Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 17 No. 22 (2023) | OPEN ACCESS

https://doi.org/10.3991/ijim.v17i22.45261

PAPER

Cybersecurity Challenges and Solutions in the Fintech Mobile App Ecosystem

Ishamuddin Mustapha[1](✉), Yamounah Vaicondam[2,3], Agha Jahanzeb[4], Burkhanov Aktam Usmanovich[5], Siti Hawa Binti Yusof[2]

[1]Malaysian Institute of Industrial Technology (MITEC), Universiti Kuala Lumpur, Kuala Lumpur, Malaysia

[2]School of Accounting & Finance, Faculty of Business and Law, Taylor's University, Subang Jaya, Selangor, Malaysia

[3]Digital Economy and Business Transformation Impact Lab, Taylor's University, Subang Jaya, Selangor, Malaysia

[4]Department of Business Administration, Sukkur IBA University, Sukkur, Pakistan

[5]Tashkent State University of Economics, Tashkent, Uzbekistan

Ishamuddin@unikl.edu.my

ABSTRACT

The rapid growth of the fintech industry, driven by the proliferation of mobile applications, has revolutionized financial services, providing unprecedented convenience to users. However, this innovation comes with inherent cybersecurity challenges that demand rigorous attention. This study delves into the complex and ever-evolving landscape of cybersecurity within the fintech mobile app ecosystem, aiming to identify challenges and present viable solutions. Cybersecurity threats in the fintech mobile app ecosystem encompass a broad spectrum, including data breaches, malware attacks, phishing schemes, and identity theft. As fintech apps handle sensitive financial data and transactions, they are prime targets for malicious actors seeking financial gain. To address these threats, this research examines current cybersecurity strategies and emerging technologies, such as advanced encryption, biometric authentication, and AI-driven anomaly detection. Furthermore, regulatory frameworks and industry standards play a crucial role in shaping cybersecurity practices within fintech. This study assesses the impact of compliance requirements on fintech companies and their ability to protect user data. Real-world case studies and incident analyses provide valuable insights into the consequences of cybersecurity breaches in this sector. Ultimately, this research aims to contribute to a comprehensive understanding of the multifaceted cybersecurity challenges faced by the fintech mobile app ecosystem and offers practical recommendations for fintech firms, regulators, and cybersecurity professionals to enhance security measures. Strengthening the security foundation is paramount to sustaining user trust, fostering continued innovation, and securing the future of mobile fintech.

KEYWORDS

fintech, mobile applications, cybersecurity, Internet of Things (IoT), financial service

1 INTRODUCTION

The exponential expansion of technology has had a significant impact on several business sectors, notably the financial sector [1]. The realm of finance and banking has seen a substantial transformation, whereby traditional customer-facing services

Mustapha, I., Vaicondam, Y., Jahanzeb, A., Usmanovich, B.A., Binti Yusof, S.H. (2023). Cybersecurity Challenges and Solutions in the Fintech Mobile App Ecosystem. *International Journal of Interactive Mobile Technologies (iJIM)*, 17(22), pp. 100–116. https://doi.org/10.3991/ijim.v17i22.45261

Article submitted 2023-08-25. Revision uploaded 2023-10-03. Final acceptance 2023-10-10.

have been replaced with digitally driven operations facilitated via applications [2]. In addition, fintech mobile applications refer to software applications specifically developed for smartphones and tablets, offering a diverse array of financial services, and facilitating various transactions [3]. These applications use technological advancements to provide users with simple and effective methods for managing their financial resources, conducting transactions, accessing banking facilities, engaging in investment activities, and other related services, all accessible via handheld devices [4]. The emergence of fintech mobile applications has swiftly garnered attention, leading to a significant transformation within the financial services sector [5]. These digital financial services have become essential components of the everyday routines of a vast number of individuals, providing a wide range of functionalities like mobile banking, peer-to-peer transactions, budgeting and financial management utilities, investing platforms, and even the ability to engage in cryptocurrency trading [6].

In addition, scholars have seen the significant influence of mobile applications in the fintech industry for enhancing financial inclusion [7], [8]. Consequently, there is a growing recognition of the need for thorough scrutiny of the security and privacy considerations associated with these apps [9]. Furthermore, research has examined the adoption patterns and behavioural dimensions of these applications, providing insights into the changing dynamics of the financial technology ecosystem [10].

However, the digital financial sector is characterised by a significant challenge about the cybersecurity that arises with fintech mobile applications [11]. The concerns discussed involve a diverse set of threats and vulnerabilities that have the potential to compromise user data, financial transactions, and the general integrity of these apps [12]. On the obstacles encountered by fintech mobile applications, with a particular focus on data breaches, identity theft, and fraud as noteworthy concerns [13]. In addition, the research emphasises the need of implementing measures to ensure the security of user authentication procedures, transaction encryption, and strong access restrictions to reduce these risks. Furthermore, the study conducted by [14] extensively examines the dynamic nature of the threat environment, specifically highlighting the rise of advanced forms of assaults such as mobile malware and phishing operations that specifically target users of fintech applications. There is an emphasis on the need for ongoing surveillance, the acquisition of threat information, and the implementation of proactive security measures to effectively address these ever-changing dangers [15]. The studies together underscore the complex and diverse nature of cybersecurity concerns in the realm of financial technology mobile applications, as well as the continual endeavours necessary to guarantee the security and reliability of these financial technologies [16], [17].

The primary objective of this research is to conduct an in-depth examination of the cybersecurity concerns that are often seen in the ecosystem of mobile applications in the financial technology sector and to suggest viable and efficient solutions to address these challenges. The study endeavours to enhance the security of mobile fintech apps by undertaking a comprehensive analysis of new threats, cybersecurity methods, and regulatory effects. It also seeks to deliver significant insights that will contribute to the field.

2 RESEARCH METHODOLOGY

The current study employed the PRISMA statement 2020 to include and exclude records from Scopus databases to incorporate high-quality materials The data were screened using the Preferred Reporting Items for Systematic Reviews and

Meta-Analyses (PRISMA) methodology, as recommended by [18], [19] and shown in Figure 1. The current study used the PRISMA Statement 2020 to enhance the reporting of literature records and relevant information. In conducting our literature evaluation, we used the search terms "cybersecurity," AND "Fintech," AND "Mobile apps" in combination. A total of 160 records were initially gathered. The current assessment included literature from several disciplines, including computer science, business management, engineering, economics, psychology, and social sciences. Hence, the resulting dataset has a total of 140 documents. Furthermore, the scope of our study was restricted to scholarly articles, reviews, and book chapters, resulting in a reduced dataset of 130 entries. Furthermore, to replicate the study's comprehensive examination of relevant scholarly findings, only publications that were published and written in the English language were included. After the completion of this phase, there were a total of 125 records that remained. The subsequent phase was the removal of redundant or absent document information. A comprehensive selection process was conducted to analyse relevant information for each identified category. A total of 119 publications were available, facilitating a straightforward synthesis. The current study utilises the PRISMA statement selection and rejection technique, as shown in Figure 1.

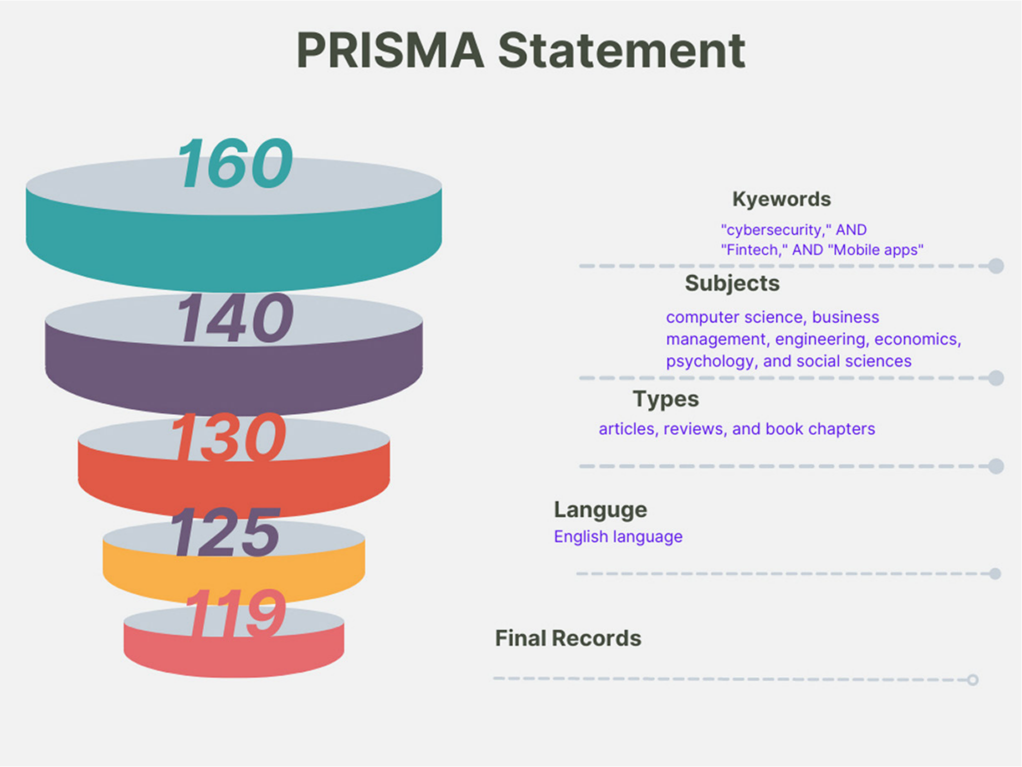
PRISMA Statement
160
140
130
125
119
Kyewords
"cybersecurity," AND "Fintech," AND "Mobile apps"
Subjects
computer science, business management, engineering, economics, psychology, and social sciences
Types
articles, reviews, and book chapters
Languge
English language
Final Records

Fig. 1. PRISMA statement for inclusion and exclusion of records

In addition, Table 1 presents crucial details pertaining to the dataset used in the present research, furnishing valuable insights into the origins of the data, the contents of the documents, the authors involved, the extent of cooperation among the authors, and the various kinds of documents included. The dataset has a time frame ranging from 2017 to 2023 and encompasses a significant compilation of 101 sources, including various scholarly outlets such as journals, books, and other forms of publishing. There is a total of 119 papers, exhibiting a notable yearly growth rate of 30.77%, hence emphasising the escalating significance of the study issue as time progresses. The contents of the paper are extensive, including 361 Keywords Plus (ID) and 388 Author's Keywords (DE), which signify a wide range of keywords and ideas related to cybersecurity concerns and solutions inside the FinTech mobile app ecosystem. This implies a thorough investigation of the topic.

Moreover, the collection has contributions from a total of 353 individuals, of whom 22 people have exclusively created individual documents. The presence of collaboration among writers is apparent, as shown by an average of 3.04 co-authors per document. It is worth noting that foreign co-authorships constitute 27.73% of partnerships, indicating the global character of research on this topic. In relation to the categorization of documents, the dataset mostly consists of articles (81), followed by book chapters (32) and reviews (6). The presence of many document formats suggests an inclusive approach towards comprehending and evaluating cybersecurity issues and resolutions inside the FinTech mobile app ecosystem. This approach encompasses a range of viewpoints and research approaches. The dataset presented herein serves as a vital and fundamental basis for conducting a thorough and current analysis of this crucial domain.

Table 1. Main information

Description	Results
Timespan	2017:2023
Sources (Journals, Books, etc.)	101
Documents	119
Annual Growth Rate %	30.77
Document Average Age	1.83
Average citations per doc	10.9
References	5360
Keywords Plus (ID)	361
Author's Keywords (DE)	388
Authors	353
Authors of single-authored docs	22
Single-authored docs	23
Co-Authors per Doc	3.04
International co-authorships %	27.73
Article	81
Book chapter	32
Review	6

Simultaneously, Figure 2 provides a comprehensive and perceptive depiction of the yearly output of scholarly publications pertaining to the subject matter of cybersecurity issues and solutions within the fintech mobile application ecosystem. The temporal scope of the study encompasses the years 2017 to 2023, during which a discernible positive trajectory is seen in the number of articles generated. In the year 2017, a total of six articles were published, which was followed by five pieces in

2018 and seven articles in 2019. Nevertheless, there is a notable upward trend seen in the following years, as shown by a major increase in the quantity of published papers annually. The number of articles published in the year 2020 amounted to 16, and this pattern persisted as the following years saw an increase in the number of articles, with 26 pieces in 2021, 29 articles in 2022, and 30 articles in 2023. The presented data highlights the escalating significance and research endeavours associated with this crucial topic, indicating the rising prominence of cybersecurity within the fintech mobile app ecosystem.

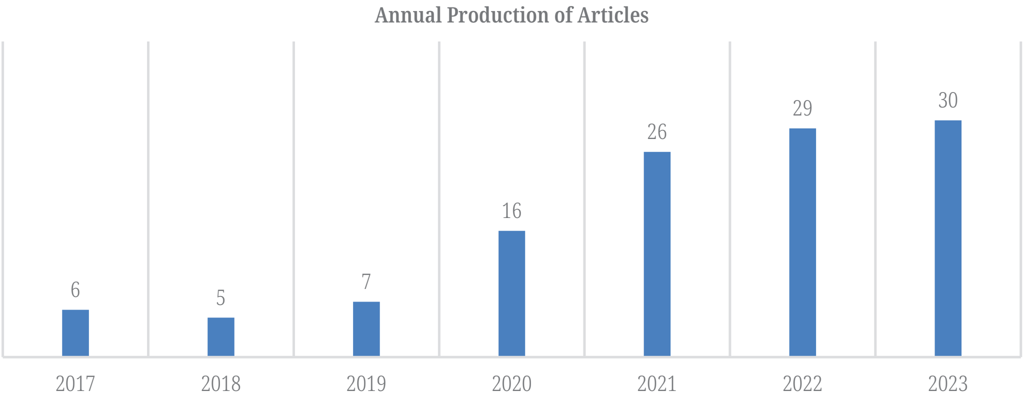

Fig. 2. The ascending trend of research publications on cybersecurity in the fintech mobile app ecosystem (2017–2023)

Also, Figure 3 offers significant insights into the many sources that have made contributions to the existing body of knowledge about the study issue of cybersecurity problems and solutions within the fintech mobile app ecosystem. The document provides a comprehensive compilation of pertinent references, along with the corresponding count of connected scholarly papers. Numerous prominent academic journals and publications have played a pivotal role in furthering research within this particular discipline. The “IEEE Internet of Things Journal” has emerged as a prominent and authoritative publication, with four articles that highlight the significance of IoT-related factors within the domains of cybersecurity and finance. Moreover, the journals “Contributions to Management Science” and “Contributions to Finance and Accounting” each include three articles, so emphasising the interdisciplinary character of research in this field and its ability to connect the domains of management, finance, and technology.

In addition, several academic sources, including “Finance: Theory and Practise,” “Global Perspectives in FinTech: Law, Finance, and Technology,” “Handbook of Research on Cybersecurity Issues and Challenges for Business and Fintech Applications,” and “IEEE Access,” have a pair of linked articles apiece. The papers together illustrate the extensive spread of information and the need of interdisciplinary cooperation in tackling cybersecurity concerns within the field of financial technology. Furthermore, the inclusion of scholarly works such as “Islamic FinTech: Insights and Solutions,” “Sustainability (Switzerland),” “Technological Forecasting and Social Change,” and “Revolutionising Financial Services and Markets Through Fintech and Blockchain” underscores the wide range of viewpoints and specialised knowledge present in the academic literature pertaining to this significant topic. In general, Figure 3 illustrates the diverse and extensive range of sources that have played a role in enhancing the comprehension of cybersecurity within the FinTech mobile app ecosystem. This depiction highlights the multidisciplinary and worldwide characteristics of research conducted in this domain.

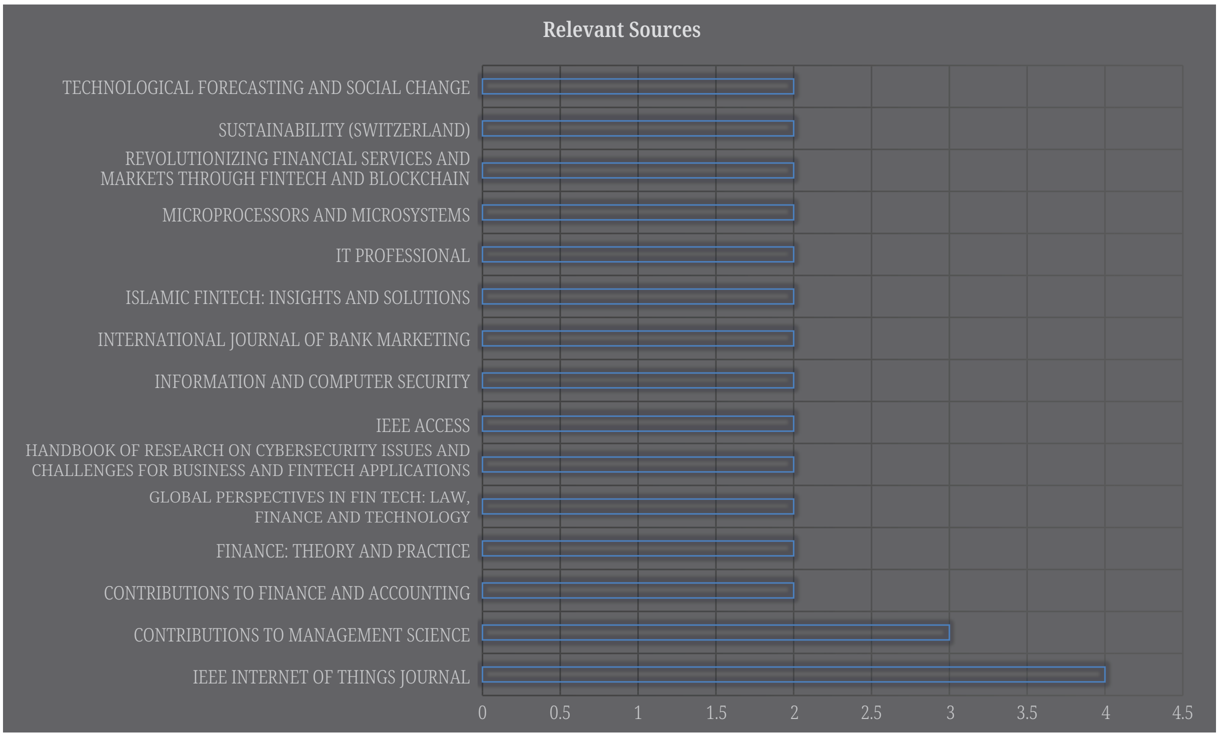

Fig. 3. Relevant sources of cybersecurity and fintech mobile apps

3 DATA ANALYSIS AND RESULTS

This study used a descriptive-analytic strategy to conduct a bibliometric inquiry. The Bibliometrix RStudio-4.2.1-win programme was applied for data analysis. The Bibliometrics R package has been more prominent in scholarly literature. The purpose of this package is to streamline the process of importing bibliographic data from Scopus into the R programming environment. To conform to a rigorous bibliometric methodology, a specialised application called Bibliometric was created, using statistical computing methods and the R programming language. The R system is generally acknowledged as the primary platform for developing statistical algorithms and is frequently used as a versatile software tool for data analysis and visualisation, as seen in the study paper entitled "Mapping Research on Using Biblioshiny" [20]. Within the wider body of literature pertaining to bibliometrics, a plethora of research and resources exist that delve into the methodology, techniques, and applications of bibliometric analysis across many academic domains [21]. Scholars seeking to perform bibliometric studies may consult these sources to get a deeper understanding of bibliometric approaches and their efficient use in research endeavours [22].

In addition, Table 2 presents a detailed analysis of worldwide citations for a chosen set of research publications, demonstrating their significance and influence within the realm of cybersecurity in the fintech mobile app ecosystem. The table comprises various elements for each entry, namely the title of the paper, the DOI (Digital Object Identifier), the total number of citations, the citations received per year, and a metric referred to as "Normalised TC" (Normalised Total Citations). The Normalised TC represents the average number of citations received by a paper annually, considering both the duration of time and the total number of citations. These indicators provide valuable insights into the importance and durability of the contributions made by each manuscript to the academic community.

Several scholarly articles have significant influence. The publication of "MHLANGA D," [23] has received a total of 114 citations, demonstrating a noteworthy average of 28.50 citations per year. This suggests a consistent level of attention and significance within the relevant academic domain. In a similar vein, it is noteworthy that the articles "MODGIL S," [24] and "FU J," [25] have garnered considerable attention in terms of citation rates. These articles have received a total of 52 and 49 citations, respectively, indicating their significant impact and influence within the scholarly community. Moreover, their strong Normalised TC values further emphasise the noteworthy contributions these articles have made to the current research environment.

On the other hand, scholarly articles such as UMOREN IA, [26] have garnered a lesser number of citations, indicating a comparatively diminished influence or a more limited scope. However, the inclusion of these entities in the table serves to underscore the wide array of research conducted within the discipline, including many subjects and areas of focus. This tool facilitates academics in the identification of influential publications, monitoring the evolution of individual articles over time, and comprehending the wider scope of scholarly contributions in the field of cybersecurity within the fintech mobile app ecosystem. The provided material has significant value for academics who want to expand upon current knowledge and effectively traverse the continuously developing realm of fintech cybersecurity.

Table 2. Overview of global citations

Paper	DOI	Total Citations	TC per Year	Normalized TC
MHLANGA D [23]	10.3390/ijfs8030045	114	28.50	4.03
STEWART H [27]	10.1108/ICS-06-2017-0039	100	16.67	2.81
LIU J [28]	10.1016/j.techfore.2020.120022	78	19.50	2.75
DEMIRGÜÇ-KUNT A [29]	10.1093/wber/lhz013	74	18.50	2.61
NG AW [30]	10.1108/JFRC-01-2017-0013	57	8.14	1.94
MODGIL S [24]	10.1016/j.techfore.2021.121415	52	26.00	8.82
MEHRBAN S [31]	10.1109/ACCESS.2020.2970430	49	12.25	1.73
FU J [25]	10.1016/j.jfi.2021.100945	49	24.50	8.31
QI BY, 2018 [32]	10.1145/3239550	46	7.67	1.29
MOSTEANU NR [33]	10.3390/joitmc7010019	38	12.67	4.10
LEE S [34]	10.3837/tiis.2017.02.027	37	5.29	1.26
HENDERSHOTT T [35]	10.1287/isre.2021.0997	37	12.33	3.99
KAUFFMAN RJ [36]	10.1016/j.elerap.2017.04.004	36	5.14	1.23
NGUYEN LD [37]	10.1109/JIOT.2021.3051923	33	11.00	3.56
UMOREN IA [26]	10.1109/MCE.2020.2988904	27	6.75	0.95
CHO T-Y [38]	10.1016/j.najef.2021.101414	21	7.00	2.27
WANG JS, 2021 [39]	10.1186/s40854-021-00260-2	21	7.00	2.27
FERREIRA CMS [40]	10.3390/s21041323	21	7.00	2.27
LI B [41]	10.1891/JFCP-18-00083	20	5.00	0.71
UDDIN MH [42]	10.1016/j.irfa.2020.101587	20	5.00	0.71
SHAHEEN M [43]	10.3390/electronics11040670	17	8.50	2.88
MORGAN PJ [44]	10.1111/aepr.12379	15	7.50	2.54
Maiti M [45]	10.1109/JIOT.2021.3063494	15	15.00	10.00

Furthermore, Table 3 presents a comprehensive chronology of author productivity over several years, emphasising the frequency of publications, total citations, and citations per year for each author within the realm of cybersecurity in the fintech mobile app ecosystem. The data elucidates intriguing trends pertaining to authorship and the influence inside this study field. Numerous writers have made significant contributions. In the year 2020, a researcher named ABBAS F. authored a solitary publication that garnered a commendable total citation count (TC) of 49. This noteworthy TC serves as an indicator of the substantial importance and influence of the scholarly contribution. In a similar vein, two notable researchers, "KIM KT" and "LI B," have contributed to the academic discourse by publishing papers in the year 2020. These works have garnered significant attention, as seen by their considerable citation counts, with TC values reaching 20. This serves as a testament to the impact and influence of their respective research endeavours.

Nevertheless, it is crucial to acknowledge that writers may have restricted or non-existent citations for certain years. For instance, two authors, "ALI G" and "ALI G," have produced scholarly articles in the years 2021 and 2022, respectively. However, it is noteworthy that their TC pY metrics exhibit very modest values, suggesting that their contributions may not have garnered much acknowledgement within the academic community. It is noteworthy that the publications authored by "DEL SARTO N" and "DUDIN MN" in 2023 did not earn any citations, indicating that their new intellectual contributions have not yet been recognised or integrated into the existing academic conversation. In contrast, it is noteworthy that "LEE J-C" has emerged as a very productive writer in the year 2023, having authored two papers and achieving a TC pY score of 12. This score indicates a prompt and substantial influence and acknowledgement within the respective academic domain.

The author "WANG JS" has shown a notable scholarly impact, as seen by their papers in 2021 and 2023, which have garnered considerable citations. In brief, the Figure depicting Author Production Over Time offers a significant overview of author contributions and influence in the domain of cybersecurity in fintech mobile applications. It effectively showcases the diverse degrees of recognition and impact among academics in this rapidly evolving topic. This information may be used by researchers to discern prominent writers and their influential contributions, hence facilitating the exploration of the dynamic realm of fintech cybersecurity academia.

Table 3. Author production over time

Author	Year	Freq	TC	TC pY
ABBAS F	2020	1	49	12.25
ALI G	2021	1	7	2.333
ALI G	2022	1	1	0.5
DEL SARTO N	2023	2	0	0
DIDA MA	2021	1	7	2.333
DIDA MA	2022	1	1	0.5
DUDIN MN	2021	1	4	1.333
DUDIN MN	2022	1	0	0
KIM KT	2020	1	20	5
KIM KT	2023	1	1	1
LEE J-C	2023	2	12	12

(Continued)

Table 3. Author production over time *(Continued)*

Author	Year	Freq	TC	TC pY
LI B	2020	1	20	5
LI B	2021	1	3	1
SAM AE	2021	1	7	2.333
SAM AE	2022	1	1	0.5
WANG JS	2021	1	21	7
WANG JS	2023	1	1	1

In addition to this, Table 4 presents a comprehensive analysis of the prevailing research subjects in the field of cybersecurity issues and solutions within the fintech mobile app ecosystem, offering valuable insights. These subjects demonstrate the changing interests and concerns of scholars in this discipline throughout time, providing insight into the primary areas of concentration and investigation. The table presents a number of significant trends. First and foremost, the term "fintech" has emerged as a very significant subject of research, appearing 11 times over various years. This frequency of occurrence demonstrates the enduring relevance and importance of fintech in the realm of cybersecurity research. The terms "blockchain" and "finance" exhibit a notable frequency of eight and seven instances, respectively, indicating a growing fascination with the convergence of blockchain technology and financial services within the fintech domain.

The subject of "cybersecurity" is a frequently discussed issue that reflects the central focus of the study field. The ongoing significance of the issue of "cybersecurity" is evident, since it has remained a topic of research in subsequent years despite reaching its pinnacle in 2018. Additional growing subjects in the field include "mobile payment systems," "network security protocols," "electronic currency," "the internet of things," and "cybersecurity measures." These subjects exhibit different levels of prevalence and progression across time, with some issues acquiring more significance in recent years. The data shown in Table 4 indicates that scholars are consistently investigating various aspects of cybersecurity concerns and solutions within the FinTech mobile app ecosystem. This study is conducted in response to the dynamic nature of financial technology and the ever-changing environment of security threats. The provided material has significant value for researchers and practitioners who want to remain well-informed about the latest and pertinent research domains within this ever-evolving discipline.

Table 4. Most trending research topics in cybersecurity challenges and solutions in the fintech mobile app ecosystem

Item	Freq	Year q1	Year Med	Year q3
Finance	7	2018	2018	2023
Fintech	11	2019	2020	2021
Cyber security	6	2018	2020	2022
Blockchain	8	2020	2021	2022
Mobile payment	5	2020	2021	2023
Network security	5	2021	2021	2023
Electronic money	6	2021	2022	2023
Internet of things	7	2021	2023	2023
Security	7	2022	2023	2023

The findings of a bibliometric analysis are shown in Table 5, which aims to identify clusters of research subjects related to the issues and solutions in the fintech mobile app ecosystem within the area of cybersecurity. The distinguishing features of each cluster are its Callon Centrality, Callon Density, Rank Centrality, Rank Density, and Cluster Frequency. These metrics provide valuable insights into the significance and interconnectedness of the many study issues. In addition, the cluster labelled as "internet" has the greatest level of Callon Density, suggesting a notable degree of interconnectivity across the many subjects within this cluster. Although it holds the highest position in terms of Callon Centrality, it is worth mentioning that this cluster exhibits a comparatively lower Cluster Frequency in relation to some other clusters. This observation implies that the emphasis within this cluster is placed on quality rather than quantity. This observation suggests a comprehensive investigation into certain facets of internet-related concerns within the realm of fintech cybersecurity.

The cluster labelled as "fintech" has a notable Cluster Frequency of 82, indicating its prominence and substantial scholarly investigation within this domain. The ranking of fourth in Callon Centrality underscores the extensive scope of subjects included within the larger fintech domain. The observed high Callon Density and Rank Density indicate that this cluster has a significant presence, as well as strong interconnections and influence within the study domain. Also, the cluster labelled as the "financial service" cluster, which holds the third position in Callon Centrality, pertains to a range of elements concerning financial services within the fintech domain. The Cluster Frequency is comparatively lower, suggesting a narrower focus within the field of inquiry. The cluster pertaining to the "Internet of Things" has a significant degree of Callon Density, indicating a pronounced interconnectivity across many subjects associated with the intersection of IoT, fintech, and cybersecurity. The entity in question has the second position in both Rank Centrality and Rank Density metrics, suggesting its notable impact and prominence within the respective domain.

Table 5. Clusters identified using bibliometric analysis

Cluster	Callon Centrality	Callon Density	Rank Centrality	Rank Density	Cluster Frequency
Internet	0	84.72222222	1	2	13
Fintech	6.019047619	111.7566687	4	3	82
Financial service	3.263888889	68.51851852	3	1	16
Internet of things	2.877777778	124.5694759	2	4	60

Finally, the topic of research was chosen as the keyword plus during the building of the thematic map and examination of its progression [46]. To achieve the best results, the word count was limited to 50 to 250, allowing for thorough research [47], [48]. The thematic map in this particular context functions as a visual depiction of the research terrain within the field of study pertaining to cybersecurity issues and solutions in the fintech mobile app ecosystem. The map uses labels to categorise clusters of interconnected research subjects, wherein a minimum cluster frequency of 15 per thousand documents is established as the criterion for inclusion. The size of the labels is changed to 0.03 to improve their visibility on the map. It is crucial to acknowledge that the dimensions of these labels are relative and established by the tool, with a value of 1 denoting the maximum size. The thematic map is structured according to two primary aspects, namely density and centrality. The organisation establishes four discrete quadrants, including developing or decreasing topics, motor themes, fundamental themes, and specialised themes. These quadrants are demarcated by dashed lines along both the horizontal and vertical axes.

In the present thematic map, certain research categories such as "financial services" and "5G communication systems" have been classified as foundational themes, reflecting their fundamental significance within the field of study. On the other hand, the concept of "Internet banking" is situated inside the quadrant denoting topics that are either progressing or regressing, implying that it might be a subject of fluctuation or diminished significance within the domain. In addition, the niche theme quadrant encompasses subjects such as "Internet of things" and "security," indicating their distinct and concentrated characteristics. On the other hand, the phrases "cloud computing," "big data," and "data analytics" are positioned in the motor theme quadrant, emphasising their substantial and dynamic significance within the realm of research. Furthermore, the terms "Fintech" and "blockchain" are situated inside the motor theme quadrant, signifying their dynamic and important role within the domain.

The thematic map, as seen in Figure 4, provides a visual representation that enables scholars to examine the comparative significance and progressions of various issues within the field of study. The use of quadrants as a means of categorising subjects offers a valuable instrument for comprehending the dynamics, interrelationships, and patterns within thematic domains. This tool becomes advantageous to researchers as it facilitates the conduct of detailed studies pertaining to the overarching themes and trends within their respective study fields.

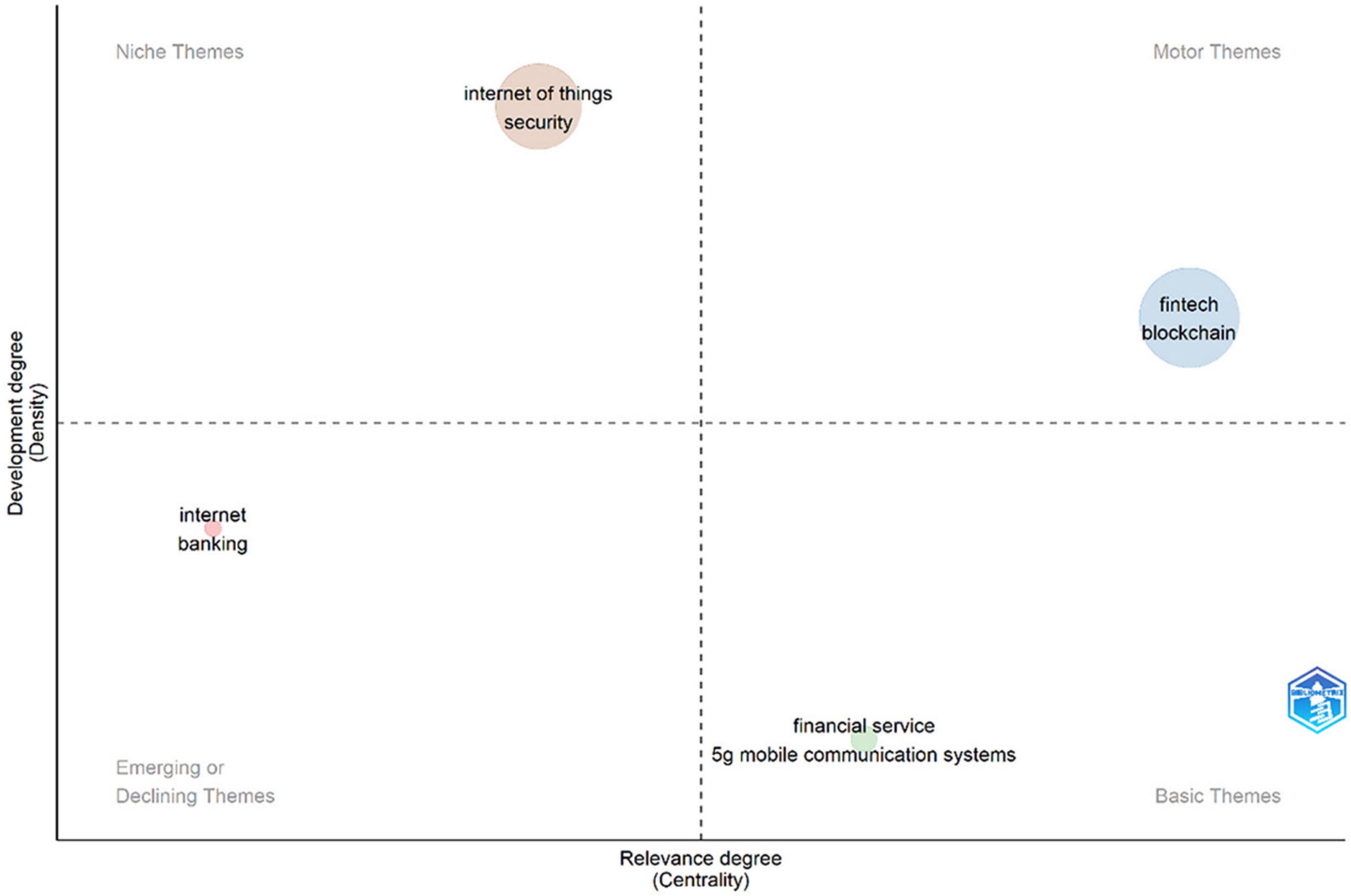

Fig. 4. Thematic map

4 DISCUSSION AND CONCLUSION

The financial technology (fintech) sector has seen a significant and fast evolution in recent times, mostly propelled by the widespread use of mobile apps [49]. The aforementioned apps have significantly transformed the manner in which individuals access and use financial services, providing enhanced ease and accessibility to consumers [50]. Nevertheless, the simplicity and accessibility provided by this convenience have been accompanied by a rise in cybersecurity risks [51]. The protection of user information and financial transactions has become of utmost importance due to the processing of sensitive financial data and transactions via mobile applications [52]. However, a primary focus of our discourse pertained to the formulation of scholarly publications within this domain. We examined prospective research article subjects that are now gaining popularity within the fintech and mobile apps industry. The subjects covered a broad spectrum, including the effects of blockchain and cryptocurrencies as well as the contribution of artificial intelligence in bolstering security within the finance industry. The extensive range of these subjects underscores the ever-changing characteristics of the field and the necessity for ongoing investigation to confront the increasing cybersecurity obstacles.

The research results show that the study titled "Examining the Dynamic Landscape of Cybersecurity in Mobile Fintech: A Comprehensive Analysis of Emerging Threats and Protective Measures for Safeguarding User Data and Financial Transactions in Mobile Fintech Applications" accurately encapsulated the central objective of the investigation, placing significant emphasis on the ever-changing nature of cybersecurity threats and the requisite strategies necessary for proficiently mitigating them. In addition, an analysis was conducted on the attributes of the dataset used in our research. The dataset exhibited a range of characteristics, including the duration, origins, textual contents, and authorship particulars. The use of this dataset was of utmost importance in facilitating a thorough examination of the scholarly terrain, discerning patterns, and evaluating the influence of diverse research publications.

Furthermore, the analysis conducted the yearly output of research records, offering valuable insights into the expansion and significance of research papers within this domain. The observed upward trend in the number of papers published between 2017 and 2023 serves to highlight the escalating significance and level of attention devoted to the field of fintech cybersecurity. The discourse underscored the increasing popularity and ongoing development of this study. Also, a comprehensive compilation of the prevailing study themes illustrate the dynamic interests and focal points of scholars within this domain. Significantly, the domains of fintech, blockchain, and the Internet of Things have emerged as major subjects, therefore highlighting the multidisciplinary character of research in the field of fintech cybersecurity. Additionally, an examination was conducted on clusters that were found using bibliometric analysis, providing insights into the interconnections and significance of research subjects. The clusters include a wide range of topics, including fundamental issues such as financial services and specialised subjects such as the Internet of Things. Together, they provide a complete perspective on the research environment. In summary, the deliberations have shed light on the intricate and diverse characteristics of cybersecurity obstacles and remedies within the realm of financial technology and mobile applications. As the sector undergoes continuous transformation, the significance of research in this domain becomes more paramount. The talks we engage in provide valuable insights that enhance our comprehension of the evolving trends, problems, and opportunities in this dynamic environment. Both researchers and practitioners could use these findings to create efficient methods and solutions that will protect user data and financial transactions within the field of fintech and mobile apps.

5 FUTURE OF FINTECH MOBILE APPLICATIONS

The continuous advancement of financial technology (fintech) and mobile apps underscores the need for persistent investigation into new cybersecurity risks. The incorporation of technologies such as blockchain, the Internet of Things (IoT), and artificial intelligence (AI) into financial technology (fintech) systems necessitates a comprehensive comprehension of the weaknesses and hazards linked to these advancements. Future studies should aim to explore the complexities associated with ensuring the security of these technologies inside mobile fintech apps and developing resilient defence mechanisms. Moreover, the multidisciplinary character of cybersecurity in the realm of financial technology necessitates the cooperation of researchers from several disciplines, such as finance, computer science, law, and cybersecurity. In order to effectively tackle the complex difficulties presented by cyber threats in the fintech industry, it is imperative that future research agendas place a high priority on adopting multidisciplinary methods. This collaborative effort has the potential to provide comprehensive solutions that address not just technology dimensions, but also incorporate legal and regulatory factors.

Additionally, the establishment of regulatory frameworks and adherence to compliance requirements significantly influence the development and implementation of cybersecurity measures within the FinTech mobile app ecosystem. Further investigation is required about the ramifications of laws on cybersecurity plans, the obstacles encountered by fintech businesses in achieving compliance, and the efficacy of regulatory measures in bolstering security. Moreover, prioritising user awareness and education is crucial in avoiding cybersecurity concerns. Subsequent investigations may be directed towards the development and assessment of educational initiatives targeting individuals using fintech services as well as professionals operating within the fintech industry. These programmes have the potential to assist users in making well-informed decisions and implementing secure practices while engaging with mobile fintech apps. In light of the continuously changing threat environment, it is essential to emphasise the significance of doing research on proactive and predictive cybersecurity solutions. The task at hand encompasses the creation of predictive models powered by artificial intelligence, the establishment of threat intelligence systems, and the implementation of real-time monitoring solutions. These measures aim to identify and address cyber risks in mobile fintech apps at an early stage, thereby preventing their escalation.

6 REFERENCES

[1] R. R. Suryono, I. Budi, and B. Purwandari, "Challenges and trends of financial technology (Fintech): A systematic literature review," *Information*, vol. 11, no. 12, pp. 1–20, 2020. https://doi.org/10.3390/info11120590

[2] S. Agarwal and J. Zhang, "FinTech, lending and payment innovation: A review," *Asia-Pacific Journal of Financial Studies*, vol. 49, no. 3, pp. 353–367, 2020. https://doi.org/10.1111/ajfs.12294

[3] H. Taherdoost, "Fintech: Emerging trends and the future of finance," in *Financial Technologies and DeFi. Financial Innovation and Technology*, Springer, Cham, 2023, pp. 29–39. https://doi.org/10.1007/978-3-031-17998-3_2

[4] D. Gabor and S. Brooks, “The digital revolution in financial inclusion: International development in the fintech era,” *New Political Economy*, vol. 22, no. 4, pp. 423–436, 2017. https://doi.org/10.1080/13563467.2017.1259298

[5] P. Gomber, R. J. Kauffman, C. Parker, and B. W. Weber, “On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services,” *Journal of Management Information Systems*, vol. 35, no. 1, pp. 220–265, 2018. https://doi.org/10.1080/07421222.2018.1440766

[6] H. Taherdoost, “Fintech: Emerging trends and the future of finance,” in *Financial Technologies and DeFi. Financial Innovation and Technology*, Springer, Cham, 2023, pp. 29–39. https://doi.org/10.1007/978-3-031-17998-3_2

[7] S. Lagan, P. Aquino, M. R. Emerson, K. Fortuna, R. Walker, and J. Torous, “Actionable health app evaluation: Translating expert frameworks into objective metrics,” *npj Digital Medicine,* vol. 3, no. 1, pp. 1–8, 2020. https://doi.org/10.1038/s41746-020-00312-4

[8] N. Khan, N. T. Van, A. Imran, H. Raza, and H. Sikandar, “Ecotourism is the future of alternative tourism for environmental sustainability and natural areas protection,” *Systematic Literature Review and Meta-Analysis Journal*, vol. 1, no. 2, pp. 99–116, 2021. https://doi.org/10.54480/slrm.v1i2.8

[9] H. Liu, P. Yao, S. Latif, S. Aslam, and N. Iqbal, “Impact of Green financing, FinTech, and financial inclusion on energy efficiency,” *Environmental Science and Pollution Research*, vol. 29, no. 13, pp. 18955–18966, 2022. https://doi.org/10.1007/s11356-021-16949-x

[10] N. T. Van, S. Irum, A. F. Abbas, H. Sikandar, and N. Khan, “Online learning—Two side arguments related to mental health,” *International Journal of Online and Biomedical Engineering*, vol. 18, no. 9, pp. 131–143, 2022. https://doi.org/10.3991/ijoe.v18i09.32317

[11] M.-S. Jameaba, “Digitization revolution, FinTech disruption, and financial stability: Using the case of Indonesian banking ecosystem to highlight wide-ranging digitization opportunities and major challenges,” *SSRN Electronic Journal*, 2020. https://doi.org/10.2139/ssrn.3529924

[12] Y. Chen, E. K. kumara, and V. Sivakumar, “Investigation of finance industry on risk awareness model and digital economic growth,” *Annals of Operations Research*, vol. 326, no. 1, p. 15, 2021. https://doi.org/10.1007/s10479-021-04287-7

[13] P. Gomber, R. J. Kauffman, C. Parker, and B. W. Weber, “On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services,” *Journal of Management Information Systems,* vol. 35, no. 1, pp. 220–265, 2018. https://doi.org/10.1080/07421222.2018.1440766

[14] A. Hanelt, R. Bohnsack, D. Marz, and C. Antunes Marante, “A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change,” *Journal of Management Studies*, vol. 58, no. 5, pp. 1159–1197, 2021. https://doi.org/10.1111/joms.12639

[15] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, “Smart airport cybersecurity: Threat mitigation and cyber resilience controls,” *Sensors,* vol. 19, no. 1, p. 19, 2018. https://doi.org/10.3390/s19010019

[16] M. Saraiva and N. Coelho, “CyberSoc implementation plan,” in *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, Istanbul, Turkey, 2022, pp. 1–6. https://doi.org/10.1109/ISDFS55398.2022.9800819

[17] N. Sun *et al.*, “Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives,” in *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1748–1774, thirdquarter 2023. https://doi.org/10.1109/COMST.2023.3273282

[18] D. Moher *et al.*, “Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement,” *PLoS Medicine*, vol. 6, no. 7, p. 1000097, 2009. https://doi.org/10.1371/journal.pmed.1000097

[19] I. Mustapha, N. Khan, and M. I. Qureshi, "Is technology affecting the way our minds operate? Digital psychology of users in the era of digitalization," *Advanced Structured Materials*, vol. 174, pp. 71–92, 2022. https://doi.org/10.1007/978-3-031-01488-8_8

[20] B. Buyamin *et al.*, "The influence of war and global economy on article publication (Bibliometric Analysis using Biblioshiny-R)," 2023. https://doi.org/10.21203/rs.3.rs-2680363/v1

[21] N. Akhtar, N. Khan, S. Qayyum, M. I. Qureshi, and S. S. Hishan, "Efficacy and pitfalls of digital technologies in healthcare services: A systematic review of two decades," *Frontiers in Public Health*, vol. 10, 2022. https://doi.org/10.3389/fpubh.2022.869793

[22] H. Sikandar, Y. Vaicondam, N. Khan, M. I. Qureshi, and A. Ullah, "Scientific mapping of industry 4.0 research: A bibliometric analysis," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 18, pp. 129–147, 2021. https://doi.org/10.3991/ijim.v15i18.25535

[23] D. Mhlanga, "Industry 4.0 in finance: The impact of artificial intelligence (AI) on digital financial inclusion," *International Journal of Financial Studies*, vol. 8, no. 3, p. 45, 2020. https://doi.org/10.3390/ijfs8030045

[24] S. Modgil, Y. K. Dwivedi, N. P. Rana, S. Gupta, and S. Kamble, "Has Covid-19 accelerated opportunities for digital entrepreneurship? An Indian perspective," *Technological Forecasting and Social Change*, vol. 175, p. 121415, 2022. https://doi.org/10.1016/j.techfore.2021.121415

[25] J. Fu and M. Mishra, "Fintech in the time of COVID-19: Technological adoption during crises," *Journal of Financial Intermediation*, vol. 50, p. 100945, 2022. https://doi.org/10.1016/j.jfi.2021.100945

[26] I. A. Umoren, S. S. A. Jaffary, M. Z. Shakir, K. Katzis, and H. Ahmadi, "Blockchain-based energy trading in electric-vehicle-enabled microgrids," *IEEE Consumer Electronics Magazine*, vol. 9, no. 6, pp. 66–71, 2020. https://doi.org/10.1109/MCE.2020.2988904

[27] H. Stewart and J. Jürjens, "Data security and consumer trust in FinTech innovation in Germany," *Information and Computer Security*, vol. 26, no. 1, pp. 109–128, 2018. https://doi.org/10.1108/ICS-06-2017-0039

[28] J. Liu, X. Li, and S. Wang, "What have we learnt from 10 years of fintech research? A scientometric analysis," *Technol Forecast Soc Change*, vol. 155, p. 120022, 2020. https://doi.org/10.1016/j.techfore.2020.120022

[29] A. Demirgüç-Kunt, L. Klapper, D. Singer, S. Ansar, and J. Hess, "The Global Findex database 2017: Measuring financial inclusion and opportunities to expand access to and use of financial services," *World Bank Economic Review*, vol. 34, pp. S2–S8, 2020. https://doi.org/10.1093/wber/lhz013

[30] A. W. Ng and B. K. B. Kwok, "Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator," *Journal of Financial Regulation and Compliance*, vol. 25, no. 4, pp. 422–434, 2017. https://doi.org/10.1108/JFRC-01-2017-0013

[31] S. Mehrban *et al.*, "Towards secure FinTech: A survey, taxonomy, and open research challenges," *IEEE Access*, vol. 8, pp. 23391–23406, 2020. https://doi.org/10.1109/ACCESS.2020.2970430

[32] B. Y. Qi and J. Xiao, "Fintech," *Commun ACM*, vol. 61, no. 11, pp. 65–69, 2018. https://doi.org/10.1145/3239550

[33] N. R. Mosteanu and A. Faccia, "Fintech frontiers in quantum computing, fractals, and blockchain distributed ledger: Paradigm shifts and open innovation," *Journal of Open Innovation: Technology, Market, and Complexity,* vol. 7, no. 1, p. 19, 2021. https://doi.org/10.3390/joitmc7010019

[34] S. Lee, "Evaluation of mobile application in user's perspective: Case of P2P lending apps in FinTech industry," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 2, pp. 1105–1115, 2017. https://doi.org/10.3837/tiis.2017.02.027

[35] T. Hendershott, X. Zhang, J. Leon Zhao, and Z. Zheng, "FinTech as a game changer: Overview of research frontiers," *Information Systems Research,* vol. 32, no. 1, pp. 1–17, 2021. https://doi.org/10.1287/isre.2021.0997

[36] R. J. Kauffman, K. Kim, S. Y. T. Lee, A. P. Hoang, and J. Ren, "Combining machine-based and econometrics methods for policy analytics insights," *Electronic Commerce Research and Applications*, vol. 25, pp. 115–140, 2017. https://doi.org/10.1016/j.elerap.2017.04.004

[37] L. D. Nguyen, I. Leyva-Mayorga, A. N. Lewis, and P. Popovski, "Modeling and analysis of data trading on blockchain-based market in IoT networks," *IEEE Internet Things Journal*, vol. 8, no. 8, pp. 6487–6497, 2021. https://doi.org/10.1109/JIOT.2021.3051923

[38] T. Y. Cho and Y. S. Chen, "The impact of financial technology on China's banking industry: An application of the metafrontier cost Malmquist productivity index," *The North American Journal of Economics and Finance*, vol. 57, p. 101414, 2021. https://doi.org/10.1016/j.najef.2021.101414

[39] J. S. Wang, "Exploring biometric identification in FinTech applications based on the modified TAM," *Financial Innovation*, vol. 7, no. 1, pp. 1–24, 2021. https://doi.org/10.1186/s40854-021-00260-2

[40] C. M. S. Ferreira, C. T. B. Garrocho, R. A. R. Oliveira, J. S. Silva, and C. F. M. da C. Cavalcanti, "IoT registration and authentication in smart city applications with blockchain," *Sensors*, vol. 21, no. 4, p. 1323, 2021. https://doi.org/10.3390/s21041323

[41] B. Li, S. D. Hanna, and K. T. Kim, "Who uses mobile payments: Fintech potential in users and non-users," *Journal of Financial Counseling and Planning*, vol. 31, no. 1, pp. 83–100, 2020. https://doi.org/10.1891/JFCP-18-00083

[42] M. H. Uddin, S. Mollah, and M. H. Ali, "Does cyber tech spending matter for bank stability?" *International Review of Financial Analysis*, vol. 72, p. 101587, 2020. https://doi.org/10.1016/j.irfa.2020.101587

[43] M. Shaheen, M. S. Farooq, T. Umer, and B. S. Kim, "Applications of federated learning; Taxonomy, challenges, and research trends," *Electronics*, vol. 11, no. 4, p. 670, 2022. https://doi.org/10.3390/electronics11040670

[44] P. J. Morgan, "Fintech and financial inclusion in Southeast Asia and India," *Asian Economic Policy Review*, vol. 17, no. 2, pp. 183–208, 2022. https://doi.org/10.1111/aepr.12379

[45] M. Maiti and U. Ghosh, "Next-generation Internet of things in fintech ecosystem," *IEEE Internet Things Journal*, vol. 10, no. 3, pp. 2104–2111, 2023. https://doi.org/10.1109/JIOT.2021.3063494

[46] M. J. Cobo, A. G. López-Herrera, E. Herrera-Viedma, and F. Herrera, "An approach for detecting, quantifying, and visualizing the evolution of a research field: A practical application to the Fuzzy Sets Theory field," *Journal of Informetrics*, vol. 5, no. 1, pp. 146–166, 2011. https://doi.org/10.1016/j.joi.2010.10.002

[47] S. Sengupta and A. Vaish, "A study on social media and higher education during the COVID-19 pandemic," *Universal Access in the Information Society*, vol. 1, pp. 1–23, 2023. https://doi.org/10.1007/s10209-023-00988-x

[48] X. Chen, Y. Lun, J. Yan, T. Hao, and H. Weng, "Discovering thematic change and evolution of utilizing social media for healthcare research," *BMC Medical Informatics and Decision Making*, vol. 19, no. 2, pp. 39–53, 2019. https://doi.org/10.1186/s12911-019-0757-4

[49] I. C. Eian, L. K. Yong, M. Y. X. Li, Y. H. Qi, and F. Z, "Cyber attacks in the era of COVID-19 and possible solution domains," *Preprints,* 2020. https://doi.org/10.20944/preprints202009.0630.v1

[50] J. B. Awotunde, E. A. Adeniyi, R. O. Ogundokun, and F. E. Ayo, "Application of big data with Fintech in financial services," in *Fintech with Artificial Intelligence, Big Data, and Blockchain. Blockchain Technologies,* P. M. S. Choi and S. H. Huang, Eds., Springer, Singapore, 2021, pp. 107–132. https://doi.org/10.1007/978-981-33-6137-9_3

[51] E. Mogaji and N. P. Nguyen, "Managers' understanding of artificial intelligence in relation to marketing financial services: Insights from a cross-country study," *International Journal of Bank Marketing*, vol. 40, no. 6, pp. 1272–1298, 2022. https://doi.org/10.1108/IJBM-09-2021-0440

[52] Y. Himeur *et al.*, "Blockchain-based recommender systems: Applications, challenges and future opportunities," *Computer Science Review*, vol. 43, p. 100439, 2022. https://doi.org/10.1016/j.cosrev.2021.100439

7 AUTHORS

Ishamuddin Mustapha, Malaysian Institute of Industrial Technology (MITEC), Universiti Kuala Lumpur, Kuala Lumpur, Malaysia (E-mail: Ishamuddin@unikl.edu.my).

Yamounah Vaicondam, School of Accounting & Finance, Faculty of Business and Law, Taylor's University, Subang Jaya, 47500, Selangor, Malaysia; Digital Economy and Business Transformation Impact Lab, Taylor's University, Subang Jaya, 47500, Selangor, Malaysia.

Agha Jahanzeb, Department of Business Administration, Sukkur IBA University, Pakistan (E-mail: agha.jahanzeb@iba-suk.edu.pk).

Burkhanov Aktam Usmanovich, Dean of the Faculty of Finance and Accounting, DSc in Economics, Professor. Tashkent State University of Economics, Tashkent, Uzbekistan (E-mail: a.burkhanov@tsue.uz; ORCID: 0000-0003-0108-8852).

Siti Hawa Binti Yusof, School of Accounting & Finance, Faculty of Business and Law, Taylor's University, Subang Jaya, 47500, Selangor, Malaysia.