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

Navigating the nexus of security and privacy in modern financial technologies

Florence Olweny *

Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya.

GSC Advanced Research and Reviews, 2024, 18(02), 167–197

Publication history: Received on 26 December 2023; revised on 06 February 2024; accepted on 09 February 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.18.2.0043

Abstract

As the financial service sector rapidly evolves with the integration of cutting-edge technologies, the intersection of security and privacy becomes paramount. This paper delves into the intricate landscape of security and privacy issues within the financial service sector, offering a comprehensive analysis of the challenges and opportunities presented by emerging technologies. From blockchain to artificial intelligence, the paper explores the vulnerabilities inherent in these innovations and the consequential threats to sensitive financial data. Through an examination of recent case studies, regulatory frameworks, and technological advancements, this work aims to provide a nuanced understanding of the evolving threat landscape. Additionally, the paper proposes strategic solutions and best practices to fortify the security and privacy architecture surrounding financial technologies, fostering a resilient and trustworthy ecosystem. This research contributes to the ongoing dialogue surrounding the imperative of safeguarding financial systems, ensuring that innovation aligns seamlessly with the imperatives of confidentiality, integrity, and availability in an era where financial services and technological advancements are inextricably linked.

Keywords: Attacks; Fintech; Privacy; Security; Threats

1. Introduction

In the contemporary digital era, the financial service sector stands at the nexus of technological innovation and unprecedented data proliferation. As financial institutions race to harness the transformative power of emerging technologies, they simultaneously grapple with the escalating challenges posed by security breaches and privacy concerns [1]-[3]. The financial industry has undergone a paradigm shift in recent years, driven by advancements such as blockchain, artificial intelligence, cloud computing, and mobile technologies [4]-[7]. While these innovations have undeniably revolutionized the efficiency and accessibility of financial services, they have also exposed vulnerabilities that demand vigilant attention. The unprecedented volumes of sensitive financial data processed and stored across interconnected networks have made the sector an attractive target for malicious actors seeking unauthorized access, data breaches, and financial fraud. As financial institutions increasingly rely on interconnected digital ecosystems, the need for robust security measures and airtight privacy safeguards has never been more pressing. The stakes are high, with potential repercussions ranging from financial losses and reputational damage to systemic threats that could undermine the stability of the entire financial system [7], [8]. Moreover, the regulatory landscape is evolving to keep pace with the rapid technological advancements, imposing new compliance requirements and expectations on financial institutions to secure their technological infrastructures.

Against this backdrop, this paper undertakes a comprehensive examination of the security and privacy challenges confronting the financial service sector. By analyzing the vulnerabilities inherent in the adoption of transformative technologies, this paper aims to shed light on the multifaceted nature of the risks faced by financial institutions. Drawing on a synthesis of academic research, industry reports, and real-world case studies, our objective is to provide a nuanced understanding of the intricate web of security and privacy issues surrounding financial technologies. The paper unfolds

* Corresponding author: Florence Olweny

in subsequent chapters, each dedicated to dissecting specific technologies and their associated security and privacy challenges. The paper explores the promises and pitfalls of blockchain applications, the ethical considerations in deploying artificial intelligence in financial decision-making, the implications of cloud computing on data security, and the vulnerabilities introduced by the ubiquity of mobile technologies in financial transactions. Through this detailed analysis, this paper strives to arm stakeholders in the financial service sector with insights and strategies to navigate this complex landscape and foster a secure, privacy-respecting environment for both institutions and their clients.

In so doing, this paper seeks to contribute to the ongoing discourse on fortifying the security and privacy foundations of financial service sector technologies. It is imperative to recognize that the landscape is dynamic, and proactive measures must be taken to stay ahead of the ever-evolving threat landscape. Only through a collective and informed effort can the integrity of financial systems be safeguarded, ensuring that the benefits of technological innovation are harnessed responsibly and sustainably.

2. Key financial service sector technologies

The financial service sector is undergoing a profound transformation driven by advancements in technology. Key technologies are shaping the industry's landscape, introducing both unprecedented opportunities and unique challenges. Below, several pivotal financial service sector technologies are extensively described.

2.1. Blockchain and Distributed Ledger Technology (DLT)

Blockchain, a decentralized and distributed ledger technology, has gained prominence for its ability to enhance security, transparency, and efficiency in financial transactions. It represents transformative innovations that have reshaped the landscape of secure and transparent digital transactions. Figure 1 presents some of the use cases of DLT in the finance industry.

Figure 1 DLT use cases in the finance industry

At its core, blockchain is a decentralized and immutable ledger that enables the secure recording and verification of transactions across a distributed network of nodes [9]-[11]. The tamper-resistant nature of blockchain, achieved through cryptographic algorithms and consensus mechanisms, ensures the integrity and transparency of data. Beyond its foundational application in crypto-currencies like Bitcoin, blockchain has found widespread use across various industries, including finance. DLT, of which blockchain is a subset, extends the concept of decentralized ledgers to diverse forms of data sharing and consensus-building, promising enhanced security, efficiency, and trust in an array of applications beyond traditional financial transactions. As the technology matures, its potential impact on supply chains, healthcare, and governance is becoming increasingly evident, ushering in an era where decentralized and transparent systems redefine how we manage and authenticate digital information [12]-[16].

Blockchain eliminates the need for intermediaries, reducing transaction costs and accelerating settlement processes. Smart contracts, self-executing contracts with coded terms, further streamline and automate agreements. While blockchain enhances security, issues such as scalability, regulatory uncertainty, and the environmental impact of some consensus algorithms (such as Proof of Work) pose challenges.

2.2. Artificial Intelligence (AI) and Machine Learning (ML)

AI and ML algorithms are revolutionizing data analysis, risk assessment, fraud detection, and customer service within the financial sector. These algorithms have emerged as transformative forces in the financial sector, revolutionizing the way institutions analyze data, make decisions, and interact with customers as shown in Figure 2. AI-powered algorithms and ML models enable financial institutions to process vast amounts of data, identify patterns, and extract actionable insights for risk management, fraud detection, and personalized customer services [17]-[21]. Whether optimizing investment portfolios, enhancing credit risk assessments, or automating customer support through chatbots, AI and ML applications have significantly increased efficiency and accuracy in decision-making processes. However, the adoption of these technologies also poses challenges, such as the need for explainability and ethical considerations. As financial institutions continue to leverage AI and ML to navigate complex market dynamics, the ongoing refinement of algorithms and the establishment of ethical frameworks remain crucial to ensure responsible and secure integration of these technologies within the financial landscape [22], [23].

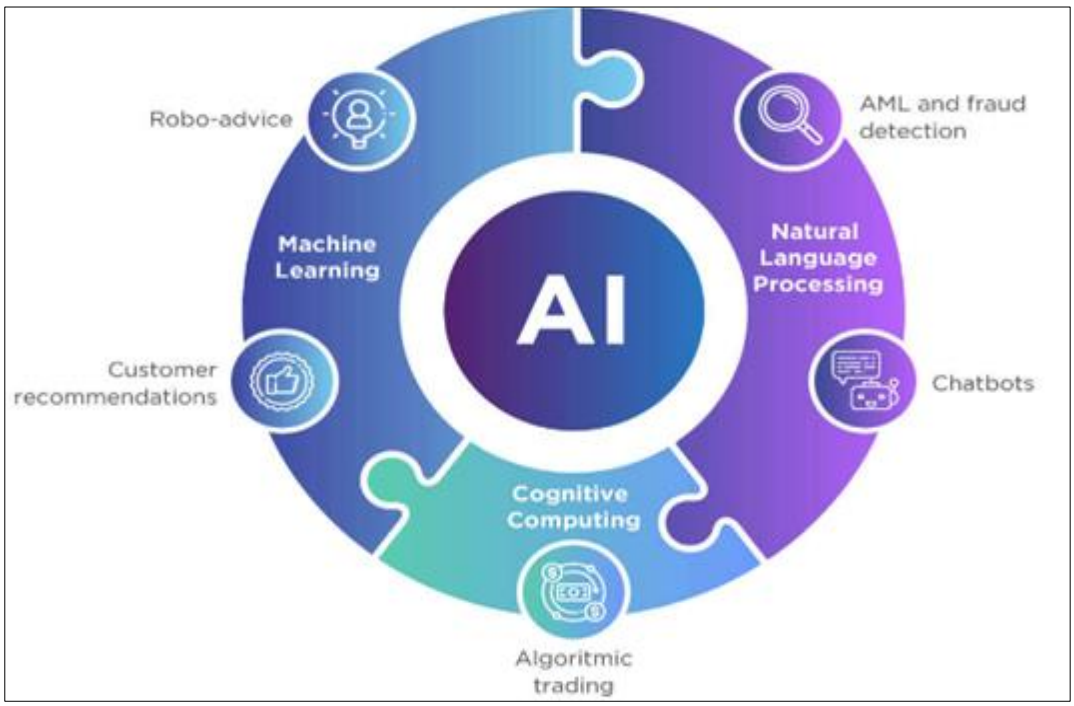

Figure 2 AI and ML in FinTech

AI-driven algorithms enable more accurate credit scoring, personalized financial advice, and predictive analytics, enhancing decision-making processes. However, ethical considerations, algorithmic biases, and the interpretability of AI decisions are critical challenges. Striking the right balance between automation and human oversight is crucial.

2.3. Cloud Computing

Cloud computing provides scalable and on-demand access to computing resources, enabling financial institutions to optimize operations and enhance agility [24], [25]. It has emerged as a fundamental enabler of innovation and efficiency in the financial sector, transforming the way institutions manage and deliver their services. By leveraging scalable and on-demand access to computing resources, financial organizations can enhance operational agility, streamline processes, and optimize costs. The cloud provides a robust infrastructure for data storage, analytics, and the development of sophisticated financial applications as shown in Figure 3. Moreover, it facilitates remote access and collaboration, allowing financial professionals to work seamlessly across geographies. However, the adoption of cloud computing in the financial sector also brings forth considerations related to data security, regulatory compliance, and the need for resilient cloud architectures [26]-[30]. As financial institutions navigate this technological shift, they must strike a balance between reaping the benefits of cloud-based solutions and implementing robust measures to safeguard sensitive financial data and maintain regulatory adherence.

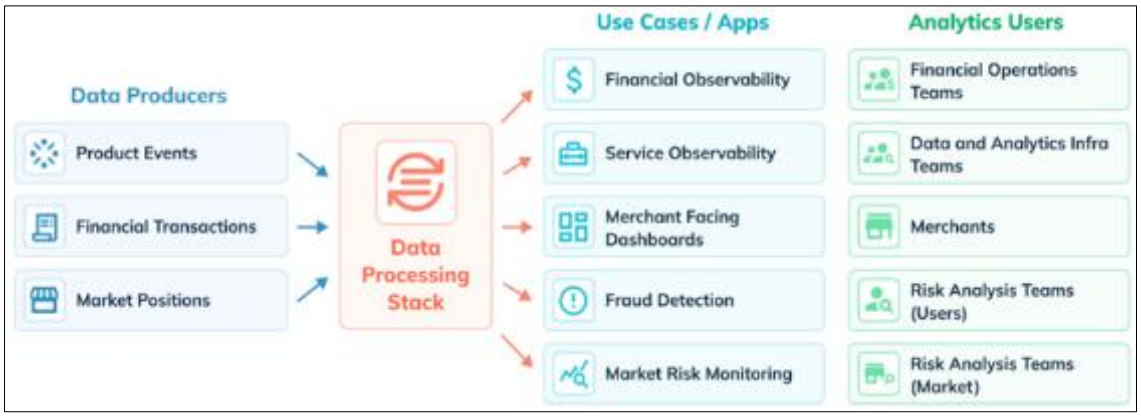

Figure 3 Cloud computing use cases in the financial sector

Cloud computing facilitates cost savings, improves collaboration, and supports the development of innovative financial products and services. However, data security concerns, regulatory compliance, and potential disruptions due to service outages are challenges associated with reliance on cloud infrastructure.

2.4. Mobile Technologies

Mobile technologies, including smartphones and tablets, have become integral to the delivery of financial services, fostering increased accessibility and convenience [31], [32]. These technologies have become integral to the financial sector, revolutionizing how individuals access and manage their financial affairs. The ubiquity of smartphones has paved the way for mobile banking, digital wallets, and contactless payments, offering users unprecedented convenience and accessibility as shown in Figure 4. Financial institutions leverage mobile apps to provide services such as account management, fund transfers, and real-time transaction monitoring, enabling customers to conduct financial transactions anytime, anywhere.

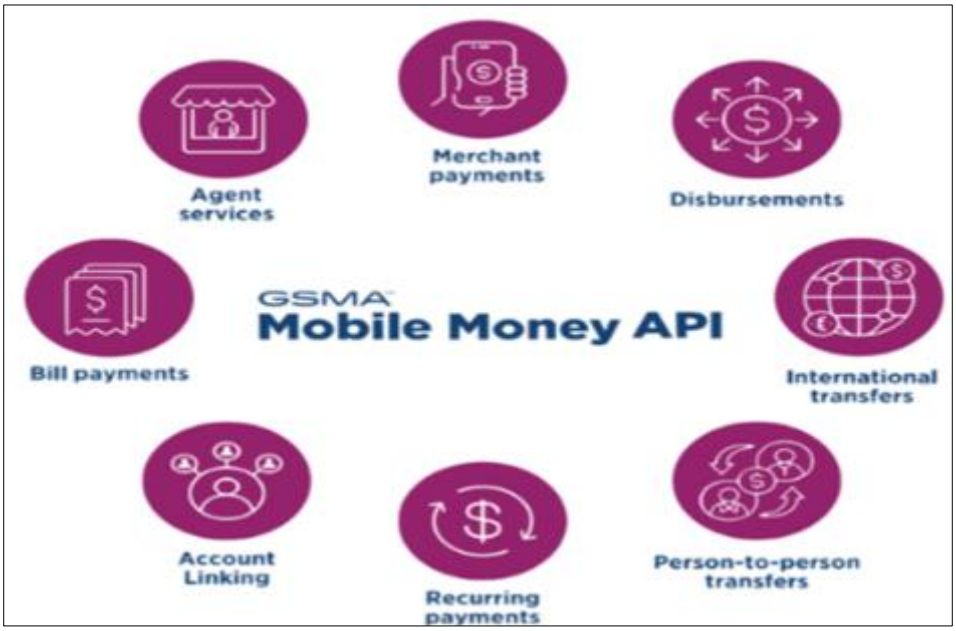

Figure 4 Mobile technology in the finance industry

The transformative impact extends beyond consumer-facing applications, with mobile technologies influencing how financial professionals collaborate, communicate, and execute transactions. However, the rapid proliferation of mobile technologies in the financial sector also introduces security challenges, including the need for robust authentication methods and safeguards against mobile-specific threats like phishing and malware [33]-[35]. As the reliance on mobile solutions continues to grow, striking a balance between convenience and security remains a paramount consideration for financial institutions navigating the mobile-driven landscape.

Mobile banking, mobile payments, and digital wallets have transformed the way consumers interact with financial institutions, enabling transactions anytime, anywhere. Unfortunately, security risks such as mobile malware, phishing, and the need for robust authentication mechanisms are key concerns. Ensuring a seamless user experience while maintaining security is a delicate balance.

2.5. Crypto-currencies and Digital Assets

Crypto-currencies, such as Bitcoin and Ethereum, have introduced decentralized digital assets that operate on blockchain technology. According to [36], cryptocurrencies and digital assets have disrupted traditional financial paradigms, introducing decentralized and secure alternatives to traditional forms of currency and assets. Figure 5 shows some of the digital assets. Led by pioneers like Bitcoin and Ethereum, crypto-currencies leverage blockchain technology to enable peer-to-peer transactions without the need for intermediaries. Beyond serving as digital currencies, they have become a burgeoning asset class with diverse applications, including smart contracts, decentralized finance (DeFi), and non-fungible tokens (NFTs). While offering potential benefits such as financial inclusion, borderless transactions, and increased transparency, the adoption of crypto-currencies also raises challenges related to regulatory frameworks, price volatility, and security considerations [37]-[39]. As financial institutions grapple with integrating digital assets into their portfolios, there is a dynamic evolution in the regulatory landscape and an exploration of how these technologies can coexist within the broader financial sector.

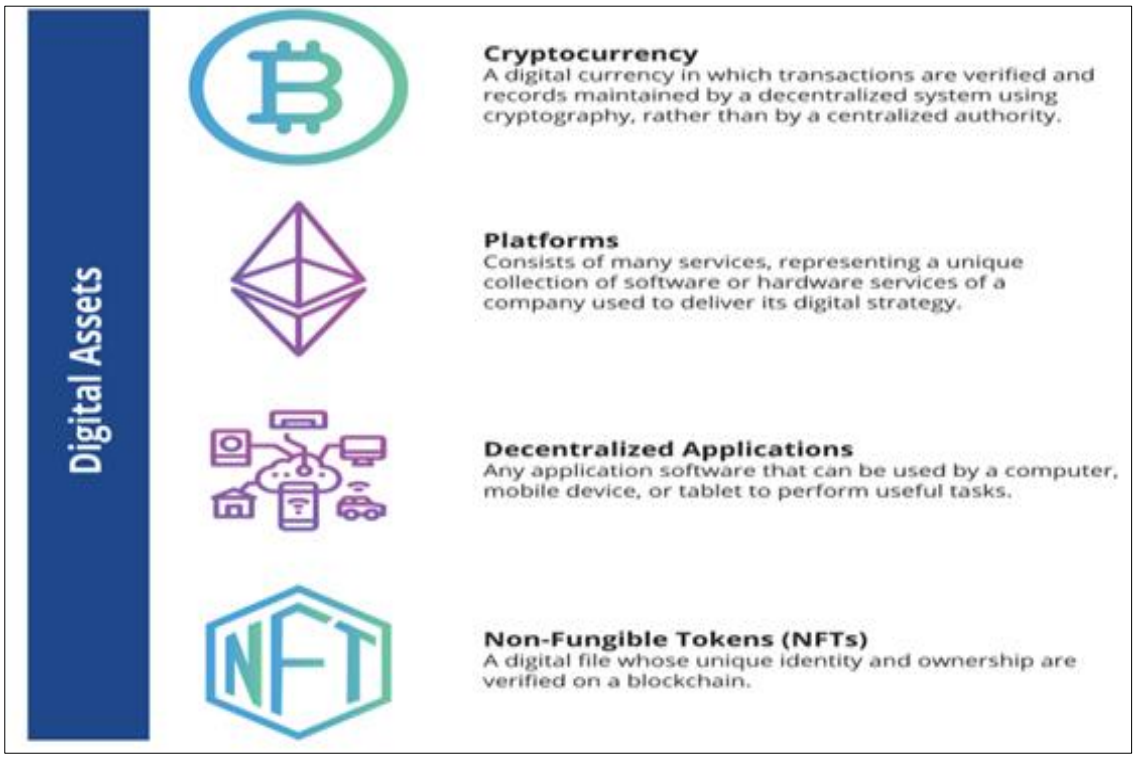

Figure 5 Roles of various digital assets

Crypto-currencies provide an alternative form of currency, facilitate cross-border transactions, and offer potential for financial inclusion as shown in Figure 6. However, regulatory uncertainties, price volatility, and concerns about illicit activities in the crypto space pose challenges for widespread adoption and acceptance by traditional financial institutions.

In summary, crypto-currencies and digital assets play a transformative role in FinTech, representing decentralized forms of digital or virtual currency that leverage cryptographic techniques for secure financial transactions. Crypto-currencies, such as Bitcoin and Ethereum, operate on blockchain technology, a decentralized and tamper-resistant ledger, ensuring transparency and immutability. Digital assets encompass a broader spectrum, including tokens, smart contracts, and various financial instruments, all existing in digital form. These innovations within FinTech enable peer-to-peer transactions, reduce reliance on traditional banking systems, and offer efficient, secure, and borderless financial solutions, thereby reshaping the landscape of global finance by providing alternatives to traditional banking and payment methods.

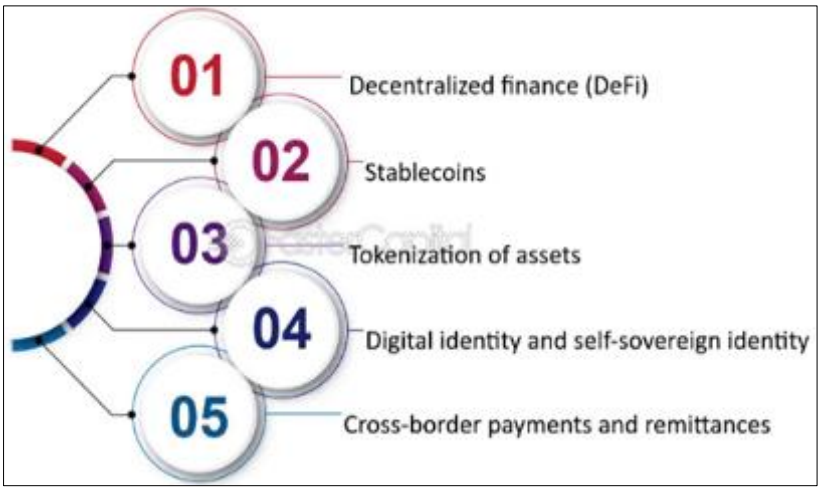

Figure 6 Crypto-currencies and Digital Assets in FinTech

2.6. RegTech (Regulatory Technology)

RegTech leverages technology to help financial institutions comply with regulatory requirements more efficiently [40] and effectively. It has emerged as a pivotal force in the financial sector, addressing the increasingly complex landscape of regulatory compliance, as shown in Figure 7. Leveraging advanced technologies such as artificial intelligence, machine learning, and data analytics, RegTech solutions automate and streamline processes associated with meeting regulatory requirements. These innovations offer financial institutions efficient tools for risk management, fraud prevention, and adherence to evolving compliance standards [41]-[44]. By enhancing the speed and accuracy of regulatory compliance tasks, RegTech not only reduces operational costs but also enables institutions to proactively navigate the intricate regulatory environment. As regulatory demands continue to evolve, the integration of RegTech is poised to play a crucial role in fostering a more agile, efficient, and compliant financial ecosystem.

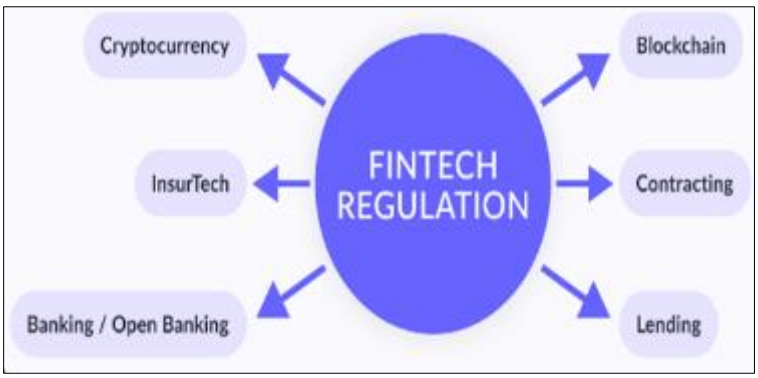

Figure 7 RegTech application domains

Automation of compliance processes, real-time monitoring, and enhanced reporting capabilities streamline regulatory adherence, reducing costs and risks. Unfortunately, balancing innovation with regulatory compliance, ensuring data privacy, and adapting to evolving regulatory landscapes are key challenges.

2.7. Cyber-security Solutions

With the increasing digitization of financial services, robust cyber-security measures are critical to protect sensitive data and maintain the trust of customers. As explained in [45], cyber-security solutions stand as the linchpin of safeguarding the financial sector against an ever-expanding array of digital threats. Given the sensitive nature of financial data, institutions rely on robust cyber-security measures encompassing encryption, advanced threat detection systems, and secure access controls to fortify their defenses as shown in Figure 8. These solutions are instrumental in thwarting cyber attacks such as data breaches, ransomware, and phishing attempts, which can compromise the confidentiality and integrity of financial information.

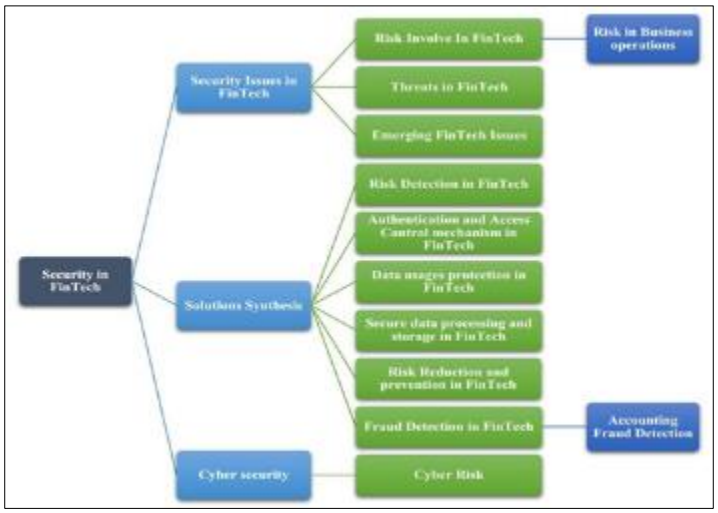

Figure 8 Cyber-security Solutions in FinTech

Continuous innovation in cyber-security, including the integration of artificial intelligence and machine learning for proactive threat detection, is imperative to stay ahead of sophisticated adversaries [46]-[50]. As the financial industry continues its digital transformation, the resilience and effectiveness of cyber-security solutions play a pivotal role in maintaining trust, ensuring regulatory compliance, and mitigating the evolving risk landscape. Cyber-security technologies encompass a range of solutions, including encryption, threat detection, and identity management, to safeguard against cyber threats such as data breaches and ransomware attacks. Evidently, cyber-security is an ongoing arms race, and financial institutions must continually invest in advanced technologies to stay ahead of evolving threats. The human factor, including social engineering attacks, remains a significant challenge.

Based on the discussions above, it is clear that key financial service sector technologies are shaping the industry's future by fostering innovation and efficiency. While they offer immense potential, addressing associated challenges is essential to ensure a secure, compliant, and resilient financial ecosystem. As financial institutions navigate this technological landscape, strategic considerations and ongoing adaptation are crucial for harnessing the benefits of these transformative technologies.

3. Need for financial service sector technologies

The need for financial service sector technologies is driven by a confluence of factors that collectively shape the modern landscape of financial services. These technologies address numerous challenges while also unlocking new opportunities for innovation and growth. The sub-sections below delve into some of the compelling needs for financial service sector technologies.

3.1. Enhanced Efficiency and Productivity

Financial technologies automate complex processes, reducing manual errors and streamlining day-to-day operations. This leads to increased efficiency [51] in tasks such as transaction processing, account management, and regulatory compliance. In addition, these technologies enable real-time processing of transactions and data, providing faster and more responsive financial services [52], [53]. This speed is crucial in today's fast-paced business environment.

3.2. Improved Customer Experience

Advanced analytics and AI-driven technologies enable financial institutions to personalize services based on individual customer behaviors and preferences [54], [55]. This personalization enhances customer satisfaction and loyalty. In addition, mobile technologies and digital platforms allow customers to access financial services seamlessly across multiple channels, providing a consistent and user-friendly experience [56], [57].

3.3. Risk Management and Compliance

Financial service sector technologies, including AI and machine learning, play a vital role in identifying patterns indicative of fraudulent activities [58]-[60]. This helps in preventing financial fraud and protecting both institutions and customers. In addition, with ever-evolving regulatory landscapes, technologies such as RegTech assist financial

institutions in automating compliance processes, reducing the risk of non-compliance and associated penalties [61], [62].

3.4. Financial Inclusion

Technologies enable the delivery of financial services to previously underserved or unbanked populations. Mobile banking, digital wallets, and blockchain-based solutions contribute to greater financial inclusion by providing access to banking services and transactions [63], [64].

3.5. Innovation and Competitive Advantage

Financial institutions leverage blockchain for secure and transparent transactions [65], [66]. Cryptocurrencies introduce new ways of transferring value and can provide cost-effective and efficient alternatives to traditional banking. In addition, the rise of fintech startups is driving innovation in the financial sector, forcing traditional institutions to adapt and innovate to maintain a competitive edge [67].

3.6. Cost Reduction and Scalability

Financial institutions benefit from the cost-effective and scalable nature of cloud computing [68]-[70]. It allows them to adapt to changing business needs without heavy upfront investments in infrastructure. In addition, technologies enable the automation of routine tasks, reducing operational costs and allowing financial institutions to allocate resources more efficiently [71].

3.7. Data Security and Privacy

As financial transactions increasingly occur in the digital realm, robust cybersecurity measures are essential to safeguard sensitive customer data and protect against cyber threats [72]-[75]. Technologies such as encryption and multi-factor authentication ensure the confidentiality and integrity of financial transactions, enhancing trust between financial institutions and customers [76]-[80].

3.8. Globalization and Cross-Border Transactions

Blockchain and distributed ledger technologies simplify and secure cross-border transactions, reducing costs and the time required for settlements [81]. In addition, Central bank digital currencies (CBDCs) and stablecoins [82] are emerging as potential solutions for facilitating cross-border transactions more efficiently than traditional methods.

3.9. Adaptation to Changing Consumer Expectations

Consumers increasingly prefer digital channels for banking and financial interactions [83]. Financial service sector technologies cater to these changing preferences, ensuring that institutions remain relevant and accessible.

In a nutshell, the compelling need for financial service sector technologies arises from a desire to address operational challenges, meet evolving customer expectations, comply with regulations, and stay competitive in an increasingly digital and interconnected world. The strategic adoption of these technologies is essential for financial institutions to navigate the complex and dynamic landscape of modern finance successfully.

4. Security and privacy issues in financial service sector technologies

Security and privacy are paramount considerations in the financial service sector, given the sensitivity and confidentiality of financial data [84], [85]. As the industry undergoes rapid technological advancements, numerous security and privacy issues emerge, necessitating robust measures to protect against threats and uphold the trust of customers. The following sub-sections extensively discuss these security and privacy issues.

4.1. Data Breaches and Unauthorized Access

Financial institutions store vast amounts of sensitive customer information. Data breaches and unauthorized access can lead to the compromise of personal and financial data, resulting in identity theft, fraud, and financial loss. Data breaches and unauthorized access represent grave concerns in the financial sector, posing serious threats to the confidentiality and integrity of sensitive information [86]-[90]. Financial institutions, holding vast amounts of personal and financial data, are prime targets for malicious actors seeking to exploit vulnerabilities for financial gain or identity theft. Data breaches, whether resulting from sophisticated cyber attacks or internal lapses, can have severe consequences, eroding customer trust, incurring financial losses, and exposing individuals to fraud. Unauthorized access, whether through

compromised credentials or system vulnerabilities, underscores the critical importance of robust security measures, including encryption, multi-factor authentication, and continuous monitoring, to fortify financial systems against unauthorized intrusions [91]-[94]. As the financial industry navigates an increasingly digital landscape, addressing these challenges requires a holistic approach to cybersecurity and vigilant efforts to stay ahead of evolving threats.

Encryption, secure access controls, and multi-factor authentication are crucial in preventing unauthorized access. Regular security audits and penetration testing help identify vulnerabilities.

4.2. Insider Threats

Malicious or negligent actions by internal employees pose a significant risk. Insiders may intentionally or unintentionally compromise data integrity, confidentiality, or availability. Insider threats present a significant risk to the security and integrity of the financial sector, as employees or trusted individuals with privileged access may intentionally or inadvertently compromise sensitive information [95]-[99]. Whether motivated by financial gain, disgruntlement, or unwittingly falling victim to social engineering tactics, insiders can pose a formidable challenge to the confidentiality of financial data. The potential impact ranges from unauthorized access and data manipulation to fraud and intellectual property theft. Mitigating insider threats necessitates a combination of robust access controls, continuous monitoring of user activities, and comprehensive employee training programs to foster awareness about security risks [100], [101]. Striking a balance between enabling legitimate access for employees and safeguarding against potential threats requires ongoing efforts to enhance organizational security postures and maintain a vigilant and proactive stance against insider risks in the financial sector.

Implementing strict access controls, monitoring employee activities, and conducting periodic security training and awareness programs help mitigate the risk of insider threats.

4.3. Phishing and Social Engineering Attacks

Cybercriminals often use phishing emails, social engineering, and other deceptive tactics to trick individuals into divulging sensitive information such as login credentials or account details. Phishing and social engineering attacks stand as pervasive threats in the financial sector, exploiting human vulnerabilities to gain unauthorized access to sensitive information [102]-[104]. In these sophisticated schemes, malicious actors employ deceptive emails, messages, or phone calls to trick individuals into disclosing confidential financial details or login credentials. Financial institutions are particularly susceptible, given the value of the data they handle. Phishing attacks can lead to unauthorized fund transfers, identity theft, and compromise of customer accounts. Combatting these threats requires a multi-faceted approach, encompassing user education, advanced email filtering systems, and continuous monitoring to detect and thwart phishing attempts [105]-[109]. As financial services increasingly rely on digital channels, the industry's ability to effectively thwart phishing and social engineering attacks becomes paramount in preserving the trust and security of both institutions and their customers.

Employee training to recognize phishing attempts, email filtering systems, and the implementation of two-factor authentication are essential in combating these threats.

4.4. Advanced Persistent Threats (APTs)

APTs involve prolonged and targeted attacks by sophisticated adversaries aiming to gain unauthorized access and maintain a persistent presence within a network. These attacks pose a significant and evolving threat to the financial services sector, characterized by highly sophisticated and targeted cyberattacks that aim to compromise sensitive information and systems over an extended period [110]-[114]. Figure 9 shows a typical lifecycle for APTs. Adversaries behind APTs often employ advanced techniques, including social engineering, spear-phishing, and zero-day exploits, to gain unauthorized access to financial institutions' networks.

Once inside, APT actors stealthily navigate through the infrastructure, maintaining persistence to exfiltrate valuable data such as customer information, financial transactions, and intellectual property [115]-[118]. The financial sector's attractiveness stems from the abundance of valuable assets and the potential for substantial financial gain. As a result, organizations in this sector must continually enhance their cybersecurity measures, adopt advanced threat detection technologies [119], and promote a robust security culture to mitigate the persistent and ever-evolving threat landscape posed by APTs.

Figure 9 APT lifecycle

Regular threat intelligence updates, intrusion detection systems, and network segmentation help detect and respond to APTs. Implementing a zero-trust security model [120] minimizes the potential impact of compromised systems.

4.5. Regulatory Compliance and Data Protection Laws

Financial institutions must comply with various regulations and data protection laws, such as GDPR, CCPA, and others, which mandate stringent requirements for the protection of customer data. According to [121], the financial services sector operates within a stringent regulatory framework, with a primary focus on regulatory compliance and data protection laws to safeguard sensitive information and maintain the integrity of financial transactions. Institutions in this sector must adhere to a complex web of regulations, including but not limited to the Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act (GLBA), and the General Data Protection Regulation (GDPR). These regulations dictate stringent requirements for the secure handling, storage, and transmission of customer data, imposing fines and penalties for non-compliance [122], [123]. The overarching goal is to ensure the confidentiality, integrity, and availability of financial data, protect consumers' privacy, and foster trust in the financial system. Financial service providers invest heavily in robust cyber-security measures, data encryption, and comprehensive compliance programs to meet these regulatory demands and uphold the highest standards of data protection in an ever-evolving digital landscape.

Implementing robust data governance frameworks, conducting regular compliance audits, and staying abreast of evolving regulations are crucial for maintaining compliance.

4.6. Cloud Security Risks

The adoption of cloud computing introduces new security challenges, including data breaches, misconfigurations, and the potential for unauthorized access to sensitive financial data. As explained in [124],The financial services sector faces notable challenges and risks in adopting cloud computing, primarily related to cloud security. While the cloud offers scalability and cost-efficiency, concerns arise regarding the confidentiality and integrity of sensitive financial data stored and processed in cloud environments. Key risks include data breaches, unauthorized access, and the potential

for service disruptions, all of which could lead to financial losses and reputational damage [125]-[129]. Moreover, regulatory compliance complexities add an additional layer of challenge, as financial institutions must ensure that their cloud service providers meet stringent security and privacy standards. Mitigating these risks requires robust encryption, identity and access management controls, continuous monitoring, and a thorough understanding of shared responsibility models between financial organizations and their cloud providers to foster a secure and compliant cloud computing environment.

Encryption of data in transit and at rest, strict access controls, and regular security assessments of cloud infrastructure help mitigate cloud security risks. Choosing reputable cloud service providers with strong security practices is essential.

4.7. Mobile Security Concerns

Mobile banking and financial apps are vulnerable to security threats such as malware, insecure connections, and device theft, potentially leading to unauthorized access to financial accounts. According to [130], mobile security concerns in the financial services sector have become paramount as the reliance on mobile devices for banking and financial transactions continues to grow. The sector faces the constant threat of mobile malware, phishing attacks, and device theft, all of which can lead to unauthorized access to sensitive financial information [131]-[133]. The proliferation of mobile banking apps introduces vulnerabilities that malicious actors may exploit, requiring financial institutions to implement robust authentication mechanisms, secure coding practices, and regular security updates for their mobile applications. Additionally, the diverse array of mobile devices and operating systems poses a challenge for ensuring uniform security standards. Financial organizations must prioritize user education on secure mobile practices, enforce strong encryption protocols, and leverage biometric authentication methods to address these mobile security concerns effectively and safeguard their customers' financial assets and information [134]-[138].

Implementing secure coding practices for mobile apps, using secure communication protocols, and enforcing strong authentication measures enhance mobile security. Regular updates and patches are crucial for addressing vulnerabilities.

4.8. Supply Chain Risks

Financial institutions rely on various third-party vendors and service providers, introducing supply chain risks. Compromises in the security of these vendors can have a cascading effect on the financial institution. These risks represent a critical concern as organizations increasingly rely on interconnected and globalized networks of vendors, partners, and service providers. The complex supply chain ecosystem in this sector introduces vulnerabilities ranging from third-party service disruptions to cyber threats and regulatory compliance issues [139]-[141]. Financial institutions often engage with multiple vendors for services like cloud computing, data processing, and cybersecurity, creating a broader attack surface. Compromises in the security posture of any link in the supply chain can have cascading effects, potentially leading to data breaches, financial fraud, and reputational damage. Mitigating supply chain risks in the financial service sector requires thorough due diligence, continuous monitoring, and the establishment of robust contractual agreements that enforce stringent cybersecurity and compliance standards throughout the entire supply chain network.

Conducting thorough security assessments of third-party vendors, ensuring contractual agreements include security provisions, and monitoring vendor security practices are vital to managing supply chain risks.

4.9. Blockchain Security Challenges

While blockchain enhances security through decentralization and immutability, it introduces challenges such as smart contract vulnerabilities, consensus algorithm weaknesses, and the potential for 51% attacks in certain blockchain networks [142], [143]. This technology has gained traction in the financial services sector for its potential to enhance transparency and security, but it also presents unique challenges. One prominent concern is the immutability of data, as once a block is added to the chain, it cannot be altered, posing challenges in the event of errors or fraudulent transactions. Additionally, the decentralized nature of blockchain networks introduces security risks related to consensus mechanisms and smart contract vulnerabilities. While blockchain enhances data integrity, it does not eliminate the need for securing the underlying infrastructure, and the public nature of some blockchain networks can expose transaction details [144]-[147]. Financial institutions must navigate these challenges by implementing robust consensus algorithms, conducting thorough code audits for smart contracts, and developing interoperability standards [148] to ensure secure integration with existing systems while harnessing the transformative potential of blockchain technology.

Implementing secure coding practices for smart contracts, choosing consensus algorithms with proven security, and regularly auditing blockchain implementations help mitigate these challenges.

4.10. Data Residency and Cross-Border Data Transfers

Different jurisdictions have varying data protection and privacy laws, raising concerns about data residency and cross-border data transfers. Compliance with these laws is essential to avoid legal repercussions. According to [149], data residency and cross-border data transfers pose significant challenges for the financial services sector, where strict regulatory frameworks govern the storage and movement of sensitive financial information. Financial institutions often operate globally, necessitating the storage and transfer of customer data across borders. However, conflicting data protection laws and privacy regulations, such as the GDPR in Europe and various data localization requirements in other jurisdictions, complicate compliance efforts. Striking a balance between meeting these regulatory obligations and enabling seamless cross-border data flows is crucial [150], [151]. Financial organizations must implement robust data governance strategies, including encryption and secure data transfer protocols, while navigating the complexities of differing legal requirements to ensure the privacy and security of customer information across international boundaries. This involves establishing clear policies, conducting thorough risk assessments, and employing technical solutions to safeguard data in transit and at rest, ultimately building trust with customers and regulatory authorities.

Implementing data localization strategies, conducting thorough legal reviews, and ensuring that data transfer mechanisms comply with relevant regulations help address these issues.

In summary, addressing security and privacy issues in financial service sector technologies requires a multifaceted approach encompassing technological measures, employee training, regulatory compliance, and proactive risk management. Financial institutions must continually adapt their security postures to counter evolving threats and ensure the confidentiality, integrity, and availability of sensitive financial data.

5. Solutions to security and privacy issues in financial service sector

Addressing security and privacy issues in the financial service sector requires a comprehensive and multi-layered approach. The following are probable solutions that institutions can implement to mitigate and manage these challenges effectively.

5.1. Encryption and Data Masking

Institutions need to employ robust encryption mechanisms to protect data both in transit and at rest. Additionally, implement data masking techniques to anonymize sensitive information, ensuring that even within the organization, only authorized personnel have access to the complete dataset. As explained in [153], encryption and data masking play pivotal roles in fortifying the security posture of the financial services sector by safeguarding sensitive information throughout its lifecycle. Encryption involves the use of algorithms to convert data into unreadable formats, rendering it inaccessible to unauthorized parties without the appropriate decryption keys. This technology ensures the confidentiality and integrity of financial data, especially during storage and transmission [154]-[158]. Data masking, on the other hand, involves disguising original data with fictional or pseudonymous values, enabling organizations to use realistic yet anonymized information for non-production purposes without compromising sensitive details. Both encryption and data masking are critical tools in compliance with data protection regulations, such as GDPR and GLBA, helping financial institutions mitigate the risk of data breaches, unauthorized access, and insider threats while maintaining the necessary functionality and usability of the data for legitimate business purposes.

5.2. Multi-Factor Authentication (MFA)

Organizations need to implement MFA to add an extra layer of security beyond passwords. By requiring users to provide multiple forms of identification, such as passwords, biometrics, or one-time codes, institutions can significantly reduce the risk of unauthorized access. Figure 10 shows a typical authentication scenario using MFA. It stands as a cornerstone of security measures in the financial services sector, enhancing identity verification beyond traditional password-based systems. Recognizing the vulnerabilities inherent in relying solely on passwords, MFA requires users to authenticate their identity through multiple verification methods, such as biometrics, smart cards, or one-time codes sent to mobile devices [159]-[163]. This layered approach significantly strengthens security, mitigating the risk of unauthorized access, phishing attacks, and credential theft. Financial institutions widely adopt MFA to meet regulatory requirements, including those outlined in PCI DSS and GDPR, and to bolster customer trust by providing an additional layer of defense against evolving cyber threats.

Figure 10 User authentication in MFA scenario

The dynamic nature of MFA not only protects sensitive financial data but also aligns with the industry's commitment to proactive cyber-security practices, fostering a robust defense against unauthorized access and potential financial fraud.

5.3. Biometric Authentication

There is need to utilize biometric authentication methods such as fingerprint recognition, facial recognition, or voice recognition to enhance user identity verification. Biometrics provide a more secure and convenient way to authenticate users. According to [164], biometric authentication has emerged as a cutting-edge security measure in the financial services sector, offering a highly secure and user-friendly method of verifying individuals' identities. As shown in Figure 11, utilizing unique biological traits such as fingerprints, facial recognition, or iris scans, biometric authentication enhances the accuracy and reliability of identity verification, mitigating the risks associated with traditional password-based systems.

Figure 11 Biometric Authentication

Financial institutions widely implement biometric solutions for access control, mobile banking, and transaction authorization, improving overall security and user experience [165]-[168]. The adoption of biometric authentication aligns with regulatory requirements, enhances fraud prevention, and fosters customer trust by providing a seamless and robust means of protecting sensitive financial information. As technology advances, the financial sector continues to leverage biometrics as a key element in its multifaceted approach to securing digital interactions and safeguarding against unauthorized access.

5.4. Regular Security Audits and Penetration Testing

Organizations must conduct regular security audits and penetration testing to identify vulnerabilities and weaknesses in systems and networks. This proactive approach helps institutions discover and address potential threats before they can be exploited, as shown in Figure 12. As explained in [169], regular security audits and penetration testing are integral components of the cyber-security strategy within the financial services sector.

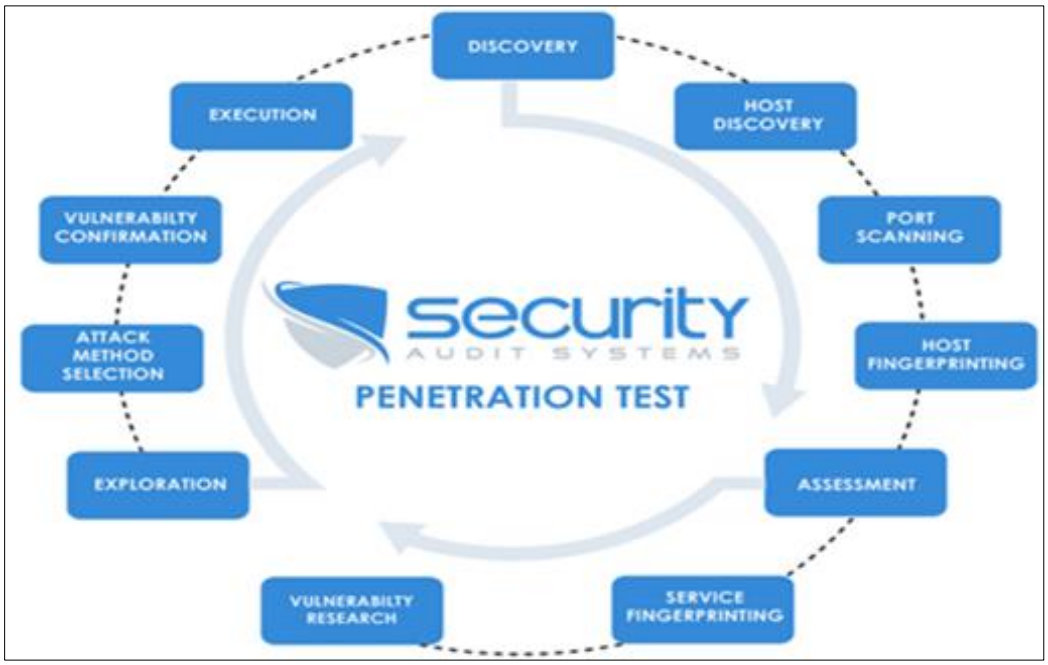

Figure 12 Activities in security audits and penetration testing

Given the ever-evolving nature of cyber threats, conducting systematic assessments of systems, networks, and applications is crucial for identifying vulnerabilities and weaknesses in the security infrastructure. Security audits, which involve comprehensive reviews of security policies, configurations, and controls, help financial institutions ensure compliance with industry regulations and best practices [170], [171]. Penetration testing takes the evaluation a step further by simulating real-world attacks to uncover exploitable vulnerabilities and assess the effectiveness of defenses. By routinely conducting these assessments, financial organizations can proactively address potential security gaps, fortify their defenses, and stay ahead of emerging threats, thereby enhancing the resilience of their systems and maintaining the integrity and confidentiality of sensitive financial data.

5.5. Employee Training and Awareness Programs

There is need to train employees on cyber-security best practices, including recognizing phishing attempts, practicing secure password management, and understanding the importance of data protection. Regular awareness programs help create a security-conscious culture within the organization [172]. These programs are pivotal in the financial services sector to build a robust human firewall against cyber threats. Recognizing that employees play a crucial role in maintaining the security posture of financial institutions, training programs focus on educating staff about cyber-security best practices, data protection policies, and the identification of social engineering tactics. These initiatives not only empower employees to make informed decisions but also cultivate a security-conscious culture within the organization. Given the evolving nature of cyber threats [173], continuous training is essential to keep employees abreast of the latest risks and mitigation strategies. By investing in comprehensive training and awareness programs, financial service providers can significantly reduce the likelihood of human errors, insider threats, and security breaches, ultimately bolstering the overall resilience of their cybersecurity defenses.

5.6. Endpoint Security Solutions

Implementation of robust endpoint security solutions can protect devices connected to the network. This includes antivirus software, firewalls, and intrusion detection systems to detect and prevent malicious activities on individual devices [174]. These solutions are paramount in the financial services sector to protect against a myriad of cyber threats targeting individual devices. Given the increasing sophistication of attacks, financial institutions deploy endpoint security solutions to safeguard endpoints such as computers, laptops, and mobile devices. These solutions typically include antivirus software, firewalls, intrusion detection and prevention systems, and device encryption tools. Endpoint security not only defends against malware, ransomware, and other malicious activities but also helps enforce security policies, monitor device activity, and respond to incidents in real-time [175]-[179]. With the growing trend of remote work and the reliance on mobile devices, robust endpoint security becomes critical for safeguarding sensitive financial data, ensuring compliance with regulations, and maintaining the trust of clients and stakeholders in the financial service sector.

5.7. Blockchain Security Best Practices

For institutions leveraging blockchain technology, they need to follow best practices for smart contract development, choose consensus algorithms with proven security, and regularly audit the blockchain network for vulnerabilities. Implementing private and permissioned blockchains can enhance control and security. According to [180], blockchain security best practices are imperative in the financial services sector to ensure the integrity and confidentiality of transactions within decentralized networks. Utilizing cryptographic techniques, financial institutions should implement robust consensus mechanisms, such as proof-of-work or proof-of-stake, to secure the blockchain against malicious actors seeking to manipulate or compromise the distributed ledger [181]-[183]. Additionally, the implementation of smart contracts should undergo rigorous code audits to identify and mitigate vulnerabilities. Institutions must adopt a principle of least privilege for network participants and deploy encryption techniques to protect data both at rest and in transit [184], [185]. Continuous monitoring, regular updates to address emerging threats, and collaboration with industry peers for information sharing are essential components of a comprehensive blockchain security strategy. Adhering to these best practices not only fortifies the financial service sector against potential attacks but also instills trust in the reliability and security of blockchain technology for financial transactions and data management.

5.8. Cloud Security Measures

When utilizing cloud services, organizations need to adopt a shared responsibility model, ensuring both the cloud service provider and the financial institution take appropriate security measures. As shown in Figure 13, organizations use encryption, access controls, and regularly audit configurations to secure cloud-based assets. These measures are paramount in the financial services sector to address the unique challenges and opportunities presented by cloud computing.

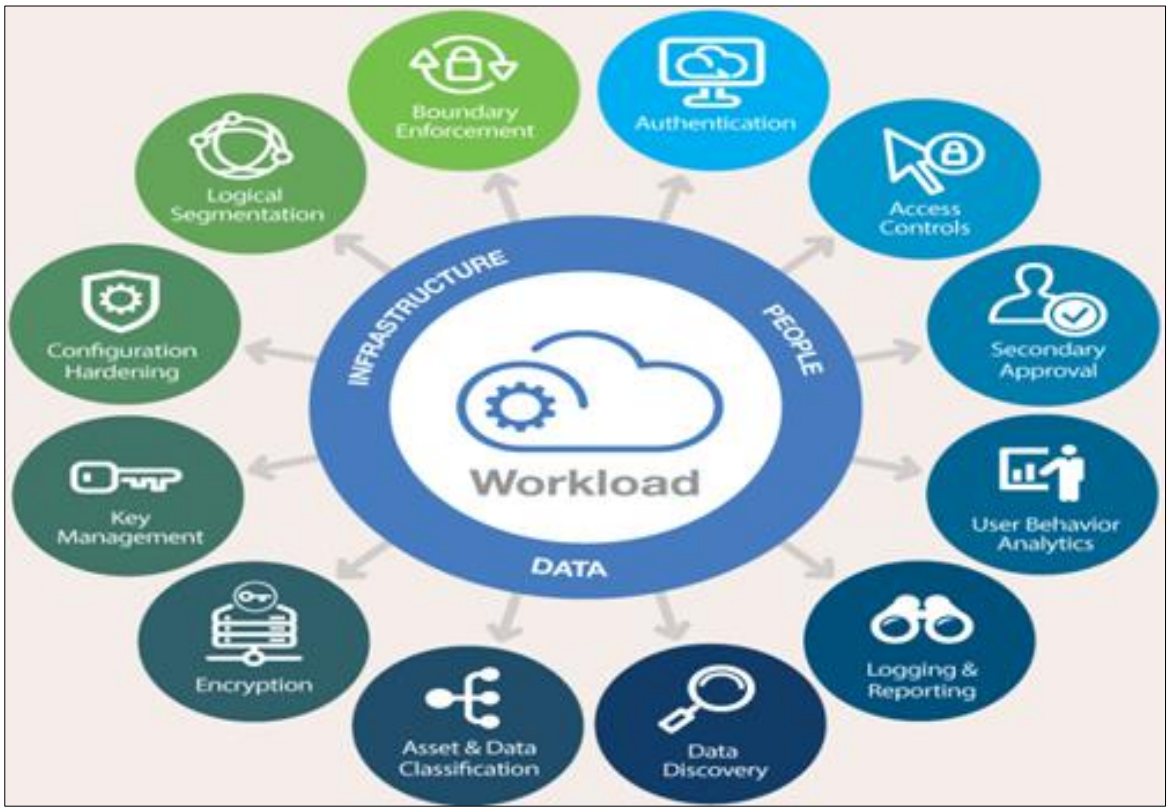

Figure 13 Cloud Security Measures

Financial institutions leverage robust encryption protocols to protect sensitive data both in transit and at rest, ensuring confidentiality and integrity. Access controls, identity and access management systems, and multifactor authentication are implemented to regulate and authenticate user access, reducing the risk of unauthorized entry [186]-[191]. Regular security audits, vulnerability assessments, and penetration testing are conducted to identify and remediate potential weaknesses in the cloud infrastructure. Compliance with industry regulations such as PCI DSS, GDPR, and regional data protection laws is ensured through comprehensive governance frameworks. Moreover, financial organizations often choose reputable and compliant cloud service providers, relying on their expertise to maintain a secure and resilient

cloud environment. These collective measures contribute to building a strong defense against cyber threats, ensuring the stability and trustworthiness of financial systems operating in the cloud.

5.9. Regulatory Compliance and Governance

There is need for organizations to stay abreast of regulatory changes and ensure compliance with data protection laws and financial regulations. Establish robust governance frameworks that include regular risk assessments, policy reviews, and compliance audits. As explained in [192], regulatory compliance and governance form the bedrock of the financial services sector, where adherence to a complex web of regulations is crucial for maintaining integrity, transparency, and trust. Financial institutions operate within a tightly regulated environment, governed by standards such as Basel III, Dodd-Frank Act, and Anti-Money Laundering (AML) laws. Robust governance frameworks are essential to ensure internal policies align with external regulations, fostering accountability and risk management. Compliance efforts extend to data protection laws like GDPR and cybersecurity standards, necessitating continuous monitoring, regular audits, and thorough documentation [193], [194]. The evolving regulatory landscape requires financial organizations to stay agile, adapt swiftly to changes, and demonstrate a commitment to ethical business practices, ultimately safeguarding the stability of the financial system and maintaining the confidence of stakeholders and customers.

5.10. Incident Response Plans

Organizations need to develop and regularly update incident response plans to swiftly and effectively respond to security incidents. This includes procedures for identifying, containing, eradicating, recovering, and learning from security breaches [195]. These plans are critical components of the cyber-security strategy in the financial services sector, where the potential impact of security incidents can be severe. These plans outline systematic and coordinated approaches to detect, respond to, and recover from security breaches, minimizing the impact on operations and mitigating financial and reputational damage. Financial institutions develop detailed incident response playbooks that specify roles, responsibilities, and communication protocols during a security incident [196]. These plans typically involve rapid identification and containment of the incident, thorough forensic analysis, and collaboration with law enforcement if necessary. Regular testing and simulations ensure the effectiveness of the incident response plans, enabling organizations to adapt to evolving cyber threats and respond decisively to protect sensitive financial data, maintain regulatory compliance, and uphold customer trust.

5.11. Supply Chain Risk Management

Implementation of a robust supply chain risk management program, which includes thorough vendor assessments, security reviews, and ongoing monitoring [197]. Supply Chain Risk Management (SCRM) is a critical aspect of business strategy that involves identifying, assessing, and mitigating potential risks and disruptions within the supply chain. It encompasses a comprehensive approach to anticipate, manage, and respond to various uncertainties that can impact the production and distribution of goods or services. These risks may include natural disasters, geopolitical events, economic fluctuations, supplier disruptions, and technological failures. Effective SCRM involves implementing proactive measures such as diversifying suppliers, creating contingency plans, utilizing technology for real-time monitoring, and fostering collaboration with key stakeholders. By addressing vulnerabilities in the supply chain, organizations can enhance resilience, minimize disruptions, and ensure the continuity of operations, ultimately safeguarding their competitive advantage and maintaining customer satisfaction.

5.12. Continuous Monitoring and Threat Intelligence

There is need for the implementation of continuous monitoring systems to detect and respond to security threats in real-time. Stay informed about the latest threat intelligence to anticipate emerging risks and vulnerabilities. According to [198], these activities are integral components of the cyber-security strategy in the financial services sector, where the landscape of cyber threats is dynamic and sophisticated. Continuous monitoring involves real-time surveillance of networks, systems, and data to promptly detect and respond to potential security incidents. Simultaneously, threat intelligence involves the collection, analysis, and dissemination of information about cyber threats and vulnerabilities. Financial institutions leverage advanced tools and technologies to monitor network traffic, user activities, and system behavior, while also integrating threat intelligence feeds to stay informed about emerging threats. This proactive approach allows organizations to identify and mitigate potential risks before they escalate, ensuring the resilience of their cybersecurity defenses [199], compliance with regulations, and the protection of sensitive financial information from evolving and sophisticated cyber threats.

5.13. Data Residency Planning

Organizations have to develop strategies for data residency compliance, considering the legal and regulatory requirements of different jurisdictions. Implement measures such as data localization or the use of secure data transfer mechanisms to address cross-border data transfer concerns. As explained in [200], data residency planning in the financial services sector is a strategic imperative to navigate the complex regulatory landscape governing the storage and processing of sensitive financial information. Given the global nature of financial operations, institutions must carefully consider where data is stored to comply with data protection laws, privacy regulations, and specific mandates on data localization. This involves assessing the legal requirements and restrictions in various jurisdictions, understanding cross-border data transfer regulations, and implementing robust data management practices [201]. Developing a comprehensive data residency plan allows financial organizations to strike a balance between regulatory compliance, operational efficiency, and data security, ensuring that client information is handled in accordance with legal frameworks while maintaining the necessary flexibility to conduct international business operations effectively.

5.14. Privacy by Design

Incorporation of privacy considerations into the design and development of financial technologies from the outset is very crucial. This includes adopting privacy-enhancing technologies, conducting privacy impact assessments, and minimizing the collection of unnecessary personal information. According to [202], privacy by design is a crucial principle in the financial services sector, emphasizing the integration of privacy considerations into the development and implementation of systems, processes, and technologies from the outset. Figure 14 illustrates the 7 principles of privacy by design. This approach ensures that privacy measures are not merely add-ons but are inherent components of every stage in the lifecycle of financial products and services. Financial institutions adopting Privacy by Design focus on minimizing the collection and processing of personal data, implementing strong encryption and access controls, and incorporating privacy-enhancing technologies [203]-[205]. By embedding privacy into the design of their systems, financial organizations can proactively address regulatory requirements, enhance data protection, and build customer trust by prioritizing privacy as a fundamental element of their service offerings.

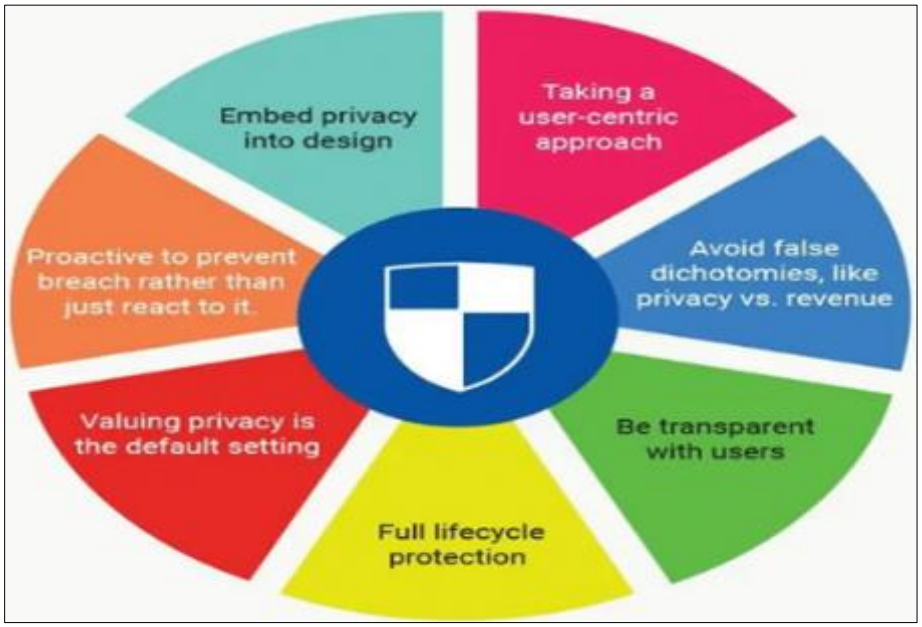

Figure 14 Principles of privacy by design

As shown in Figure 14, the first principle focuses on being proactive and preventing privacy-invasive events before they occur. The second principle ensures that privacy is the default setting, meaning that individuals' privacy is automatically protected without any user action. The third principle emphasizes embedding privacy into the design, rather than bolting it on as an afterthought. The fourth principle advocates for full functionality, stressing that privacy measures should not diminish the system's capabilities. The fifth principle promotes end-to-end security, safeguarding information throughout its lifecycle. The sixth principle involves visibility and transparency, ensuring that users are informed about privacy practices. Lastly, the seventh principle emphasizes respect for user privacy, striving to keep the individual in control of their personal information. Together, these principles form a comprehensive framework for building privacy into the foundation of systems and processes.

5.15. Collaboration with Regulatory Bodies

There is need to engage proactively with regulatory bodies and industry associations to stay informed about evolving security and privacy requirements. Collaborate with regulators to ensure that implemented security measures align with industry standards and expectations. As discussed in [206], collaboration with regulatory bodies is a cornerstone of governance and compliance in the financial services sector. Financial institutions actively engage with regulatory authorities to ensure adherence to a myriad of evolving regulations and standards governing the industry. This collaboration involves open communication, regular reporting, and constructive dialogue to address regulatory expectations and requirements. Financial organizations seek to stay ahead of regulatory changes by participating in consultations and providing feedback on proposed policies. This collaborative relationship not only helps financial institutions navigate the complex regulatory landscape but also demonstrates a commitment to transparency, accountability, and proactive compliance [207]. Such collaboration is essential for maintaining the stability and integrity of the financial system while fostering a regulatory environment that balances innovation with the protection of consumers and the overall financial market.

In summary, a holistic approach that combines technological solutions, employee training, regulatory compliance, and proactive risk management is essential for addressing security and privacy issues in the financial service sector. By adopting these extensive solutions, institutions can better safeguard sensitive information, maintain customer trust, and navigate the dynamic landscape of financial technologies securely.

6. Research gaps and future research directions

Research in security and privacy within the financial service sector technologies is essential for addressing evolving threats and ensuring the resilience of the industry. However, there are several research gaps and future directions that merit attention to enhance the security and privacy posture of financial technologies. Some of these research gaps and potential avenues for future research are discussed below.

6.1. Quantum-Safe Cryptography

Gap: With the advent of quantum computing, traditional cryptographic algorithms may become vulnerable [208]. Research is needed to develop and standardize quantum-safe cryptographic solutions to ensure the long-term security of financial systems.

Research Directions: Investigate quantum-resistant encryption algorithms, assess their feasibility in financial applications, and explore the integration of quantum-safe cryptography into existing financial infrastructure.

6.2. Privacy-Preserving Technologies

Gap: Preserving user privacy while still extracting valuable insights from financial data is challenging [209]-[211]. Current technologies often struggle to strike the right balance between data utility and individual privacy.

Research Directions: Explore advanced privacy-preserving techniques, including homomorphic encryption, secure multi-party computation, and differential privacy. Develop methods that allow financial institutions to derive meaningful insights without compromising individual privacy.

6.3. Explainability and Transparency in AI Models

Gap: The lack of explainability in AI and machine learning models used in financial decision-making raises concerns about transparency and accountability [212].

Research Directions: Investigate techniques for making AI models more interpretable and understandable, especially in critical financial applications. Develop standards and frameworks for explaining complex algorithms to regulators, auditors, and end-users.

6.4. Security of Decentralized Finance (DeFi)

Gap: The rise of DeFi introduces new challenges related to smart contract vulnerabilities, decentralized governance, and the security of blockchain-based financial platforms [213].

Research Directions: Explore novel security models for decentralized financial systems, identify and address vulnerabilities in smart contracts, and develop governance mechanisms that balance decentralization with security and compliance.

6.5. Adversarial Machine Learning in Fraud Detection

Gap: Adversarial attacks against machine learning models used for fraud detection pose a significant threat [214]. Attackers can manipulate training data or inputs to evade detection.

Research Directions: Investigate robust machine learning models that can withstand adversarial attacks in financial fraud detection. Develop techniques for detecting and mitigating adversarial attempts to manipulate financial data.

6.6. Blockchain Scalability and Security

Gap: As blockchain adoption increases, scalability remains a challenge [215]. Additionally, ensuring security in scalable blockchain networks is a complex problem.

Research Directions: Explore innovative solutions for blockchain scalability, such as sharding and layer 2 solutions. Conduct research on the security implications of these scalability solutions and propose methods to enhance the resilience of large-scale blockchain networks.

6.7. Regulatory Technology (RegTech)

Gap: RegTech solutions are essential for ensuring compliance with financial regulations, but there is a need for more standardized approaches and interoperability.

Research Directions: Investigate the development of standardized APIs and frameworks for RegTech solutions. Explore ways to enhance the interoperability of RegTech platforms to facilitate seamless integration with diverse financial systems.

6.8. Behavioral Biometrics for User Authentication

Gap: Traditional authentication methods may be vulnerable to attacks, and there is a need for more secure and user-friendly alternatives.

Research Directions: Investigate the feasibility and security of behavioral biometrics, such as keystroke dynamics and mouse movement, for user authentication in financial applications. Examine the usability and resilience of these methods under different scenarios.

6.9. Cross-Border Data Governance

Gap: With global financial transactions, there is a lack of standardized cross-border data governance frameworks [216], leading to challenges in complying with diverse data protection regulations.

Research Directions: Research and propose frameworks for cross-border data governance that align with various data protection laws. Explore technological solutions that facilitate compliant cross-border data transfers in the financial sector.

6.10. Societal and Ethical Implications

Gap: The societal and ethical implications of financial technologies, especially concerning bias in algorithms and access to financial services, need deeper exploration.

Research Directions: Investigate the ethical considerations surrounding financial technologies, including bias in algorithms, discriminatory impacts, and implications for financial inclusion. Develop frameworks for ethical AI deployment in the financial service sector.

6.11. Human-Centric Security

Gap: The human factor is often a weak link in security. There is a need for research on human-centric security measures that consider user behavior, cognition, and decision-making.

Research Directions: Explore methods for integrating human-centric security measures, such as user education, psychological insights, and usability considerations, into the design of financial technologies. Investigate how human factors influence the effectiveness of security measures.

6.12. Secure Tokenization and Token Standards

Gap: Tokenization is widely used for enhancing security in payment systems [127], but there is a lack of standardized tokenization approaches and token standards.

Research Directions: Research and propose standardized tokenization approaches for secure financial transactions. Investigate the development of token standards that facilitate interoperability and security across diverse financial systems.

Therefore, addressing these research gaps and pursuing future research directions will contribute to strengthening the security and privacy foundations of financial service sector technologies. Researchers, practitioners, and policymakers play a crucial role in collaboratively advancing knowledge and developing practical solutions to ensure the continued trustworthiness of financial systems in an ever-evolving technological landscape.

7. Conclusion

This paper has delved into the intricate realm of security and privacy research gaps within the financial service sector technologies, identifying critical challenges that demand attention from the research community, industry stakeholders, and policymakers alike. As financial technologies evolve and permeate various aspects of the industry, it is imperative to address these gaps to fortify the security and privacy foundations upon which the sector relies. The identified research gaps underscore the need for innovative and adaptive solutions to counter emerging threats. From quantum-resistant cryptography to the security implications of decentralized finance (DeFi), the gaps illuminate areas where current understanding and practices may fall short in providing robust protection for sensitive financial data. Moreover, the societal and ethical implications of financial technologies call for a deeper exploration, emphasizing the importance of aligning technological advancements with ethical considerations and societal well-being. The outlined future research directions serve as a roadmap for scholars and practitioners seeking to contribute to the ongoing discourse on security and privacy in the financial service sector. Quantum-safe cryptographic solutions, privacy-preserving technologies, and advancements in explainability of AI models are among the key areas that hold promise for shaping the future landscape of secure financial technologies. The intersection of blockchain scalability and security, along with the human-centric aspects of security, presents exciting opportunities for researchers to bridge gaps and advance our understanding of how these technologies can be harnessed securely. As the financial industry continues to navigate cross-border challenges and compliance with data protection laws, innovative solutions and frameworks for governance become paramount research priorities. The research gaps and future directions outlined in this paper collectively emphasize the need for a holistic and interdisciplinary approach. Collaboration between researchers, industry experts, and regulators is crucial to developing effective and sustainable solutions. By addressing these gaps and pursuing the identified research directions, we can cultivate a more resilient and trustworthy financial service sector, ensuring that technological advancements go hand-in-hand with robust security measures and a steadfast commitment to protecting user privacy. As we look ahead, this paper aims to inspire a collective effort to fortify the digital foundations of finance and uphold the integrity and confidentiality of financial transactions in an increasingly interconnected world.

Compliance with ethical standards

Disclosure of conflict of interest

The author has no any conflict of interest.

References

[1] George AS. Securing the future of finance: how AI, Blockchain, and machine learning safeguard emerging Neobank technology against evolving cyber threats. Partners Universal Innovative Research Publication. 2023 Oct 11, 1(1):54-66.

[2] Khan HU, Malik MZ, Nazir S, Khan F. Utilizing bio metric system for enhancing cyber security in banking sector: a systematic analysis. IEEE Access. 2023 Jul 25.

[3] Allahrakha N. Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age. Legal Issues in the Digital Age. 2023 Jul 24, 4(2):78-121.

[4] Ahmad AY, Tiwari A, Nayeem MA, Biswal BK, Satapathy DP, Kulshreshtha K, Bordoloi D. Artificial Intelligence Perspective Framework of the Smart Finance and Accounting Management Model. International Journal of Intelligent Systems and Applications in Engineering. 2024, 12(4s):586-94.

[5] Rane N, Choudhary S, Rane J. Enhanced product design and development using Artificial Intelligence (AI), Virtual Reality (VR), Augmented Reality (AR), 4D/5D/6D Printing, Internet of Things (IoT), and blockchain: A review. Virtual Reality (VR), Augmented Reality (AR) D. 2023 Nov 25, 4.

[6] 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.

[7] Wang Y, Su Z, Guo S, Dai M, Luan TH, Liu Y. A survey on digital twins: architecture, enabling technologies, security and privacy, and future prospects. IEEE Internet of Things Journal. 2023 Apr 3.

[8] Sadaf M, Iqbal Z, Javed AR, Saba I, Krichen M, Majeed S, Raza A. Connected and automated vehicles: Infrastructure, applications, security, critical challenges, and future aspects. Technologies. 2023 Sep 4, 11(5):117.

[9] Chernov A, Chernova V. Global blockchain technology market analysis-current situations and forecast. Economic and Social Development: Book of Proceedings. 2018 Sep 26:143-52.

[10] Lăzăroiu G, Bogdan M, Geamănu M, Hurloiu L, Luminița L, Ștefănescu R. Artificial intelligence algorithms and cloud computing technologies in blockchain-based fintech management. Oeconomia Copernicana. 2023 Sep 30, 14(3):707-30.

[11] 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.

[12] Gan Q, Lau RY. Trust in a 'trust-free'system: Blockchain acceptance in the banking and finance sector. Technological Forecasting and Social Change. 2024 Feb 1, 199:123050.

[13] Prakash N, Solanki S, Gabriel EE, Bangari M. Blockchain Technology–Revamping the Indian Financial Sector Landscape and Roadblocks Ahead. PalArch's Journal of Archaeology of Egypt/Egyptology. 2020 Nov 29, 17(6):1084-92.

[14] Kołodziej M. Development factors of blockchain technology within banking sector. InContemporary Trends and Challenges in Finance: Proceedings from the 6th Wroclaw International Conference in Finance 2021 (pp. 125-138). Springer International Publishing.

[15] Ali O, Ally M, Dwivedi Y. The state of play of blockchain technology in the financial services sector: A systematic literature review. International Journal of Information Management. 2020 Oct 1, 54:102199.

[16] 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.

[17] Irfan M, Elmogy M, El-Sappagh S, editors. The impact of AI innovation on financial sectors in the era of industry 5.0. IGI Global, 2023 Sep 5.

[18] Pattnaik D, Ray S, Raman R. Applications of artificial intelligence and machine learning in the financial services industry: A bibliometric review. Heliyon. 2023 Dec 13.

[19] Ahmadi S. A Comprehensive Study on Integration of Big Data and AI in Financial Industry and Its Effect on Present and Future Opportunities. International Journal of Current Science Research and Review. 2024 Jan 6, 7(01).

[20] Andronie M, Iatagan M, Uță C, Hurloiu I, Dijmărescu A, Dijmărescu I. Big data management algorithms in artificial Internet of Things-based fintech. Oeconomia Copernicana. 2023, 14(3):769-93.

[21] Yenurkar GK, Mal S, Nyangaresi VO, Hedau A, Hatwar P, Rajurkar S, Khobragade J. Multifactor data analysis to forecast an individual's severity over novel COVID-19 pandemic using extreme gradient boosting and random forest classifier algorithms. Engineering Reports. 2023:e12678.

[22] Kaur K, Kumar Y, Kaur S. Artificial Intelligence and Machine Learning in Financial Services to Improve the Business System. InComputational Intelligence for Modern Business Systems: Emerging Applications and Strategies 2023 Nov 4 (pp. 3-30). Singapore: Springer Nature Singapore.

[23] Go EJ, Moon J, Kim J. Analysis of the current and future of the artificial intelligence in financial industry with big data techniques. Global Business & Finance Review (GBFR). 2020, 25(1):102-17.

[24] 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.

[25] Buyya R, Ilager S, Arroba P. Energy-efficiency and sustainability in new generation cloud computing: A vision and directions for integrated management of data centre resources and workloads. Software: Practice and Experience. 2024 Jan, 54(1):24-38.

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

[27] Vivek D, Rakesh S, Walimbe RS, Mohanty A. The Role of CLOUD in FinTech and RegTech. Annals of the University Dunarea de Jos of Galati: Fascicle: I, Economics & Applied Informatics. 2020 Oct 1, 26(3).

[28] Horian K, Gorian E. Information security ensuring in the financial sector as part of the implementation of the National Program “Data Economy Russia 2024”. InInternational Scientific Conference" Far East Con"(ISCFEC 2020) 2020 Mar 17 (pp. 635-644). Atlantis Press.

[29] Swathi G, Pahuja A. FinTech Frontiers: Cloud Computing and Artificial Intelligence Applications for Intelligent Finance Investment and Blockchain in the Financial Sector. International Journal of Intelligent Systems and Applications in Engineering. 2024, 12(4s):654-9.

[30] 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.

[31] Thoti KK. Exploring the employees’ behavioral intention towards disruptive technologies: A study in Malaysia. Human Resources Management and Services. 2024 Jan 16, 6(1).

[32] Chu AB. Mobile technology and financial inclusion. InHandbook of Blockchain, Digital Finance, and Inclusion, Volume 1 2018 Jan 1 (pp. 131-144). Academic Press.

[33] Ünvan Ya, Ergenç C. How the Rise of Digital Banking is Disrupting Traditional Financial Services Opportunities and Challenges For Banks and Customers. Sosyal Bilimlerde Akademik Analiz ve Yorumlar. 2023:51.

[34] Saeed S, Altamimi SA, Alkayyal NA, Alshehri E, Alabbad DA. Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors. 2023 Jul 25, 23(15):6666.

[35] 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.

[36] Lee JY. A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. Business Horizons. 2019 Nov 1, 62(6):773-84.

[37] Ghosh A, Gupta S, Dua A, Kumar N. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. Journal of Network and Computer Applications. 2020 Aug 1, 163:102635.

[38] Ulrich K, Guaita Martínez JM, Carracedo P, Soriano DR. Blockchain technology-based crypto assets: new insights into the evolution of the understanding of digital entrepreneurship. Management Decision. 2023 Aug 11.

[39] Far SB, Rad AI, Asaar MR. Blockchain and its derived technologies shape the future generation of digital businesses: a focus on decentralized finance and the Metaverse. Data Science and Management. 2023 Sep 1, 6(3):183-97.

[40] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[41] Teichmann F, Boticiu S, Sergi BS. RegTech–Potential benefits and challenges for businesses. Technology in Society. 2023 Feb 1, 72:102150.

[42] Campbell-Verduyn M, Lenglet M. Imaginary failure: RegTech in finance. New Political Economy. 2023 May 4, 28(3):468-82.

[43] Firmansyah B, Arman AA. Generic Solution Architecture Design of Regulatory Technology (RegTech). Indonesian Journal of Electrical Engineering and Informatics (IJEEI). 2023 Jun 15, 11(2).

[44] McCarthy J. The regulation of RegTech and SupTech in finance: ensuring consistency in principle and in practice. Journal of Financial Regulation and Compliance. 2023 Mar 29, 31(2):186-99.

[45] 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.

[46] Mishra S. Exploring the Impact of AI-Based Cyber Security Financial Sector Management. Applied Sciences. 2023 May 10, 13(10):5875.

[47] Efijemue O, Obunadike C, Taiwo E, Kizor S, Olisah S, Odooh C, Ejimofor I. Cybersecurity Strategies for Safeguarding Customers Data and Preventing Financial Fraud in the United States Financial Sectors. International Journal of Soft Computing., 14(3):10-5121.

[48] Jasur A. Cybersecurity and risk management in the financial sector. International Bulletin of Young Scientist. 2023 Jul 30, 1(1).

[49] Kuzior A, Yarovenko H, Brożek P, Sidelnyk N, Boyko A, Vasilyeva T. Company Cybersecurity System: Assessment, Risks and Expectations. Production Engineering Archives. 2023, 29(4):379-92.

[50] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014, 16(5):137-44.

[51] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[52] Edu AS. Positioning big data analytics capabilities towards financial service agility. Aslib Journal of Information Management. 2022 Jun 10, 74(4):569-88.

[53] Ionescu SA, Diaconita V. Transforming Financial Decision-Making: The Interplay of AI, Cloud Computing and Advanced Data Management Technologies. International Journal of Computers Communications & Control. 2023 Oct 30, 18(6).

[54] Rosário AT, Dias JC. How has data-driven marketing evolved: Challenges and opportunities with emerging technologies. International Journal of Information Management Data Insights. 2023 Nov 1, 3(2):100203.

[55] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec, 39(10):e13126.

[56] Dutta S, Pramanik HS, Datta S, Kirtania M. Imperatives, Trends and Dynamics of Digital Transformation as Banks Adopt Technology and Intelligent Systems. InIntelligent Systems in Digital Transformation: Theory and Applications 2022 Nov 15 (pp. 323-348). Cham: Springer International Publishing.

[57] Elliot EA, Hinson RE, Annan A, Eppler MJ. Digital Channels Catalysing Businesses in Fast-Expanding African Markets. InDigital Service Delivery in Africa: Platforms and Practices 2022 Feb 7 (pp. 17-51). Cham: Springer International Publishing.

[58] Aziz LA, Andriansyah Y. The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. Reviews of Contemporary Business Analytics. 2023 Aug 5, 6(1):110-32.

[59] Kute DV, Pradhan B, Shukla N, Alamri A. Deep learning and explainable artificial intelligence techniques applied for detecting money laundering–a critical review. IEEE access. 2021 Jun 4, 9:82300-17.

[60] Ghrabat MJ, Hussien ZA, Khalefa MS, Abduljabba ZA, Nyangaresi VO, Al Sibahee MA, Abood EW. Fully automated model on breast cancer classification using deep learning classifiers. Indonesian Journal of Electrical Engineering and Computer Science. 2022 Oct, 28(1):183-91.

[61] Freij Å. Using technology to support financial services regulatory compliance: current applications and future prospects of regtech. Journal of Investment Compliance. 2020 Dec 15, 21(2/3):181-90.

[62] Grassi L, Lanfranchi D. RegTech in public and private sectors: the nexus between data, technology and regulation. Journal of Industrial and Business Economics. 2022 Sep, 49(3):441-79.

[63] Mhlanga D. Block chain for digital financial inclusion towards reduced inequalities. InFinTech and Artificial Intelligence for Sustainable Development: The Role of Smart Technologies in Achieving Development Goals 2023 Jul 25 (pp. 263-290). Cham: Springer Nature Switzerland.

[64] Popescu AD. Empowering financial inclusion through fintech. Social Sciences and Education Research Review. 2019, 6(2):198-215.

[65] 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.

[66] Rane N, Choudhary S, Rane J. Blockchain and Artificial Intelligence (AI) integration for revolutionizing security and transparency in finance. Available at SSRN 4644253. 2023 Nov 17.

[67] Caragea D, Cojoianu T, Dobri M, Hoepner A, Peia O, Romelli D. Competition and innovation in the financial sector: Evidence from the rise of FinTech start-ups. Journal of Financial Services Research. 2023 Aug 10:1-38.

[68] Yenugula M, Sahoo S, Goswami S. Cloud computing for sustainable development: An analysis of environmental, economic and social benefits. Journal of future sustainability. 2024, 4(1):59-66.

[69] Rashmi M, William P, Yogeesh N, Girija DK. Blockchain-based cloud storage using secure and decentralised solution. InInternational Conference on Data Analytics and Insights 2023 May 11 (pp. 269-279). Singapore: Springer Nature Singapore.

[70] Zhang H, Ma J, Qiu Z, Yao J, Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Multi-GPU Parallel Pipeline Rendering with Splitting Frame. InComputer Graphics International Conference 2023 Aug 28 (pp. 223-235). Cham: Springer Nature Switzerland.

[71] Khatri MR. Integration of natural language processing, self-service platforms, predictive maintenance, and prescriptive analytics for cost reduction, personalization, and real-time insights customer service and operational efficiency. International Journal of Information and Cybersecurity. 2023 Sep 2, 7(9):1-30.

[72] Kasowaki L, Ali K. Cyber Hygiene: Safeguarding Your Data in a Connected World. EasyChair, 2024 Jan 6.

[73] Milson S, Tabib A. Cyber Resilience Blueprint: Fortifying Against Modern Threats. EasyChair, 2024 Jan 6.

[74] Tariq E, Akour I, Al-Shanableh N, Alquqa E, Alzboun N, Al-Hawary S, Alshurideh M. How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks. International Journal of Data and Network Science. 2024, 8(1):69-76.

[75] Nyangaresi VO, Ogundoyin SO. Certificate based authentication scheme for smart homes. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[76] Ali G, Dida MA, Elikana Sam A. A secure and efficient multi-factor authentication algorithm for mobile money applications. Future Internet. 2021 Nov 25, 13(12):299.

[77] Prabakaran D, Ramachandran S. Multi-factor authentication for secured financial transactions in cloud environment. CMC-Computers, Materials & Continua. 2022 Jan 1, 70(1):1781-98.

[78] Obaidat M, Brown J, Obeidat S, Rawashdeh M. A hybrid dynamic encryption scheme for multi-factor verification: a novel paradigm for remote authentication. Sensors. 2020 Jul 29, 20(15):4212.

[79] Ahmad MO, Tripathi G, Siddiqui F, Alam MA, Ahad MA, Akhtar MM, Casalino G. BAuth-ZKP—A Blockchain-Based Multi-Factor Authentication Mechanism for Securing Smart Cities. Sensors. 2023 Mar 2, 23(5):2757.

[80] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Jan, 11(24):12040.

[81] Hongmei Z. A cross-border e-commerce approach based on blockchain technology. Mobile Information Systems. 2021 Jul 15, 2021:1-0.

[82] Bordo MD. Central bank digital currency in historical perspective: Another crossroad in monetary history. National Bureau of Economic Research, 2021 Aug 23.

[83] Mogaji E. Redefining banks in the digital era: a typology of banks and their research, managerial and policy implications. International Journal of Bank Marketing. 2023 Dec 1, 41(7):1899-918.

[84] Aldboush HH, Ferdous M. Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust. International Journal of Financial Studies. 2023 Jul 10, 11(3):90.

[85] 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.

[86] Markos E, Peña P, Labrecque LI, Swani K. Are data breaches the new norm? Exploring data breach trends, consumer sentiment, and responses to security invasions. Journal of Consumer Affairs. 2023 Jul, 57(3):1089-119.

[87] Gibson D, Harfield C. Amplifying victim vulnerability: Unanticipated harm and consequence in data breach notification policy. International Review of Victimology. 2023 Sep, 29(3):341-65.

[88] Hassan A, Ahmed K. Cybersecurity's impact on customer experience: an analysis of data breaches and trust erosion. Emerging Trends in Machine Intelligence and Big Data. 2023 Sep 23, 15(9):1-9.

[89] Thomas L, Gondal I, Oseni T, Firmin SS. A framework for data privacy and security accountability in data breach communications. Computers & Security. 2022 May 1, 116:102657.

[90] 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.

[91] Davis SR. Ten Easy Steps to Reduce Your Risk of Cyberattack or Data Breach. The Judges' Journal. 2023 Jun 22, 62(3):28-32.

[92] Duggineni S. Impact of controls on data integrity and information systems. Science and Technology. 2023, 13(2):29-35.

[93] Sharma P, Barua S. From data breach to data shield: the crucial role of big data analytics in modern cybersecurity strategies. International Journal of Information and Cybersecurity. 2023 Sep 5, 7(9):31-59.

[94] 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.

[95] Chirayath SS. Insider Threats and Strategies to Manage Insider Risk. InHuman Reliability Programs in Industries of National Importance for Safety and Security 2023 Sep 30 (pp. 51-59). Singapore: Springer Nature Singapore.

[96] Darem AA, Alhashmi AA, Alkhaldi TM, Alashjaee AM, Alanazi SM, Ebad SA. Cyber threats classifications and countermeasures in banking and financial sector. IEEE Access. 2023 Oct 23, 11:125138-58.

[97] Moneva A, Leukfeldt R. Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures. Journal of Criminology. 2023 Dec, 56(4):416-40.

[98] Naveenan RV, Suresh G. Cyber risk and the cost of unpreparedness of financial institutions. InCyber Security and Business Intelligence 2023 Dec 11 (pp. 15-36). Routledge.

[99] Qiu Z, Ma J, Zhang H, Al Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Concurrent pipeline rendering scheme based on GPU multi-queue and partitioning images. InInternational Conference on Optics and Machine Vision (ICOMV 2023) 2023 Apr 14 (Vol. 12634, pp. 143-149).

[100] Alahmari S, Renaud K, Omoronyia I. Moving beyond cyber security awareness and training to engendering security knowledge sharing. Information Systems and e-Business Management. 2023 Mar, 21(1):123-58.

[101] Hu S, Hsu C, Zhou Z. Security education, training, and awareness programs: Literature review. Journal of Computer Information Systems. 2022 Jul 4, 62(4):752-64.

[102] Adu-Manu KS, Ahiable RK, Appati JK, Mensah EE. Phishing Attacks in Social Engineering: A Review. Journal of Cybersecurity (2579-0072). 2022 Oct 1, 4(4).

[103] 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.

[104] 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.

[105] Siddiqi MA, Pak W, Siddiqi MA. A study on the psychology of social engineering-based cyberattacks and existing countermeasures. Applied Sciences. 2022 Jun 14, 12(12):6042.

[106] Abu Hweidi RF, Eleyan D. Social Engineering Attack Concepts, Frameworks, and Awareness: A Systematic Literature Review. International Journal of Computing and Digital Systems. 2023 Feb 28.

[107] Fuertes W, Arévalo D, Castro JD, Ron M, Estrada CA, Andrade R, Peña FF, Benavides E. Impact of social engineering attacks: A literature review. Developments and Advances in Defense and Security: Proceedings of MICRADS 2021. 2022:25-35.

[108] Duarte N, Coelho N, Guarda T. Social engineering: the art of attacks. InAdvanced Research in Technologies, Information, Innovation and Sustainability: First International Conference, ARTIIS 2021, La Libertad, Ecuador, November 25–27, 2021, Proceedings 1 2021 (pp. 474-483). Springer International Publishing.

[109] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22, 6(7):154.

[110] Sharma A, Gupta BB, Singh AK, Saraswat VK. Advanced Persistent Threats (APT): evolution, anatomy, attribution and countermeasures. Journal of Ambient Intelligence and Humanized Computing. 2023 May 6:1-27.

[111] Jadala VC, Pasupuleti SK, Sai Baba CM, Hrushikesava Raju S, Ravinder N. Analyzing and Detecting Advanced Persistent Threat Using Machine Learning Methodology. InSustainable Communication Networks and Application: Proceedings of ICSCN 2021 2022 Jan 17 (pp. 497-506). Singapore: Springer Nature Singapore.

[112] Imran M, Siddiqui HU, Raza A, Raza MA, Rustam F, Ashraf I. A performance overview of machine learning-based defense strategies for advanced persistent threats in industrial control systems. Computers & Security. 2023 Nov 1, 134:103445.

[113] Chen T, Zheng C, Zhu T, Xiong C, Ying J, Yuan Q, Cheng W, Lv M. System-Level Data Management for Endpoint Advanced Persistent Threat Detection: Issues, Challenges and Trends. Computers & Security. 2023 Sep 21:103485.

[114] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[115] Javed SH, Ahmad MB, Asif M, Almotiri SH, Masood K, Ghamdi MA. An intelligent system to detect advanced persistent threats in industrial internet of things (I-IoT). Electronics. 2022 Feb 28, 11(5):742.

[116] Chen Z, Liu J, Shen Y, Simsek M, Kantarci B, Mouftah HT, Djukic P. Machine learning-enabled iot security: Open issues and challenges under advanced persistent threats. ACM Computing Surveys. 2022 Dec 3, 55(5):1-37.

[117] Gan C, Lin J, Huang DW, Zhu Q, Tian L. Advanced Persistent Threats and Their Defense Methods in Industrial Internet of Things: A Survey. Mathematics. 2023 Jul 14, 11(14):3115.

[118] Sakthivelu U, Vinoth Kumar CN. Advanced Persistent Threat Detection and Mitigation Using Machine Learning Model. Intelligent Automation & Soft Computing. 2023 Jun 1, 36(3).

[119] Kumar S, Chinthaginjala R, Anbazhagan R, Nyangaresi VO, Pau G, Varma PS. Submarine Acoustic Target Strength Modelling at High-Frequency Asymptotic Scattering. IEEE Access. 2024 Jan 1.

[120] Kang H, Liu G, Wang Q, Meng L, Liu J. Theory and Application of Zero Trust Security: A Brief Survey. Entropy. 2023 Nov 28, 25(12):1595.

[121] Didenko AN. Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond. Uniform Law Review. 2020 Mar 1, 25(1):125-67.

[122] Fiero AW, Beier E. New global developments in data protection and privacy regulations: Comparative analysis of European Union, United States, and Russian legislation. Stan. J. Int'l L.. 2022, 58:151.

[123] Sengupta S. Financial Data Protection in Indian Regulatory Policy: From'Secrecy'and'Confidentiality'to'Privacy'. J. Indian L. & Soc'y. 2021, 12:85.

[124] 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.

[125] Shevchenko PV, Jang J, Malavasi M, Peters GW, Sofronov G, Trück S. The nature of losses from cyber-related events: risk categories and business sectors. Journal of Cybersecurity. 2023 Jan 1, 9(1):tyac016.

[126] Fitriani R, Subagiyo R, Asiyah BN. Mitigating IT Risk of Bank Syariah Indonesia: A Study of Cyber Attack on May 8, 2023. Al-Amwal: Jurnal Ekonomi dan Perbankan Syari'ah. 2023 Jun 26, 15(1):86-100.

[127] Lehto M. Cyber-attacks against critical infrastructure. InCyber Security: Critical Infrastructure Protection 2022 Apr 3 (pp. 3-42). Cham: Springer International Publishing.

[128] Abdel-Rahman M. Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. Eigenpub Review of Science and Technology. 2023 Jul 15, 7(1):138-58.

[129] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11, 2(3): 399-406.

[130] Afroze D, Rista FI. Mobile financial services (MFS) and digital inclusion–a study on customers' retention and perceptions. Qualitative Research in Financial Markets. 2022 Sep 22, 14(5):768-85.

[131] Dzidzah E, Owusu Kwateng K, Asante BK. Security behaviour of mobile financial service users. Information & Computer Security. 2020 Nov 4, 28(5):719-41.

[132] Ambore S, Richardson C, Dogan H, Apeh E, Osselton D. A resilient cybersecurity framework for Mobile Financial Services (MFS). Journal of Cyber Security Technology. 2017 Oct 1, 1(3-4):202-24.

[133] 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.

[134] Sharma S, Saini A, Chaudhury S. A survey on biometric cryptosystems and their applications. Computers & Security. 2023 Sep 1:103458.

[135] Al Hwaitat AK, Almaiah MA, Ali A, Al-Otaibi S, Shishakly R, Lutfi A, Alrawad M. A new blockchain-based authentication framework for secure IoT networks. Electronics. 2023 Aug 27, 12(17):3618.

[136] 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.

[137] Salem M, Taheri S, Yuan JS. Utilizing transfer learning and homomorphic encryption in a privacy preserving and secure biometric recognition system. Computers. 2018 Dec 29, 8(1):3.

[138] 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.

[139] Moretto A, Grassi L, Caniato F, Giorgino M, Ronchi S. Supply chain finance: From traditional to supply chain credit rating. Journal of Purchasing and Supply Management. 2019 Mar 1, 25(2):197-217.

[140] Tiwari S, Sharma P, Choi TM, Lim A. Blockchain and third-party logistics for global supply chain operations: Stakeholders' perspectives and decision roadmap. Transportation Research Part E: Logistics and Transportation Review. 2023 Feb 1, 170:103012.

[141] Song H, Li M, Yu K. Big data analytics in digital platforms: how do financial service providers customise supply chain finance?. International Journal of Operations & Production Management. 2021 Jun 1, 41(4):410-35.

[142] Sayeed S, Marco-Gisbert H. Assessing blockchain consensus and security mechanisms against the 51% attack. Applied sciences. 2019 Apr 29, 9(9):1788.

[143] 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.

[144] Wenhua Z, Qamar F, Abdali TA, Hassan R, Jafri ST, Nguyen QN. Blockchain technology: security issues, healthcare applications, challenges and future trends. Electronics. 2023 Jan 20, 12(3):546.

[145] Trivedi C, Rao UP, Parmar K, Bhattacharya P, Tanwar S, Sharma R. A transformative shift toward blockchain-based IoT environments: Consensus, smart contracts, and future directions. Security and Privacy. 2023 Sep, 6(5):e308.

[146] Mollajafari S, Bechkoum K. Blockchain technology and related security risks: towards a seven-layer perspective and taxonomy. Sustainability. 2023 Sep 7, 15(18):13401.

[147] Yadav AK, Singh K, Amin AH, Almutairi L, Alsenani TR, Ahmadian A. A comparative study on consensus mechanism with security threats and future scopes: Blockchain. Computer Communications. 2023 Mar 1, 201:102-15.

[148] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[149] Lukings M, Habibi Lashkari A. Comparative Legal Strategies. InUnderstanding Cybersecurity Law in Data Sovereignty and Digital Governance: An Overview from a Legal Perspective 2022 Oct 15 (pp. 181-204). Cham: Springer International Publishing.

[150] Walters R. Data Flows and Data Protection Law. InCybersecurity and Data Laws of the Commonwealth: International Trade, Investment and Arbitration 2023 Jul 22 (pp. 49-74). Singapore: Springer Nature Singapore.

[151] Meltzer JP. Balancing commitments to cross-border data flows with domestic regulation. InThe Elgar Companion to the World Trade Organization 2023 Dec 12 (pp. 223-242). Edward Elgar Publishing.

[152] Chen J, Yao B, Lu Q, Wang X, Yu P, Ge H. A safety dynamic evaluation method for missile mission based on multi-layered safety control structure model. Reliability Engineering & System Safety. 2024 Jan 1, 241:109678.

[153] 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.

[154] Srivastava N, Sharma H, Maliyal A, Verma M, Sinha K. Fortifying Data Security in the Evolving Digital Landscape: Challenges and Solutions. InHandbook of Research on Innovative Approaches to Information Technology in Library and Information Science 2024 (pp. 209-232). IGI Global.

[155] Bremer J, Lehnhoff S. Encrypted Decentralized Optimization for Data Masking in Energy Scheduling. InProceedings of the 3rd International Conference on Big Data Research 2019 Nov 20 (pp. 103-109).

[156] Rieyan SA, News MR, Rahman AM, Khan SA, Zaarif ST, Alam MG, Hassan MM, Ianni M, Fortino G. An advanced data fabric architecture leveraging homomorphic encryption and federated learning. Information Fusion. 2024 Feb 1, 102:102004.

[157] Yang LC. Security and Privacy Concerns in Information Usability. InProceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision 2024 (pp. 679-684).

[158] 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.

[159] 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.

[160] Aburbeian AM, Fernández-Veiga M. Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning. AI. 2024 Jan 10, 5(1):177-94.

[161] Basha PH, Prathyusha G, Rao DN, Gopikrishna V, Peddi P, Saritha V. AI-Driven Multi-Factor Authentication and Dynamic Trust Management for Securing Massive Machine Type Communication in 6G Networks. International Journal of Intelligent Systems and Applications in Engineering. 2024, 12(1s):361-74.

[162] Anoh NG, Kone T, Diedie GH, Babri M. Multi-factor authentication system for securing mobile money transactions using mobile money services in Ivory Coast. International Journal of Innovation and Applied Studies. 2024, 41(3):785-94.

[163] 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.

[164] Mansour A, Eddermoug N, Sadik M, Sabir E, Azmi M, Jebbar M. A Lightweight Seamless Unimodal Biometric Authentication System. Procedia Computer Science. 2024 Jan 1, 231:190-7.

[165] Gernot T, Rosenberger C. Robust biometric scheme against replay attacks using one-time biometric templates. Computers & Security. 2024 Feb 1, 137:103586.

[166] Hossam Eldein Mohamed FA, El-Shafai W. Cancelable biometric authentication system based on hyperchaotic technique and fibonacci Q-Matrix. Multimedia Tools and Applications. 2024 Jan 6:1-39.

[167] Li N, Wang Z, Yang X, Zhang Z, Zhang W, Sang S, Zhang H. Deep-Learning-Assisted Thermogalvanic Hydrogel E-Skin for Self-Powered Signature Recognition and Biometric Authentication. Advanced Functional Materials. 2024:2314419.

[168] 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.

[169] Kaur G, Bharathiraja N, Singh KD, Veeramanickam MR, Rodriguez CR, Pradeepa K. Emerging Trends in Cybersecurity Challenges with Reference to Pen Testing Tools in Society 5.0. Artificial Intelligence and Society 5.0. 2024 Jan 22:196-212.

[170] Seara JP, Serrão C. Intelligent System for Automation of Security Audits (SIAAS). EAI Endorsed Transactions on Scalable Information Systems. 2024, 11(1).

[171] Josyula HP, Reddi LT, Parate S, Rajagopal A. A Review on Security and Privacy Considerations in Programmable Payments. International Journal of Intelligent Systems and Applications in Engineering. 2024, 12(9s):256-63.

[172] AlDaajeh S, Saleous H, Alrabaee S, Barka E, Breitinger F, Choo KK. The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security. 2022 Aug 1, 119:102754.

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

[174] Shen Q, Shen Y. Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach. Computers & Security. 2024 Jan 1, 136:103537.

[175] Ansarullah SI, Kirmani MM, Mushtaq Z, ud din Dar GM. Cyber Security: Future Trends and Solutions. InCyber Security for Next-Generation Computing Technologies 2024 (pp. 1-15). CRC Press.

[176] Verma R, Koul S, Ajaygopal KV. Evaluation and Selection of a Cybersecurity Platform— Case of the Power Sector in India. Decision Making: Applications in Management and Engineering. 2024 Jan 1, 7(1):209-36.

[177] Addimulam SC. Industrial Control Systems for Cyber-Security Networks in Data Science. International Journal of Intelligent Systems and Applications in Engineering. 2024, 12(9s):72-8.

[178] Che Mat NI, Jamil N, Yusoff Y, Mat Kiah ML. A systematic literature review on advanced persistent threat behaviors and its detection strategy. Journal of Cybersecurity. 2024 Jan 1, 10(1):tyad023.

[179] Al Sibahee MA, Nyangaresi VO, Abduljabbar ZA, Luo C, Zhang J, Ma J. Two-Factor Privacy Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks. IEEE Internet of Things Journal. 2023 Dec 7.

[180] König L, Korobeinikova Y, Tjoa S, Kieseberg P. Comparing blockchain standards and recommendations. Future Internet. 2020 Dec 7, 12(12):222.

[181] De Novi G, Sofia N, Vasiliu-Feltes I, Zang CY, Ricotta F. Blockchain Technology Predictions 2024: Transformations in Healthcare, Patient Identity, and Public Health. Blockchain in Healthcare Today. 2023, 6.

[182] Chithaluru P, Al-Turjman F, Dugyala R, Stephan T, Kumar M, Dhatterwal JS. An enhanced consortium blockchain diversity mining technique for IoT metadata aggregation. Future Generation Computer Systems. 2024 Mar 1, 152:239-53.

[183] Lin Q, Li X, Cai K, Prakash M, Paulraj D. Secure Internet of medical Things (IoMT) based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking. Information Sciences. 2024 Jan 1, 654:119783.

[184] Luna M, Fernandez-Vazquez S, Castelao ET, Fernández ÁA. A blockchain-based approach to the challenges of EU's environmental policy compliance in aquaculture: From traceability to fraud prevention. Marine Policy. 2024 Jan 1, 159:105892.

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

[186] Chauhan M, Shiaeles S. An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. Network. 2023 Sep 12, 3(3):422-50.

[187] Ugale S, Potgantwar A. Container Security in Cloud Environments: A Comprehensive Analysis and Future Directions for DevSecOps. Engineering Proceedings. 2023 Dec 18, 59(1):57.

[188] Samunnisa K, Vijaya Kumar GS, Madhavi K. Cloud Security Solutions Through Machine Learning-Approaches: A Survey. Int. J. of Aquatic Science. 2021 Jun 1, 12(2):1958-72.

[189] Chatterjee D, Hassan MM, Islam N, Ray A, Barbhuyan MF. A Futuristic Approach to Security in Cloud Data Centers Using a Hybrid Algorithm. Engineering Proceedings. 2023 Dec 14, 59(1):47.

[190] Xu M, Du H, Niyato D, Kang J, Xiong Z, Mao S, Han Z, Jamalipour A, Kim DI, Shen X, Leung VC. Unleashing the power of edge-cloud generative ai in mobile networks: A survey of aigc services. IEEE Communications Surveys & Tutorials. 2024 Jan 12.

[191] 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.

[192] Bui H, Krajcsák Z. The impacts of corporate governance on firms' performance: from theories and approaches to empirical findings. Journal of Financial Regulation and Compliance. 2024 Jan 10, 32(1):18-46.

[193] Ewens M, Xiao K, Xu T. Regulatory costs of being public: Evidence from bunching estimation. Journal of Financial Economics. 2024 Mar 1, 153:103775.

[194] Ahmad S, Ullah S, Akbar S, Kodwani D, Brahma S. The impact of compliance, board committees and insider CEOs on firm survival during crisis. International Review of Financial Analysis. 2024 Jan 1, 91:102979.

[195] Almohammad A, Georgakis P. Automated Approach for Generating and Evaluating Traffic Incident Response Plans. Engineering Proceedings. 2023 Jun 28, 39(1):13.

[196] Allen PC. Surviving the storm: The key to cyber resilience and incident response in healthcare. InHealthcare Management Forum 2024 Jan (Vol. 37, No. 1, pp. 26-29). Sage CA: Los Angeles, CA: SAGE Publications.

[197] Shubailat O, Al-Zaqeba M, Madi A, Ababneh A. Customs intelligence and risk management in sustainable supply chain for general customs department logistics. Uncertain Supply Chain Management. 2024, 12(1):387-98.

[198] Al-Hawawreh M, Moustafa N, Slay J. A threat intelligence framework for protecting smart satellite-based healthcare networks. Neural Computing and Applications. 2024 Jan, 36(1):15-35.

[199] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[200] Pool J, Akhlaghpour S, Fatehi F, Burton-Jones A. A systematic analysis of failures in protecting personal health data: a scoping review. International Journal of Information Management. 2024 Feb 1, 74:102719.

[201] Bednorz J. Working from anywhere? Work from here! Approaches to attract digital nomads. Annals of Tourism Research. 2024 Mar 1, 105:103715.

[202] Abba Ari AA, Ngangmo OK, Titouna C, Thiare O, Mohamadou A, Gueroui AM. Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges. Applied Computing and Informatics. 2024 Jan 5, 20(1/2):119-41.

[203] Li Y, Yan H, Huang T, Pan Z, Lai J, Zhang X, Chen K, Li J. Model architecture level privacy leakage in neural networks. Science China Information Sciences. 2024 Mar, 67(3):132101.

[204] Verma G. Blockchain-based privacy preservation framework for healthcare data in cloud environment. Journal of Experimental & Theoretical Artificial Intelligence. 2024 Jan 2, 36(1):147-60.

[205] 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.

[206] El Jalbout S, Keivanpour S. Development of a body of knowledge for design for disassembly and recycling of high-tech products: a case study on lithium-ion batteries. Journal of Industrial and Production Engineering. 2024 Jan 2, 41(1):19-39.

[207] Krayem A, Thorin E, Wallin F. Experiences from developing an open urban data portal for collaborative research and innovation. Applied Energy. 2024 Feb 1, 355:122270.

[208] Kulkarni S, Tripathi RK, Joshi M. A Study on Data Security in Cloud Computing: Traditional Cryptography to the Quantum Age Cryptography. InSystem Design Using the Internet of Things with Deep Learning Applications 2023 Oct 6 (pp. 147-174). Apple Academic Press.

[209] García-Rodríguez J, Krenn S, Slamanig D. To pass or not to pass: Privacy-preserving physical access control. Computers & Security. 2024 Jan 1, 136:103566.

[210] Miao J, Wang Z, Wu Z, Ning X, Tiwari P. A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things. Expert Systems with Applications. 2024 Mar 1, 237:121329.

[211] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11, 10:26257-70.

[212] Peters U. Explainable AI lacks regulative reasons: why AI and human decision-making are not equally opaque. AI and Ethics. 2023 Aug, 3(3):963-74.

[213] Springler E. A neoliberal agenda: decentralized financial innovation to enhance sustainable finance. InUnderstanding Green Finance 2024 Jan 9 (pp. 134-145). Edward Elgar Publishing.

[214] Paya A, Arroni S, García-Díaz V, Gómez A. Apollon: A robust defense system against Adversarial Machine Learning attacks in Intrusion Detection Systems. Computers & Security. 2024 Jan 1, 136:103546.

[215] Pandey C. Scalability Challenges and Opportunities in Blockchain-based Systems: A Systematic Review. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 2020 Dec 15, 11(3):2022-31.

[216] Coche E, Kolk A, Ocelík V. Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business. Journal of International Business Policy. 2023 Oct 6:1-6.

[217] Rani P, Sachan RK, Kukreja S. Academic Payment Tokenization: An Online Payment System for Academia Utilizing Non-Fungible Tokens and Permissionless Blockchain. Procedia Computer Science. 2023 Jan 1, 230:347-56.