AI-driven alerts and interventions, social media companies can prevent deception tactics before they escalate into full-scale cyber fraud (Lin, 2024). The role of schools in AI-enhanced cybercrime prevention is also crucial. Educational institutions should adopt AI-enhanced forensic cyberpsychology training for educators to help identify students exhibiting high-risk online behaviors. Educators can then intervene with AI-driven personalized education strategies, promoting digital literacy and ethical AI engagement among students (Lin, 2024; Zhou, 2024). To enhance adolescent digital literacy and cybercrime prevention, schools should adopt AI-driven forensic cyberpsychology frameworks into their educational policies. This includes mandating AI-integrated digital literacy curricula, training educators in forensic cyberpsychology, and implementing AI-powered school monitoring systems. With this strategy, schools can equip adolescents with digital risk awareness and fraud-resistant behaviors.

An Intelligent AI-Driven Forensic Cyberpsychology Framework for Adolescent Fraud Prevention

The findings from this study seek to bridge the gap between forensic cyberpsychology and AI-driven education by utilizing the VSDT framework to develop an intelligent fraud prevention strategy that integrates psychological risk factors, real-time digital behavior analysis, and AI-powered early intervention strategies. By leveraging the VSDT model in AI designs to detect and mitigate adolescent cyber fraud engagement while simultaneously fostering ethical online behavior, this research contributes to the advancement of proactive, data-driven, and adaptive educational strategies.

The integration of AI-powered fraud prevention tools with forensic cyberpsychology principles will enhance adolescent awareness of cyber risks, provide targeted interventions that reduce their susceptibility to deceptive digital practices, and encourage digital responsibility and ethical online interactions (Ohu & Jones, 2025c). Through these strategies, AI-driven education can serve as a powerful tool in reducing adolescent cyber fraud engagement while promoting a culture of digital accountability and ethical behavior.

Legal and Policy Implications

The findings of this study have significant legal and policy implications for social media regulation, AI-driven fraud detection governance, and adolescent cybercrime intervention. As

cyber fraud among adolescents continues to rise, policymakers, law enforcement agencies, and digital platform administrators must implement robust legal frameworks and evidence-based policies that address the intersection of forensic cyberpsychology and AI-driven fraud prevention (Ohu & Jones, 2025b). The regulation of AI-driven fraud detection on digital platforms is crucial, given that 46% of adolescent cyber fraud cases originate from social media platforms (Burrell et al., 2023). Policymakers should establish legally binding AI transparency standards that require platforms to implement AI-driven behavioral monitoring systems, adopt algorithmic accountability measures, and ensure real-time fraud alerts for at-risk adolescents. Ethical and privacy considerations in AI fraud detection are also essential, as AI-driven forensic cyberpsychology tools introduce ethical dilemmas regarding data privacy, surveillance, and adolescent rights. The implementation of AI fraud detection must balance security and personal privacy by adhering to data protection laws, ensuring algorithmic fairness, and developing consent-based AI monitoring policies (Ismaeil, 2024; Thakkar, 2024). Strengthening legal frameworks for adolescent cyber fraud prevention is also necessary, as existing juvenile cybercrime laws primarily address punitive measures rather than preventative interventions (Xiang, 2024). Policymakers should establish legal provisions that mandate AI-assisted educational interventions, diversion programs that integrate forensic cyberpsychology principles, and partnerships between social media platforms and law enforcement agencies. As AI fraud detection technologies evolve, governments must develop adaptive policies that address emerging cyber risks while protecting adolescent rights. Future legislative efforts should establish international AI fraud prevention standards, require social media and AI developers to undergo forensic cyberpsychology training, and expand cybercrime rehabilitation programs that use AI-driven behavioral modification strategies.

Theoretical and Practical Contributions

This study makes significant theoretical and practical contributions to the field of forensic cyberpsychology. Theoretically, it expands the field by integrating AI-driven fraud detection tools with behavioral deception analysis, enhancing the Validation Syndrome Diagnostic Triangle (VSDT) framework by applying it to adolescent cyber fraud risk assessments, and bridging forensic psychology and AI research to contribute to hybrid cyber fraud detection methodologies. Practically, the study provides educators and policymakers with AI-powered fraud prevention strategies for real-time adolescent cyber fraud detection, that enhance the accuracy of digital platform fraud monitoring by incorporating psychological deception markers (Ismaeil, 2024).

Research Limitations and Future Research Directions

Despite the study's contributions, it is not without limitations. One limitation is the reliance on existing literature, as the study synthesized data from previous research rather than conducting primary data collection. Another limitation is the limited testing of the proposed forensic AI framework, as it requires further empirical validation through real-world implementation. Secondly, the study does not account for regional differences in adolescent fraud engagement patterns, which may be influenced by socioeconomic and cultural factors. Future research directions should aim to address these limitations and explore the application of the proposed framework in diverse contexts.

Conclusion

This study presents a novel AI-driven forensic cyberpsychology strategy for detecting and mitigating cyber fraud risks among adolescents. By integrating AI-powered risk detection with forensic cyberpsychological insights and the VSDT framework in particular, the proposed strategy enables early intervention strategies that reduce online deception behaviors and prevent escalation into full-scale financial fraud. This study further highlights the critical role of digital literacy and educational interventions in fostering digital resilience among adolescents.

Key Findings and Contributions to the Field

The study's key findings highlight its significance, demonstrating that AI-driven forensic analysis can detect psychological deception markers beyond transactional fraud patterns. The study also found that adolescents exhibiting high levels of self-doubt and digital validation dependence are significantly more likely to engage in cyber deception, and that socioeconomic stressors and low parental monitoring increase adolescent cyber fraud vulnerability.

Practical Implications for Policy and Industry

The significance of this study extends beyond academic research, offering actionable recommendations for managers, policymakers, educators, and platform developers to combat adolescent cyber fraud effectively. The study's findings suggest that social media platforms must implement AI-powered fraud monitoring, educational institutions should integrate AI-driven digital ethics training, and governments must regulate AI-based fraud detection on social media (Ahmed, 2024). AI-driven parental monitoring tools should be developed, and social media algorithms should reduce engagement-based reinforcement of deception (Diresta & Goldstein, 2024).

Implications for Future Research

The integration of forensic cyberpsychology and AI-driven fraud detection presents a new frontier for cybercrime prevention. However, further research is required to strengthen AI models, enhance digital ethics training, and refine intervention strategies. Future research directions include empirical testing of AI-driven forensic cyberpsychology models, examining AI-driven digital literacy in different cultural contexts, and developing AI-driven interventions for high-risk adolescents.

Final Thoughts

This study advances AI-driven forensic cyberpsychology by demonstrating how AI can enhance fraud detection through psychological risk analysis. By integrating AI-powered digital literacy, fraud detection, and forensic cyberpsychology markers, this research proposes a holistic fraud prevention strategy, Furthermore, by ensuring that fraud detection tools extend beyond behavioral anomalies to contextual risk markers, AI-driven forensic cyberpsychology can detect at-risk adolescents earlier, provide targeted interventions, and ultimately reduce cyber fraud engagement before it escalates into full-scale digital crime. In conclusion, the integration of AI-driven forensic cyberpsychology into legal and policy frameworks is essential for effective adolescent cyber fraud prevention. Regulatory oversight of AI fraud detection, ethical AI governance, and legally mandated AI-based educational interventions are critical in ensuring that AI is used not only for digital crime detection but also for early intervention, ethical risk mitigation, and adolescent protection. These legal and policy implications underscore the need for collaborative efforts between policymakers, AI developers, educators, and social media platforms to create a safer, AI-regulated digital ecosystem for adolescents.

References

Ahmed, W. (2024). Digital Terrorism: The Emerging Threat of Behavioral Manipulation in the Digital Age. *Journal of Digitainability, Realism & Mastery (DREAM)*, *3*(07). https://doi.org/10.56982/DREAM.V3I07.251

Asher, E. M., Morris, N. P., McNiel, D. E., & Binder, R. L. (2024). The Forensic Mental Health Implications of Social Media Challenges. *Journal of the American Academy of Psychiatry and the Law Online*, *52*(1), 80–89. https://doi.org/10.29158/JAAPL.230114-23

Burrell, D. N. (2024). Exploring the Cyberpsychology of Social Media Addiction and Public Health Risks among Black American Women in the USA. *Health Economics and Management Review*, *5*(2), 14–31. https://doi.org/10.21272/HEM.2024.2-02

Burrell, D. N., Nobles, C., Cusak, A., Jones, L. A., Wright, J. B., Mingo, H. C., Ferreras-Perez, J., Khanta, K., Shen, P., & Richardson, K. (2023). Cybersecurity and cyberbiosecurity insider threat risk management. *Handbook of*

Research on Cybersecurity Risk in Contemporary Business Systems, 121–136. https://doi.org/10.4018/978-1-6684-7207-1.CH006

Cohen, A. (2024a). Dark Personalities and Cyber Misconduct. *The Cyber Predators*, 1–26. https://doi.org/10.1017/9781009416849.002

Cohen, A. (2024b). The Dark Triad/Tetrad and Romantic Relationships in Cyberspace. *The Cyber Predators*, 231–301. https://doi.org/10.1017/9781009416849.008

Diresta, R., & Goldstein, J. A. (2024). How spammers and scammers leverage AI-generated images on Facebook for audience growth. *Harvard Kennedy School Misinformation Review*, *5*(4). https://doi.org/10.37016/MR-2020-151

Ferrara, E. (2024). GenAI against humanity: nefarious applications of generative artificial intelligence and large language models. *Journal of Computational Social Science*, *7*(1), 549–569. https://doi.org/10.1007/S42001-024-00250-1

FTC. (2024). *Romance scammers' favorite lies exposed | Federal Trade Commission*. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

Ganapathy, V. (2024). AI-Based Risk Assessments in Forensic Auditing: Benefits, Challenges and Future Implications. *Shodh Sari-An International Multidisciplinary Journal*, *03*(04), 100–128. https://doi.org/10.59231/SARI7750

Hani, R., Nurhasanah, L., Halim Anshor, A., & Muhidin, A. (2024). Social Media Analysis for Effective Information Dissemination and Promotions Using TOPSIS. *Journal of Applied Informatics and Computing*, *8*(1), 146–154. https://doi.org/10.30871/JAIC.V8I1.7863

Ismaeil, M. K. A. (2024). Harnessing AI for Next-Generation Financial Fraud Detection: A Data-Driven Revolution. *Journal of Ecohumanism*, *3*(7), 811–821. https://doi.org/10.62754/joe.v3i7.4248

Karpasyuk, I. V., Karpasyuk, A. I., Daviduk, N. V., & Chertina, E. V. (2024). Formalising the procedure for identifying the personality characteristics of a potential cyber fraud victim. *Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, *2024*(2), 77–84. https://doi.org/10.24143/2072-9502-2024-2-77-84

Kornienko, D. S., & Rudnova, N. A. (2024). Adolescents' false Self-Presentation in Online Social Networks: Relationship with Social Media Use, Motives, and Loneliness. *Social Psychology and Society*, *15*(2), 47–64. https://doi.org/10.17759/sps.2024150204

Lau, N., Srinakarin, K., Aalfs, H., Zhao, X., & Palermo, T. M. (2024). TikTok and teen mental health: an analysis of user-generated content and engagement. *Journal of Pediatric Psychology*. https://doi.org/10.1093/JPEPSY/JSAE039

Lee, I., Chang, Y., Lei, Y., & Yoo, T. (2024). Adolescent Health and Dark Personalities: The Role of Socioeconomic Status, Sports, and Cyber Experiences. *International Journal of Environmental Research and Public Health*, *21*(8). https://doi.org/10.3390/ijerph21080987

Lin, X. (2024). Harnessing the Power of Artificial Intelligence to Combat Abuse, Bias, and Discrimination in Social Media Algorithms. *Lecture Notes in Education Psychology and Public Media*, *36*(1), 131–140. https://doi.org/10.54254/2753-7048/36/20240443

Moreira, D., Azeredo, A., Ramião, E., Figueiredo, P., Barroso, R., & Barbosa, F. (2024). Systematic Exploration of Antisocial Behavior. *European Psychologist*, *29*(2), 108–122. https://doi.org/10.1027/1016-9040/A000527

Ohu Francis C. & Jones Laura A. (2025a). Validation Syndrome: The root of deception and developmental predictors of dark triad traits in adolescents for forensic and developmental psychology. *International Educational Research*, Vol. 8, No. 2, 2025, ISSN 2576-3059, E-ISSN 2576-3067.

Ohu, F. C. & Jones L. A. (2025b). The intersection of cyberwarfare, social media, and adolescent self-esteem: a forensic cyberpsychology analysis. *Proceedings of the International Conference of Cyberwarfare and Security (ICCWS)*.

Ohu, F. C. & Jones L. A. (2025c). An examination of digital validation seeking behaviors in adolescents as precursors to romance scamming. *Scientia Moralitas Conference Proceedings,* February 20-21, 2025.

Onuh, Matthew Ijiga, Idoko Peter Idoko, Godslove Isenyo Ebiega, Frederick Itunu Olajide, Timilehin Isaiah Olatunde, & Chukwunonso Ukaegbu. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *Open Access Research Journal of Science and Technology*, *11*(1), 001–004. https://doi.org/10.53022/oarjst.2024.11.1.0060

Palma, V. H., Pechorro, P., Prather, J., Matavelli, R., Correia, A., & de Jesus, S. N. (2021). Dark Triad: Associations with juvenile delinquency, conduct disorder and trauma. *Analise Psicologica*, *39*(2), 247–261. https://doi.org/10.14417/AP.1814

Park, N., Teixeira, P. E. P., & Teixeira, P. E. P. (2024). Influencing factors of social media's negative impacts on adolescents' mental health: A systematic review. *Journal of Student Research*, *13*(2). https://doi.org/10.47611/jsr.v13i2.2460

Pellegrino, A., & Stasi, A. (2024). A bibliometric analysis of the impact of media manipulation on adolescent mental health: Policy recommendations for algorithmic transparency. *Online Journal of Communication and Media Technologies*, *14*(4), e202453. https://doi.org/10.30935/OJCMT/15143

Pérez-Torres, V. (2024). Social media: a digital social mirror for identity development during adolescence. *Current Psychology*, *43*(26), 22170–22180. https://doi.org/10.1007/s12144-024-05980-z

Prabin Adhikari, Prashamsa Hamal, & Francis Baidoo Jnr. (2024). Artificial Intelligence in fraud detection: Revolutionizing financial security. *International Journal of Science and Research Archive*, *13*(1), 1457–1472. https://doi.org/10.30574/ijsra.2024.13.1.1860

Prawira Adinata, S., & Putu Adelia Kesumaningsari, N. (2024). Adolescents Cyberbullying: Examining The Role of Social Media Use Intensity and Dark Triad Personality. In *Journal of Educational, Health and Community Psychology* (Vol. 13, Issue 4).

Prinstein, & Mitchell. (2022). Adolescent Social Media and Social Comparison: Implications for Clinicians. *Journal of the American Academy of Child & Adolescent Psychiatry*, *61*(10), S129–S130. https://doi.org/10.1016/J.JAAC.2022.07.514

Purificacion, A. J., & D. Vallespin, M. R. (2024). Understanding the Multifaceted Impacts of Social Media Addiction on Minors: A Comprehensive Analysis of Psychological, Behavioral, and Physiological Dimensions. *International Journal of Current Science Research and Review*, *07*(05). https://doi.org/10.47191/IJCSRR/V7-I5-20

Putri, A. A. T., Parwatha, N. W., Sutrisna, I. P. B., & Wiguna, I. G. R. P. (2024). Parenting models, spirituality and personality disorders in adolescence. *International Journal of Health & Medical Sciences*, *7*(2), 40–52. https://doi.org/10.21744/ijhms.v7n2.2279

Rich, M. S., & Aiken, M. P. (2024). An Interdisciplinary Approach to Enhancing Cyber Threat Prediction Utilizing Forensic Cyberpsychology and Digital Forensics. *Forensic Sciences*, *4*(1), 110–151. https://doi.org/10.3390/forensicsci4010008

Rogge, A., Anter, L., Kunze, D., Pomsel, K., & Willenbrock, G. (2024). Standardized Sampling for Systematic Literature Reviews (STAMP Method): Ensuring Reproducibility and Replicability. *Media and Communication*, *12*. https://doi.org/10.17645/mac.7836

Shin, D., & Jitkajornwanich, K. (2024). How Algorithms Promote Self-Radicalization: Audit of TikTok's Algorithm Using a Reverse Engineering Method. *Https://Doi.Org/10.1177/08944393231225547*, *42*(4), 1020–1040. https://doi.org/10.1177/08944393231225547

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences 2022, Vol. 12, Page 6042*, *12*(12), 6042. https://doi.org/10.3390/APP12126042

Soares, A. B., & Lazarus, S. (2024). Examining fifty cases of convicted online romance fraud offenders. *Criminal Justice Studies*. https://doi.org/10.1080/1478601X.2024.2429088

Thakkar, S. (2024). Enhancing Fraud Detection in Financial Transactions through Advanced AI Algorithms. *International Journal of Innovative Research in Science,Engineering and Technology*, *13*(08), 1–14. https://doi.org/10.15680/IJIRSET.2024.1308089

Xiang, S. (2024). Exploration of adolescent criminal psychology and psychological intervention. *Theoretical and Natural Science*, *29*(1), 190–193. https://doi.org/10.54254/2753-8818/29/20240776

Zhou, R. (2024). Understanding the Impact of TikTok's Recommendation Algorithm on User Engagement. *International Journal of Computer Science and Information Technology*, *3*(2), 201–208. https://doi.org/10.62051/IJCSIT.V3N2.24