GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(REVIEW ARTICLE)

Check for updates

A review of online scams and financial frauds in the digital age

Amos Kipngetich *

Jaramogi Oginga Odinga University of Science and Technology.

GSC Advanced Research and Reviews, 2025, 22(01), 302-329

Publication history: Received on 10 December 2024; revised on 24 January 2025; accepted on 27 January 2025

Article DOI: https://doi.org/10.30574/gscarr.2025.22.1.0025

Abstract

The rapid proliferation of digital technologies has revolutionized the global economy and transformed how individuals and businesses interact. However, this digital transformation has also given rise to a surge in online scams and financial frauds, posing significant threats to individuals, organizations, and financial institutions. This review paper explores the evolving landscape of online scams and financial frauds in the digital age, focusing on prevalent schemes such as phishing, identity theft, online payment fraud, cryptocurrency-related scams, and social engineering attacks. It examines the methods employed by cybercriminals, the psychological and technological factors that make victims susceptible, and the socioeconomic impacts of these fraudulent activities. The paper also highlights the roles of legislation, cybersecurity advancements, and public awareness in combating digital fraud. By synthesizing current research, case studies, and global trends, this review provides a comprehensive overview of the challenges posed by online scams and financial frauds and outlines effective strategies to mitigate their impact in an increasingly connected world.

Keywords: Fraud; scams; security; technologies; artificial intelligence

1. Introduction

The digital age has transformed the way individuals, businesses, and governments operate, offering unparalleled convenience and connectivity. With the advent of the internet, mobile devices, and cloud computing, activities such as banking, shopping, and communication have become more accessible than ever before [1]-[3]. Figure 1 shoes a typical online shopping system. However, this digital revolution has also provided fertile ground for online scams and financial frauds to flourish. Cybercriminals have adapted to technological advancements, leveraging sophisticated methods to exploit vulnerabilities in digital systems and human behavior [4], [5].

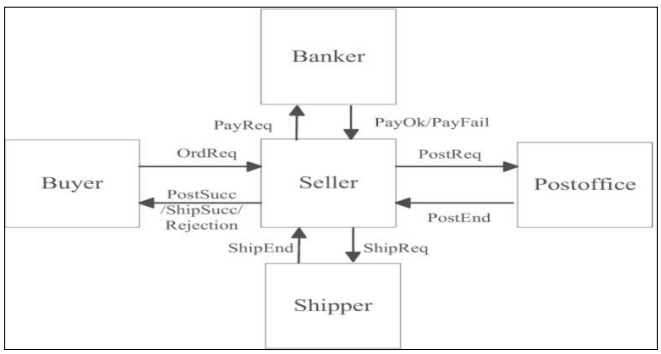

Figure 1 Online shopping system

* Corresponding author: Amos Kipngetich

Online scams and financial frauds encompass a broad spectrum of illicit activities, ranging from phishing emails and identity theft to cryptocurrency scams and ransomware attacks [6], [7]. As shown in Figure 2, these crimes often target individuals, small businesses, and even large corporations, causing significant financial and psychological harm. The scale of these operations is staggering; reports from global cybersecurity agencies highlight billions of dollars lost annually due to digital fraud, with many cases going unreported or unresolved.

One of the defining characteristics of online scams and financial frauds is their dynamic and adaptive nature [8]. Cybercriminals continually refine their techniques, taking advantage of emerging technologies such as artificial intelligence, blockchain, and the Internet of Things (IoT) to create increasingly complex and deceptive schemes [9],[10]. At the same time, the global and borderless nature of the internet complicates law enforcement efforts, making it challenging to track and prosecute offenders effectively.

The growing prevalence of online scams and financial frauds necessitates a comprehensive understanding of their mechanisms, impact, and mitigation strategies [11], [12]. This review paper aims to provide an in-depth analysis of the current landscape of digital fraud, focusing on common types of scams, the psychological and technical factors enabling their success, and the societal implications of these crimes. Furthermore, it examines the role of legislation, technological advancements, and public awareness campaigns in combating these threats, offering insights into effective measures for prevention and response.

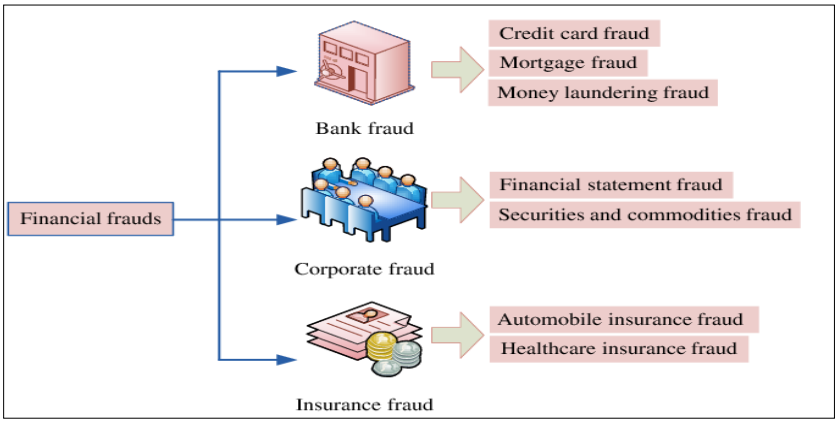

Figure 2 Online scams and financial frauds

As the digital economy continues to expand, addressing the challenges posed by online scams and financial frauds is critical to ensuring trust, security, and resilience in the digital ecosystem. This paper seeks to contribute to this ongoing effort by synthesizing existing research, highlighting gaps in knowledge, and proposing directions for future studies and interventions.

1.1. The rise in online scams and financial frauds

The rise in online scams and financial frauds has been driven by the increasing reliance on digital technologies and the internet in everyday life [13], [14]. As more people and businesses engage in online transactions, cybercriminals have seized the opportunity to exploit weaknesses in digital platforms and human behavior. The exponential growth of e-commerce, online banking, and digital wallets has created a fertile environment for fraudulent activities.

As shown in Figure 3, phishing attacks, one of the most common forms of online scams, have become more sophisticated, often involving personalized messages and cloned websites to deceive users into divulging sensitive information [15]-[19].

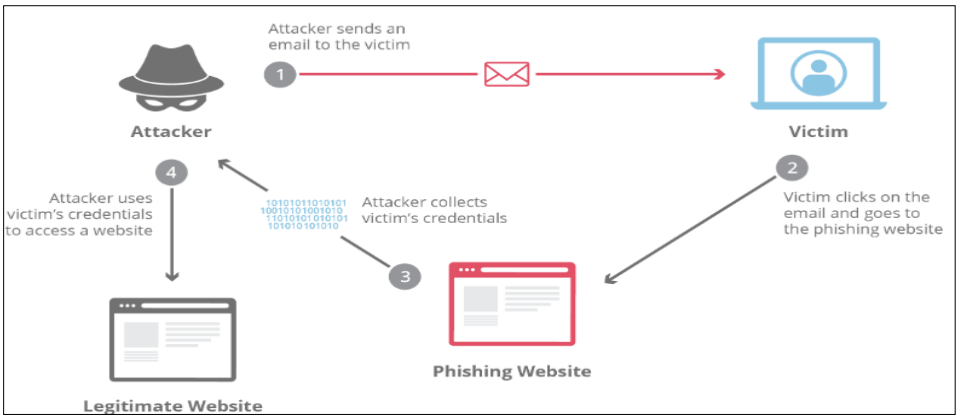

Figure 3 Phishing attack

Similarly, identity theft has surged, with criminals using stolen personal data to commit financial fraud, access accounts, or impersonate victims [20]. These scams exploit trust and a lack of awareness among users, making them particularly effective.

The rise of cryptocurrencies has added another dimension to online financial frauds [21], [22]. While blockchain technology promises secure and transparent transactions, it has also been misused for fraudulent schemes, including initial coin offering (ICO) scams, Ponzi schemes, and crypto wallet hacks [23], [24]. The pseudonymous nature of cryptocurrencies makes it challenging to trace transactions and recover lost funds, further emboldening cybercriminals.

Social engineering attacks, such as business email compromise (BEC) and romance scams, have also seen a sharp increase. Figure 4 gives an illustration of a typical social engineering attack occurs. These schemes rely on psychological manipulation to trick victims into transferring money or sharing confidential information. Advances in artificial intelligence [25] have enabled scammers to create convincing deepfake videos or audio clips, adding another layer of complexity to these attacks.

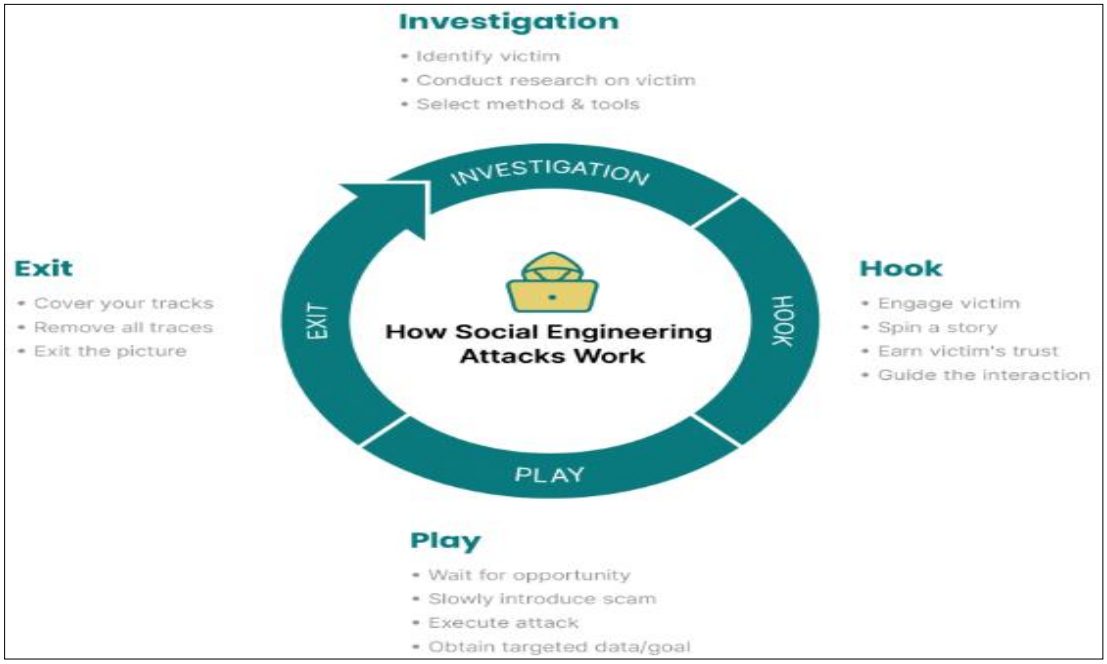

Figure 4 Social engineering

The global COVID-19 pandemic further accelerated the prevalence of online scams and financial frauds [26], [27]. As businesses and individuals transitioned to remote work and digital communication, cybercriminals exploited

vulnerabilities in unsecured networks and increased online activity [28]. Pandemic-related scams, such as fake vaccine sales, stimulus check frauds, and charity scams, became rampant during this period.

The economic and psychological impact of these frauds is significant. Victims often suffer financial losses, damaged credit, and emotional distress [29]. Businesses may face reputational harm, legal liabilities, and operational disruptions. Moreover, the sheer volume and sophistication of these crimes strain law enforcement and cybersecurity resources [30], highlighting the urgent need for proactive measures.

Addressing the rise in online scams and financial frauds requires a multi-faceted approach. Public awareness campaigns can educate individuals about recognizing and avoiding scams, while organizations must invest in robust cybersecurity measures [31], [32]. Governments and regulatory bodies play a crucial role in enacting legislation and fostering international cooperation to combat cross-border fraud. Technological advancements, such as machine learning-based fraud detection systems, can also enhance efforts to identify and prevent fraudulent activities.

1.2. Notable online scams and financial frauds

Numerous high-profile online scams and financial frauds have demonstrated the scale and sophistication of these threats. Below are some of the most notable examples:

Phishing scams: Widely regarded as one of the most prevalent online frauds, phishing scams involve fraudulent emails or messages designed to trick recipients into revealing personal information, such as passwords or credit card details [33]-[35]. High-profile cases have targeted major organizations, including banks and social media platforms, resulting in significant data breaches.

Ponzi and pyramid schemes: Online Ponzi schemes have ensnared millions of victims by promising high returns on investments with little to no risk [36]. One infamous example is the Bernie Madoff scandal [37], which caused billions of dollars in losses, highlighting how digital communication can amplify the reach of such frauds.

Cryptocurrency scams: The rise of cryptocurrencies has given birth to a new class of frauds, including fake initial coin offerings (ICOs), fraudulent trading platforms, and pump-and-dump schemes [38], [39]. For instance, the OneCoin scam defrauded investors of over $4 billion, making it one of the largest crypto frauds in history.

Ransomware attacks: Cybercriminals use ransomware to encrypt victims' data [40], demanding payment—often in cryptocurrency—in exchange for the decryption key. This form of attack is illustrated in Figure 5. Notable incidents, such as the WannaCry and REvil ransomware attacks [41], [42], have targeted hospitals, corporations, and governments, causing widespread disruption.

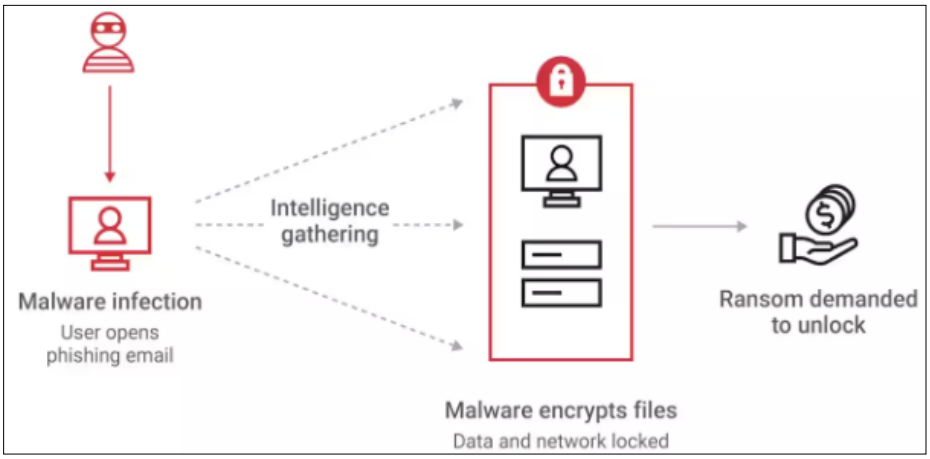

Figure 5 Ransomware attack

Romance scams: Exploiting the emotional vulnerability of victims, romance scams involve building fake relationships online to manipulate individuals into sending money [43], [44]. Reports indicate millions lost annually to such schemes, with victims often targeted on dating platforms and social media.

Business Email Compromise (BEC): BEC scams involve impersonating [45] executives or suppliers to trick businesses into making unauthorized payments. In one of the largest cases, a Lithuanian man scammed two major U.S. companies out of $100 million using fake invoices and emails [46].

Online shopping and auction fraud: Fraudulent e-commerce websites and fake sellers on legitimate platforms deceive customers into paying for goods that are never delivered [47], [48]. These scams surged during the pandemic as more people turned to online shopping.

Tech support scams: Scammers pose as legitimate tech support representatives, convincing victims to grant remote access to their devices or pay for unnecessary services [49], [50]. These scams often target the elderly, exploiting their lack of technical knowledge.

These notable cases underscore the adaptability and ingenuity of cybercriminals. Each example highlights different tactics, motivations, and targets, emphasizing the importance of vigilance and continuous efforts to combat online scams and financial frauds.

1.3. Probable remedies

Addressing online scams and financial frauds requires a multi-layered approach that combines technological innovations, public education, and legal frameworks. Table 1 provides an elaborate description of some effective security solutions.

Table 1 Probable remedies to online scams and financial frauds

Remedy	Description
Advanced authentication mechanisms	Implementation of multi-factor authentication (MFA) adds an additional layer of security by requiring users to verify their identity through multiple means, such as passwords, biometrics, or one-time codes [51]-[55]. Behavioral biometrics, such as keystroke dynamics and mouse movements, can further enhance security by identifying anomalies in user behavior.
AI-powered fraud detection systems	Artificial intelligence and machine learning algorithms [56] can analyze patterns in online transactions to identify suspicious activities in real-time. These systems use anomaly detection to flag deviations from normal user behavior, enabling proactive responses to potential threats [57]-[60].
Encryption and secure communication	End-to-end encryption ensures that sensitive data, such as login credentials and financial information, remains secure during transmission [61]-[66]. Secure protocols like HTTPS and encrypted email services reduce the risk of data interception by attackers.
Cyber hygiene and user awareness	Public awareness campaigns can educate individuals about common scams, warning signs, and best practices for staying safe online [67], [68]. Organizations can provide regular cybersecurity training to employees to reduce human errors that lead to breaches, such as falling for phishing emails.
Regulatory measures and international cooperation	Governments and regulatory bodies must enforce stringent data protection laws and hold organizations accountable for implementing robust cybersecurity measures [69], [70]. Cross-border collaboration among law enforcement agencies can facilitate the tracking and prosecution of cybercriminals operating globally.
Secure payment gateways and anti-fraud tools	Payment gateways with built-in fraud detection mechanisms can identify and block unauthorized transactions. Tools such as tokenization replace sensitive payment data with unique identifiers, reducing the risk of data theft during transactions [71]-[74].
Incident response and recovery plans	Organizations should establish clear incident response protocols to minimize damage during cyberattacks, including isolating affected systems and notifying stakeholders [75], [76]. Regular backups of critical data can ensure rapid recovery in the event of ransomware attacks or other breaches.

Blockchain for transaction transparency	Blockchain technology can enhance security and transparency in financial transactions, making it more difficult for fraudsters to manipulate data [77]-[81]. Smart contracts can automate and secure contractual agreements, reducing the risk of human error and tampering.
Threat intelligence sharing	Collaboration among organizations and cybersecurity firms to share threat intelligence can provide early warnings about emerging scams and vulnerabilities [82]-[86]. Platforms like Information Sharing and Analysis Centers (ISACs) enable real-time exchange of cybersecurity information.
Monitoring and analytics	Continuous monitoring of digital platforms using analytics tools can help identify vulnerabilities and rectify them promptly [87]-[91]. Predictive analytics can identify emerging fraud trends and enable organizations to take preemptive measures.
Public-private partnerships	Collaboration between governments, private sector entities, and non-profits can enhance the reach and effectiveness of anti-fraud initiatives [92], [93]. Joint efforts can focus on creating standardized cybersecurity practices, improving reporting mechanisms, and funding research into new solutions.
Proactive consumer protections	Financial institutions can offer additional safeguards, such as transaction alerts and spending limits, to protect consumers [94]. Insurers can develop fraud protection policies to mitigate financial losses for individuals and businesses.

By integrating these solutions, the digital ecosystem can become more resilient to online scams and financial frauds, protecting individuals and organizations alike from significant harm.

1.4. Challenges with current solutions

The rise of online scams and financial fraud has outpaced the development of comprehensive security solutions, creating a challenging environment for individuals, organizations, and governments. Table 2 gives an extensive analysis of the challenges associated with current security solutions.

Table 2 Challenges with current solutions

Challenge	**Explanation**
Reactive rather than proactive measures	Most security solutions are reactive, addressing fraud after it occurs rather than preventing it. For example: Fraud detection systems often flag suspicious activities post-transaction, leading to delayed responses [95]. Scammers exploit the gap between fraud execution and detection, causing significant damage before countermeasures [96] are enacted.
Fragmented ecosystem	*Diverse stakeholders*: Banks, payment gateways, online platforms, and regulators often operate independently [97], leading to inconsistent security measures. *Incompatibility*: Security solutions implemented by different stakeholders may lack interoperability, creating vulnerabilities at integration points [98]-[100].
Social engineering exploits	Many scams rely on psychological manipulation rather than technical vulnerabilities, making them difficult to counter with traditional technical solutions. Examples include: Phishing attacks [101] that exploit human error. Scams targeting vulnerable populations, such as the elderly, who may lack digital literacy [102].
Sophistication of fraud techniques	Fraudsters are leveraging advanced technologies to outpace security measures: *AI and automation*: Bots are used to create convincing fake websites, automate phishing attempts, and evade detection [103, [104].

	Deepfakes: Synthetic media is used to impersonate individuals in video or voice communications [105], bypassing traditional identity verification systems. *Cryptocurrencies*: Fraudsters use untraceable [106] cryptocurrency transactions to launder money.
Lack of Standardization	*Global variability*: Different countries and regions have varying levels of security standards and regulations [107], creating loopholes for international fraudsters. *Inconsistent compliance*: Financial institutions may implement standards like PCI DSS or GDPR differently, leading to vulnerabilities [108].
Resource constraints	*Financial*: Smaller organizations often lack the budget to implement robust security measures [109]. *Human Resources*: A shortage of cybersecurity professionals limits the ability to monitor, analyze, and respond to threats effectively [110].
User-centric weaknesses	*Password vulnerabilities*: Many users reuse weak passwords across platforms, making them susceptible to credential-stuffing attacks [111]. *Awareness gaps*: A lack of awareness about scams leads to mistakes like clicking on phishing links or sharing personal information [112]. *BYOD policies*: Bring Your Own Device (BYOD) practices in workplaces often compromise security due to inconsistent personal device protections [113], [114].
Insufficient real-time capabilities	Many existing systems struggle to process and act on data in real time: Fraudulent transactions may go undetected until after funds are transferred. Real-time identity verification is often bypassed by sophisticated attackers [115].
Legal and jurisdictional challenges	*Cross-border crimes*: Online scams often involve perpetrators in jurisdictions with weak enforcement mechanisms [116], making prosecution difficult. *Legal ambiguity*: Emerging threats [117], such as fraud in decentralized finance (DeFi), often lack clear regulatory guidelines.
Overwhelming false positives	Fraud detection systems often generate a high number of false positives [118], leading to: Legitimate users being inconvenienced or locked out of their accounts. Increased operational costs due to the need for manual verification.
Lack of trust and transparency	*Opaque processes:* Users are often unaware of the measures in place to protect them [119], leading to mistrust. *Reputational risk*: Institutions that fail to communicate their efforts effectively may suffer reputational damage even if they are secure.
Emerging technologies and IoT vulnerabilities	The rapid proliferation of Internet of Things (IoT) devices introduces new vulnerabilities, as many devices lack robust security features [120]-[122]. Fraudsters exploit these weaknesses to infiltrate networks and execute scams.
Insider threats	Malicious insiders or employees with insufficient training can unintentionally or intentionally compromise security systems [123]-[127]. Insider fraud remains one of the most challenging types of scams to detect and prevent.
Limited collaboration	*Data silos*: Organizations often hesitate to share fraud data due to privacy concerns or competitive reasons [128], reducing collective intelligence. *Delayed reporting*: Victims may delay reporting scams, hindering real-time threat detection and mitigation.
Inadequate user-centric design	*Complex security processes*: Solutions requiring extensive user interaction, such as multi-factor authentication, can frustrate users and lead to non-compliance [129]-[132]. *accessibility issues*: Security measures may not be inclusive of users with disabilities or low technical expertise.

Evolving threat landscape	Fraudsters constantly adapt to new security measures, creating an arms race between scammers and security providers [133], [134]. The dynamic nature of threats makes it challenging for static systems to remain effective [135], [136].

Based on Table 2, it is clear that current security solutions for online scams and financial fraud face several challenges, including the rapidly evolving tactics of cybercriminals who constantly adapt their methods to bypass traditional safeguards. Phishing, social engineering, and advanced malware are becoming more sophisticated, making it harder for existing detection systems to identify threats in real-time. Additionally, the increasing reliance on digital platforms and the growing complexity of financial transactions create larger attack surfaces for fraudsters to exploit. Many security systems struggle with balancing user convenience and robust protection, often leading to friction that discourages users from adopting them. The lack of standardized security protocols across platforms and regions further complicates efforts to address global financial fraud, leaving consumers and businesses vulnerable to loss.

1.5. Research gaps and future directions

The increasing sophistication of online scams and financial frauds has outpaced current security measures, highlighting numerous research gaps and potential areas for improvement. The following are some of the prominent research gaps and future directions for advancing security against online scams and financial frauds.

2. Cross-domain collaboration and information sharing

While financial institutions, law enforcement, and cybersecurity organizations collect data on fraud, there is limited sharing of threat intelligence due to privacy concerns, legal barriers, and competitive reasons. This fragmentation hampers the development of a unified defense against scammers [137]. This limited sharing of threat intelligence due to privacy concerns, legal barriers, and competitive reasons significantly hampers the development of a unified defense against scammers [138]. Organizations are often reluctant to share sensitive data about fraud attempts or cyberattacks, fearing breaches of privacy, violations of data protection laws, or the potential loss of competitive advantage [139]. This fragmentation results in isolated responses to emerging threats, with companies unable to benefit from a broader, collective understanding of evolving scam tactics [140], [141]. As a result, fraudsters can exploit gaps in individual defenses, targeting uncoordinated systems. To combat this, industries must foster greater collaboration through secure, anonymized threat intelligence sharing platforms, supported by clear regulatory frameworks that address privacy and legal concerns while enabling a more cohesive and effective defense against fraud.

Research into frameworks and standards for secure data sharing could help improve cross-domain collaboration. Innovations like blockchain-based data-sharing platforms might ensure secure and transparent collaboration between stakeholders while maintaining privacy and compliance with regulations [142]-[147].

2.1. Real-time fraud detection and prevention

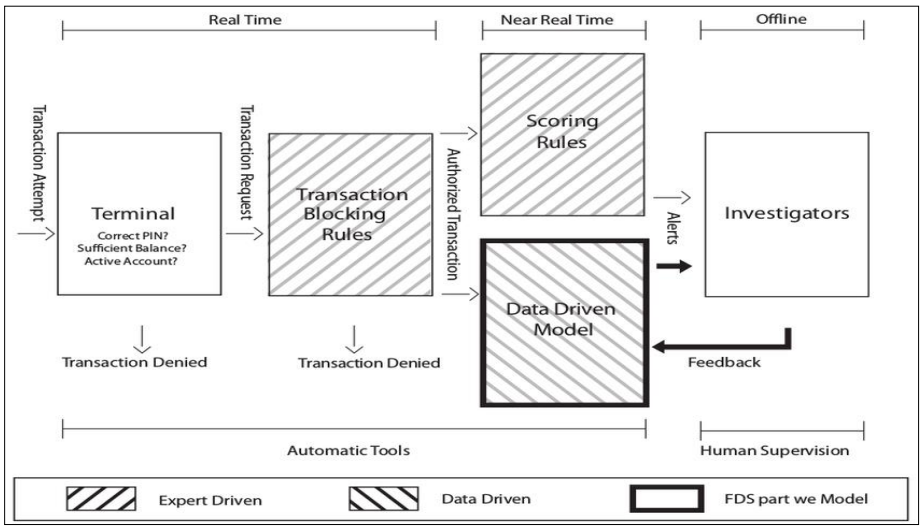

Figure 6 Real-time fraud detection and prevention

Many current fraud detection systems rely on rule-based approaches and post-transaction analysis, which leads to delayed responses [148]. As shown in Figure 6, rule-based systems operate by checking transactions against predefined criteria or patterns, such as large transfers or suspicious behavior, but these rules are often static and fail to adapt quickly to evolving fraud tactics [149], [150]. Post-transaction analysis further compounds the issue, as it typically occurs after a transaction has been completed, allowing fraud to go undetected until it's too late. These delayed responses can result in significant financial losses, reputational damage, and regulatory penalties [151], [152].

To improve effectiveness, fraud detection systems need to adopt more dynamic, AI-driven approaches that use machine learning to identify emerging threats in real-time, allowing for faster and more proactive responses to fraud attempts before they escalate. Fraudsters are exploiting this delay to carry out their attacks effectively.

Research into real-time fraud detection systems powered by AI and machine learning (ML) can help detect fraud before it happens [153]-[157]. Future systems could use behavioral biometrics, real-time data analysis, and predictive modeling to identify anomalies as they occur, improving the accuracy and speed of fraud prevention.

2.2. AI and machine learning for social engineering detection

A significant portion of online scams relies on social engineering tactics such as phishing, vishing (voice phishing), and other manipulative techniques [158]. Phishing typically involves fraudulent emails or websites designed to steal sensitive information, like login credentials or financial details, by masquerading as legitimate entities [159]. Vishing, on the other hand, involves phone calls or voice messages where attackers impersonate trusted figures, such as bank representatives or government officials, to trick victims into revealing personal information or transferring funds [160]. These scams often prey on emotions like fear, urgency, or curiosity, making them difficult to detect and resist. As attackers become more sophisticated in mimicking trusted communication channels, it becomes crucial to invest in user education, multi-layered security measures, and AI-driven threat detection systems (such as the one shown in Figure 7) to combat these pervasive social engineering tactics [161], [162]. Traditional detection methods focus on technical threats but fail to address these psychological attacks effectively.

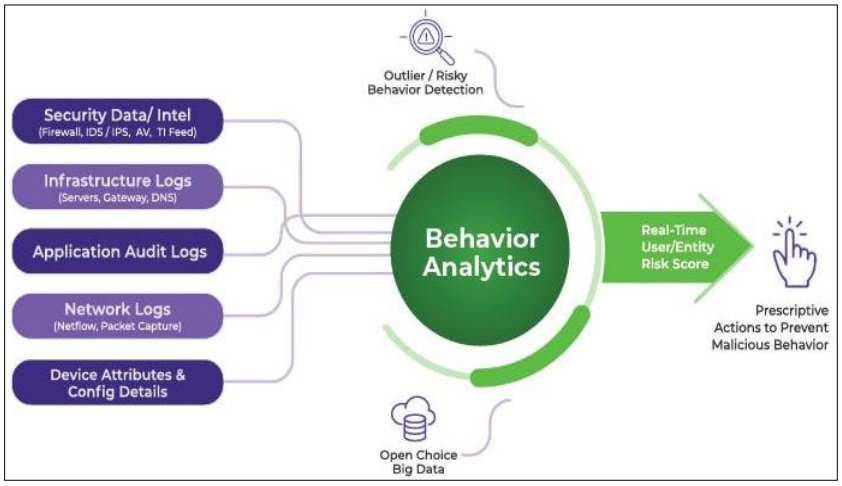

Figure 7 AI-driven threat detection system

More research is needed into developing AI models capable of identifying and preventing social engineering attacks [163]-[167]. For instance, natural language processing (NLP) techniques could be applied to analyze communication patterns in emails, text messages, and phone calls to detect suspicious language indicative of phishing attempts or fraudulent communications.

2.3. Privacy-preserving security

Increasing emphasis on data privacy laws (e.g., GDPR, CCPA) can conflict with security measures, especially in fraud detection, which requires access to large datasets for effective identification of fraud.

Research into privacy-preserving machine learning techniques like federated learning (shown in Figure 8), which allow systems to learn from data without compromising personal privacy, could help balance security and privacy concerns. As explained in [168], federated learning enables models to be trained across decentralized devices or servers without

the need to share sensitive personal data directly. Instead of collecting data in a central location, the system processes data locally on the user's device and only shares aggregated insights, such as model updates, with a central server [169], [170]. This approach helps protect privacy while still allowing systems to learn and improve based on diverse datasets. By incorporating federated learning, organizations can enhance security and privacy for users, especially in sectors like healthcare, finance, and IoT, where sensitive data is involved, all while still benefiting from the power of machine learning to detect fraud or optimize services [171], [172]. These methods would enable the use of sensitive user data for fraud detection without violating privacy regulations. As shown in Figure 8, multiple decentralized devices or systems to collaboratively train a model without sharing sensitive data. Instead of pooling data in a central server, each device or node processes its own data locally, generates model updates, and only shares these updates (not the raw data) with a central server.

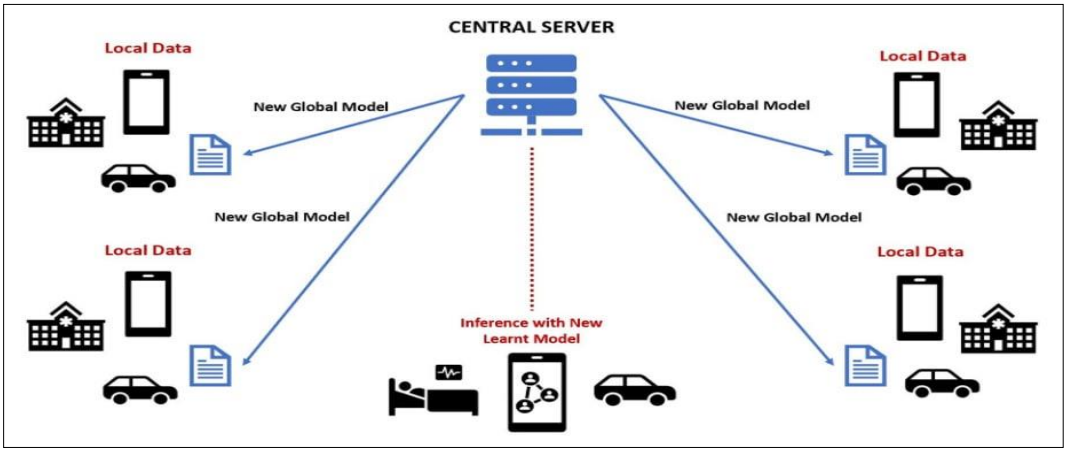

Figure 8 Federated learning

This method enhances privacy and security by ensuring that personal or confidential data never leaves the device, reducing the risk of data breaches. In the context of cybersecurity, federated learning can be used to detect anomalies, identify threats, or improve security models while maintaining user privacy and mitigating potential attack vectors associated with centralized data storage.

2.4. Multi-Factor Authentication (MFA) usability and security

While multi-factor authentication is a widely adopted security measure, it can be cumbersome for users and is still vulnerable to advanced attacks, such as SIM-swapping and phishing [173]. According to [174], MFA (illustrated in Figure 9) is a widely adopted security measure that enhances protection by requiring users to verify their identity through multiple methods, such as passwords, biometrics, or one-time codes. However, despite its effectiveness, MFA can be cumbersome for users, leading to friction and lower adoption rates, particularly when additional steps disrupt the user experience [175]. Furthermore, even MFA is not immune to advanced attacks like SIM-swapping, where fraudsters hijack a victim's phone number to intercept authentication codes, or sophisticated phishing schemes that trick users into divulging MFA credentials [176]-[180]. These vulnerabilities highlight the need for more secure and user-friendly alternatives, such as hardware tokens, push notifications tied to trusted devices, or emerging passwordless technologies that reduce reliance on easily compromised factors while maintaining robust protection.

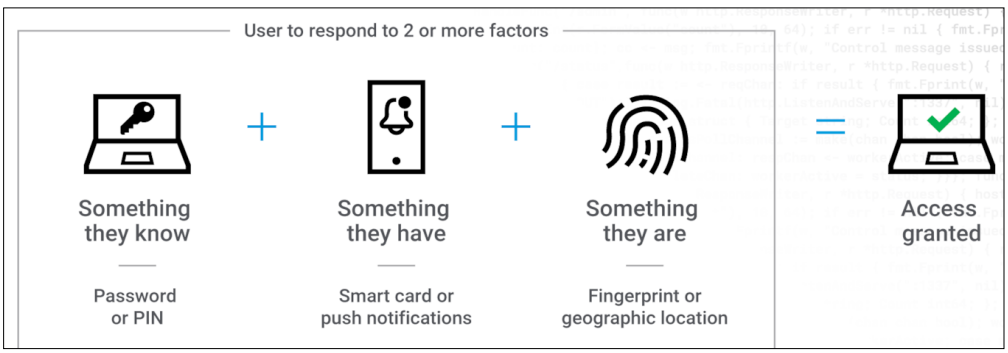

Figure 9 Multi-Factor Authentication

Research could focus on enhancing usability and security of MFA systems. For example, new methods like biometric-based authentication, continuous authentication, and context-aware authentication (where user behavior, location, and device are considered) [181], [182] could make MFA more seamless while improving security.

2.5. Blockchain for fraud detection and prevention

Cryptocurrencies and blockchain-based systems have introduced new avenues for financial fraud due to their decentralized and pseudonymous nature, making it difficult to trace transactions [183]. While blockchain offers transparency by recording all transactions on a public ledger, the pseudonymity it provides enables bad actors to mask their identities, facilitating schemes like money laundering, ransomware payments, and fraudulent initial coin offerings (ICOs). Decentralized exchanges (DEXs) and peer-to-peer transactions further exacerbate these risks by bypassing traditional financial oversight [184]-[186]. Additionally, vulnerabilities in smart contracts and blockchain (depicted in Figure 10) bridges are frequently exploited in hacks and scams [187]. Combating these challenges requires implementing robust regulatory frameworks, developing advanced analytics tools for blockchain forensics, and fostering global collaboration to monitor and address illicit activities in the cryptocurrency ecosystem.

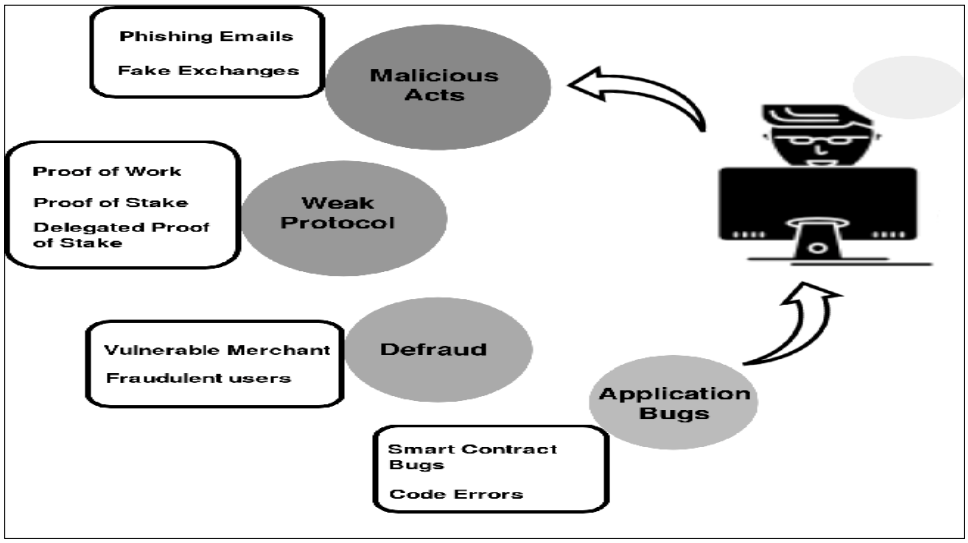

Figure 10 Smart contract attacks

Research into blockchain-based fraud detection systems could help trace illicit activities without compromising privacy [188]-[192]. Smart contracts and public ledgers could be utilized for transparent transactions, ensuring that fraud can be detected early while preventing unauthorized transactions in a decentralized manner.

2.6. Identity and trust management

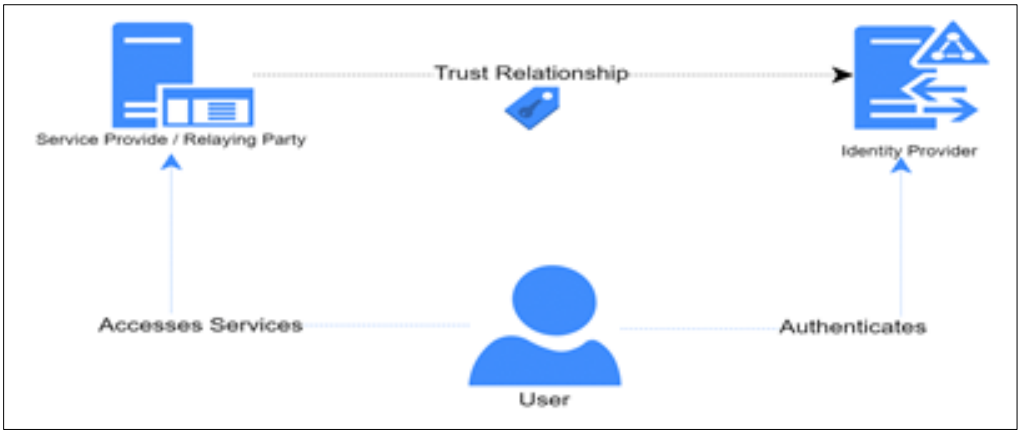

Figure 11 Trust and federated identity management

Identity verification is a critical area vulnerable to fraud, especially in cases involving account takeovers or synthetic identities [193]. Figure 11 gives an illustration of a sample trust and federated identity management. Account takeovers occur when fraudsters gain unauthorized access to legitimate accounts, often using stolen credentials from data breaches or phishing attacks. Synthetic identity fraud, on the other hand, involves creating fake identities by combining real and fabricated information, allowing fraudsters to bypass traditional verification systems [194], [195]. These schemes exploit weaknesses in outdated verification processes, such as reliance on static data like Social Security numbers or knowledge-based authentication, which are easily compromised.

Strengthening identity verification requires advanced methods, including biometrics, AI-driven anomaly detection, and multi-factor authentication, to ensure that only legitimate users can access accounts and services [196], [197]. By prioritizing adaptive and layered approaches, organizations can better protect against identity-related fraud while enhancing user trust. Current solutions often rely on static identity data (e.g., passwords, identification numbers), which are increasingly easy to compromise.

Research could focus on dynamic and adaptive identity management systems that incorporate multiple layers of verification, such as biometric data, behavioral analytics, and contextual information [198]-[202]. Additionally, the development of self-sovereign identities (SSIs) using blockchain could give individuals control over their digital identities, reducing the chances of identity theft.

2.7. Decentralized Finance (DeFi) security

The rise of decentralized finance (DeFi) platforms has created new opportunities for scams, frauds, and exploitation due to their decentralized nature and lack of clear regulations [203]. DeFi platforms operate on blockchain networks, enabling peer-to-peer transactions without intermediaries, which attracts users seeking transparency and autonomy. However, this lack of centralized control also creates opportunities for fraudsters to exploit coding vulnerabilities, manipulate smart contracts, and execute rug pulls—schemes where developers abandon projects after collecting investor funds [204], [205]. Additionally, the pseudonymous nature of blockchain transactions complicates efforts to track and recover stolen assets. The regulatory vacuum surrounding DeFi further exacerbates these risks, leaving investors unprotected and creating inconsistent standards across jurisdictions [206]. Addressing these challenges requires robust security audits, the development of industry best practices, and regulatory frameworks that balance innovation with consumer protection. Figure 12 compares the centralized and decentralized transactions.

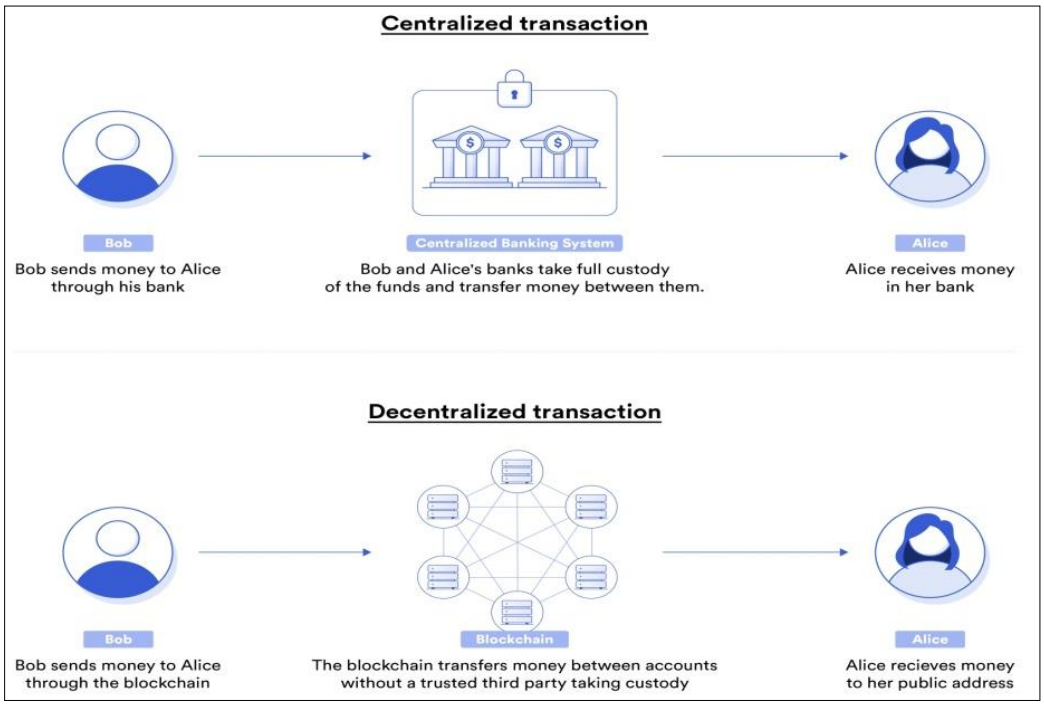

Figure 12 Centralized Vs decentralized transactions

Research into DeFi security protocols [207] could explore ways to safeguard decentralized financial systems against fraud and scams. This could involve the development of secure smart contracts, oracles, and auditing systems that can

verify the integrity of DeFi protocols before funds are transferred or transactions are executed [208]. Secure smart contracts, oracles, and auditing systems are critical to ensuring the integrity of DeFi protocols, particularly as these platforms handle significant user funds and operate without centralized oversight. Smart contracts, which automate transactions based on pre-defined conditions, must be rigorously developed and tested to prevent vulnerabilities that attackers can exploit [209], [210]. Oracles, which connect smart contracts to real-world data, play a pivotal role but require robust mechanisms to avoid data manipulation or tampering. Comprehensive auditing systems, both automated and manual, can verify the accuracy, security, and reliability of DeFi protocols before funds are transferred or transactions are executed [211], [212]. By integrating these components, the ecosystem can reduce risks of exploits, build user trust, and establish a foundation for scalable and secure financial operations within the decentralized landscape.

2.8. Fraud detection in digital ecosystems

As financial fraud increasingly targets digital ecosystems like mobile apps, e-commerce platforms, and social media, there is a lack of holistic fraud detection systems that span across platforms [213]. The absence of holistic fraud detection systems (such as the one depicted in Figure 13) spanning across platforms creates significant vulnerabilities in today's interconnected digital environment. Most fraud detection systems are siloed, tailored to specific industries, organizations, or transaction types, which limits their effectiveness in identifying fraud schemes that exploit multiple touchpoints [214]. For instance, a fraudster might initiate an attack in one domain, such as social media, and carry it through to another, like e-commerce or digital banking, exploiting the lack of cross-platform visibility.

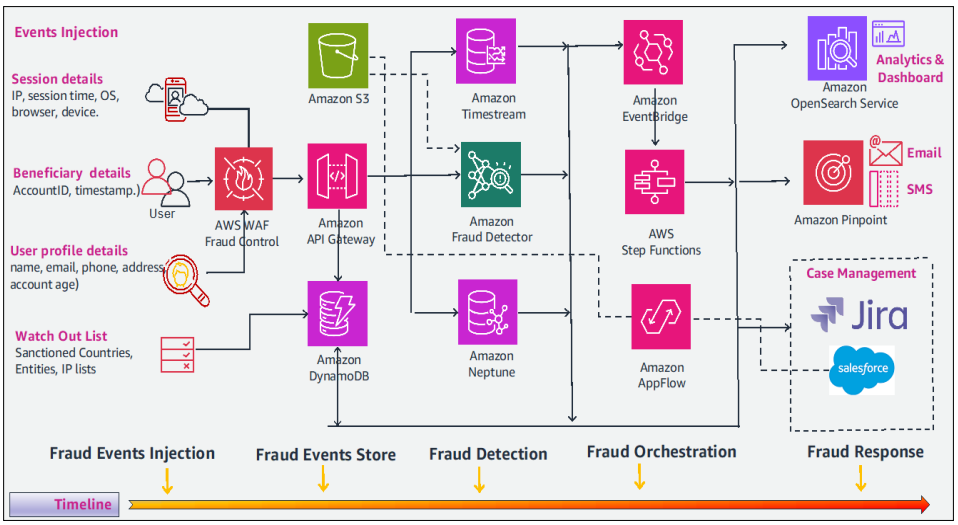

Figure 13 Machine learning-based banking fraud detection

This fragmentation is further exacerbated by inconsistent data-sharing practices and varying regulatory standards, which impede the development of a unified approach to fraud prevention [215]. Without comprehensive systems that aggregate and analyze data across platforms, it becomes difficult to detect complex fraud patterns, such as synthetic identity fraud or coordinated attacks involving multiple parties.

To address this gap, organizations need to adopt integrated fraud detection frameworks that leverage advanced technologies like AI and blockchain for cross-platform data analysis and real-time threat detection. These systems should also facilitate secure collaboration between stakeholders, including financial institutions, technology providers, and regulatory bodies, to establish shared intelligence networks. Building such holistic solutions is essential to closing the gaps that fraudsters exploit and ensuring robust security across the digital ecosystem.

Research into cross-platform fraud detection could help monitor digital activity in real-time across various environments. Data fusion techniques could allow for analyzing multiple data streams from different platforms (e.g., social media, banking apps, and e-commerce sites) [216] to identify fraudulent activities that involve multiple vectors.

2.9. Behavioral and psychological profiling

Current fraud detection methods tend to focus on transactional data and network patterns but often overlook the psychological and behavioral factors that underpin social engineering attacks [217]-[221].

Research into behavioral profiling could identify patterns in users' interaction with systems and highlight deviations that suggest malicious activity. This could include analyzing user typing patterns, mouse movements, or even emotion recognition to flag potential fraud or scams [222], [223].

2.10. Automated investigation and response systems

Manual fraud investigations are time-consuming and resource-intensive [224]. Current solutions often involve reactive responses rather than automated, proactive countermeasures. This reactive approach typically involves incident detection, analysis, and remediation, which can be time-consuming and leave systems vulnerable during the response window [225]. It also allows attackers to exploit the lag between breach detection and containment, leading to greater financial and reputational damage.

Proactive countermeasures, such as those powered by artificial intelligence (Figure 14), machine learning, and predictive analytics, are increasingly necessary to combat sophisticated threats in real time. These technologies can analyze vast datasets, identify patterns, and predict potential vulnerabilities before they are exploited [226]. However, their adoption has been uneven, hindered by high implementation costs, integration challenges, and a lack of skilled personnel. Transitioning to automated, proactive security frameworks requires a cultural and operational shift in organizations, prioritizing continuous monitoring, adaptive threat modeling, and collaborative intelligence-sharing systems. Such an evolution is critical to staying ahead of evolving cyber threats and reducing the reliance on reactive damage control.

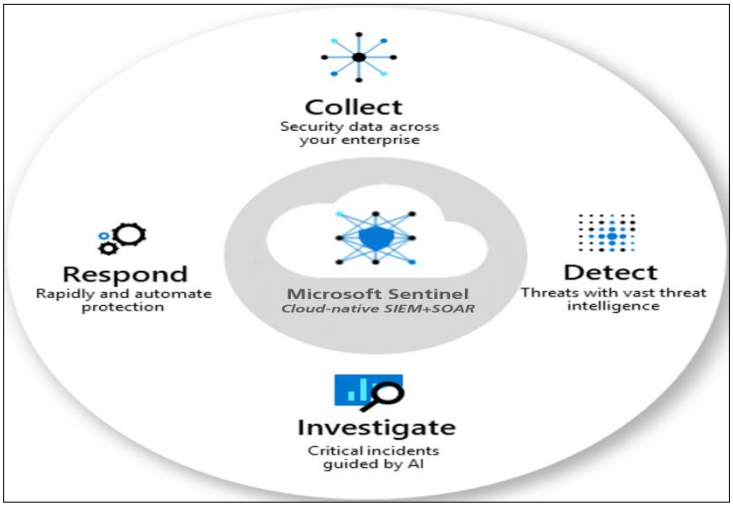

Figure 14 Automated investigation and response system

Future systems could leverage automated investigation tools powered by artificial intelligence [227] and case management systems that can instantly evaluate suspicious activity, trigger responses, and even resolve minor fraud cases without human intervention. This would reduce the burden on security teams and enable faster, more scalable responses.

2.11. Scalability of security measures

The increasing volume of online transactions and user activity makes it difficult for security measures to scale effectively [228]. The surge in online transactions and user activity, fueled by e-commerce, digital banking, and remote work, has outpaced the ability of traditional security measures to scale effectively. As millions of transactions occur daily across diverse platforms, the sheer volume of data presents a challenge for identifying fraudulent activity without overwhelming systems with false positives or delayed responses [229]. Legacy security solutions often struggle to keep up with the speed and complexity of modern online interactions, leaving gaps for sophisticated fraud schemes to exploit.

Moreover, the diversity of digital payment methods, including mobile wallets, cryptocurrencies, and peer-to-peer platforms, introduces additional layers of complexity, each requiring tailored security protocols. Cybercriminals capitalize on these gaps, using automation and advanced technologies like AI to launch large-scale, real-time attacks [230]. To address these challenges, organizations must adopt scalable and intelligent security systems that leverage machine learning to detect anomalies, ensure real-time threat mitigation, and minimize operational bottlenecks [231]. Collaboration across industries and governments is also essential to establish shared threat intelligence and develop

globally consistent standards to protect the growing digital economy. Fraud detection systems may struggle with large-scale data or fail to adapt to a rapidly growing digital landscape.

Research into scalable security architectures could explore the use of distributed systems or cloud-based security solutions that dynamically adjust to the growing volume of digital transactions [232], ensuring effective protection against fraud.

2.12. Impact of Emerging Technologies (AI, IoT, 5G) on fraud

Emerging technologies like IoT, 5G, and AI present new opportunities for fraudsters while challenging existing security systems. The vast increase in connected devices introduces new attack surfaces [233], [234]. The proliferation of IoT devices increases attack surfaces, as many devices lack robust security protocols, enabling unauthorized access, data breaches, and manipulation of connected systems. Meanwhile, 5G enhances connectivity and data transmission speeds, which fraudsters can leverage for swift and large-scale attacks, such as botnets or phishing campaigns, that traditional security systems may struggle to mitigate in real time.

AI poses a dual-edged challenge: while it strengthens fraud detection through predictive analytics and anomaly detection, it also empowers attackers to craft sophisticated scams [235]. Techniques like deepfake technology and AI-driven social engineering make it harder to distinguish between legitimate and fraudulent activities [236]. Furthermore, the convergence of these technologies creates interconnected ecosystems where a breach in one area can cascade into broader, more complex security issues [237]. Addressing these challenges requires developing adaptive security frameworks, investing in next-generation encryption, and fostering collaboration between technology providers, governments, and cybersecurity experts to preemptively counter these evolving threats.

Research could focus on developing robust security frameworks tailored to emerging technologies, such as creating secure IoT networks, mitigating risks in 5G-enabled environments, and ensuring AI-powered systems are resistant to adversarial attacks and fraud [238]-[242].

2.13. Regulatory and legal research

As online scams and financial fraud evolve, there is a gap in consistent, international regulations that can provide clear guidance on how to address and prosecute new types of fraud.

Future research should focus on developing global regulatory frameworks that can keep pace with the rapidly evolving fraud landscape [243], [244]. These frameworks should emphasize cross-border cooperation, real-time data sharing, and the adoption of innovative technologies like artificial intelligence and blockchain to detect and prevent fraudulent activities. Regulatory bodies need to harmonize standards to reduce jurisdictional gaps that fraudsters exploit, while fostering collaboration between public and private sectors to enhance vigilance and response capabilities [245], [246]. Additionally, frameworks must be flexible, incorporating adaptive policies that can anticipate emerging threats, such as cyber-enabled crimes and deepfake-based scams, ensuring robust protection for individuals and businesses worldwide [247], [248]. This could include proposing new standards for cross-border fraud detection and prosecution, ensuring that law enforcement can effectively track and apprehend fraudsters operating across jurisdictions.

It is evident that the rapidly evolving nature of online scams and financial frauds demands continuous innovation in both technical and non-technical solutions. Closing the research gaps outlined above will not only lead to better fraud detection and prevention systems but will also improve the overall security and trust in online financial systems. With ongoing collaboration, technological advancements, and regulatory updates, the fight against online fraud can become more effective in the years to come.

3. Conclusion

The rapid advancement of digital technologies has transformed the landscape of online scams and financial frauds, presenting unprecedented challenges for individuals, businesses, and governments alike. The complexity and sophistication of these fraudulent activities continue to evolve, leveraging cutting-edge technologies such as artificial intelligence, blockchain, and social engineering tactics to deceive victims and bypass traditional security measures. As this digital transformation accelerates, so too must the development of innovative and adaptive security solutions to combat these emerging threats. This review highlights the various types of online scams and financial frauds that dominate the digital age, ranging from phishing and identity theft to more complex crimes such as account takeovers, crypto fraud, and scams in decentralized finance (DeFi). The ongoing struggle between fraudsters and security providers reveals significant gaps in the current state of online protection, particularly in the areas of real-time

detection, cross-platform collaboration, and user education. Moreover, the proliferation of IoT devices and the rise of social engineering tactics underscore the need for a comprehensive and integrated approach to online security. Future research must focus on developing proactive fraud prevention mechanisms that can detect and mitigate fraud before it occurs, with an emphasis on real-time analytics, machine learning, and privacy-preserving technologies. Moreover, a collaborative, global effort involving stakeholders from the public and private sectors is crucial for creating effective security frameworks and standards that can adapt to the ever-changing nature of online scams. Ultimately, as the digital world continues to expand, it is essential that cybersecurity measures evolve in tandem with these changes. By addressing the current challenges and research gaps, we can strengthen defenses against online scams and financial frauds, ensuring a safer and more trustworthy digital environment for all users. Collaboration, innovation, and a forward-thinking approach will be key to overcoming these persistent threats and protecting the integrity of digital financial systems in the years to come.

References

[1] Gill SS, Wu H, Patros P, Ottaviani C, Arora P, Pujol VC, Haunschild D, Parlikad AK, Cetinkaya O, Lutfiyya H, Stankovski V. Modern computing: Vision and challenges. Telematics and Informatics Reports. 2024 Jan 8:100116.

[2] Obi OC, Dawodu SO, Daraojimba AI, Onwusinkwue S, Akagha OV, Ahmad IA. Review of evolving cloud computing paradigms: security, efficiency, and innovations. Computer Science & IT Research Journal. 2024 Feb 2;5(2):270-92.

[3] Mishra RK, Agarwal R. Impact of digital evolution on various facets of computer science and information technology. Digital Evolution: Advances in Computer Science and Information Technology. 2024 Jun;17.

[4] AllahRakha N. Transformation of Crimes (Cybercrimes) in Digital Age. International Journal of Law and Policy. 2024 Feb 25;2(2).

[5] Radhi BM, Hussain MA, Abduljabbar ZA, Nyangaresi VO, Aldarwish AJ. A Review on IoTs Applications and Security Threats via Data Transfer over Networks. InComputer Science On-line Conference 2024 Apr 25 (pp. 562-579). Cham: Springer Nature Switzerland.

[6] Nicholls J, Kuppa A, Le-Khac NA. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. Ieee Access. 2021 Dec 8;9:163965-86.

[7] Agarwal U, Rishiwal V, Tanwar S, Yadav M. Blockchain and crypto forensics: Investigating crypto frauds. International Journal of Network Management. 2024 Mar;34(2):e2255.

[8] Bello HO, Ige AB, Ameyaw MN. Adaptive machine learning models: concepts for real-time financial fraud prevention in dynamic environments. World Journal of Advanced Engineering Technology and Sciences. 2024 Jul;12(02):021-34.

[9] Sarkar G, Shukla SK. Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology. 2023 Oct 11:100034.

[10] Nyangaresi VO, Alsolami E, Ahmad M. Trust-enabled Energy Efficient Protocol for Secure Remote Sensing in Supply Chain Management. IEEE Access. 2024 Aug 12.

[11] Bhat AH, Kolhe D. Crime and Fraud at the Community level: Social Networking Understanding into Economic crimes and Psychology Motivations. Journal of Social Sciences and Economics. 2024 Nov 21;3(2):127-46.

[12] Karpoff JM. The future of financial fraud. Journal of Corporate Finance. 2021 Feb 1;66:101694.

[13] Bansal U, Bharatwal S, Bagiyam DS, Kismawadi ER. Fraud detection in the era of AI: Harnessing technology for a safer digital economy. InAI-Driven Decentralized Finance and the Future of Finance 2024 (pp. 139-160). IGI Global.

[14] Abubakari Y. The espouse of women in the online romance fraud world: Role of sociocultural experiences and digital technologies. Deviant Behavior. 2024 May 3;45(5):708-35.

[15] Jawad M, Yassin AA, AL-Asadi HA, Abduljabbar ZA, Nyangaresi VO. Towards Building Multi-factor Authentication Scheme for Users in the Healthcare Sector Based on Blockchain Technology. InComputer Science On-line Conference 2024 Apr 25 (pp. 694-713). Cham: Springer Nature Switzerland.

[16] Schmitt M, Flechais I. Digital Deception: Generative artificial intelligence in social engineering and phishing. Artificial Intelligence Review. 2024 Dec;57(12):1-23.

[17] Ayeni RK, Adebiyi AA, Okesola JO, Igbekele E. Phishing Attacks and Detection Techniques: A Systematic Review. In2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG) 2024 Apr 2 (pp. 1-17). IEEE.

[18] Pinjarkar L, Hete PR, Mattada M, Nejakar S, Agrawal P, Kaur G. An Examination of Prevalent Online Scams: Phishing Attacks, Banking Frauds, and E-Commerce Deceptions. In2024 Second International Conference on Advances in Information Technology (ICAIT) 2024 Jul 24 (Vol. 1, pp. 1-6). IEEE.

[19] Goenka R, Chawla M, Tiwari N. A comprehensive survey of phishing: Mediums, intended targets, attack and defence techniques and a novel taxonomy. International Journal of Information Security. 2024 Apr;23(2):819-48.

[20] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[21] Trozze A, Kamps J, Akartuna EA, Hetzel FJ, Kleinberg B, Davies T, Johnson SD. Cryptocurrencies and future financial crime. Crime Science. 2022 Dec;11:1-35.

[22] Sanz-Bas D, del Rosal C, Náñez Alonso SL, Echarte Fernández MÁ. Cryptocurrencies and fraudulent transactions: Risks, practices, and legislation for their prevention in Europe and Spain. Laws. 2021 Jul 9;10(3):57.

[23] Boreiko D. Initial Coin Offerings pitfalls: Scams, flops, and security breaches. InUnderstanding Initial Coin Offerings 2024 Mar 8 (pp. 176-200). Edward Elgar Publishing.

[24] Hornuf L, Kück T, Schwienbacher A. Initial coin offerings, information disclosure, and fraud. Small Business Economics. 2022 Apr;58(4):1741-59.

[25] Ali AH, Jasim HM, Abduljabbar ZA, Nyangaresi VO, Umran SM, Ma J, Honi DG. Provably Efficient and Fast Technique for Determining the Size of a Brain Tumor in T1 MRI Images. In2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2024 Feb 19 (pp. 608-613). IEEE.

[26] Ma KW, McKinnon T. COVID-19 and cyber fraud: Emerging threats during the pandemic. Journal of Financial Crime. 2021 May 12;29(2):433-46.

[27] Zhang Y, Wu Q, Zhang T, Yang L. Vulnerability and fraud: evidence from the COVID-19 pandemic. Humanities and Social Sciences Communications. 2022 Nov 28;9(1):1-2.

[28] Bispham M, Creese S, Dutton WH, Esteve-Gonzalez P, Goldsmith M. Cybersecurity in working from home: An exploratory study. InTPRC49: The 49th Research Conference on Communication, Information and Internet Policy 2021 Aug 1.

[29] Shang Y, Wu Z, Du X, Jiang Y, Ma B, Chi M. The psychology of the internet fraud victimization of older adults: A systematic review. Frontiers in psychology. 2022 Sep 5;13:912242.

[30] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[31] Shillair R, Esteve-González P, Dutton WH, Creese S, Nagyfejeo E, von Solms B. Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security. 2022 Aug 1;119:102756.

[32] Bada M, Nurse JR. Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security. 2019 Jun 19;27(3):393-410.

[33] Alkhalil Z, Hewage C, Nawaf L, Khan I. Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science. 2021 Mar 9;3:563060.

[34] Ali MM, Mohd Zaharon NF. Phishing—A cyber fraud: The types, implications and governance. International Journal of Educational Reform. 2024 Jan;33(1):101-21.

[35] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Aldarwish AJ, Neamah HA. Smart Grid and Renewable Energy Security Challenges: A Review. InComputer Science On-line Conference 2024 Apr 25 (pp. 805-825). Cham: Springer Nature Switzerland.

[36] Peng Z, Boyle PP. Ponzi Schemes: A Review. Available at SSRN 5019934. 2024 Sep 27.

[37] Boddy CR. Insights into the bernie madoff financial market scandal which identify new opportunities for business market researchers. International Journal of Market Research. 2024 Jan;66(1):149-67.

[38] Tiwari M, Gepp A, Kumar K. The future of raising finance-a new opportunity to commit fraud: a review of initial coin offering (ICOs) scams. Crime, Law and Social Change. 2020 May;73:417-41.

[39] De Andrés P, Arroyo D, Correia R, Rezola A. Challenges of the market for initial coin offerings. International review of financial analysis. 2022 Jan 1;79:101966.

[40] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[41] Deochakke A, Tyagi AK. Analysis of Ransomware Security on Cloud Storage Systems. InInternational Conference on Advancements in Interdisciplinary Research 2022 May 6 (pp. 47-59). Cham: Springer Nature Switzerland.

[42] Zakaria WZ, Abdollah MF, Abdollah O, SMM SW. Ransomware Behavior on Windows Endpoint: An Analysis. Journal of Social Science and Humanities. 2023;6(5):25-31.

[43] Wiederhold BK. Digital desires, real losses: the complex world of online romance fraud. Cyberpsychology, Behavior, and Social Networking. 2024 May 1;27(5):300-2.

[44] Amirkhani S, Alizadeh F, Randall D, Stevens G. Beyond Dollars: Unveiling the Deeper Layers of Online Romance Scams Introducing "Body Scam". InExtended Abstracts of the CHI Conference on Human Factors in Computing Systems 2024 May 11 (pp. 1-6).

[45] Abdali HK, Hussain MA, Abduljabbar ZA, Nyangaresi VO, Aldarwish AJ. Comprehensive Challenges to E-government in Iraq. InComputer Science On-line Conference 2024 Apr 25 (pp. 639-657). Cham: Springer Nature Switzerland.

[46] Fayyad-Kazan H, Hejase HJ, Darwish CD, Hejase AJ. A Pilot Study to Assess the Success Rate of Email Scams by Phishing: Case in Lebanon. Contemporary Studies in Applied Sciences. 2024;1(1):1-21.

[47] Gowda C. Understanding Fraud Risk in E-Commerce with Special Emphasis on Credit Card Fraud and Triangulation Fraud. Issue 6 Indian JL & Legal Rsch.. 2022;4:1.

[48] Paul H, Nikolaev A. Fake review detection on online E-commerce platforms: a systematic literature review. Data Mining and Knowledge Discovery. 2021 Sep;35(5):1830-81.

[49] Dupuis D, Smith D, Gleason K. Old frauds with a new sauce: digital assets and space transition. Journal of Financial Crime. 2023 Jan 2;30(1):205-20.

[50] Falade PV. Analysis of 419 Scams: The Trends and New Variants in Emerging Types. Int. J. Sci. Res. in Computer Science and Engineering Vol. 2023 Oct;11(5).

[51] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[52] Ometov A, Bezzateev S, Mäkitalo N, Andreev S, Mikkonen T, Koucheryavy Y. Multi-factor authentication: A survey. Cryptography. 2018 Jan 5;2(1):1.

[53] Suleski T, Ahmed M, Yang W, Wang E. A review of multi-factor authentication in the Internet of Healthcare Things. Digital health. 2023 May;9:20552076231177144.

[54] Mostafa AM, Ezz M, Elbashir MK, Alruily M, Hamouda E, Alsarhani M, Said W. Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication. Applied Sciences. 2023 Sep 30;13(19):10871.

[55] Dahiya P, Kant U. Multi-Factor Authentication Methods in Intelligent Systems. InIntelligent Manufacturing and Industry 4.0 2025 (pp. 142-160). CRC Press.

[56] Xu X, Patibandla RL, Arora A, Al-Razgan M, Awwad EM, Nyangaresi VO. An Adaptive Hybrid (1D-2D) Convolution-based ShuffleNetV2 Mechanism for Irrigation Levels Prediction in Agricultural Fields with Smart IoTs. IEEE Access. 2024 Apr 3.

[57] Marripudugala M. AI-Powered Fraud Detection in the Financial Services Sector: A Machine Learning Approach. In2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) 2024 Oct 23 (pp. 795-799). IEEE.

[58] Bello OA, Olufemi K. Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. Computer Science & IT Research Journal. 2024;5(6):1505-20.

[59] Trivedi C, Kumar S. The Next Frontier: AI-Powered Strategies Shaping the Landscape of Fraud Detection Startups. In2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) 2024 May 25 (pp. 350-356). IEEE.

[60] Adhikari P, Hamal P, Jnr FB. Artificial Intelligence in fraud detection: Revolutionizing financial security. International Journal of Science and Research Archive. 2024;13(01):1457-72.

[61] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[62] Hazra R, Chatterjee P, Singh Y, Podder G, Das T. Data Encryption and Secure Communication Protocols. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 546-570). IGI Global.

[63] Olaiya OP, Adesoga TO, Adebayo AA, Sotomi FM, Adigun OA, Ezeliora PM. Encryption techniques for financial data security in fintech applications. International Journal of Science and Research Archive. 2024;12(1):2942-9.

[64] Kumar KS, Reddy PJ, GnanaTeja P, Babu CS, Ande PK, Sai NR. Encryption in the Cloud: Analysing Deep into the Layers of Security. In2024 International Conference on Expert Clouds and Applications (ICOECA) 2024 Apr 18 (pp. 81-86). IEEE.

[65] Islam MS, Zamani M, Hamlen KW, Khan L, Kantarcioglu M. Ensuring End-to-End IoT Data Security and Privacy Through Cloud-Enhanced Confidential Computing. InIFIP Annual Conference on Data and Applications Security and Privacy 2024 Jul 13 (pp. 71-91). Cham: Springer Nature Switzerland.

[66] Ahmad AY, Verma N, Sarhan N, Awwad EM, Arora A, Nyangaresi VO. An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model. IEEE Access. 2024 Mar 18.

[67] Darem AA, Alkhaldi TM, Alahmari M, Alhashmi AA, Alashjaee AM, Alanazi SM, Ebad SA. Beyond Technical Barriers: A Multidimensional Conceptual Framework for Understanding and Countering Cyber Scam Susceptibility. International Journal of Human–Computer Interaction. 2024 Oct 22:1-26.

[68] Van Steen T, Norris E, Atha K, Joinson A. What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?. Journal of Cybersecurity. 2020;6(1):tyaa019.

[69] Nguyen MT, Tran MQ. Balancing security and privacy in the digital age: an in-depth analysis of legal and regulatory frameworks impacting cybersecurity practices. International Journal of Intelligent Automation and Computing. 2023 Sep 12;6(5):1-2.

[70] Michael K, Kobran S, Abbas R, Hamdoun S. Privacy, data rights and cybersecurity: Technology for good in the achievement of sustainable development goals. In2019 IEEE International Symposium on Technology and Society (ISTAS) 2019 Nov 15 (pp. 1-13). IEEE.

[71] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[72] Kotha R. Security Threats in Today's Payment Processing and Advanced Technological Solution. North American Journal of Engineering Research. 2023 May 13;4(2).

[73] Banerjee S, Shukla S, Menon KS. The Tokenisation Framework and Its Privacy Discontents: Issues and Solutions. NUJS L. Rev.. 2022;15:208.

[74] Mangi FA. Fortifying Fintech Security: Advanced Strategies for Protecting Financial Data and Assets. Emerging Science Research. 2025 Jan 6:01-11.

[75] Edwards DJ. Incident Response Management. InCritical Security Controls for Effective Cyber Defense: A Comprehensive Guide to CIS 18 Controls 2024 Sep 29 (pp. 497-526). Berkeley, CA: Apress.

[76] Alshuraify NA, Yassin AA, Abduljabbar ZA, Nyangaresi VO, Aldarwish AJ. Blockchain-Based CCTV Surveillance Cameras for Oil and Gas Industry Pipelines. InComputer Science On-line Conference 2024 Apr 25 (pp. 730-744). Cham: Springer Nature Switzerland.

[77] Martinez D, Magdalena L, Savitri AN. Ai and blockchain integration: Enhancing security and transparency in financial transactions. International Transactions on Artificial Intelligence. 2024 Nov 4;3(1):11-20.

[78] Farayola OA. Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. Finance & Accounting Research Journal. 2024 Apr 7;6(4):501-14.

[79] Akash TR, Islam MS, Sourav MS. Enhancing business security through fraud detection in financial transactions. Global Journal of Engineering and Technology Advances. 2024;21(02):079-87.

[80] Rabbani H, Shahid MF, Khanzada TJ, Siddiqui S, Jamjoom MM, Ashari RB, Ullah Z, Mukati MU, Nooruddin M. Enhancing security in financial transactions: a novel blockchain-based federated learning framework for detecting counterfeit data in fintech. PeerJ Computer Science. 2024 Sep 23;10:e2280.

[81] Alshuraify NA, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Monitoring and surveillance systems based IoTs with Blockchain: Literature Review. Basrah Researches Sciences. 2024 Dec 31;50(2):42-63.

[82] Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security. 2018 Jan 1;72:212-33.

[83] Kayode-Ajala O. Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. Applied Research in Artificial Intelligence and Cloud Computing. 2023 Aug 4;6(8):1-21.

[84] Cascavilla G, Tamburri DA, Van Den Heuvel WJ. Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers & Security. 2021 Jun 1;105:102258.

[85] Tahmasebi M. Beyond defense: Proactive approaches to disaster recovery and threat intelligence in modern enterprises. Journal of Information Security. 2024 Feb 27;15(2):106-33.

[86] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[87] Makhdoom I, Abolhasan M, Lipman J, Liu RP, Ni W. Anatomy of threats to the internet of things. IEEE communications surveys & tutorials. 2018 Oct 11;21(2):1636-75.

[88] Jimmy FN. Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023. 2024 Apr 12;2(1):129-71.

[89] Ofoegbu KD, Osundare OS, Ike CS, Fakeyede OG, Ige AB. Proactive cyber threat mitigation: Integrating data-driven insights with user-centric security protocols. Computer Science & IT Research Journal. 2024;5(8).

[90] Priyadharshini SL, Al Mamun MA, Khandakar S, Prince NN, Shnain AH, Abdelghafour ZA, Brahim SM. Unlocking Cybersecurity Value through Advance Technology and Analytics from Data to Insight. Nanotechnology Perceptions. 2024:202-10.

[91] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[92] Agustini AT, Mustakini JH. A systematic literature review of blockchain technology and accounting issues: Is it a hype or hope?. South African Journal of Accounting Research. 2024 Sep 10:1-35.

[93] Kuldova TØ. Philanthrocapitalism and the compliance-industrial complex: doing 'Good', fighting crime, and foreclosing alternatives. InCompliance, Defiance, and 'Dirty'Luxury: New Perspectives on Anti-Corruption in Elite Contexts 2024 Aug 1 (pp. 91-121). Cham: Springer Nature Switzerland.

[94] Soana G, de Arruda T. Central Bank Digital Currencies and financial integrity: finding a new trade-off between privacy and traceability within a changing financial architecture. Journal of Banking Regulation. 2024 Mar 20:1-20.

[95] Gade KR. Event-Driven Data Modeling in Fintech: A Real-Time Approach. Journal of Computational Innovation. 2023 Jan 11;3(1).

[96] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[97] Anagnostopoulos I. Fintech and regtech: Impact on regulators and banks. Journal of Economics and Business. 2018 Nov 1;100:7-25.

[98] Fischer-Hübner S, Alcaraz C, Ferreira A, Fernandez-Gago C, Lopez J, Markatos E, Islami L, Akil M. Stakeholder perspectives and requirements on cybersecurity in Europe. Journal of information security and applications. 2021 Sep 1;61:102916.

[99] Albouq SS, Abi Sen AA, Almashf N, Yamin M, Alshanqiti A, Bahbouh NM. A survey of interoperability challenges and solutions for dealing with them in IoT environment. IEEE Access. 2022 Mar 25;10:36416-28.

[100] Carlos Ferreira J, Elvas LB, Correia R, Mascarenhas M. Enhancing EHR Interoperability and Security through Distributed Ledger Technology: A Review. InHealthcare 2024 Oct 2 (Vol. 12, No. 19, p. 1967). MDPI.

[101] Radhi BM, Hussain MA, Abduljabbar ZA, Nyangaresi VO. Secure and Fast Remote Application–Based Authentication Dragonfly Using an LED Algorithm in Smart Buildings. In2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2024 Feb 19 (pp. 509-517). IEEE.

[102] Burton A, Cooper C, Dar A, Mathews L, Tripathi K. Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. Experimental gerontology. 2022 Mar 1;159:111678.

[103] Shao C, Ciampaglia GL, Varol O, Yang KC, Flammini A, Menczer F. The spread of low-credibility content by social bots. Nature communications. 2018 Nov 20;9(1):1-9.

[104] Ruffo G, Semeraro A, Giachanou A, Rosso P. Studying fake news spreading, polarisation dynamics, and manipulation by bots: A tale of networks and language. Computer science review. 2023 Feb 1;47:100531.

[105] Farid H. Creating, using, misusing, and detecting deep fakes. Journal of Online Trust and Safety. 2022 Sep 20;1(4).

[106] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[107] Button M, Stiernstedt P. Comparing private security regulation in the European Union. InThe Rise of Comparative Policing 2021 Aug 26 (pp. 35-51). Routledge.

[108] Chakraborty G. Evolving profiles of financial risk management in the era of digitization: The tomorrow that began in the past. Journal of Public Affairs. 2020 May;20(2):e2034.

[109] Edmund E. Risk Based Security Models for Veteran Owned Small Businesses. International Journal of Research Publication and Reviews. 2024 Dec;5(12):4304-18.

[110] Culot G, Fattori F, Podrecca M, Sartor M. Addressing industry 4.0 cybersecurity challenges. IEEE Engineering Management Review. 2019 Jul 9;47(3):79-86.

[111] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28;15(13):10264.

[112] Butavicius M, Taib R, Han SJ. Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. Computers & Security. 2022 Dec 1;123:102937.

[113] Lam H, Beckman T, Harcourt M, Shanmugam S. Bring Your Own Device (BYOD): Organizational Control and Justice Perspectives. Employee Responsibilities and Rights Journal. 2024 Mar 20:1-9.

[114] Halim II, Buja AG, Zain JM, Ngah AH, Bansal R. BYOD Security Policy Model: A Systematic Literature Review. Journal of Advanced Research in Applied Sciences and Engineering Technology. 2024 Oct 14:170-86.

[115] Zhou J, Joshi P, Zeng H, Li R. Btmonitor: Bit-time-based intrusion detection and attacker identification in controller area network. ACM Transactions on Embedded Computing Systems (TECS). 2019 Nov 15;18(6):1-23.

[116] Peters A, Jordan A. Countering the cyber enforcement gap: Strengthening global capacity on cybercrime. J. Nat'l Sec. L. & Pol'y. 2019;10:487.

[117] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[118] Ismaeil MK. Harnessing AI for Next-Generation Financial Fraud Detection: A DataDriven Revolution. Journal of Ecohumanism. 2024;3(7):811-21.

[119] Brunotte W, Specht A, Chazette L, Schneider K. Privacy explanations–a means to end-user trust. Journal of Systems and Software. 2023 Jan 1;195:111545.

[120] Malhotra P, Singh Y, Anand P, Bangotra DK, Singh PK, Hong WC. Internet of things: Evolution, concerns and security challenges. Sensors. 2021 Mar 5;21(5):1809.

[121] Humayun M, Tariq N, Alfayad M, Zakwan M, Alwakid G, Assiri M. Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey. IEEE Access. 2024 Feb 13.

[122] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[123] Jaiswal A, Dwivedi P, Dewang RK. Machine learning approaches to detect, prevent and mitigate malicious insider threats: State-of-the-art review. Multimedia Tools and Applications. 2024 Oct 4:1-41.

[124] Asasfeh A, Alnawayseh SE, AbdElkareem R, Salahat M. Human Factors In Security Management: Understanding And Mitigating Insider Threats. In2024 2nd International Conference on Cyber Resilience (ICCR) 2024 Feb 26 (pp. 1-10). IEEE.

[125] Alzaabi FR, Mehmood A. A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. IEEE Access. 2024 Feb 26;12:30907-27.

[126] Jones LA. Unveiling Human Factors: Aligning Facets of Cybersecurity Leadership, Insider Threats, and Arsonist Attributes to Reduce Cyber Risk. SocioEconomic Challenges. 2024 Jul 2;8(2):44-63.

[127] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[128] Agahari W, Ofe H, de Reuver M. It is not (only) about privacy: How multi-party computation redefines control, trust, and risk in data sharing. Electronic markets. 2022 Sep;32(3):1577-602.

[129] Alsheavi A, Hawbani A, Othman W, Wang X, Qaid G, Zhao L, Al-Dubai A, Zhi L, Ismail AS, Jhaveri R, Alsamhi S. IoT Authentication Protocols: Challenges, and Comparative Analysis. ACM Computing Surveys. 2024 Oct 28.

[130] Pureti N. Strengthening Authentication: Best Practices for Secure Logins. International Journal of Advanced Engineering Technologies and Innovations. 2023 Jan 30;1(01):271-93.

[131] Seah CS, Loh YX, Falahat M, Loh WS, Nuar AN. Guardians of Trust: Fortifying Payment Gateway Security for Digital Prosperity. InAugmenting Retail Reality, Part A: Blockchain, AR, VR, and the Internet of Things 2024 Dec 9 (pp. 43-58). Emerald Publishing Limited.

[132] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19;11(3):55.

[133] Gupta H, Soni P, Kumar R. The Evolutionary Arms Race-Safeguarding Financial Stability through Advanced Fraud Detection Techniques. In2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET) 2024 Aug 23 (pp. 1-6). IEEE.

[134] Rohilla A. Strengthening Financial Resilience: A Holistic Approach to Combatting Fraud. Indian Journal of Economics and Finance (IJEF). 2024 May 30;4(1):20-31.

[135] Abdelkader S, Amissah J, Kinga S, Mugerwa G, Emmanuel E, Mansour DE, Bajaj M, Blazek V, Prokop L. Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. Results in engineering. 2024 Jul 30:102647.

[136] Hegedüs DL, Balogh Á, Érsok M, Erdődi L, Olcsák L, Bánáti A. Beyond Static Defense: Dynamic Honeypots for Proactive Threat Engagement. In2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI) 2024 May 23 (pp. 000547-000552). IEEE.

[137] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[138] Jesus V, Bains B, Chang V. Sharing is caring: Hurdles and prospects of open, crowd-sourced cyber threat intelligence. IEEE Transactions on Engineering Management. 2023 Jun 7;71:6854-73.

[139] Tounsi W. What is cyber threat intelligence and how is it evolving?. Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT. 2019 May 15:1-49.

[140] Ainslie S, Thompson D, Maynard S, Ahmad A. Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Computers & Security. 2023 Sep 1;132:103352.

[141] Rajamäki J, McMenamin S. Utilization and Sharing of Cyber Threat Intelligence Produced by Open-Source Intelligence. InInternational Conference on Cyber Warfare and Security 2024 Mar 21 (Vol. 19, No. 1, pp. 607-611).

[142] Abdali HK, Hussain MA, Abduljabbar ZA, Nyangaresi VO. Implementing Blockchain for Enhancing Security and Authentication in Iraqi E-Government Services. Engineering, Technology & Applied Science Research. 2024 Dec 2;14(6):18222-33.

[143] Kumi S, Lomotey RK, Deters R. A Blockchain-based platform for data management and sharing. Procedia Computer Science. 2022 Jan 1;203:95-102.

[144] Makhdoom I, Zhou I, Abolhasan M, Lipman J, Ni W. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security. 2020 Jan 1;88:101653.

[145] Garcia RD, Ramachandran GS, Jurdak R, Ueyama J. Blockchain-aided and privacy-preserving data governance in multi-stakeholder applications. IEEE Transactions on Network and Service Management. 2022 Nov 28;19(4):3781-93.

[146] Shi P, Wang H, Yang S, Chen C, Yang W. Blockchain-based trusted data sharing among trusted stakeholders in IoT. Software: practice and experience. 2021 Oct;51(10):2051-64.

[147] Alzaidi ZS, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Development Anonymous Authentication Maria et al.'s Scheme of VANETs Using Blockchain and Fog Computing with QR Code Technique. In2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) 2024 Jul 1 (pp. 2247-2252). IEEE.

[148] Ozioko AC. The Use of Artificial Intelligence in Detecting Financial Fraud: Legal and Ethical Considerations. Multi-Disciplinary Research and Development Journals Int'l. 2024 Aug 20;5(1):66-85.

[149] Korkanti S. Enhancing Financial Fraud Detection Using LLMs and Advanced Data Analytics. In2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) 2024 Oct 23 (pp. 1328-1334). IEEE.

[150] Wu Z, Liu J, Wu J, Zheng Z. Transaction Tracking Based on Personalized PageRank Algorithm. InBlockchain Transaction Data Analytics: Complex Network Approaches 2024 Jun 20 (pp. 179-203). Singapore: Springer Nature Singapore.

[151] Ye Z, Misra U, Cheng J, Zhou W, Song D. Specular: Towards secure, trust-minimized optimistic blockchain execution. In2024 IEEE Symposium on Security and Privacy (SP) 2024 May 19 (pp. 3943-3960). IEEE.

[152] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[153] Manoharan G, Dharmaraj A, Sheela SC, Naidu K, Chavva M, Chaudhary JK. Machine learning-based real-time fraud detection in financial transactions. In2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) 2024 May 9 (pp. 1-6). IEEE.

[154] Khurana R. Fraud detection in ecommerce payment systems: The role of predictive ai in real-time transaction security and risk management. International Journal of Applied Machine Learning and Computational Intelligence. 2020;10(6):1-32.

[155] Sharma R, Mehta K, Sharma P. Role of Artificial Intelligence and Machine Learning in Fraud Detection and Prevention. InRisks and Challenges of AI-Driven Finance: Bias, Ethics, and Security 2024 (pp. 90-120). IGI Global.

[156] Thennakoon A, Bhagyani C, Premadasa S, Mihiranga S, Kuruwitaarachchi N. Real-time credit card fraud detection using machine learning. In2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) 2019 Jan 10 (pp. 488-493). IEEE.

[157] Yenurkar G, Mal S, Nyangaresi VO, Kamble S, Damahe L, Bankar N. Revolutionizing Chronic Heart Disease Management: The Role of IoT-Based Ambulatory Blood Pressure Monitoring System. Diagnostics. 2024 Jun 19;14(12):1297.

[158] Nadeem M, Zahra SW, Abbasi MN, Arshad A, Riaz S, Ahmed W. Phishing attack, its detections and prevention techniques. Int. J. Wirel. Secur. Netw. 2023 Sep;1:13-25.

[159] Mashtalyar N, Ntaganzwa UN, Santos T, Hakak S, Ray S. Social engineering attacks: Recent advances and challenges. InInternational Conference on Human-Computer Interaction 2021 Jul 3 (pp. 417-431). Cham: Springer International Publishing.

[160] Kheruddin MS, Zuber MA, Radzai MM. Phishing Attacks: Unraveling Tactics, Threats, and Defenses in the Cybersecurity Landscape. Authorea Preprints. 2024 Jan 15.

[161] Gupta S, Pritwani M, Shrivastava A, Moharir M, AR AK. A Comprehensive Analysis of Social Engineering Attacks: From Phishing to Prevention-Tools, Techniques and Strategies. In2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) 2024 Aug 28 (pp. 1-8). IEEE.

[162] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[163] Alahmed Y, Abadla R, Al Ansari MJ. Exploring the Potential Implications of AI-generated Content in Social Engineering Attacks. In2024 International Conference on Multimedia Computing, Networking and Applications (MCNA) 2024 Sep 17 (pp. 64-73). IEEE.

[164] Garg R. Preventing cyber attacks using artificial intelligence. i-manager's Journal on Software Engineering. 2023 Oct 1;18(2).

[165] Edwards L, Zahid Iqbal M, Hassan M. A multi-layered security model to counter social engineering attacks: a learning-based approach. International Cybersecurity Law Review. 2024 Apr 18:1-24.

[166] Birthriya SK, Ahlawat P, Jain AK. A comprehensive survey of social engineering attacks: taxonomy of attacks, prevention, and mitigation strategies. Journal of Applied Security Research. 2024 Jul 1:1-49.

[167] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[168] Chamikara MA, Bertok P, Khalil I, Liu D, Camtepe S. Privacy preserving distributed machine learning with federated learning. Computer Communications. 2021 Apr 1;171:112-25.

[169] Truex S, Baracaldo N, Anwar A, Steinke T, Ludwig H, Zhang R, Zhou Y. A hybrid approach to privacy-preserving federated learning. InProceedings of the 12th ACM workshop on artificial intelligence and security 2019 Nov 11 (pp. 1-11).

[170] Truong N, Sun K, Wang S, Guitton F, Guo Y. Privacy preservation in federated learning: An insightful survey from the GDPR perspective. Computers & Security. 2021 Nov 1;110:102402.

[171] Ali M, Naeem F, Tariq M, Kaddoum G. Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. IEEE journal of biomedical and health informatics. 2022 Jun 13;27(2):778-89.

[172] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[173] Burton SL. Advancing Cybersecurity: Strategic Insights Into Multifactor Authentication. Organizational Readiness and Research: Security, Management, and Decision Making. 2025:247-82.

[174] Hammoudeh MA, Ebrahim A, Mohamed E, Almansour R, Ibrahim R. Enhancing Security Using E-Authentication System. InInternational Conference on Innovation of Emerging Information and Communication Technology 2023 Sep 11 (pp. 471-486). Cham: Springer Nature Switzerland.

[175] Abduhari ES, Shaik TC, Adidul AB, Ladja JH, Saliddin ES, Adin AJ, Rumbahali FA, Sali AB, Jemser JM, Tahil SK. Access Control Mechanisms and Their Role in Preventing Unauthorized Data Access: A Comparative Analysis of RBAC, MFA, and Strong Passwords. Natural Sciences Engineering and Technology Journal. 2024 Dec 26;5(1):418-30.

[176] Blessing J, Hugenroth D, Anderson RJ, Beresford AR. SoK: Web Authentication in the Age of End-to-End Encryption. arXiv preprint arXiv:2406.18226. 2024 Jun 26.

[177] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan;13(2):691.

[178] Fathima AR, Saravanan A. An approach to cloud user access control using behavioral biometric-based authentication and continuous monitoring. International Journal of Advanced Technology and Engineering Exploration. 2024 Oct 1;11(119):1469.

[179] Mali S. Assessing the Effectiveness of Multi-Factor Authentication in Cloud-Based Big Data Environments. Internet of Things and Cloud Computing. 2024 Aug;9(1):17-27.

[180] Shende SW, Tembhurne JV, Ansari NA. Deep learning based authentication schemes for smart devices in different modalities: progress, challenges, performance, datasets and future directions. Multimedia Tools and Applications. 2024 Feb 8:1-43.

[181] Jeong JJ, Zolotavkin Y, Doss R. Examining the current status and emerging trends in continuous authentication technologies through citation network analysis. ACM Computing Surveys. 2022 Dec 7;55(6):1-31.

[182] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[183] Jamwal S, Cano J, Lee GM, Tran NH, Truong N. A survey on ethereum pseudonymity: Techniques, challenges, and future directions. Journal of Network and Computer Applications. 2024 Sep 7:104019.

[184] Alghuried A, Alkinoon M, Mohaisen M, Wang A, Zou CC, Mohaisen D. Blockchain security and privacy examined: Threats, challenges, applications, and tools. The ACM Distributed Ledger Technologies: Research and Practice, ACM DLT. 2024.

[185] Tyagi AK, Balogun BF, Tiwari S. Role of Blockchain in Digital Forensics: A Systematic Study. Global Perspectives on the Applications of Computer Vision in Cybersecurity. 2024:197-222.

[186] Sivakumar N, Jagatheeshkumar G. An Intelligent Blockchain based Framework for secured Cryptocurrency Exchanges to Detect Fraudulent Transactions. In2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) 2024 Jun 24 (pp. 1-8). IEEE.

[187] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1;24:100969.

[188] Ashfaq T, Khalid R, Yahaya AS, Aslam S, Azar AT, Alsafari S, Hameed IA. A machine learning and blockchain based efficient fraud detection mechanism. Sensors. 2022 Sep 21;22(19):7162.

[189] Sangal S, Duggal G, Nigam A. Blockchain's double-edged sword: thematic review of illegal activities using blockchain. Journal of Information, Communication and Ethics in Society. 2024 Mar 4;22(1):58-81.

[190] Hassan MU, Rehmani MH, Chen J. Anomaly detection in blockchain networks: A comprehensive survey. IEEE Communications Surveys & Tutorials. 2022 Sep 12;25(1):289-318.

[191] Venčkauskas A, Grigaliūnas Š, Pocius L, Brūzgienė R, Romanovs A. Machine learning in money laundering detection over blockchain technology. IEEE Access. 2024 Aug 29.

[192] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[193] Yousefi M, Rajabi E. Digital Identity Verification Methods in Financial Services: Enhancing Security and Compliance. Business, Marketing, and Finance Open. 2024 Mar 1;1(2):25-40.

[194] Irvin-Erickson Y. Identity fraud victimization: a critical review of the literature of the past two decades. Crime Science. 2024 Feb 10;13(1):3.

[195] Saluja S. Identity theft fraud-major loophole for FinTech industry in India. Journal of Financial Crime. 2024 Jan 11;31(1):146-57.

[196] Kayser CS, Back S, Toro-Alvarez MM. Identity Theft: The Importance of Prosecuting on Behalf of Victims. Laws. 2024 Nov 7;13(6):68.

[197] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InFuture Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings 2022 Sep 18 (pp. 16-36). Cham: Springer International Publishing.

[198] Oduri S. Continuous Authentication and Behavioral Biometrics: Enhancing Cybersecurity in the Digital Era. International Journal of Innovative Research in Science Engineering and Technology. 2024;13(7):13632-40.

[199] Aboukadri S, Ouaddah A, Mezrioui A. Machine learning in identity and access management systems: Survey and deep dive. Computers & Security. 2024 Jan 23:103729.

[200] Ayeswarya S, Singh KJ. A comprehensive review on secure biometric-based continuous authentication and user profiling. IEEE Access. 2024 Jun 10.

[201] Awad AI, Babu A, Barka E, Shuaib K. AI-powered biometrics for Internet of Things security: A review and future vision. Journal of Information Security and Applications. 2024 May 1;82:103748.

[202] Nyangaresi VO, Yenurkar GK. Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor networks. High-Confidence Computing. 2023 Nov 24:100178.

[203] Wronka C. Financial crime in the decentralized finance ecosystem: new challenges for compliance. Journal of Financial Crime. 2023 Jan 2;30(1):97-113.

[204] Bodo B, De Filippi P. Trust in context: the impact of regulation on blockchain and DeFi. Regulation & Governance. 2022.

[205] Alamsyah A, Kusuma GN, Ramadhani DP. A Review on Decentralized Finance Ecosystems. Future Internet. 2024 Feb 26;16(3):76.

[206] Ali K, Shahzad A, Chaudhary HK. The Role of Decentralized Finance (DeFi) in Reshaping Global Financial Inclusion: Opportunities and Risks. Social Science Review Archives. 2024 Oct 29;2(2):560-79.

[207] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[208] Iyer R, Maralapalle V, Patil D, Irfan M. The Future of Smart Contracts: Pioneering a New Era of Automated Transactions and Trust in the Digital Economy. InAI-Driven Decentralized Finance and the Future of Finance 2024 (pp. 225-251). IGI Global.

[209] Parisi C, Budorin D. DeFi Security. InWeb3 Applications Security and New Security Landscape: Theories and Practices 2024 Jun 5 (pp. 3-18). Cham: Springer Nature Switzerland.

[210] Bourveau T, Brendel J, Schoenfeld J. Decentralized Finance (DeFi) assurance: early evidence. Review of Accounting Studies. 2024 Sep;29(3):2209-53.

[211] Guelida O, Jai Andaloussi S, Ouchetto O. Smart Contracts in Finance and Banking Systems in the Era of Industry 5.0: A Systematic Review. Industry 5.0 and Emerging Technologies: Transformation Through Technology and Innovations. 2024 Nov 12:317-46.

[212] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[213] Raharjo B, Fitrianto Y. Prediction and Detection of Scam Threats on Digital Platforms for Indonesian Users Using Machine Learning Models. Journal of Technology Informatics and Engineering. 2024 Dec 25;3(3):350-69.

[214] Morić Z, Dakic V, Djekic D, Regvart D. Protection of Personal Data in the Context of E-Commerce. Journal of cybersecurity and privacy. 2024 Sep 20;4(3):731-61.

[215] Cardona LF, Guzmán-Luna JA, Restrepo-Carmona JA. Bibliometric analysis of the machine learning applications in fraud detection on crowdfunding platforms. Journal of Risk and Financial Management. 2024 Aug 13;17(8):352.

[216] Meng T, Jing X, Yan Z, Pedrycz W. A survey on machine learning for data fusion. Information Fusion. 2020 May 1;57:115-29.

[217] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[218] Tambe Ebot AC, Siponen M, Topalli V. Towards a cybercontextual transmission model for online scamming. European Journal of Information Systems. 2024 Jul 3;33(4):571-96.

[219] Arisdakessian S, Wahab OA, Mourad A, Otrok H, Guizani M. A survey on IoT intrusion detection: Federated learning, game theory, social psychology, and explainable AI as future directions. IEEE Internet of Things Journal. 2022 Aug 31;10(5):4059-92.

[220] Pimentel A, Steinmetz KF. Enacting social engineering: the emotional experience of information security deception. Crime, Law and Social Change. 2022 Apr;77(3):341-61.

[221] Hatfield JM. Social engineering in cybersecurity: The evolution of a concept. Computers & Security. 2018 Mar 1;73:102-13.

[222] Moon P, Yenurkar G, Nyangaresi VO, Raut A, Dapkekar N, Rathod J, Dabare P. An improved custom convolutional neural network based hand sign recognition using machine learning algorithm. Engineering Reports. 2024:e12878.

[223] Palaniappan K, Duraipandi B, Balasubramanian UM. Dynamic behavioral profiling for anomaly detection in software-defined IoT networks: A machine learning approach. Peer-to-Peer Networking and Applications. 2024 Jul;17(4):2450-69.

[224] Bello OA, Folorunso A, Onwuchekwa J, Ejiofor OE, Budale FZ, Egwuonwu MN. Analysing the Impact of Advanced Analytics on Fraud Detection: A Machine Learning Perspective. European Journal of Computer Science and Information Technology. 2023;11(6):103-26.

[225] Nespoli P, Papamartzivanos D, Mármol FG, Kambourakis G. Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks. IEEE Communications Surveys & Tutorials. 2017 Dec 7;20(2):1361-96.

[226] Yusof ZB. Effectiveness of Endpoint Detection and Response Solutions in Combating Modern Cyber Threats. Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures. 2024 Dec 4;8(12):1-9.

[227] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25;4(1):10-9.

[228] Albshaier L, Almarri S, Hafizur Rahman MM. A review of blockchain's role in E-Commerce transactions: Open challenges, and future research directions. Computers. 2024 Jan 17;13(1):27.

[229] Roy A, Tinny SS. Cybersecurity and Blockchain for Secure Financial Transactions: Evaluating, Implementing, and Mitigating Risks of Digital Payments. International Journal of Applied and Natural Sciences. 2024 Aug 1;2(1):38-48.

[230] Alkadi O, Moustafa N, Turnbull B. A review of intrusion detection and blockchain applications in the cloud: approaches, challenges and solutions. IEEE Access. 2020 Jun 3;8:104893-917.

[231] Fadhil J, Zeebaree SR. Blockchain for Distributed Systems Security in Cloud Computing: A Review of Applications and Challenges. Indonesian Journal of Computer Science. 2024 Apr 1;13(2).

[232] Al-Maliki H, AL-Asadi HA, Abduljabbar ZA, Nyangaresi VO. Reliable Vehicular Ad Hoc Networks for Intelligent Transportation Systems based on the Snake Optimization Algorithm. Engineering, Technology & Applied Science Research. 2024 Dec 2;14(6):18631-9.

[233] Nair MM, Deshmukh A, Tyagi AK. Artificial intelligence for cyber security: Current trends and future challenges. Automated Secure Computing for Next-Generation Systems. 2024 May 3:83-114.

[234] Shafik W. Artificial Intelligence-Enabled Cybersecurity and Internet of Things Applications in Smart Cities. InBuilding Tomorrow's Smart Cities With 6G Infrastructure Technology 2025 (pp. 301-334). IGI Global Scientific Publishing.

[235] Awadallah A, Eledlebi K, Zemerly J, Puthal D, Damiani E, Taha K, Kim TY, Yoo PD, Choo KK, Yim MS, Yeun CY. Artificial intelligence-based cybersecurity for the metaverse: research challenges and opportunities. IEEE Communications Surveys & Tutorials. 2024 Aug 12.

[236] Bhardwaj A. Cybercrime, Digital Terrorism, and 5G Paradigm: Attack Trends of the New Millennium. In5G and Fiber Optics Security Technologies for Smart Grid Cyber Defense 2024 (pp. 1-27). IGI Global.

[237] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[238] Hassan A, Nizam-Uddin N, Quddus A, Hassan SR, Rehman AU, Bharany S. Navigating IoT Security: Insights into Architecture, Key Security Features, Attacks, Current Challenges and AI-Driven Solutions Shaping the Future of Connectivity. Computers, Materials & Continua. 2024 Dec 1;81(3).

[239] Kavitha D, Thejas S. AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation. IEEE Access. 2024 Nov 8.

[240] Alsadie D. Artificial Intelligence Techniques for Securing Fog Computing Environments: Trends, Challenges, and Future Directions. IEEE Access. 2024 Sep 19.

[241] Patel K, Vadher A, Patel M, Thaker J, Bhise A. AI-Based Security System for 5G Enabled IoT. In2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE) 2024 Feb 22 (pp. 1-7). IEEE.

[242] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[243] Shandilya SK, Datta A, Kartik Y, Nagar A. Navigating the Regulatory Landscape. InDigital Resilience: Navigating Disruption and Safeguarding Data Privacy 2024 Jan 2 (pp. 127-240). Cham: Springer Nature Switzerland.

[244] Abrahams TO, Ewuga SK, Kaggwa S, Uwaoma PU, Hassan AO, Dawodu SO. Mastering compliance: a comprehensive review of regulatory frameworks in accounting and cybersecurity. Computer Science & IT Research Journal. 2024 Jan 11;5(1):120-40.

[245] Syaufi A, Zahra AF, Gholi FM. Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes. International Journal of Cyber Criminology. 2023 Jul 19;17(1):85-101.

[246] Siqi C, Rajamanickam R, Manap NA, Zahir ZM. Application of Blockchain Technology in Cross-Border Telecommunications Network Fraud to Ensure China's Judicial Justice. Jurnal IUS Kajian Hukum dan Keadilan. 2024 Dec 29;12(3):472-86.

[247] Eyo I, Okebugwu GC. Analysis of Fundamental Challenges in the Combat of Transnational Crimes. International Journal of Research and Innovation in Social Science. 2024;8(4):1297-318.

[248] Qu J, Cheng H. Policing telecommunication and cyber fraud: Perceptions and experiences of law enforcement officers in China. Crime, Law and Social Change. 2024 Feb 29:1-23.