Jurnal Komunikasi: Malaysian Journal of Communication
https://ejournal.ukm.my/mjc
Jilid 41(1) 2025: 107-124

A Systematic Literature Review on Online Scams: Insights into Digital Literacy, Technological Innovations, and Victimology

MUHAMMAD ADNAN PITCHAN*
Universiti Kebangsaan Malaysia

ALI SALMAN
Universiti Malaysia Kelantan

NADHIRAH MUHAMAD ARIB
Universiti Teknologi Malaysia

ABSTRACT

The rapid proliferation of digital technologies has ushered in a new era of connectivity while simultaneously exposing users to an increasingly complex landscape of online scams. This systematic literature review synthesizes findings from over 40 recent studies to explore the multifaceted dimensions of online fraud. Framed by three research questions, the review examines the role of digital literacy in mitigating scam vulnerability, evaluates advanced technological methodologies for fraud detection, and investigates the socio-demographic and psychological factors influencing victim recovery. Methodologically, the study employs the PRISMA framework, a widely used guideline for systematic reviews, to ensure rigor in the identification, screening, and selection of peer-reviewed articles published between 2020 and 2024. Key findings highlight the critical role of digital literacy and financial education in empowering individuals against online fraud, with nuanced challenges posed by overconfidence and limited awareness campaigns. Technological advancements, particularly in machine learning and artificial intelligence, demonstrate transformative potential in fraud detection, achieving accuracy rates exceeding 90% in various applications. Additionally, victimology research underscores the emotional and psychological toll of scams, emphasizing the need for tailored support mechanisms and community-driven awareness initiatives. The review identifies significant implications for policy, practice, and future research, advocating for interdisciplinary collaboration to enhance digital resilience. By integrating education, technology, and regulatory measures, this study provides a comprehensive roadmap for addressing the evolving threat of online scams, ensuring a safer digital ecosystem for individuals and institutions alike.

Keywords: *Online scams, digital literacy, fraud detection, cybersecurity, victimology.*

INTRODUCTION

The rapid proliferation of digital technologies has transformed how individuals interact, communicate, and conduct transactions in the modern era. This unprecedented connectivity has, however, exposed users to a spectrum of cyber threats, among which online scams are a significant and pervasive issue. These scams, leveraging the digital domain's anonymity and reach, have evolved in complexity, scale, and impact. From phishing and smishing to

*Corresponding author: adnan86@ukm.edu.my
E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2025-4101-07
Received: 14 February 2025 | Accepted: 20 February 2025 | Published: 30 March 2025

cryptocurrency fraud and social engineering attacks, the digital landscape is fraught with innovative yet malicious schemes that exploit human and technological vulnerabilities.

Online scams manifest in diverse forms, targeting individuals, businesses, and governments alike. For instance, Abu-Salih et al. (2024) investigate multi-topic social spam detection on platforms like Twitter, proposing a novel machine learning approach that combines topic-dependent and topic-independent behaviour analysis. This study highlights the importance of identifying spammers' activities across varying topics to improve detection efficacy. Similarly, Haq et al. (2024) address the issue of phishing URLs, introducing a deep learning-based system utilizing a 1D convolutional neural network that achieved an impressive accuracy of 99.7% in detecting phishing attempts. These contributions underscore the critical role of advanced algorithms in tackling online threats. Beyond technical methodologies, studies also explore the socio-economic and psychological dimensions of online scams. Luo (2024) provides a detailed examination of the industrialization of cybercrime in China, shedding light on how cybercriminal organizations mimic legitimate firms in structure and operation. Suzuki (2024), on the other hand, investigates consumer fraud victimization in Japan, emphasizing the role of routine activities and social networking behaviours in influencing fraud risk. These findings reveal the multi-faceted nature of online scams, necessitating interdisciplinary approaches to address their complexities.

Advancements in artificial intelligence (AI) have further revolutionized the threat landscape. Schmitt and Flechais (2024) delve into the implications of generative AI in amplifying social engineering attacks, presenting a framework that integrates realistic content creation, advanced targeting, and automated attack infrastructure. This study emphasizes the dual-edged nature of AI—as a tool for both enabling and countering cyber threats. Similarly, Mahmud et al. (2024) propose a hybrid deep learning model for detecting smishing attacks, achieving unparalleled accuracy through the integration of Bidirectional Gated Recurrent Units (Bi-GRUs) and Convolutional Neural Networks (CNNs). The integration of contextual knowledge into cybersecurity models has emerged as a promising avenue. Mahmud et al. (2024) introduce AIIOC, a novel model for extracting Indicators of Compromise (IOC) using a multi-granularity attention mechanism and symbolic rule encoding, achieving significant improvements in accuracy and interpretability. Sudar et al. (2024) focus on adversarial phishing detection, leveraging web-scraped features and ensemble learning algorithms to develop an interactive tool for URL verification. These studies demonstrate the growing emphasis on enhancing model robustness and user accessibility in combating online scams.

Financial and cryptocurrency fraud represents another critical domain within online scams. Isaia et al. (2024) examine the protective role of financial literacy against online fraud, identifying overconfidence as a risk factor. Gürfidan (2024) proposes RG-Guard, a deep learning-powered system for detecting suspicious cryptocurrency transactions in metaverse ecosystems. The system's ability to block high-risk transactions in real-time marks a significant advancement in preventing financial fraud. Financial and cryptocurrency fraud remains a major threat in the rapidly evolving digital landscape. With the increasing adoption of digital assets and blockchain technology, cybercriminals have become more sophisticated in exploiting vulnerabilities within online financial systems. The decentralised and difficult-to-trace nature of cryptocurrencies provides an ideal avenue for various types of fraud, including

fake investment schemes, Ponzi scams, and market manipulation designed to deceive inexperienced investors. The lack of strict regulations and limited public understanding of cryptocurrency further contribute to heightened risks in this ecosystem. To combat these challenges, online fraud prevention measures must be comprehensive and effective. Technologies such as artificial intelligence (AI) and big data analytics can enhance the detection of suspicious transaction patterns with greater speed and accuracy. Additionally, stricter regulatory frameworks for digital asset trading platforms are essential to ensuring transparency and accountability in financial transactions.

However, technology alone is not enough without improved public awareness. Many individuals still fall victim to scams promising high returns in a short period without fully understanding the associated risks. Therefore, digital financial education must be strengthened to help people recognise fraudulent tactics and protect themselves from becoming victims. Moreover, close collaboration between governments, financial institutions, and technology industry players is crucial in creating a safer digital financial ecosystem. Initiatives such as establishing monitoring centres for suspicious transactions, providing efficient fraud reporting channels, and imposing stricter penalties on cybercriminals can significantly reduce online fraud cases. As the digital world continues to evolve, so do the threats of online fraud. Therefore, a continuous, innovative, and adaptable approach is necessary to safeguard users in an increasingly complex digital financial environment.

This systematic literature review (SLR) presents a comprehensive analysis of online scams in the digital age, synthesizing insights from recent advancements in detection, mitigation, and prevention techniques. Structured around three primary research questions, this review explores the role of digital literacy in reducing vulnerability to online scams, the effectiveness of various technological methods in detecting and preventing online fraud, and the impact of victim demographics and societal perceptions on the recovery process for scam victims.

By addressing these questions, the review provides a holistic perspective on the current state of online scam detection and prevention. Given the interdisciplinary nature of online scam research, where psychology explores victim susceptibility, law enforcement tackles legal frameworks, and technology drives detection mechanisms, this study integrates insights from these domains to present a comprehensive analysis. It collates findings from diverse methodologies, contexts, and domains to offer researchers, practitioners, and policymakers a deeper understanding of the evolving threat landscape and the innovative solutions being developed to counteract online scams. The findings underscore the critical role of digital literacy in empowering individuals, the importance of technological innovation in fraud prevention, and the influence of societal and demographic factors on victim recovery. Therefore, this study aims to bridge existing knowledge gaps by systematically reviewing the latest developments in scam prevention and identifying areas for future research. This SLR highlights the need for continuous advancements in technology, education, and policy to enhance digital safety, foster resilience against cyber threats, and maintain trust in the digital ecosystem.

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2025-4101-07

LITERATURE REVIEW

Online scams have become a pervasive issue in the digital age, leveraging technological advancements to exploit vulnerabilities in human behaviour, systems, and organizational frameworks. This review synthesizes findings from various studies to understand the nature of scams, their psychological and technical dimensions, and strategies for prevention and mitigation. Behavioural dependencies like internet addiction significantly contribute to individuals' susceptibility to scams. Internet addiction, characterized by compulsive engagement with online gaming, social media, and other digital activities, creates opportunities for scammers to exploit victims through identity theft and fraudulent activities. Deindividuation and anonymity in online interactions further amplify this risk, necessitating public health programs aimed at awareness and prevention (Kakulte et al., 2024). Similarly, Wilson et al. (2024) explore scam susceptibility in Malaysia, revealing that public attitudes, limited awareness, and insufficient law enforcement exacerbate vulnerabilities. These findings underscore the dynamic nature of online scams and the urgent need for adaptive prevention strategies.

The linguistic strategies employed by scammers reveal sophisticated techniques designed to manipulate targets. A study analysing failed scams in the Filipino language highlights the use of persuasive elements like emotional appeal, credibility, and logical arguments. These strategies are supported by specific linguistic markers, such as cognitive verbs and pronouns, that scammers use to create trust and urgency in their communications. Understanding these strategies can guide the development of more effective fraud prevention systems (Ibañez, 2024). Online transaction fraud continues to threaten the security of financial systems. Modern approaches leveraging statistical and machine learning models have proven effective in identifying fraudulent patterns. However, these methods face limitations in adapting to dynamic fraud behaviours. A survey comparing detection algorithms provides insights into their performance in terms of accuracy, sensitivity, and specificity, offering a roadmap for future research (Huke et al., 2024).

Graph Neural Networks (GNNs) offer significant advancements in fraud detection by aggregating transaction data into patterns that traditional method often misses. By employing relational graph convolutional networks, researchers demonstrated that GNNs outperform classical machine learning and deep learning methods in identifying coordinated fraudulent activities (Harish et al., 2024). The introduction of FraudNLP, a publicly available dataset for online fraud detection, further facilitates novel applications of natural language processing in identifying scam patterns (Boulieris et al., 2024).

Identity theft, particularly in the FinTech industry, has been identified as a predominant form of online fraud. Preventive strategies, including modernized detection models and regulatory measures, are crucial to combat these challenges effectively (Saluja, 2024). Similarly, phishing attacks remain a persistent threat, effectively addressed through ensemble learning techniques that combine models like Random Forest, Support Vector Machines, and CatBoost to improve detection accuracy and recall (Singh et al., 2024). Qu and Cheng (2024) introduce self-supervised learning techniques for credit card fraud detection, which enhance performance by addressing data imbalance and noise. Effective anti-fraud measures require robust policy frameworks and collaboration among stakeholders. Musa and

Jacob (2024) advocate for legislative approaches that align with emerging trends and risk management principles. In the financial sector, Chhabra Roy and P. (2024) propose a proactive cyber fraud response framework integrating early warning systems with machine learning models to mitigate risks in real-time. The metaverse, a convergence of augmented reality (AR) and virtual reality (VR), introduces unique challenges in cybersecurity. Privacy concerns and perceived risks significantly impact user behaviour, creating vulnerabilities for identity theft and digital asset loss. Theoretical models and actionable strategies are essential to enhance user protection in these dynamic virtual environments (Al-Emran et al., 2024; Gaurav et al., 2024).

Victimology studies provide valuable insights into the psychological and emotional impact of scams. Sentiment analysis of victim narratives shows distinct emotional stages during fraud victimization, emphasizing the importance of tailored intervention strategies (J. Wang et al., 2024). Early detection methods, such as honeytokens in relational databases, can complement existing security measures by providing organizations with tools to identify and mitigate data breaches promptly (Prabahker et al., 2024). Psychological manipulation is a cornerstone of online scams, exploiting human vulnerabilities such as trust, fear, and urgency. Ibañez (2024) investigates scams in Filipino online transactions, identifying linguistic markers such as personal pronouns and emotional language used to deceive targets. Similarly, Yu et al. (2024) analyse victims' emotional trajectories, showing transitions from anticipation to anxiety and eventual distrust

The role of victim service providers in addressing identity theft and financial fraud is critical. Organizational factors like external partnerships and availability of support services significantly influence their effectiveness. Enhancing these services through logistical improvements and policy support can mitigate the impact of cybercrimes on victims (Maher et al., 2024). Furthermore, public awareness campaigns and collaborative efforts between stakeholders are essential to foster resilience against scams. Interviews with stakeholders, including scammers, highlight the need for coordinated strategies to improve cybersecurity education and enforcement (Wilson et al., 2024). The COVID-19 pandemic has shaped the landscape of cybercrime, with stay-at-home orders creating opportunities for scammers to exploit digital platforms. Studies reveal that the digital realm challenges traditional crime theories, underscoring the need for a nuanced understanding of cybercrime patterns during societal disruptions (Goncalves & Stafford, 2024). Routine activity theory, when applied to cybercrime victimization, provides insights into the interaction between risk factors and digital behaviours (Goncalves & Stafford, 2024; Luo, 2024).

Cybercrime and digital terrorism represent growing threats, amplified by the accelerated adoption of 5G networks. The increased connectivity and data transmission speeds introduce new vulnerabilities that cybercriminals can exploit, requiring a paradigm shift in cybersecurity strategies to address real-time threats effectively. While existing research highlights various defensive mechanisms, many frameworks struggle to keep pace with rapidly evolving cyber threats. This gap underscores the urgency of continuous adaptation in security protocols and international cooperation to create a robust digital environment resilient to sophisticated cyberattacks (Bhardwaj, 2024).

The literature highlights the multifaceted nature of online scams, impacting individuals, organizations, and society at large. Studies on fraud detection have focused on leveraging artificial intelligence and machine learning to identify suspicious patterns, yet challenges remain in minimizing false positives and adapting to emerging scam techniques. Meanwhile, psychological research has provided valuable insights into victim susceptibility, revealing how cognitive biases and social engineering tactics manipulate individuals into falling for scams. Despite these advancements, there is still a lack of interdisciplinary approaches that integrate technological, psychological, and regulatory perspectives to form a comprehensive defence strategy. Addressing these challenges requires a holistic framework that combines behavioural insights, advanced technologies, and targeted public awareness campaigns to enhance digital resilience.

METHODOLOGY

Recent research has systematically explored various facets of online scams across global contexts. This section highlights the significance of a comprehensive analysis of digital scams and outlines the methodology employed to address the study's research questions. The final part of this section focuses on steps to address identified challenges through potential scholarly interventions. This study adopts the PRISMA (Pre-Recording Systematic Reviews and Meta-Analysis) framework, a widely accepted standard for systematic literature reviews. PRISMA ensures methodological rigor by providing guidelines for evaluating studies, particularly randomized studies, which are integral to systematic analyses.

The review utilized two leading databases, Scopus and Web of Science, recognized for their extensive coverage in educational research. These databases were chosen due to their rigorous indexing criteria, ensuring the inclusion of high-quality, peer-reviewed studies. Additionally, they provide broad international coverage and are widely used in systematic reviews within the field of education and social sciences. While these databases are robust, their scope can be further improved for enhanced comprehensiveness. Other sources, such as Google Scholar or institutional repositories, were considered but excluded due to concerns over inconsistent indexing and potential inclusion of non-peer-reviewed materials. The review process involved key stages, including identification, screening, eligibility assessment, and data abstraction. The systematic review process consisted of three main phases to identify relevant studies. The first phase involved generating keywords and related terms using resources such as dictionaries, thesauruses, encyclopaedias, and prior research. These terms were then used to create search strings for Scopus and Web of Science (see Table 1). This search retrieved 240 papers across both databases in the initial phase.

Table 1: The search strings

Database	Search String	Access Date
Scopus	TITLE-ABS-KEY ("online scam*" OR "internet fraud" OR "digital scam*" OR "cyber fraud" OR "online fraud" OR "phishing" OR "identity theft")	1 Dec 2024
WOS	TS=("online scam*" OR "internet fraud" OR "digital scam*" OR "cyber fraud" OR "online fraud" OR "phishing" OR "identity theft")	7 Dec 2024

Screening, Eligibility, and Extraction

During the initial screening phase, titles and abstracts of the retrieved articles were reviewed. Of the 9655 articles identified, 1525 were deemed relevant based on inclusion and exclusion criteria and progressed to the eligibility stage. At the eligibility stage, the researcher carefully reviewed the titles and abstracts of these 1276 articles to determine their suitability for addressing the study's research objectives. This process resulted in 47 articles being selected for the data extraction phase.

Table 2: Selection criteria for searching

Criterion	Inclusion	Exclusion
Language	English	Non-English
Time line	2020 – 2024	< 2020
Literature type	Journal (Article)	Conference, Book, Review
Publication Stage	Final	In Press
Country	All country	

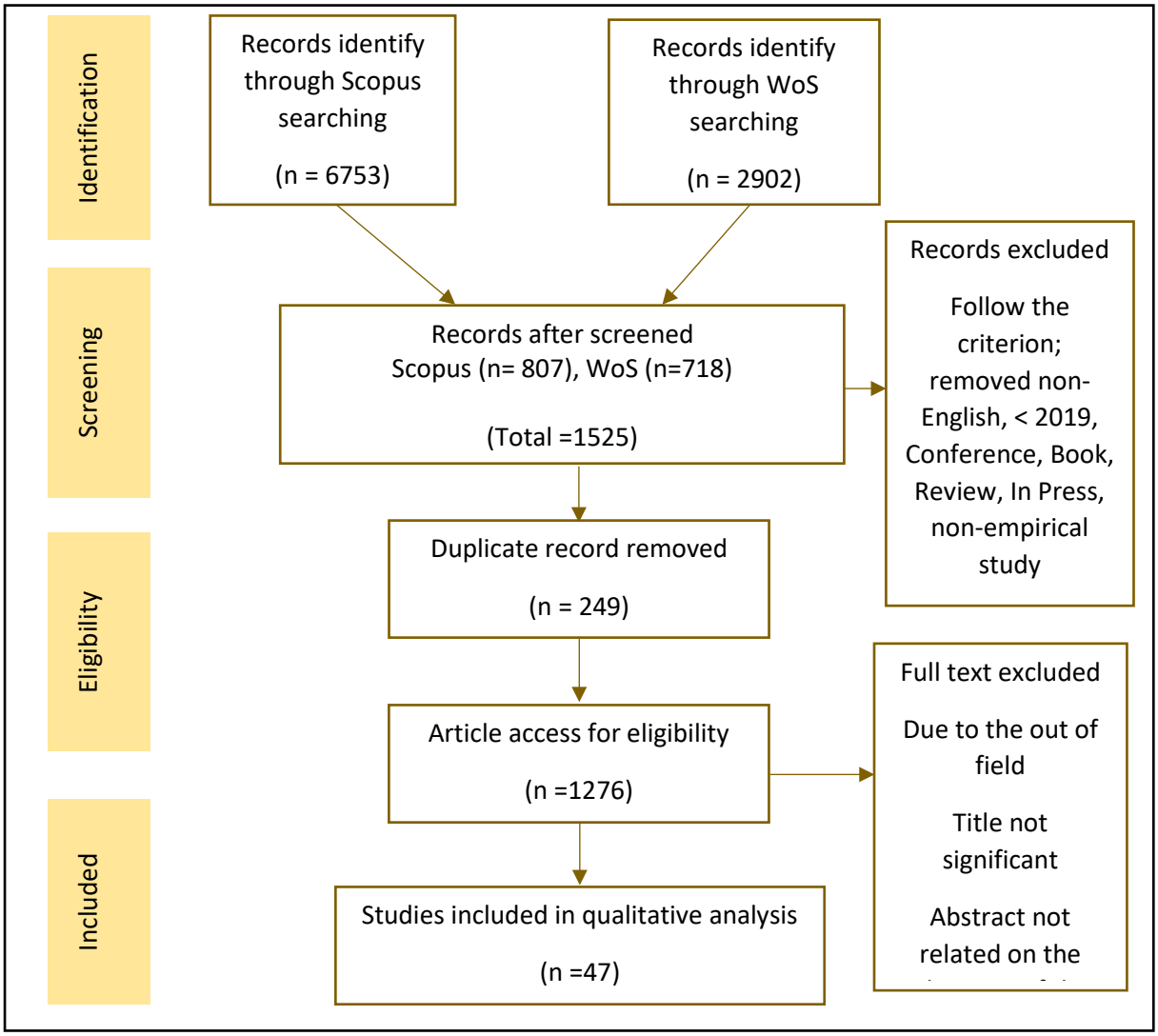

Figure 1: Flow diagram of the proposed searching study (Moher et al., 2009)

Data Abstraction and Analysis

This study employed an integrative analysis as a core assessment strategy to comprehensively examine and synthesize diverse research designs, including quantitative, qualitative, and mixed methods approaches. The primary aim of this thorough analysis was to identify key topics and subtopics within the research domain. The thematic development process began with initial data collection, during which the authors meticulously reviewed a curated selection of 47 publications, extracting relevant assertions and materials closely aligned with the study's thematic focus, as illustrated in Figure 2. Following this, the authors conducted an in-depth evaluation of significant studies on e-learning implementation. This involved a detailed analysis of the methodologies employed across these studies and their corresponding findings. Through collaborative discussions among the authors and co-authors, coherent themes were developed, grounded in the evidence derived from the study's context. Throughout the data analysis process, the team maintained a detailed log to document analyses, perspectives, ambiguities, and other critical insights essential for data interpretation.

RESULTS AND FINDINGS

Online scams are a multifaceted and growing concern, leveraging advancements in technology and exploiting human vulnerabilities. Drawing on insights from over 40 scholarly sources, this detailed thematic analysis explores three key areas: Digital Literacy and Awareness, Technological Innovations in Fraud Detection, and Victimology and Socio-Demographic Dynamics. These findings provide a robust foundation for understanding and addressing the evolving landscape of online scams.

Digital Literacy and Awareness

Digital literacy is a critical tool for reducing susceptibility to online scams. Research by Li et al. (2024) demonstrates that improved digital skills, coupled with financial education, significantly mitigate vulnerability to fraud, especially among high-risk groups such as rural residents, women, and older adults. These protective effects are amplified by enhanced cognitive skills but can be undermined by excessive social trust, emphasizing the need for balanced awareness strategies. However, challenges persist. Isaia et al. (2024) found that while basic financial knowledge reduces the likelihood of victimization, individuals with overconfidence in their financial literacy are paradoxically more susceptible to fraud. This trend became more pronounced during the COVID-19 pandemic, as increased online exposure heightened risks.

In regions like Vietnam, limited awareness campaigns leave many users unprepared to identify scams, though prior victimization enhances vigilance (Pham et al., 2024). Specific demographics, such as younger individuals using dating apps, face unique risks, with victims experiencing financial losses, privacy breaches, and mental health challenges (Chan et al., 2024). Educational interventions tailored to these environments are essential for fostering digital resilience.

Communities also play a crucial role in combating scams. Childs (2024) highlights how online cryptocurrency forums like Reddit serve as collective hubs for sharing knowledge and strategies, empowering users to recognize scams and establish norms for protective behavior. These findings underscore the importance of fostering both individual and community-level awareness initiatives to combat online fraud.

Technological Innovations in Fraud Detection

Technological advancements have revolutionized the field of fraud detection, with machine learning (ML) and artificial intelligence (AI) at the forefront. Chen et al. (2024) developed innovative fraud detection models that analyze spatial and temporal patterns in transactions, achieving superior accuracy compared to traditional methods. Similarly, ensemble methods such as XGBoost and random forests excel in identifying scam profiles on social media platforms, with Bokolo & Liu (2024) reporting over 90% accuracy.

Quantum secure digital payment (QSDP) protocols represent a breakthrough in secure transactions. By eliminating vulnerabilities in measurement devices, Q. Wang et al. (2024) demonstrated how QSDP protocols can prevent identity theft and data breaches. Another innovative approach, SecureFD, combines graph neural networks with multi-party computation to enable collaborative fraud detection while preserving user privacy (Liu et al., 2024). In the realm of real-time detection, Abbassi et al. (2024) propose a fusion of unsupervised learning methods with big data analytics, achieving an accuracy rate of 99%. Similar strides are reported by Nayak et al. (2024), who utilize the XGBoost algorithm for fraud prediction, highlighting the potential of AI-driven solutions in mitigating financial losses. Despite these advancements, challenges such as scalability, privacy concerns, and adapting to emerging threats remain.

Technological solutions extend beyond transaction monitoring to systemic protections. Giridi et al. (2024) introduced convolutional neural networks (CNNs) for counterfeit logo detection, while Alqahtani & Abu-Khadrah (2024) emphasized the role of machine learning in identifying phishing attempts. These advancements demonstrate the potential of technology to mitigate a wide range of online fraud risks.

Victimology and Socio-Demographic Dynamics

Understanding the human dimension of online scams is crucial for effective prevention and recovery. Research in Australia highlights societal biases in victim perception, with "ideal victimhood" influencing support mechanisms and resource allocation. Nataraj-Hansen (2024) found that victims of romance and investment scams often face societal blame, which can hinder recovery efforts. Familial identity theft, where relatives exploit trust for personal gain, adds another layer of complexity, as victims struggle with emotional and financial repercussions in the absence of cohesive support systems (Betz-Hamilton et al., 2024).

Sociodemographic factors significantly influence fraud risks. In Japan, Suzuki (2024) found that frequent online interactions with strangers correlate with higher consumer fraud exposure. Similarly, university students in China report heightened fear and perceived risk of cyber fraud, driven by low self-control and vicarious victimization experiences (Qu et al.,

2024). These findings highlight the need for tailored interventions addressing behavioral and psychological dimensions of fraud prevention.

Mental health outcomes are a critical concern for scam victims. Chan et al. (2024) reported that victims of cyber fraud on dating apps experience poorer mental health compared to non-victims, particularly when financial losses or privacy breaches are involved. Addressing these issues requires a combination of education programs, support services, and public awareness campaigns. Institutional accountability also plays a role in managing fraud. Yekta & Neyland (2024) explored the pressures faced by customer service centers in fraud detection, highlighting the need for robust decision-making frameworks that balance cost, timeliness, and accountability. Improved institutional practices can enhance both prevention efforts and victim support systems.

This detailed analysis underscores the complexity of online scams, highlighting the interplay between digital literacy, technological innovation, and victimology. Enhancing digital education through targeted programs, leveraging advanced technologies for fraud detection, and addressing societal biases in victim support are essential steps toward mitigating online fraud risks. The findings emphasize the importance of interdisciplinary collaboration among educators, technologists, policymakers, and community leaders to create a secure and equitable digital environment. Future research should focus on integrating these approaches to address emerging fraud challenges and support victims more effectively.

DISCUSSION

The present study provides a comprehensive analysis of the dynamics surrounding online scams, with a particular focus on the role of victim awareness, technological innovations in scam detection, and regulatory frameworks. The findings highlight the critical importance of these factors in mitigating the impact of scams, offering significant insights for both academic researchers and practitioners in digital security, law enforcement, and policy development. Additionally, the study underscores the need for stronger legal frameworks and policy interventions, including cross-border cooperation, stricter enforcement of cybercrime laws, and enhanced consumer protection mechanisms to combat the evolving nature of online scams.

Victim Awareness and Resilience emerged as a foundational theme in understanding online fraud prevention. The research underscores the pivotal role that digital literacy and financial education play in equipping individuals with the tools needed to recognize, resist, and report scams. Li et al. (2024) demonstrate that higher cognitive abilities and financial knowledge correlate strongly with enhanced scam detection, while Pham et al. (2024) emphasize the necessity for educational campaigns targeting vulnerable populations, particularly youth engaged in high-risk online activities. This finding underscores the need for a holistic approach to digital education, one that not only teaches individuals how to use technology but also how to navigate the complexities of digital security and online risks. By fostering resilience through education, societies can reduce the long-term impact of scams, which have become pervasive in today's digital ecosystem.

Technological Innovations in scam detection represent a transformative shift in how fraud can be identified and prevented. The application of advanced machine learning algorithms, such as XGBoost and graph neural networks, offers unprecedented accuracy and efficiency in detecting scams. Kumar et al. (2024) and Abbassi et al. (2024) illustrate how these technologies, when applied to large-scale datasets, can identify patterns indicative of fraud, thus reducing the latency in detecting fraudulent activities. Real-time systems, empowered by big data analytics, are particularly noteworthy in their ability to flag suspicious transactions and initiate immediate corrective measures. Backiyalakshmi and Umadevi (2024) further emphasize the value of these real-time interventions, which help mitigate financial losses before they escalate. Additionally, the use of privacy-preserving technologies, such as Secure Multi-Party Computation (SMPC), introduces a layer of confidentiality that facilitates collaborative fraud detection across various entities without compromising individual privacy. These innovations represent the cutting edge of scam detection, aligning technological advancements with the increasing need for privacy and security in the digital age.

The Regulatory and Policy Implications explored in this study reveal the complexities of adapting existing frameworks to address the unique challenges posed by online scams, particularly in decentralized environments. Global regulations, such as the General Data Protection Regulation (GDPR), have provided a necessary foundation for data protection, yet local adaptations are essential for addressing region-specific challenges. Wilson et al. (2024) and Qu and Cheng (2024) highlight the success of localized anti-scam campaigns, such as those in Malaysia, which combine government, financial institutions, and law enforcement efforts to create a unified front against fraud. The rise of decentralized platforms like cryptocurrencies and the metaverse presents a unique challenge to traditional regulatory structures due to their anonymity and cross-border nature. Childs (2024) and Gaurav et al. (2024) call for regulatory innovations to manage these new threats effectively. Thus, the intersection of technological advancements and regulatory frameworks is crucial to creating a multi-layered defense against online scams. This highlights the need for continual policy adaptation to keep pace with emerging digital trends and risks.

IMPLICATIONS

The implications of this comprehensive study on online scams reveal several profound insights that significantly impact both theoretical understanding and practical applications in fraud prevention. The research demonstrates that successful fraud prevention relies heavily on the interplay between human awareness, technological innovation, and regulatory frameworks. Particularly noteworthy is the finding that individuals with stronger cognitive abilities and financial literacy are better equipped to detect and resist scams, suggesting that educational interventions should be a cornerstone of fraud prevention strategies. These findings emphasize that organizations and institutions must move beyond simple technological solutions and adopt a more holistic approach that encompasses both human and technical elements. For instance, financial institutions implementing advanced fraud detection systems should complement these technologies with robust customer education programs, creating a multi-layered defence against scams.

The study also highlights the need to strengthen policies and stricter regulations in tackling online scams. Collaboration between governments, the technology industry, and the financial sector is essential in creating a safer digital ecosystem. Measures such as AI-based transaction monitoring, stricter laws against cyber fraud, and widespread public awareness campaigns on the latest scam tactics must be intensified to reduce cybercrime rates. Furthermore, the study shows that online fraud is not merely a technological issue but also a social problem influenced by demographic, psychological, and cultural factors. For example, individuals who experience social isolation or have limited exposure to digital technology are more vulnerable to becoming victims. Therefore, a more inclusive approach tailored to specific target groups should be implemented to enhance awareness and resilience against cyber threats.

From a technological innovation perspective, increasingly advanced machine learning models enable threat detection systems to operate proactively rather than just reactively. However, the development of AI must also be accompanied by clear ethical controls and accountability to prevent the misuse of such technology by cybercriminals. Additionally, the role of media and digital platforms in spreading awareness about online fraud should not be overlooked. Technology companies must take proactive steps to filter fraudulent content and provide more user-friendly security tools. More interactive and evidence-based awareness campaigns can also help improve public understanding of cyber threats and encourage better digital security practices.

Moreover, the study emphasizes the importance of cross-border collaboration in addressing online fraud, as cybercrime often involves complex international networks. Cooperation between countries in data sharing, legal harmonization, and the development of more comprehensive cybersecurity strategies can help mitigate risks and enhance enforcement effectiveness. However, the implementation of such measures is not without challenges, including regulatory delays, ethical concerns, and disparities in technological capabilities between nations. In conclusion, this study outlines the need for a holistic approach that incorporates technology, education, policy, and international cooperation in efforts to combat online fraud. By strengthening each of these aspects, a safer, more resilient, and confident digital society can be built to face the increasingly complex challenges of the cyber world.

LIMITATIONS

The study faces several significant limitations that merit careful consideration when interpreting its findings and applying its recommendations. A primary constraint lies in the geographical bias of the research data, which predominantly originates from developed nations with advanced technological infrastructure. This limitation raises important questions about the generalizability of findings to developing regions, where technological resources, regulatory frameworks, and cultural contexts may differ substantially. Another crucial limitation stems from the inherently dynamic nature of online scams.

The constant evolution of fraudulent techniques means that specific technological solutions and prevention strategies discussed in the research may have varying degrees of effectiveness over time. This challenge is particularly evident in the context of machine

learning solutions, where the quality and availability of training data can significantly impact detection accuracy. Furthermore, the implementation of privacy-preserving technologies, while essential for protecting sensitive information, introduces additional computational complexities that may affect the real-time response capabilities of fraud detection systems.

RECOMMENDATIONS

Looking toward future directions and recommendations, several key areas deserve attention. Researchers should conduct longitudinal studies to better understand how scamming techniques evolve over time and how prevention strategies can adapt accordingly. There is also a pressing need to investigate the effectiveness of different educational approaches across various demographic groups and cultural contexts. From a policy perspective, developing international cooperation frameworks for addressing cross-border online scams is crucial, particularly in decentralized environments. Technical recommendations include investing in more sophisticated AI models that can detect novel scam patterns while minimizing false positives, and improving the integration of privacy-preserving technologies in fraud detection systems. Educational initiatives should focus on designing and implementing comprehensive digital literacy programs that specifically target vulnerable populations, with materials that can be easily adapted for different cultural contexts and age groups. Furthermore, developing ongoing training programs for financial institutions and law enforcement personnel is essential to keep pace with evolving scam techniques. These future directions emphasize the need for a multi-faceted approach that combines technological innovation, policy development, and educational initiatives to effectively combat online scams in an increasingly complex digital landscape.

CONCLUSION

This study presents a nuanced understanding of the multifaceted nature of online scams, emphasizing the interdependence of victim awareness, technological innovation, and regulatory frameworks in addressing the growing threat of online fraud. The findings underscore the critical need for a coordinated approach that integrates digital literacy, advanced technologies, and dynamic regulatory strategies.

For academics, this paper contributes to the evolving body of knowledge on digital security and online fraud by highlighting the importance of victim awareness as a critical precursor to scam resilience, and by presenting cutting-edge technological solutions for fraud detection. The research also offers valuable insights into how local regulatory frameworks can be adapted to the challenges posed by decentralized digital environments, providing a foundation for further exploration into these complex issues. For practitioners, including policymakers and technology developers, the study emphasizes the need to prioritize education and public awareness as foundational strategies in the fight against scams. Additionally, it advocates for the integration of advanced machine learning models and privacy-preserving technologies into existing fraud detection systems, ensuring that both security and privacy concerns are addressed. The research also calls for a reevaluation of current regulatory structures, with a focus on decentralized platforms like cryptocurrencies, to safeguard against emerging threats.

For general readers, this paper provides a broader perspective on the issue of online scams, illustrating the ways in which technology, education, and law can work together to protect individuals from digital fraud. The findings not only inform the ongoing dialogue in academic and professional circles but also offer practical recommendations that can help individuals and communities better navigate the risks of the digital world. This study sought to address the research questions on how digital literacy, technological advancements, and regulatory measures influence scam prevention. The findings demonstrate that while technological innovations enhance fraud detection, their effectiveness is contingent upon user awareness and robust policy frameworks.

In conclusion, the mitigation of online scams is a complex, multifactorial challenge that requires an integrated approach. By advancing victim awareness, enhancing technological capabilities, and developing adaptive regulatory frameworks, this research paves the way for a more secure digital future. Looking ahead, the rapid evolution of cyber threats underscores the need for continuous innovation in digital security strategies, emphasizing the importance of cross-sector collaboration to stay ahead of emerging fraud tactics. The findings urge stakeholders across sectors to continue working together, leveraging their respective expertise to develop more effective strategies in the ongoing battle against online scams.

BIODATA

Muhammad Adnan Pitchan is a Senior Lecturer at the Centre for Research in Media and Communication, Faculty of Social Sciences and Humanities, Universiti Kebangsaan Malaysia (UKM). His research areas include new media, cyber law, cybersecurity policy, and cyber well-being. Email: adnan86@ukm.edu.my

Ali Salman is an Associate Professor at the Faculty of Language Studies and Human Development, Universiti Malaysia Kelantan (UMK). His areas of expertise are new media and technology. Email: ali.salman@umk.edu.my

Nadhirah Muhamad Arib is a Senior Lecturer at the Faculty of Social Sciences and Humanities, Universiti Teknologi Malaysia (UTM). Her area of expertise is counseling for crime victims. Email: nadhirah.ma@utm.my

REFERENCES

Abbassi, H., Mendili, S. E., & Gahi, Y. (2024). Real-Time Online Banking Fraud Detection Model by Unsupervised Learning Fusion. *HighTech and Innovation Journal*, *5*(1), 185–199. https://doi.org/10.28991/HIJ-2024-05-01-014

Abu-Salih, B., Qudah, D. A., Al-Hassan, M., Ghafari, S. M., Issa, T., Aljarah, I., Beheshti, A., & Alqahtani, S. (2024). An intelligent system for multi-topic social spam detection in microblogging. *Journal of Information Science, 50*(6), 1471–1498. https://doi.org/pcj3

Al-Emran, M., Al-Sharafi, M. A., Foroughi, B., Iranmanesh, M., Alsharida, R. A., Al-Qaysi, N., & Ali, N. (2024). Evaluating the barriers affecting cybersecurity behavior in the Metaverse using PLS-SEM and fuzzy sets (fsQCA). *Computers in Human Behavior*, *159,* 108315. https://doi.org/10.1016/j.chb.2024.108315

Alqahtani, H., & Abu-Khadrah, A. (2024). Enhance the accuracy of malicious uniform resource locator detection based on effective machine learning approach. *Bulletin of Electrical Engineering and Informatics*, *13*(6), 4422–4429. https://doi.org/pcj4

Betz-Hamilton, A. E., Lurtz, M., & Astle, N. (2024). Treating familial identity theft using the collaborative relational model. *Journal of Financial Therapy*, *15*(2), 76–90. https://doi.org/10.4148/1944-9771.1347

Bhardwaj, A. (2024). Cybercrime, digital terrorism, and 5G paradigm: Attack trends of the new millennium. In G. Prabhakar, N. Ayyanar, & S. Rajaram (Eds.), *5G and fiber optics security technologies for smart grid cyber defense* (pp. 1-27). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-2786-9.ch001

Bokolo, B. G., & Liu, Q. (2024). Advanced algorithmic approaches for scam profile detection on Instagram. *Electronics (Switzerland)*, *13*(8), 1571. https://doi.org/pcj5

Boulieris, P., Pavlopoulos, J., Xenos, A., & Vassalos, V. (2024). Fraud detection with natural language processing. *Machine Learning*, *113*(8), 5087–5108. https://doi.org/gsrr4t

Chan, C.-K., Wang, X., & Yang, X. (2024). Prevalence and relationships of dating application usage, cyber-fraud and mental health among emerging adults in Hong Kong. *Psychiatry Research Communications*, *4*(4), 100197. https://doi.org/pcj6

Chen, C.-T., Lee, C., Huang, S.-H., & Peng, W.-C. (2024). Credit card fraud detection via intelligent sampling and self-supervised learning. *ACM Transactions on Intelligent Systems and Technology*, *15*(2), 1–29. https://doi.org/10.1145/3641283

Chhabra Roy, N., & P, S. (2024). Proactive cyber fraud response: A comprehensive framework from detection to mitigation in banks. *Digital Policy, Regulation and Governance*, *26*(6), 678–707. https://doi.org/10.1108/DPRG-02-2024-0029

Childs, A. (2024). 'I guess that's the price of decentralisation…': Understanding scam victimisation experiences in an online cryptocurrency community. *International Review of Victimology*, *30*(3), 539–555. https://doi.org/10.1177/02697580231215840

Gaurav, A., Gupta, B. B., & Chaurasia, P. (2024). Navigating the threat landscape in the metaverse: Emerging risks and security strategies. In B. Gupta (Ed.), *Metaverse security paradigms* (pp. 204-227). IGI Global Scientific Publishing. https://doi.org/pcj7

Giridi, S. V, Sree, M. K., Nandini, M., & Utukuru, S. (2024). Fake logo detection using convolutional neural networks: A deep learning approach. *Proceedings of the 5th International Conference on Smart Electronics and Communication, ICOSEC 2024*, 1492–1495. https://doi.org/10.1109/ICOSEC61587.2024.10722695

Goncalves, V. S., & Stafford, M. C. (2024). The effects of Covid-19 stay-at-home orders on street and cybercrimes in a Brazilian city. *Journal of Criminal Justice*, *95*, 102314. https://doi.org/10.1016/j.jcrimjus.2024.102314

Gürfidan, R. (2024). Suspicious transaction alert and blocking system for cryptocurrency exchanges in metaverse's social media universes: RG-guard. *Neural Computing and Applications, 36*(30), 18825–18840. http://doi.org/10.1007/s00521-024-10122-4

Haq, Q. E. U., Faheem, M. H., & Ahmad, I. (2024). Detecting phishing URLs based on a deep learning approach to prevent cyber-attacks. *Applied Sciences (Switzerland), 14*(22), 10086. https://doi.org/10.3390/app142210086

Harish, S., Lakhanpal, C., & Jafari, A. H. (2024). Leveraging graph-based learning for credit card fraud detection: a comparative study of classical, deep learning and graph-based approaches. *Neural Computing and Applications*, *36*(34), 21873–21883. https://doi.org/10.1007/s00521-024-10397-7

Huke, A., Jadhav, A., Shaikh, M. S., Pathan, S., Mate, G. S., & Prasad, C. (2024). Transact safe: A machine learning shield against online fraud. *15th International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT 2024*, *2*, 3413–3419.

Ibañez, K. R. C. (2024). Scammer strategies and social actions in online Filipino transactions. *Southeastern Philippines Journal of Research and Development*, *29*(1), 43–75. https://doi.org/10.53899/spjrd.v29i1.287

Isaia, E., Oggero, N., & Sandretto, D. (2024). Is financial literacy a protection tool from online fraud in the digital era? *Journal of Behavioral and Experimental Finance, 44*, 100977. http://doi.org/10.1016/j.jbef.2024.100977

Kakulte, A., Dhamija, S., Kelkar, P., & Chaudhury, S. (2024). Internet addiction and cyber fraud. In S. Chaudhury (Ed.), *A guide to clinical psychology: Therapies* (pp. 219–234). Nova Science Publishers, Inc.

Li, P., Li, Q., & Du, S. (2024). Does digital literacy help residents avoid becoming victims of frauds? Empirical evidence based on a survey of residents in six provinces of east China. *International Review of Economics and Finance*, *91*, 364–377. https://doi.org/10.1016/j.iref.2024.01.056

Liu, X., Fan, X., Ma, R., Chen, K., Li, Y., Wang, G., & Xu, W. (2024). Collaborative fraud detection on large scale graph using secure multi-party computation. *CIKM '24: Proceedings of the 33rd ACM International Conference on Information and Knowledge Management*, 1473–1482. https://doi.org/10.1145/3627673.3679863

Luo, Q. (2024). Cybercrime as an industry: Examining the organisational structure of Chinese cybercrime. *Humanities and Social Sciences Communications, 11*(1), 1554. http://doi.org/10.1057/s41599-024-04042-w

Maher, C. A., Corsello, R. M., Engle, T. A., Kuhlman, J. D., & Nedelec, J. L. (2024). Correlates of victim services for fraud and identity theft among victim service providers. *Journal of Criminal Justice*, *95,* 102318. https://doi.org/10.1016/j.jcrimjus.2024.102318

Mahmud, T., Prince, M. A. H., Ali, M. H., Hossain, M. S., & Andersson, K. (2024). *Enhancing cybersecurity: Hybrid deep learning approaches to smishing attack detection*. Systems, *12*(11), 490. http://doi.org/10.3390/systems12110490

Musa, A., & Jacob, S. E. (2024). Legal and regulatory policies for cybersecurity and information assurance in emerging healthcare systems. In Imoize, A. L., Meshram, C., Awotunde, J. B., Farhaoui, Y., & Do, D.-T. (Eds.), *Cybersecurity in Emerging Healthcare Systems* (pp. 533–577). Institution of Engineering and Technology. https://www.scopus.com/record/display.uri?eid=2-s2.0-85209961133&origin=inward&txGid=b89aab32bbf8652e7101999349bb4178

Nataraj-Hansen, S. (2024). "More intelligent, less emotive and more greedy": Hierarchies of blame in online fraud. *International Journal of Law, Crime and Justice*, *76,* 100652. https://doi.org/10.1016/j.ijlcj.2024.100652

Nayak, R., Jain, A., Saxena, M., & Kumar, R. (2024). Cyber security for personal data. In P. Dubey, G. S. Chhabra, B. T. Hung, & U. Ghugar (Eds.), *Developing AI, IoT and Cloud computing-based tools and applications for women's safety* (pp. 123–141). CRC Press. https://doi.org/10.1201/9781003538172-9

Pham, K.-L., Le, T.-D., Tran, A.-D., Tran, M.-T., & Dang-Nguyen, D.-T. (2024). Vietnamese user awareness against scams in cyberspace: An empirical survey. *SCID '24: Proceedings of the 1st Workshop on Security-Centric Strategies for Combating Information Disorder, 6*, 1-6. https://doi.org/10.1145/3660512.3665525

Prabahker, N., Bopche, G. S., & Arock, M. (2024). Generation and deployment of honeytokens in relational databases for cyber deception. *Computers and Security*, *146,* 104032. https://doi.org/10.1016/j.cose.2024.104032

Qu, J., & Cheng, H. (2024). Policing telecommunication and cyber fraud: Perceptions and experiences of law enforcement officers in China. *Crime, Law and Social Change*, *82*, 283–305. https://doi.org/10.1007/s10611-024-10143-z

Qu, J., Lin, K., Wu, Y., & Sun, I. Y. (2024). Fear and perceived risk of cyber fraud victimization among Chinese University students. *Crime, Law and Social Change*, *82*, 543–562. https://doi.org/10.1007/s10611-024-10155-9

Saluja, S. (2024). Identity theft fraud- major loophole for FinTech industry in India. *Journal of Financial Crime*, *31*(1), 146–157. https://doi.org/10.1108/JFC-08-2022-0211

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review, 57*(12). https://doi.org/pcj9

Singh, P., Hasija, T., & Ramkumar, K. R. (2024). Optimizing phishing detection systems with ensemble learning: Insights from a multi-model voting classifier. *Proceedings of the 5th International Conference on Smart Electronics and Communication, ICOSEC 2024*, 1336–1341. https://doi.org/10.1109/ICOSEC61587.2024.10722407

Sudar, K. M., Rohan, M., & Vignesh, K. (2024). Detection of adversarial phishing attack using machine learning techniques. *Sadhana - Academy Proceedings in Engineering Sciences, 49*(3), 232. http://doi.org/10.1007/s12046-024-02582-0

Suzuki, A. (2024). Routine activities and consumer fraud victimization: findings from a social survey in Chiba Prefecture, Japan. *Crime Prevention and Community Safety, 26*(4), 373–384. http://doi.org/10.1057/s41300-024-00219-2

Wang, J., Zhang, L., Xu, L., & Qian, X. (2024). The dynamic emotional experience of online fraud victims during the process of being defrauded: A text-based analysis. *Journal of Criminal Justice*, *94,* 102231. https://doi.org/10.1016/j.jcrimjus.2024.102231

Wang, Q., Liu, J., Li, G., Han, Y., Zhou, Y., & Cheng, L. (2024). A measurement-device-independent quantum secure digital payment. *Physica A: Statistical Mechanics and Its Applications*, *655,* 130178. https://doi.org/10.1016/j.physa.2024.130178

Wilson, S., Hassan, N. A., Khor, K. K., Sinnappan, S., Abu Bakar, A. R., & Tan, S. A. (2024). A holistic qualitative exploration on the perception of scams, scam techniques and effectiveness of anti-scam campaigns in Malaysia. *Journal of Financial Crime*, *31*(5), 1140–1155. https://doi.org/10.1108/JFC-06-2023-0151

Yekta, S., & Neyland, D. (2024). Online fraud detection: 'In the moment' digital accountability in a data-sensitive setting. *Big Data and Society*, *11*(3). https://doi.org/pckb

Yu, X., Zhang, K., Suo, Z., Wang, J., Wang, W., & Zou, B. (2024). An efficient authentication scheme syncretizing physical unclonable function and revocable biometrics in Industrial Internet of Things. *Journal of King Saud University - Computer and Information Sciences*, *36*(8), 102166. https://doi.org/10.1016/j.jksuci.2024.102166