ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 16 (2026) No. 1, pp. 18-36
DOI:10.33168/JSMS.2026.0102

Cybersecurity Challenges in E-finance and Their Impact on Consumer Trust

Sushila Raut[1], Dipendra Karki[2*]

[1]Research Scholar, Nepal Commerce Campus, Faculty of Management, Tribhuvan University, Nepal

[2]Assistant Professor, Faculty of Management, Nepal Commerce Campus, Tribhuvan University, Nepal

susilaraut99@gmail.com, dipendra.karki@ncc.tu.edu.np (Corresponding author)

Abstract. The financial technology industry has experienced a complete transformation because people and businesses now depend on digital financial services. The development creates new security challenges since it enables phishing attacks, ransomware, data breaches and identity theft to jeopardize consumer trust and financial security. This research aims to study how cybersecurity risks affect consumer trust in e-finance by examining the primary factors and their effects on consumer behavior and security measures. The study examines research patterns and collaborative networks through bibliometric analysis of peer-reviewed articles published during the time period from 2020 to 2024 using the R programming package for citation analysis, co-citation mapping and keyword frequency analysis. The research results show that "Cybersecurity" is the most commonly used term and "China" is the most frequently mentioned country, which demonstrates the requirement for complete cybersecurity solutions that combine technical defenses with legal protections and public education programs to enhance financial technology security. The research provides essential insights to financial institutions and governments, and technology providers who want to create security systems that protect against risks while enabling financial innovation through their plans to build secure electronic financial networks.

Keywords: Blockchain, Cybersecurity, Digitalization, E-finance

1. Introduction

The agile digital revolution has created electronic finance as a new economic conflict, which transforms how people and businesses manage their financial activities. E-finance provides digital banking services together with digital wallet solutions, investment platforms and other technology-based financial services to deliver exceptional customer convenience and operational efficiency. The field has experienced developments, which now face two challenges because cybersecurity problems have increased security threats. The combination of financial technology and cybersecurity creates obstacles which directly reduce customer confidence that businesses need to operate successfully in the e-finance sector. Financial institutions now understand that cybersecurity functions as an essential element of corporate governance while serving as a technical security matter because it protects both stakeholder trust and market stability (Issayeva et al., 2023).

E-finance security faces cybersecurity threats, which include phishing attacks, ransomware, identity theft, data breaches and advanced persistent attacks that endanger financial organizations and put personal and financial information at risk for millions of consumers worldwide. Reports from organizations such as the World Economic Forum (2023) and the Financial Stability Board (2022) indicate a consistent rise in cyberattacks targeting financial sectors, highlighting the vulnerabilities of even the most complex systems.

E-finance shows customers financial services through online platforms, which use electronic communication and computing systems. This concept has changed the concept of traditional finance by providing more accessible, efficient and convenient interactions between businesses, financial institutions and consumers. Digital technology improvements, which include mobile banking applications, online payment systems and blockchain technology, have caused people to change their financial practices about saving and investing, borrowing and paying (Ghimire et al., 2022; Karki et al., 2024). These innovations have reduced the need for physical branches, allowing financial services to be accessible to users from anywhere with an internet connection. The scope of e-finance extends across various domains such as online banking, e-trading, crowdfunding, and digital wallets. By highlighting financial processes, it enhances user experience while minimizing operational costs for organizations. E-finance also promotes financial inclusion by providing access to banking services for underserved populations in remote or underdeveloped areas. But with these several benefits come the challenges and risks, such as the misuse of the information in cyberspace, a rise in cybercrime and other cyber frauds. In this century, cybercrime has become one of the retaliation tools anyone can employ to threaten or defraud someone. According to the most recent statistics from January 2021, it was found that approximately 5 billion active internet users exist, which has increased the likelihood that a user will fall victim to this type of crime and frauds which has been on the rise for a few decades (George & Nagadeepa, 2023)

Cybercrime in electronic finance is increasing in today's world, making it a big matter of concern with the rise of the internet and digital banking. Cybercriminals have been developing advanced measures for achieving ways to gain access to financial data and accounts, resulting in fraud, theft and other financial losses. Since e-finance has become an indispensable part of everyday life, offering convenience and accessibility in managing financial transactions. The quick growth of electronic finance systems has created substantial security problems which need to be investigated. The security problems which affect sensitive consumer information include data breaches and phishing attacks, combined with identity theft and security weaknesses in financial systems. E-finance platforms experience increasing cyberattacks, which use advanced attack techniques to disrupt their operations, thus causing financial institutions to lose customer trust and endangering the viability of their digital payment systems. The research aims to identify fundamental reasons behind security problems which affect customer confidence while suggesting better security solutions for the online financial transaction system. The research will examine how cybercrimes affect e-financial operations while

assessing existing cybersecurity threats and determining the effectiveness of security measures in decreasing cybercrime and cyberattack risks.

The existing body of research explores the technical aspects of cybersecurity for e-finance systems, yet fails to investigate how these challenges affect consumer trust. The existing research primarily concentrates on establishing and improving security solutions, which include encryption systems, firewall technology and mechanisms for detecting intrusions and verifying user identities. Cybersecurity solutions provide essential protection against online threats, but they only address one part of the problem. The human factor remains hidden because people tend to disregard how cybersecurity risks affect consumer behavior and their trust level determines whether they will keep using e-finance services. The financial sector faces an immediate need to study cyberattack methods, which have become more advanced and frequent since hackers now use phishing attacks, ransomware and data breaches to target its platforms. Emerging security threats which include AI-based phishing attacks and supply chain disruptions require organizations to implement security systems that can evolve and predict future threats (Talib, 2025). Research has extensively focused on financial losses and reputational damage, yet the psychological effects on consumers remain unstudied because it includes their fear of fraud and their reluctance to use new technologies, and they lose trust in digital financial systems. Businesses need to understand these elements because consumer trust serves as the fundamental factor which determines whether e-finance services will succeed or fail (Dahal et al, 2025; Joshi et al., 2024).

Dandapani (2017) found that there is a lack of interdisciplinary research that integrates insights from cybersecurity, consumer behavior, and financial technology (fintech). Cybersecurity researchers focus on technical solutions while consumer trust studies examine social and psychological aspects without connecting them to specific cyber threat challenges. The organization of research into separate areas prevents researchers from creating complete methods that will protect financial systems and preserve consumer trust.

The study of how regulatory systems interact with company practices to shape consumer trust in electronic financial systems remains incomplete. The present study does not demonstrate how European data protection regulations, such as GDPR and international data protection laws, affect consumer safety and trustworthiness of products. Financial institutions need to improve their methods for sharing security information with customers because they need to build trust after cyberattacks. The problem becomes more difficult because e-finance technologies keep advancing through their development of mobile banking applications, blockchain solutions and AI-based financial tools. The new technologies create fresh opportunities, yet they produce distinct security threats through their decentralized systems and machine-learning algorithms. The existing studies do not study the way emerging technologies affect cybersecurity and consumer trust, which creates a significant research gap for investigators to address. The proposed research aims to develop a complete framework which shows the effects of cybersecurity issues on consumer trust and behavior in electronic financial systems. The information enables organizations to create security measures which protect their digital financial systems from attacks while enhancing system reliability and performance.

The research was conducted because consumer trust directly impacts the success of e-finance platforms. E-finance represents a fast-growing field which can improve financial accessibility and drive economic development. The complete advantages of the system remain inaccessible until proper cybersecurity solutions are implemented. Our research interests came from our personal technology, finance and consumer psychology interests, which we want to use for building trustworthy financial systems. We selected this research project because it examines a model digital economy study which includes multiple academic disciplines and shows our personal and professional growth that will benefit society and influence public policy development.

The electronic financial system has become a vital component of economic growth that drives economic progress in the current digital economy. The system enables users to make payments without any difficulties while it expands access to financial services and boosts operational performance throughout all financial institutions. Users need to establish a sense of protection because only then will they start to use the platform. The number of major cyberattacks, which include data breaches and fraud incidents that target financial services organizations has reached dangerous levels. The research exists to create more secure e-finance systems which build user trust to achieve digital economy success and sustainable development. The field of study which examines how technology connects with finance and human behavior creates special research opportunities.

People typically view cybersecurity as a technical issue, but it extends its effects to consumer behavior and, regulatory requirements and business activities. The study seeks to explore an interdisciplinary domain which unites cybersecurity research with studies of consumer behavior and financial technology research. The research provides complete solutions to stakeholders by analyzing all relevant components of the research problem. The researcher studies how digital finance affects economic systems through its power to generate fresh business opportunities. The researcher shows intense concern about cyber threats, which he believes can undo all progress made to this point. The researcher sees e-finance as highly promising, but he needs to find secure methods which will protect its security gaps until sustainable solutions bring forth technological progress. The research studies two separate aspects, which include the social impact of cybersecurity problems and the specific challenges which e-finance systems deal with. For many individuals, especially those from developing areas, e-finance serves as their initial experience with official banking services. The security issues which undermine trustworthiness create increased financial access challenges for these communities. The changing security threats create a regulatory problem because they force policymakers to develop effective solutions for consumer protection. The research develops effective solutions which will enable policymakers, together with financial institutions and technology companies, to design secure digital financial systems that accommodate all users.

The research study investigates cybersecurity issues which affect electronic financial systems and their impact on customer trust. The research study seeks to identify e-finance platforms which face their most severe cybersecurity risks, which lead to consumer trust problems, while studying how these risks affect user behavior and assessing existing security systems which protect customer data.

The research examines how e-finance cybersecurity threats impact consumer trust, which has become essential to the modern digital economy. The study investigates how cyber threats impact consumer behavior because it provides financial institutions, technology companies, and policymakers with the necessary information to develop secure and trustworthy systems. The research results improve financial inclusion because they show ways to establish consumer trust in e-finance platforms for areas that lack access to financial services. The research connects technical solutions with consumer-focused methods to create an all-inclusive view, which enables digital financial services to develop sustainably. The system protects the vital trust required for people to embrace and use electronic financial systems throughout the global interconnected environment.

The article maintains an organizational structure which consists of four essential components. The first part consists of the background of the study, including the introduction of the topic, the significance and the objective of the study. The second part shall be a literature review, which explains the review of the literature methodology on which the article shall be prepared or based. The study presents its third section, through which it shows its research findings and results, which researchers explain. The final section presents both the study summary and its recommendations for upcoming research work.

2. Literature Review

Cybersecurity protects electronic financial operations from current cyber threats, which affect today's digital economy and worldwide financial system. Protection of confidential data and financial operations from online banking and digital financing, cryptocurrency and various financial platforms needs to be established. Cyberattacks, which include phishing, ransomware and data breaches, present major security threats that result in financial damages, identity theft and decreased trust from customers. Financial data protection and system security require strong cybersecurity measures, which include encryption, multi-factor authentication, and real-time monitoring. The digital ecosystem continues to grow, so organizations need to make cybersecurity their top priority because it protects electronic financing operations and maintains financial stability, and builds customer trust (Khadka et al., 2024; Sharma et al., 2023).

Asmar and Tuqan (2024) studied the importance of cybersecurity in digital banking, where the study emphasizes the critical need for effective cybersecurity measures in digital banks due to the rapid technological advancements and the increasing prevalence of cyber threats targeting financial institutions. The research demonstrates how security systems can use machine learning methods, which include support vector machines (SVM), recurrent neural networks (RNN), hidden Markov models (HMM), and local outlier factor (LDF) to identify and stop digital banking cybersecurity threats. The deep learning models which include convolutional neural networks and transformers demonstrate better capabilities to identify advanced fraud patterns together with detecting unusual transactions that occur in real-time (Chen et al., 2025; Zhang et al., 2024).

George and Nagadeepa (2023) studied the Rising Impacts of Cybercrimes in Electronic Financing. They stated that cybercrimes are complicated, and it is particularly challenging to find solutions. However, when cybercrime rates rise, they may be detrimental to enterprises and national economies. Therefore, it is essential that steps be taken to solve the issue. In order to assess the impact of cybercrime on discouraging the use of e-banking in the financial sector, the study aims to offer a research model.

Laurent and Sinz (2019), in their article, performed binary logistic regression, which helped them find out that only perceived usefulness and device security significantly affected the respondents' payment intention. The multiple regression, intending to predict the respondents' intention to use based on the factor scores from the PCA, revealed that perceived usefulness, usability and ergonomics, device security and organizational trust were significant. Lastly, the final regression suggested that overall trust and security significantly affected the respondents' intention to use e-finance. In essence, they found that both dimensions are affecting the technological acceptance of users of mobile payment applications.

Artie and Kwok (2017), in their study finds that adopting a strategic approach that seizes opportunities associated with Fintech, the financial regulator harnesses comprehensive risk-based mechanisms to embrace exposures to cyber risks while promoting institutionalization of cybersecurity among the regulated firms with strategic controls. This study suggests a pathway for the evolution of a profession with both technical and ethical competence for mitigating the emerging risks arising from Fintech. However, such an approach is yet to be tested with respect to efficacy for the unexplored territories of fraud exposures, resulting from swift Fintech developments across borders.

The article by Pritee et al. (2024) showed how user authentication and authorization methods establish secure systems while traditional methods fail to protect personal information and digital assets from unauthorized access. The article presents machine learning and deep learning models as advanced solutions which improve user authentication and authorization systems for emerging cybersecurity applications. The research presents a complete overview of all application domains and popular datasets and their associated pre-processing techniques and algorithms, which enable Machine learning and Deep learning to function in user authentication and authorization systems. The study presents current issues in the field together with possible future research paths, which will assist

researchers and cybersecurity professionals as a valuable research resource.

The literature on cybersecurity in e-finance underscores the critical importance of protecting digital financial systems against emerging cyber risks. Research shows that cyberattacks are increasing at a fast pace, which creates a need for security systems that include encryption and multi-factor authentication and continuous monitoring. Organizations use regulatory requirements and industrial partnerships to establish security procedures that protect sensitive financial information. User education and awareness programs stand out as essential methods for decreasing human mistakes, which constitute a major security weakness (Rai & Dahal, 2024). The implementation of behavioral interventions through gamified security training and nudges leads to better user security protocol compliance, which results in decreased insider threats (Bada et al., 2019). The reviewed literature shows that organizations need to implement a complete security system which combines advanced technology, strong policy development and customer involvement to protect their electronic financial systems from constant cybersecurity threats.

The article has been based on the data collected from the period 2020 to 2024, which has brought some gaps in data analysis due to the unavailability of full data for the year 2025. Also, the data has been limited to the ones published in dimensions, which causes a miss in data from other sources.

3. Methodology

This study employs a bibliometric analysis approach to explore global trends and insights into Cybersecurity risks in electronic finance. For the study, the articles published in the dimensions shall be taken as a major force for analysis. Papers which are peer-reviewed with an emphasis on cybersecurity threats that were published during the last five years, from 2020 to 2024, shall be taken as selection criteria. The bibliometric package of R-programming software is used in the study to examine several aspects of the area and the analysis of the data gathered. While co-citation analysis looks at the connections between major studies and periodic research themes, citation analysis helps in identifying the most relevant articles and authors. The article highlights the recurring topics that emerge in relevant issues by examining keyword frequency. A visual portrayal of the relationships among authors and articles is another pro of network analysis, which provides light on the cooperative character of the relevant field of study. Thus, the dimensions database has been used in the study's bibliometric analysis.

The relevant articles were selected based on the following criteria:

- *Keywords:* ("Cybersecurity" OR "Cyberthreats" OR "data security" OR "Fraud prevention" OR "Information security") AND ("e-finance" OR "digital finance" OR "Financial Technology" OR "online banking" OR "Mobile Banking")
- *Document Type:* Peer-reviewed articles
- *Publication Period:* 2020-2024
- Open-access availability

Data generated through dimension was extracted in CSV format and analyzed using Biblioshiny (R programming package). Citation analysis identified influential authors and research trends, while network analysis visualized collaboration patterns. The result obtained through this analysis has been presented using visualizations like network maps and graphs, focusing on the evolution of research trends. The impact of key authors, and the global discourse on cybersecurity risks and evolution of electronic Finance. Ethical considerations have been adhered to by properly citing all sources of data and ensuring that the analysis is done transparently and objectively.

The detailed process, as suggested by Donthu et al. (2021), is in Figure 1.

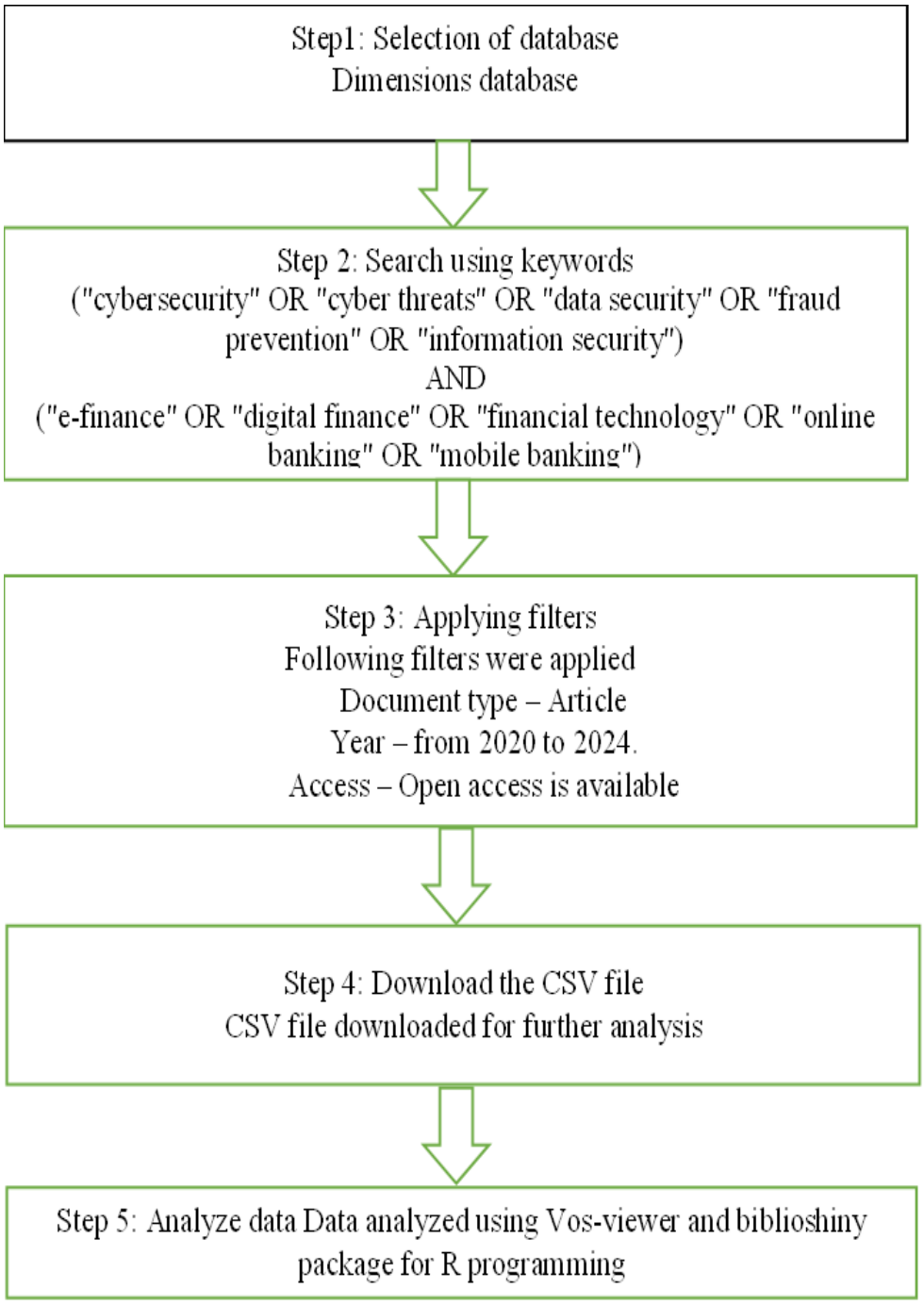


Fig. 1: Flowchart showing Bibliometric Analysis

For the analysis purpose, the data in the retrieved literature was exported to Microsoft Excel. The exported data included annual growth of publications, types of documents, languages, countries, authors, institutions, journals, citations, and funding literature. The literature was also exported to the R Studio program to create network visualizations maps.

4. Presentation and Analysis

The search query in the dimension found several results, including books, journals and articles related to cybersecurity challenges in e-finance and their impact on consumer trust. To make the result specific “article” filter was applied, and only 489 documents were taken from the years 2020 to 2024

for the purpose of the study.

Table 1. Main Information about Data

Description	Results
Main information about data	
Timespan	2020:2024
Sources (Journals, Books, etc.)	183
Documents	489
Annual growth rate %	51.56
Document average age	2.35
Average citations per doc	18.95
References	0
Document contents	
Keywords plus (id)	283
Author's keywords (de)	283
Authors	
Authors	1608
Authors of single-authored docs	66
Authors collaboration	
Single-authored docs	67
Co-Authors per Doc	3.69
International co-authorships %	23.52
Document types	
Article	489

Source: Bibliometric in R-studio programming

Table 1 provides an overview of a bibliometric analysis of research articles related to cybersecurity challenges and the impact of consumer trust in electronic financing for the period of five years. The observed growth pattern matches the international trend of increased digital finance usage and the subsequent academic research into its security effects, which recent bibliometric studies on fintech and cybersecurity have demonstrated (Jafri et al., 2025). The result showed the annual growth rate of 51.56%, indicating a declining trend in the number of articles published over the period. The average of 2.35 has been seen for the age of the document, suggesting that the dataset consists of relatively recent research. Each article receives an average of 18.95 citations, showing a strong impact, whereas a recording of no references in the dataset might indicate a limitation in the metadata extraction. Regarding authorship and collaboration, the dataset includes contributions from 1608 authors, with 66 authors producing single-authored articles. The analysis shows a strong tendency towards collaborative research and also shows that 23.52% of the articles involve international co-authorship, indicating significant global collaboration. The finding shows the production over 5 years, for which the production per year shall be shown in the bar graph in Figure 2.

Figure 2 shows the articles produced during the five years from 2020 to 2024, where the year lies on the x-axis and the number of productions in y-axis. This shows the growing trend in production over the period. The maximum production has been recorded during the year 2024, and the minimum during the year 2020.

However, the data for the year 2025 has not been included for the study purpose as it has been limited only up to the date of data collection, which has brought a very small unit of production during the year.

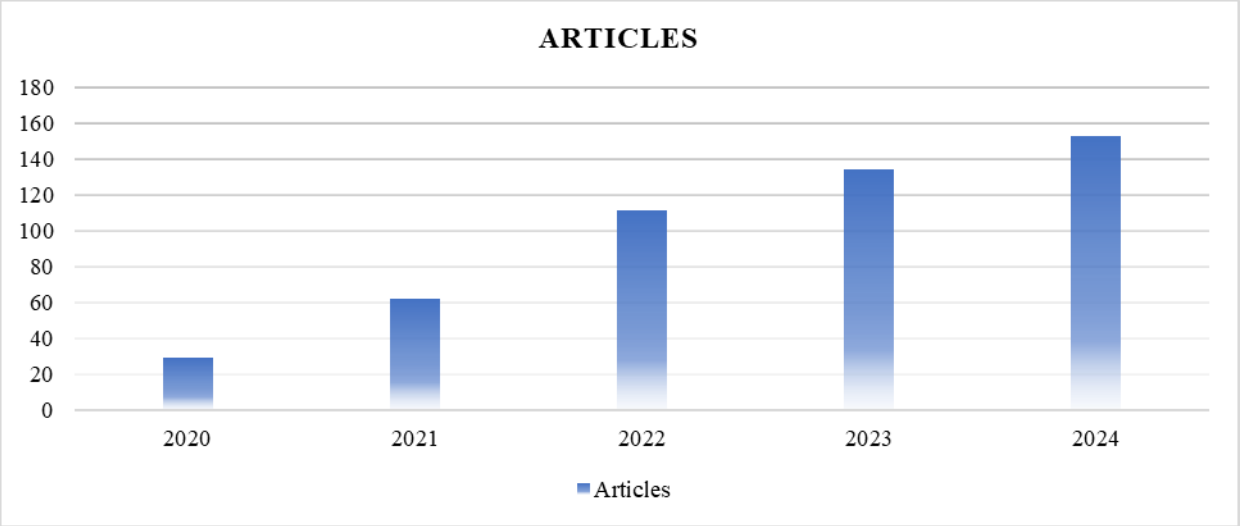


Fig. 2: Articles Production over the Year

Sources of Data

The data generated shows that 489 articles have been published during the period 2020-2024, among which 29 articles were published during the year 2020, 62 articles published during the year 2021, 111 articles during 2022, 134 articles during the year 2023, 134 articles during the year 2023, 2024 articles during 2024. The most relevant sources of these data are shown in Table 2.

Table 2. Relevant Sources of Data

Sources	Articles
Heliyon	65
Plos one	41
Sensors	33
Frontiers in psychology	18
International journal of environmental research and public health	17
Scientific reports	17
F1000research	11
Frontiers in public health	10
Peerj computer science	8
Environmental science and pollution research	7
Journal of medical internet research	7
Computational intelligence and neuroscience	6
Electronic commerce research	6
Electronic markets	6
Financial innovation	6

Source: Bibliometric in R programming

Table 2 presents the distribution of research articles across various academic journals. Heliyon leads with the highest number of publications (67), followed by PLOS ONE (42) and Sensors (34). These journals are known for their interdisciplinary focus, suggesting that the research analyzed spans multiple domains. Identifying these sources helps in understanding where the major academic discussions are taking place.

Authors Analysis

Author analysis examines the influence, productivity, and collaboration patterns of authors within cybersecurity threats and electronic finance. The method identifies essential contributions together with co-authorship relationships and citation measurement to determine an author's scholarly impact.

Most Relevant Authors

Table 3. Most Relevant Authors

Authors	**No. of documents**
Wang Y	9
Zhang Y	6
Li J	5
Li X	5
Liu J	5
Li S	4
Li Y	4
Okoye CC	4
Wang Z	4
Xu Y	4

Source: Bibliometric

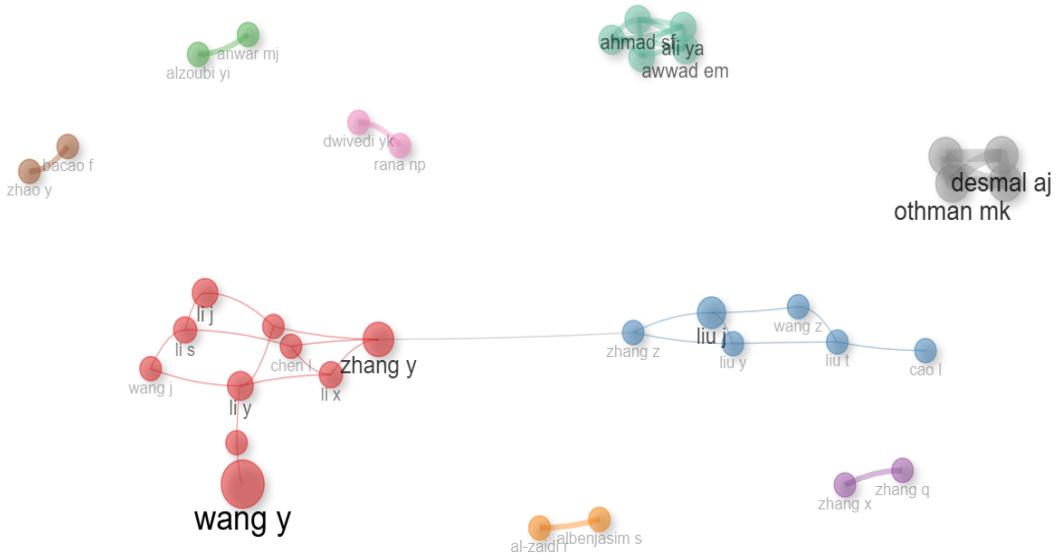
Table 3 highlights the most relevant authors in terms of research contributions in the concerned topic, measured by the number of articles published and their fractional count. Zhang X is the most prolific author, indicating significant involvement in multiple papers, followed by Wang Z and LI S as a substantial contribution. The fractionalized count provides insights into an author's weighted contributions to publications. This analysis helps to suggest an international and possibly interdisciplinary collaboration within the dataset.

Co-authorship Analysis

The co-authorship analysis can be shown in the network form, where nodes (circles) represent authors and the edges show the collaboration on research papers by them. The size of nodes suggests the significance of an author within the network, likely based on the number of publications or centrality within collaborations. (Barabás, Fülöp, & Molontay 2019).

Figure 3 shows the co-authorship network of different authors in relevance to cybersecurity risks and electronic finance-related articles. The major observations include: the diagram shows multiple clusters that represent different groups of authors collaborating within their respective networks. The larger clusters (red and then blue) show major research collaborations with the central author (wang y) developing an important role in connecting multiple co-authors. Central and peripheral Authors which means some authors have larger nodes, indicating a higher number of co-authored publications. These central figures likely have a strong effect within the research group, whereas peripheral authors with smaller nodes or fewer connections represent low coordination.

The diagram also shows some interconnected clusters (e.g. The red and blue clusters are linked by a single bridge) while others are entirely isolated, signifying independent collaboration in research.



Source: Bibliometrix

Fig. 3: Co-authorship Network

Overall, this visualisation provides insight into the structure of collaborations within the cybersecurity risks and evolution of electronic finance, highlighting key contributions and the extent of teamwork among them.

Clustering by Coupling

Clustering by coupling analysis is used to identify researchers working on similar topics by analyzing how often the citation of the same reference has been done, revealing collaboration networks and thematic research areas as this technique helps to group authors, documents or institutions based on shared citations pattern (Barabás, Fülöp, & Molontay, 2019).

Table 4 shows the list of authors with their corresponding Normalized local citation scores and cluster membership based on a bibliometric analysis. This helps to identify authors within a specific cluster of co-authorship, focusing on the effect in terms of citations and their role in the research network. The analysis identifies a tightly interconnected research cluster with LIU H emerging as the most influential author, having the highest NLC score of 22. The clustering suggests strong co-authorship ties, with all authors belonging to cluster 1, emphasizing focused research collaborations. Though the finding shows variation in citation scores, the group collectively contributes to a specialized domain, with Liu H likely leading in foundational or widely referenced work.

Table 4. Clustering by Coupling

Authors	Normalized Local Citation Score	Cluster
Dwivedi Yk	141.33	2
Raman R	105	2
Kouvonen A	72.5	2
Zhao Y	46.25	2
Liu H	22	1
Zhou Y	16	1
Li W	15.5	1
Zhang K	14.5	1
Li S	6.88	1

Liu X	4.5	1
Zhao X	3.5	1
Yang Y	3	1
Liu F	2.5	1
Zhao H	1.5	1
Wu X	1	1

This can also be seen in the network (visualization) in Figure 4.

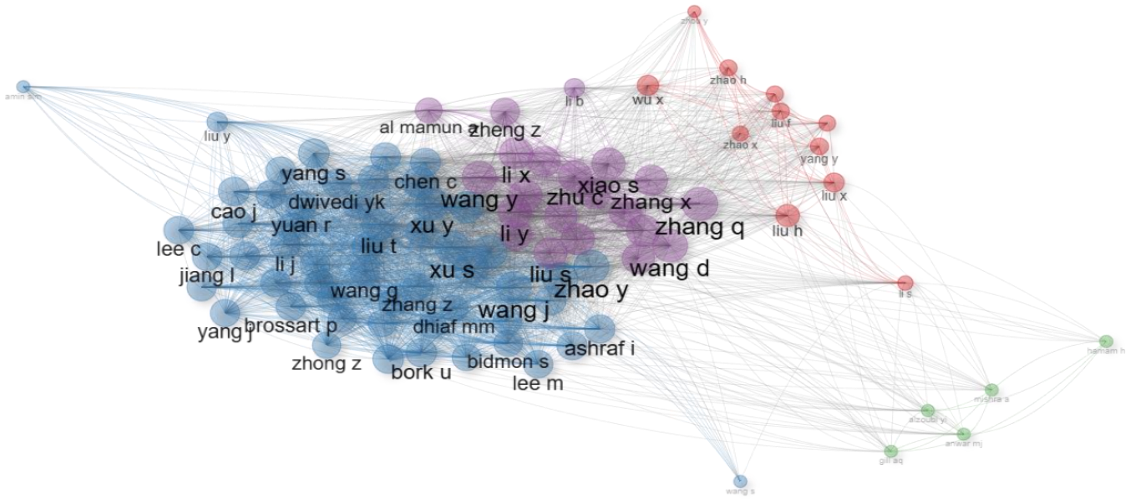


Fig. 4: Clustering by Coupling

This network visualization represents the authors as nodes and their citation relationships as edges. Larger nodes indicate authors with higher citation scores, while thicker edges represent stronger connections due to more shared references. Here, cluster 1 appears as a densely connected group (blue in the figure) where authors like Liu H, Zhou Y and Li W would have larger nodes due to their higher citation scores. WU X and Liu F, with lower citation scores, have smaller nodes and potentially fewer strong connections. The network visually depicts how closely these authors are related through shared citations, focusing on the key influencers and collaborative trends.

Citation Analysis

Citation analysis is a method used to evaluate the impact and influence of scholarly articles by examining citation patterns. It helps researchers understand the intellectual structure of a field by identifying highly cited papers, influential authors and key research trends. The most cited global articles in the related field of cybersecurity threats and the evolution of electronic finance are shown in Table 5.

Table 5. Most Global Cited Documents

Paper	DOI	Total Citations	TC per Year	Normalized TC
Allioui H, 2023, Sensors	10.3390/S23198015	215	71.67	14.42
Al-adwan AS, 2023, education and information technologies	10.1007/S10639-023-11816-3	212	70.67	14.22
Albshaier L, 2024, Computers	10.3390/computers13010027	40	20	12.78
Almogren AS, 2024, Heliyon	10.1016/j.heliyon. 2024.e31887	35	17.5	11.18

Tian W, 2024, Frontiers in psychology	10.3389/fpsyg.2024.1268549	28	14	8.94
Tay l, 2022, heliyon	10.1016/j.heliyon. 2022.e09766	194	48.5	7.69
Mahajan HB, 2022, Applied nanoscience	10.1007/s13204-021-02164-0	190	47.5	7.53
Acosta-enriquez bg, 2024, bmc psychology	10.1186/s40359-024-01764-z	21	10.5	6.71
Calderon-monge E, 2023, Review of managerial science	10.1007/s11846-023-00647-8	89	29.67	5.97
Kaihlanen A, 2022, BMC Health Services Research	10.1186/s12913-022-07584-4	142	35.5	5.63
Wang c, 2023, heliyon	10.1016/j.heliyon. 2023.e18349	83	27.67	5.57
Van kessel R, 2025, Bulletin of the world health organization	10.2471/blt.24.292057	1	1	5.5
Monlezun DJ, 2025, bulletin of the world health organization	10.2471/blt.24.291643	1	1	5.5
Oladipo jo, 2024, International journal of science and research archive	10.30574/ijsra.2024.11.1.0258	17	8.5	5.43

Source: Bibliometric in R programming

Table 5 shows the research articles that have received maximum number of global citations in the field of cybersecurity threats and evolution of electronic finance, along with the total citations, average of citations per year and the normalized total citations. Highly cited papers are influential as they provide foundational theories, empirical evidence, or widely accepted findings in the relevant topic. Here, according to the findings of my analysis, the article published in 2023 has the highest number of citations (215), consisting of an average of 21.5 citations per year and a normalized total citation of 12.2, which indicates that the paper is highly considered by researchers in the related field.

Most Cited Countries

Table 6 below shows the countries where the articles have been cited the most for study. The finding shows that the articles have mostly been cited in China, with a total of 1634, and the average article citation is 14.30. Authors and researchers from other countries such as India, Jordan, Malaysia, Saudi Arabia, Spain, the USA, France, Canada and the United Kingdom also use these data as citations for the analysis, which indicates the relevance of the study in the global network as well.

Table 6. Most Cited Countries

Country	TC	Average Article Citations
China	1634	14.3
India	1155	36.1
Jordan	423	47
Malaysia	415	20.8
Saudi Arabia	405	21.3
Spain	354	39.3
Usa	322	21.5
France	297	37.1
Canada	293	32.6

United Kingdom	265	44.2

Source: Bibliometric in R-programming

Most Relevant Affiliations

The most relevant affiliation analysis in bibliometrics showcases the institutions with the highest number of research articles in the particular dataset. The affiliation indicates the name of the university, department, or research institute, and the frequency indicates the number of articles contributed by each institution in the dataset. For the context of cybersecurity threats and the evolution of electronic finance, Table 7 has been extracted from the R Studio program.

The analysis shows that the LSE Health Department of Health policy, London School of Economics and Political Science (LSE), has the highest number of articles, which indicates a strong research presence in the dataset. The analysis shows the multidisciplinary contributions as the dataset includes institutions specializing in health policy, computer science, exercise science, psychology, and agriculture, showing a diverse range of research areas.

Table 7. Most Relevant Affiliations

Affiliation	**Articles**
Department of exercise science, university of South Carolina, Columbia, USA	11
The first affiliated hospital of Shenzhen University, Shenzhen University, Shenzhen, Guangdong, China	10
Andalusian research institute in data science and computational intelligence Dasci	9
Department of computer science and engineering, east west university, Bangladesh	9
Faculty of computer science and information technology, University Malaya, Kuala Lumpur, Malaysia	9
Academy of smart agricultural engineering innovations, Zhongkai university of agriculture and engineering, 510225, Guangzhou, China	8
Guangzhou key laboratory of agricultural product quality, safety traceability information technology, Zhongkai university of agriculture and engineering, 510225, Guangzhou, China	8
College of information science and technology, Zhongkai university of agriculture and engineering, 510225, Guangzhou, China	8
School of computer science and engineering, Hunan university of science and technology, Xiangtan 411201, China.	8
Guangdong province key laboratory of waterfowl healthy breeding, 510225, Guangzhou, China	7

Source: Bibliometric in R-programming

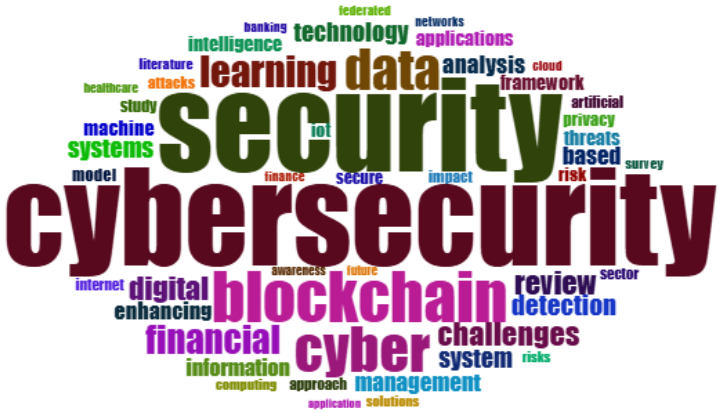
Keywords Analysis

Keywords analysis is a fundamental technique in bibliometrics used to identify the most frequently occurring terms in a set of research articles. It helps the researchers detect the trend, themes and key topics in a particular field. This helps in mapping relationships between different concepts, tracking the evolution of research topics and highlighting the major area of interest. (Verma and Gustafsson, 2020). The types of keyword analysis include: Frequency Analysis (Identifies the most used keywords in a dataset), Co-occurrence network (Visualizes how often keywords appear together, revealing topic clusters) and Thematic Mapping (Classifies keywords into quadrants to show research development). For my study on cybersecurity threats in e-finance and the impact on consumer trust in electronic finance, the most commonly used words can be shown in Table 8.

Table 8. *Most Frequent Words*

Words	Occurrences
Cybersecurity	117
Security	37
blockchain	33

Learning data	28
challenges	26
Financial	26
information	24
intention	21
management	21
Aged	18



Source: Bibliometric in R-programming

Fig. 5: Word Cloud

Co-occurrence Network

Co-occurrence network is a visualization approach used in bibliometric analysis which indicates the frequently used and highly connected terms or words found in the article related to a specific field of study.

The analysis by R-studio provides the map of co-occurrence network in the relevant field of cybersecurity threats and evolution of electronic finance.

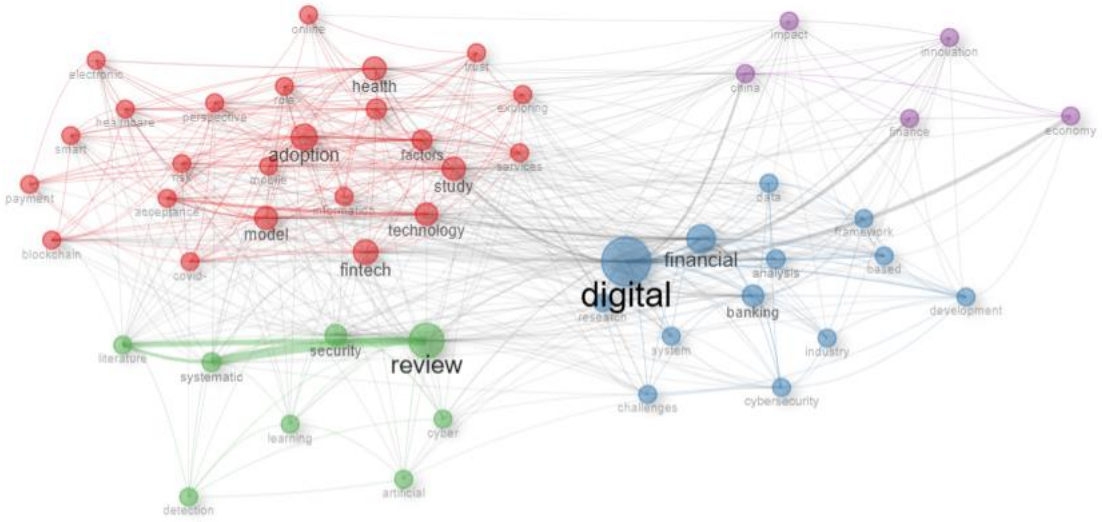


Fig. 6: Co-occurrence Network

From Figure 6 following analysis can be made on the basis of the nodes, color codes or the connections between the nodes. The term “digital” appears as the most central and largest node, which indicates its important role in the research domain, whereas other terms, such as financial, banking and review stays as secondary central terms, suggesting a focus on digital financial systems, digital banking and literature reviews.

The analysis can also be made in accordance to thematic cluster where the each color coded cluster signifies certain points: Red cluster (This suggests on how digital banking technologies, are being adopted), Green Cluster (Indicates discussions around cybersecurity, AI, and systematic learning approaches), Blue Cluster (Suggests an emphasis on digital financial services, cybersecurity and financial data analysis) Purple Cluster (Indicates a focus on the broader economic and financial implications of digital transformations).

Further, analysis can also be made on the basis of connection nodes, as a dense connection between digital, financial, and banking suggests a research focus on digital banking and financial innovations. Research shows that technology adoption establishes strong connections between digital technology acceptance and digital technology implementation. The link between security and banking demonstrates that cybersecurity functions as an essential component of financial systems. The network analysis shows that the main theme revolves around the digital transformations in financial services. The research study examines three main areas, which include financial technology adoption and cybersecurity and the economic effects which follow.

5. Discussion

The research reveals two key points which show how electronic finance systems face their main cybersecurity problems, which lead to decreased consumer confidence. The cases and complexity of cyberattacks such as phishing, ransomware, identity theft, and data breaches increased significantly, triggering enormous concerns about security during online transactions. The bibliometric analysis of five years shows that multiple cybersecurity improvement attempts, which used encryption, multi-factor authentication and live monitoring, failed to establish customer trust as the key factor which determines e-finance platform usage and maintenance.

The study presents an interdisciplinary cybersecurity assessment for electronic finance systems, which combines technological development with regulatory standards and customer identity verification systems. Financial institutions need to bridge their existing communication gap with

customers about their security control measures because they have implemented more efficient security systems (Gurung et al., 2024; Karki & Dahal, 2024). The study demonstrates that emerging technologies, including blockchain and AI-driven cybersecurity solutions, show potential but require widespread acceptance and regulatory support to succeed. For instance, Blockchain technology uses its immutable and transparent system to decrease digital transaction fraud, but organizations must overcome difficulties when they try to connect it with their existing systems (Tapscott & Tapscott, 2016; Yaga et al., 2022).

The research demonstrates how international collaboration helps reduce cybersecurity threats because the analysis of author partnerships and research citations shows an increasing pattern of international research collaboration in cybersecurity studies, which addresses the worldwide cybersecurity threat. The existing cybersecurity regulations across various regions worldwide create a regulatory imbalance which needs standardized rules to establish cybersecurity practices.

6. Conclusion

The cybersecurity threats which directly harm consumer confidence, together with their impact on financial stability, create major obstacles that prevent electronic finance from achieving its growth and sustainable development. The study findings demonstrate that organizations require a complete solution which combines security technology innovations with governmental regulations and public awareness programs to achieve effective risk management.

The digital finance revolution needs financial institutions and technology providers to create security solutions which protect both consumer interests and system weaknesses with assistance from policymakers. Cybersecurity systems need to establish consumer trust as their main goal, while they must create basic security procedures which analyze risks and teach users about electronic finance services. Future frameworks must be human-centric, which requires them to use behavioral insights for creating security systems that achieve both strong protection and easy usability (Hadlington, 2017). Future research needs to investigate how cyber risks develop over time while studying their effects on consumers and the capacity of regulatory bodies to protect secure and stable financial technology systems. The process of overcoming these challenges will both improve access to financial services and protect the sustainable future of digital financial systems throughout our interconnected world.

References

Ali, S., Islam, N., & Rauf, B. A. (2022). Cybersecurity threats in digital financial services: Risks, challenges, and mitigation strategies. *Journal of Financial Innovation and Security*, *15*(3), 201–220.

Asmar, M., & Tuqan, A. (2024). *Integrating machine learning for sustaining cybersecurity in digital banks*. *Heliyon, 10(17),* e37571.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cybersecurity awareness campaigns: Why do they fail to change behavior? International Conference on Cyber Security for Sustainable Society, https://doi.org/10.48550/arXiv.1901.02672

Baidoo, R., & Agyekum, F. K. (2020). The role of consumer trust in the adoption of e-finance services. *International Journal of Business and Finance Studies, 8*(4), 112–128.

Barabás, B., Fülöp, O., & Molontay, R. (2019). The co-authorship network and scientific impact of László Lovász. *Journal of Combinatorial Mathematics and Combinatorial Computing, 108*, 187–192.

Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). Deep learning in financial fraud detection: Innovations, challenges, and applications. *Data Science and Management.* https://doi.org/10.1016/j.dsm.2025.08.002

Dahal, R. K., Bhattarai, G., & Karki, D. (2020). Determinants of technological and innovation performance of the Nepalese cellular telecommunications industry from the customers' perspective. *Advances in Science, Technology and Engineering Systems Journal, 5*(6), 1013–1020. http://dx.doi.org/10.25046/aj0506122

Dahal, R. K., Sharma, B. B., Ghimire, B., Karki, D., & Joshi, S. P. (2025). An Informatics-Based Analysis of Consumer Trust, Website Design, and E-Commerce Logistics in Nepal. *Journal of Logistics, Informatics and Service Science, 12*(8), 40–57. https://doi.org/10.33168/JLISS.2025.0803

Dandapani, K. (2017). Electronic finance–recent developments. *Managerial Finance*, *43*(5), 614–626.

Donthu, N., Kumar, S., Pandey, N., & *Soni, G.* (2020). A retrospective overview of Asia Pacific Journal of Marketing and Logistics using a bibliometric analysis. *Asia Pacific Journal of Marketing and Logistics, 33*(3), 783–806. https://doi.org/10.1108/APJML-04-2020-0216

Gartner, M., & Smith, R. J. (2021). The interplay of cybersecurity and consumer trust: Implications for financial institutions. *Journal of Cybersecurity Policy and Management*, *9*(2), 145–168.

George, S., & Nagadeepa, C. (2023). A study on the rising impacts of cybercrimes in electronic financing. *Role of Management and Business Practices for Sustainable Development*, 63.

Ghimire, B., Rai, B., & Dahal, R. K. (2022). Understanding and adoption of Internet banking: Nepalese perspective. *KMC Research Journal, 6*(6), 13–31. https://doi.org/10.3126/kmcrj.v6i6.59368

Gurung, R., Dahal, R. K., Ghimire, B., & Dahal, P. (2024). Non-performing assets and bank profitability in Nepal: Evidence from a panel data. *Journal of Logistics, Informatics and Service Science, 11*(3), 384–398. http://dx.doi.org/10.33168/JLISS.2024.0325

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. http://dx.doi.org/10.1016/j.heliyon.2017.e00346

Issayeva, G. K., Zhussipora, E. E., Aitymbetova, A. N., Kuralbayeva, A. S., & Abdykulova, D. B. (2023). The impact of cybersecurity breaches on firm's market value: The case of the USA. *Economy: Strategy and Practice, 18*(4), 200–219. https://doi.org/10.51176/1997-9967-2023-4-200-219

Jafri, J. A., Mohd Amin, S. I., & Abdul Rahman, A. H. (2025). Financial technology (Fintech) research trend: a bibliometric analysis. *Discover Sustainability 6*(1). https://doi.org/10.1007/s43621-025-01225-6

Joshi, S. P., Dahal, R. K., Karki, D., & Ghimire, B. (2024). Consumer behavior and decision-making in health insurance policy purchases in Nepal. *Nepalese Journal of Insurance and Social Security, 7*(1) 100–116. https://doi.org/10.58665/njiss.66

Karki, D., & Dahal, R. K. (2024). Service quality dimensions and investor satisfaction on online stock trading system in Nepal. *Journal of Service, Innovation and Sustainable Development, 5*(1), 63–81. http://dx.doi.org/10.33168/SISD.2024.0106

Karki, D., Bhattarai, G., & Dahal, R. K. (2024). User acceptance determinants in m-banking adoption. *Nurture*, *18*(1), 201–213. https://doi.org/10.55951/nurture.v18i1.565

Khadka, P. B., Karki, D., Dahal, R. K., & Khanal, D. (2024). Mapping the landscape of green finance and banking performance research: A bibliometric analysis. *Journal of Service, Innovation and Sustainable Development, 5*(1), 176–193. https://doi.org/10.33168/SISD.2024.0110

Laurent, D., & Sinz, R. (2019). FinTech: The role of perceived cybersecurity and organizational trust (Dissertation). Umeå University, Faculty of Social Sciences, Umeå School of Business and Economics (USBE), Business Administration.

Murthy, D. V., & Kiran, C. (2023). Regulatory challenges in cybersecurity for e-finance: A global perspective. *Journal of Financial Regulation and Technology*, *18*(3), 310–328.

Ng, A. W. & Kwok, B. K. B. (2017). Emergence of fintech and cybersecurity in a global financial Centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance*, *25*(4) 422–434.

Pritee, Z. T., Anik, M. H., Alam, S. B., Jim, J. R., & Kabir, M. (2024). *Machine learning and deep learning for user authentication and authorization in cybersecurity: A state-of-the-art review*. *Computers & Security, 140*, 103747.

Pew Research Center. (2022). Public attitudes toward data security and privacy in the digital age.

Talib, H. A. (2025). Artificial intelligence in cybersecurity: Advancements and challenges in data protection. *Bilad Alrafidain Journal for Engineering Science and Technology*, *4*(2) 13–27. https://dx.doi.org/10.56990/bajest/2025.040202

Thangamuthu, M. A. CYBER SECURITY-CYBER LAW. *Cyber Security*, 40.

Rai, B., & Dahal, R. K. (2024). Social media marketing initiatives and brand loyalty. *Nepal Journal of Multidisciplinary Research*, *7*(1), 22–39. https://doi.org/10.3126/njmr.v7i1.65241

Sharma, B. B., Shahi, B. J., & Dahal, R. K. (2023). Customer loyalty and relationship marketing in the Nepalese telecommunications sector. *The Harvest*, *2*(1), 1–16. https://doi.org/10.3126/harvest.v2i1.54405

Tapscott, D. & Tapscott, A. (2016) Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World. Penguin, New York. https://www.amazon.com/Blockchain-Revolution-Technology

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2022). Blockchain technology overview. *NIST Interagency Report, 8202*, 1–67. https://doi.org/10.6028/NIST.IR.8202

Zhang, Y., Jia, G., & Fan, J. (2024). Transformer-based anomaly detection in high-frequency trading data: A time-sensitive feature extraction approach. *Annals of Applied Sciences*, *5*(1). Retrieved from https://annalsofappliedsciences.com/index.php/aas/article/view/12