Journal of Big Data

RESEARCH Open Access

Role of authentication factors in Fin-tech mobile transaction security

Habib Ullah Khan[1*], Muhammad Sohail[1], Shah Nazir[2], Tariq Hussain[3*], Babar Shah[4] and Farman Ali[5]

*Correspondence: habib.khan@qu.edu.qa; uom.tariq@gmail.com

[1] Department of Accounting & Information Systems, College of Business &, Economics Qatar University, Doha, Qatar
[2] Department of Computer Science, University of Swabi, Swabi, Pakistan
[3] School of Computer Science and Information Engineering, Zhejiang Gongshang University, Hangzhou, China
[4] College of Technological Innovation, Zayed University, Dubai 19282, UAE
[5] Department of Computer Science and Engineering, School of Convergence, College of Computing and Informatics, Sungkyunkwan University, Seoul, South Korea

Abstract

Fin-Tech is the merging of finance and technology, to be considered a key term for technology-based financial operations and money transactions as far as Fin-Tech is concerned. In the massive field of business, mobile money transaction security is a great challenge for researchers. The user authentication schemes restrict the ability to enforce the authentication before the account can access and operate. Although authentication factors provide greater security than a simple static password, financial transactions have potential drawbacks because cybercrime expands the opportunities for fraudsters. The most common enterprise challenge is mobile-based user authentication during transactions, which addresses the security issues against fraudsters. The confirmation of a user legitimation before the money transaction is highlighted by mechanisms and technologies from previous studies that may be helpful in user authentication. This study aims to identify the technologies for user authentication and the opportunity for their transformation to mobile money transaction security despite having all the legally required data for a transaction. This proposed review has identified the role of multifactor authentication techniques for authentication to mitigate the risk of fraudulent transactions—the analysis through 92 articles taken from famous publishers. The most relevant articles address authentication problems, of which 54 percent describe money transaction security, and the rest highlight the supporting technology for user authentication. The study platform described the technology-based approaches with the appreciation of new ideas for secure money transactions. The QR code and multifactor authentication are key terms that increased security by 46%. In addition, this also ensures the user is legitimate using advanced technologies and algorithms to predict and discover transaction risks and discourage fraudsters from trying.

Keywords: Artificial intelligence, Fin-Tech, Multifactor authentication, Money Transfer, Security, Risk mitigation

Introduction

Fin-Tech refers to financial operations based on technology, including money transactions to operate financial activities, including transactions to handle business and customers. It makes simple, easier, more accessible, and generally more affordable financial transactions for customers and businesses.

The encrypted blockchain, two-factor, and three-factor authentication have been widely accepted—fin-Tech attempts to streamline the transaction process, eliminating potentially unsecured processes for all parties involved. The best example is a mobile service, such as Venmo or CashApp, which allows users to pay each other 24 h daily, sending cash to their preferred bank account immediately. The receiver would need to go to the bank to deposit the funds if you chose to pay with cash or cheque instead.

Mobile commerce is described as doing business or providing a service using a mobile application connected to the internet to conduct a transaction using a mobile device for any money. It may be used to make online purchases, pay bills, send money to others, make hotel reservations, and order your favourite meals from nearby restaurants. Mobile commerce generates more security issues than traditional e-Commerce since it conducts online business [1]. The massive use of mobile devices for online payments cannot satisfy the security requirements of protecting sensitive data or user privacy in e-commerce. However, maintaining mobile transactions' sustainable and steady advancement is difficult for online authentication technology based on traditional methods [2].

Online financial scams are among the most prevalent cybercrimes, likely due to rising digital currency usage. One of the simple cybercrimes that fraudsters target is using stolen credit or debit cards. The most common scam is with 39% in the category of fraud in Europe. The vast impact of scams was about 79% financial harm. The consequences are a financial loss of 66% and 29% no loss [3, 4].

The analysis paints a clear picture of why better authentication is necessary for online banking. It outlines the critical security issues and criminal activity that requires authentication improvement and demonstrates how customers and financial institutions are driving the expansion of the online channel to deploy better authentication in the online banking environment. There are numerous solutions accessible. This study clarifies them and offers a resource for understanding them. Through the industrial experience base, technology is highly involved in security. It is available, as well as a set of recommendations for choosing and implementing improved authentication [5].

The message is one of the most popular and tested mobile services with worldwide accessibility across all global systems for mobiles (GSM)/code division multiple access (CDMA). The confirmation text is the short messaging service. The current short message service (SMS) can only secure plain text between the sender and various mobile phone users and servers for many purposes. The SMS lacks a built-in mechanism for text message authentication and provides no security for text messages sent as data [6].

A triangle relationship can be a schematic representation of an electronic commerce transaction between a person and an operator of the value service. On one side, the individual wants to benefit from the user's offer. A specific digital identification that specifies the social standing and their commercial relationship with the operator, such as proof of their capacity to pay for a service, is required to contact the operator. Through his identity and service management system, the operator manages the access rights to his valuable services and assigns these rights to authorized users or clients. A person who wants to utilize the user service must produce identification to prove her identity [7].

The automated teller machine ATM, credit card, debit card, and other cards are now frequently used for bank transactions and are essential in the banking industry. In this study, a biometric authentication system that combines the usage of a proximity sensor with a biometric authentication technique is proposed. This concept combines a shuffling keypad approach and a biometric fingerprint mechanism to increase the security level of ATM transactions [8]. The electro card usage poses issues related to the safety and security of financial transactions. It is suggested and discussed how to use mobile technologies to strengthen the security and protection of electronic bank card transactions. However, the customer reads the one-time password sent through short message service SMS and enters it in the username and password section [9].

The security issues so that future services might be better and more secure to categorize contemporary. Mobile Fin-Tech payment service sources into hardware manufacturers, operating system makers, payment platform insurers, and financial institutions; the study first defined existing and Fin-tech payment services by comparing them. Regarding reciprocal authentication, authorization, integrity, privacy, and availability, it defends the standards that mobile Fin-Tech payment services must satisfy and the security issues that both current and future mobile Fin-Tech payment services will face. Future mobile Fin-Tech payment systems are anticipated to become more secure due to the proposed study [10].

Multifactor authentication (MFA) is a fast-growing technology. Initially, only simple keywords were used to protect the data; after that, the password was used to protect personal accounts, called one-factor authentication, and two-factor authentication, which involves a one-time password (OTP) after verifying the password. However, fraudsters try to use different ticktacks to get the user data for fraudulent transactions to prevent fraud; it is essential to involve Biometric authentication called three-factor or can be more than there called multi-factor authentication. The integration of biometrics came from simple figure print IoT devices used in personal identification in the government sectors, but it is now integrated into mobile phones. The use of figure print is the physical identification of a person.

The improvement in the financial technology security the user authentication is concerned with using MFA approaches such as biometric and quick response (Q.R.) codes and the combination of personal identification number (PIN) and OTP instead of two-factor authentication (2FA) using (PIN) and subscriber identity module (SIM). The MFA may be obtained by implementing various security algorithms to identify the user that ensures user authentication to maintain data confidentiality, integrity, and privacy [11]. The proposed study has highlighted the technology for authentication that can quickly transform into user authentication. Except for having authentic information, it also should require biometric authentication during transactions, which may not be shareable like (one-time password) OTP, to ensure that the user is legitimate or fake.

The study objectives are:

- To analyze the previous study in comprehensive research about security authentication in Fin-Tech from the perspective of user authentication approaches. The extensive detail will outline the approaches and mechanisms reported for mobile secure money transfer systems in Fin-Tech.
- To extract detailed information about the user authentication framework to ensure user authentication, address fraud detection based on a multifactor authentica-

tion approach for secure mobile money transactions, and protect the user account from unauthorized access in Fin-Tech.
- To identify the various technologies in terms of hardware and software used in the previous system for secure mobile money transfer in the Fin-Tech sector and highlight the implemented method and its outcome in the user authentication system.
- To learn about the supporting features, technologies, and functions used for user authentication in the Fin-Tech mobile money secure transaction system.
- To highlight a previous SLR study based on current issues for mobile money secure transactions, whereas the Fin-Tech, make recommendations for developing an optimal security solution for mobile money transactions, and identify current challenges for researchers that will be useful in future research work.

The proposed paper is divided into sections, in which Sect. "Background study" has the research background and related studies about the proposed field. The intended information extraction methodology for the systematic literature review SLR task is outlined in Sect. "Methodology". Results from previous user authentication for safe mobile money transactions in Fin-Tech are presented in Sect. "Results and discussions". Explains the drawbacks, advantages, and benefits of the suggested SLR and identify the field's subsequent developments. Conclusions and challenges for future work are included in Sect. "Conclusion and future work".

Background study

The proposed study is to identify the multifactor authentication (MFA) role in user authentication for secure transactions via mobile devices. The mobile-based applications assist the money transaction in a secure environment to ensure the security of the user credential information. Transaction fraud may be caused by the leakage of user credential information. The massive technological developments have made the system vulnerable, where the fake app used to steal the user credential information for fraudulent transactions is concerning. The study was based on how to stop the transaction of someone having all the information, including OTP. Much work has been reported in the Fin-tech fields of money transactions in the last decade through mobile phones and bank applications. This paper section shows the relevant work written in the proposed area. The adversary model for mobile-based money transactions via random oracle model addresses users' strong security during online payment [12]. The Machine Learning-Assisted Secure Mobile Electronic Payment Framework effectively identifies fraud in mobile transactions and malware and user authentication. The effective Random Oracle Model is utilised to determine the existence of malware on a host system and the difficulties with multifactor authentication presented by mobile payments [13]. The safe IoT device-based trustworthy e-banking defence may be transferred to the mobile world. Regarding a secure transaction environment where trusted devices use tried-and-true methods, mobile-based financial transaction fraud detection is concerned [14].

The visual cryptographic scheme is used to check the transaction authentication number. The transaction information displays the transaction details and an authentication number while the card is encrypted [15]. The two-factor authentication uses a random code based on a secure online transaction algorithm, which is highly desired by businesses for a safe manner to make online purchases without a code working, or an unauthorized user cannot utilize the stolen card information for purchasing purposes. This is the security for the consumer credential information of credit card corporations from suffering financial loss [16]. The user authentication method for mobile applications uses biometric authentication on every feature within a single platform in a secure and user-friendly manner concerning the level of risk [17]. The efficient homomorphic media access control (MAC) use to guess the attacker randomly. It is a small finite field for authentication in network coding [18].

The innovative mechanism is independent of the manufacturer of the mobile device and the mobile network provider. It employs tamper-resistant components already present at the transaction terminals. The secured near-field transaction model will be helpful for mobile identification, payment, and access control in various security-sensitive IoT situations [19]. It is challenging to discern between legitimate and unauthorized users when detecting fraudsters in online transactions from gadgets [20]. The Quantum entanglement offers a blueprint for using built-in security advantages and user biometrics as authentication data with quantum communication. The authentication process is implemented over the user and server against a specific transaction, altering the quantum one-time passcode QOTP methodology [21]. The decentralized blockchain-based infrastructure for roaming authentication is fraud-proof. Smart contracts construct a roaming authentication protocol that includes user or app registration, authentication, and revocation. We use the Bloom filter for the revocation procedure for more efficiency [22].

Furthermore, a concrete architecture of a certificate-less signatures (CLS) scheme with better security is described to address the security vulnerabilities mentioned earlier. Assuming it is impossible to solve the discrete logarithm issue, the better technique may be strictly demonstrated using the forking lemma in the random oracle model. Finally, from our enhanced CLS technique, a secure transaction strategy for smartphones [23]. The acquired and inherence information are used as the three authentication factors for user authentication. As mentioned earlier, the authentication strategy alludes to the potential for executing the procedure in the mobile environment of the mobile application with assured authentication assistance [24]. The convergence of biometric information technologies for communication sparked the desire for more practical, cutting-edge, and enhanced security solutions. Because of the poor recognition rate caused by duplication, many biometrics technologies involve certain risks when used as a secure authentication solution for financial services. As a result, it is best to avoid this issue from emerging to improve the security of financial services and safeguard information. This study suggested an authentication security model for finger vein solutions. [25].

An image-based identity secure authentication approach more rigorously addresses the authenticated system [26]. The (SMS) text messages are used to register the authentication in the mobile phones for authorized users. This is a summary of two polls and several securities expert interviews. The SMS was evaluated as a practical way to reduce impersonation when using Internet resources, particularly in the banking sector [27]. The innovative blockchain anti-quantum transaction authentication method creates compact nondeterministic wallets. The critical thing to remember is that Seed Key is a collection of master public and private keys from which public and private keys are produced. Our new authentication approach, which may expand a lattice space to numerous lattice spaces with the associated key, uses the Bonsai Trees technique [28]. User identification via biometrics has been introduced. This contains characteristics like palm, finger, and iris prints for more precise personal identification. The suggested solution is best for personal identification and requires strong security while making online purchases, doing net banking transactions, etc. If the match rate for any unique biometric characteristic is lower than 80%, the user must be authenticated using a one-time [29]. Reliable message authentication codes are more effective than any others in the literature. The central concept behind the suggested methods is to develop more effective authentication processes using the security that the encryption algorithm may give rather than utilizing solo authentication components [30].

The module authenticates the user identification using a capacitive fingerprint sensor before establishing Bluetooth communication with an Android application loaded on the smartphone. The program handles both peer-to-peer payments made through near-field communication and fast response codes at the merchant point of sale. The tokenization mechanism significantly improves the security of the transaction. The application may also create a digital id [31]. Data security and privacy are provided through face recognition and fingerprint matching. This voting application via ATMs makes it very convenient for consumers to cast more ballots [32]. The photos are identical, and the user's mobile number receives a one-time password for login access. The Python library runs machine learning and deep learning algorithms for authentication using image processing [33]. The first step of the protocol establishes a session key for communications. The second phase of node authentication employs the ring signature. When a node signs a signature on behalf of others, the ring signature can lower computation costs. Other nodes can confirm the signature, and the signing node stays anonymous. Another benefit of ring signatures is that there is no restriction on the number of participants [34]. The continuous authentication for mobile banking apps utilizing behavioural biometrics is described, and its resource utilization performance is examined. The design uses data from the accelerometer, gyroscope, magnetometer sensors, touchscreen activity, and banking applications on Android smartphones [35].

User authentication via biometrics is possible using quantum entanglement and the known features of quantum encryption. Besides the end-user vulnerabilities, the analysis supports man-in-the-middle attacks for the existing and proposed models [36]. It is essential to acknowledge the examination of Fin-Tech and digital payment activities as a new technological sub-discipline within the field of digital forensics. The field of digital forensics is ideally situated to support practitioners with research to improve investigations into Fin-Tech and technological financial activities [37]. The multifactor authentication system was created to accommodate the preferences of international banks. Specifically, multifactor authentication systems are now used in the banking industry in terms of best practices, legal compliance, attack resistance, and complexity. We also look at any connections between these standards [38]. The iris reading is a biometric measurement using the user's smartphone. Analysis was also done on the fear of infection moderating impact on the postulated correlations [39].

The system that uses two-factor authentication uses a one-time visual password. To strengthen for mobile authentication method with simply an id and password or an authentication protocol from a bank, it is an enhancement of the OTP technique that implements the one-time graphical passcode [40]. Comparing the suggested scheme to similar methods with similar countermeasures and security qualities, the proposed scheme performed best in security and is appropriate for application [41]. The primary concept in preventing credential stuffing is multifactor authentication. However, threat actors may get around it by using interactive social engineering due to the availability of credential data sets, contact information, and association with demographic data. As privacy-protecting technologies decrease the observable difference between legal and fraudulent user sessions, alternative defence methods like network source profiling and device fingerprinting have become less effective [42]. The automatic validation of online security protocols computational models' tool and Scyther tools are used to validate this framework using formal methodologies empirically. For application scenarios, security research demonstrates that the suggested method performs better than the already-used SMS payment mechanisms [43]. The Fintech ecosystem has vulnerabilities, but the financial institutions and startups have the most since they employ cutting-edge technology to update outdated financial institutions into modern Fin-Tech ones. Technology developers must know threats that might exploit technological weaknesses and vulnerabilities connected to cyber security issues [44].

Methodology

The proposed systematic literature review mainly concerns the security and fraud detection or access control systems for users to transfer money from one account to another. This scheme is manageable in situations where the criminal person uses the credential information of another person to access their account to transfer the money from their account to their account. This study provides the guidelines and direction for a specific advanced and robust system to detect criminal operations, aside from two-factor authentication (2FA) applications and SMS receiving. This literature study has been done systematically based on previous studies on the problem. This methodology section is done with the help of tools and techniques for conducting research. The systematic literature review adopted from previous studies from the journals of famous publishers in the area of problem is the step-by-step method to explain the proposed review adequately. The collection was based on different parameters from five IEEE, Springer, Elsevier, Wiley, and Taylor & Francis publisher libraries. The search queries were used for the extraction of the information. The statistical methods will identify the limitations or difficulties encountered after collecting and testing the data to obtain the desired results.

Systematic ultrapure review process

This systematic literature study consists of all the information taken from the suggested publishers and downloaded from their libraries to fulfil the objective regarding the research title and address the research problems. The proposed literature review is followed by specific steps, in which the first one is identifying problems, which indicates the title of the proposed systematic literature review. The next step is creating a research question formulated according to the problem addressed and the research objectives. The query schedule identifies databases from its libraries for searching for related information to address the problems. The results and discussion include the calculated results for the objective-based information Tables, and the arguments consist of reviews of the results, the findings, and the conclusion. The finding and conclusion sections have the whole meaning of information about our review study, and the conclusion has the final decision on the systematic literature review. The conclusion of the research work must follow the objectives of the research work. The last paragraph consists of future challenges to provide a new path for the researcher for further forward movement.

In Fig. 1, after the research problem is identifying the research question or extracting the information, the scheduling of these questioners and modification for search concerning searching libraries in the final is the result, and discussion after then is the identification of the conclusion and future work.

Research questions identification

The research questions identify the relationship between the current problems with the past that addresses the solution. The research title, the identified research question, is the query for extracting the relevant information. The research questions are the research queries used to achieve the research objectives. The research objectives are supposed to be under the domain of the research problem, made up of searching keywords. It is the second of the review study after the confirmation of research objectives. The research question is depended upon the strength of the objective. This study identified four research questions to extract the desired information to achieve the study objective. These research questions have been used to extract the Information from the general specified to the problem to achieve a comprehensive systematic review has shown in Table 1 represents a set of research questions with its detail. Furthermore, these research questions have been divided into Keywords and small titles for searching purposes in different libraries (Fig. 2). Figure 2 describes the overall process of data extraction, defining the keywords, research questions, and final selection of studies. The figure shows establishing a precise research objective or question, conducting systematic searches for and selecting pertinent studies from a range of sources, searching and filtering research using predetermined inclusion and exclusion criteria, employing a standardized process to extract important data from a subset of trials, combining and examining the data

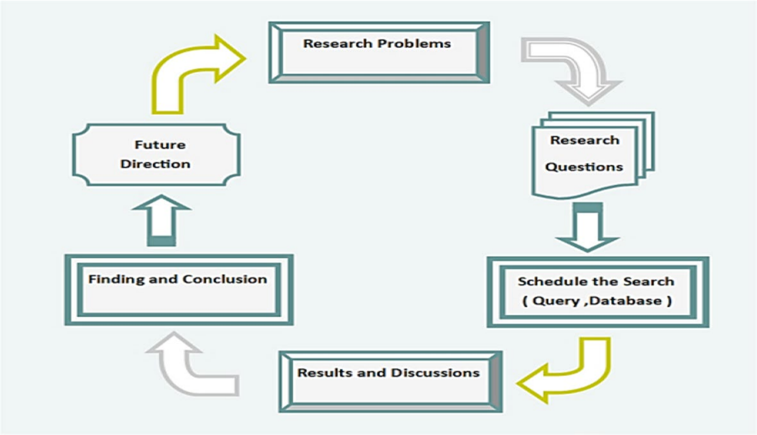

Fig. 1 Literature review process

Table 1 Review questions for money transaction authentication of secure fin-tech system

	Research questions	Research question objectives
Q1	What approaches are proposed for user authentication in Fin-Tech secure money transfers to ensure the user is legitimate?	The main objective of this question is to highlight the different approaches used that guarantee user authentication before money transfers from his account to another account in a secure method
Q2	What are the features and factors used to develop from taking guarantee secure transaction and user authentication in Fin-Tech?	This question aims to identify the different factors used for authentication purposes for secure mobile money transfers stepwise after the authentication and confirmation of the legitimation
Q3	What mechanisms/applications and supporting technologies have been applied in the previous system to avoid fraud in money transactions?	To identify the technologies that are used in support of account holder authentication, including the required applications and suitable mechanisms to avoid the fraud of money transfer using the credential information of the legitimate user
Q4	What requirements ensure the user's authentication before the money transfer to promote a reliable system to transform the expert system into fintech?	To identify the basic requirements to take guarantee about the user authentication except for the availability of credential information using a mobile phone and study the role of expert system in the user authentication process for secure Fin-tech Money transfer

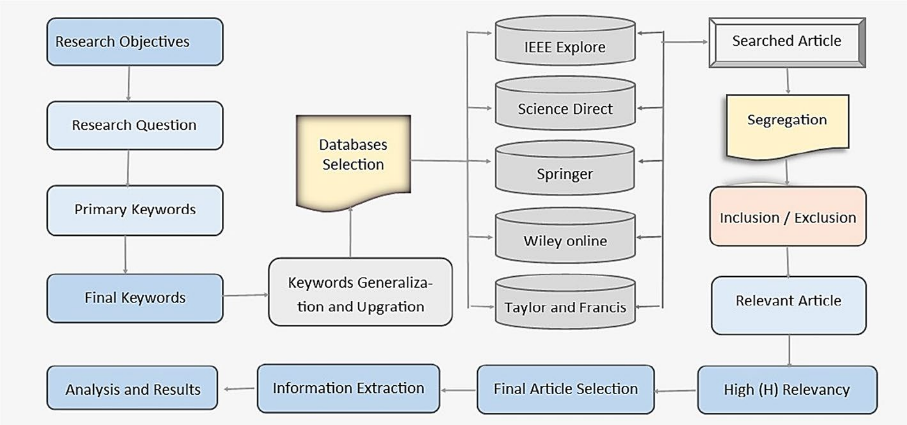

Fig. 2 Research steps for data extraction

that was extracted to find trends, patterns, and insights, evaluating the reliability and caliber of the studies that were included, making a summary of the results, and, if necessary, completing a meta-analysis using the combined evidence to draw inferences and implications.

Library selection for information extraction

The library selection was based on specific crates defined by research objectives. The articles selected from the fool studies are shown in Table 1. The popular libraries selected out of global libraries with the most relevant article are chosen for the literature review study as proposed. The selected study pool contains some journal articles and book sections with pertinent information.

a) Search procedure from digital libraries

Initially, the most relevant articles that have been studied address current issues. Furthermore, the selected articles are considered for the development, guidance, and direction for the assistance of future work. The proposed research work addresses the current problem that has been searched from five libraries. The involved libraries have searched from the IEEE Explore database ha used to search for the concerns article from the journal IEEE Publisher. Secondly, Science Direct has used to extract the concerns information from any journal of Elsevier Publisher Thirdly, has used Wiley from Wiley online in fourth Stringer, and fifth Tayler and Francis. The information extraction has been done to achieve the study objectives, as shown in Table 2. The proposed study has been obtained with the use of the following:

- Searched by titles
- Searched by keywords
- Searched by queries
- Criteria for selection

Table 2 Proposed study extraction based on keywords, titles, and query

Publishers	Databases	Queries, titles, and keywords	Resulted	Date
IEEE	IEEE explore	Mobile authentication factors for transaction	91	24-July-2022
		Authentication for secure mobile money transaction	52	26-July-2022
		secure mobile transaction	868	27-July-2022
		Mobile-based user authentication techniques or technology for security	155	29-July-2022
Elsevier	Science direct	Mobile authentication factors for money transaction	691	31-July-2022
		Authentication for secure mobile money transaction	736	01-Aug-2022
		Fin-tech secure mobile authentication for secure money transfer	70	3-Aug-2022
		Fin-tech mobile-based user authentication factors or techniques or technology for security	87	4-Aug-2022
Springer	Springer online	mobile authentication factors for money transaction	24	8-Aug-2022
		Authentication for secure mobile money transaction	23	16-Aug-2022
		secure mobile authentication for secure money transfer	30	18-Aug-2022
		Fin-tech mobile-based user authentication factors or techniques or technology for security	24	20-Aug-2022
		Mobile authentication technologies for banking	87	22-Aug-2022
Wiley	Wiley online	Authentication factors form mobile money transaction	482	24-Aug-2022
Taylor and Francis	T&F Online Library	Factor-based authentication for secure mobile money transaction	196	28-Aug-2022

b) Searching procedures

The papers for the proposed literature review have been downloaded from different journals of a publisher using individual Databases of libraries. This study has literature from different journals, IEEE, Springer, Elsevier, Wiley, Tayler, and Francis. The key term is the use of Specific topic queries and keywords used to extract the information based on criteria in which inclusion and exclusion are also concerns. The obtained result from the searched libraries is shown in Table 2, filtered by years from 2013 to 2022, and also searched only journal articles and some books.

c) Searching for articles by title

The title of an article represents the main problem. It is most important to identify the specific groups of titles for searching the proposed literature review in which the information addressed the problem, the issues, techniques, and its solution. The implementation of the title is applied where the key world result is too low.

d) Searching of articles by key words

Keywords are mostly also most words you enter into the journal database to search the article in a specific knowledge domain. It is the representation of the original concepts related to your concern topic. The right keyword is vital for searching for a piece of specific information that might be impossible to reach the goals without the perfect keywords in multiple steps of the process to identify the keyword for the central concept of our related problems with the help of synonyms and antonyms that could also be used to describe the problem.

Making queries for searching

The search query is the combination of keywords to specify the desired result to be obtained. The query was entered with the intent of finding relevant articles having information address the problem. The queries in Table 1 combine the essential world from generalized and particular searches using the 'OR' and 'AND' operations.

In Table 3 above, the formulated queries have provided the base for searching approaches where we focused on the search of more near to the research problem to achieve the objective of the proposed study. The queries as mentioned in Table 3 above. It shows the combination of keywords related to our proposed research to identify the supporting technology for mobile money transaction security.

Table 3 Formulated queries for searching the relevant articles

1."Mobile" AND "Money Transfer" AND "Fraud."
2. “Mobile" AND "Money Transfer" AND "Fraud" OR "Authentication."
3. "Mobile" AND "Money Transaction" AND "Fraud" AND "Technique
4. "Mobile" AND "Transaction" AND "Multifactor authentication.”
5. "Mobile," "ATM," and "Fraudsters."

Table 4 Relevant material selection from the downloaded publishers

Publishers	Database	Pages	Results (R)	Selected	Relevant	H. relevant	Final selection
IEEE	IEEE explorer	1–10	1166	464	152	73	34
Elsevier	Science direct	1–10	1584	382	9	45	28
Wiley	Wiley search	1–10	482	70	35	10	8
Springer	Stringer search	1–10	188	90	40	27	15
Taylor and Francis	Google scholar	1–10	196	70	30	15	7
Total		1–50	4581	1104	266	187	92

Table 5 Year-wise segregation of relevant materials corresponding to problems for analysis

Publishers	References	Total
IEEE	[12, 14, 18, 19, 22–24, 26, 28, 30, 31, 41, 46–63]	31
Elsevier	[15, 16, 29, 34, 35, 37, 38, 42, 45, 64–82]	30
Wiley	[13, 21, 36, 43, 83–87]	9
Springer	[25, 39, 44, 88–99]	15
Tailer and Frances	[17, 20, 27, 33, 40, 100, 101]	7

e) Inclusion/exclusion criteria

The inclusion/exclusion was based on the information relevancy in which the implementation of the filter during a search is a concern. The downloaded article is containing in a range of 10 years from 2013 to 2022, including journal articles and books where the conference papers and most past papers are excluded by filtration techniques to obtain the research objectives based on identified keywords, titles, and queries searched in the title, abstract, introduction methodologies, results, and conclusion as shown in Table 3.

f) Selected articles for review

The collection of relevant research articles is classified into publishers with references to indicate their publisher. Five selected libraries are taken from Table 3, as shown in Table 4. These are the most popular and much-reviewed digital libraries, where many researchers tried to publish their articles with novelty addresses to the problem. The sample selected papers out of the population is 92 [12–43, 45] articles selected after filtration of relevancy for analysis. The selected papers, based on the desired criteria, address the objectives. The pieces of information have been extracted by title, abstract, introduction, result, and conclusion. The proposed study has been done using five libraries IEEE Explorer, science direct, Wiley online library, Springer search library, and Taylor and Francis online search library for the above publisher, shown in Table 4, in which 34 articles are downloaded from IEEE 28 from Elsevier, eight from Wiley, 15 from springer, and 7from Taylor and Francis.

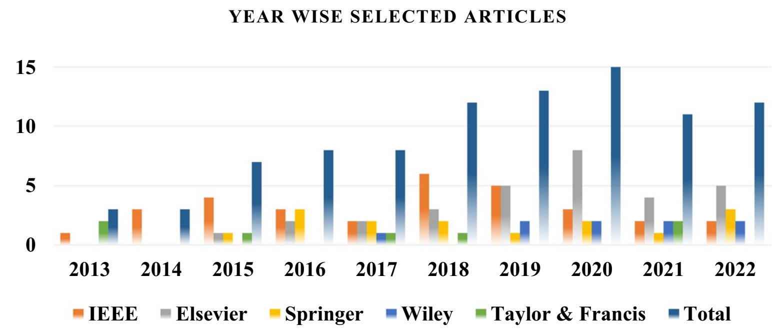

Fig. 3 Year-wise number of downloaded relevant publications

Table 6 The collected articles from journals and books concerning publication years

Year	Journals	Books	Conferences	No. of Articles
2013	[40, 101]			2
2014	[14, 30, 58]			3
2015	[15, 18, 27, 53, 54, 56, 94, 97]			8
2016	[25, 26, 29, 46, 61, 82, 91, 93]			8
2017	[16, 31, 43, 46, 59, 76, 88, 99]			8
2018	[12, 17, 28, 42, 57, 60, 63, 70, 90, 102]			10
2019	[19, 20, 24, 32, 35, 47–49, 51, 78–80, 83, 84, 92]			15
2020	[21, 34, 36–38, 41, 50, 52, 55, 65, 72, 75, 77, 81, 87, 95, 96]		[78]	18
2021	[13, 62, 66, 67, 73, 74, 86, 100]	[44]	[103]	10
2022	[22, 23, 33, 39, 64, 68, 69, 71, 85, 89, 98, 104]			12
		Total		92

g) Classifications of papers

Publishers classify research articles relevant to the topic by collecting research articles, which are classified in publishers with references to indicate their publisher. Five selected libraries are from Table 4, as shown in Table 5. These are the most popular for advanced searchable and mostly reviewable digital libraries about technologies enhancement for the future with some novelty address to the problem. The selected articles are 92 out of the population with excellent user authentication and transaction security ideas. Filtration of relevancy for analysis. The selected papers were based on defined criteria to address the objectives. The search process has been done by title, abstract, introduction, result, conclusion, and direction of the study from libraries IEEE Explorer, science direct, Wiley online library, Springer search library, and Taylor and Francis. The online search library for the above publisher is shown in Table 5, in which 364 articles are downloaded thirty-four from IEEE, twenty-eight from Elsevier, eight from Wiley, fifteen from Springer, and seven from Taylor and Francis, the most popular publishers.

Figure 3 represents the trend of Fin-Tech security authentication issues. Figure 3 shows the number of journal articles and books in the year of publication. The number of articles to be analysed year-wise is taken from Table 6, from 2013 to 2022. The

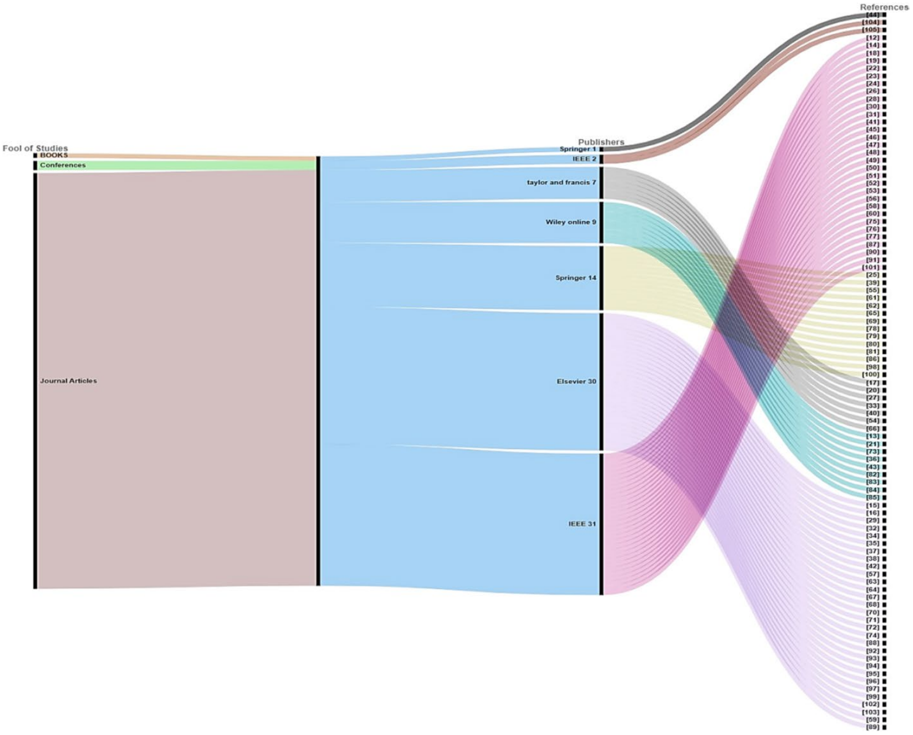

Fig. 4 Publisher consistency articles with their references

Table 7 The research question-based objectives and identification

Category	References	q_1	q_2	q_3	q_4	q_5	Total
C1	[13–25, 27–29, 31–37, 39, 42, 43, 68, 70, 75, 91, 93, 94]	1	1	1	1	0	4
C2	[54]	1	0	1	1	0	3
C3	[89, 101]	1	1	0	1	0	3
C4	[12, 67, 88]	0	1	1	1	0	3
C5	[26, 30, 38, 40, 45–48, 51, 52, 55–60, 62–64, 66, 69, 71, 74, 76, 77, 82, 86, 90, 96, 97, 100, 104]	1	0	0	1	0	2
C6	[41, 50, 53, 61, 65, 72, 73, 76, 78, 80, 83–85, 87, 92, 95, 99]	1	0	0	0	0	1
C7	[44, 79]	0	0	0	1	0	1
C8	[81, 98]	0	0	0	1	1	2

selected papers three from 2013, Three from 2014, is seven is, in 2015 is, eight from 2016, eight from 2017, twelve from 2018, thirteen from 2019 is, fifteen from 2020, eleven from 2021 with one book, and twelve from 2022. The total articles are 92 containing relevant information concerning the literature review that addresses the problems.

This systematic survey is shown in Fig. 4, which represents the fool of study that consists of 1 book and 92 journal articles for analysis; which book was downloaded from Springer and published in the year 2021; the rest of all the articles are from journals in which, 31 from IEEE, 30 from Elsevier, seven from Taylor and Francis, 14 from springer, and nine from Wiley.

Objectives-based data extraction for decision making

The purpose of this literature study was to collect information about Fin-Tech security based on defined Objectives for indication of current and future challenges to the researcher and also awareness about the trend of technologies in finch for secure transactions; for this purpose, the collected information regarding the research questioners are:

q1: Factors-based User Authentication.

q2: Technology has been used for Fin-tech security purposes.

q3: Authentication for secure mobile money transition.

q4: The obtained is supporting the authentication of the user against any fraud in the transaction.

q5: A.I. and machine supporting Fin-tech sec.

Table 7 has been obtained based on the questionnaire answered by the articles. Here we are classified into the categories where they obtained the same type of objectives concerns to the proposed study. C1 consists of articles in the reference column, as shown in Table 7. Five main questions support the proposed research obtained from previous studies. Ninety-two essential articles from Reference [13–102] answered the above questions. Some articles received the same objectives, which provide strong evidence supporting the proposed study and are significant in the research work further the calculation values dependent on it. Based on the questionnaire, some articles answer the same question and come under the same category, which is the

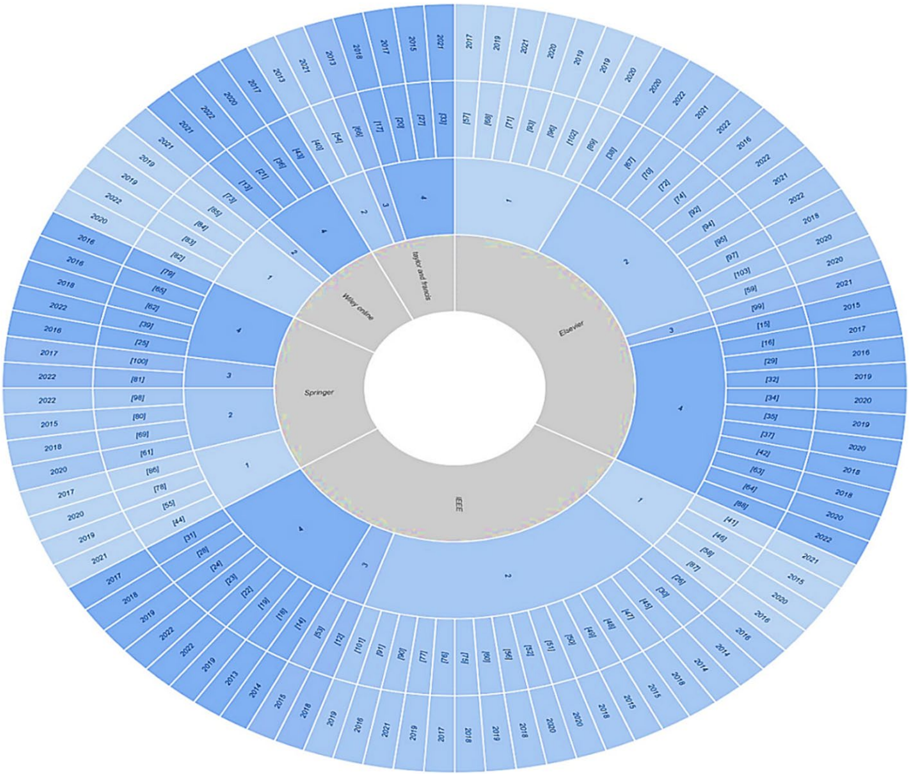

Fig. 5 Objectives-based publication

classification of the article dependent upon the answers of the questioners. There are eight categories classified in the article. Category (C1) consists of 33 articles obtained the question (q)1 to q4, where q5 is an absent total of 4 questions answered out of five, C2 has 1 article with three questions, and C3 has two articles with three different questions, and so on. The prominent uniqueness in the same question number defendant upon the unique valve of the question that can obtain the unique value by adding the value of different objectives of the same number of questions.

Figure 5 shows all the cited articles publisher-wise with-it years and the number of objectives obeyed according to the predefined criteria. The selected papers consist of a book section or journal article) downloaded from a digital library using their online search engine. The selected libraries are (IEEE, Springer, Science Direct, Wiley Online, and Taylor and Francis) at the top of the search list. Most researchers are trying to identify the current problem with the help of literature. The collected relevant papers are from the session 2013 to 2022, and they cover all of the recent issues and their solutions in various ways from 2013 to the present. Figure 5 has been divided into tracks and sectors, where the first track from the centre shows the publisher, which consists of IEEE, Springer, Elsevier, Taylor & Francis, and Wiley. The second track includes references against that publisher and objectives, whereas the third track represents references in the numbers. The last track represents the article's year of publication against the publisher, objectives, and references. Whereas in the sector, it shows the year of publication, from 2013 to 2022. Most references are selected from relevant papers in the proposed systematic literature review article. This shows the level of relevancy of the problem with its appropriate solution based on different technologies used to address the security issues.

Table 8 consists of information regarding prescribed objectives to address the challenges, opportunities, and technological concerns of the problem. It satisfied research question 1, where all the required information is desired using unique queries according to question 1. This literature review highlighted the authentication for secure transactions: the challenges, technologies, and their results to secure the financial transaction and mitigate the risk. Twenty-one articles are the most concerned with our problem and address the security authentication problem in money transactions. The other articles consist of technological approaches supporting Fin-tech transaction security. Table 8 discusses the technologies that play the most vital role in user authentication and provide supportive technologies for money transactions in financial technologies. The development of vast technologies increases the vulnerabilities in financial transactions.

Table 9 represents features with supportive technologies used in the previous study. These supporting technologies work for user authentication purposes which is desirable for Fin-tech secure money transactions. User authentication is the first step for financial security. Table 9 shows all those features that use authentication technologies, which the biometrics, password, OTP, QR codes, MAC addresses, IMEI, artificial intelligence (A.I.) and machine learning are superior for the authentication process. User authentication from mobile money transactions is the current challenge for the researcher concerning the role of IMEI/MAC address and AI. The users can restrict mobile-based transactions through the sender's systematic transactions instead of manual sources. The application can be made by assigning privileges only and only to personal devices; if someone takes

Table 8 Supporting technology of authentication for secure transaction

Refs.	Problems	Techniques	Challenges	Results
[12]	In insecure public communication networks, mobile payments	Mobile payments through certificate less cryptographic primitives are secure based on a random Oracle model	Security for online transaction	Reasonable and user-acceptable scheme for online transactions
[13]	Multi factors security evaluation system for mobile payments,	Machine learning approach	Payment fraud detection which ensures a safe and secure mobile payment platform	The consequences are enhancement of security and reliability
[14]	Security in banking due to the lack of trust	Tip ring ring sleeve (TRRS) Connector,	environment to secure transactions	strong security of authentication for transaction
[15]	Transaction security	Visual cryptographic scheme	The implementation of secure payment based on technology to provide guarantees for mobile-based 2FA	security of our scheme against various attacks
[16]	The model could protect the stolen credit card used by someone	Online transaction algorithm	The issue with credit card protection is the prevention of thieves accessing without a valid code to prevent the stolen card information from making purchases	This model protects the stolen card
[17]	Reestablishing and maintaining customer trust in mobile money services Improving Mobile Money Security	Biometric for authentication	To authenticate legitimate users,	3% enhancement authentication for a further level of security
[18]	Security attacks	For authentication, homomorphic MAC	Approaches to avoid the presented attack	Enhancement in attack resistance
[19]	Unsecure mobile payment	Near field communication technology mobile secure transaction scheme	Secure mobile transaction	Mobile secure payment
[20]	Authentication for secure transaction	One-time password (OTP), GPS, identification number (PIN)	Fraudsters prevention from performing online transactions	At the maximum rate of detection rate of the proposed system
[21]	OTP schemes vulnerabilities for classical execution	Scheme for (QOTP) Quantum OTP with biometrics	The trusted third-party holders take the user's biometric data to authenticate	Secured transactions based on control of no cloning and quantum cryptography principles
[22]	User authentication	Decentralization of fraud-proof roaming blockchain-based authentication framework	Roaming authentication ensures that Legitimate users allow to access the network securely	Security feature-based acceptable authentication delay
[23]	Mobile transaction security	The certificate less signature (CLS) scheme	Secure transaction security	Based on the improved CLS scheme, secured mobile transaction
[24]	User authentication in a mobile environment	Biometrics, dynamic OTP	User authentication	Provided authentication factors to the Android platform for user authentication

Table 8 (continued)

Refs.	Problems	Techniques	Challenges	Results
[25]	Low level of recognition success rate	Finger vein technology	Required the development of a secure system for information security	Protected the information based on finger and vein solution
[26]	Authentication	Message authentication codes, artificial-noise-aided MACs	The resistance of critical recovery attack	Authentication accuracy increased
[27]	Authentication for authorized users of financial systems	Message service (SMS) text messages	Reducing identity theft	Security, especially in the financial industry
[28]	Transaction authentication	Blockchain, private key (Seed Key)	Transaction authentication in blockchain technology	Theoretical support of Blockchain application
[29]	Transaction security	Biometric, finger scene, eye iris, and palm print use the rivest cipher (RC4), discrete wavelet transform (DWT) algorithms	Ensure hustle-free transactions	80% authentication can be possible with a one-time password
[30]	To be authenticated must also be encrypted	Novel techniques for authenticating short encrypted messages	Confidentiality and integrity are required in a message system	To utilize the security that the encryption algorithm can provide to design more efficient authentication
[31]	Secure mobile payment	Near-field communication (NFC) technology	Unknown payment has received recent attention	The best way to secure mobile payment
[32]	Authentication for mobile transaction	Biometric, Fingerprint, and Face recognition	Money security and privacy	Easy, fast, and secure transaction
[33]	Customer authentication	CNN, region-based convolutional neural networks (RCNN), and deep face are deep learning algorithm	Image is fake or real, with image chain for OTP	The accuracy of this experiment is 75.35,
[34]	Identity Problem	Authenticated key agreement (AKA), Certificate less AKA, Public key Infrastructure (PKI),	Mitigate the vulnerabilities above	Blockchain-based Wireless Body Area Network (WBAN) security
[35]	Continuous authentication	Behavioural biometrics, sensors, accelerometer, gyroscope, magnetometer, and touchscreen	Banking application with continuous authentication	Secured authentication
[36]	Authentication	Biometric cryptography utilizes, for authentication, quantum entanglement property to generate OTP (QOTP)	Man-in-the-middle prevention and identification of vulnerabilities	Resisted the attack
[37]	Financial security	Cryptography and network protocols	Fraud, extortion, money laundering, and financing activities protection	Enhancement in Financial security
[38]	Authentication for online banking	Multi factors authentication	Authentication for banking	Multifactor authentication accuracy is greater

Table 8 (continued)

Refs.	Problems	Techniques	Challenges	Results
[39]	Mobile base secure payments	Biometric, payment services directive (PSD2)	Transaction security against the risk	higher perception of authentication risk
[40]	Mobile-based banking authenticating	Graphical OTP	Problem by suggesting Two-Factor authentication	Digital certificate from banks enhanced the security
[41]	Authentication	wireless sensor network (WSN)	Factor-based authentication	Enhancement in authentication
[42]	Authentication security for mobile-based transactions	PIN and fingerprint biometrics authentication	Authentication for payment	Biometrics authentication is a concern and significant for individual security
[43]	Transaction security	SMS security based on elliptic curve cryptography	In a global communication system, SMS is not secure	Security framework for SMS banking
[44]	Transaction vulnerabilities	Nil	Cyber security	Security information's

Table 9 The supporting technologies and features highlighted in the articles for the proposed System

Feature	Technology used	Functions	References
Biometric	Finger-drawn signatures on touch devices Sensors, electro cardio gram, phono cardiograph, convolutional neural network (CNN), Electroencephalogram Fast identity online Swipe-V-lock Al m print-based key generation system voice recognition technology	Common spatial patterns (CSP) values, electrocardiogram (ECG) data for authentication, and conventional biometric methods were the significant elements in training the model. A classification method called linear discriminant analysis (LDA) was applied for specific user data collection. The server-based authentication approach uses the distributed management of compliance-based biometric data. Viable methods for banking security and authentication. Using a backdrop image to swipe the smartphone screen. Behavioural biometrics can secure mobile payments, improve usability, and stop fraud. When using biometrics for two-factor authentication, OTP is employed to strengthen the security of weak passwords. Information security now includes promising technologies like cryptology and biometrics	[50–60, 63, 70, 75–77, 92–94, 96, 100, 101]
Password	Graphical passwords (G.P.s) Smartwatch worn	To further enhance the security of Fin-Tech applications, the route map is a map- and route-based G.P. Wrist movements are made by the cardholder while inputting a PIN or password, which is employed as an authentication factor. Strategies to encourage the usage of safe passwords are examined, and their implications are discussed. Users construct passwords according to trends and patterns. It thoroughly looks at how easily these real-world passwords may be guessed. Information is sent to a password manager	[69, 73, 74, 78, 90, 104]

Table 9 (continued)

Feature	Technology used	Functions	References
OTP	Image-based password System (IBPS) Time-based one-time password (TOTP) Embedded hardware OTP Linear congruential generator (LCG) Authentication code by hash algorithm Mobile identity Authentication mechanism	The second element for robust authentication after the password is OTP. To appropriately safeguard the system from unwanted third-party auditors, the system uses an automated blocker protocol (ABP) and time-based one-time password (TOTP) for cloud user verification. For instance, OTP is produced on the server and delivered to clients by SMS. Embedded hardware OTP generating device using dual tone multi-frequency (DTMF) signals for remote requests The OTP produced by LCG is not repeating, and it is difficult to predict the randomness. OTP is crucial for safe banking financial transactions. A more secure authentication method is the one-time password (OTP). It ensures that both entities are genuine throughout a single session	[46–48, 82, 86, 91, 95]
Q.R. code	Digital watermarking-a data Hiding technique The bank's SPAQ website AES encryption algorithm	VQ-compressed code, which is utilized for picture authentication and print-and-scan, visual cryptography, code, and one-time PIN, is a significant tool (OTP). For safe financial transfers, a two-factor authentication protocol is used for a time-based one-time password (TOTP). Defend against phishing attacks. An extra layer of protection will be provided through the public critical infrastructure (PKI)-maintained, quick response (Q.R.) code security mechanism. Here, robust authentication is carried out utilizing Q.R. matrix barcodes, which have a large storage capacity for plain-text and encrypted data. Financial services are more secure using the integrated Q.R. code in the Adhere card and biometric authentication. W codes protect private data. High levels of convenience and security are achieved with visual authentication techniques	[46, 61, 62, 68, 72, 83–85, 87, 89, 97, 99]

Table 9 (continued)

Feature	Technology used	Functions	References
MAC and IMEI	Channel state information A secure hash algorithm (SHA) is a cryptographic hashing algorithm Address resolution protocol (ARP) International mobile equipment identity	Techniques of device identification employ this technology. The suggested technique can increase security regarding confidentiality duration and secrecy capability. The international mobile equipment identity (IMEI) uses the backstage covert automatic identifying form of authentication Algorithms for hybrid encryption algorithm (HEA)	[64–66, 71, 80, 102]
A.I. and machine learning	Generalized algorithm A.I. and machine learning techniques	Prospects of artificial intelligence (A.I.) in security, outstanding challenges that require additional A.I. investigation, and machine learning techniques to identify fraudulent bank card transactions. One of the known methods for identifying credit card fraud has been created using behaviour analysis and machine learning techniques. It has been designed to detect fraudulent transactions using reinforcement learning, supervised learning, unsupervised learning, and parametric/non-parametric methods. Through A.I. and machine learning approaches, online fraud in e-Commerce and financial transactions is prevented and controlled. Approaches to authentication based on machine learning	[49, 67, 79, 81, 88, 98]

your required information, he will not be able to use your account, where the A.I. will learn and store the information tracks for experience in fraud detection. The IEMI and Mac address as a private key can address the security by successive interference cancellation (SIC) scheme in the dedication of smartphones [105]. These authentication technologies are generally implemented by all financial Organizations for specific operations. A.I. monitors the data to calculate the risk score based on previous activities to decide whether the transaction is genuine or fraudulent [106]. A.I. provides a high degree of security with its feature for a secure transaction using algorithms for clarification and verification [107]. The monitoring of chat and communication helps keep track [108]. It is helpful in cyber security for authentication [109]. To create geographically dispersed data and a history model provenance and lineage tracking trusted A.I. [110].

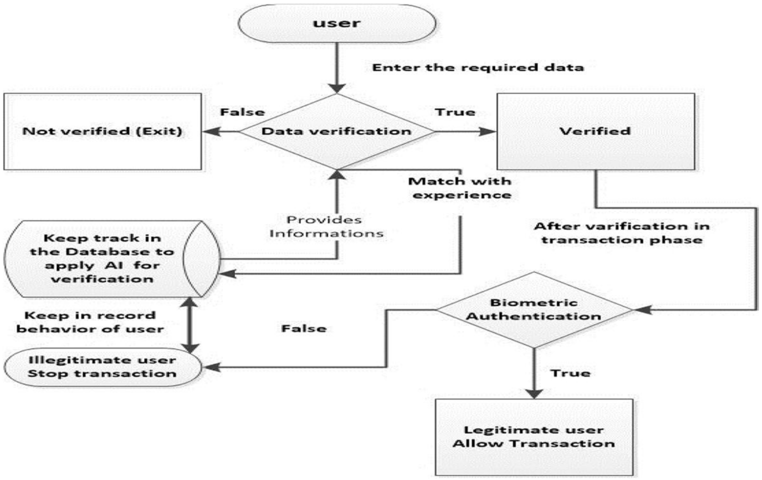
user
Enter the required data
False
True
Not verified (Exit)
Data verification
Verified
Match with experience
Provides Informations
After varification in transaction phase
Keep track in the Database to apply AI for verification
Keep in record behavior of user
False
Biometric Authentication
Illegitimate user Stop transaction
True
Legitimate user Allow Transaction

Fig. 6 User verification from use case diagram for transaction

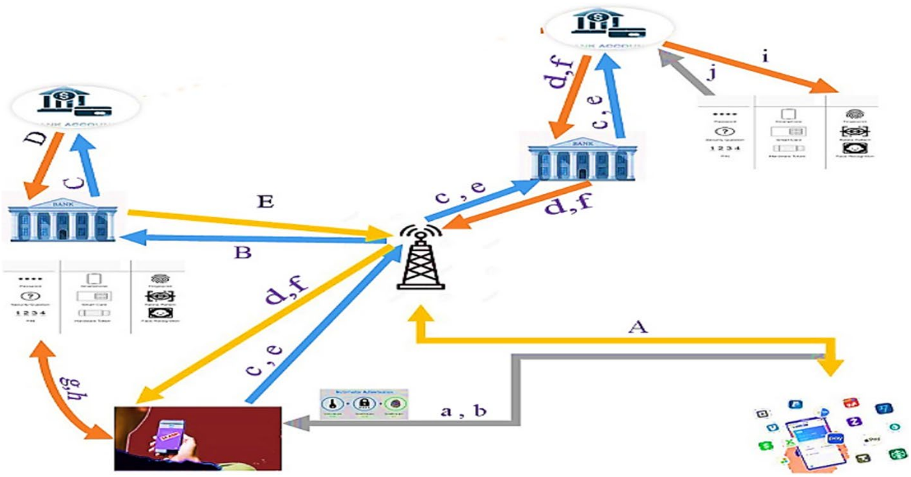

Fig. 7 Money transaction scenario and challenges

Figure 6 represents the use case diagram to show the steps in baking finance transactions that make it easy for the operational team to fix the vulnerabilities in the fin-tech system. The user requires confidential information to log in to the account. Furthermore, strong security is the second authentication requirement for transaction defence upon the devices to get the biometric information. In the first step, enter the username and password, and the system verifies the username and password if it corrects the user's login to the system. If one of these is incorrect, the system denies accessing the account after the login the user authorized for the transaction. Still, in this case, the login user may be fake, so during the transaction, the system asks for the third factor of authentication in addition to a one-time password if the required authentication factor is a match to the bio matric information to the account holder the transaction will be done otherwise the process will be cancelled. The system will be kept store track of this operation for further A.I. implementation on this operation for risk detection.

Figure 7 represents the functional scenario in which the fraudsters tried to get confidential information in case of success during the transaction. The role of MFA in authentication is shown in Fig. 7. The alphabets 'a' represents the request message for confidential information fraud takes. In case 'b' is provided confidential information obtained by technical approach to the fraudster shown as 'c' is the implementation of that confidential information for the transaction. 'd' is the transaction authentication in the form of 'g,' 'h,' e is the trying for authentication, 'I' is for matching the authentication, 'j' is the acknowledgement for validation and 'f' represent the final decision could be transaction perform or cancellation. The consequences of the above Fig. 7 involve biometric authentication during a transaction that has not been used before and is essential for the physical authentication of the sender.

Results and discussions

This secretin analyzed the previous study to achieve the literature study objectives to address the current problem. From the above research, the questions obtained the results for specific objectives achievement. This section provides the development, and the discussion will include all the final decision steps taken from the previous literature study. All the information directs the navigation systems in the availability of different hardware devices used by technologies to avoid the authentication issue to secure transactions.

Table 10 Technologies used in the previous studies from Table 8 [12–44]

Categories	Technologies	References	Frequency
Authentication for transaction (AT)	Biometric	[17, 29, 32, 39, 42]	5
	Graphical OTP	[20, 40]	2
	Blockchain crypto and algorithms	[15, 16, 28, 37, 43]	5
	NFC	[19, 31]	2
	ML	[13]	1
	CLS	[12, 23]	2
	General	[44]	1
	TRRS	[14]	1
	SMS	[27, 30]	2
	MFA protocols	[38]	1
Authentication for control access (ACA)	Biometric	[21, 24, 25, 35, 36]	5
	Blockchain crypto and algorithms	[22]	1
	MAC	[18]	1
	ML	[33]	1
	CLS	[34]	1
	Message code	[26]	1
	WSSN	[41]	1

Table 11 Technologies classified based on their functions from Table 10

Classification	Biometric/MFA	OTP/2FA	ML	Blockchain crypto and algorithms	Others
Technologies	[17, 21, 24, 25, 29, 32, 35, 36, 38, 39, 42]	[20, 26, 27, 30, 40]	[13, 33]	[15, 16, 22, 28, 37, 43]	[12, 14, 19, 23, 31, 34, 41, 44]

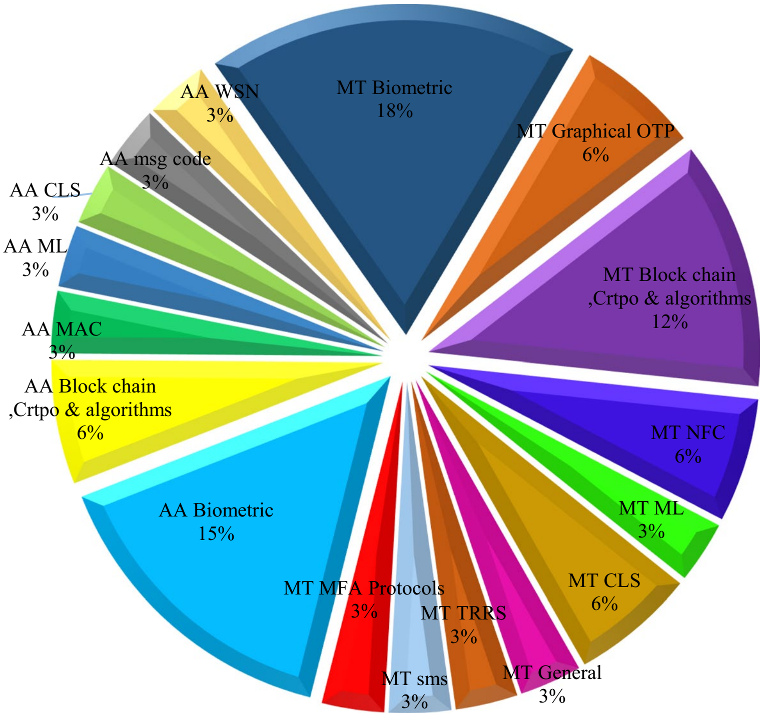

Fig. 8 Studies about technologies, problems, challenges, and results

To ensure the user is legitimate, what approaches are proposed for authentication in fin-tech secure money transfers?

The literature described multifactor authentication procedures to check the user's identity for financial transactions. Table 8 addresses the relevant problem to my study title, which mainly highlights financial security. To address that, security issues have been implemented to enhance the security system for financial transactions in which the biometric, OTP, GPRS, and physical device addresses are highlighted.

Table 10 Authentication for Transaction (AT) and Authentication for Control Access (ACA) concern the problem of achieving authentication objectives. Table 10 analyzes the technologies used by the previous researcher during the last article, as highlighted in Table 8. To classify the technologies for further calculation from both AT and ACA.

Table 11 has been used to classify the above technologies based on similarities for further analysis to include in the final decision. The Biometric or MFA consists of eleven articles, OTP or 2FA consists of 2 articles, Machine learning (ML) consists of two articles, block chain composed of 6 papers, and others comprised of 8 articles. These 22 articles included 92 articles analyzed for the proposed study. Furthermore,

Table 12 Supporting technologies for user authentication from Table 9

Feature	Technologies	Refs.	Frequency
Biometric	Fingerprint, vein scan image, voice recognition, touch screen signature	[44–64]	22
Password	Graphical password Smartwatch worm	[65–70]	6
OTP	Time base, embedded code	[71–77]	7
Q.R. code	Digital watermark, hash technique, AES encryption	[78–89]	12
MAC and IMEI	ARP, SHA algorithm	[90–95]	6
A.I. and machine learning	Deep learning, CNN, and A.I	[96–101]	6

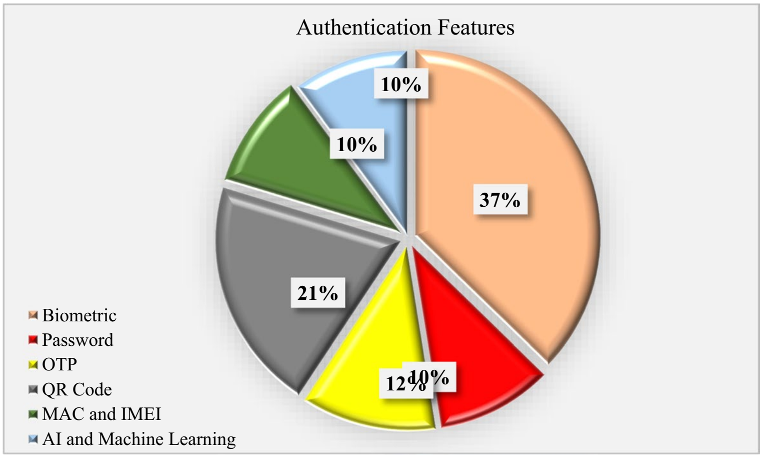

Fig. 9 The supporting technologies used for user authentication

to calculate the values of technologies based on its paper belong to which categories to cross-check with Tables 8 and 10.

The above Fig. 8 shows the maximum and minimum technologies applied for protection in the previous study in which Biometric is 18% has been used for mobile money transaction purposes, which is the maximum some other unique procedures have been used.

What are the different features and factors used to develop take guarantee for secure transaction and user authentication in Fin-Tech?

The downloaded relevant articles contain supportive targets, technological software, or hardware tools mentioned in Table 11. The secure transaction could be secure with the help of authentication technologies. Usually, mobile technology authentication is a concern for identifying the legitimate user for allowing access to the account. The security-embedded system is helpful for the improvement of secure systems. The set of tools and technologies considered in the authentication security phase is recorded in Table 11.

Table 13 Conference-based issues identification

Year	Publisher	Conference	Challenges	Refs.
2020	IEEE	11th Annual (UEMCON)	ML, based credit card transaction detection	[78]
2021	IEEE	12th Annual (UEMCON)	Transaction placement problem	[103]

Table 14 Scope value Initialization to the objectives

Symbols	Objectives	Scope
q_1	Factors-based user authentication	0.9
q_2	Technology has been used for Fin-tech security purposes	0.7
q_3	Authentication for secure mobile money transition	0.5
q_4	The obtained supports the authentication of a user against any fraud in a transaction	0.3
q_5	A.I. and machine-supporting Fin-tech security	0.15

What mechanisms/applications and supporting technologies have been applied in the previous system to avoid fraud in money transactions?

The user authentication functions against the authentication technologies. In case of account data loss, biometric authentication consists of some functions classified into some features to provide robust security to the user account based on technological approaches. The technological system can provide a secure environment for finance. The different functions shown in Table 11 help in user authentication from Table 10, Furthermore the improvement of technological security by transforming it into the financial sector for authentication and secure transaction.

The above Table 12. Shows the supporting technologies that provide a guideline for secure financial transition authentication. The combinations of different technologies related to their concern features address the security authentication problems. Seven features have been discussed with other technologies highlighted in the article and are mentioned as references.

In Fig. 9 above, the user authentication supporting technologies has used that can be easily implemented on the Fin-Tech. Biometric use is 37%, QR code 21%, and OTP 12%, which shows the intention of the researcher to include new technology in Fin-Tech for money transaction security.

What requirements ensure the user's authentication before the money transfer to promote a reliable system to transform the expert system into fin-tech?

The consequences of a technology-based secure system are to check the compatibility of the available applications based on some performance suitable for authentication to secure mobile money transactions. This mechanism is ultimately used for application evaluation based on its functional capabilities and port abilities. The identification technologies from Tables 11 and 12 are the most compatible for financial security and more helpful for current and future challenges.

Table 15 Objectives-based categories analysis

Cat:	q1	q2	q3	q4	q5	T	A	∏	(CAP)
C1	0.9	0.7	0.5	0.3	0	2.4	32	76.8	53.63128
C2	0.9	0	0.5	0.3	0	1.7	1	1.7	1.187151
C3	0.9	0.7	0	0.3	0	1.9	2	3.8	2.653631
C4	0.9	0	0	0.3	0	1.2	2	39.6	27.65363
C5	0.9	0	0	0	0	0.9	33	15.3	10.68436
C6	0	0	0	0.3	0	0.3	17	0.6	0.418994
C7	0	0	0	0.3	0.15	0.45	2	0.9	0.628492
C8	0	0.7	0.5	0.3	0	1.5	3	4.5	3.142458

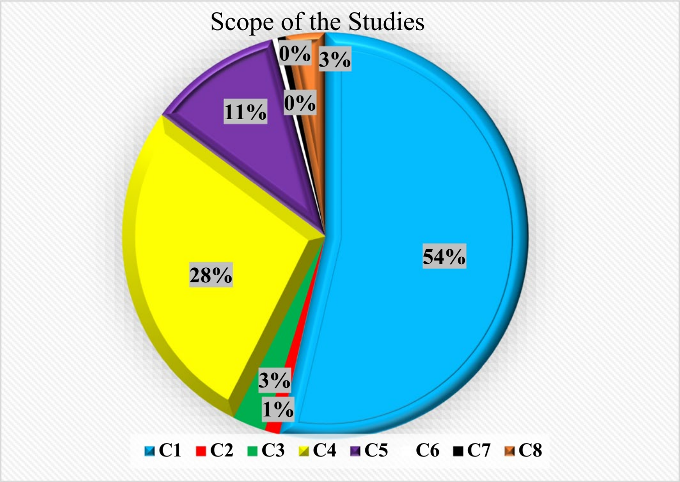

Fig. 10 Classification of similar objectives achievement

Future direction based on conference study

This study aims to identify relevant challenges and technologies based on mature conferences above the 10th, which consist of solid work and acceptable concepts for current challenges regarding the concern problems.

Table 13 shows the direction and trend that attract the researcher's attention to the concerns issues.

Scope of the study

The scope of the study is calculated by the obtained studies based on the research questions using their keywords for desired information to achieve the research work's objectives that address the research problem.

The obtained information piece's scope is based on its objective requirements. In Table 14, q is the symbol that represents individual objectives scope (S) is the value.

$$\mathrm{Uniquevalue} = \forall : \sum_{n=1}^{n=5} S_n \tag{1}$$

where n is the number of combinations of scope values, the Eq. (1) represents the sum of any number of values out of the scope value must be unique, representing the individual combinational of objectives. The categories have been taken from the Table for further optimization. In Table 7, q1, q2, q3, q4, and q5 represent the scope value, T (Total) represents the sum of the importance of the questions, A is the number of articles contained in categories, $\prod$ is the product of A and T, and category percentile.

(CAP). It has been used to calculate the percentile that shows the percentage, as shown in Table 14, the participation of the objectives taken from previous work.

$$\mathrm{T} = \sum_{i=1}^{i=5} \mathrm{q}_i \tag{2}$$

where i = 1, 2, ... 5.

The Eq. (2) is the sum of the scope values shown in Table 15.

Figure 10 above shows the achievements of the objective base on the extract from the number of articles reprinted by groups. The above Fig. 10 explains the result value of Table 15 calculated from the scope of questioner obtained by the articles. Table 14 identifies the objective's specific value depending on our study's scope. The uniqueness is represented by

$qi \neq qj$ where $i \neq j$.

Table 16 represents the overall calculation for results in which C1 to C8 are categories consisting of articles obtained from Table 7 represented by a group of technologies collected from previous technologies implemented. Table 14, where q1 to q5 is objectively obtained by the paper regarding or proposed study. The calculated values of the technologies are in Table 14 and Table 15 concerning the importance of categories of articles from Table 7. The maximum average value shows a higher ranking for achieving the objectives of the proposed study.

Table 16 Technologies concerns to the categories

Technology	C1	C2	C3	C4	C5	C6	C7	C8	Total
Biometric	**14**	**1**	**1**	0	**14**	**3**	0	0	33
Password	0	0	0	0	**4**	**2**	0	0	6
OTP	**4**	0	**0**	0	**7**	**1**	0	0	12
Q.R. code	**1**	0	**1**	0	**3**	**7**	0	0	12
MAC and IMEI	**1**	0	0	0	**4**	**2**	0	0	7
A.I. and machine learning	**2**	0	0	**2**	**1**	0	**1**	**2**	8
Blockchain and algorithm	**6**	0	0	**0**	0	0	**0**	0	6
Other techniques	**5**	0	0	**1**	0	**1**	**1**	0	8
Total									92

These values in bold were given to the model

Objectives achievement concerning technology

The technology has used articles belonging to which categories regarding concerns and objectives based on the questionnaire.

$$\mathrm{Xmn} = \begin{array}{c} \\ \mathrm{T}_1 \\ \vdots \\ T_{\ \mathrm{n}} \\ \\ \end{array} \begin{bmatrix} \mathrm{C}_1 & \ldots\ldots\ldots\ldots & \mathrm{C}_\mathrm{n} \\ \mathrm{X}_{11} & \ldots\ldots\ldots & \mathrm{X}_{1\mathrm{n}} \\ & & \\ \vdots & \ddots & \vdots \\ \mathrm{X}_{\mathrm{m}1} & \ldots\ldots\ldots\ldots & \mathrm{X}_{\mathrm{mn}} \end{bmatrix} \tag{3}$$

Technology Article $\in \mathrm{C_n}$ where $1 \le \mathrm{n} \le 8$.

Above Table 16 is the combined analysis of Tables 11 and 12 concerning categories in Tables 7, 14, and 15 of the article concerning the questioners.

The next step is to calculate the technologies' weightage concerns the proposed study from Table 16. Take CAP to multiply with quantity belonging to.

$$\mathrm{CAP_l} \times \mathrm{X_{mn}} \tag{4}$$

where l, m, n = 1,2,3,…,8

$$\mathrm{Average(Av_i)} = \sum\nolimits_{n=1}^{n=8} C_n \tag{5}$$

$$\mathrm{Weight(WT_i)} = \frac{1}{\sum_{i=1}^{8} Avi} \times \mathrm{Av_i} \tag{6}$$

To use the statistical aggregation supplied in the previous article [111].

The above Table 17. Represents the support of the technology in the proposed study regarding the objectives and its scope. The weight of the technology shows the role of authentication in the proposed research for the sender. In contrast, in some situations, two-factor authentication is failed in case of a lost password, and OTP, and the system will verify the person physically.

Figure 11Represents the weight of the technologies concern to the objectives in percentage in which the biometric is 36% concern to the proposed study in second OTP is 13% both are belonging to MFA and 2FAs and Qr Code is also in equal benefit which is now started in different areas but required to implement in the transaction for better security**.** Implementing both technologies can increase security by 49% from the current security**.**

Limitations

Regarding the proposed systematic literature, the highlighted limitations are:

- Selection boundaries: this literature study relevant to the related domain address the proposed systematic review problem. The articles selection process has been done by limited sources where only five digital libraries were used in the search procedure for the literature study out of relevant research papers. Many other libraries are available for gathering relevant publications with some neglected information.

Table 17 The resulting weights of technologies concerning categories analysis

Technology	C1	C2	C3	C4	C5	C6	C7	C8	Average	(WT_i)
Biometric	750.82	53.63	53.63	0	750.82	160.89	0	0	221.2238	0.358696
Password	0	0	0	0	214.52	107.26	0	0	40.2225	0.065217
OTP	214.52	0	0	0	375.41	53.63	0	0	80.445	0.130435
Q.R. code	53.63	0	53.63	0	160.89	375.41	0	0	80.445	0.130435
MAC and IMEI	53.63	0	0	0	214.52	107.26	0	0	46.92625	0.076087
A.I. and machine learning	107.26	0	0	107.26	53.63	0	53.63	107.26	53.63	0.086957
Blockchain and algorithm	321.78	0	0	0	0	0	0	0	40.2225	0.065217
Other techniques	268.15	0	0	53.63	0	53.63	53.63	0	53.63	0.086957

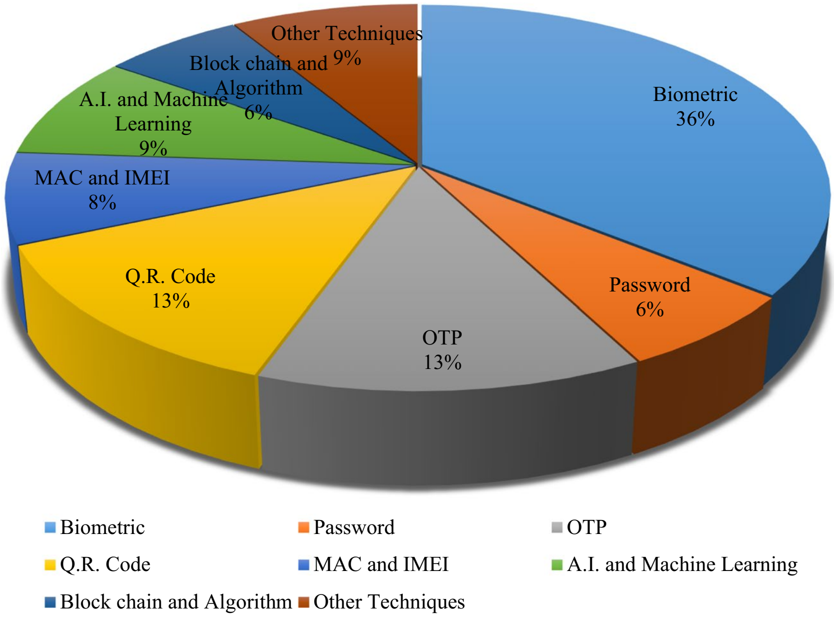

Fig. 11 Weights of the technologies in the propose study

- Duration: the proposed research work is prepared only the papers in the range of (2013–2022) in which the previous articles from 2013 are omitted from the analysis. The systematic research process has been selected from a limited range of publications. The proposed work gathers only the recent state-of-the-art approaches for the proposed financial security authentication.
- Selection study: this systematic literature review excludes all the conference articles.

Advantages

The ignorance of the above limitations of the proposed research work caused by advantages are:

- Analysis possibilities: the selection of the limited library sources, where the researchers focused on the high-level and famous publishers that contain all the detail about technology that is helpful for authentication, whereas the other published may not be extra information than these popular libraries, which is easy to analyze for the conclusion.
- Recent work-study: the proposed research work has been prepared only from the latest article (2013–2022) that conflicts with the current issues.
- Selection study: the systematic literature review excludes all the conference articles which are not primarily implementable.

Conclusion and future work

During the last decade, financial transactions through the internet faced security issues in which illegal money transactions used confidential steel information of legitimate users for money transactions. Fintech money transaction security has inspired the world by making financial transitions possible through intelligent apps that use user authentication to stop fraudsters from making illegal transactions. Authentication using smartphone devices is challenging research in this modern and vast technological era. The analysis was carried out by 92 articles downloaded from five publishers, where, because of the proposed study, 46 per cent of the studies highlighted authentication in the context of security, in which 54 per cent of the studies specifically about user authentication based on authentication factors for secure money transactions in Fin-Tech. Furthermore, in MFA, the biometric authentication after the OPT verification is concerning and extendable. Even though technology is improving, there are still problems with the security of money transactions.

The security can be more robust by allowing the transaction only from verified devices. Personal information can be hacked by fraudsters for illegal transactions. The password is not as considered a vital entity for protection. OTP makes it secure up to a specific limit. In case someone loses their password and OTP, the machine can detect the user based on the previous technology because only OTP a password is not enough for a machine to recognize a person. To address that type of security issue, another biometric technology must include during each transaction in which the system can verify a person's physical body, which is still not in use in the banking transaction system. The proposed study has identified the different technology Qr code and MFA for biometric authentication of users can increase by 49% the security from the current level of protection.

Furthermore, we can apply the A.I. technology to store the transaction tracks, behaviour, time situation, and result to keep the system proactive against uncertain situations to make the MFA technology more advanced.

Author contributions

HUK conceptualized this study, conducted experiments, wrote the original draft, and revised the manuscript; MS and SN conducted the experimental plan, supervised the work, and revised the manuscript; BS, TH and FA contributed to the evaluation of the developed technique, analysis of results and revised the manuscript. All authors reviewed the manuscript.

Funding

Qatar National Library, Doha, Qatar supports this publication. In part this publication is supported by Qatar University, internal Grant IRCC-2021-010.

Availability of data and materials

No data were used to support this study.

Declarations

Ethical approval and consent to participate

We confirm that relevant guidelines and regulations are carried out in all methods.

Competing interests

The authors declare that the research was conducted without any commercial or financial relationships that could be construed as a potential conflict of interest. The authors declare no competing interests.

Received: 10 December 2022 Accepted: 2 August 2023
Published online: 08 September 2023

References

1. Kumar D, Goyal N. Security issues in M-commerce for online transaction. In: 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). 2016. p. 409–14.
2. Fan K, Li H, Jiang W, Xiao C, Yang Y. U2F based secure mutual authentication protocol for mobile payment. In: Proceedings of the ACM turing 50th celebration conference-China. 2017. p. 1–6.
3. Hussain T, Yang B, Rahman HU, Iqbal A, Ali F, Shah B. Improving source location privacy in social internet of things using a hybrid phantom routing technique. Comput Secur. 2022. https://doi.org/10.1016/j.cose.2022.102917.
4. Bijwaard D. Survey on "scams and fraud experienced by consumers"—final report. 2020.
5. Williamson GD, Money–America's G. Enhanced authentication in online banking. Citeseer. 2006.
6. Hwu J-S, Chen R-J, Lin Y-B. An efficient identity-based cryptosystem for end-to-end mobile security. IEEE Trans Wireless Commun. 2006;5:2586–93.
7. Müller L. Authentication and transaction security in E-business. In: IFIP International Summer School on the Future of Identity in the Information Society. 2007. p. 175–97.
8. Hassan A, George A, Varghese L, Antony M, Sherly K. The biometric cardless transaction with shuffling keypad using proximity sensor. In: 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA). 2020. p. 505–8.
9. Sajić M, Bundalo D, Bundalo Z, Sajić L, Kuzmić G. "Programmable electronic payment card transaction limit implemented using mobile electronic technologies. In: 2018 7th Mediterranean Conference on Embedded Computing (MECO). 2018. p. 1–5.
10. Kang J. Mobile payment in Fintech environment: trends, security challenges, and services. HCIS. 2018;8:1–16.
11. Ali G, Dida MA, Elikana Sam A. A secure and efficient multi-factor authentication algorithm for mobile money applications. Future Internet. 2021;13:299.
12. Yeh KH. A secure transaction scheme with certificateless cryptographic primitives for IoT-based mobile payments. IEEE Syst J. 2018;12:2027–38.
13. Wang F, Yang N, Shakeel PM, Saravanan V. Machine learning for mobile network payment security evaluation system. Trans Emerging Tel Tech. 2021. https://doi.org/10.1002/ett.4226.
14. Ortiz-Yepes DA, Hermann RJ, Steinauer H, Buhler P. Bringing strong authentication and transaction security to the realm of mobile devices. IBM J Res Dev. 2014;58:4:1-4:11.
15. Maeng Y, Mohaisen A, Lee M-K, Nyang D. Transaction authentication using complementary colors. Comput Secur. 2015;48:167–81.
16. Gualdoni J, Kurtz A, Myzyri I, Wheeler M, Rizvi S. Secure online transaction algorithm: securing online transaction using two-factor authentication. Proced Comput Sci. 2017;114:93–9.
17. Alotaibi SN, Furnell S, Clarke N. A novel transparent user authentication approach for mobile applications. Inf Secur J Glob Perspect. 2018;27:292–305.
18. Li C, Chen L, Lu R, Li H. Comment on "an efficient homomorphic MAC with small key size for authentication in network coding." IEEE Trans Comput. 2015;64:882–3.
19. Turk I, Angin P, Cosar A. RONFC: a novel enabler-independent NFC protocol for mobile transactions. IEEE Access. 2019;7:95327–40.
20. Khattri V, Singh DK. Implementation of an additional factor for secure authentication in online transactions. J Organ Comput Electron Commer. 2019;29:258–73.
21. Sharma MK, Nene MJ. Dual factor third-party biometric-based authentication scheme using quantum one time passwords. Secur Privacy. 2020;3:e129.
22. Xue K, Luo X, Ma Y, Li J, Liu J, Wei DSL. A distributed authentication scheme based on smart contract for roaming service in mobile vehicular networks. IEEE Trans Veh Technol. 2022;71:5284–97.
23. Qiao Z, Yang Q, Zhou Y, Zhang M. Improved secure transaction scheme with certificateless cryptographic primitives for IoT-based mobile payments. IEEE Syst J. 2022;16:1842–50.
24. Maciej B, Imed EF, Kurkowski M. Multifactor authentication protocol in a mobile environment. IEEE Access. 2019;7:157185–99.
25. Noh KS. A study on the authentication and security of financial settlement using the finger vein technology in wireless internet environment. Wireless Pers Commun. 2016;89:761–75.
26. Wu X, Yang Z, Ling C, Xia XG. Artificial-noise-aided message authentication codes with information-theoretic security. IEEE Trans Inf Forensics Secur. 2016;11:1278–90.
27. Awasthi A. Reducing identity theft using one-time passwords and SMS. EDPACS. 2015;52:9–19.
28. Yin W, Wen Q, Li W, Zhang H, Jin Z. An anti-quantum transaction authentication approach in blockchain. IEEE Access. 2018;6:5393–401.
29. Malathi R. An integrated approach of physical biometric authentication system. Proced Comput Sci. 2016;85:820–6.
30. Alomair B, Poovendran R. Efficient authentication for mobile and pervasive computing. IEEE Trans Mob Comput. 2014;13:469–81.
31. Majumder A, Goswami J, Ghosh S, Shrivastawa R, Mohanty SP, Bhattacharyya BK. Pay-Cloak: a biometric back cover for smartphones: facilitating secure contactless payments and identity virtualization at low cost to end users. IEEE Consumer Electron Mag. 2017;6:78–88.
32. Sudharsan K, Kumar VDA, Venkatesan R, Sathyapreiya V, Saranya G. Two three step authentication in ATM machine to transfer money and for voting application. Proced Comput Sci. 2019;165:300–6.
33. Ara A, Sharma A, Yadav D. An efficient privacy-preserving user authentication scheme using image processing and blockchain technologies. J Dis Math Sci Cryptogr. 2022;25:1137–55.
34. Mwitende G, Ye Y, Ali I, Li F. Certificateless authenticated key agreement for blockchain-based WBANs. J Syst Archit. 2020;110:101777.
35. Basar OE, Alptekin G, Volaka HC, Isbilen M, Incel OD. Resource usage analysis of a mobile banking application using sensor-and-touchscreen-based continuous authentication. Proced Comput Sci. 2019;155:185–92.

36. Sharma MK, Nene MJ. Two-factor authentication using biometric based quantum operations. Secur Privacy. 2020;3:e102.
37. Nikkel B. Fintech forensics: Criminal investigation and digital evidence in financial technologies. Forensic Sci Int Digit Invest. 2020;33:200908.
38. Sinigaglia F, Carbone R, Costa G, Zannone N. A survey on multi-factor authentication for online banking in the wild. Comput Secur. 2020;95:101745.
39. Liébana-Cabanillas F, Muñoz-Leiva F, Molinillo S, Higueras-Castillo E. Do biometric payment systems work during the COVID-19 pandemic? Insights from the Spanish users' viewpoint. Financ Innov. 2022;8:1–25.
40. Irfanullah, Hussain T, Iqbal A, Yang B, Hussain A. Real time violence detection in surveillance videos using convolutional neural networks. Multimed Tools Appl. 2022. https://doi.org/10.1007/s11042-022-13169-4.
41. Wu F, Li X, Xu L, Vijayakumar P, Kumar N. A novel three-factor authentication protocol for wireless sensor networks with IoT notion. IEEE Syst J. 2020;15:1120–9.
42. Ogbanufe O, Kim DJ. Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. Decis Support Syst. 2018;106:1–14.
43. Bojjagani S, Sastry V. A secure end-to-end SMS-based mobile banking protocol. Int J Commun Syst. 2017;30:e3302.
44. Kaur G, Habibi Lashkari Z, Habibi Lashkari A. Cybersecurity vulnerabilities in FinTech. In: Kaur G, Lashkari ZH, Lashkari AH, editors. Understanding cybersecurity management in FinTech. Berlin: Springer; 2021. p. 89–102.
45. Sae-Bae N, Memon N. Online signature verification on mobile devices. IEEE Trans Inf Forensic Secur. 2014;9:933–47.
46. Mayron LM. Biometric authentication on mobile devices. IEEE Secur Priv. 2015;13:70–3.
47. Yang W, Wang S, Hu J, Zheng G, Chaudhry J, Adi E, et al. securing mobile healthcare data: a smart card based cancelable finger-vein bio-cryptosystem. IEEE Access. 2018;6:36939–47.
48. Odelu V, Das AK, Goswami A. A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Trans Inf Forensic Secur. 2015;10:1953–66.
49. Seepers RM, Strydis C, Sourdis I, Zeeuw CID. Enhancing heart-beat-based security for mhealth applications. IEEE J Biomed Health Inform. 2017;21:254–62.
50. Shila DM, Srivastava K. CASTRA: seamless and unobtrusive authentication of users to diverse mobile services. IEEE Internet Things J. 2018;5:4042–57.
51. Şengel Ö, Aydın MA, Sertbaş A. An efficient generation and security analysis of substitution box using fingerprint patterns. IEEE Access. 2020;8:160158–76.
52. Kuzu RS, Piciucco E, Maiorana E, Campisi P. On-the-fly finger-vein-based biometric recognition using deep neural networks. IEEE Trans Inf Forensic Secur. 2020;15:2641–54.
53. Habibu T, Luhanga ET, Sam AE. A study of users' compliance and satisfied utilization of biometric application system. Inf Secur J Glob Perspecti. 2021;30:125–38.
54. Henne K. Surveillance in the name of governance: aadhaar as a fix for leaking systems in India. In: Haggart B, Henne K, Tusikov N, editors. Information, technology and control in a changing world. Berlin: Springer; 2019. p. 223–45.
55. Rui Z, Yan Z. A survey on biometric authentication: toward secure and privacy-preserving identification. IEEE Access. 2018;7:5994–6009.
56. Mahfouz A, Mahmoud TM, Eldin AS. A survey on behavioral biometric authentication on smartphones. J Inf Secur Appl. 2017;37:28–37.
57. Ingale M, Cordeiro R, Thentu S, Park Y, Karimian N. Ecg biometric authentication: a comparative analysis. IEEE Access. 2020;8:117853–66.
58. Mason J, Dave R, Chatterjee P, Graham-Allen I, Esterline A, Roy K. An investigation of biometric authentication in the healthcare environment. Array. 2020;8:100042.
59. Kim S-K, Yeun CY, Damiani E, Lo N-W. A machine learning framework for biometric authentication using electrocardiogram. IEEE Access. 2019;7:94858–68.
60. Sarkar A, Singh BK. A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimed Tools Appl. 2020;79:27721–76.
61. Nagaraju S, Parthiban L. Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. J Cloud Comput. 2015;4:22.
62. Goode A. Biometrics for banking: best practices and barriers to adoption. Biometric Technol Today. 2018;2018:5–7.
63. Li W, Tan J, Meng W, Wang Y. A swipe-based unlocking mechanism with supervised learning on smartphones: design and evaluation. J Netw Comput Appl. 2020;165:102687.
64. Kang B-S, Lee K-H. 2-Channel authentication technique using cardiac impulse based OTP. J Comput Virol Hack Tech. 2016;12:163–7.
65. Kaman S, Swetha K, Akram S, Varaprasad G. Remote user authentication using a voice authentication system. Inf Secur J A Glob Perspect. 2013;22:117–25.
66. Furnell S. Assessing website password practices—unchanged after fifteen years? Comput Secur. 2022;120:102790.
67. Meng W, Zhu L, Li W, Han J, Li Y. Enhancing the security of FinTech applications with map-based graphical password authentication. Future Gener Comput Syst. 2019;101:1018–27.
68. Chang B, Li Y, Wang Q, Zhu W-T, Deng RH. Making a good thing better: enhancing password/PIN-based user authentication with smartwatch. Cybersecurity. 2018;1:7.
69. Kennison SM, Jones IT, Spooner VH, Chan-Tin DE. Who creates strong passwords when nudging fails. Comput Hum Behav Rep. 2021;4:100132.
70. Kanta A, Coray S, Coisel I, Scanlon M. How viable is password cracking in digital forensic investigation? Analyzing the guessability of over 3.9 billion real-world accounts. Forensic Sci Int: Digit Invest. 2021;37:301186.
71. Събев П, Petrov M. Android password managers and vault applications: data storage security issues identification. J Inf Secur Appl. 2022;67:103152.
72. Roger AG. One-time password attacks. In: Grimes RA, editor. Hacking multifactor authentication. Hoboken: Wiley; 2021. p. 205–26.
73. Srinivas K, Janaki V. A Novel approach for generation of OTP'S using image's. Proced Comput Sci. 2016;85:511–8.

74. Erdem E, Sandıkkaya MT. OTPaaS—one time password as a service. IEEE Trans Inf Forensics Secur. 2019;14:743–56.
75. Alves JM, Rodrigues TG, Beserra DW, Fonseca JC, Endo PT, Kelner J. Multi-factor authentication with openid in virtualized environments. IEEE Lat Am Trans. 2017;15:528–33.
76. Boakye-Boateng K, Kuada E, Antwi-Boasiako E, Djaba E. Encryption protocol for resource-constrained devices in fog-based IoT Using one-time pads. IEEE Internet Things J. 2019;6:3925–33.
77. de Ribeiro Mello E, Silva Wangham M, Bristot Loli S, da Silva CE, da Cavalcanti Silva G, de Chaves SA, et al. Multi-factor authentication for shibboleth identity providers. J Internet Serv Appl. 2020;11:8.
78. El-Booz SA, Attiya G, El-Fishawy N. A secure cloud storage system combining time-based one-time password and automatic blocker protocol. EURASIP J Inf Secur. 2016;2016:13.
79. Subpratatsavee P, Kuacharoen P. Transaction authentication using HMAC-based one-time password and QR code. In: Park JJ, Stojmenovic I, Jeong HY, Yi G, editors. Computer science and its applications. Berlin: Springer; 2015. p. 93–8.
80. Ajish S, Kumar KA. Secure mobile internet banking system using QR code and biometric authentication. In: Pandian AP, Fernando X, Haoxiang W, editors. Computer networks, big data and IoT. Berlin: Springer; 2022. p. 791–807.
81. Sun J, Shrestha K, Park H, Yadav P, Parajuli S, Lee S, et al. Bridging R2R printed wireless 1 bit-code generator with an electrophoretic QR code acting as WORM for NFC carrier enabled authentication label. Adv Mater Technol. 2020;5:1900935.
82. Ramalho JF, Dias LM, Fu L, Botas AM, Carlos LD, Carneiro Neto AN, et al. Customized luminescent multiplexed quick-response codes as reliable temperature mobile optical sensors for eHealth and internet of things. Adv Photonics Res. 2022;3:2100206.
83. Kang B, Jia J, Gao W, Zhang N. Research on improved character encoding methods based on QR code. Chin J Electron. 2019;28:1170–6.
84. Ramalho JF, Correia SF, Fu L, António LL, Brites CD, André PS, et al. Luminescence thermometry on the route of the mobile-based internet of things (IoT): how smart QR codes make it real. Adv Sci. 2019;6:1900950.
85. Wu W-C. Quantization-based image authentication scheme using QR error correction. EURASIP J Image Video Process. 2017;2017:13.
86. Tkachenko I, Puech W, Destruel C, Strauss O, Gaudin JM, Guichard C. Two-level QR code for private message sharing and document authentication. IEEE Trans Inf Forensics Secur. 2016;11:571–83.
87. Fu Z, Fang L, Huang H, Yu B. Distributed three-level QR codes based on visual cryptography scheme. J Vis Commun Image Represent. 2022;87:103567.
88. Kabra N, Bhattacharya P, Tanwar S, Tyagi S. MudraChain: blockchain-based framework for automated cheque clearance in financial institutions. Future Gener Comput Syst. 2020;102:574–87.
89. Xiong L, Zhong X, Xiong NN, Liu RW. QR-3S: a high payload QR code secret sharing system for industrial internet of things in 6G networks. IEEE Trans Industr Inf. 2021;17:7213–22.
90. Lin P. Distributed secret sharing approach with cheater prevention based on QR code. IEEE Trans Industr Inf. 2016;12:384–92.
91. Jiang P, Wu H, Xin C. A channel state information based virtual MAC spoofing detector. High-Confid Comput. 2022;2:100067.
92. Anathi M, Vijayakumar K. An intelligent approach for dynamic network traffic restriction using MAC address verification. Comput Commun. 2020;154:559–64.
93. Bairwa AK, Joshi S. Mutual authentication of nodes using session token with fingerprint and MAC address validation. Egypt Inf J. 2021;22:479–91.
94. Alsunaidi SJ, Almuhaideb AM. Investigation of the optimal method for generating and verifying the smartphone's fingerprint: a review. J King Saud Univ Comput Inf Sci. 2022;34:1919–32.
95. Satrya GB, Shin SY. Enhancing security of SIC algorithm on non-orthogonal multiple access (NOMA) based systems. Phys Commun. 2019;33:16–25.
96. Yu Y, He J, Zhu N, Cai F, Pathan MS. A new method for identity authentication using mobile terminals. Proced Comput Sci. 2018;131:771–8.
97. Waqas M, Tu S, Halim Z, Rehman SU, Abbas G, Abbas ZH. The role of artificial intelligence and machine learning in wireless networks security: principle, practice and challenges. Artif Intell Rev. 2022. https://doi.org/10.1007/s10462-022-10143-2.
98. Domashova J, Kripak E. Identification of non-typical international transactions on bank cards of individuals using machine learning methods. Proced Comput Sci. 2021;190:178–83.
99. Adewumi AO, Akinyelu AA. A survey of machine-learning and nature-inspired based credit card fraud detection techniques. Int J Syst Assur Eng Manag. 2017;8:937–53.
100. Fang H, Wang X, Tomasin S. Machine learning for intelligent authentication in 5G and beyond wireless networks. IEEE Wirel Commun. 2019;26:55–61.
101. Noor U, Anwar Z, Amjad T, Choo K-KR. A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. Future Gener Comput Syst. 2019;96:227–42.
102. Singh SK, Rathore S, Park JH. BlockIoTIntelligence: a blockchain-enabled intelligent IoT architecture with artificial intelligence. Future Gener Compu Syst. 2020;110:721–43.
103. Shivanna A, Ray S, Alshouiliy K, Agrawal DP. Detection of fraudulence in credit card transactions using machine learning on azure ML. In: 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). 2020. p. 268–73.
104. Ren L, Ward PAS. Understanding the transaction placement problem in blockchain sharding protocols. In: 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). 2021. p. 695–701
105. Satrya GB, Shin SY. Security enhancement to successive interference cancellation algorithm for non-orthogonal multiple access (NOMA). In: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). 2017. p. 1–5.

106. Singh P, Singh M. Fraud detection by monitoring customer behavior and activities. Int J Comput Appl. 2015;111:23.
107. Isaac RA, Chaturvedi P, Gareja P, Grover R. Secured E-banking system using artificial intelligence. Int J Emerg Technol Eng Res (IJETER). 2018;6.
108. Maduwantha MC, Vithana V. "MumCare": an artificial intelligence based assistant. Int J Electr Comput Eng Res. 2021;1:21–8.
109. Attkan A, Ranga V. Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex Intell Syst. 2022. https://doi.org/10.1007/s40747-022-00667-z.
110. Dillenberger DN, Novotny P, Zhang Q, Jayachandran P, Gupta H, Hans S, et al. Blockchain analytics and artificial intelligence. IBM J Res Dev. 2019;63:5:1-5:14.
111. Khan HU, Sohail M, Nazir S. Features-based IoT security authentication framework using statistical aggregation, entropy, and MOORA approaches. IEEE Access. 2022;10:109326–39.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.