Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM
e-ISSN: 2788-7421 p-ISSN: 2958-0544

A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech

Guma Ali[1]*, Maad M. Mijwil[2], Bosco Apparatus Buruga[3], Mostafa Abotaleb[4]

[1]Department of Computer and Information Science (CIS), Muni University, Arua, 00256, Uganda
[2]Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq
[3]Department of Library and Information Services, Muni University, Arua, 00256, Uganda
[4]Department of System Programming, South Ural State University, Chelyabinsk, Russia

*Corresponding Author: Guma Ali

DOI: https://doi.org/10.52866/ijcsm.2024.05.03.004
Received January 2024; Accepted March 2024; Available online June 2024

ABSTRACT: The fourth industrial revolution has seen the evolution and wide adoption of game-changing and disruptive innovation "financial technologies (FinTech)" around the globe. However, the security of FinTech systems and networks remains critical. This paper comprehensively reviews the evolving landscape of cybersecurity issues within the FinTech sector and explores effective mitigation measures. Four independent researchers reviewed relevant literature from IEEE Xplore Digital Library, ScienceDirect, Taylor & Francis, Emerald Insight, Springer, SAGE, Wiley Online Library, Hindawi, MDPI, ACM Digital Library, IGI Global, and Google Scholar. The research paper begins by examining the history and evolution of FinTech, drivers for the growth of FinTech, segments of the FinTech industry, FinTech ecosystem, FinTech business model, and FinTech application. Subsequently, it then delves into an analysis of the most pressing cybersecurity issues confronting FinTech firms, such as privacy concerns, data breaches, malware attacks, hacking, insider threats, identity theft, social engineering attacks, distributed denial-of-service attacks, and others. In response to these cybersecurity issues, the paper evaluates various mitigation strategies and best practices adopted by FinTech firms and regulatory bodies globally. These measures include technological solutions such as authentication and access control mechanisms, cryptography, big data analytics, intrusion detection/prevention systems, regular data backup, artificial intelligence and machine learning, cloud computing technologies, blockchain technologies, and fraud detection and prevention systems. The paper also emphasizes the importance of FinTech regulatory sandboxes, regulatory compliance, basic security training, continuous monitoring of threats, zero-trust policy, robust cybersecurity culture, regular testing, and stringent security policies to strengthen the FinTech ecosystem's cyber resilience. Based on empirical research, industry reports, and regulatory guidelines, this review brings together existing information and highlights upcoming trends in FinTech cybersecurity. It emphasizes the importance of a collaborative strategy combining industry stakeholders, regulators, legislators, and cybersecurity specialists to address the growing cyber threat situation successfully. Ultimately, this research will help develop robust security mechanisms for FinTech systems and networks to achieve sustainable financial inclusion.

Keywords: comprehensive review, cyberattacks, cybersecurity, FinTech, mitigation measures

1. INTRODUCTION

The substantial and rapid growth in computing technologies, Internet connectivity, and smartphone penetration has witnessed the emergence of disruptive innovations known as "financial technologies" that have shaped the traditional banking and financial industry in emerging countries. This fourth industrial revolution disruptive innovations are the game changers driving financial inclusion among the unbanked population. Financial technology, also known as FinTech, refers to the application and use of newly developed and cutting-edge technological innovations by the banking and financial industry to efficiently deliver financial services, thereby spurring and promoting the development and emergence of new business models, applications, processes, and products [1-4]. This technology helps businesses, business owners, and individuals to better manage their financial operations, processes, and lives by employing specialized software and algorithms in computers, smartphones, and tablets [5], [6]. FinTech uses emerging technologies such as big data, data analytics, artificial intelligence, and the Internet of Things (IoT) [7-12], machine learning, blockchain [13], [14], mobile embedded systems, cloud computing [15-17], deep learning, cryptocurrencies [18-20], cryptography, quantum computing [21], [22], biometrics, cybersecurity [23], [24], open-source computing,

application programming interfaces (APIs) [25], [26], image processing, natural language processing [27], and robotic process automation [5], [28-30], to provide customers with better financial services through attractive, user-friendly solutions which effectively fulfil their needs and demands.

FinTech broadly encompasses five areas: insurance, banking, e-commerce, lending, and personal financial management [18]. Apple Pay, Alipay, Wechatpay, PayPal Here, Google Wallet, Ripple, Paylax, and PayU are among the FinTech payment service providers. The integration of various disruptive technologies distinguishes them to gain a competitive advantage by providing higher-quality financial services and automation; the firms they threaten to disrupt are more established and influential; they are customer-centric and operate on an agile business model [31], [32]. During the global COVID-19 pandemic, there was a tremendous increase in the use of FinTech services and products to provide individuals with financial services [33], [34]. The main focus of FinTech is regulation technology, digital identity, payment and remittances, asset management solutions, and financial software [1], [24].

The FinTech market has expanded dramatically, with over 12,500 startups globally providing financial services to over 1.7 billion unbanked people [32], [35], [36]. According to Statista Market Insights, the worldwide FinTech sector income in 2023 is anticipated at US$79.38 billion and is projected to exceed US$141.18 billion in 2028 [37]. With 83% FinTech investment, the United States of America is the world's largest FinTech market, followed by the United Kingdom and China, owing to their government's support and investment and loosened government financial regulation. The FinTech sector in Indonesia and Southeast Asia is predicted to be worth US$1200 billion by 2025, with financing services worth US$92 billion. In Africa, US$1.6 billion was invested in 153 FinTech deals by 2021 [38].

FinTech provides a variety of services, including digital cash and currency, e-wallet, online payment and transaction, mortgage and real estate, cryptocurrency, crowdfunding, digital invoicing, online investment, financial data analysis, wealth management, digital leasing, loan, digital advising, e-insurance [30], [33], [39], [40], lending platforms, e-government services, the stock market [11], [41], InsurTech, asset management, WealthTech, RegTech, fund transfer, peer-to-peer (P2P) lending, e-aggregators, mobile payment [17], [20], [25], [30], [42-44], utility bill payments, offshore remittance, risk management, Robo-advisory [19], [45], and personal investment management [23]. Easy usage, compatibility, mobility, flexibility, security, simplicity of service delivery at a lower cost, and increasing market share [28], [30], [33], [34], [46-48]; transparency, and timeliness [32], [45], [49-51]; improved service quality [13], [19], [52], [53]; global financial market access, digital marketing, and data analysis [18], [40], [46], [54]; boosting innovation, financial stability and accessibility, productivity, profitability, and financial inclusion [8], [30], [39], [55-61], are some of the benefits offered by the innovation to customers, investors, and enterprises.

Despite the benefits provided by FinTech, the technology's growth is hampered by severe existential cybersecurity issues such as malware, social engineering attacks, hacking, crypto-jacking, zero-day attacks, insider threats, man-in-the-middle attacks, data breaches, identity theft, distributed denial-of-service attacks, supply chain attacks, advanced persistent threat, salami attacks, shoulder-surfing attacks, brute-force attacks, cloud environment security risks, blockchain risks, IoT risks, money laundering, and cryptocurrency-related risks [18], [23], [49], [51], [62-69]. These security breaches have resulted in reputational damage, loss of customer trust, password and revenue loss, industrial espionage, data and equity value loss, money laundering, cyberterrorism, higher operational costs, and disruption of FinTech systems and services [18], [70], [71]. As a result, cybersecurity is strongly recommended for the FinTech industry to ensure the confidentiality, integrity, availability, authenticity, authorization, non-repudiation, accountability, and auditability of users and financial data [70], [19], [72] so that FinTech stakeholders can receive quality financial services.

The study provides an in-depth review of the critical cybersecurity issues and their mitigation measures in the FinTech industry. This study's significant contributions include:

- To examine FinTech's history and evolution, drivers, segments, ecosystem, business model, and application.
- To provide a comprehensive overview of the various cybersecurity issues in the FinTech industry.
- To explore the mitigation measures available for improving cybersecurity in FinTech.

The rest of the paper is structured in the following order.

2. HISTORY AND EVOLUTION OF FINTECH

FinTech has been evolving for over a decade, with five essential phases, including FinTech 1.0 (1866-1967), FinTech 2.0 (1967-2008), FinTech 3.0 (2008-2014), FinTech 3.5 (2014-2017), and FinTech 4.0 (2018-to date), each with new technologies deployed.

2.1 FinTech 1.0 (1866-1967)

During the FinTech 1.0 period, infrastructure such as steamships, telegraphs, railroads, and worldwide telex networks was created to facilitate financial communication and trading between nations. The first transatlantic cable was built in 1866 to create a network infrastructure and global linkages; Fedwire in 1918 to transfer electronic funds using Telegraph and Morse code, Pantelegraph for signature verification; dinner cards in 1950 to make cashless restaurant payments, credit cards in 1958 to alleviate the problem of carrying cash, and screen-based stock data in 1960, which led to a massive rise in the financial market. Many insurance, banking, and joint-stock companies emerged

during this period. These innovations were crucial in the first industrial revolution, laying the groundwork for FinTech 2.0 [10], [19], [73-76].

2.2 FinTech 2.0 (1967–2008)

The remarkable innovations in this FinTech 2.0 era are the Telex, which replaced the Telegraph in 1966, the installation of automated teller machines (ATM) in 1967 by the Barclays Bank, the Interbank Computer Bureau of the United Kingdom that introduced the modern computerized payment systems and electronic clearing services in 1968. In 1971, the National Association of Securities Dealers Automated Quotations (NASDAQ) established the first electronic stock market, and in 1973, the Society for Worldwide Interbank Financial Telecommunications (SWIFT) was introduced to enable financial institutions to transfer massive amounts of money across borders. The use of mainframe computers in banks increased in the 1980s, as did the growth of electronic banking (e-banking). Tradeplus introduced electronic trade for its customers in 1982, and NBS/WF promoted digital banking to customers to help them manage their money in 1983/1985. The growth of electronic commerce occurred in the mid-1990s, with Wells Fargo developing online consumer banking in 1995, and in 1998, the new cashless payment system "PayPal" was introduced. Many traditional banks used FinTech in 2000 to provide alternative support to their primary channel of payments. Furthermore, the 2008 financial crisis caused a fundamental shift in the need for the FinTech sector. FinTech 3.0 was made possible by the growth of the Internet [10], [19], [73-76].

2.3 FinTech 3.0 (2008–2014)

The swift rise and adoption of the smartphone and the 2008 global financial crisis made the general public lose trust in the traditional banking system, resulting in a fundamental shift in the need for FinTech 3.0. Many people use smartphones worldwide to access the Internet and financial services. Similarly, it has attracted a slew of new FinTech startups, in addition to the existing traditional financial institutions that digitized banking services and opened the door for new products and services. Many established banks from the FinTech 2.0 era left and rebranded as startups in FinTech 3.0. The introduction of Bitcoin in 2009 and other cryptocurrencies based on blockchain technology, P2P lending/payment platforms in 2011, mobile wallets (Google Wallet in 2011 and Apple Pay in 2014), credit scoring, Banking as a Service (BaaS) platforms (Treezor and SolarisBank), RegTech, small-ticket loans, insurance technology (InsurTech), property technology (PropTech), wealth technology (WealthTech), and government technology (GovTech), and others have all had a significant impact on the financial world by providing low-cost services [10], [19], [73-76].

2.4 FinTech 3.5 (2014-2017)

The FinTech 3.5 era explains how people in emerging nations access the Internet and the global spread of electronic banking. It examines how new entrants such as China and India, which have the most prominent FinTech usage, did not expand their physical banking infrastructure. Instead, they swiftly accepted innovative technologies to provide digital banking services, growing the FinTech business. Similarly, several African countries expanded their Internet coverage during this period, expanding online banking services throughout the continent. During this period, some of the most prevalent FinTech breakthroughs are Alipay in China, Payment banks in India, Indian firms developing software as a Service 2 (SaaS 2)-like financial software, and M-Pesa mobile money in Africa [10], [75], [76].

2.5 FinTech 4.0 (2018-to date)

The FinTech 4.0 era comprises the digitization and datafication of finance, new entrants like BigTechs, e.g., Meta, Google, Amazon, Tencent, Alibaba, and the dominance of digital finance platforms. BigTechs use advanced analytical methods like artificial intelligence to process the big data collected from the various activities on their platforms [77]. It also looks at how disruptive technologies like blockchain and open banking are shaping the future of financial services. Another significant event is how machine learning alters customer interactions with banks and insurance businesses, how artificial intelligence technologies are battling card fraud and money laundering, and how customer behaviour is forecasted by dynamically detecting new card fraud tendencies. Other technologies in FinTech 4.0 include virtual and augmented reality, digital banking, digital lending, web-based crowdfunding frameworks, InsurTech, PropTech, customer rewards, and RegTech. It also involves integrated payment providers developing and implementing quick response (QR) code-based payment systems [10], [75], [76], [77].

Figure 1 summarises the essential technologies in the five phases of FinTech evolution.

Figure 1. Summarises the essential technologies in the five phases of FinTech evolution

3. DRIVERS FOR THE GROWTH OF FINTECH

The widespread adoption and growth of FinTech are due to several factors, such as:

- The development and penetration of the emerging technological innovations are enabling many people to access financial services, processes, and business models from anywhere and at any time [32], [73], [78-86].
- Favourable financial regulations, supervisory requirements for existing financial institutions and new entrants, and government-supporting financial inclusion policies for the unbanked population are driving the FinTech industry's rapid growth [45], [79-86].
- The significant benefits gained from using FinTech include the ease of accessibility, compatibility, mobility, flexibility, security, convenience, transparency, timeliness, improved and simplified service delivery at a lower cost, interoperability, innovation, financial stability, profitability, productivity, financial inclusion, and increased market share, are propelling the FinTech industry [25], [28], [33], [46], [51], [59], [60], [80-86].
- The 2008 global financial crisis made the general public lose trust in the traditional banking system, driving many existing banks and new entrants or startups to adapt and invest in FinTech. Similarly, several customers shifted their expectations and preferences to the FinTech industry [18], [45], [80-86].
- The rising rivalry among global technology behemoths such as Apple and Google have resulted in the fast expansion of FinTech [80-86].

Figure 2 presents the drivers for the Growth of FinTech.

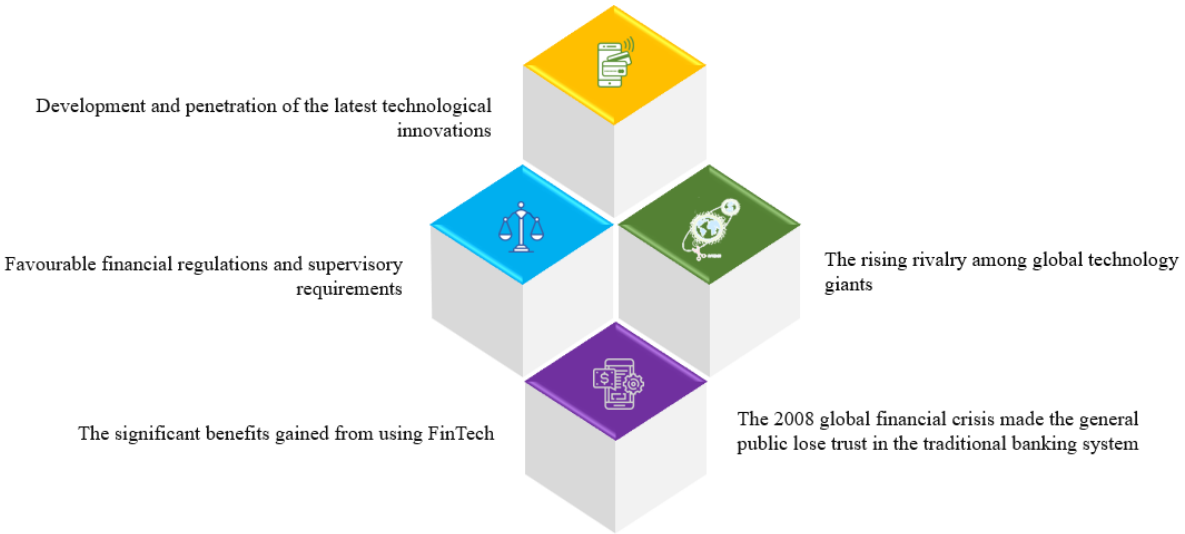

Figure 2. Presents the drivers for the Growth of FinTech

4. SEGMENTS OF THE FINTECH INDUSTRY

Gurdip et al. [18], Alt et al. [20], Baliker et al. [23], and Choudhary and Thenmozhi [84] identified several segments of the FinTech industry, which include the following:

4.1 Payment technology (PayTech)

Payment technology refers to digital payments, e-payments, and money transfers from one account to another via computers, smartphones, QR code payments, credit cards, point-of-sale, debit cards, corporate cards, prepaid cards, bulk invoice payments, and so on. Many FinTech businesses are working to improve payment systems' security, speed, and dependability to assure quick and safe transactions.

4.2 Banking as a Service (BaaS)

Banking as a Service refers to FinTech companies digitally offering banking services and products using third-party distributors. BaaS provides APIs to many third-party organizations and customers with a single platform to connect to banks to quickly and easily access financial services at a lower cost. The global BaaS market is estimated to reach $11.34 billion by 2030.

4.3 Insurance technology (InsurTech)

Insurance technology refers to disruptive innovations such as artificial intelligence, machine learning, and big data to provide customers with digital and autonomous insurance services and products. InsurTech companies use cutting-edge technologies to offer customer-centric insurance products and services like digital insurance, insurance comparison websites, bulk employee insurance products, employee group insurance plans, and insurance comparison platforms, which can be accessed through insurance infrastructure APIs because of increased insurance policyholders. Many organizations and customers opt for InsurTech because of the lower cost of recruiting new customers, the possible global economic expansion, enhanced customer experience, the provision of various methods, contracts, and goods digitally, improved fraud detection and security mechanisms, and many more.

4.4 Regulation technology (RegTech)

Regulation technology refers to using technology to ease customers' compliance and regulatory requirements to ensure minimal non-compliance and streamlined customer onboarding processes. Many RegTech companies offer know-your-customer and identity verification services, tax compliance, charge consistency, digital onboarding, anti-money laundering compliance, fraud detection tools, and risk management tools and software. The leading RegTech companies include ClearTax, EaseMyGST, Khata Book, and many more. RegTech helps to improve operational efficiency and easy regulatory compliance and guarantees less opposition.

4.5 Wealth technology (WealthTech)

Wealth technology uses advanced technologies to provide risk appetite, suggestions and willingness to invest, investment advice, wealth management, mutual funds and alternate investment platforms. The crucial areas of WealthTech companies include online portfolio management, wealth-as-a-Services (WaaS), embedded wealth, online broker, Robo retirement, and white-label Robo advisors. For example, Fidelity uses a robo-advisor to aid them with online planning and investment management. WealthTech helps improve the customers' financial investment needs, increase operational efficiency, lower costs, and improve the customer experience in personal finance systems, investment, and wealth management platforms.

4.6 Lending technology (LendTech)

Lending technology refers to using financial technologies to provide clients and organizations with fast and smooth personalized credit facilities. LendTech companies are transforming and reshaping the credit supply by innovating how traditional banks offer credit facilities to serve the underserved global population. The LendTech companies are using loan origination systems, loan management systems, credit scoring, credit bureaus, collections management, education loans, alternate credit scoring, buy now pay later (BNPL), P2P lending, instant gold loans, fixed-term finance and trade finance services for their clients to have access to the credit facilities. For example, OppFi, a consumer lending application that expands credit access to customers, Braviant Holdings uses big data and artificial intelligence to create a next-generation approach to the lending process, and many more.

4.7 Blockchain/Cryptocurrency

Blockchain/Cryptocurrency refers to a distributed storage of records in a decentralized ledger that cannot be modified. Several FinTech companies are using blockchain technology to provide transparent and decentralized finance to eliminate the barriers of the currency approval process by the central government. Nevertheless, regulators and FinTech

companies are carefully working to unify crypto investments and build trust among people because there is no solid regulatory mechanism to govern cryptocurrencies.

4.8 Cybersecurity

To build customers' trust in FinTech, FinTech companies are investing billions of dollars in building a robust cybersecurity environment globally to support digital financial work, enhance customer experience, and earn respect.

Figure 3 summarises the segments of the FinTech Industry.

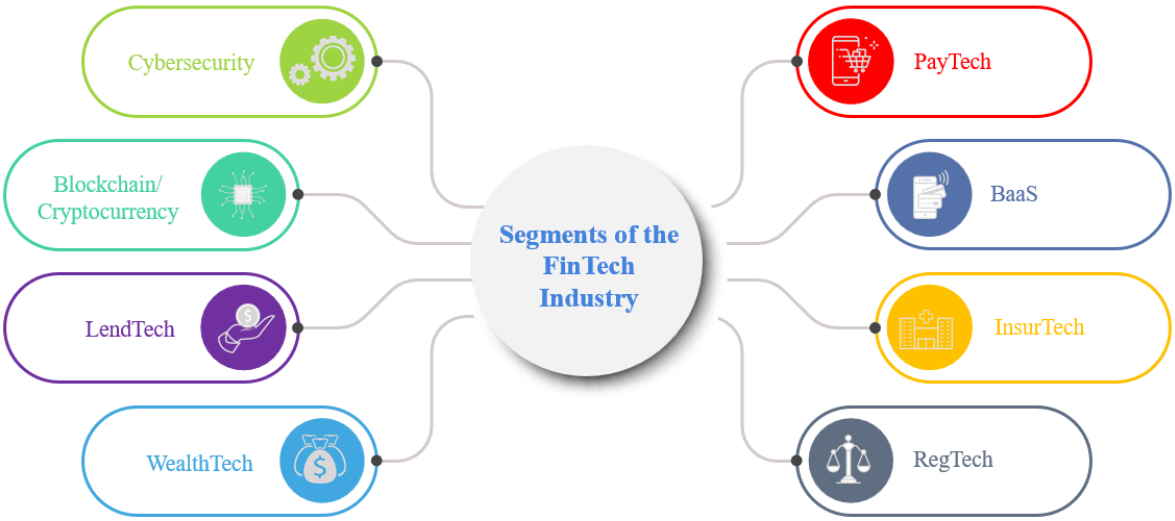

Figure 3. Summarises the segments of the FinTech Industry

5. FINTECH ECOSYSTEM

Rania et al. [87] define the FinTech ecosystem as a structure in which the different FinTech stakeholders, such as FinTech startups, technology developers, government, financial customers, and traditional financial institutions, are influenced by such an innovation. The five elements in the FinTech ecosystem are described as follows:

5.1 FinTech startups

FinTech startups are entrepreneurial companies that use technological innovations in different financial areas to target a market niche and provide personalized financial services to clients at a lower cost than traditional financial institutions [31]. FinTech Startups form the heart of the FinTech ecosystem that significantly contribute to this innovation. They include risk management startups, payment platforms, asset management, lending, loyalty programs, wealth management, trading, crowdfunding, exchange services, capital markets, regulatory technology, insurance companies, and others [9], [11], [81], [87-92].

5.2 Technology developers

Technology developers provide FinTech startups with digital platforms and channels that quickly create a convenient environment to launch innovative financial services [31]. They offer digital platforms and tools such as social media, big data analytics, cloud computing, artificial intelligence, blockchain technology, cryptocurrency, smartphones, extensive data management, algorithmic trading strategies, mobile network providers, and many more. FinTech startups launch innovative mobile financial applications to pay for online services using digital wallets [9], [11], [81], [87-92].

5.3 Government

The government provides FinTech companies and startups with new regulations or relaxes existing laws to allow them to provide low-cost and accessible financial services to their clients [88]. They provide economic policies and development plans to promote innovation and global financial competitiveness in startups [31], [43], [58] and provide other services such as licensing financial services, tax relaxation, financial rules and standards, and capital requirements [9], [11], [81], [87-92].

5.4 Financial customers

Financial customers are individuals and small and medium-sized businesses that are the primary source of income for FinTech companies [9], [11], [31], [43], [81], [88], [90-92]. They also include individuals and organizations that apply for mortgages, loans, and equity services from the government [87], [89].

5.5 Traditional financial institutions

Traditional financial institutions are enterprises and businesses that re-evaluate their business strategies to achieve a competitive edge by working with various FinTech startups [31]. They play a vital role in the FinTech ecosystem by understanding the strength of FinTech disruption and identifying the market possibilities it would create. Traditional financial institutions include banks, insurance companies, stock markets, and venture capitalists who embrace the FinTech startups' innovative technologies and collaborate with them to transform their businesses [9], [11], [81], [87-92].

The five elements in the FinTech ecosystem are summarised in Figure 4.

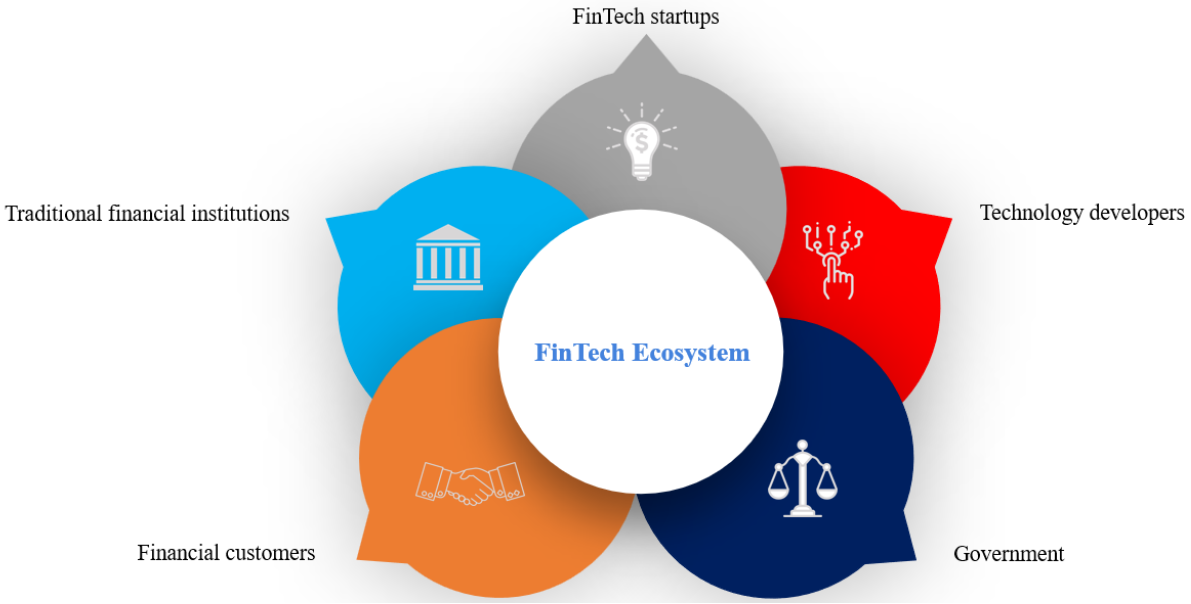

Figure 4. Shows the five elements of the FinTech ecosystem

6. FINTECH BUSINESS MODEL

The FinTech companies and startups implement several FinTech business models in the market, which include the following:

6.1 Payment gateway

These platforms allow clients to pay for products and services on the retailer's website. FinTech startups and companies provide their clients with digital wallets and mobile applications to enable them to make consumer retail payments, P2P mobile payments, foreign real-time payments, wholesale corporate payments, and exchange and remittances for products and services online quickly. The digital wallets and mobile platforms are also connected to other payment systems to provide extra features. Popular digital wallets include Google Wallet, Apple Pay, Alipay, Wechatpay, PayPal, Stripe, CitiPay, Venmo, American Express, and M-Pesa. They generate income via transaction fees, exchange fees, and merchant partnerships. These modes of payment are secure, fast, convenient, and multi-channel accessible [13], [20], [93], [94].

6.2 Crowdfunding platform

This is an innovative FinTech solution for raising money conveniently to finance projects and businesses from many people using the Internet and digital payment platforms. Many entrepreneurs, FinTech companies, startups, and established enterprises solicit alternative funds for their businesses, new products and services through crowdfunding because it provides access to a pool of potential investors. The project initiator, the contributors, and the moderating organization are the three main actors in crowdfunding. Reward-based crowdfunding, donation-based crowdfunding, equity crowdfunding, debt crowdfunding, and royalty-based crowdfunding are the different types of crowdfunding models. Examples of popular crowdfunding companies include Indiegogo, Mightycause, StartEngine, GoFundMe, Patreon, Crowdcube, Kickstarter, Fundable, GiveForward, and FirstGiving [13], [20], [93], [94].

6.3 Peer-to-Peer Lending

This online lending platform allows individuals to borrow money by connecting them directly with lenders without relying on a third party like traditional financial intermediaries (banks). They use technology to match borrowers and lenders, facilitate the borrowing and lending process, create loan listings and a decentralized marketplace for loans, and

specify the loan amount, interest rate, and return expectations. Online platforms, direct lending, credit assessment, risk management, and transparency and disclosure are the main features of P2P lending. The leading P2P lending platforms include Prosper Marketplace, Zopa, Funding Circle, Kiva, LendingClub, RateSetter, Peerform, Upstart Holdings, and SoFi. P2P lending earns income by charging fees or taking a certain amount of the loan. They offer several benefits, such as providing loans with lower interest rates, better lending processes for lenders and borrowers, helping investors gain better returns in comparison to debt markets, increased access to loans for underserved individuals or small businesses, and sound investment opportunities for money lenders [13], [20], [93], [94].

6.4 Digital banking

There is broad adoption of digital banking in the FinTech industry because of Internet penetration, wide usage of mobile devices, and mobile banking applications, which come with a wide range of powerful features and services that allow people to check their bank accounts, pay bills, deposit money, transfer money directly from their mobile devices and anywhere as long as there is an Internet connection. PNC Financial Services Group, Narmi, Federal Reserve Bank of Chicago, Leader Bank, and FirstBank are famous FinTech Banks with digital banking. They offer several benefits, such as high security of customers' mobile accounts, convenience, easy usage of mobile banking applications, customers can easily manage and track their financial transactions effectively, less human resource requirements, and reduced transaction rates. Most digital banks implement artificial intelligence and machine learning to secure against fraud and other anti-money laundering software [13], [20], [93], [94].

6.5 WealthTech

This FinTech business model provides clients and enterprises with innovative solutions and services to manage their wealth effectively. It uses artificial intelligence data analysis algorithms to recommend assets for Robo-advisers and wealth managers to invest in based on their needs. This FinTech business model is possible through technologies such as gamification of processes, Robo-advisory, technology-driven wealth, sentiment analysis, and portfolio management tools. The WealthTech business model also provides their clients and businesses with services such as value proposition, target market, technology infrastructure, automated financial planning, investment management, access to markets, financial education and content, regulatory compliance, revenue streams, customer support, partnerships and integrations, and scalability and growth. They generate revenue by charging management fees based on a percentage of the assets under their management and via subscription models. The WealthTech business model has benefited from changing demographics, target market, client behaviour that supports automated investment strategies, regulatory environment, transparent fee structure, and many more. Popular robo-advisors include Betterment, Acorns, Wealthfront, Charles Schwab, Motif, SoFi, Folio, Ellevest, M1 [13], [20], [93], [94].

6.6 InsurTech

In the FinTech industry, InsurTech startups and established businesses use technology to provide innovative insurance services and products to clients more efficiently and with a more significant customer experience, streamlined healthcare billing operations, and better prices for insurance services and products. They employ technologies such as artificial intelligence, machine learning, big data, data analytics, blockchain, and IoT devices to assess risks accurately, understand customer behaviour, provide better customer services, provide personalized policies, insurance products and services, and automate claims processes, and helps to maintain claims faster and more efficiently. Lemonade, Next Insurance, Zego, Hippo, Oscar Health, Policygenius, Acko, Kin Insurance, Root Insurance, Clearcover, GoHealth, Metromile, Coverfox, and Bright Health are the popular InsurTech companies disrupting the insurance industry. InsurTech startups and established businesses earn income through premium policies and partnering with insurance companies. InsurTech solutions allow insurers to expand their data collection and analyze customer data quickly to identify the best policies, improve risk analysis, and make comparing different insurance policies easier [13], [20], [93], [94].

6.7 RegTech

RegTech solutions use technology to comply with regulations and simplify compliance processes within the financial sector. In the FinTech industry, RegTech is applied to know your customer and anti-money laundering, risk management, reporting and compliance, cybersecurity and data protection, and regulatory change management. They use advanced technologies, such as artificial intelligence, machine learning, natural language processing, and data analytics, to help companies swiftly and accurately evaluate compliance risks and find solutions to avoid financial losses, simplify compliance processes, monitor threats, and ensure regulatory adherence. The popular RegTech companies disrupting the insurance industry include Ascent, ComplyAdvantage, Chainalysis, Continuity, Forter, Trunomi, Hummingbird, Sift Science, PaymentWorks, Elliptic, Alloy, Exiger, Symphony Ayasadi AI, BehavioSec. RegTech earns income by licensing its software and providing subscription-based services to its clients. RegTech adoption in FinTech comes with several benefits, such as enabling financial firms to efficiently and effectively comply with regulations, increase efficiency, reduce costs, gain a competitive advantage in the market, improve accuracy, save

firms time and money, enhance risk management, help to detect suspicious patterns in client activity and alerts customers and bank workers in case of fraud, and better regulatory compliance [13], [20], [93], [94].

6.8 Neo banking

Neo banking refers to creating digital banks to offer banking and financial services efficiently and customer-centred without having physical branches. The FinTech, coupled with the COVID-19 pandemic, has contributed to this disruptive innovation of neo-banking in the financial industry, and they are characterized by a digital-first approach, streamlined account opening, enhanced user experience, agile and innovative, lower fees and transparent pricing, strong focus on security, and collaborations with traditional banks. Chime, N26, Wise, Starling Bank, Bunq, Varo, Revolut, and Monzo are the popular global Neo banks. They provide various banking services such as online account opening, current and savings accounts, bill payments, money transfers, savings, loans, online bank account management, and budgeting tools. Neo Banks generate income by charging fees on transactions and interchange and loaning out customer deposits. Neo banking has various benefits, such as fast transactions, user-friendly platforms, high efficiency, instant transfers, flexibility, cost-effective and quality banking services, competitive interest rates, and quick registration. They also provide access to extra services such as investment, insurance, and P2P payments [93], [94].

6.9 Robo-advisors

Robo-advisors are digital investment platforms that use artificial intelligence-based algorithms to provide financial advice, manage investments based on recommendations from investors with less human interference, and automatically generate and maintain investors' portfolios. It involves several processes, including investors' information collection, financial goal analysis, risk profile design, ideal portfolio suggestion, and portfolio management. Robo-advisors use artificial intelligence, machine learning algorithms, robot process automation, big data, portfolio optimization, and other theoretical models to provide investors with intelligent automated investment advice, asset allocation, and portfolio management services based on risk tolerance, income goals and preferences. Wealthfront, Betterment, Robo-Advisor by Schwab, Vanguard Personal Advisor Services, SoFi Invest, Fidelity Go, Acorns, and Ellevest are typical examples of robo-advisors. Robo-advisors generate revenue by charging subscription fees, management fees, account fees, performance fees, transaction fees, wrap fees, and referral fees. They have several benefits, such as providing 24/7 access to low-cost financial advice, improving financial institutions' efficiency, reducing errors, automating investment processes, cheap and easily accessible, providing data-driven decision-making, user-friendly interfaces, adhering to regulatory standards, providing targeted services to meet investors' personalized asset allocation needs, conducting accurate financial analyses of customers who wish to invest, and creating a customized portfolio on the web for the investors [13], [20], [93], [94].

6.10 Blockchain and Cryptocurrency

With blockchain technology in FinTech, financial records are stored in a distributed and decentralized ledger, making the data difficult to alter or modify. Many blockchain-based startups and established companies use distributed ledger technology to offer solutions to various financial services such as digital currencies, smart contracts, and supply chain management. These startups and established companies make revenue by charging transaction fees, licensing blockchain technology, and providing value-added services together with the blockchain. Blockchain and cryptocurrency offer several opportunities, such as decentralization, efficiency, secure transactions, efficient cross-border payments, transparency, smart contracts, tokenization of assets, initial coin and security token offerings, financial inclusion, and data security and privacy [13], [20], [93], [94].

Figure 5 shows the summary of the FinTech Business Model.

7. FINTECH APPLICATION

The significant applications of FinTech include electronic commerce, digital banking, digital payments, Robo-Advisory, InsureTech, RegTech, wealth management, online lending, crowdfunding platforms, personal finance and budgeting, cryptocurrency and blockchain, cloud computing solutions, social media, Neobanking, artificial intelligence, big data analytics, robotics process automation, and many more [11], [95-97]. Despite the growing demand for FinTech due to the benefits it offers, disruptive innovation suffers from cybersecurity issues that interrupt their indispensable business services, harm mobile devices, servers, and computer networks, damage the reputation of FinTech firms and startups, and cause financial losses to clients, startups, and firms.

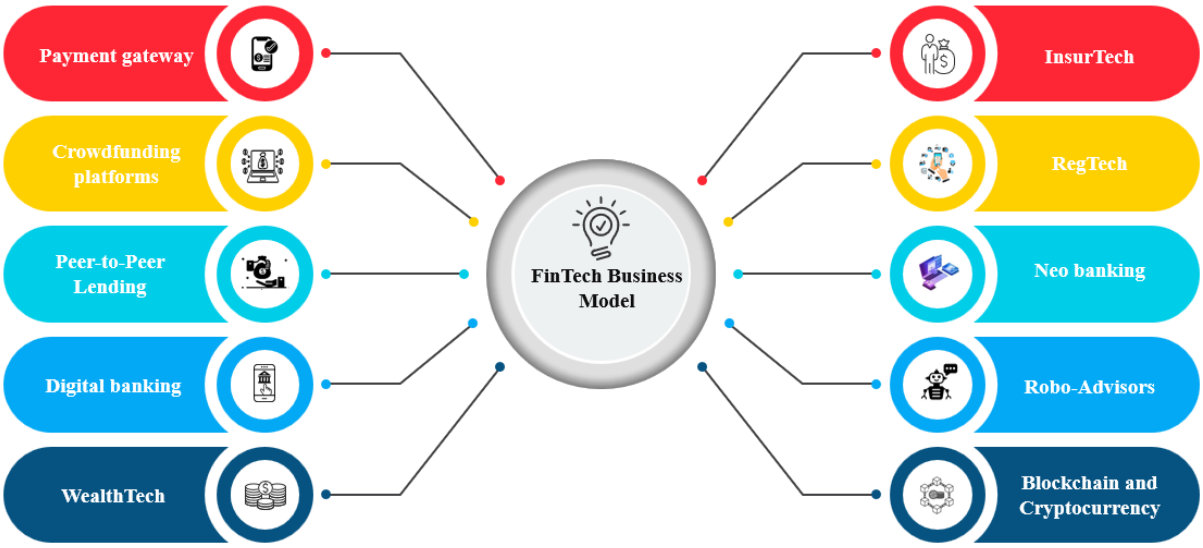

Figure 5. The summary of the FinTech Business Model

8. CYBERSECURITY ISSUES

With the advent of emerging technologies, cybercrimes in FinTech are constantly rising because hackers are using modern strategies such as malicious codes and sophisticated software to alter the FinTech systems and secret codes that can compromise the data. In FinTech, cybercrime is fraudulent activity perpetrated using mobile devices and other networking tools to compromise the integrity of FinTech systems, cause reputational damage and financial loss, cause fear and anxiety to clients, compromise sensitive data, and destroy technology. Cybersecurity statistics show that 2,200 cyber-attacks occur daily every 39 seconds [98], and cybercrime costs will be $23.82 trillion by 2027 [98], [99].

Cybercriminals target FinTech-enabled mobile payment services to compromise their confidentiality, integrity, availability, authenticity, authorization, non-repudiation, accountability, and auditability [100], [101]. The security principles in FinTech that must be maintained include:

- *Confidentiality*

Confidentiality protects FinTech's sensitive login credentials and financial information during acquisition, transmission, or storage from passive attacks or being shared by unauthorized people or systems [102]. Therefore, it guarantees that authorized people and entities can only access, use, edit, share, or delete sensitive information [103]. FinTech confidentiality is compromised if an unauthorized person accesses the sensitive information it stores, and it is the most attacked security service.

- *Integrity*

Integrity is a security principle that ensures sensitive login credentials and financial information are not modified or destroyed during collection, processing, transmission, or storage without permission [102-104]. It must ensure that the information transmitted via wireless communication and received at the intended destination by FinTech systems, applications, networks, and users is completely uncompromised and accurate.

- *Availability*

Availability is a security service that ensures that FinTech systems, networks, services, and information are accessible and reliable to authorized users and systems [102-104].

- *Authenticity*

Authenticity is a security principle that validates and verifies users' identities, and only authorized users are granted access to the FinTech system, services, and network. It helps to thwart impersonation by requesting users to prove their identities before accessing the systems and their resources.

- *Authorization*

Authorization is a security service that determines or permits what actions or resources FinTech users can access based on their access control policy, rights, and privileges. After successful user authentication, authorization is performed.

- *Non-repudiation*

Non-repudiation is a security principle where there is proof that the information has been sent, and the recipient of the information is provided with the sender's identity so that, in future, the parties cannot deny having sent or received

information. In FinTech, this security principle helps prove the identities of the users who performed a service, and the FinTech firm cannot deny having received payments for the service offered to the user [104].

- *Accountability*

Accountability is a security service that audits the actions and processes of all the users or parties that interacted with the FinTech systems/applications, and each action and process can be traced uniquely to each user or party.

- *Auditability*

Auditability refers to the security principle that verifies the activities in FinTech systems, applications, and networks.

The imminent cybersecurity issues faced by FinTech startups, established companies, and clients are discussed below.

8.1 Privacy issues

Ali et al. [105] define privacy in FinTech as the state where others do not violate a customer's rights. However, in the FinTech industry, most of the employees' and clients' rights are infringed on by both disgruntled insiders and outsiders. The typical privacy issues include (1) the disclosure of confidential FinTech clients' financial and personal records by the FinTech companies without their concerns, and selling clients' data to third parties threatens their privacy. For example, Alipay has been accused of disclosing its clients' personal information to a third party without informing its customers [57], [98], [105]; (2) in FinTech, customers perform mobile transactions using their mobile devices, and these devices can be stolen and hacked, thus exposing their payment information which cybercriminals can use to commit fraud and identity theft. For example, in the USA, Dave mobile banking provider was attacked by hackers who illegally accessed the clients' data [59], [106]; (3) some clients typically request FinTech companies to use their account information to perform some tasks on their behalf and in case such information lands in the hands of disgruntled employees, they can use them to conduct illegal transactions thus invading the client's privacy [107-109]; (4) FinTech services providers collect, process and analyze the customers' data and if such data is not securely stored, their privacy can be violated ; (5) some employees of the FinTech companies and startups steal customers' data and sell them to the company's competitors for their gains, therefore, violating customers' privacy [57]; (6) the confidentiality of FinTech startups, clients, systems or networks can be breached through cyber-attacks such as physical, replay, masquerade, and many more; and finally, (7) FinTech startups and established companies usually develop web applications and APIs for their clients to use. In case they are abandoned, and attackers and disgruntled employees gain access to such abandoned applications and APIs together with the data stored in them, they can be sold to third parties.

8.2 Data breaches

With the digitization of businesses and financial institutions, FinTech firms and startups use innovations for financial transactions, leading to increased financial and client data breaches. The data breach, also known as data leakage, information leakage, and data spill, refers to a security incident where attackers, hackers, and disgruntled employees illegally or unintentionally access and leak clients' confidential financial and personal information stored in the FinTech company database(s), servers, computers, mobile devices, and other storage devices to suspicious party [18]. Globally, cybercriminals always target financial institutions such as banks and credit card companies to have access to their financial records. Since the FinTech system databases store financial data like payment card information and customer credentials, they are prone to data leakages and breaches [66-68], [80]. Some of the common FinTech data breach incidences include (1) According to the investigation, which was completed on 2 June, 2022, Flagstar Bank, a financial provider in the United States, experienced a massive data breach in December 2021, exposing 1.5 million customers' social security numbers, banking information, and customer information such as names, addresses, and birthdays; (2) Revolut, a FinTech startup known for its banking app suffered a data breach where 50,150 customers globally and 20,000 in Europe had their names, email addresses, telephone numbers and payment card data, compromised by a third party who accessed Revolut's database through social engineering methods; (3) On April 2022, Block, a FinTech startup experienced a data breach where 8.2 million customers' full names, brokerage account numbers, brokerage portfolio values, brokerage portfolio holdings, and stock trading activity for one trading day were leaked; (4) In August 2020, Experian South Africa, a leading FinTech startup experienced a data breach where an attacker who claimed to be a representative of one of Experian's clients persuaded the employees of the company to reveal customers' confidential data such as their mobile phone numbers, home phone numbers, work numbers, email addresses, residential addresses, places of work, work addresses, job titles, and job start dates, which they later used for creating marketing and leads for insurance and credit-related services. This resulted in the identity theft of 200 million customer records and a loss of US$1.3 billion; (5) First American Financial Corp data was breached in May 2019, where over 885 million financial and personal records related to real estate transactions were exposed over a website design error; and (6) Equifax, an American multinational consumer credit reporting agency, also had its data breached where 147 million US accounts and 200,000 credit card numbers were illegally accessed. This data breach was due to

an internal process where Equifax failed to renew the encryption certificate on one of their security tools, making it easy for the hackers to extract data in encrypted form without being detected [18], [23], [110].

8.3 Malware attacks

Cybercriminals launch malicious software to encrypt, delete, alter, monitor, and steal confidential information and registry files; disrupt and damage mobile devices, servers, and computer networks; and gain unauthorized access to FinTech applications and networks [66-69], [80]. Malware is constantly evolving, and it infects systems either by tricking authorized users into downloading and installing them by opening an infected file, visiting malware-spreading websites or connecting to a computer infected with malware without their knowledge [102]. Cross-platform malware has been developed to spread and infect the various FinTech platforms [23]. Petrosyan [111] reported that between October 2021 and September 2022, the common cyber-attack among financial and insurance organizations was malware, which attacked 40% of the organizations globally. Twenty-two million devices and 721.5 million credentials are exposed to malware by cybercriminals [112]. In 2022, 61% of consumers and 39% of corporate users in FinTech were targeted by financial malware attacks globally [113]. The number of mobile devices infected with mobile malware has increased, and mobile banking malware is rampant in countries such as Bangladesh, Nigeria, India, Indonesia, Pakistan, Tanzania, Kenya, Philippines, Russia and many countries in Central, South and East Asia because of increase in the use of FinTech services. For example, Emotet and Zeus banking malware are used to steal banking credentials and spread other malware. Globally, banks and financial institutions use SWIFT systems to transfer financial information securely. Hackers target and infect SWIFT/ATM infrastructure in India with malware after detecting vulnerabilities in the banking system. In February 2016, cyber criminals hacked into the Central Bank of Bangladesh using APT malware, stole the credentials to access the SWIFT system and successfully requested to transfer a foreign exchange reserve of US$81 million owned by the Central Bank of Bangladesh from the Federal Reserve Bank of New York. When such malware is executed, it can transfer money from any bank and financial institution globally [114]. In 2018, hackers also used the same method used in the Central Bank of Bangladesh to steal close to US$2 million from the City Union Bank of India and also from other banks in South America [114]. Likewise, Attackers in Taiwan used malware to steal over 70 million new Taiwan dollars from teller machines. Hackers typically, after compromising the network and computer systems, can install and spread the malware in the network and the victim's mobile devices to create a backdoor that can be utilized for accessing the victim's confidential information such as usernames and passwords, and credit card numbers and bypass authentication and verification processes [64], [114]. The common malware in FinTech is classified into Ransomware and Trojan horses [18], [102], [115].

- **Ransomware**

Ransomware is an evolving and skyrocketing concern in the global FinTech industry. Ransomware is defined as malicious software that cybercriminals release to compromise their victims' computers, mobile devices, servers, and networks by encrypting files, data, directories or the entire system so that they become inaccessible to legitimate users unless a considerable amount of ransom is paid in dollars, cryptocurrency or other currencies in exchange for the decryption key [99], [102], [115], [116]. In most cases, ransomware attacks target FinTech companies because they contain vast amounts of confidential data, and such attacks ordinarily last for more than 24 hours [62], [67], [69], [80]. Between 2021 and 2022, many FinTech companies were hit by ransomware attacks [18], [64], [99]. Cybercriminals use multiple channels, such as phishing emails, social engineering, and exploit kits, to deliver ransomware attacks [99]. In 2022, there were 236.7 million ransomware attacks globally; 72% of IT officers made payments in the form of ransom to recover from such attacks, and global ransomware damage is estimated to cost US$265 billion by 2031 [117]. The most common ransomware attacks in the FinTech industry include (i) AON ransomware attacks: On 25 February 2022, AON, a global insurance and reinsurance broker, was attacked by ransomware, which resulted in limited disruption to their services; (ii) Finastra ransomware attack: On 20 March 2020, Finastra FinTech company received information about a ransomware attack that could disrupt the company's critical services for North American clients and the company decides to control the attack by shutting down their servers; (iii) WannaCry and NoPetya ransomware attacks caused disaster in the financial stability of prominent FinTech companies [18], [110]. The most significant ransom payment was the US$40 million paid by CNA Financial Corporation to hackers for reclaiming its data in 2021.

- **Trojan horse**

With the increasing number of FinTech applications, the volume of financial data keeps growing, thus attracting the attention of cybercriminals. They use malware, such as a Trojan horse, to infect the victims' mobile devices and steal data. Ahsan et al. [102] and Rapti et al. [115] define a Trojan horse as malicious software masquerading as a legitimate program. However, once the users download and install them on their mobile devices, they can copy, modify, delete, and steal confidential financial data from their devices and create a backdoor for the attackers to access the mobile devices. The attackers use social engineering techniques like spoofing and phishing to influence users to install Trojans into their mobile devices. The most common Trojan horses include the Trojan banker, Trojan dropper, Trojan-SMS, and Trojan spy [18]. There is an increase in mobile banking Trojans in the FinTech industry infecting the clients' mobile devices and payment applications. They intercept SMS-based authentication, finger taps, and

fingerprints and send them back to cyber criminals to take control of mobile banking and perform fraudulent transactions, bypass security measures implemented by banks, and also incorporate infostealer and remote access Trojans capabilities to collect customers' online banking credentials such as bank accounts, credit/debit card numbers, and other electronic payment details. According to the report by Kaspersky, there was a global increase in mobile banking Trojans, with 196,476 detections by 2022. More than 190 disguised legitimate applications are available in official application stores, spreading Harly Trojan, which has gained over 4.8 million downloads [118]. For example, the Google Play store has downloaders for banking Trojans like Sharkbot, Anatsa/Teaban, Xenomorph, and many more, all masquerading as utilities. Examples of mobile banking Trojans include (i) Zanubis banking Trojan, which has targeted over 40 applications; (ii) Zeus Trojan, which infects banking systems and steals confidential information such as customer's banking credentials; (iii) Qakbot steals users' banking credentials and keystrokes; (iv) AhMyth which is a remote access trojan to gather confidential information from the users' devices and perform actions like keylogging, sending SMS, taking screenshots, and activating the camera; (v) Anubis which is remote access trojan that performs actions such as keylogging, audio recording; (vi) Hiddad; (vii) Zloader banking Trojan; and (viii) Godfather Trojan that infects over 400 Android-based banking and cryptocurrency applications. It captures clients' input data and sends notifications to unsuspicious clients to collect codes for the two-factor authentication security system, which is sent to cybercriminals to access customers' wallets.

8.4 Hacking

Lately, there has been an increase in the hacking of FinTech applications and systems because of the widespread use of mobile devices like smartphones to access FinTech services. Hacking refers to the unlawful activities performed by cybercriminals to compromise mobile devices and networks to illegally gain access to confidential information such as usernames and passwords, debit and credit card numbers, bank information, and other personal details. Once the hackers access the stolen sensitive data, they can fraudulently withdraw money from their victims' accounts [119]. During the COVID-19 crisis, there was an increase in the attacks on FinTech systems by hackers, such as bank loan scams where bank customers were sent SMS requesting them to fill out an online form with their bank details, resulting in their bank accounts being hacked [119]. FinTech applications and systems are better understood by hackers than IT officers, thus making it easy for them to be compromised. In FinTech, hackers can use different methods such as attacking the FinTech applications and networks directly by spreading zero-day malware, which creates a backdoor for them, Internet protocol (IP) spoofing, social engineering techniques, port scanning, packet sniffers, password cracking, buffer overflow attacks, and many more [23], [63], [120]. Nivedita [117] reported that hackers stole US$29 million from a FinTech company and US$3 billion worth of cryptocurrency. The primary motives behind hacking in FinTech are espionage and disruption of services. There are several hacking incidents on FinTech, including (1) On 17 January 2022, hackers exploited the weaknesses in Multichain – a platform to swap tokens between blockchains - and stole about US$1.4 million. Hackers also used social engineering and exploited the vulnerabilities in Mailchimp to get confidential information from MailChimp employees, customers, and hardware cryptocurrency wallets; (2) On 31 October 2020, cyber criminals hacked into Cermati, an Indonesian FinTech company's system and stole 2.9 million clients' information such as clients national ID numbers, taxpayer registration numbers, bank accounts, full names, email addresses, physical addresses, occupations, company name, mothers' names, and phone numbers, which was later leaked and sold in a forum owned by hacker for US$2,200; (3) On 3 October 2020, Pegasus Technologies, a company that processes mobile money transactions for MTN Uganda and Airtel was attacked by hackers who made mobile money transfer services be suspended temporarily in Uganda and over US$3.2 million was stolen during the hacking; (4) On March 2019, Paige A. Thompson, a former software engineer of AWS hacked the servers of AWS which had data for Capital One and this affected over 100 million people in the United States and over 6 million in Canada. The hacker used firewall misconfiguration to access the personal information database hosted by AWS. The data stolen included American social security numbers, Canadian social insurance numbers, bank account numbers, and other relevant information such as peoples' names, addresses, credit scores, credit limits, balances, and many more. He later uploaded the data on GitHub, and this attack made Capital One incur costs between US$100 million and US$150 million as damages [18], [121]; (5) In December 2019, Chile's ATM interbank network, Redbanc, was hacked by cybercriminals after convincing the Redbanc employee during a fake Skype job interview to download a malicious program for submitting his application form. After successfully downloading and installing the malicious program, the hackers used it to access Redbanc's network; (6) On September 2017, hackers exploited the weaknesses in a software owned by Equifax and hacked the system and stole confidential customers' information such as customer names, phone numbers, social security numbers, home addresses, date of birth, and driver's license numbers. This attack was claimed to have been committed by four members of China's military and affected over 147.7 million Americans. (7) On 19 December 2017, a South Korean cryptocurrency exchange, YouBit, was hacked two times that year, which led to 17% of its digital currency being stolen. The company later pronounced itself bankrupt and stopped trading due to the attack [110]; and (8) On February 2016, anonymous hackers used fraudulent orders on the SWIFT payments system and transferred a foreign exchange reserve of US$81 million owned by the Central Bank of Bangladesh from the Federal Reserve Bank of New York and sent to accounts at Rizal Commercial Banking Corp [114], [119], [121]. Due to the latest technologies hackers use to hide their identities, data security in FinTech is still a significant concern [5].

8.5 Insider threats

Because of the increased collaboration tools and remote working, insider threats have become a primary cybersecurity concern that FinTech startups and established businesses must address. Gurdip et al. [18] and Saxena et al. [122] define insider threat as a malicious threat perpetrated by the organization's employees, disgruntled employees, former employees, partners, contractors and business associates who have information about the organization's security practices, systems, data, and authorized access to computer and network systems. Insider threats in FinTech can be (i) malicious insider threats - committed by authorized employees and other people who are granted the rights and permissions to access, write, read, and transfer confidential financial information from financial institutions. Malicious insider threats include disclosing sensitive financial data or abusing their privilege of accessing the FinTech systems for personal interest or causing damage and disruption to the FinTech systems and applications; (ii) negligent insider threats such as unintentional errors by employees or dangers created by their actions due to ignorance [122]; and (iii) compromised insider threats - which are perpetrated by people who have authentic access to the organization's systems and networks but whose authentication credentials have been seized by cybercriminals. The cybercriminals then use the seized insiders' credentials to access FinTech's systems and perform malicious activities as if legitimate employees performed them. Since the insiders know how the FinTech systems and applications work, it becomes difficult to detect such frauds if they intentionally or unintentionally compromise the system and data [69]. McKnight and Tipton [123] reported that between 2020 and 2022, the global insider threat incidents rose to 44%, and the cost for each incident was US$15.38 million. Examples of insider threats in FinTech include (1) In May 2022, Qian Sang, a research scientist with Yahoo, stole Yahoo's AdLearn product intellectual property information by downloading the 570,000-page document on his mobile device after receiving a job opportunity from Yahoo's competitor, the Trade Desk. Yahoo believes that Sang's action will give the competitor control of Yahoo's trade secrets; (2) On 27 October 2020, an employee working as a credit analyst for ABSA South Africa sold 200,000 confidential customers' personal information such as account numbers, identity numbers, names and surnames, addresses, contact details, and financial data to third parties that could have used them to commit fraud; (3) In June 2019, a Canadian financial service cooperative, Desjardins Group, had its data breached by a disgruntled employee who illegally accessed the social security numbers, names, email addresses, and transaction records of 4.2 million associates and made the company pay costs worth US$108 million for damages; and (4) On March 2019, Paige A. Thompson, a former software engineer of Amazon Web Services (AWS) illegally accessed the servers of AWS which had data for Capital One, and this affected over 100 million people in the United States and over 6 million in Canada. This data breach negatively damaged Capital One's brand reputation, causing a 5% decline in sales, and the company paid costs worth US$150 million for damages [18], [110].

8.6 Identity theft

Identity theft proliferates in the FinTech industry, costs FinTech startups billions of dollars, and discourages people from using FinTech services [42], [124]. Identity theft in FinTech refers to a criminal act where attackers steal or fraudulently obtain customers' personally identifiable information such as personal identification numbers (PINs), usernames and passwords, ID numbers, credit card numbers, social security numbers, driver's license numbers, and other identifying information, to impersonate as their victims and misuse them for committing fraud and other crimes. Most FinTech startups have applications that can be accessed by their customers using mobile devices, and they have become targets for cybercriminals. The adversaries use hacking, phishing, malware, pharming, API attacks, traffic redirections, shoulder-surfing, and keyloggers to access their victims' personally identifiable information [66-68], [124]. Petrosyan [125] reported that 43% of the victims of identity theft spend their time solving the issue, and 33% freeze their credit cards. US companies are estimated to lose US$635.4 billion due to identity theft in 2023. Examples of identity theft in FinTech include (1) On 4 December 2021, hackers attacked Bitmart, a crypto trading platform, stole the private key of Ethereum and Binance smart chain hot wallets and withdrew US$150 million in assets; (2) On 12 June 2021, cybercriminals attacked Intuit, an American financial software company, and compromised TurboTax customers' personal and financial data in their account takeover and later on fraudulently gained access to their victims' accounts using the stolen credentials; and (3) On 16 August 2021, a cybercriminal was arrested by Nigeria's police for quickly hacking Access Bank and First Bank of Nigeria. They withdrew money from the bank accounts using missing or stolen subscriber identity module (SIM) cards [110].

8.7 Social engineering attacks

Social engineering is the most common attack in the FinTech industry since it is easy for cybercriminals to exploit FinTech customers and startups. A social engineering attack is a malicious act by cybercriminals to psychologically manipulate customers into divulging confidential information such as PINs, usernames and passwords, credit card numbers, social security numbers, and other identifying information to illegally gain access to systems and networks, access their victims' funds and take over their accounts [105], [126]. The popular and well-known social engineering attacks in FinTech are phone calls or emails claiming to be from FinTech startups to update customers' account details or fake support to solve technical problems with the FinTech systems and applications that require customers' confidential information. Sometimes, cybercriminals install malware that can be remotely accessed to monitor and

exploit their victims' mobile devices and FinTech applications and make fraudulent payments [69], [80]. Hossain et al. [72] reported that social engineering attacks contribute to 29% of all breaches. Seventy-five per cent of security professionals agreed that social engineering is a dangerous threat, and hackers use it to attack Twilio and illegally access customers' data and the company's internal systems [117]. The common cases of social engineering attacks in FinTech are when (i) cybercriminals utilized social engineering techniques and counterfeit websites like fake iOS App Store and iOS app-testing websites to spread 167 counterfeit Android and iOS financial trading, banking, and cryptocurrency applications to gullible users to steal money which a cybersecurity firm 'Sophos' later identified on 12 May 2021; and (ii) the use of social engineering techniques by the Carbanak group to steal money from the bank. The group sent spear-phishing emails with Carbanak backdoor attachments to bank employees to allow them to collect information related to the bank's financial tools and the fund transfer system to US$1 billion. The most common form of social engineering attack in FinTech is phishing.

- **Phishing attacks**

Phishing is a severe, widespread threat responsible for almost all data breaches in the financial sector. It is where cybercriminals masquerade as credible organizations or employees of FinTech startups and use deceitful emails, text messages, phone calls, and websites with malware downloads to acquire confidential information such as PINs, usernames and passwords, credit card numbers, social security numbers, bank account numbers, and online banking and company login credentials from customers or take actions that subject the customers and startups to cybercrimes or transfer money to the attackers [18], [99], [102], [126]. FinTech startups are targets of phishing scams due to the increased number of clients using their services. During the COVID-19 pandemic, phishing was rampant among FinTech, and attackers could use it conveniently and cheaply to trick their victims into revealing their confidential information, leading to increased identity theft [66], [67], [68], [80], [114]. Cybercriminals in FinTech use several forms of phishing, such as whaling, classic phishing, SMS phishing (Smishing), voice phishing (Vishing), and angler phishing [64], [105], [126]. Nivedita [117] reported that phishing attacks are the most common cybercrime in the financial sector; over 255 million attacks occurred in 2022, costing companies over US$4.91 million. The prevalent cases of phishing attacks include (1) On 23 December 2021, cybercriminals attacked OCBC Bank of Singapore using phishing, where a link was sent to the bank customers requesting them to type in their credentials. Seven hundred ninety customers' bank accounts were compromised, and over US$13.7 million was drained from them; (2) On 6 November 2021, the developer of bZx, a decentralized finance platform, was sent a phishing email with an attached malicious Word document. The attackers compromised the developer's mnemonic wallet phrase and drained US$55 million from their wallet. They also stole two private keys for bZx's polygon and Binance smart chain blockchains; (3) On 22 September 2021, researchers reported that attackers used phishing techniques to install the Drinik banking trojan malware on Android phone banking used by India's customers. The malware was able to steal customers' confidential data and money; (4) Researchers also report that between May and August 2021, there was a 300% rise in phishing attacks on Chase Bank. The cybercriminals developed XBALTI phishing kits that impersonated the Chase banking portal and were able to collect customers' social security numbers, email addresses, passwords, banking and credit card information, and home addresses. (5) On 19 February 2021, investors of Sequoia Capital - an American venture capital firm – were warned about a phishing attack that led to personal and financial information breaches; and (6) On 11 October 2020, attackers used phishing to target the accounts of 4000 customers of BetterSure - a South African home insurance company. They used a phishing email to access the internal email accounts of the employees of the BetterSure administration [110].

8.8 Distributed Denial-of-Service (DDoS) attacks

There has been an increase in the volume and intensity of DDoS attacks in the FinTech sector because of the lack of rate limits and resource restrictions in FinTech applications. Alsumaidaie et al. [65] define a DDoS attack as an attack where cybercriminals use hijacked Internet-connected devices known as zombies or botnets to overwhelm the FinTech systems, applications, and networks with fake traffic so that they become unavailable for intended users and disrupt the normal operations of the FinTech services. In DDoS attacks, the phoney traffic that overwhelms FinTech systems, applications, and websites comes from several distributed sources, thus shutting down the services and depleting resources and bandwidth [105]. Defending against DDoS attacks is often difficult because the attackers use many zombies to send fake traffic to their targets. Some FinTech companies hire cybercriminals to carry out DDoS attacks, also known as "DDoS-for-hire service", against their competitors or purchase them from the dark web so that they can be out of the business [127]. Cybercriminals use client/server architecture, multiple compromised online devices, malware, and botnets (such as Andromeda and Conficker botnets) to orchestrate DDoS attacks by sending several fake traffic requests targeting FinTech networks, systems, applications, and websites or overwhelm the general network [18], [127]. It is reported that global DDoS attacks will reach 15.4 million by 2023. In 2022, more than 60% of malicious DDoS attacks, including those on financial institutions, rose by 22% [117]. The most common examples of DDoS attacks in the FinTech industry include (1) On 28 February 2022, a crowdsourced community of hackers known as the "Ukrainian IT Army" formed by the Ukrainian government launched DDoS attacks on the Moscow Stock Exchange and Sberbank and put their websites offline; (2) On 15 February 2022, cybercriminals launched DDoS

attacks on Ukraine's defence ministry web portal and the state-owned banking and terminal services which were taken down; (3) On 8 September 2021, cybercriminals took down the websites of Australia and New Zealand Banking Grp Ltd and Kiwibank and the national postal service through a DDoS attack; (4) On 23 September 2020, cybercriminals used computer servers in Russia, China, and Vietnam to launch a powerful DDoS attack on several Hungarian banking and telecommunication services that disrupted their services; (5) On 25 February 2020, a group of cybercriminals called the "Silence Hacking Crew" used DDoS attacks to attack Australian banks and other financial institutions and demanded ransom to be paid in Monero cryptocurrency to stop the attack; and (6) On 6 September 2019, attackers used DDoS to send a massive volume of traffic to overwhelm the website of Hong Kong Exchanges and Clearing Limited (HKEx). The attack slowed the website and displayed limited information about exchange rates [110].

8.9 Cryptojacking

The value of cryptocurrency and the availability of cloud computing resources have resulted in the growth of cryptojacking, which has become prevalent in the FinTech sector. According to Gurdip et al. [18], cryptojacking is a cybercrime where attackers illegally install malware or use their victim's computing resources to secretly mine cryptocurrencies without incurring electricity, hardware and other mining resource costs. Attackers use several methods to cryptojack their victims, such as (1) sending a phishing email with a malicious link to their victims and convincing them to click the link. Upon clicking the malicious link, malware is automatically loaded and runs in the background of the victims' machines [18]; (2) injecting a cryptomining script on a website and ads sent to several websites. When their victims visit such websites, the infected ads are displayed in their web browsers, the implanted cryptomining script is automatically executed on their computers, and cryptomining is run on behalf of the attackers. If new blocks are successfully added to the blockchain, the attackers receive rewards in the form of cryptocurrency coins or steal from cryptocurrency wallets; and (3) access or steal cloud platform login credentials of FinTech startups to help them log into the cloud environment and run cryptojacking code to acquire vital resources on a large scale from the company's cloud platform(s). The specified allows the attackers to mine crypto faster and on a bigger scale [99]. Nivedita [117] reported that in 2022, there was a 269% increase in cryptojacking attacks on the financial sector and 139.3 million cases of cryptojacking. The massive cryptojacking attack cost US$615 million, and hackers stole US$3 billion worth of cryptocurrency in 2022. Cryptojacking is common because cybercriminals find it simple to implement, straightforward and less risky. The attack can be detected when the victim's computing resource performance decreases, overheats, the central processing unit is used more than once, and there are changes in the web page. The typical examples of cryptojacking include (1) On 1 January 2021, Pro-Ocean, an improved version of cryptojacking malware that has better worm and rootkit abilities, was launched by a Chinese cybercrime group called Rocke targeting cloud applications such as Apache ActiveMQ, Oracle WebLogic, and Redis to mine Monero cryptocurrency; and (2) In 2019, cybercriminals launched cryptojacking on eight applications which were found in the Microsoft Store. The applications had corrupt JavaScript codes and were trained to mine Monero cryptocurrency. Microsoft Store identified and removed the eight applications after consuming massive resources, such as decreased performance from the target devices [110].

8.10 Supply chain attacks

FinTech startups integrate several third-party products and services into their ecosystem, which have become a target of many cybercriminals. Managing these cyber threats in the supply chain has become a serious security challenge. Supply chain attacks, third-party attacks, value-chain attacks or backdoor breaches are emerging and progressively spreading and becoming sophisticated cyber threats. A supply chain attack is a cyberattack where cybercriminals infiltrate the FinTech system and network through trusted third-party(ies) who have access to the FinTech startup's data and system. Due to the new types of attacks, supply chain attacks are increasing, and the attackers focus on the weaker links in the FinTech startup's supply chain, such as the third-party providers or their products and services other than the FinTech startup [69]. Nelson [128] reported that in 2022, there was a 15% rise in supply chain attacks worldwide, and the average attack cost was US$4.4 million. Eighty-four per cent of IT and security experts think software supply chain attacks will be among the top cyber threats in the coming years. Cybercriminals start carrying out supply chain attacks by identifying weaknesses and flaws in the supply chain, such as insecure protocols, software bugs, insecure coding practices, defenceless server infrastructure, misconfigurations, and many more. They then exploit vulnerabilities by injecting malware, like a keylogger, to infect the third party. The malware will create a backdoor for the attackers or steal login credentials for unauthorized access to the FinTech startup's system and confidential company and customer transaction information. The malware can also modify the source codes and release malicious patches to infect all the people using the service(s), which are difficult to detect and prevent. Supply chain attacks can be implemented by (i) compromising the third-party software or hardware, (ii) infecting the computer's booting code or software updates with malware, and (iii) interfering with hardware parts. Compromising the trusted third party in the supply chain makes it easy for attackers to infiltrate the target FinTech startup and bypass the security system. The typical examples of supply chain attacks in the FinTech industry include (1) In 2021, the REvil ransomware gang used two vulnerabilities in the Kaseya software to launch a supply chain ransomware attack by installing ransomware via a malicious patch from Kaseya's VSA server, which propagated to

servers managed by Kaseya in networks of managed services providers (MSPs). The attackers used the servers as back doors so that the victims could not detect or prevent the infection as it spread, and they managed to compromise and encrypt thousands of nodes in many firms. The gang then asked for a ransom of US$70 million to provide decryption keys for all affected MSPs and customers; (2) In 2020, a group of hackers used a supply chain attack to infiltrate SolarWinds' production environment by embedding a backdoor called SUNBURST into Orion's network monitoring product via a software update. The update and the backdoor were downloaded and installed by 18,000 customers, leading to massive data breaches and security issues. The backdoor made it easy for hackers to masquerade accounts and clients of victim organizations and have remote access to corporate and government servers and system files. (3) In November 2020, Check Point Research identified several vulnerabilities in Atlassian applications that attackers could exploit to gain access by using a single sign-on token and then performing fraudulent activities on the client's account. Many organizations that use Atlassian's solutions were affected by this attack; and (4) In 2018, a hacker group "Magecart" launched a supply chain attack on British Airways using virtual card skimming software that compromised the airline's third-party vendor which later spread to British Airways, Ticketmaster, and other firms. The attack made it easy for the hackers to access the British Airways website and mobile app, disrupted the trading system, and leaked and stole over 380,000 transactions on the airline's website and customers' confidential information such as passenger names, home addresses, email addresses, and credit card details [110].

8.11 Advanced Persistent Threat (APT)

Advanced persistent threats continue to evolve, posing a dangerous security threat for financial institutions. Jabar and Singh [129] and Genge et al. [130] define the APT as a type of cyberattack where cybercriminals use innovative hacking techniques to illegally access and hide their presence within a FinTech startup's system and network for a long time while performing various activities such as monitoring, intercepting and stealing highly confidential information, infecting hosts with malware, spreading malware from one network to another, and altering the behaviour of essential network components. The attack is executed by hackers who have vast knowledge and have carefully planned to infiltrate the target FinTech startup's system and network while evading the existing security measures, thereby making it very hard to detect and stop, thus increasing costs for the organization since they act stealthily. There are several phases involved in APT, which include (1) gaining access to the FinTech startup's system and network by using malicious files, junk email, a susceptible application, and weak spots on the network; (2) establishing a Foothold by in planting malware that can enable the attackers to establish a network of tunnels and backdoors that will help them to traverse within the FinTech startup's system and network undetected; (3) intensifying access to the FinTech startup's system and network by compromising administrator login credential which will help the attackers to manipulate the startup's system and network and obtain control and authority; (4) staging the attack; and (5) exfiltrating the data and clean-up. They prepare how to transfer the captured information to their outside system for analysis without detection. This can be done via a compromised system or the encryption of sensitive data to make it unrecognizable. Attackers will conduct DoS/DDoS attacks to distract the FinTech security team from detecting them while transferring the information to the outside system and then remove data transfer evidence. In 2022, it was reported that APTs are among the prevalent cyberattacks targeting finance, healthcare, and government sectors. On average, US$4.27 million is spent on APT, and the damage is estimated to cost US$10.5 trillion by 2025. The APT protection market will increase at a compound annual growth rate (CAGR) of 16.6% and is estimated to reach US$21 billion in 2027 [129]. Cybercriminals use several techniques to initiate APT in FinTech, such as employing zero-day exploits, social engineering, vendor attacks, ransomware, physical access, phishing, malware, rootkits, watering holes, exploit kits, spear phishing, DNS tunnelling, SQL injection attacks, rogue Wi-Fi, exploiting software vulnerabilities, drive-by-downloads, encrypted communication channels, and others [129]. The most prominent banks and other financial institutions worldwide are victims of APT. The typical examples of APT in the FinTech sector include (1) On June 2023, Lazarus Group (APT38), a North Korean hacking group, attacked Harmony's Horizon Bridge, a California-based crypto firm, using APT and stole US$100 million in cryptocurrency. The group has reportedly stolen US$600 million from the Axie Infinity-linked Ronin-bridge. APT38 is known for targeting banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT system endpoints, and ATMs in more than 38 countries globally. The group is reported for attempting to steal over US$1.1 billion; and (2) Since 2018, a hacking group known as Evilnum (APT TA4563) has been targeting financial institutions that use FinTech platforms. The hacking group uses social engineering, spear-phishing, and custom-built malware to target FinTech platforms that support foreign exchanges, cryptocurrency, and decentralized finance (DeFi). The spear-phishing emails used by APT TA4563 infect FinTech platforms and other devices with the Evilnum malware and other malicious code. After infecting the FinTech platforms, it can steal confidential information such as passwords, customer records, credit card numbers, browser cookies, email credentials, and many more.

8.12 Zero-day attacks

Zero-day attacks are becoming more common in the FinTech sector, and they are severe security threats since there are no defences to detect and prevent them. Ahsan et al. [102] and Peppes et al. [131] define a zero-day attack as a

cyber-attack where cybercriminals identify vulnerabilities in FinTech software and system that is not known to the software developers and release malware to attack the FinTech software/system, steal confidential information, harm the system, and gain access or control over the system and hardware before the developers detect and create patches or updates to fix the vulnerabilities. Cybercriminals use zero-day attacks together with other attacks so that the intrusion detection techniques do not notice them, and it becomes hard for the FinTech security team to defend against them [132]. Zero-day vulnerabilities can be poor access controls, omitted data encryption and authorizations, SQL injections, broken algorithms, buffer overflows, errors, password security issues, and uniform resource locator redirects. Many cyber criminals use zero-day attacks to exploit new vulnerabilities in software and systems, but other adversaries exploit existing weaknesses that have not been patched or fixed. Financial institutions are high targets for zero-day attacks because they process sensitive financial information. Before carrying out zero-day attacks, the attackers typically conduct a background check of the financial institutions' software/system security vulnerabilities and only attack those with weak security defences. In 2021, Mandiant Threat Intelligence identified 80 zero-day exploits, and there was an 80% successful data breach due to zero-day attacks. A successful zero-day attack costs an average of US$8.94 million, according to the Ponemon Sullivan Privacy Report. The attackers use worms, viruses, Trojans, network attacks, and other malware to implement zero-day attacks [132]. The typical examples of Zero-day attacks in the FinTech industry include (1) On 10 July 2021, cyber criminals hacked into Accellion's legacy File Transfer Appliance using zero-day attacks, breaching data belonging to the American investment banking giant - Morgan Stanley. The hackers exploited numerous zero-day vulnerabilities in Accellion's legacy File Transfer Appliance and managed to steal customers' information from the Accellion File Transfer Appliance server of its third-party vendor, Guidehouse. The cybercriminals threatened to sell their victims' compromised data online if the ransom was not paid; (2) In June 2021, cybercriminals hacked into the LinkedIn API using a zero-day attack, and data for over 700 million users was compromised. The data stolen included users' email addresses, phone numbers, geolocation records, genders, and social media details. The hackers released the data set of 500 million users to the public and threatened to sell the 700 million users' complete data set. (3) In November 2019, cyber criminals hacked into Alibaba's Chinese retail website, Taobao, through zero-day attacks and scraped data belonging to 1.1 billion users using crawler software to gather customers' information [110].

8.13 Salami attacks

With the influx of FinTech, there has been a massive increase in cyberattacks, including Salami, which usually go unnoticed. A Salami attack is a type of cyberattack where software developers or employees of financial institutions install malware into FinTech servers to fraudulently siphon a small amount of money from the accounts of every FinTech client and deposit it into another account opened with a different name and owned by the software developers or employee without their victims' noticing [105], [133], [134]. The goal of a salami attack is to steal a small amount of money from every client for a long time without being detected, which can result in severe consequences for FinTech startups and clients [105]. The amount deducted unnoticed from each client can add up to considerable money and may result in substantial losses. Most of the victims of salami attacks usually do not report the deductions to the financial institutions since the amount deducted is small. Salami attacks can be internal or external. (1) Internal attacks are perpetrated by disgruntled employees or internal software developers of FinTech startups who are familiar with the security system of FinTech platforms, and (2) external attacks are perpetrated by former employees or outside developers who have inside information about the FinTech security system and try to steal from the clients of the FinTech. The attackers use mathematical routines like value calculations based on 2 or 3 decimal places and rounding to the nearest number while forgetting other decimals. The remaining fraction of the money is transferred into the attacker's account without alerting the FinTech startup. The most common examples of salami attacks in FinTech include (1) Willis Robinson, a 22-year-old employee of Taco Bell from Libertytown, Maryland, reprogrammed the cash register of the drive-up window to charge one cent for each US$2.99 item and deposit US$2.98 per transaction into his account. He was later arrested and imprisoned after accumulating US$3,600 for some time; and (2) In 2002, a bank employee of Sumitomo Mitsui Banking Corporation in Japan installed malware on the bank's server to deduct a small amount of money from each bank customer for some years and deposited it into his account. The employee collected a total of ¥200 million (US$1.8 million) before he was intercepted [135].

8.14 Shoulder-surfing attacks

Most FinTech applications require the clients to use conventional PIN-entry methods that accept Textual PINs or usernames and passwords, credit/debit card numbers, and bank account numbers for regular logins, authentications, and authorizations, which are highly vulnerable to shoulder-surfing attacks. A shoulder-surfing attack is a form of cyber-attack where cybercriminals steal FinTech clients' and employees' confidential information such as PINs, usernames and passwords, credit card numbers, bank account numbers, and other sensitive data by directly looking over their shoulders to read their screen or eavesdropping on their victims' sensitive conversation or even capturing their keystrokes using sophisticated hidden cameras, binoculars, closed-circuit television (CCTV), and secret microphones recording in crowded places like ATMs, mobile money service centres, mobile money or credit card payments in

shopping centres, filling out a form, logging onto a FinTech application or website, remotely accessing FinTech systems in public [105]. The attackers will later retrieve the recorded data from the hidden cameras, binoculars, CCTV, and secret microphones to perform fraudulent activities such as illegally accessing FinTech, bank, and mobile money accounts and applications, draining money from the victims' accounts, and unauthorized credit/debit card purchases on behalf of their victims [105]. Shoulder-surfing attacks are rampant because of the wide diffusion of mobile devices, such as smartphones used by most FinTech clients, and the simplicity of the conventional PIN-entry smartphone methods. Most of the login credentials, such as PINs, usernames and passwords, credit card numbers, and bank account numbers, are entered when they are plain or unmasked, therefore making it easy for the adversaries standing or sitting nearby their victims to observe and memorize them by using eye-tracking technology and analyze the victims' finger motions at a distance through hidden cameras and binoculars. There are still some clients of FinTech, such as mobile money subscribers in rural areas, who are using feature phones that implement the USSD technology for conducting mobile money transactions and ATM money withdrawals. Data is entered into this technology in plaintext, making it susceptible to shoulder-surfing attacks [105], [136]. The most common examples of shoulder-surfing attacks in the FinTech industry include (1) a bank customer who sits in a coffee shop waiting for coffee and decides to use their mobile banking applications or website by logging into it by entering their usernames and passwords without realizing that the next stranger is observing the login credentials. Once the stranger gets access to the login credential, they can later use it to gain access to the customers' bank accounts; (2) a FinTech customer who decides to pay for items bought in the store or supermarket using their credit or debit card by swapping it and entering the secret PIN into a card reader without knowing that the next stranger(s) in the queue is pretending to be using their phone but secretly recording the PIN which they can later use to perform fraudulent transactions; (3) a FinTech customer telling a friend or relative in public the Netflix login details over the phone without knowing that a stranger is eavesdropping on their conversation and writing down or recording the Netflix login details. Suppose the Netflix login details are the same as the victim's email address and password. In that case, the stranger can use the Netflix login details to log into the customer's email address and read the confidential information in the inbox; (4) perform mobile money transactions in a crowded place where the mobile money agent initiates the process and requests the customer to enter their four or 5-digit mobile money PIN. When the customer confirms the transaction by entering their secret PIN, a stranger in the queue can look over their victim's shoulder to observe their mobile money PIN or use a hidden camera to record the four or 5-digit PIN since the PIN is simple and unmasked. Once the stranger accesses the victim's phone, they can perform fraudulent transactions on their behalf [105], [126]; and (5) A FinTech employee who decides to log in to a FinTech corporate/business system in a public place. While entering their username and password into the system, a stranger nearby secretly observes the login details. The stranger can later use login details to sign in to the corporate system and perform fraudulent activities.

8.15 Man-in-the-middle attacks

With the massive and increasing usage of FinTech services, there is also an escalation in cyberattacks, such as man-in-the-middle (MiTM) attacks, with severe consequences for FinTech startups and clients. A man-in-the-middle attack is a form of cyberattack where cybercriminals or intruders fraudulently and successfully insert themselves in between a legitimate communication between two or more parties (i.e., users and applications), secretly eavesdrop on their conversion, intercept, modify, relay, and steal messages or network traffic or impersonate as one of the authorized parties in the communication without other parties noticing in real-time [102], [105], [133]. Once the adversaries successfully insert themselves into the FinTech communication network, they can steal confidential login credentials such as usernames and passwords, social security numbers, credit card numbers, bank account details, and other sensitive financial information. MiTM attacks in FinTech can be both passive and active. Nivedita [117] reported that in 2021, among the successful cyber-attacks, 19% were MiTM attacks, and in 2022, interception of confidential login credentials and banking information by attackers contributed to over 50% and around US$2 billion was lost due to the MiTM attacks globally. The methods used by adversaries to execute MiTM attacks include phishing attacks, session hijacking, malware, spoofing, unsecured public Wi-Fi eavesdropping, secure sockets layer (SSL) hijacking, SSL browser exploit against SSL/transport layer security (TLS) (BEAST), and SSL Stripping ([102]). Man-in-the-middle attacks involve two steps, i.e., data interception and decryption. (1) During data interception, the adversaries use malware or the methods mentioned above to insert themselves into the communication between the two parties or eavesdrop on the customer who signs into an unsecured Wi-Fi connection and intercept message transfer between the customer's mobile device and FinTech servers. They use unsecured communication channels where the messages are transmitted in plaintext or network sniffer software like Auvik, Wireshark, NetworkMiner, SolarWinds Network Packet Sniffer, ManageEngine NetFlow Analyzer, Telerik Fiddler, WinDump, TCPdump, to grab messages or network traffic. The attackers can also modify and resend the captured messages to the recipients without the parties noticing them [102], [105], [126]. (2) After the adversaries intercept the messages, if the messages are encrypted, they must decrypt them using SSL BEAST, SSL hijacking, SSL stripping, and HTTPS spoofing without the customer and FinTech servers noticing [102]. The notable examples of MiTM attacks in the FinTech industry include (1) In 2017, attackers used the MiTM attack to penetrate banking networks, allowing them to steal customers' login credentials and view and collect their financial information. Researchers later identified critical vulnerabilities with the certificate technology

that is used by many banks such as HSBC, Co-op, Allied Irish Bank, and NatWest; (2) In 2017, cybercriminals identified vulnerabilities with the unsecured domain connections of Equifax - one of the biggest American credit reporting agencies. The attackers inserted malicious code in Equifax's HTTP request, allowing them to execute a MiTM attack on the insecure domain connections. They compromised and stole over 100 million customers' personally identifiable information. In the same year, adversaries also spoofed the Equifax website and compromised the records of over 143 million Americans. The attackers created a fake website with fake DNS and spoofed the SSL, where the customers were redirected to the phoney website, and their data was intercepted; and (3) In 2015, cybercriminals used MiTM attack techniques to intercept European corporate bank accounts and monitor communications, redirect financial transactions, and steal over €6 million from European firms [110].

8.16 SQL injection

Cyber-attacks are an exponential concern for FinTech startups and customers. Structured query language (SQL) injection is rampant and has perilous web application weaknesses affecting data confidentiality and integrity. Al-Khater et al. [137] define SQL injection (SQLi) as a cyberattack where cybercriminals compromise databases by injecting malicious SQL codes into a FinTech website application or program to penetrate the backend database, thus giving the attackers unauthorized privileges to view, steal, modify or access sensitive information such as the login credentials or perform other malicious actions. SQLi targets applications and websites that use SQL databases such as MySQL, Oracle, and Microsoft SQL Server. In 2022, SQLi was the primary source of serious vulnerabilities worldwide for web applications. The total number of SQLi attacks was 274,000, and it takes less than 10 seconds for adversaries to execute SQLi on a susceptible website [117]. Over 1 billion user IDs and passwords and 130 million card details were stolen by hackers using SQLi attacks. SQLi is used with other malware, such as worms and trojans. The most common examples of SQLi in FinTech include (1) In early 2023, cybercriminals used SQLi techniques to attack Amazon web services' web application firewalls and stole an administrator session cookie. The attackers used JavaScript object notation (JSON) commands to bypass the web application firewalls. This attack was later discovered by the Israeli-American security firm Claroty; (2) On 1 November 2017, cyber criminals hacked into the konsoleH platform of Hetzner - a South African data centre operator and largest website hosting company - leaking customers' confidential information, FTP passwords, domain names, bank account details, and other personal data. The attackers used SQLi flaws to access the konsoleH control panel database that allows users to manage the web space with greater efficiency and accessibility; (3) Between 25-26 December 2017, hackers deployed SQLi into the DA Davidson - a financial services holding company - website during the Christmas holiday and managed to retrieve and steal the confidential information of 192,000 customers. This was detected after the attackers attempted to blackmail the company some weeks later, and (4) Cybercriminals also identified weaknesses in LinkedIn’s system and implemented SQLi to access the confidential information of over 167 million users illegally. The sensitive information stolen included users’ email addresses and hashed passwords, later sold on the dark web [110].

8.17 Brute-force attacks

In recent years, brute-force attacks have risen in the FinTech industry because of remote access to financial services. A brute-force attack has been defined as a type of cyber-attack where cybercriminals use trial-and-error methods, such as mathematical methods or referring to a dictionary or other techniques, to guess or crack login credentials, encryption keys, credit card numbers, hashed tokens, promo codes, and decrypt encrypted data that can be used to gain unauthorized access to FinTech systems, platforms or networks [105]. The adversaries target usernames and passwords, ID numbers, PINs, API keys, encryption keys, SSH logins, and credit card numbers. They use simple brute-force attacks, dictionary attacks, hybrid brute-force attacks, reverse brute-force attacks, or credential stuffing with computers and malware to guess or crack them. Most FinTech systems and applications use weak authentication methods such as usernames and passwords, numeric PINs, OTP, and credit card numbers, which are susceptible to brute-force attacks [126]. Although brute-force attacks are resource-intensive and time-consuming, they are reliable and have a high success rate of gaining unauthorized access to FinTech systems, networks, and applications [105]. In 2019, more than two-thirds of all data breaches resulted from password compromise, which led to financial losses for firms and clients. The average cost of stolen or compromised credentials in 2022 was US$4.50 million, and it took hackers 22 seconds to attempt 2.18 trillion combinations of passwords and usernames. The attackers use malware, scripts or bots, and other tools like Hydra, Chaos, CrackMapExec, and PoshC2 to automate the brute-force attack process. Many adversaries begin the process of brute-force attacks with famous words or by combining letters, numbers, and symbols to crack into usernames and passwords. They speed the process of cracking by using a highly distributed network of botnets infected with malware, which they control without the knowledge of the owners of the devices. The botnets help to bypass rate-limiting restrictions and breach SSH servers belonging to financial institutions. Attackers also use cloud or cloud services to launch brute-force attacks by exploiting computing resources without making long-time investments. The adversaries who lack some skills also purchase automated tools with leaked credentials and other value-adds like management consoles from the dark web as malware kits for launching brute-force attacks. After setting up their tools and seeding them with the essential lists, the attackers can begin cracking the login credentials,

and if successful, the validated credentials will enable them to sign in to the FinTech system, impersonating legitimate users. While inside the FinTech system or network, they can install backdoors, steal confidential information, and make fraudulent transactions. The notable examples of brute-force attacks in the FinTech industry include (1) On 1 July 2021, cybercriminals linked to a boutique software development firm in Shiraz, Iran, used a crypto-mining botnet called MrbMiner to launch brute-force attacks against Microsoft SQL Servers databases to get into insecure accounts. After successful cracking, the botnet creates a backdoor for the attackers to access the database and download a cryptocurrency miner. This attack was later discovered by a cybersecurity company called Sophos; (2) In 2021, hackers used specialized tools and skills in technical systems to gain access to T-Mobile's testing environments and employed brute-force attacks to infiltrate servers holding customer data. The attackers stole 100 million users' personal information and initially put it for 6 Bitcoin but later sold it for US$200; and (3) In March 2018, hackers launched brute-force attacks on the popular open-source Magento platform used by hundreds of e-commerce sites to crack credit card numbers and install crypto-mining malware. The attackers compromised weak passwords for about 1,000 open-source accounts, which were used to steal confidential information and spread malware [110].

8.18 Cloud environment security risks

Cloud computing in FinTech is a revolutionary innovation that transforms and facilitates remote secure information access for startups and clients. Cloud computing in FinTech refers to the type of computing where financial data are stored and processed from remote servers and storage. Cloud computing has become vital, and many FinTech startups are investing heavily in cloud services so that FinTech systems are accessible to many customers, users' data are stored in the cloud, and improved digital products and services are delivered to the clients. The cloud services include infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), which are private, public, or hybrid. The dominant FinTech cloud service providers are AWS, Microsoft Azure, Google Cloud, and Alibaba Cloud [18]. Payment gateways, digital wallets, Internet banking services, mobile apps, websites, and other secure online payments are some FinTech services carried out through a cloud-based computing system [115]. The global multi-cloud networking in the FinTech market values is estimated to reach US$1.9 billion by 2031 with a CAGR of 18.2% from 2022 to 2031. Cloud exploitation increased by 95%, and global cloud data breaches in the third quarter of 2022 increased by 37%, reaching 15 million. The prevalent cases of Cloud environment security risks in the FinTech industry include (1) In February 2022, a misconfiguration of Google Cloud Storage led to the disclosure of more than 23 million sports retailer customers' personal information. A misconfiguration of Microsoft Azure's storage bucket in March 2022 resulted in the leakage of over 5 million users' financial data and personally identifiable information from the health application. Over 533 million Facebook user records were exposed in April 2022 due to the misconfiguration of AWS. In May 2022, close to 12,000 employees of McDonald's across North America had their personal information, such as social security numbers and bank account details, exposed to the public due to a cloud misconfiguration; (2) On 16 July 2021, a misconfiguration of one of BackNine's storage servers hosted on Amazon's cloud resulted in the exposure of 711,000 files including completed insurance applications that contained applicants and their family's confidential personal and medical information; and (3) In 2019, a software engineer hacked the cloud-based server of Capital One and compromised credit card applications for 100 million customers. The hacker used the firewall misconfiguration to access the personal information database hosted by AWS illegally. The compromised confidential information included customers' names, addresses, American and Canadian social security numbers, date of birth, credit scores, and contact information, which was later posted on GitHub [18], [110]. Some of the key challenges/risks the FinTech firms are facing through the adoption of cloud computing include the lack of adequate cloud security and data privacy measures that led to compromise and corruption of confidential personal and financial information stored in the cloud servers, cloud malware and botnets, security system misconfiguration, insider attacks, cloud-based data management risks, cloud ransomware attacks, compliance challenges, DoS attacks, cloud sprawl, insecure access control, supply chain attacks, inadequate notifications and alerts about cyber threats, brute-force attacks in the cloud, API threats [18], [115].

8.19 Blockchain risks

Blockchain technology has emerged as a disruptive innovation in FinTech, revolutionizing businesses with decentralized transactions. Renduchintala et al. [138] define Blockchain as a decentralized, cryptographically secure, transparent, immutable, and distributed ledger that records transactions in blocks and tracks digital assets across a peer-to-peer network or network of nodes so that there is up-to-date information to all the participants with no third party or intermediaries involved. Each record in the Blockchain is a block; the blocks are chained together using a cryptographic hash and are irreversible. Every block has information about the cryptographic hash of the previous block, the timestamp, and transaction data. New blocks can only be added to the existing chain after Blockchain network members verify the validity of the transactions through a consensus mechanism [89], [114]. Blockchain is classified as public, private, consortium, and hybrid and has unique characteristics such as decentralization, auditability, distribution, consistency, fault-tolerant, transparency, automation, traceability, privacy, and reliability, which can improve FinTech applications effectively [23], [89], [138-140]. Ethereum, Ripple, Cardano, Stellar, Hyperledger

Fabric, EOS, Corda, and Tron are Blockchain platforms for building FinTech applications [138]. Blockchain FinTech application is decentralized finance (DeFi) that uses decentralized smart contracts and a secure distributed ledger to provide financial services such as borrowing, investing, lending, and exchanging crypto assets by eliminating intermediaries or bank control over financial services and money [42], [141]. The acceptance of FinTech Blockchain keeps mounting, with the market value expected to reach US$50.7 billion by 2032. Much as Blockchain technology has benefited the FinTech industry, it is also encountering challenges and risks such as interoperability concerns, hacking of the FinTech Blockchain platforms, spreading of Malware, centralization issues, regulatory and standardization uncertainty, ensuring the integrity of data, balancing privacy with transparency, ensuring trust and anonymity in platform-mediated networks, transaction confidentiality [140], [141]. Some of the common examples of Blockchain risks in the FinTech industry include (1) On 23 March 2022, a North Korean state-backed hacking group, "Lazarus Group" hacked into a Blockchain project Ronin by exploiting a feature in the technology that allowed users to transfer digital assets from one crypto network to another, thus, resulting in a loss of US$615 million in ether and USD Coin tokens; (2) On 17 January 2022, cyber criminals hacked into Multichain by exploiting a weakness in the Blockchain service resulting in a loss of US$1.4 million; (3) On 1 December 2021, cyber criminals hacked into Blockchain startup MonoX Finance by exploiting a weakness in the program used for drafting smart contracts by increasing the prices of the MONO token and using it to withdraw all the deposited tokens resulting in a company losing US$31 million; (4) On 10 August 2021, hackers took advantage of the weaknesses in the Chinese Blockchain site "Poly Network" to steal thousands of digital tokens leading to a loss of US$600 million; and (5) On 17 February 2021, three North Korean computer programmers were charged with partaking in an extensive illegal conspiracy such as undertaking various destructive cyberattacks, deploying several malicious cryptocurrency programs, developing and illegally marketing a Blockchain system and stealing and extorting over US$1.3 billion and cryptocurrency from financial institutions and corporations [110].

8.20 Internet of Things (IoT) risks

Recently, there has been a massive adoption of IoT and next-generation IoT (Nx-IoT) intelligent technologies in the banking and FinTech sectors to create a smart economic world. Barros et al. [142] and Bouzidi et al. [143] define IoT as a collective network of unique addressable physical objects, wireless technologies, and other smart devices that are equipped with sensors, actuators, software, network connectivity, and other technologies to enable collection and sharing of data, processing and analyzing unparalleled data, communication among the devices and the cloud, and making intelligible decisions without human intervention. Smart devices in the IoT include laptops, smartphones, tablets, wearable devices, radio frequency identification (RFID) tags, sensors, actuators, and other smart devices that are connected over the Internet to allow machine-to-human and machine-to-machine communication where data can be shared daily to the remote server and other devices [144], [145]. The IoT architecture comprises sensory devices, the network, and data management and analysis, which are grouped into the three layers of perception, the network, and the application [146]. Many IoT intelligent technologies, such as smart security systems, digital wearables, and smart payments, are extensively used in the FinTech industry to boost payment processing, analyze comprehensive financial data, and provide robust security [147]. A mobile point-of-sale system, cashless payments, smart banking and ATMs, personalized experience, optimized voice technology, enhanced security, improved spending data, better fraud detection, smart contracts, smart retail banking, and enhanced risk assessment are some of the examples where IoT is used in the banking, financial services & insurance (BFSI) sector. According to Statista, 29 billion IoT devices will be connected worldwide by 2030, and every individual, on average, will have fifteen connected devices by 2030. The worldwide BFSI market for IoT is estimated to reach US$1319.08 billion by 2026 [148]. There will be challenges and attacks faced by IoT in FinTech that will result in the loss of vast sums of money estimated to be between US$3.9 trillion and US$11.1 trillion in 2025 [149]. Through green finance programs such as M-Pesa, M-KOPA, BanQu, and others, many developing economies contribute to developing IoT-based FinTech [148]. While IoT-based FinTech has benefited the BFSI industry, it has also encountered several challenges and concerns, including data privacy and security concerns, data management concerns, data density, lack of standards, hacking, DoS and DDoS attacks, data theft, identity theft, system complexity, user trust concerns, integration concerns, and data ownership concerns [80], [149].

8.21 Money laundering and Cryptocurrency-related risks

Globally, FinTech money laundering has become a big issue in the financial sector. Money laundering is the process of making an illicitly obtained sum of money appear lawful and clean while concealing its origins and ownership and reinvesting it in a legitimate economy or financial system [150]. Criminals and syndicates utilize money laundering to make money obtained fraudulently look legitimate, which can be used to finance various organized criminal operations. Money launderers focus on FinTech because clients utilize anonymous accounts to perform massive transactions on a system with a limitless money flow. Furthermore, money launderers are increasingly exploiting the weaknesses and vulnerabilities in traditional anti-money laundering/countering the financing of terrorism (AML/CFT) frameworks to engage in illegitimate and criminal activities such as drug trafficking, tax evasion, human

trafficking, laundering, robberies, financial fraud, and others. In 2022, LexisNexis carried out research and found that among the financial crimes encountered by financial institutions, 67% were in digital payments, while over 60% were in money laundering. The global amount of money laundered was projected to be between US$2 trillion and US$5 trillion. In 2020, money laundering systems contributed to 2-5% of the total gross domestic product (GDP) worldwide, and global financial institutions like banks were penalized US$10.4 billion for engaging in money laundering violations. Money launderers utilize a variety of tactics to conceal money, including cash-intensive businesses, smurfing, ghost corporations, high-value assets, drug trafficking, international and domestic terrorism, and arms trafficking. Money laundering involves placement, layering, and integration [150]. During the placement phase, the launderers deposit the proceeds of the illegal activity(ies) into financial institutions, casinos, and established businesses in both the domestic and international markets, i.e., large sums of money divided into small amounts and deposited into several bank accounts before being sent overseas to be deposited into foreign accounts or used to purchase high-value goods that can later be resold, and the payment is made using check or wire transfer. The famous examples of crime in the placement stage are the blending of funds, invoice fraud, smurfing, offshore accounts, carrying small sums of cash abroad, and aborted transactions. In the layering phase, several money transfers are made from one account and deposited into other accounts in various financial institutions across many countries, where the money can be converted into other monetary instruments such as checks, wire transfers, stocks, real estate, and securities or insurance coverage investments, genuine businesses, and bonds. This phase entails using many bank accounts, experts as intermediates, corporations and trusts, and layers of sophisticated financial transactions. Meanwhile, in the integration phase, income produced from unlawful goods is given legitimacy by reintroducing 'clean up' riches into the actual economy, such as depositing money derived through the sale of goods and securities. After completing this step, the wealth will appear legal, and no restrictions will prevent the launderer from using it, such as using payment instruments offered by the financial system for any transaction. It is impossible to discern between legal and illicit riches at this stage, and the launderer can spend the money without being detected [150]. Cryptocurrencies are becoming a popular method of laundering money in the FinTech industry because of their anonymity and decentralization, which has several systemic breaches. Money launderers use tumblers to mix Bitcoins with other money to obscure the relationship between the sender and recipient. There is a rapid growth in online gambling platforms utilizing cryptocurrency payment methods to perform money laundering [151]. These cryptocurrencies have become a source of money laundering since standards and international regulations do not legally regulate them, and hackers use them to steal data [150]. The notable examples of money laundering in the FinTech industry include (1) In February 2020, the chief executive officer of the Coin Ninja media platform and the founder of the DropBit cryptocurrency wallet, Larry Harmon, was arrested by the U.S. federal government for carrying out money laundering activities and running a money exchange business without obtaining a license from FinCEN. He was accused of laundering more than 354,468 Bitcoin (US$311 million) [150]; (2) In February 2020, two Dutch citizens were arrested by the Dutch tax authorities and the Fiscal Intelligence and Investigation Services for laundering millions of euros in cryptocurrency. The authority recovered 260,000 unnamed cryptocurrencies, over 6.6 pounds of gold, and credit and debit cards in ownership of cryptocurrency and euros. One of them was found using Bestmixer.io, a Bitcoin mixing service that was already banned [150]; (3) In 2020, the former chief executive officer of Wirecard, an online payment company, was arrested in Germany for a serious financial scandal such as the €1.9 billion which was thought to be deposited as trust funds in two banks in the Philippines but never happened. Wirecard was also accused of processing payments for a Maltese online casino, a Malta-based gaming company “CenturionBet”, and other Maltese gambling companies, and laundering money for a member of the most powerful and dangerous mafia organizations in Europe known as “Ndrangheta” and other organized crime groups [150]; (4) In October 2019, a Canadian citizen and the president of Crypto Capital Corporation, Ivan Manuel Molina Lee, was arrested and extradited to Warsaw by Polish police for international money laundering of 1.5 billion zlotys (€350 million). The Crypto Capital Corporation was known for providing banking services to Bitfinex cryptocurrency exchange firms and other main trading platforms. Ivan Manuel Molina Lee opened bank accounts in the Bank Spółdzielczy, a small rural bank in Skierniewice, to launder illicit proceeds using BitFinex and Global Trading Solutions. He was also accused of using cryptocurrency exchange companies to launder money for the Colombian drug cartels [150]; (5) In September 2018, the result of the independent investigation, which was carried out between 2007 and 2015, revealed that over €200 billion was involved in the suspicious transactions which are considered the biggest international money laundering that took place at Danske Bank’s Estonian branch. In 2018, Deutsche Bank also acknowledged their involvement in the Danish bank scandal since they participated in managing nearly €130 billion that came from the Danske Bank’s Estonian branch [150] and (6) Several companies and financial institutions have been fined for neglecting the anti-money laundering regulations among which include (i) the Malaysian lender AmBank stung which was fined US$700 million for its involvement in 1MDB financial scandal, (ii) BlockFi, a crypto firm was fined US$100 million, (iii) Helix, a cryptocurrency organization was fined US$60 million for darknet money laundering offences, (iv) Bittrex, a crypto trading platform was fined US$29.3 million for violating several sanctions, and (v) Wise was fined US$360,000 for violating AML requirements and failure to identify and confirm the sources of money or wealth of its high-risk customers.

These cybersecurity issues in FinTech violate the security objectives of confidentiality, integrity, availability, authenticity, authorization, non-repudiation, accountability, and auditability. They have resulted in malfunctions of

critical financial systems, privacy breaches, stealing of confidential financial and client information, interruption of crucial FinTech services, espionage, reputational damage, repudiation, financial losses to the FinTech startups and the governments, exposure to regulatory fines, difficulty enforcing the AML regulations and laws, the spread of malware, hijack of FinTech accounts, redirecting traffic from a FinTech system, identity theft, DoS, APT attack, disclosure of trade secrets and intellectual property, and loss of customers' trust in FinTech services [23], [59], [99], [117], [131], [152], [153].

Table 1 summarizes the cybersecurity issues on FinTech systems, platforms, and networks.

Table 1. Cybersecurity issues on FinTech systems, platforms, and networks

References	Year	Title	Cybersecurity Issues
[80]	2024	A Review on Cybersecurity in FinTech: Threats, Solutions, and Future Trends	Data breaches, Malware attacks, Ransomware, Social engineering attacks, Phishing attacks, and IoT risks
[67]	2024	A systematic literature review of the role of trust and security on FinTech adoption in banking	Data breaches, Malware attacks, Ransomware, Identity theft, and Phishing attacks
[68]	2024	Human factors in cybersecurity: Navigating the FinTech landscape	Data breaches, Malware attacks, Identity theft, and Phishing attacks
[69]	2024	A critical review of emerging cybersecurity threats in financial technologies	Malware attacks, Ransomware, insider threats, Social engineering attacks, and Supply chain attacks
[65]	2023	Intelligent Detection of Distributed Denial of Service Attacks: A Supervised Machine Learning and Ensemble Approach	DDoS attacks
[66]	2023	Cybersecurity Challenges and Solutions in the FinTech Mobile App Ecosystem	Data breaches, Malware attacks, and Identity theft
[59]	2023	Data Defense: Examining FinTech's Security and Privacy Strategies	Privacy issues, Money laundering and cryptocurrency-related risks
[23]	2023	On the Applications of Blockchain in FinTech: Advancements and Opportunities	Data breaches, Malware attacks, Money laundering and cryptocurrency-related risks
[5]	2023	FinTech is enabler or disruptive to the Banking Industry: An analytical study.	Hacking
[131]	2023	The Effectiveness of Zero-Day Attacks Data Samples Generated via GANs on Deep Learning Classifiers	Zero-day attacks, Money laundering and cryptocurrency-related risks
[141]	2023	Emerging advances of blockchain technology in finance: a content analysis	Blockchain risks
[147]	2023	Service Deployment Strategy for Predictive Analysis of FinTech IoT Applications in Edge Networks	IoT risks
[153]	2023	SQL injection attack detection in network flow data	Money laundering and cryptocurrency-related risks
[149]	2023	Trustworthy and Efficient Routing Algorithm for IoT-FinTech Applications Using Nonlinear Lévy Brownian Generalized Normal Distribution Optimization	IoT risks
[57]	2022	Does the COVID-19 Pandemic Motivate Privacy Self-Disclosure in Mobile Fintech Transactions? A Privacy-Calculus-Based Dual-Stage SEM-ANN Analysis	Privacy issues
[114]	2022	A Blockchain-Enabled System for Enhancing FinTech Industry of the Core Banking Systems	Malware attacks, Hacking, Social engineering attacks
[102]	2022	Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning - A Review	Malware attacks, social engineering attacks, MiTM attacks
[115]	2022	Role of Bangladesh Bank on Cybersecurity in FinTech	Malware attacks, Cloud environment security risks
[121]	2022	A Survey of FinTech Research and Policy Discussion	Hacking
[133]	2022	Towards the Advancement of Cashless	Salami attacks

		Transaction: A Security Analysis of Electronic Payment Systems	
[42]	2022	The Impact of FinTech and Blockchain Technologies on Banking and Financial Services	Blockchain risks
[138]	2022	A Survey of Blockchain Applications in the FinTech Sector	Blockchain risks
[140]	2022	Research on Multi-Dimensional Trust Evaluation Mechanism of FinTech Based on Blockchain	Blockchain risks
[132]	2022	Comparative Evaluation of AI-Based Techniques for Zero-Day Attack Detection	Zero-day attacks
[72]	2022	Cyber Threats and Scams in FinTech Organizations: A brief overview of financial fraud cases, future challenges, and recommended solutions in Bangladesh	Social engineering attacks
[107]	2021	Understanding China's FinTech sector: development, impacts and risks	Privacy issues
[18]	2021	Understanding Cybersecurity Management in FinTech	Data breaches, Malware attacks, Hacking, Insider threats, social engineering attacks, DDoS attacks, Cryptojacking, Cloud environment security risks
[62]	2021	Cyber Security Solutions for Businesses in Financial Services	Malware attacks
[63]	2021	FinTech firms and banks sustainability: Why cybersecurity risk matters?	Data breaches
[127]	2021	The Economics of FinTech	DDoS attacks
[124]	2021	Cyber-Identity Theft and FinTech Services	Identity theft
[105]	2020	Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures	Privacy issues, social engineering attacks, DDoS attacks, Salami attacks, Shoulder-surfing attacks, MiTM attacks, Brute-force attacks
[108]	2020	FinTech and financial inclusion: Opportunities and challenges	Privacy issues
[119]	2020	Cybersecurity hazards and financial system vulnerability: a synthesis of literature	Hacking
[122]	2020	Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses	Insider threats
[126]	2020	Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda	Social engineering attacks, MiTM attacks, Brute-force attacks
[150]	2020	Electronic Money Laundering, The Dark Side of FinTech	Money laundering and cryptocurrency-related risks
[135]	2020	Bank herding in loan markets: Evidence from geographical data in Japan	Salami attacks
[110]	n.d.	Carnegie Endowment for International Peace and BAE Systems	Privacy issues, Data breaches, Malware attacks, Hacking, Insider threats, Identity theft, social engineering attacks, DDoS attacks, Cryptojacking, Supply chain attacks, Zero-day attacks, MiTM attacks, SQL Injection, Brute-force attacks, Blockchain risks

9. CYBER SECURITY

Cybersecurity refers to a set of practices, strategies, processes, and technologies to protect digital devices, programs, networks, financial and client data, operational procedures, and intellectual property from unintentional or unauthorized breaches, access, and disruptions by cyber criminals [102], [115], [116], [120], [154]. With the digitization of the financial sector, many mobile devices are connected to the Internet to access FinTech services, and the amount of data stored and shared online has proliferated, thus forcing FinTech startups and established firms to invest vast amounts of money in data protection and building robust cybersecurity systems [155]. Cybersecurity, therefore, helps to ensure data privacy, confidentiality, integrity, availability, authenticity, non-repudiation, and

accountability [114], [156], [157]. According to the Cyber Security Market 2021-2028 report, the global cybersecurity market is expected to reach US$366.10 billion by the end of 2028 [158]. Cybersecurity is critical to the success, trust, and protection of FinTech startups and clients. As a result, the literature emphasizes the current cybersecurity deployed by FinTech organizations. The following are some of the mitigating measures employed by FinTech firms to safeguard against cyber-attacks and threats:

9.1 Authentication and access control mechanisms

FinTech systems provide authentication and access controls by safeguarding financial information and login credentials using cryptography-based techniques [59]. Authentication in FinTech is confirming or validating employees' and clients' claimed identities by comparing their available login credentials with the copy stored in the FinTech systems' databases to determine their identity and allow only authorized people to access the FinTech systems and platforms [18]. Their identities are verified using authentication factors such as knowledge, possession, inherence, location, and behaviour [105]. FinTech employee and customer authentications are performed via mobile devices and the server so that they may access sensitive login credentials and financial information in real-time. Single sign-on, password-based authentication, single-factor authentication, biometric authentication, certificate-based authentication, two-factor authentication, multi-factor authentication, and token-based authentication are currently available in FinTech systems and platforms [18], [35], [43], [55], [66], [72], [80], [159-162]. In FinTech, an access control mechanism is a security measure meant to detect and block unauthorized access to FinTech systems while granting authorized access to a FinTech system and its resources [18]. They are critical in ensuring the security, confidentiality, availability, and integrity of FinTech systems and protecting confidential login credentials and financial data against unauthorized access, theft, and manipulation [59]. Authentication is frequently used in access control mechanisms, where FinTech users must authenticate their identity using login credentials. Authorization comes after authentication and determines what activities or resources a FinTech employee and clients may access depending on their authenticated identity and the access control rules. FinTech startups may decrease the risk of unauthorized access and potential security breaches by implementing suitable access control mechanisms, securing sensitive data, and ensuring compliance with legislation and privacy standards. The various access control mechanisms implemented in FinTech systems and platforms include mandatory access control, discretionary access control, role-based access control, attribute-based access control, rule-based access control, remote access control, and time-based access control [18], [59]. Access control mechanisms identify and authenticate FinTech users to access financial services, grant and restrict access based on the identities of the users, and monitor and record all attempts to access a FinTech service [18], [59], [163].

9.2 Cryptography

FinTech firms extensively employ cryptographic controls like encryption and hashing to secure login credentials and financial information from unauthorized access in the public network infrastructure [59], [100]. Triple data encryption (3DES), advanced encryption standards (AES), Twofish, Blowfish, Rivest, Shamir, and Adleman (RSA), and elliptic curve cryptography (ECC) are the most often utilized encryption algorithms in FinTech platforms [43], [66], [80]. They assist FinTech startups in achieving several security objectives such as confidentiality, authentication, integrity, access controls, and non-repudiation, as well as in securing data in transit and at rest [35], [59], [163], [164]. AES protects the confidential payment data of FinTech clients, such as credit/debit card details, account numbers, usernames and passwords, and other financial information. Encryption also ensures that data communicated across the FinTech system is safe and cannot be intercepted by unauthorized persons [160]. Cryptography ensures data security, integrity, confidentiality, user authentication, user identity verification, non-repudiation, safe payments, regulatory agreement, fraud detection and prevention, and resilience against cyberattacks in the FinTech sector.

9.3 Regulatory compliance

With the adoption of FinTech services, several governments are developing new regulations, laws, policies, and guidance to secure their FinTech data. Regulatory compliance in FinTech refers to FinTech companies adhering to policies, standards, laws, regulations, guidelines, and specifications established by the government, industry associations, and regulatory bodies to protect clients' interests and money, ensure data privacy, protect against money laundering and cyberattacks, avoid penalties and sanctions, and govern the industry. FinTech companies must follow these regulations to protect consumer and financial data, which differ by country. FinTech firms follow several regulatory and compliance measures to safeguard their security and privacy [59]. The most popular FinTech compliance regulations include Anti-Money Laundering (AML) Regulations, Commodity Futures Trading Commission (CFTC), Consumer Financial Protection Act (CFPA), Consumer Financial Protection Bureau (CFPB), Decentralized Finance Regulations, Electronic Fund Transfer Act (EFTA), Electronic Signatures in Global and National Commerce (E-Sign), Federal Deposit Insurance Corporation (FDIC), Federal Trade Commission (FTC), Financial Action Task Force (FATF), Financial Crimes Enforcement Network (FinCEN), Payment Card Industry Data Security Standard (PCI DSS), Financial Industry Regulatory Authority (FINRA), General Data Protection Regulation (GDPR), Jumpstart Our Business Startups (JOBS), Know Your Customer (KYC) Regulations, National Credit Union Administration (NCUA),

Office of the Comptroller of the Currency (OCC), Payment Card Industry Data Security Standard (PCI DSS), Payment Services Directive (PSD2), Securities and Exchange Commission (SEC) Regulations, the Commodity Futures Trading Commission (CFTC), the Federal Information Security Modernization Act (FISMA), The Truth in Lending Act (TILA), International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001, and many more [5], [18], [59], [66], [78], [165]. Regulatory compliance is essential in the FinTech industry because it creates a level playing field for FinTech firms, helps to scale FinTech businesses, reduces FinTech firms' exposure to regulatory penalties and fines, protects FinTech firms' reputation, increases FinTech firms' profitability, improves efficiency, ensures financial security, business continuity, protects FinTech firms from cybersecurity threats, and ensures the security and privacy of financial data [18], [59], [163], [166].

9.4 Intrusion detection systems and intrusion prevention systems

To ensure cybersecurity, robust intrusion detection systems (IDS) and intrusion prevention systems (IPS) are being deployed by FinTech companies in their FinTech systems, platforms, and networks to monitor network traffic for suspicious activities, generate warnings when malicious actions are detected, and automatically block/prevent potential threats and attacks and unauthorised access from cyber criminals on the networks. In FinTech, an IDS is a security system that monitors and analyzes FinTech network traffic, system or platform activities to detect suspicious transactions and unauthorized behaviour and issues alerts when they are discovered. Intrusion detection systems do not take action automatically to prevent harmful transactions or illegal behaviour from taking control of FinTech networks and systems. Every malicious activity or violation is recorded centrally in the security information and event management (SIEM) system or alerts the system administrator or a security operations centre (SOC) analyst to investigate the incident and take the appropriate action to eradicate the danger. They are based on a predictive model that scans network traffic, system logs, and other relevant data sources to look for patterns and anomalies in real-time or near-real-time to distinguish between malicious and legitimate connections. They are accomplished by segmenting the network, detecting and monitoring security incidents, controlling access to FinTech systems by providing required permits for the services, managing and monitoring FinTech user access privileges, controlling access to the FinTech network infrastructure, conducting threat intelligence and penetration testing, frequent vulnerability assessments, reviewing FinTech application codes, and reviewing digital technology architecture, classifying confidential FinTech employee and client data ([70]). An IPS, on the other hand, is defined as a security system that monitors and analyzes FinTech network traffic, system or platform activities to detect suspicious or unauthorized behaviour and automatically blocks or prevents intrusion/potential threats and attacks on the network before causing damages, as well as terminates malicious connections and content by sending alerts to the security team. It is a proactive security solution that prevents unauthorized access to FinTech systems and networks, sensitive login credentials and financial data breaches, and other suspicious actions from jeopardizing the integrity and confidentiality of the FinTech network. Intrusion prevention systems have been incorporated into next-generation firewalls or unified threat management solutions to scan massive FinTech network traffic without slowing down network performance and prevent DoS and DDoS attacks, Worms, Viruses, and other vulnerabilities.

9.5 Fraud detection and prevention system

FinTech firms use a variety of strategies to detect and prevent fraud in the industry. Jain et al. [1], Kumari and Devi [42], and Faccia [160] reported that STET, SNCE, SADAD, SPEI, NSPK, Interac, Faster Payments, EFTPOS, EBA Clearing, China UnionPay, and BKM Express are using advanced fraud detection tools such as network analysis, location-based strategy, risk-based authentication, advanced data analytics, transactional logs, user behaviour analysis, data visualisation, time-series data, natural language processing, machine learning, real-time transaction monitoring, real-time monitoring, and transaction terms passing relational data, and prevention tools like biometrics authentication, blockchain technology, continuous data monitoring, educating stakeholders, managing fraud cases, transaction monitoring, multi-factor authentication, encryption, tokenisation, no-code workflows, strict customer onboarding process, strict procedures when changing status, transaction screening and monitoring, predictive scoring to alert about frauds, three-dimensional secure, machine learning to rank high-risk alerts, risk assessment, and verifying user identities, to monitor transactions and identify potential fraud in FinTech. These systems use algorithms based on statistical analysis to analyze transaction-related data, identify suspicious patterns and behaviours, report probable fraud for further investigation, and stop fraudulent transactions [42], [69], [160], [163]. The fraud detection and prevention systems help improve after-sales inspections and clarify obligations in the case of fraud. Small FinTech firms have difficulty creating these systems due to the high construction expenses and enormous data processing.

9.6 Regular data backup

FinTech companies are urged to regularly store backups of their customers and financial service data on a different server or in the cloud to ensure their safety, security, and availability [18]. Data backup in FinTech is defined as the process of creating copies of sensitive databases, login credentials, and financial information regularly and storing them in a secure secondary, tertiary, and quaternary storage location to ensure their availability in the event of targeted

ransomware attacks and other attacks, disasters, data loss, or damage. Backup is an essential component of data security in the FinTech business, as data loss can result in significant expenses, and there is a need to have a plan in place for recovering data in the event of a disaster, system failure, data loss, or corruption. The approach must include frequent data backups, testing data recovery procedures, and storing backup data safely, which must be automated in most circumstances.

9.7 Basic security training

Governments and FinTech firms must spend time and money training their personnel on the most recent cyber dangers and best practices for Internet security. All FinTech clients and the general public must also be trained regularly on fundamental security procedures such as protecting sensitive login credentials and confidential information such as bank accounts, credit card details, bank balances, unauthorized software, and trash disposal. These training programs will enable them to respond quickly and effectively to cyberattacks like phishing and social engineering [18], [163].

9.8 Big data analytics

Big data analytics is revolutionizing the FinTech industry's operations by providing security for FinTech systems and platforms. Big data analytics is defined in FinTech as gathering, reviewing, and analyzing enormous volumes of raw financial data using various tools and methods to identify relevant trends, patterns, correlations, and insights to make data-driven decisions. It processes and examines vast volumes of data integrated from several sources in real or near-real time using various artificial intelligence tools, machine learning methods, analytical techniques like clustering and regression, and algorithms. FinTech startups are using big data analytics to analyze massive amounts of transactional data, customer behaviour, spending patterns, historical patterns, and network analysis, which aids in the development of fraud detection systems that identify anomalies such as suspicious transactions, hacking and login attempts, malware, and bot activities in real-time. Advanced analytics approaches predict attacks and fraudulent activities, identify patterns, analyze and reduce risks, and detect fraud utilizing sector-specific trends. Through risk management intelligence, digital applications are also used to alert clients about the security of their money and other security risks. Furthermore, big data analytics assists FinTech businesses in regulatory compliance by analyzing vast volumes of data to identify trends that suggest potential regulatory infringements. FinTech firms may use advanced analytics to comply with laws, decrease non-compliance risk penalties, and maintain a safe financial environment.

9.9 Use of artificial intelligence and machine learning

FinTech startups are enhancing the security of their services with artificial intelligence and machine learning. Artificial intelligence is defined as a branch of computer science that develops computers, computer-controlled robots, or computer systems that perform tasks that require human intelligence, such as visual perception, problem-solving, speech recognition, decision-making, understanding natural language, and using sensors to perceive their environment autonomously or with less human intervention. Artificial intelligence aims to create self-sufficient systems that imitate human behaviour by replicating natural intellect to solve complex problems. On the other hand, machine learning is a branch of artificial intelligence that employs algorithms and statistical models to enable computer systems to train data and make predictions, interpret data patterns, make decisions based on past experiences, and improve their performance on a specific task without being explicitly programmed. It solves business issues by using algorithms and analytics to develop predictive models. It is widely used in domains like image and speech recognition, natural language processing, recommendation systems, autonomous vehicles, and many more [54]. The global market for artificial intelligence in the FinTech business is predicted to be US$4,963.8 million in 2023, rising to US$11,890 million by 2030. FinTech cybersecurity professionals are leveraging artificial intelligence, machine learning, and analytics technologies to swiftly analyze massive volumes of data to detect suspicious behaviours or to detect, predict, and prevent fraud, emerging risks, unauthorized data access and usage, and other threats in real time. To identify and prevent financial fraud, they use cognitive computing techniques like real-time monitoring and alerting, tokenization, anomaly detection, geo-location, risk management, and network analysis [66], [80], [160], [163]. With artificial intelligence powering FinTech systems, platforms, and networks, fraud analysts can focus on higher-level security issues, while FinTech businesses can deliver services to their clients via artificial intelligence-driven chatbots. Artificial intelligence models increase client security by resetting forgotten passwords and allowing clients to utilize biometrics for additional authentication security. Using artificial intelligence and machine learning in FinTech aids in monitoring financial transactions, and artificial intelligence algorithms may discover abnormal patterns that differ from the clients' everyday spending habits, and suspicious behaviours can be quickly recognized before they occur [78]. Artificial intelligence, machine learning, deep learning, natural language processing, knowledge representation and reasoning, and rule-based expert systems aid in the automation of specific security measures and activities for rigorous control and robust security [167], [168]. Machine learning helps detect insider threats, analyse FinTech network traffic and user behaviour, and detect social engineering, intrusion, and malware [164], [169]. Natural language processing assists in analysing customer support inquiries and detecting potential fraud attempts before they occur. It also aids in the

detection of suspicious messages or phone calls from clients by exploring the different languages used and identifying probable fraudulent activity [160]. Predictive analytics detect potential fraud before it occurs by analyzing prior transaction data from clients, recognizing trends, and providing notifications to the appropriate parties [160].

9.10 Cloud computing technologies

FinTech firms are deploying their systems and platforms in the cloud to store and manage their financial data securely. Most recent cloud service providers use strong security measures such as encryption, data loss prevention solutions, tokenization, access controls, API security solutions, next-generation firewalls, single sign-on solutions, intrusion detection and prevention systems, endpoint security, virus protection, zero-trust security verification, penetration testing, audits, virtual private networks, and other security mechanisms to protect against unauthorized access and cyber threats. Many FinTech businesses are utilizing hybrid cloud architecture, which includes a more secure framework for developing FinTech systems and platforms and securely storing data. Cloud service providers offer hybrid cloud computing servers to ensure end-to-end data security [72], [164]. Distributed data storage in cloud systems is also possible with hybrid cloud computing servers. FinTech companies employ hybrid cloud services to secure sensitive clients and financial data, implement multi-factor authentication, and protect against fraudulent operations [59]. Cloud service providers assist FinTech firms in meeting essential standards and regulations such as PCI DSS, GDPR, and ISO 27001, as well as increasing and decreasing cloud resources and services based on their needs and demands. To ensure the successful implementation of FinTech services in the cloud, the cloud service providers' security professionals must continuously monitor and measure cloud security metrics and indicators such as availability, reliability, confidentiality, integrity, and scalability. FinTech firms must select cloud service providers with a well-known reputation. FinTech firms must use cloud service providers that implement excellent security protocols and employ modern encryption standards and data storage solutions.

9.11 FinTech regulatory sandboxes

The broad use of FinTech services has not satisfied all current institutional and regulatory requirements, causing financial authorities worldwide to develop FinTech regulatory sandboxes to stimulate innovation in the financial industry while being vigilant to emerging risks. A FinTech regulatory sandbox is a technical environment created by regulators to allow FinTech startups to conduct experiments and test new innovative financial ideas, business models, products, services, solutions, technologies, and policies in a live and controlled ecosystem under the regulators' supervision [39]. Applying the standards is blended with the testing criteria in the sandbox to prevent innovative ideas from being repressed by expensive regulatory requirements and allow regulators to oversee FinTech companies as they test their products and services before implementation. The regulatory sandbox incorporates adequate mechanisms to defend against the effects of failure and maintain the financial system's safety and soundness. Enhanced Regulatory Sandbox (Australia), Central Bank of Bahrain’s FinTech & Innovation Unit (Bahrain), Canadian Securities Administrators Regulatory Sandbox (Canada), International Financial Services Centres Authority Regulatory Sandbox (India), Capital Markets Authority (Kenya), National Technology and Innovation Sandbox (Malaysia), Bank of Russia's Regulatory Sandbox (Russia), Monetary Authority of Singapore FinTech Regulatory Sandbox (Singapore), Financial Conduct Authority Regulatory Sandbox (United Kingdom), are some of the examples of FinTech regulatory sandbox. This FinTech regulatory sandbox provides a safe and confined environment for startups to experiment and test financial innovations like products, services, and business models with clients inside and outside the existing regulatory framework. It lowers the costs of innovation and the obstacles to entry, allowing regulators to gather critical information before taking regulatory action. They promote financial inclusion by encouraging the development of low-cost products or services for the unbanked population, new distribution channels for remote and marginalized people and communities to access the formal financial system, and reduced security risks for business networks by categorizing them as vulnerable, valuable, or high-risk [52]. It also improves product development and investment opportunities, makes it easier to create policies that promote innovation, helps to create a level playing field for new startups to enter the market, and ensures that any problems with business models, products, services, solutions, technologies, and policies are identified and fixed early in the development process. It lowers legal and testing costs for both regulators and innovators through purpose-built structures, mechanisms, and capabilities; it promotes competition by allowing new startups to compete on an equal playing field with more prominent and established FinTech firms; it enables more informed decision-making in product design and development through access to real-time data; and it allows capacity building and knowledge of financial trends and innovations within FinTech regulatory institutions.

9.12 Blockchain technologies

FinTech startups are implementing blockchain-based systems to improve their security by allowing their clients to prove their identity only once before conducting transactions, managing and sharing personal data, signing in without a password, and signing any document electronically. Blockchain technology has distinct characteristics like decentralization, encryption, immutability, and distributed ledger that aid in the security of FinTech systems and platforms. Blockchain technology receives significant investment in FinTech because it provides decentralized and

traceable storage [138]. The shared immutable ledgers secure transaction data over the FinTech Network using advanced cryptographic techniques such as asymmetric encryption mechanisms with public and private keys, allowing different parties in the business network to collaborate, manage data, and reach agreements. Ethereum enables the development of a secure application code that is resistant to fraud and malicious third parties. It also generates market-leading technologies to protect data privacy in the software stack layers with restricted data sharing in the business network to promote trust and transparency while maintaining confidentiality and privacy. The smart contract enables both parties to make an agreement and conduct transactions without the intervention of third parties while preserving security and trustworthiness. It employs mutualized standards, protocols, and shared procedures to provide network participants with a single shared source of truth [80]. Blockchain enables FinTech clients to utilize biometric fingerprints stored on a distributed ledger to identify themselves [42], [72]. Furthermore, blockchain technology allows FinTech organizations to track the entire transaction process safely and reliably.

9.13 Regular testing

FinTech firms must test their systems and applications regularly to ensure data security, and this can be accomplished efficiently by establishing a professional security testing team, doing penetration testing, and completing an IT security audit.

9.14 Continuous monitoring of threats

FinTech firms must constantly monitor threats in their systems, platforms, and networks. Some strategies to identify and prevent complex threats in FinTech systems, platforms, and networks include global threat intelligence, contextual awareness, and custom rules. When threats are found, startups, employees, and clients must be notified immediately so that corrective actions may be taken. Furthermore, centralized visibility might be a helpful approach to monitoring threats [163], [170], [171].

9.15 Implementing zero-trust policy

Since insiders are responsible for most security breaches in FinTech, all employees and clients must be verified before using FinTech resources. In FinTech, implementing a zero-trust policy helps to prevent insider threats, brute-force attacks, privilege escalation, and data theft. It is recommended that FinTech system users have rigorous role-based and least-privilege access. Furthermore, FinTech firms must maintain strict password and multi-factor authentication standards and encrypt personal login credentials and financial data [172], [173].

9.16 Creating a robust cybersecurity culture

FinTech firms must have a strong cybersecurity culture to prevent attackers from exploiting human errors. A robust cybersecurity culture may be accomplished by regularly teaching FinTech employees how to detect fraud, educating employees and customers on what to click and what not to click, and establishing a clear line of command so that employees know what and whom to report to if something suspicious occurs [170], [174].

9.17 Implementing stringent security policies

FinTech firms are requested to enforce strict policies to build a solid foundation for risk management. The policies must be well-planned, and the following factors must be considered when developing the policies. (i) establishing clear goals, objectives, and expectations; (ii) choosing and applying security frameworks; (iii) planning security processes, procedures, and tools; (iv) planning the best incident response and disaster backup plans; (v) establishing roles and responsibilities; (vi) continuously monitoring security risks; (vii) stressing on developing cyber resilience; and (viii) regular policy updates are required [163], [175], [176].

Other mitigating measures include (i) use of firewalls to prevent unauthorized persons from accessing the FinTech network and managing, controlling, and filtering network traffic; (ii) the use of antivirus software that must be updated regularly; (iii) apply updates and patches to solve known vulnerabilities in FinTech platforms and operating systems; (iv) implement a cyber-resilience policy; (v) utilize Endpoint security solutions; and (vi) remove unnecessary software from FinTech servers and clients' mobile devices to prevent malicious activities [18].

Cybersecurity in the FinTech industry protects confidential financial and customer data and assets, ensures the integrity of financial transactions, enhances client trust, detects fraud and compliance with regulatory standards, increases productivity, protects the reputation of FinTech startups and intellectual property, improves collaboration among the FinTech stakeholders, ensures the security of remote works, and many more.

10. MATERIALS AND METHODS

A comprehensive literature review methodology was used in this study. A comprehensive review is a systematic, scientifically structured evaluation of a specific literature base that leverages the rigour of original research to reduce result bias. The methodology was divided into three parts. The first phase ascertains the research questions used in the

study; the second phase defines the research strategy for obtaining pertinent research publications. It also explains the specific search keywords and the appropriate criteria for selecting the research papers [177]. The third phase describes how the data was analyzed.

10.1 Phase 1. Planning the comprehensive review

This phase involves identifying the need for a comprehensive literature review method, defining the research questions the review will address, and the basic review procedures to achieve the study's goal. Research questions were used to support the review procedure, and the papers were selected using extensive online searches in the different publishing houses and libraries, and inclusion and exclusion criteria were applied. Table 2 shows the research questions for the comprehensive review study.

Table 2. Summary of the research questions and motivations

Research Questions	Motivations
RQ1: What are the key cybersecurity issues in the FinTech industry?	To identify the cybersecurity issues in the FinTech industry.
RQ2: What are the available mitigation measures for improving cybersecurity in FinTech?	To identify the mitigation measures available for improving cybersecurity in FinTech.

10.2 Phase 2. Conducting the comprehensive review

The steps in selecting the relevant papers and the search process are based on comprehensive literature review methods, as shown in Figure 6.

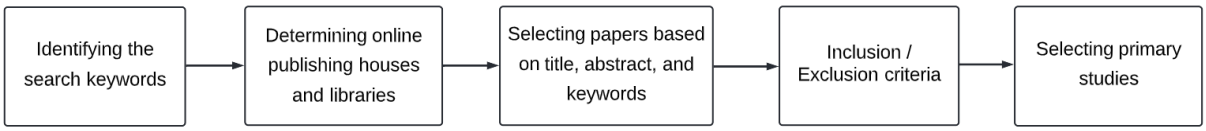

Figure 6. The steps in selecting the relevant studies [177]

There are four main steps involved in the identification of relevant papers, which are described as follows:

Step 1. Selecting the research studies: This involves finding many research papers related to the study, determining the sources to search from, and identifying the keywords to use. The keywords for searching the research papers in online databases, publishing houses, and libraries are defined by breaking down the research questions into separate terms and creating a list of synonyms and abbreviations. The keywords are divided into two (2) categories, each of which includes synonyms of the keywords pertinent to the research question:

- Category 1: Find research papers related to financial technology: ("Financial Technology" OR "FinTech" OR "History of FinTech" OR "Evolution of FinTech" OR "Drivers for the Growth of FinTech" OR "Segments of FinTech" OR "FinTech Ecosystem" OR "FinTech Business Model" OR "FinTech Application").
- Category 2: Find research papers related to cybersecurity issues and their mitigation measures ("Cybersecurity issues in Financial Technology" OR "Cybersecurity issues in FinTech") AND ("Cyber Security in FinTech" OR "Mitigation Measures in FinTech").

Step 2. Specifying the sources of research studies: When the search keywords were identified, the researchers determined the online publishing houses, digital libraries, and journals to search from. The researchers used the chosen keywords to search for related studies from online publishing houses and digital libraries such as IEEE Xplore Digital Library, ScienceDirect, Taylor & Francis, Emerald Insight, Springer, SAGE, Wiley Online Library, Hindawi, MDPI, ACM Digital Library, IGI Global, and Google Scholar.

Step 3. Selecting the primary research studies: The researchers used multiple stages to choose the relevant research papers that answered the above research questions.

The first stage includes filtering and sorting important research papers by scanning through their titles, abstracts, and keywords, where 195 research papers were retrieved from different Journal Articles, Conference Proceedings, Book chapters, Reports, and Websites that matched the keywords. Figure 7 shows the categories of research papers selected for the study.

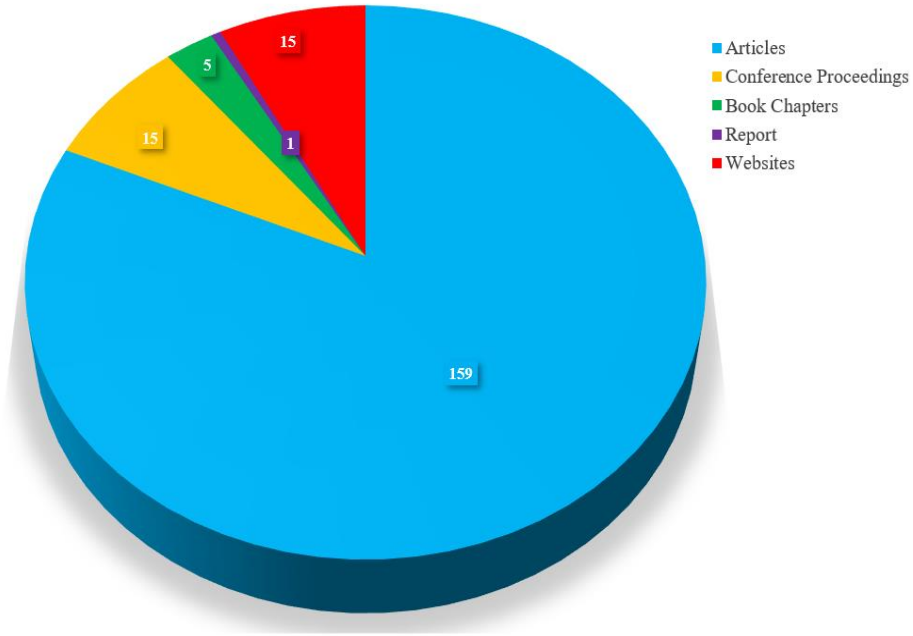

Figure 7. Categories of research papers

The second stage applies inclusion and exclusion criteria to reduce and select the relevant research studies to be reviewed, as summarised in Table 3.

Table 3. Inclusion and exclusion criteria for selecting the relevant research studies

Inclusion Criteria	Exclusion Criteria
Studies related to FinTech	Studies not written in English.
Studies related to cybersecurity issues in the FinTech industry	Reviews and surveys without results and reasonable research contributions
Studies related to mitigation measures for improving cybersecurity in FinTech	FinTech studies whose content lacks relevance, originality, and impact
FinTech studies published from January 2020 to March 2024	FinTech studies published before January 2020

In the third stage, after applying inclusion and exclusion criteria, studies not written in English, reviews and surveys without results and reasonable contributions, FinTech studies that lack relevance, originality, and impact, and studies published before January 2020 were eliminated from the research papers retrieved from online publishing houses and digital libraries. A total of 195 relevant research papers were reviewed, of which 27 were from IEEE Xplore Digital Library, 39 from MDPI, 18 from ScienceDirect, 6 from Taylor & Francis, 1 from Emerald Insight, 7 from Springer, 3 from SAGE, 1 from Wiley Online Library, 1 from Hindawi, 1 from ACM Digital Library, 5 from IGI Global, and 86 from Google Scholar. Figure 8 shows the distribution of the research papers based on online publishing houses and digital libraries.

Figure 9 shows the distribution of paper sources based on the digital libraries.

The researchers started searching the research papers in March 2023 and continued until the review paper was submitted for publication. Figure 10 shows the distribution of the research paper sources based on the year of publication.

Figure 11 shows the distribution of the number of research papers from different digital libraries based on the year of publication.

10.3 Phase 3. Analysing the data

The selected research papers were grouped based on the major areas identified in the abstract, such as FinTech history and evolution, FinTech drivers, FinTech segments, FinTech ecosystem, FinTech business model, FinTech applications, cybersecurity issues in FinTech, and mitigation measures in FinTech. A thematic analysis was used to extract each paper's key concepts, methodologies, and findings. The study focused on understanding the cybersecurity issues in FinTech and their mitigation measures.

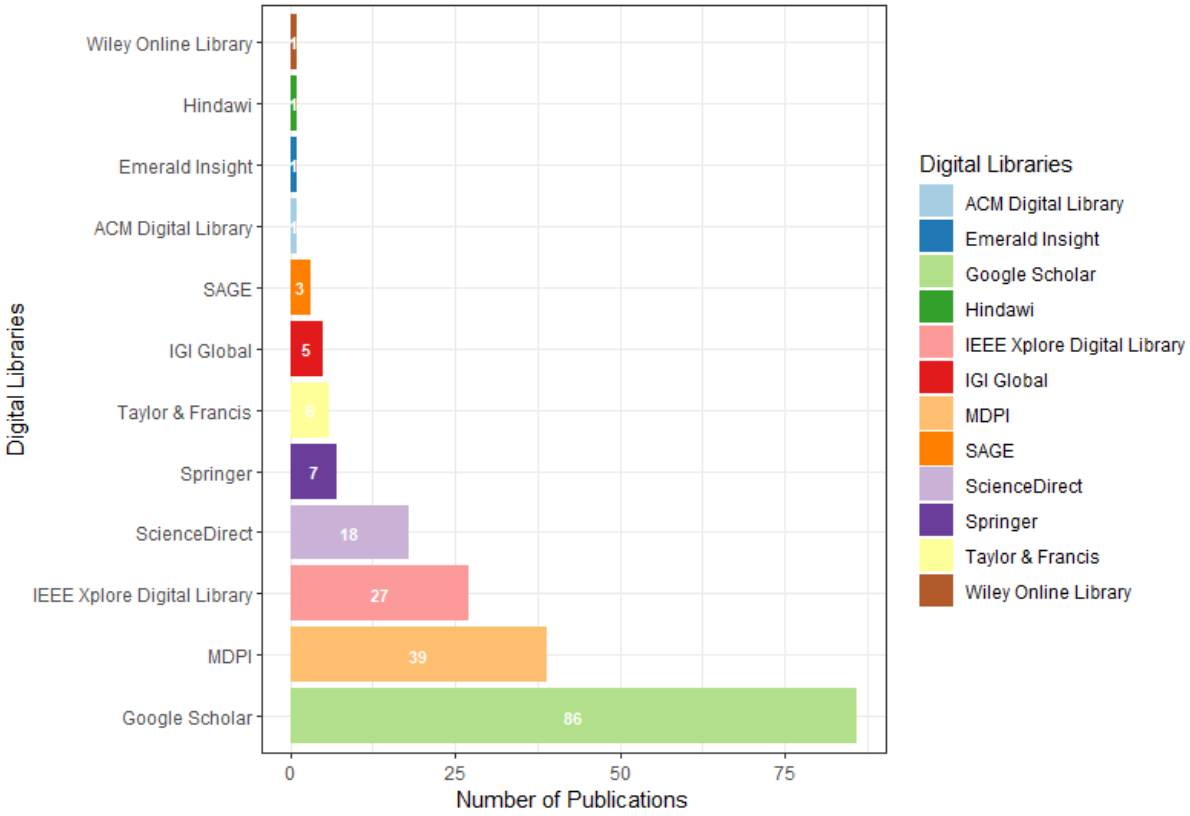

Figure 8. Distribution of the research papers based on online publishing houses and digital libraries

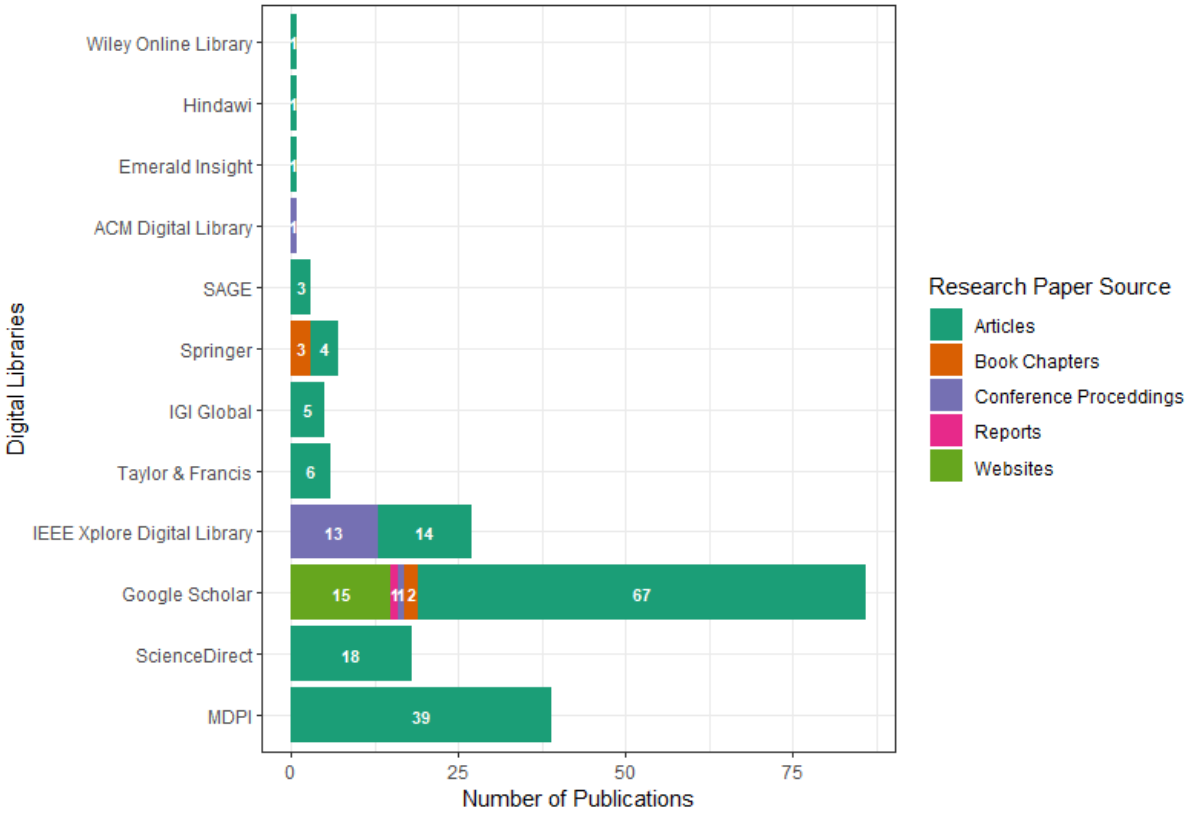

Figure 9. Distribution of research paper sources based on the digital libraries

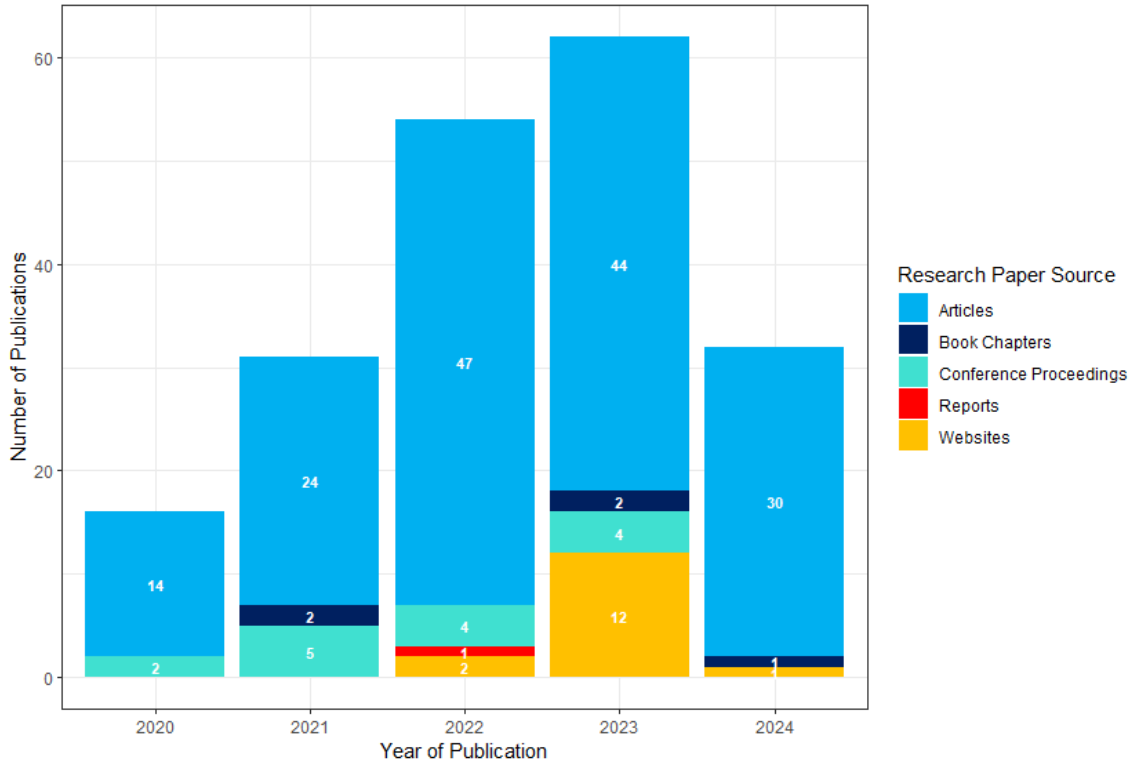

Figure 10. Distribution of the research paper sources based on the year of publication

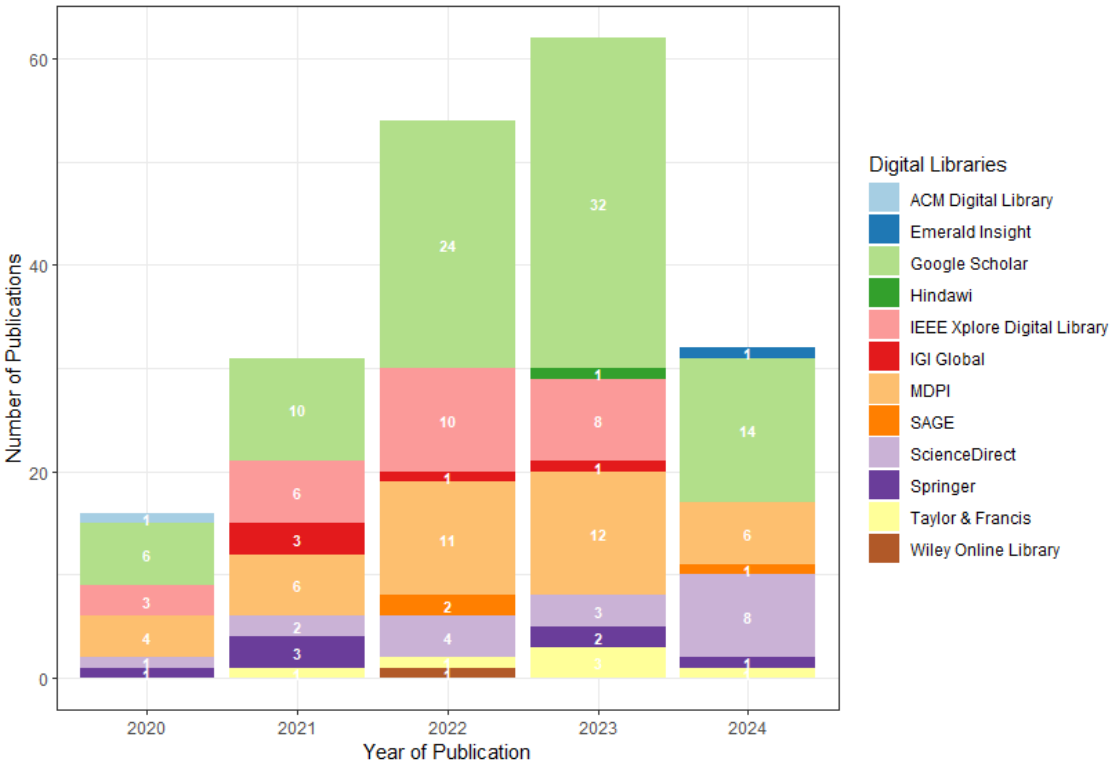

Figure 11. Distribution of the number of research papers from different digital libraries based on the year of publication

11. RESULTS AND DISCUSSION

The following security issues were identified and discussed through the comprehensive literature review.

Privacy issues: FinTech companies store sensitive financial and customer information that cybercriminals can steal or sell to third parties without their consent, thus violating their confidentiality, integrity, authentication, authorization, accountability, and transparency [178], causing substantial financial losses and reputational damage to FinTech firms and customers [174], [179], [180]. Several mitigation measures, such as the (i) use of encryption, (ii) access control, (iii) employee training and awareness, (iv) regular security audits and assessments, and (v) compliance with regulations, are implemented to deal with privacy issues [26], [59], [178], [181-185].

Data breaches: The vast amount of confidential login credentials and financial data in FinTech systems and applications are susceptible to data leakages [26], [185], which results in the compromise of confidentiality, integrity, availability, authentication, and authorization; loss of financial data and money; reputational damage; customer distrust; and legal liabilities [26], [59], [66-68], [80], [183]. Techniques such as (i) encryption, (ii) access control, (iii) employee training and awareness, (iv) regular data backup, and (v) compliance with regulations must be employed to thwart data breaches [26], [59], [178], [181-185].

Malware attacks: Cybercriminals use malware, such as ransomware and trojan horses, to infect FinTech systems and steal confidential financial data like customer login credentials, bank account, and credit card numbers [66-69], [80], [182], [185], [186]. Upon successful installation, ransomware can encrypt financial data and demand a ransom payment for the decryption key [183]. This attack violates FinTech firms', customers', employees', and systems' confidentiality, integrity, availability, authentication, authorization, and non-repudiation [67], [69], [80]. Resiliency against Malware attacks is enhanced by employing (i) cryptography, (ii) access control, (iii) user training and awareness, (iv) regular data backup, (v) behavioural analytics, (vi) intrusion detection systems, (vii) antivirus and antimalware software, and (viii) Firewalls [26], [59], [178], [181-186].

Hacking: Cybercriminals target legacy FinTech systems that are not secure by hacking them using malware and other cyber-attack vectors, resulting in violations of security principles like confidentiality, integrity, availability, authenticity, authorization, and non-repudiation [187], [188] and financial losses for FinTech service providers [59]. Several mitigation techniques, such as (i) the use of strong authentication and access control, (ii) data encryption, (iii) backup and recovery, (iv) monitoring and incident response, and (v) employee education and training, are enforced against hacking [59], [181-184].

Insider threats: Employees, third-party vendors, contractors, trusted business partners, or former employees of FinTech firms pose significant threats by intentionally or accidentally disclosing sensitive user login credentials and financial data, fraud, spreading malware in the FinTech system, infringement of intellectual property, and disruption of critical FinTech infrastructures [69], [182], [183], [185]. This threat violates the security principles of authenticity, integrity, availability, and confidentiality. Techniques such as (i) the use of strong authentication and access control, (ii) data encryption, (iii) behavioural analytics, (iv) employee training and awareness, and (v) implementing zero-trust policy are proposed to deal with insider threats [26], [59], [181-184], [189].

Identity theft: Cybercriminals obtain legitimate FinTech customers' identifiable information and login credentials from different sources, such as the (a) dark web, (b) social media, (c) shoulder-surfing clients' login credentials, (d) phishing, (e) hacking FinTech systems and clients' mobile devices, and (f) winning victims' trust to reveal them confidential information [185]. Once they have access to their victim's personal identification information and login credentials, the fraudsters can use them to apply for credit cards and loans, access their victims' FinTech accounts and perform financial services [66-68], [182], thus violating confidentiality, authentication, authorization, integrity, non-repudiation. To resist identity theft, measures such as (i) the use of strong authentication and access control, (ii) employee education and training, and (iii) a response plan are proposed [59], [183].

Social engineering attacks: Cybercriminals use social engineering to manipulate FinTech customers and employees to reveal their login credentials and sensitive financial information, which are used to access the FinTech system or perform fraudulent transactions illegally [69], [80], [187], [190]. Phishing is the most common social engineering technique used by fraudsters, where emails, SMS, or phone calls are used to persuade FinTech customers and employees to share their confidential information and login credentials or perform specific actions appearing to be coming from legitimate FinTech firms but fraudulent [66-68], [80] [182-186]. This attack compromises the security principles of authentication, authorization, confidentiality, integrity, and non-repudiation. Security against social engineering attacks is ensured by (i) using strong authentication and access control, (ii) data encryption, (iii) use of IDS and IPS, (iv) Firewalls, (v) employee education and training, (vi) endpoint protection solutions, (vii) having incident response plan, and (viii) regular security audits and assessments [59], [181-184].

DDoS attacks: Adversaries launch these attacks to prevent FinTech employees, customers, and third parties from accessing FinTech systems and services. At times, cybercriminals use DDoS attacks together with ransomware attacks to take complete control of FinTech systems and demand payment of a ransom to give FinTech Firms access to their devices, networks, systems, or encrypted data [174], [185]. This attack targets the availability of FinTech networks and services, resulting in loss of revenue, reputation damage, and loss of customer trust [183], [186], [191]. The security against DDoS attacks is ensured by (i) implementing IPS, (ii) Firewall configuration, (iii) anomaly detection, and (iv) having an incident response plan [18], [183], [192].

Cryptojacking: Fraudsters use cryptojacking to secretly mine cryptocurrency from FinTech firms using other people's computer resources. They lure their victims into clicking a malicious link sent via a phishing email, automatically loading the malicious code into the victim's machine [18]. Cryptojacking violates confidentiality, integrity, and availability security principles. Resiliency against cryptojacking is enhanced by (i) implementing IDS and IPS, (ii) Firewalls, (iii) using blockchain analysis tools, (iv) user education, (v) enforcing endpoint security solutions, and (vi) regular security audits [26], [171], [183].

Supply chain attacks: Most FinTech firms use the network of third-party vendors to support their financial infrastructures with payment networks/processors, Internet service, cloud services, data analytics, and IT services. However, third-party service providers may have security weaknesses which can be compromised by cybercriminals, resulting in data leakage, failure of FinTech service, cyber espionage, and reputational damage [69], [182], [183] and violation of security principles such as confidentiality, integrity, and privacy. Access control and authentication, data encryption, security training and awareness, continuous monitoring, and incident response plans are the mitigation measures enforced against supply chain attacks [59], [181-184].

APT: Hackers use advanced attack techniques, different methods, and tools to compromise FinTech systems and networks and their confidential financial data [187]. Advanced persistent threat violates the security principles of confidentiality, integrity, availability, authentication, authorization, and auditability. Security against APT is ascertained by (i) implementing IDS and IPS, (ii) strong access controls, (iii) employee training and awareness, (iv) using behavioural analytics, (v) continuous monitoring and auditing, (vi) endpoint protection, and (vii) having incident response plan [26], [59], [182], [183], [189][196].

Zero-day attacks: Cybercriminals take advantage of the weaknesses in the newly released FinTech systems and applications with unknown or unaddressed bugs to compromise the security of the system by creating a backdoor that they can use to bypass the authentication process or alter and sell the confidential financial information to third-parties [133], [187]. Zero-day attacks compromise the security principles of confidentiality, integrity, availability, authentication, authorization, and non-repudiation. Techniques such as (i) the implementation of IDS and IPS, (ii) employee education and training, (iii) data backup and recovery, (iv) behavioural analytics, (v) use of endpoint security solutions, and (vi) having incident response plan are proposed to deal with zero-day attacks [26], [182], [183], [189].

Salami attacks: By installing malware onto FinTech servers, the fraudsters can steal small amounts of money from FinTech customers' mobile wallets without notice and deposit it into their accounts [105], [133]. This attack compromises confidentiality, integrity, availability, non-repudiation, authentication, and authorization. The security against salami attacks is ensured by (i) implementing strong access controls, (ii) educating employees, (iii) using advanced analytics and artificial intelligence, and (iv) implementing fraud detection mechanisms [26], [59], [182], [183], [189].

Shoulder-surfing attacks: Adversaries use hidden cameras, binoculars, CCTV, and secret microphones, eavesdrop on their victims' sensitive conversations, and look over their victims' shoulders in ATMs, mobile money service centres, shopping centres, and other crowded or public places to steal their login credentials and additional sensitive financial information [105], [136]. Through shoulder-surfing attacks, the attackers can compromise the security principles of confidentiality and authentication. To resist this attack, [59], [183] recommended implementing (i) multi-factor authentication and (ii) emphasized security awareness training.

MiTM attacks: Cybercriminals eavesdrop on the communication between FinTech employees, customers, applications or the entire network, inject false data and commands or alter the message and resend it to the intended recipients without either party realizing it [133], [185]. This results in the compromise of confidentiality, integrity, authenticity, and non-repudiation. Mitigation measures such as (i) data encryption, (ii) recommended strong authentication, (iii) security awareness training, and (iv) regular security audits and monitoring were proposed to address MiTM attacks [59], [181-184].

SQLi: Adversaries can inject malicious code inside the FinTech application to obtain customer data [18], which results in the hacking of FinTech customers' databases [133] and violation of confidentiality, integrity, authentication, and authorization. The security against SQLi is ensured by (i) using a Web application Firewall, (ii) customer and employee training on security, and (iii) regular security audits [18], [183].

Brute-force attacks: Cybercriminals can guess or crack FinTech users' login credentials and other confidential information using trial-and-error methods or referring to a dictionary. Upon guessing the login credentials successfully, they can illegally access their victims' FinTech accounts [105], [126], thus compromising the FinTech systems and users' confidentiality, integrity, availability, authentication, and auditability. Resiliency against brute-force attacks is enhanced by (i) employing multi-factor authentication, (ii) IDS/IPS, (iii) security awareness training, and (iv) implementing a zero-trust policy [59], [183], [193].

Cloud environment security risks: FinTech firms opt for cloud computing services to increase their performance by linking with financial firms and their targeted markets. However, this cutting-edge technology comes with security risks, such as (i) a lack of suitable cloud security measures, which has resulted in (i) data leakage, (ii) Web-based systems complexity, and (iii) uncertainty of the cloud computing technical details [115], [194]. The security risks in the cloud environment have compromised confidentiality, integrity, availability, authentication, authorization, and auditability. Several mitigation measures such as (i) implementing strong authentication and access control, (ii) data

encryption, (iii) data backup and recovery plan, (iv) employee training and awareness programs, (v) compliance with security standards and regulations, (vi) regular security audits and penetration testing; and (vii) developing and implementing incident response plan, have been proposed to thwart cloud environment security risks [26], [59], [178], [181-185].

Blockchain risks: Many FinTech firms use blockchain platforms to secure their customers' and employees' sensitive login credentials and financial information. Nevertheless, blockchain-based transactions in FinTech still have vulnerabilities or risks that attackers can exploit. These risks include (a) hacking of the blockchain platforms, (b) malware infection of the blockchain platforms and networks, (c) hash functions collision, which gives the attackers the privilege to replace or alter the input data without tempering with its digest, (d) unauthorized transactions due to signature forgery, (e) compromise of confidentiality, integrity, availability, authentication, authorization, non-repudiation, and privacy, (f) breaking of cryptosystems using quantum computers, and (g) loss of private key, which results into loss of control on FinTech customers and employees' digital assets on the blockchain [89]. Security against blockchain risks is enforced by (i) using encryption, (ii) access control, (iii) monitoring and anomaly detection, (iv) having a disaster recovery plan, and (v) regular audits and testing [59], [181-184].

IoT risks: FinTech companies use IoT technologies to streamline payment processes, analyze large amounts of financial data, and give robust security to FinTech systems and applications [147]. However, this technology faces numerous risks and concerns, including (a) data privacy and security issues, (b) data management issues, (c) data density, (d) a lack of standards, (e) hacking, (f) DoS and DDoS attacks, (g) data theft, (h) identity theft, (i) system complexity, (j) integration issues, and (k) data ownership concerns [80], [149]. Different mitigation measures such as (i) secure authentication and access control, (ii) data encryption, (iii) strong Firewall, (iv) continuous monitoring and anomaly detection, (v) user education and awareness, and (vi) security testing and auditing have been proposed and implemented to address IoT risks [59], [181-184].

Money laundering and cryptocurrency-related risks: FinTech services are forms of anonymous financial transactions and involve transferring money by bypassing banks. It promotes money laundering by hiding income from tax authorities since it uses cryptocurrency for financial transactions [186], [195], thus violating confidentiality, integrity, non-repudiation, authentication, authorization, and non-repudiation. Several mitigation techniques and measures, such as (i) the use of blockchain analysis tools, (ii) regulatory compliance, (iii) the use of data analytics, (iv) user training and awareness, (v) natural language processing, and (vi) monitoring and reporting suspicious activities have been proposed to protect FinTech systems, applications, networks, and users against money laundering and cryptocurrency-related risks [26], [59], [171], [182], [183], [185].

Table 4 Summarises the cybersecurity issues, compromised security services, and mitigation measures in FinTech.

Table 4. Summarises the cybersecurity issues, compromised security services, and mitigation techniques in FinTech

References	Cybersecurity Issues	Compromised Security Services	Mitigation Measures
[26], [59], [66], [80] [174], [178], [180-185]	Data privacy concerns	Confidentiality Integrity Authentication Authorization Accountability Transparency	Encryption Access control Employee training and awareness Regular security audits and assessments Compliance with regulations
[26], [59], [66], [80], [178], [181-184]	Data breaches	Confidentiality Integrity Availability Authentication Authorization	Data encryption Access control Regular security training Data backup and recovery plan Compliance with regulations
[59], [66], [80], [183]	Malware attacks	Confidentiality Integrity Availability Authentication Authorization Non-repudiation	Cryptography Access control User training and awareness Regular data backup Behavioural analytics IDS Antivirus & antimalware software Firewalls
[59], [66], [80], [181-184]	Hacking	Confidentiality Integrity Availability Authenticity Non-repudiation Accountability	Strong authentication and access control Employee education and training Data encryption Backup and recovery Monitoring and incident response

[59], [66], [80], [181-184], [189]	Insider threats	Authenticity Integrity Confidentiality Availability	Employee training and awareness Strict access controls Monitoring and auditing Encryption and data protection Behavioural analytics Implementing zero-trust policy
[59], [66], [80], [183]	Identity theft	Confidentiality Authentication Authorization Integrity Non-repudiation	Access control Educate employees and individuals Establish a response plan
[59], [66], [80], [181-184]	Social engineering attacks	Authentication Authorization Confidentiality Integrity Non-repudiation	Employee training and awareness Strict access control Regular security audits and assessments Encryption and data protection Incident response plan
[18], [183], [192]	DDoS attack	Availability	IDS and IPS Firewalls Endpoint protection solutions Intrusion prevention systems Firewall configuration Anomaly detection Incident response plan
[26], [80], [171], [183]	Cryptojacking	Confidentiality Integrity Availability	IDS and IPS Firewall protection Blockchain analysis tools User education Endpoint security solutions Regular security audits
[59], [66], [80], [181-184]	Supply chain attacks	Confidentiality Integrity Privacy	Access control and authentication Data encryption Security training and awareness Continuous monitoring Incident response plan
[59], [66], [80], [182], [183], [189]	APT	Confidentiality Integrity Availability Authentication Authorization Auditability	IDS and IPS Strong access controls Employee training and awareness Behavioural analytics Endpoint protection Incident response plan Continuous monitoring and auditing
[26], [182], [183], [189]	Zero-day attacks	Confidentiality Integrity Availability Authentication Authorization Non-repudiation	IDS and IPS Employee education and training Data backup and recovery Behavioural analytics Endpoint security solutions Incident response plan
[26], [59], [66], [80], [182], [183], [189]	Salami attacks	Confidentiality Integrity Availability Non-repudiation Authentication Authorization	Implement strong access controls Educate employees Use advanced analytics and artificial intelligence Establish fraud detection mechanisms
[59], [66], [80], [183]	Shoulder-surfing attacks	Confidentiality Authentication	Multi-factor authentication Security awareness training
[59], [66], [80], [181-184]	MiTM attacks	Confidentiality Integrity Authenticity	Encryption Strong authentication Security awareness training

		Non-repudiation	Regular security audits and monitoring
[18], [183]	SQLi	Confidentiality Integrity Authentication Authorization	Web application firewall Security training Regular security audits
[59], [66], [80], [183]	Brute-force attacks	Confidentiality Integrity Availability Authentication Auditability	Multi-factor authentication Security awareness training IDS/IPS Implementing zero-trust policy
[26], [59], [66], [80], [178], [181], [183-185]	Cloud environment security risks	Confidentiality Integrity Availability Authentication Authorization Auditability	Strong authentication and access control Data encryption Data backup and recovery plan Employee training and awareness programs Compliance with security standards and regulations Regular security audits and penetration testing Incident response plan
[59], [66], [80], [181-184]	Blockchain risks	Confidentiality Integrity Availability Authentication Authorization Non-repudiation Privacy	Encryption Access control Regular audits and testing Monitoring and anomaly detection Disaster recovery plan
[59], [66], [80], [181-184]	IoT risks	Confidentiality Integrity Availability Authentication Authorization Privacy	Secure authentication and access control Encryption Implementing a strong firewall Continuous monitoring and anomaly detection User education and awareness Security testing and auditing
[26], [59], [66], [69], [80], [171], [182], [183], [185]	Money laundering and cryptocurrency-related risks	Confidentiality Integrity Non-repudiation Authentication Authorization Non-repudiation	Blockchain analysis tools Regulatory compliance Big data analytics User training and awareness Natural language processing Suspicious activity reporting

12. CONCLUSIONS

The growing popularity of FinTech has brought about substantial changes in financial services and made it a target for cybercriminals. This presents new vulnerabilities and challenges that must be adequately managed to maintain the integrity and security of FinTech systems. Therefore, this comprehensive review investigated cybersecurity issues and mitigation strategies to help pave the way for secure and reliable FinTech systems, foster innovation, and revolutionize the FinTech sector.

Throughout this review, the researchers have examined various cybersecurity issues facing the FinTech sector, such as privacy issues, data breaches, malware attacks, hacking, insider threats, identity theft, social engineering attacks, DDoS attacks, cryptojacking, supply chain attacks, APT, zero-day attacks, salami attacks, MiTM attacks, SQLi, brute-force attacks, cloud environment security risks, blockchain risks, IoT risks, and money laundering and cryptocurrency-related risks. Moreover, the researchers explored various mitigation measures and best practices used by industry stakeholders, including authentication and access control mechanisms, cryptography, regulatory compliance, IDS and IPS, fraud detection and prevention systems, regular data backup, basic security training, big data analytics, use of artificial intelligence and machine learning, implementing zero-trust policy, FinTech regulatory sandboxes, cloud computing technologies, blockchain technologies, frequent testing, continuous monitoring of threats,

creating a robust cybersecurity culture, implementing stringent security policies, use of firewalls, use of antivirus software, removal of unnecessary software from FinTech servers and clients' mobile devices, applying updates and patches to solve known vulnerabilities, implementing cyber-resilience policy, and utilizing Endpoint security solutions.

However, cybersecurity is not a static endeavour but a dynamic and continuing process that needs constant adaptation and vigilance. As technology evolves and cyber-attacks become more sophisticated, FinTech businesses, regulatory agencies, and other key stakeholders must work closely together and proactively recognize and resolve new cyber risks.

In conclusion, successfully mitigating cybersecurity risks in FinTech requires a multidimensional strategy that includes technology innovation, regulatory compliance, risk management methods, and a cybersecurity awareness culture at all firm levels. By embracing these principles and subscribing to a comprehensive cybersecurity architecture, the FinTech sector can promote trust, resilience, and sustainability in a digitally transformed financial environment.

Funding

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] R. Jain, S. Kumar, K. Sood, S. Grima and R. Rupeika-Apoga, “A Systematic Literature Review of the Risk Landscape in Fintech,” Risks, vol. 11, no. 2, pp. 1–15, 2023.

[2] W. Almack, “Fostering Responsible Innovation in Fintech,” Loyola of Los Angeles Law Review, vol. 56, no. 1, pp. 227–266, 2023.

[3] M. Jawarneh, M. Shawer, Abu and A. Shariah, “Investigating the Impact of Financial Technology (Fintech) on Small and Medium Enterprises in Developing Nations,” Iconic Research and Engineering Journals, vol. 6, no. 8, pp. 212–221, 2023.

[4] O. Lavrinenko, E. Čižo, S. Ignatjeva, A. Ohotina and K. Krukowski, “Financial Technology (FinTech) as a Financial Development Factor in the EU Countries,” Economies, vol. 11, no. 2, pp. 1–20, 2023.

[5] V. A. Thiruma, “FinTech is enabler or disruptive to the Banking Industry: An analytical study,” World Journal of Advanced Research and Reviews, vol. 17, no. 1, pp. 067–072, 2023.

[6] R. Rupeika-Apoga, S. Wendt and V. Geyfman, “Shareholders in the Driver’s Seat: Unraveling the Impact on Financial Performance in Latvian FinTech Companies,” Risks, vol. 12, no. 3, pp. 1–16, 2024.

[7] Q. Fang, “Application of FinTech in Digital Banking Operations in the Information Age,” Applied Mathematics and Nonlinear Sciences, vol. 9, no. 1, pp. 1–12, 2024.

[8] A. A. Aldaarmi, “FinTech Service Quality of Saudi Banks: Digital Transformation and Awareness in Satisfaction, Re-Use Intentions, and the Sustainable Performance of Firms,” Sustainability, vol. 16, no. 6, pp. 1–19, 2024.

[9] I., Kalenyuk, O. Куклін, Y. Panchenko, A. Djakona and M. Bohun, “Financial Innovations in the Smart City Ecosystem,” Finansovo-kreditna Dìâl′nìst′: Problemi Teorìï Ta Praktiki, vol. 1, no. 54, pp. 102–113, 2024.

[10] W. Zhou, “The Transformative Impact of FinTech on Financial Services: A Comprehensive Analysis. In Advances in economics, business and management research,” Atlantis Press, p. 85–91, 2024.

[11] Q. Liu, K. L. Chan and R. Chimhundu, “FinTech research: systematic mapping, classification, and future directions,” Financial Innovation, vol. 10, no. 1, pp. 1–33, 2024.

[12] Q. Chen, “Fintech Innovation in Micro and Small Business Financing,” International Journal of Global Economics and Management, vol. 2, no. 1, pp. 284–290, 2024.

[13] I. Harsono and I. A. P. Suprapti, “The Role of FinTech in Transforming Traditional Financial Services,” Accounting Studies and Tax Journal (COUNT), vol. 1, no. 1, pp. 1–11, 2024.

[14] G. Dicuonzo, M. Palmaccio and M. Shini, “ESG, governance variables and FinTech: an empirical analysis,” Research in International Business and Finance, vol. 69, pp. 1–9, 2024.

[15] Takeda, A.; Ito, Y. “A review of FinTech research,” International Journal of Technology Management, vol. 86, no. 1, pp. 67–88, 2021.

[16] Painoli, G.; Kumar; Dhinakaran, D.; Paul; Vijai, C. “Impact of Fintech on the Profitability of Public and Private Banks in India,” Annals of the Romanian Society for Cell Biology, vol. 25, no. 6, pp. 5419–5431, 2021.

[17] G. Wu and Q. Peng, “Bridging the Digital Divide: Unraveling the Determinants of FinTech Adoption in Rural Communities,” SAGE Open, vol. 14, no. 1, pp. 1–16, 2024.

[18] K. Gurdip, Z. H. Lashkari and A. H. Lashkari, “Understanding Cybersecurity Management in FinTech,” Springer Cham, p. 1-182, 2021.

[19] R. Patil and S. Bharathi, "A Study on the Business Transformation, Security issues and Investors Trust in Fintech Innovation," Cardiometry, vol. 24, pp. 918–932, 2022.
[20] R. Alt, G. Fridgen and Y. Chang, "The future of FinTech - Towards ubiquitous financial services," Electronic Markets, vol. 34, no. 1, pp. 1–13, 2024.
[21] K. Najaf, A. Haj Khalifa, S.M. Obaid, A.A.Rashidi and A. Ataya, "Does sustainability matter for Fintech firms? Evidence from United States firms," Competitiveness Review, vol. 33, no. 1, pp. 161-180, 2023.
[22] X. Ren, G. S. Aujla, A. Jindal, R. S. Batth and P. Zhang, "Adaptive Recovery Mechanism for SDN Controllers in Edge-Cloud Supported FinTech Applications," IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2112–2120, 2021.
[23] C. Baliker, M. Baza, A. Alourani, A. Alshehri, H. Alshahrani and K. R. Choo, "On the Applications of Blockchain in FinTech: Advancements and Opportunities," IEEE Transactions on Engineering Management, pp. 1–18, 2023.
[24] O. Doherty and S. Stephens, "Hard and soft skill needs: higher education and the Fintech sector," Journal of Education and Work, pp.1–16, 2023.
[25] M. Bouteraa, B. Chekima, N. Lajuni and A. Anwar, "Understanding Consumers' Barriers to Using FinTech Services in the United Arab Emirates: Mixed-Methods Research Approach," Sustainability, vol. 15, no. 4, pp. 1-22, 2023.
[26] R. Jain, D. Prajapati and A. Dangi, "Transforming the Financial Sector: A Review of Recent Advancements in FinTech," International Journal for Research Trends and Innovation, vol. 8, no. 2, pp. 250-267, 2023.
[27] H. A. Alshari and M. A. Lokhande, "The relationship between the risks of adopting FinTech in banks and their impact on the performance," Cogent Business & Management, vol. 10, no. 1, pp. 1–35, 2023.
[28] O. Mapanje, S. Karuaihe, C. L. Machethe and M. Amis, "Financing Sustainable Agriculture in Sub-Saharan Africa: A Review of the Role of Financial Technologies," Sustainability, vol. 15, no. 5, pp. 1–20, 2023.
[29] M. A. Hammadi, J. a. J. Del Río, M. Ochoa-Rico, O. A. Montero and A. Vergara-Romero, "Risk Management in Islamic Banking: The Impact of Financial Technologies through Empirical Insights from the UAE," Risks, vol. 12, no. 2, pp. 1–15, 2024.
[30] A. Tarawneh, A., Abdul-Rahman, S. I. M. Amin and M. F. Ghazali, "A Systematic Review of FinTech and Banking Profitability," International Journal of Financial Studies, vol. 12, no. 1, pp. 1–21, 2024.
[31] R. Benazir, A. Oeshwik and S. Shireen, "Fintech in Bangladesh: Ecosystem, Opportunities and Challenges," International Journal of Business and Technopreneurship, vol. 11, no. 1, pp. 73–90, 2021.
[32] E. G. Ng, B. Tan, Y. Sun and T. Meng, "The strategic options of fintech platforms: An overview and research agenda," Information Systems Journal, pp. 192–231, 2022.
[33] R. Sajid, H. Ayub, B. F. Malik and A. Ellahi, "The Role of Fintech on Bank Risk-Taking: Mediating Role of Bank's Operating Efficiency," Human Behavior and Emerging Technologies, vol. 2023, pp. 1–11, 2023.
[34] P. K. Ozili, D. Mhlanga, R. Ammar and M. Fersi, "Information Effect of FinTech and Digital Finance on Financial Inclusion during the COVID-19 Pandemic: Global Evidence," FinTech, vol. 3, no. 1, pp. 66–82, 2024.
[35] S. Ambore, H. Dogan and E. Apeh, "Development of Usable Security Heuristics for Fintech," 34th British HCI Conference (HCI2021), p. 121-132, 2021.
[36] KPMG. Pulse of Fintech KPMG: Amstelveen, The Netherlands, 2022.
[37] Statista, "Revenue of fintech industry worldwide from 2017 to 2023, with forecasts from 2024 to 2028(in billion U.S. dollars)," https://www.statista.com/aboutus/our-research-commitment, retrieved, 2024.
[38] M. P. Manggala, I. Wahidah and A. T. Hanuranto, "Security and Usability of User Authentication for Fintech Data Protection in Indonesia," 2022 International Conference on Decision Aid Sciences and Applications (DASA), p. 546-550, 2022.
[39] Q. V. Nguyen and V. C. Dang, "The effect of FinTech development on financial stability in an emerging market: The role of market discipline," Research in Globalization, vol. 5, pp. 1–15, 2022.
[40] S. Balaskas, M. Koutroumani, K. Komis and M. Rigou, "FinTech Services Adoption in Greece: The Roles of Trust, Government Support, and Technology Acceptance Factors," FinTech, vol. 3, no. 1, pp. 83–101, 2024.
[41] B. Chen, X. Yang and Z. Ma, "Fintech and Financial Risks of Systemically Important Commercial Banks in China: An Inverted U-Shaped Relationship," Sustainability, vol. 14, no. 10, pp. 1–20, 2022.
[42] A. Kumari and N. C. Devi, "The Impact of FinTech and Blockchain Technologies on Banking and Financial Services," Technology Innovation Management Review, vol. 12, no. 1/2, pp. 1–11, 2022.
[43] U. Baig, S. Zehra, S. Anjum and M. Hussain, "FinTech Past and Future: Ecosystem, Business Model and its Proximate Challenges," Pakistan Business Review, vol. 24, no. 1, pp. 40–61, 2022.
[44] M. B. Legowo, F. A. Sorongan and S. Subanidja, "Envisioning the Future of Collaboration for Banking and FinTech Industry," 2022 5th International Conference of Computer and Informatics Engineering (IC2IE), 2022.
[45] K. Mahmud, M. M. A. Joarder and K. Muheymin-Us-Sakib, "Adoption Factors of FinTech: Evidence from an Emerging Economy Country-Wide Representative Sample," International Journal of Financial Studies, vol. 11, no. 1, pp. 1–27, 2022.
[46] M. Asif, M. N. Khan, S. Tiwari, S. K. Wani and F. Alam, "The Impact of Fintech and Digital Financial Services on Financial Inclusion in India," Journal of Risk and Financial Management, vol. 16, no. 2, pp. 1–12, 2023.

[47] S. K., Cele and N. Mlitwa, "Fintechs in South Africa: Impact on regulation, incumbents and consumers," SA Journal of Information Management, vol. 26, no. 1, pp. 1–12, 2024.
[48] M. B. Amnas, M. Selvam and S. Parayitam, "FinTech and Financial Inclusion: Exploring the Mediating Role of Digital Financial Literacy and the Moderating Influence of Perceived Regulatory Support," Journal of Risk and Financial Management, vol. 17, no. 3, pp. 1–20, 2024.
[49] V. Juita, H. Roza and R. Rahayu, "Impact, benefits, security, and privacy of fintech adoption in Indonesia: A literature review," Operations Management and Information System Studies, vol. 2, no. 3, pp. 141-151, 2022.
[50] R. I. Akintoye, O. A. Ogunode, M. O. Ajayi and A. Joshua, "Cyber Security and Financial Innovation of Selected Deposit Money Banks in Nigeria," Universal Journal of Accounting and Finance, vol. 10, no. 3, pp. 643–652, 2022.
[51] S. F. Tan and G. C. Chung, "An Evaluation Study of User Authentication in the Malaysian FinTech Industry With uAuth Security Analytics Framework," Journal of Cases on Information Technology, vol. 25, no. 1, pp. 1–27, 2023.
[52] A. Shala and R. Perri, "Regulatory barriers for fintech companies in Central and Eastern Europe," Eastern Journal of European Studies, vol. 13, no. 2, pp. 292–316, 2022.
[53] M. Anifa, S. Ramakrishnan, S. Joghee, S. Kabiraj and M. M. Bishnoi, "Fintech Innovations in the Financial Service Industry," Journal of Risk and Financial Management, vol. 15, no. 7, pp. 1–19, 2022.
[54] B. Stojanović, J. Bozic, K. Hofer-Schmitz, K. Nahrgang, A. Weber, A. Badii, M. Sundaram, E. Jordan and J. Runevic, "Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications," Sensors, vol. 21, no. 5, pp. 1–43, 2021.
[55] J. Wang, "Verification Techniques in FinTech Compared from User Perspectives," Social Science Computer Review, vol. 0, no. 0, pp. 1–18, 2022.
[56] C. Cai, M. Marrone and M. Linnenluecke, "Trends in FinTech Research and Practice: Examining the Intersection with the Information Systems Field," Communications of the Association for Information Systems, vol. 50, pp. 803–834, 2022.
[57] Y. Yuan, G. W. Tan and K. Ooi, "Does COVID-19 Pandemic Motivate Privacy Self-Disclosure in Mobile Fintech Transactions? A Privacy-Calculus-Based Dual-Stage SEM-ANN Analysis," IEEE Transactions on Engineering Management, pp. 1–15, 2022.
[58] Z. Siddiqui and C. A. Rivera, "FinTech and FinTech ecosystem: A review of literature," Risk Governance and Control: Financial Markets & Institutions, vol. 12, no. 1, pp. 63–73, 2022.
[59] F.U. Rehman, H.M. Attaullah, F. Ahmed and S. Ali, "Data Defense: Examining Fintech's Security and Privacy Strategies," Engineering Proceedings, vol. 32, no. 1, pp. 1-8, 2023.
[60] A. S. Israa and A.-A. I. Adel, "Fintech in the Fourth Industrial Revolution: Literature Review on Usage and Concerns of e-Wallet Payment Transactions," 2023 International Conference on Cyber Management and Engineering (CyMaEn), p. 24-28, 2023.
[61] K. Lukiyanto, M. Trisilia, S. Vinanti and M. Wijayaningtyas, "Perception of the Role of Fintech on Formal Workers During the COVID-19 Pandemic (Study on Construction Workers)," KnE Social Sciences, vol. 9, no. 10, pp. 52–60, 2024.
[62] S. Akhtar, P. Sheorey, S. Bhattacharya and V. R. K. Kumar, "Cyber Security Solutions for Businesses in Financial Services," International Journal of Business Intelligence Research, vol. 12, no. 1, pp. 82–97, 2021.
[63] K. Najaf, I. Mostafiz and R. Najaf, "Fintech firms and banks sustainability: Why cybersecurity risk matters?," International Journal of Financial Engineering, vol. 8, no. 2, 2021.
[64] M. Alawida, A. E. Omolara, A. Jantan and M. M. Al-Rajab, "A deeper look into cybersecurity issues in the wake of Covid-19: A survey," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 10, pp. 8176–8206, 2022.
[65] M. S. I. Alsumaidaie, K. M. A. Alheeti, and A. K. Alaloosy, "Intelligent Detection of Distributed Denial of Service Attacks: A Supervised Machine Learning and Ensemble Approach," Iraqi Journal for Computer Science and Mathematics, vol. 4, no. 3, pp. 12–24, 2023.
[66] I. Mustapha, Y. Vaicondam, A. Jahanzeb, B. A. Usmanovich and S. H. B. Yusof, "Cybersecurity Challenges and Solutions in the FinTech Mobile App Ecosystem," International Journal of Interactive Mobile Technologies, vol. 17, no. 22, pp. 100–116, 2023.
[67] J. A. Jafri, S. I. M. Amin, A. M. A. Rahman and S. M. Nor, "A systematic literature review of the role of trust and security on FinTech adoption in banking," Heliyon, vol. 10, no. 1, pp. 1–20, 2024.
[68] J. O. Oladipo, C. C. Okoye, O. A. Elufioye, T. Falaiye and E. E. Nwankwo, "Human factors in cybersecurity: Navigating the FinTech landscape," International Journal of Science and Research Archive, vol. 11, no. 1, pp. 1959–1967, 2024.
[69] U. J. Umoga, E. O. Sodiya, O. O. Amoo and A. Atadoga, "A critical review of emerging cybersecurity threats in financial technologies," International Journal of Science and Research Archive, vol. 11, no. 1, pp. 1810–1817, 2024.

[70] J. A. R. C. Jayalath and S. C. Premaratne, "Analysis of Key Digital Technology Infrastructure and Cyber Security Consideration Factors for Fintech Companies," International Journal of Research Publications, vol. 84, no. 1, pp. 128–135, 2021.
[71] B. J. Nikkel, "Fintech forensics: Criminal investigation and digital evidence in financial technologies," Forensic Science International: Digital Investigation, vol. 33, pp. 1–17, 2020.
[72] M. J. Hossain, R. H. Rifat, M. H. Mugdho, M. Jahan, A. A. Rasel and M. A. Rahman, "Cyber Threats and Scams in FinTech Organizations: A brief overview of financial fraud cases, future challenges, and recommended solutions in Bangladesh," 2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), p. 190-195, 2022.
[73] R. P. Livea and S. Lipsa, "A Systematic Analysis on FinTech and Its Applications," 2021 International Conference on Innovative Practices in Technology and Management (ICIPTM), p. 131-136, 2021.
[74] M. M. Alshater, I. Saba, I. Supriani and M. R. Rabbani, "Fintech in Islamic finance literature: A review," Heliyon, vol. 8, no. 9, pp. 1-24, 2022.
[75] A. Kaur, P. Kumar, S. Taneja and E. Özen, "Fintech emergence - an opportunity or threat to banking," International Journal of Electronic Finance, vol. 13, no. 1, pp. 1–19, 2023.
[76] M. Kou, Y. Yang and K. Chen, "Financial technology research: Past and future trajectories," International Review of Economics & Finance, vol. 93, no. Part A, pp. 162–181, 2024.
[77] D. Arner, R. Buckley, K. Charamba, A. Sergeev and D. Zetzsche, "Governing FinTech 4.0: BigTech, Platform Finance, and Sustainable Development," Journal of Corporate & Financial Law, vol. 27, no. 1, pp. 1–71, 2022.
[78] N. S. Sharma, N. B. Kotaiah, N. S. Singh, N. K. Sagar and N. S. K, N. N. S. Durga, "Privacy-Preserving in FinTech using Deep Learning with Federated Learning in Cryptocurrency," Journal of Pharmaceutical Negative Results, vol. 13, no. 9, pp. 532–542, 2022.
[79] I. A. Bajwa, S. U. Rehman, A. Iqbal, Z. Anwar, M. Ashiq and M. A. Khan, "Past, Present and Future of FinTech Research: A Bibliometric Analysis," SAGE Open, vol. 12, no. 4, pp. 1–22, 2022.
[80] P. K. Kamuangu, "A Review on Cybersecurity in FinTech: Threats, Solutions, and Future Trends," Journal of Economics, Finance and Accounting Studies, vol. 6, no. 1, pp. 47–53, 2024.
[81] C. Wijaya, B. Y. Nugroho and M. F. Arkanuddin, "The Important Role of Financial Architecture Regulation Toward Fintech P2P Lending Ecosystem," Indonesian Journal of Business and Entrepreneurship, vol. 1, no. 1, pp. 13–24, 2024.
[82] B. L. Del Gaudio, S. Gallo and D. Previtali, "Exploring the drivers of investment in Fintech: Board composition and home bias in banking," Global Finance Journal, vol. 60, pp. 1–16, 2024.
[83] D. Sharma and P. Munjal, "Determining the key drivers of FinTech adoption in India," International Journal of Process Management and Benchmarking, vol. 16, no. 4, pp. 533–554, 2024.
[84] P. Choudhary and M. Thenmozhi, "Fintech and financial sector: ADO analysis and future research agenda," International Review of Financial Analysis, vol. 93, pp. 103201, 2024.
[85] S. K. A. Rizvi, B. Rahat, B. Naqvi and M. Umar, "Revolutionizing finance: The synergy of fintech, digital adoption, and innovation," Technological Forecasting and Social Change, vol. 200, pp. 123112, 2024.
[86] A. J. Kassner, "Factors influencing investment into PropTech and FinTech – only new rules or a new game," Journal of European Real Estate Research, pp. 1–17, 2024.
[87] A. Rania, A. Yomna, K. Sumathi and E. Rabab, "FinTech Global Outlook and The Bahraini Landscape: Empirical Exploratory Analysis and Documentary Evidence," 2021 International Conference on Decision Aid Sciences and Application (DASA), p. 1007-1015, 2021.
[88] M. S. Albarrak and S. A. Alokley, "FinTech: Ecosystem, Opportunities and Challenges in Saudi Arabia," Journal of Risk and Financial Management, vol. 14, no. 10, pp. 1–13, 2021.
[89] K. Nelaturu, H. Du and D. Le, "A Review of Blockchain in Fintech: Taxonomy, Challenges, and Future Directions," Cryptography, vol. 6, no. 2, pp. 1–52, 2022.
[90] P. Tamasiga, H. Onyeaka and E. H. Ouassou, "Unlocking the Green Economy in African Countries: An Integrated Framework of FinTech as an Enabler of the Transition to Sustainability," Energies, vol. 15, no. 22, pp. 1–28, 2022.
[91] B. A. Karaki, O. Al_Kasasbeh and G. Alsheikh, "FinTech and FinTech Ecosystem: A Case of Jordan-based SWOT Analysis," Review of Economics and Finance, vol. 21, 2061–2067, 2023.
[92] M. Kaur, A. Wasim, K. Hári and R. Kattumuri, "FinTech entrepreneurial ecosystem in India: Role of incubators and accelerators," Global Finance Journal, vol. 60, pp. 100933, 2024.
[93] R. R. Suryono, I. Budi and B. Purwandari, "Detection of fintech P2P lending issues in Indonesia," Heliyon, vol. 7, no. 4, pp. 1–10, 2021.
[94] F. Giglio, "Fintech: A Literature Review," International Business Research, vol. 15, no. 1, 80–85, 2022.
[95] R. Ebrahim, S. Kumaraswamy and Y. Abdulla, "FinTech in Banks: Opportunities and Challenges. In Innovative Strategies for Implementing FinTech in Banking," IGI Global, p. 100-109, 2021.
[96] T. D. V. V. R. Gudlur, "Fintech Future Business & Cyber Vulnerabilities and Challenges," 2023 IEEE 8th International Conference on Software Engineering and Computer Systems (ICSECS), p. 1–4, 2023.

[97] G. Wu, J. Luo and K. Tao, "Research on the influence of FinTech development on credit supply of commercial banks: the case of China," Applied Economics, vol. 56, no. 6, pp. 639–655, 2024.
[98] J. Nivedita, "160 Cybersecurity Statistics 2023," https://www.getastra.com/blog/security-audit/cyber-security-statistics/#:~:text=Cybersecurity%20statistics%20indicate%20that%20there,cost%20%248%20trillion%20by%202023, retrieved, 2023.
[99] M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, "Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview," Mesopotamian Journal of Cybersecurity, vol. 2023, pp. 57–63, 2023.
[100] Y. Hwang, S. Park and S. Park, "Sustainable Development of a Mobile Payment Security Environment Using Fintech Solutions," Sustainability, vol. 13, no. 15, pp. 1–15, 2021.
[101] A. Despotović, A. Parmaković and M. Miljković, "Cybercrime and Cyber Security in Fintech. In Digital Transformation of the Financial Industry. Contributions to Finance and Accounting," Springer, p. 255-272, 2023.
[102] M. Ahsan, K. E. Nygard, R. Gomes, M. Chowdhury, N. I. Rifat and J. F. Connolly, "Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning - A Review," Journal of Cybersecurity and Privacy, vol. 2, no. 3, pp. 527–555, 2022.
[103] N. Li, M. Xu, Q. Li, J. Liu, S. Bao, Y. Li, J. Li and H. Zheng, "A review of security issues and solutions for precision health in Internet-of-Medical-Things systems," Security and Safety, vol. 2, pp. 1–41, 2023.
[104] A. Yazdinejad, B. Zolfaghari, A. Azmoodeh, A. Dehghantanha, A. Dehghantanha, E. D. G. Fraser, A. G. Green, C. Russell and E. Duncan, "A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures," Applied Sciences, vol. 11, no. 16, pp. 1–24, 2021.
[105] G. Ali, M. A. Dida and A. E. Sam, "Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures," Future Internet, vol. 12, no. 10, pp. 1–27, 2020.
[106] B. Govindraj, "Understanding Fintech Security Concerns for a Safer Fintech Ecosystem," https://www.appsealing.com/fintech-security-concerns/, retrieved, 2023
[107] X. Hua and Y. Huang, "Understanding China's fintech sector: development, impacts and risks," European Journal of Finance, vol. 27, no. 4–5, pp. 321–333, 2021.
[108] M. Hollanders, "FinTech and financial inclusion: Opportunities and challenges," Journal of Payments Strategy & Systems, vol. 14, no. 4, pp. 315–325, 2020.
[109] B. Saliba, J. Spiteri and D. Cortis, "Insurance and wearables as tools in managing risk in sports: Determinants of technology take-up and propensity to insure and share data," Geneva Papers on Risk and Insurance-Issues and Practice, vol. 47, no. 3, pp. 499–519, 2021.
[110] Timeline of Cyber Incidents Involving Financial Institutions. (n.d.). Carnegie Endowment for International Peace and BAE Systems. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline, retrieved, 2023.
[111] A. Petrosyan, "Global most frequent cyber-attacks in financial industry 2022," https://www.statista.com/statistics/1323911/cyber-attacks-on-financial-organizations-worldwide-by-type/, retrieved, 2023.
[112] T. Pathe, "Malware Infections Deemed the Most Prolific and Persistent Threat to Businesses," https://thefintechtimes.com/malware-infections-deemed-the-most-prolific-and-persistent-threat-to-businesses/, retrieved, 2023.
[113] A. Petrosyan, "Global victims of financial desktop malware 2020-2022, by user type," https://www.statista.com/statistics/1319921/pc-global-financial-malware-attack-by-user-type/#statisticContainer, retrieved, 2023.
[114] S. Al-Jeshi, A. Tarfa, H. Al-Aswad, W. Elmedany and C. A Balakrishna, "Blockchain Enabled System for Enhancing Fintech Industry of the Core Banking Systems," 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), p. 209-213, 2022.
[115] S. S. Rapti, N. Fahria and S. R. Das, "Role of Bangladesh Bank on Cybersecurity in FinTech," IGI Global, p. 71–90, 2022.
[116] M. A. Ahmed, H. Sindi and M. Nour, "Cybersecurity in Hospitals: An Evaluation Model," Journal of Cybersecurity and Privacy, vol. 2, no. 4, pp. 853–861, 2022.
[117] J. Nivedita, "How Many Cyber Attacks Per Day: The Latest Stats and Impacts in 2023," https://www.getastra.com/blog/security-audit/how-many-cyber-attacks-per-day/, retrieved, 2023.
[118] Kaspersky, "Crimeware and financial cyberthreats in 2023," https://securelist.com/crimeware-financial-cyberthreats-2023/108005/, retrieved, 2022.
[119] M. H. Uddin, M. H. Ali and M. K. Hassan, "Cybersecurity hazards and financial system vulnerability: a synthesis of literature," Risk Management, vol. 22, pp. 239–309, 2020.
[120] Y. H. Yusoff, M. N. Jamaludin, M. A. A. Ramdan, N. A. A. Aziz, R. M. M. Halim and M. S. A. Bakar, "Factors Influencing the Emergence of Fintech in Malaysia: A Concept Paper," International Journal of Academic Research in Economics and Management and Sciences, vol. 11, no. 3, pp. 429–440, 2022.
[121] F. Allen, X. Gu and J. Jagtiani, "A Survey of Fintech Research and Policy Discussion," Review of Corporate Finance, vol. 1, no. 2021, pp. 259-339, 2022.

[122] N. Saxena, E. Hayes, E. Bertino, P. O. Ojo and K. R. Choo, "Burnap, P. Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses," Electronics, vol. 9, no. 9, pp. 1–29, 2020.
[123] D. R. McKnight and T. Tipton, "10 risks and cybersecurity strategies for banks in 2023," https://www.crowe.com/insights/10-risks-and-cybersecurity-strategies-for-banks-in-2023#:~:text=Cryptojacking%2C%20AI%2Dbased%20attacks%2C,costing%20companies%20more%20as%20well, retrieved, 2023.
[124] K. O. Asante-Offei and W. Yaokumah, "Cyber-Identity Theft and Fintech Services," Journal of Information Technology Research, vol. 14, no. 3, pp. 1–19, 2021.
[125] A. Petrosyan, "Identity theft consequences for victims worldwide 2023," https://www.statista.com/statistics/1389549/identity-theft-impact-victims-worldwide/#statisticContainer, retrieved, 2023.
[126] G. Ali, M. A. Dida and A. E. Sam, "Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda," Information, vol. 11, no. 6, pp. 1–24, 2020.
[127] S. Kaji, T. Nakatsuma and M. Fukuhara, "The Economics of Fintech," Springer Nature, p. 1-216, 2021.
[128] E. Nelson, "5 Growing Cyber Risks Facing the Financial Sector In 2023," https://agio.com/5-growing-cyber-risks-facing-hedge-fund-private-equity-firms-and-financial-advisors-in-2023/#gref, retrieved, 2023.
[129] T. Jabar and M. M. Singh, "Exploration of Mobile Device Behavior for Mitigating Advanced Persistent Threats (APT): A Systematic Literature Review and Conceptual Framework," Sensors, vol. 22, no. 13, pp. 1–38, 2022.
[130] B. Genge, P. Haller and A. Roman, "E-APTDetect: Early Advanced Persistent Threat Detection in Critical Infrastructures with Dynamic Attestation," Applied Sciences, vol. 13, no. 6, pp. 1–22, 2023.
[131] N. Peppes, T. Alexakis, E. Adamopoulou and K. Demestichas, "The Effectiveness of Zero-Day Attacks Data Samples Generated via GANs on Deep Learning Classifiers," Sensors, vol. 23, no. 2, pp. 1–21, 2023.
[132] S. Ali, S. U. Rehman, A. Imran, G. Adeem, Z. Iqbal and K. Kim, "Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection," Electronics, vol. 11, no. 23, pp. 1–25, 2022.
[133] I. T. Moon, M. Shamsuzzaman, M. F. Mridha and A. S. Rahaman, "Towards the Advancement of Cashless Transaction: A Security Analysis of Electronic Payment Systems," Journal of Computer and Communications, vol. 10, no. 07, pp. 103–129, 2022.
[134] O. J. Eze, J. T. Okpa, C. D. Onyejegbu and B. O. Ajah, "Cybercrime: Victims' Shock Absorption Mechanisms," IntechOpen, p. 110, 2023.
[135] R. Nakagawa, "Bank herding in loan markets: Evidence from geographical data in Japan," International Review of Finance, vol. 22, no. 1, pp. 72–89, 2020.
[136] A. Binitie Patience, N. Anujeonye Christiana and Ezzeh P. Oguguo, "Security against Shoulder Surfing Attack Adaptable to Feature Phones using USSD Technology," International Journal of Innovative Science and Research Technology, vol. 7, no. 12, pp. 560–568, 2022.
[137] W. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq and M. S. Khan, "Comprehensive Review of Cybercrime Detection Techniques," IEEE Access, vol. 8, pp. 137293–137311, 2020.
[138] T. Renduchintala, H. Alfauri, Z. Yang, R. Di Pietro and R. Jain, "A Survey of Blockchain Applications in the FinTech Sector," Journal of Open Innovation: Technology, Market, and Complexity, vol. 8, no. 4, pp. 1–43, 2022
[139] A. A. Sadawi, M. Hassan and M. Ndiaye, "A Survey on the Integration of Blockchain with IoT to Enhance Performance and Eliminate Challenges," IEEE Access, vol. 9, pp. 54478–54497, 2021.
[140] Y. Song, C. Sun, Y. Peng, Y. Zeng and B. Sun, "Research on Multi-Dimensional Trust Evaluation Mechanism of FinTech Based on Blockchain," IEEE Access, vol. 10, pp. 57025–57036, 2022.
[141] R. Weerawarna, S. J. Miah, X. Shao, "Emerging advances of blockchain technology in finance: a content analysis," Personal and Ubiquitous Computing, pp. 1–14, 2023.
[142] .T. Barros, E. F. Da Silva Neto, J. S. Neto, A. De Souza, V. C. Aquino and E. S.Teixeira, "The Anatomy of IoT Platforms - A Systematic Multivocal Mapping Study," IEEE Access, vol. 10, pp. 72758–72772, 2022.
[143] M. Bouzidi, N. Gupta, F. A. Cheikh, A. Shalaginov and M. Derawi, "A Novel Architectural Framework on IoT Ecosystem, Security Aspects and Mechanisms: A Comprehensive Survey," IEEE Access, vol. 10, pp. 101362–101384, 2022.
[144] N. Arora and P. D. Kaur, "Augmenting Banking and FinTech with Intelligent Internet of Things Technology," 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), p. 648-653, 2020.
[145] S. A. Siddiqui, S. Hameed, S. A. A. Shah, I. Ahmad, A. Aneiba, D. Draheim and S. Dustdar, "Toward Software-Defined Networking-Based IoT Frameworks: A Systematic Literature Review, Taxonomy, Open Challenges and Prospects," IEEE Access, vol. 10, pp. 70850–70901, 2022.
[146] Y. Liu, W. Yu, W. Rahayu and T. S. Dillon, "An Evaluative Study on IoT ecosystem for Smart Predictive Maintenance (IoT-SPM) in Manufacturing: Multi-view Requirements and Data Quality," IEEE Internet of Things Journal, vol. 10, no. 13, pp. 11160–11184, 2023.

[147] A. Munusamy, M. Adhikari, V. Balasubramanian, M. M. Khan, V. G. Menon, D. B. Rawat and S. N. Srirama, "Service Deployment Strategy for Predictive Analysis of FinTech IoT Applications in Edge Networks," IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2131–2140, 2023.
[148] L. S. Vailshery, "IoT connected devices worldwide 2019-2030," https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/#statistic Container, retrieved, 2022.
[149] A. S. Sadiq, A. L. Dehkordi, S. Mirjalili, S. Too and P. Pillai, "Trustworthy and Efficient Routing Algorithm for IoT-FinTech Applications Using Nonlinear Lévy Brownian Generalized Normal Distribution Optimization," IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2215–2230, 2023.
[150] A. Faccia, N. R. Moşteanu, L. P. L. Cavaliere and L. J. Mataruna-Dos-Santos, "Electronic Money Laundering, The Dark Side of Fintech," ICIME 2020: Proceedings of the 2020 12th International Conference on Information Management and Engineering, p. 29–34, 2020.
[151] A. G. Buja, M. Katan, N. M. H. Nasrijal, S. F. S. Alwi and T. G. Siang, "Into the Look: Security Issues, Crypto-Hygiene, and Future Direction of Blockchain and Cryptocurrency for Beginners in Malaysia," 2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE), p. 1-6, 2021.
[152] F. Alarfaj and N. A. Khan, "Enhancing the Performance of SQL Injection Attack Detection through Probabilistic Neural Networks," Applied Sciences, vol. 13, no. 7, pp. 1–11, 2023.
[153] I. S. Crespo-Martínez, A. Campazas-Vega, Á. M. Guerrero-Higueras, V. R. Del Castillo, C. Álvarez-Aparicio and C. Fernández, "SQL injection attack detection in network flow data," Computers & Security, vol. 127, pp. 1-11, 2023.
[154] A. Alrubaiq and T. Alharbi, "Developing a Cybersecurity Framework for e-Government Project in the Kingdom of Saudi Arabia," Journal of Cybersecurity and Privacy, vol. 1, no. 2, pp. 302–318, 2021.
[155] M. Vučinić, "Fintech and Financial Stability Potential Influence of FinTech on Financial Stability, Risks and Benefits," Journal of Central Banking Theory and Practice, vol. 9, no. 2, pp. 43–66, 2020.
[156] B. K Mohd and A. H. Abdul Aziz, "A Framework on The Integrity of Fintech in Information Security from Islamic Perspective," International Journal of Islamic Economics and Finance Research, vol. 2, no. 2, pp. 62-75, 2020.
[157] M. Rizinski, H. Peshov, K. Mishev, L. T. Chitkushev, I. Vodenska and D. Trajanov, "Ethically Responsible Machine Learning in Fintech," IEEE Access, vol. 10, pp. 97531–97554, 2022.
[158] Fortune Business Insights, "Cyber Security Market to Reach USD 366.10 Billion by 2028 Surging Number of E-Commerce Platforms to Amplify Market Growth: Says Fortune Business Insights. https://www.globenewswire.com/news-release/2022/01/05/2361317/0/en/Cyber-Security-Market-to-Reach-USD-366-10-Billion-by-2028-Surging-Number-of-E-Commerce-Platforms-to-Amplify-Market-Growth-Says-Fortune-Business-Insights.html, retrieved, 2022.
[159] A. Saxena, S. Tripathi and Nath, "Exploring the security risks and safety measures of mobile payments in FinTech environment in India," International Journal of Management, vol. 12, no. 2, pp. 408–417, 2021.
[160] A. Faccia, "National Payment Switches and the Power of Cognitive Computing against Fintech Fraud," Big Data and Cognitive Computing, vol. 7, no. 2, pp. 1-28, 2023.
[161] G. Ali, M. A. Dida and A. E. Sam, "A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications," Future Internet, vol. 13, no. 12, pp. 1–31, 2021.
[162] V. Merab, K. Nanuli and S. Maka, "Loan-Debt Peculiarities of the Population in Georgia," European Science Review, vol. 11–12, pp. 59–63, 2021.
[163] G. Singh, R. Gupta and V. Vatsa, "A Framework for Enhancing Cyber Security in Fintech Applications in India," 2021 International Conference on Technological Advancements and Innovations (ICTAI), p. 274-279, 2021.
[164] S. Mehrban, M. S. Khan, M. Nadeem, M. Hussain, S. Jeon, O. Hakeem, S. Saqib, L. M. Kiah, F. Abbas and M. Hassan, "Towards Secure FinTech: A Survey, Taxonomy, and Open Research Challenges," IEEE Access, vol. 8, pp. 23391–23406, 2020.
[165] K. Nayak, P. Singh and P. Dave, "Does data security and trust affect the users of FinTech?," International Journal of Management, vol. 12, no. 1, pp. 191–206, 2021.
[166] Y. Chang and J. Hu, "Research on Fintech, Regtech and Financial Regulation in China," Open Journal of Business and Management, vol. 08, no. 01, pp. 369–377, 2020.
[167] M. M. Mijwil, I. E. Salem, and M. M. Ismaeel, "The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review," Iraqi Journal For Computer Science and Mathematics, vol.4, no. 1, pp.87–101, 2023.
[168] I. H. Sarker, A.S.M. Kayes, S. Badsha, H. Alqahtani, P. Watters and A. Ng, "Cybersecurity Data Science: An Overview from Machine Learning Perspective," Journal of Big Data, vol. 7, pp. 1-29, 2020.
[169] A. A. McCarthy, E. Ghadafi, P. Andriotis and P. A. Legg, "Functionality-Preserving Adversarial Machine Learning for Robust Classification in Cybersecurity and Intrusion Detection Domains: A Survey," Journal of Cybersecurity and Privacy, vol. 2, no. 1, pp. 154–190, 2022.
[170] M. Vučinić and R. Luburić, "Fintech, Risk-Based Thinking and Cyber Risk," Journal of Central Banking Theory and Practice, vol. 11, no. 2, pp. 27–53, 2022.

[171] J. R. Bhat, S. A. AlQahtani and M. Nekovee, "FinTech enablers, use cases, and role of future internet of things," Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 1, pp. 87–101, 2023.
[172] A. J. King, C. Williams, A. Heching, D. Moshkovich and Y. Tock, "Trust Anchor: Zero Trust Architecture for Digital Payments," Social Science Research Network, pp. 1–4, 2022.
[173] K. S. P. Nivarthi and G. Gatla, "Fighting Cybercrime with Zero Trust," American Academic Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS), vol. 90, no. 1, pp. 371–381, 2022.
[174] S. AlBenJasim, T. Dargahi, H. Takruri and R. Al-Zaidi, "FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study," Journal of Computer Information Systems, pp. 1–17, 2023.
[175] Y. Bu, H. Li and W. Xiao-Qing, "Effective regulations of FinTech innovations: the case of China," Economics of Innovation and New Technology, vol. 31, no. 8, pp. 751–769, 2022.
[176] H. H. Aldboush and M. Ferdous, "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, vol. 11, no. 3, pp. 1–18, 2023.
[177] L. Alhoraibi, D. M. Alghazzawi, R. M. Alhebshi and O. Rabie, "Physical Layer Authentication in Wireless Networks-Based Machine Learning Approaches," Sensors, vol. 23, no. 4, pp. 1–34, 2023.
[178] A. Junaidi, R. Wulandari, E. Susilowati, N. Safitri and M. Ikhsan, "A Literature Review on Fintech Innovations: Examining the Evolution, Impact, and Challenges," SEIKO: Journal of Management & Business, vol. 6, no. 2, pp. 438–448, 2023.
[179] S. M. Sapian, N. Abdulkadir and N. Ibrahim, "Trade finance in digital era: Can FinTech harness the current risks and challenges?," The Journal of Muamalat and Islamic Finance Research, vol. 18, no. 1, pp. 78–89, 2021.
[180] M. A. Sumlinski, W. Lian, D. Vasilyev, Y. Yang, Y. Liu, B. Garcia-Nunes, C. P. Marulanda, A. Siddiq and B. Bakker, "The Rise and Impact of Fintech in Latin America," International Monetary Fund, vol. 2023(003), pp. 1–61, 2023.
[181] N. Thakur and V. Sharma, "Enhancing Fintech Security - A Comparative Analysis of Advanced Security Algorithms," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), p. 230-235, 2023.
[182] S. Gopal, P. Gupta and A. Minocha, "Advancements in Fin-Tech and Security Challenges of Banking Industry," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), p. 1-6, 2023.
[183] M. N. Ali, M. Qualbi and M. Sajjad, "Cybersecurity Risks and Mitigation Strategies in Fintech," International Journal of Research Publication and Reviews, vol. 4, no. 4, pp. 1395–1398, 2023.
[184] E. Cambaza, "The Role of FinTech in Sustainable Healthcare Development in Sub-Saharan Africa: A Narrative Review," FinTech, vol. 2, no. 3, pp. 444–460, 2023.
[185] Y. Kwon, J.-D. Lee and J. Owens, "Managing Fintech Risks: Policy and Regulatory Implications," Asian Development Bank, p. 1-12, 2023.
[186] O. Gulyás and G. Kiss, "Impact of cyber-attacks on the financial institutions," Procedia Computer Science, vol. 219, pp. 84–90, 2023.
[187] R. Ankele, K. Nahrgang, B. Stojanović and A. Badii, "SoK: Cyber-Attack Taxonomy of Distributed Ledger- and Legacy Systems-based Financial Infrastructures," IACR Cryptology ePrint Archive, vol. 2020/1440. pp. 1-28, 2020.
[188] M. F. Barroso and J. Laborda, "Digital transformation and the emergence of the Fintech sector: Systematic literature review," Digital Business, vol. 2, no. 2, pp. 1–18, 2022.
[189] A. R. Kunduru, "Artificial Intelligence Advantages in Cloud Fintech Application Security," Central Asian Journal of Mathematical Theory and Computer Sciences, vol. 4, no. 8, pp. 48–53, 2023.
[190] A. Davtyan, "Cyber Vulnerability of Japanese Banking/Financial System," The EUrASEANs: Journal on Global Socio-economic Dynamics, vol. 1, no. 32, pp. 53–59, 2022.
[191] N. Sambuli, "When the Rubber Meets the Road: Cybersecurity and Kenya's Digital Superhighway," Carnegie Endowment for International Peace. https://carnegieendowment.org/2023/10/12/when-rubber-meets-road-cybersecurity-and-kenya-s-digital-superhighway-pub-90766, retrieved, 2023.
[192] A. Asha and S. K. Suresh, "Credit card fraud detection using artificial neural network," Global Transitions Proceedings, vol. 2, no. 1, pp. 35–41, 2021.
[193] M. C. Șcheau, C. M. Rangu, F. V. Popescu and D. M. Leu, "Key Pillars for FinTech and Cybersecurity," Acta Universitatis Danubius, vol. 18, no. 1, pp. 194-210, 2022.
[194] A. Vajid and A. W. Farooqi, "Issues and Challenges to Fintech Industry in India," EPRA International Journal of Economic and Business Review, vol. 10, no. 12, pp. 16–22, 2022.
[195] A. D. T. Kizi, T. G. Khahharovna, E. Dostonbek, B. Ogli and M. T. Jumaboevich, "Fintech Development in the Republic of Uzbekistan," Journal of Advanced Research and Stability, vol. 2, no. 1, pp. 71–82, 2023.
[196] G. Ali and M. M. Mijwil, "Cybersecurity for Sustainable Smart Healthcare: State of the Art, Taxonomy, Mechanisms, and Essential Roles," *Mesopotamian Journal of CyberSecurity*, vl.4, n.2, pp.20–62, May 2024.