REVIEW ARTICLE

ADHYAYAN Volume 13, Issue 2, 2023 Print ISSN: 2249-1066 Online ISSN: 2455-8656

Collaborative Security in Wireless Networks and Vulnerabilities Assessment for Fintech E-payment Companies: A Bibliometric Analysis

Aanchal N. Verma

Department of Management, Lucknow Public College of Professional Studies, Lucknow, Uttar Pradesh, India.

Abstract

The purpose behind the technical analysis and science mapping in front of researchers to make them aware of the Internet of Things and mobile networking for providing collaborated security along with a visualized presentation to the financial and engineering researchers about the virtual vulnerability assessment issues. The objectives of this study are to analyze the available review of the literature and measure the most cited Journals through citation analysis and co-authorship analysis. The approach of BA (Bibliometric Analysis) has been executed in order to visualize literature reviews systematically. The researcher performed an in-depth study with reference to Collaborative Security and wireless networks (582), Collaborative Security and vulnerability assessment (253) and WiFi Security and Vulnerability Assessment (34) studies are available. The figures have been made through executing data over VOSviewer and tables are formed after compiling various affiliations. This technical study will help provide a literature base for more research to be executed in the arena of Information Systems (IS), Engineering, Computer Sciences, and Financial Technology. Also, it will provide a conceptual record for those practitioners and policymakers who are interested in performing exploratory research on wifi security assessment. It has been observed that more work can be done quantitatively for having certain measures regarding the virtual aspects of collaborative security amid its issues related to payment systems. Just mentioned the data are from Google Scholar and Dimensions.

Keywords: Collaborative Security, WI-FI vulnerabilities assessment, Fintech, E-payment, Bibliometric Analysis.

Adhyayan: A Journal of Management Sciences (2023); DOI: 10.21567/adhyayan.v13i2.07

Introduction

Collaborative security is an approach with the aspects of collective responsibility, the thought of global security, taking care of fundamental properties and values and providing confidence and protecting opportunities of the users doing payments through online platforms or performing marketing tasks etc. So many threats are there in the recent security mechanisms like slow reactions to new attacks; Mobile arena defects; hidden distributed attacks etc. To handle these attacks efficiently, collaborative security worked positively through coordinating nodes for executing specific powerful actions to stop attacks and also to identify vulnerabilities for protecting high sensitive core information. Surveys went for the six variants of collaborative security i.e., analytical timeliness, architecture, infrastructural network, shared information, analysis target and interoperability. Collaborative security is basically the usage of nodes to make security-related decisions. Vulnerability assessment is a process for testing that is used to identify and allocate severity levels for available defects. (Meng *et al*., 2015)

Vulnerabilities assessment can be done with the help of detecting security threats as mentioned in some literature like Leakage of Privacy (Enck 2010; Arapinis 2012; Schmidt; Barkan 2008), data tempering and

Corresponding Author: Aanchal N. Verma, Department of Management, Lucknow Public College of Professional Studies, Lucknow, Uttar Pradesh, India, e-mail: aanchalnigam.lpcps@gmail.com

How to cite this article: Verma, A.N. (2023). Collaborative Security in Wireless Networks and Vulnerabilities Assessment for Fintech E-payment Companies: A Bibliometric Analysis. Adhyayan: A Journal of Management Sciences, 13(2):42-51.

Source of support: Nil

Conflict of interest: None

increase in privilege authorization (Grace; Cho 2010; Zhou 2012), Violated Authentication, Spamming, Trap routing. (Cho and c, 2010; Jammali and Fourati, 2015)

In the words of *Amer, Barberis and Buckley (2015)* the term financial technology or 'FinTech' entered in the market to give financial services to customers at ease through technological shifting from traditional to digital payment. According to the views of *Blake and Vanham (2016)* Fintech is the use of technology considering the technological advancements to provide financial services. Fintechs is a kind of *"nimble piranhas, each focusing on a small part of a bank's business model to attack".Murad (2015)*

Research Gap

There is a gap identified regarding the associating link between collaborative security in wireless networks and vulnerability assessment in fintech E-payment companies that needs to be explored. (Of *et al.*, 2021) The available literature does not elaborate the correlated network between these two vast arenas in the field of technology. Although different patterns and wireless network safety are being discussed by several authors, still there is a scarcity of bibliometric analysis to evaluate the overall impact of Fintech (Arner *et al.*, 2020) E-payment vulnerability assessments towards wireless networks which is a crucial part of safety and security factors (Ng and Kwok, 2017; Pikkarainen *et al.*, 2004; Saksonova and Kuzmina-Merlino, 2017)

This research study focuses on the financial technology payment type sector due to its trending effect as a digital tool to satisfy, aware, and serve customers in the market available to exploit technologically integrated tools. The initiation of this paper is with the introductory section focusing on the base terms in centric i.e., Wi-Fi vulnerability assessment, Collaborative security, wireless networks and Fintech E-payment services followed by a theoretical background review of the literature. Bibliometric analysis has been performed and at last implications, limitation, future scope and conclusion is being constructed for the beneficial usage of study by the practitioners, academicians, payment companies, etc.

Theoretical Background

Collaborative security, vulnerabilities assessment and wireless networks

The typical structure of a collaborative security system includes a Monitoring Unit, Decision Unit, Collaboration Unit, and Shared Information (Rehman *et al.*, 2021; Saied, 2013). The work of the monitoring unit is to inspect the potential threats and anomalies with the help of already-mentioned norms. The next step is to send the outcome to the successor collaboration unit. (Abera *et al.*, n.d.; Laeven *et al.*, 2015; Miranda *et al.*, 2020) The abnormalities of networking or local software are being reported. The Decision Unit provides security-related decisions on the basis of observational reports to have a gist about the nodes connectivity and virus attacks. The Collaboration Unit is the main element of Collaborative security systems and helps in explaining the mechanism for communicating node signals and tech association. Shared Information in a data structure is distributed amongst the nodes and also has a watch on the data processing. So, these WNS is playing a significant role nowadays to keep payment security safe and quick. (Liu *et al.*, 2017; Pascacio *et al.*, 2021; Saied, 2013) The study was conducted in order to understand the demand of security in 5G networking in which there is a chance of vulnerability of security breaches. The eminent technologies like heterogeneous networks, massive multiple-input multiple-output and millimeter wave has been exaggerated to grasp the solutions to present challenges. As an outcome, small cell deployments and D2D connections are being provided to be explored (Yang *et al.*, 2015). The implementation of SDN (Software Defined Network) in 5G system may solve the issue of data trafficking and act as a significant element for the future gen communication networks. STRIDE methodology has been adopted for revealing the available vulnerable security threats for mobile systems. (M. Chen *et al.*, 2016) For SDN-MNs, TOPSIS (Technique for Order Preferences by Similarity to an Ideal Solution), AHP (Analytic Hierarchy Process) have been implemented for making 5G experiences better in terms of Wireless networks and collaborative security assessment. (Luo *et al.*, 2015) Wireless networks now-a-days comes along with tremendously strong vulnerable security threats, due to which its essential to provide solutions for the same in a convenient manner like signal- hiding techniques, encrypted coding, securing WAP (Wireless Access Points), network auditing, etc. (Choi *et al.*, 2008)

Discussion happened about the system-based methodologies to identify the performance-related problems in WCN (Wireless Communication Networks) (Kavitha and Sridharan, 2010). This study generated the outcomes related to the neighboring devices for access points and the modules contain several inactive elements to penetrate in the activated systems of

wireless networks (Adya *et al.*, n.d.; Cortés-leal *et al.*, 2022). Exploring about the mobile payment systems (Gupta *et al.*, 2021) and various models compared in this paper by his team to provide a solution for all security-related problems. Security standards mainly used in MPS like PCI DSS (Payment Card Industry Data Security Standard has been discussed. Comparison has been done between account-based and token-based payment systems. Symmetric key and Public Key encryptions are being discussed along with its pros and cons. Description executed regarding a novel approach that helps in verifying the corrective level of data with the help of attestment of the generation and processing of data through control-flow attestation. DIAT helps devices in autonomous collaborative networking and effective interactions, securitized networks of one device to another. They evaluated the simulated scheme in the environment to illustrate the scalability at large –scale. The design and models with approaches are being included in this research. (Abera *et al.*, n.d.) Also focus went on a systematic review regarding Collaborative Indoor Positioning Systems (CIPSs) which showed an extra edge in the usage of infrastructural architecture available for collaborative positioning amongst consumers for wireless technologies (Wi-Fi, Ultra-Wideband and Bluetooth). He also focused indoor and outdoor-based satellite navigation systems. Information shared from 84 articles ranging the period from 2006–2020 to showcase system architecture and its security issues. (Pascacio *et al.*, 2021) The process of edge caching, content retrieval, delivery updates and its benefits to the users at an extent are being discussed at a root level. Importance of placement optimization for users, service providers as well as network operators in order to take care about the safety and security of data. (Wu *et al.*, 2021) There has been a focal point of radio access networks (RANs) in the foggy situation as a commendable future-gen wireless network dimension. The cache placement problems through diverse content preferences and flexi physical layer transmission schemes and is been presented and an approximation algorithmic solution is being proposed for mobile users. (Liu *et al.*, 2017) The real-time location system at a low cost and low power for tracking and identifying assets or moving people inside any boundary of a factory or office. The network contained wall-plugged nodes with self-configured, self-healed and calibrated for the reduction of maintenance costs. (Giorgetti *et al.*, n.d.) Illustration related to various mechanisms about the fintech innovative technical pros with the help of Machine Learning. (K. Chen, 2018) The researchers discussed the IOT (Internet of Things) (Nikolov, 2018) for industrial purposes that has been in usage with exclusive connectivity as compared to old-time traditional networking systems. TSCH (Time Slotted Channel Hopping) MAC is being defined to throw an idea regarding nodal transmission. 76 schedules from different parts of the globe were analyzed on the basis of operation: Collaborative, Centralized, Hybrid, Autonomous and Static. To identify the flaws tolerance, scalability, non-converge cast traffic framework, and hybrid scheduling schema. (Urke, 2022) As a payment solution, Dandapani (2017) pointed out in his work about the development of research in electronic finance in the field of payment systems, infrastructural arena, costs, benefits and protections. Cyber security is also a matter of fact to be considered as well as trading activity of quantum.

Fintech e-payment solutions and network security

There has been several ways to prevent online fintech payment solutions from any kind of fraudulent practices. So there are many software are being available for capturing virus and creating a strong firewall for security and authentication. Cybersecurity issues and illicit finance are also been discussed and also suggested to grab information on areas like Firm Value, Corporate Governance, Security Issuance, etc. in Fintech firms. (Das, 2017) The researchers showcased outcomes based on the existing literature study through executing content and bibliometric analysis over 84 articles and concluded that the rate of cyber crimes has increased after fintech growth along with asymmetrical technology. Identified risks are operational risk, financial stability risk, default risk, financial illiteracy risk, regulatory and money laundering risks and many more. (Jain *et al.*, 2023) The main factors of choosing QR codes to make online payments quick, safe and secure. They applied UTAUT, an integrated model on the basis of 424 responses that are being analyzed using PLS-SEM technique. As an outcome, a conclusive statement come up that attitude, subjective norms and perceived usefulness together make an impact on the decision-making to use QR codes. (Chang *et al.*, 2021) Work has been done on the single-chain-based extension framework for the financial technology of Blockchain. A four-layer module has been designed to find out the way of improve in the security features of simplified verification of payment. (Moonsamy *et al.*, 2012; Qu and Michael, 2010)This framework included a financial

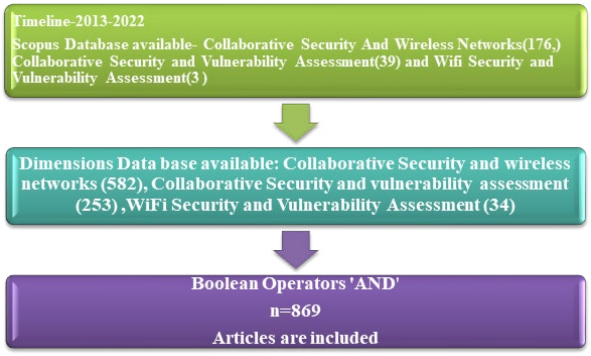
regulatory body and oracle group to provide a novel structural data extension mechanism. Experimental outcomes have shown efficiency verification for further improvement (Ji *et al.*, 2020). An evaluation of the famous eight smartphones was performed found out about the restricted permissions that are provided for taking pictures an unintentionally open themselves to various threats. A system detection tool was developed by the researcher known as Woodpecker to have check on the Android-permission-based security framework through the process of data flow analysis available in Woodpecker (Grace *et al.*, n.d.). A systematic literature review has been performed in order to understand the combined effect of Federated Learning (FL) and Edge computing combined with Deep learning and its architectural elements. (Abreha *et al.*, 2022)

Meta-data on collaborative security for WI-FI vulnerabilities assessment

- As per the reports, out of 100 there are 98 top fintech firms or startups that are sensitive or in a vulnerable condition to confront the websites and mobile app attacks despite of the fact that they are provided with ample of funds and market support as per reports.
- In the words of Immuni Web, a web security company around 100% of the payment systems have a variety of issues like problems of security, privacy and compliance which are correlated with the skipped web applications, application program interfaces (APIs) and sub-domains as per the non-intrusive checks.
- As per some bank-based research reports, out of 100 famous nationalized and private banks, 97 are being a vulnerable position for website and mobile attacks which enable hackers to steal highly sensitive data or information that are related with data security.
- There are few simple and known website vulnerabilities like XSS i.e. Cross-Site Scripting, Highly sensitive data exposure, and misconfigured security systems. Having all these problems and circumstances, they are featured in the Owasp Top 10 vulnerabilities in applications that are well-known and have well-established mitigation methods. (Meng, 2013; Schmidt *et al.*, n.d.)
- There are at least one security vulnerability with a medium risk in the mobile applications that has been tested on the other hand 97% have at least two medium or high-risk vulnerabilities. (Bolonin and Balykin, 2021; Chu, 2018; Ravikumar, 2019)
- As per few tests that have been executed resulted in giving data on about 56% of mobile applications back-end processes are having serious typical misconfigurations with some privacy policies issues related to Secure Socket Layer/Transport Security Layer configuration and ineffective web server security hardening. (Campbell-Verduyn *et al.*, 2021; Puschmann, 2017)
- As per the reports it has been revealed that around 62% of the financial technology startup's main websites has failed in the data security standard compliance test organized through the payment card industry compliance test. The major problem that has been found was outdated open source and commercial software along with its components' unsuitability for the security of a system.
- 64% of the fintechs' main websites has failed in the processing of the (GDPR) General Data Protection Regulation compliance. One of the main compliance issue came up as Vulnerable web software which has been followed by the disclaimers of the missing cookie or security flags unsetting on cookies that is used for the tracking of transfer personally identifiable information (PII) or other sensitive information and skipped inaccessible privacy policies. (Bömer and Maxin, 2018; Giorgetti *et al.*, n.d.)

Threat Transmitters

- **Exploits** have benefits for designing, coding or configuration problems that create some issues like SQL injection, cross-site scripting, Buffer overflows, (SSL) Secure Sockets Layer and (TLS) Transport Layer Security manipulation attacks.
- **Abuse** includes attacking modes in the form of non-exploit types which mainly focus on the logics of business. This performs scraping, aggregating,



Flowchart 1: PRISMA FLOWCHART: Inclusion Exclusion Criteria

account brute-forcing, scalping, spamming and other-often automated scenarios.

- **Access violations** happened due to licit exploiter who is taking the benefit of loopholes in the policies authentication procedure of the application.
- **Fake Applications** use to create fraudulent wallet applications and execute it in the form of adversaries through which users are trapped after tapping on the link unintentionally
- **Rooted Device** may be understood by an example of broken devices that can be bypassed to stealing important information.

Research Methodology

The Bibliometric analysis has been executed to find out the connection amongst three terminologies i.e. collaborative security, Wi-Fi vulnerability assessment and wireless networks. Time span was taken in between 2013-2022. With the help of Flowchart 1, the author has implemented inclusion exclusion to refine available researches. The Boolean operator is used 'AND' to find out a connection between all three terms. The papers are searched in the following ways: a) 'Collaborative Security' AND 'Wireless Networks'; b) 'Collaborative Security' AND 'Vulnerability Assessment'; c) 'Wifi Security' AND 'Vulnerability Assessment'. There are 253 papers in (a), 582 papers in (b) and 34 papers in (c) extracted from Dimensions. Other than these many more are available on Google Scholar and as far as the renowned database of Scopus is concerned, the numbers are 176, 39, and 3 respectively. However, after extracting duplicate papers, only few papers were taken into consideration for bibliometrical analysis and further evaluation. Author's country affiliations, co-authorship analysis, co-occurrence analysis and citation analysis are performed in this study. Furthermore, the researchers suggest implementing other analyses in future studies. For studying a), co-authorship analysis, co-occurrence analysis, and bibliographic coupling of sources and countries were also performed. For b) and c) only co-authorship analysis and co-occurrence map are being created. The rest may be evaluated in future studies. Also, the paper has compiled meta-data with the help of certain reports and data available online, in white papers, types of virus for security breaches in fintech e-payment platforms and threat transmitters causing fintech vulnerability.

Bibliometric Analysis

There has been an immense work done by researchers in the field of collaborative wireless security and vulnerability assessment. (Amoozadeh *et al.*, 2015; Barroso and Laborda, 2022; Sahi *et al.*, 2022) The relevant databases available in literature form were evaluated and analyzed with the help of Bibliometric or Bibliographic analysis. The main goal behind using this approach was to perform an in-depth study of the recent security for wireless networking for mobile networks. (Choi *et al.*, 2008; Luo *et al.*, 2015; Nazir *et al.*, 2021) The data has been extracted from the Dimensions and renowned publications of Scopus in all three terminologies of collaborative security, wireless networks and vulnerability assessment in fintech companies for online payments systems. The research has been increased as per the timeline goes further.

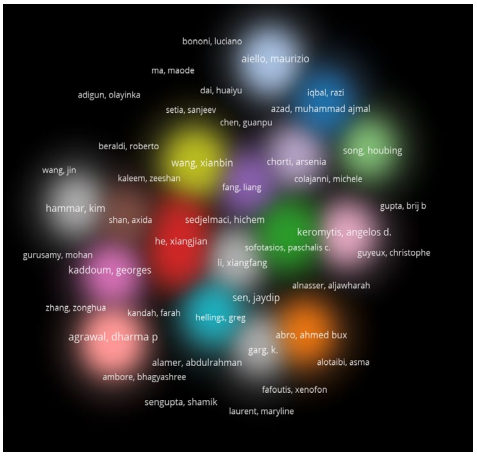
'Collaborative Security' AND 'Wireless Networks'

Co-Authorship Analysis

There has been co-authorship analysis executed for the first searched document i.e., Collaborative Security AND (Boolean operator) Wireless Networks. In Figure 1, total of 176 documents are being extracted from the Scopus and 582 papers are available on the Dimensions. The full counting method undertaken and the analysis unit are the authors. 54 Clusters with 141 links and the total link strength is 294. Authors like Keromytis, Angelos; and Dharma Agrawal are few of all those who worked on this burning topic.

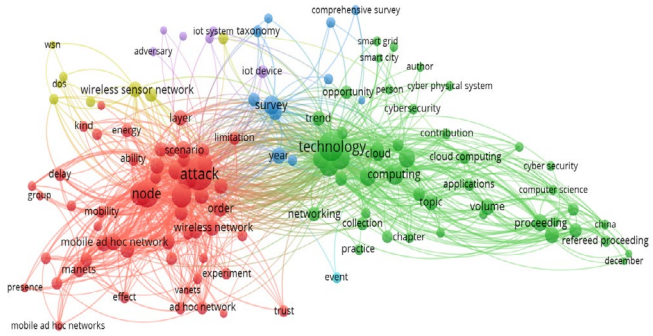
Co-occurrence Analysis

In Figure 2, out of 9054 terms, 228 meet the threshold but 60% of the relevant are being selected, so it's 137 n number. 6 clusters and 4988 clinks with total link strength of 15203 amongst the terms. Cluster 1 (Red)



Source: VOSviewer output

Figure 1: Co-Authorship Analysis through Density Visualization



Source: VOSviewer Output

Figure 2: Co-Occurrence Analysis for title and abstract fields from the Dimensions

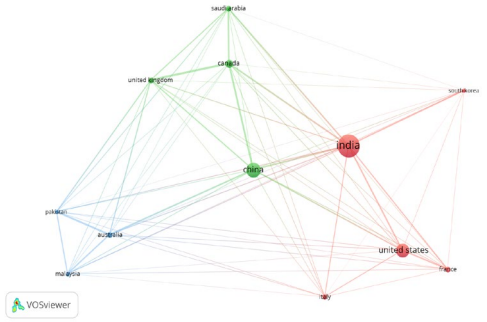


Figure 3: Bibliographic coupling (countries)

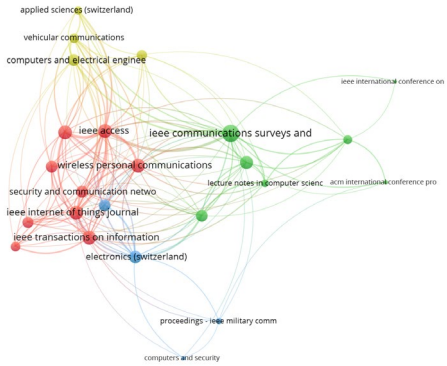


Figure 4: Bibliographic coupling (sources)

with 55 items named security and networking, and Cluster 2 (Green) with 47 items named innovation and communication. Cluster 3 (Blue) 11 items named cyber insights. Cluster 4 (Yellow) with 8 items known as wireless network. Cluster 5 (Purple) 6 items named IOT framework. Cluster 6 (Sky blue) only 1 item so not named specifically.

Bibliographic Coupling (Countries)

On the Scopus database, which is considered to be the most renowned knowledge base in the arena of global research the bibliographic coupling performed. In Figure 3, with a total of 176 documents in this domain, 12 items with 3 clusters formation, 66 links and total link strength goes to 4986 assuring the strong database stage. Cluster 1 (Red- 5 items) is highest in India followed by Cluster 2 (Green- 4 items) China and Cluster 3 (Blue- 3 items) in Australia.

Bibliographic Coupling (Sources)

In Figure 4, with a total 176 documents, 24 items are considered with 4 clusters having 150 links and 696 total link strength. Bold and big size circles have shown the main sources, i.e. IEEE access; IEEE communication surveys, and wireless personal communication tutorials.

'Collaborative Security' AND 'Vulnerability Assessment'

Co-authorship Analysis

There are 285 papers available from the Dimensions and 39 from the Scopus. Co-authorship analysis has been executed on the ris. format of the Dimensions papers. In Figure 5, out of 522 authors, 91 meet the threshold with 29 clusters, 143 links and 285 total link strength. Liu, yang having 16 total link strength; Joosen, Wouter with 14 total link strength and Korczynski, Maciej with 14 total link strength are required to mention as per diagrammatic representation.

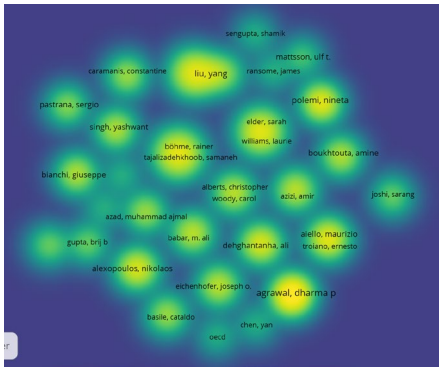
Co-Occurrence (Keyword Analysis)

In Figure 6, based on 39 papers from the renowned Scopus, 71 items with 6 clusters 440 links and 628 total link strength. Cluster 1 (Red- 18 items) was named as collaboration and vulnerability; Cluster 2 (Green- 14 items) was denoted to intrusion; Cluster 3 (Yellow- 12 items) was named as cyber threats and security; Cluster 4 (dark Blue-12 items) Artificial Intelligence Reviews; Cluster 5 (Blue- 9 items) known as operational network and lastly Cluster 6 (Purple- 6 items) named as Internet of Things security.

'WiFi Security' AND 'Vulnerability Assessment'

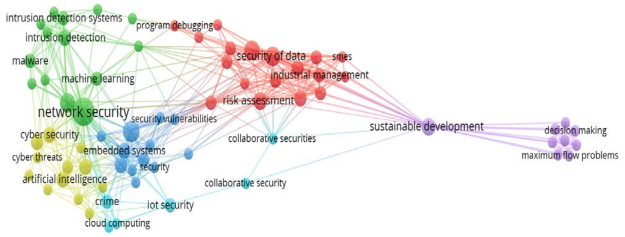
Co-Authorship Analysis

There are 34 papers available on Dimensions and only 3 on Scopus database have these terminologies. In Figure 7, out of 52 authors, 29 meet the threshold with at least 1 citation at a minimum level. 13 clusters formed with 32 links and density visualization is going to be represented. Authors named Gauravaram, and Bhattacharya have maximum link strength.



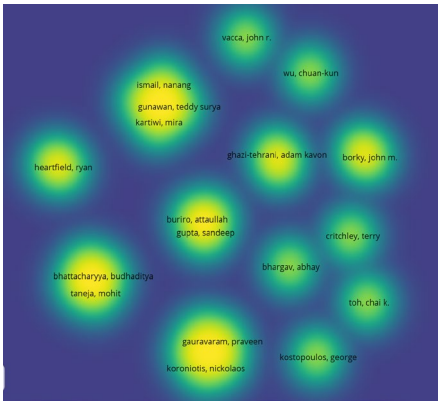
(Source: VOSviewer Output)

Figure 5: Co-Authorship analysis through density visualization



(Source: VOSviewer Output**)**

Figure 6: Co-occurence analysis through network visualization



Source: (VOSviewer Output)

Figure 7: Co-authorship analysis through density visualization

Co-Occurrence (Keyword Analysis)

The co-occurrence analysis has been executed for title and abstract fields with binary counting method. In Figure 8, out of 997 terms, 44 meet the threshold on a minimum occurrence of 3 for a particular term. 3 clusters with 763 links and 1561 total link strength has been received as an output. Cluster 1 with 19 items has been identified as 'Networking'; Cluster 2 with 14 items named as 'Cybersecurity' and Cluster 3 with 11 items named after 'Artificial Intelligence'.

Limitations of the Study

The current study tried to present a clearer picture of the Wi-fi vulnerabilities assessment and collaborative security but still, there are few loopholes that need to be taken care of in future research. For database creation, the Mendeley software has been used for create references from Scopus, Dimensions, etc. Certain restrictions are being implemented while searching the research studies and white papers and then the quality data are extracted from WoS, Google Scholar, Science Direct also.

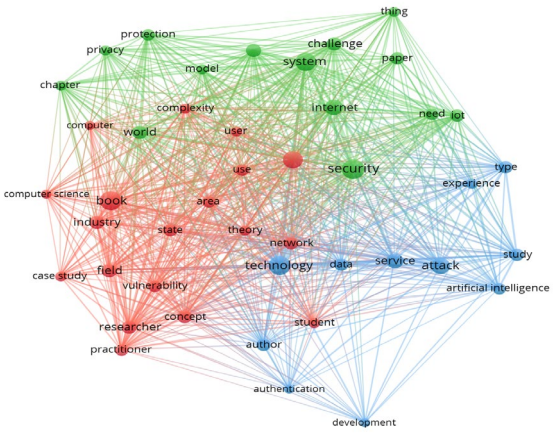
There is another constraint regarding the terminologies that need to be searched for this research. A vast study can be performed with topics like cybersecurity and vulnerability assessment and can be added on with digitalization, artificial intelligence, fintech innovation, strategic modeling, and many more conceptual frameworks for more conclusive and exclusive studies.

There are certain setbacks related to the extraction procedure executed for bibliometric analysis Bibliographic coupling may also be included as a structured graph for journals along with the other data presented. Furthermore, more analytical tools like Biblioshiny, BibExcel, etc. could be selected for processing future research studies.

Implications of the Study

This study focuses on correlating the bond between collaborative security and vulnerability assessment that is associated with the fintech E-payment companies with the help of a bibliographic aspect. The base of the study gets more stronger as the researchers try to compile the current reports available on various websites, Government white papers etc. Also, types of viruses and payment applications are being detailed in order to help the practitioners and companies as well as the academicians.

The policy-makers will benefit along with the Government as financial technology is creating new benchmarks in the world of online payment arena. This study may be implemented in under-developed economies after gathering outcomes of the analysis.



Source: (VOSviewer Output)

Figure 8: Co-occurrence (Keyword Analysis) through network visualization

There has been an ample shift of technological advancement due to COVID-19 in the banking and payment sectors. The practical implications for dynamic fintech wireless networking will transform businesses.

Conclusion and Future Scope of Study

Several literature reviews presented the views of authors regarding collaborative security which plays a significant role in providing safety and security to online users. The science mapping is presented in order to showcase a clear picture of research works performed on hot topics like security-defined networks (SDNs), wireless sensor networks (WSNs), and its impact on payment applications. There has been an increase in research development that has been found with the help of bibliometric performance and network analysis (BPNA). More than 90000 work data is available on Dimensions and Google Scholar itself. Vulnerability issues of the software applications may be solved with the collaborative security in wireless networks and the adoption of a secure software development life cycle (SSDLC) can help in advancements of payment to the users as well as issue solution makers. There are ample opportunities that have been created by online platforms for customers in order to attract them to make online payments or fund transfers without any hassle or delay. Application systems, antivirus, firewalls with strong modules and anti-theft software will cure the problem but not prevent the main cause. It's high time to create such a collaborated system with the help of AI, IoT to assess the available vulnerabilities and reanalyze existing systems of payment authorization at online platforms.

Further research can be performed on the basis of analysis and various network formats and architectural advancements to utilize artificial intelligence for the betterment of payment networks in the financial technological arena. Also, some quantitative research can be performed to understand the security features for cloud-based services included in online payment/fund transfers. Also, other types of research approaches like systematic literature review, meta-analysis, scoping review, etc. could be applied for more variations in outcome.

References

Abera, T., Bahmani, R., Brasser, F., Ibrahim, A., Sadeghi, A. R., and Schunter, M. (2019. (n.d.). *February)*. Data Integrity Attestation for Resilient Collaboration of Autonomous Systems. In?NDSS.

Abreha, H. G., Hayajneh, M., and Serhani, M. A. (2022). Federated Learning in Edge Computing: A Systematic Survey. *Sensors*, *22*, 450. https://doi.org/10.3390/s22020450

Adya, A., Dunagan, J., and Wolman, A. (n.d.). *Centrifuge : Integrated Lease Management and Partitioning for Cloud Services*.

Amoozadeh, M., Raghuramu, A., Chuah, C., and Ghosal, D. (2015). *Security Vulnerabilities of Connected Vehicles Streams and their Impact on Cooperative Driving*. https://doi.org/10.1109/mcom.2015.7120028

Arapinis, M., Mancini, L., Ritter, E., Ryan, M., Golde, N., Redon, K., and Borgaonkar, R. (2012). New privacy issues in mobile telephony: Fix and verification. *Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS?12)*.

Arner, D. W., Buckley, R. P., Zetzsche, D. A., and Veidt, R. (2020). Sustainability, FinTech and Financial Inclusion. *European Business Organization Law Review*, *21*(1), 7–35. https://doi.org/10.1007/s40804-020-00183-y

Barkan, E., Biham, E., and Keller, N. (2008). *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication *. 2729*, 392–429. https://doi.org/10.1007/s00145-007-9001-y

Barroso, M., and Laborda, J. (2022). Digital transformation and the emergence of the Fintech sector : Systematic literature review. *Digital Business*, *2*(2), 100028. https://doi.org/10.1016/j.digbus.2022.100028

Bolonin, A., and Balykin, V. (2021). Payment Systems in Digital Economy. *Springer*, 97–108. https://doi.org/10.1007/978-3-030-71337-9_7

Bömer, M., and Maxin, H. (2018). Why fintechs cooperate with banks—evidence from germany. *Zeitschrift Fur Die Gesamte Versicherungswissenschaft*, *107*(4), 359–386. https://doi.org/10.1007/s12297-018-0421-6

Campbell-Verduyn, M., Rodima-Taylor, D., and Hütten, M. (2021). Technology, small states and the legitimacy of digital development: combatting de-risking through blockchain-based re-risking? *Journal of International Relations and Development*, *24*(2), 455–482. https://doi.org/10.1057/s41268-020-00198-5

Chang, V., Chen, W., Xu, Q. A., and Xiong, C. (2021). Towards the customers' intention to use QR codes in mobile payments.? *Ournal of Global Information Management (JGIM),?*, *29*(6), 1–21.

Chen, K. (2018). Financial innovation and technology firms: A smart new world with machines. *International Symposia in Economic Theory and Econometrics*, *25*, 279–292. https://doi.org/10.1108/S1571-038620180000025012

Chen, M., Qian, Y., Mao, S., Tang, W., and Yang, X. (2016). Software-Defined Mobile Networks Security. *Mobile Networks and Applications*, *January*, 729–743. https://doi.org/10.1007/s11036-015-0665-5

Cho, C. Y., and c, D. B. (2010). Eui Chul Richard Shin. In I. Proceedings (Ed.), *and Dawn Song Inference and analysis of ? formal models of botnet command and control protocols*. of the 17th ACM Conference on Computer and Communications Security (CCS?10). 426?439.

Choi, M., Robles, R. J., Hong, C., and Kim, T. (2008). *Wireless Network Security : Vulnerabilities , Threats and Countermeasures*. *3*(3), 77–86.

Chu, A. B. (2018). Mobile Technology and Financial Inclusion. *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1: Cryptocurrency, FinTech, InsurTech, and Regulation*, 131–144. https://doi.org/10.1016/B978-0-12-810441-5.00006-3

Cortés-leal, A., Del-valle-soto, C., Cardenas, C., Valdivia, L. J., and Puerto-flores, J. A. Del. (2022). *Performance Metric Analysis for a Jamming Detection Industrial Wireless Sensor Networks*.

Das, S. R. (2017). *The Future of FinTech Lumascape*. *May*.

Enck, W., Gilbert, P., Chun, B., Cox, L. P., Jung, J., McDaniel, P., and Sheth, A. N. (2010). TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones. *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation (USENIX?10)*.

Giorgetti, G., Farley, R., Chikkappa, K., Ellis, J., and Kaleas?(2012)?Cortina, T. (n.d.). collaborative indoor positioning using low-power sensor networks,? *Ournal of Location Based Services,?*, *6*(3), 137–160. https://doi.org/?10.1080/17489725.2012.690217

Grace, M., Zhou, Y., Wang, Z., Jiang, X., and Drive, O. (n.d.). *Systematic Detection of Capability Leaks in Stock Android Smartphones*.

Gupta, D., Rani, S., Ahmed, S. H., Verma, S., Ijaz, M. F., and Shafi, J. (2021). Edge Caching Based on Collaborative Filtering for Heterogeneous ICN-IoT Applications. *Sensors*, *21*, 5491. https://doi.org/10.3390/s21165491

Jain, R., Kumar, S., Sood, K., and Grima, S. (2023). *A Systematic Literature Review of the Risk Landscape in Fintech*.

Jammali, N., and Fourati, L. C. P. A. (2015, October). physiological feature based key agreement for wireless body area network. *Proceedings of the International Conference on Wireless Networks and Mobile Communications (WINCOM)*.

Ji, Y., Gu, W., Chen, F., Xiao, X., Sun, J., Liu, S., He, J., Li, Y., Zhang, K., Mei, F., and Wu, F. (2020). *SEBF : A Single-Chain based Extension Model of Blockchain for Fintech Institue of High Performance Computing and Bigdata , Nanjing University of Posts and Telecommuni-*. 4497–4505.

Kavitha, T., and Sridharan, D. (2010). *Security Vulnerabilities In Wireless Sensor Networks : A Survey*. *5*, 31–44.

Laeven, L., Levine, R., and Michalopoulos, S. (2015). Financial innovation and endogenous growth. *Journal of Financial Intermediation*, *24*(1), 1–24. https://doi.org/10.1016/j.jfi.2014.04.001

Liu, J., Bai, B., Zhang, J., and Letaief, K. B. (2017). Cache Placement in Fog-RANs: From Centralized to Distributed Algorithms. *IEEE Trans. Wirel. Commun*, *16*, 7039.

Luo, S., Dong, M., Ota, K., Wu, J., and Li, J. (2015). *A Security Assessment Mechanism for Mobile Networks*. 31843–31858. https://doi.org/10.3390/s151229887

Meng, G. (2013). *Collaborative Security : A Survey and Taxonomy*. *V*(212), 1–38.

Meng, G., Liu, Y., Zhang, J., Pokluda, A., and Boutaba, R. (2015). Collaborative security: A survey and taxonomy. ACM Comput. *Surv.*, *48*, 1. https://doi.org/http://dx.doi.org/10.1145/2785733

Miranda, C., Kaddoum, G., Bou-Harb, E., Garg, S., and Kaur, K. (2020). A Collaborative Security Framework for Software-Defined Wireless Sensor Networks. *In?IEEE Transactions on Information Forensics and Security*, *15*, 2602–2615. https://doi.org/10.1109/TIFS.2020.2973875

Moonsamy, V., Alazab, M., and Batten, L. (2012). *Towards an understanding of the impact of advertising on data leaks*. International Journal of Security and Networks.

Nazir, R., Ali, A., Shibin, K., and Munwar, D. (2021). Survey on Wireless Network Security. *Archives of Computational Methods in Engineering*, *0123456789*. https://doi.org/10.1007/s11831-021-09631-5

Ng, A. W., and Kwok, B. K. B. (2017). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. In *Journal of Financial Regulation and Compliance* (Vol. 25, Issue 4, pp. 422–434). https://doi.org/10.1108/JFRC-01-2017-0013

Nikolov, A. L. G. (2018). *Wireless network vulnerabilities estimation*. *82*(2), 80–82.

Of, I. J., Vol, G. S., and Online, P. (2021). *No Title*. *0744*, 240–262. https://doi.org/10.34109/ijebeg.202113112

Pascacio, P., Casteleyn, S., Torres-Sospedra, J., Lohan, E. S., and Nurmi, J. (2021). Collaborative Indoor Positioning Systems: A Systematic Review. *Sensors*, *21*, 1002. https://doi.org/10.3390/s21031002

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., and Pahnila, S. (2004). Consumer acceptance of online

banking: An extension of the technology acceptance model. *Internet Research*, *14*(3), 224–235. https://doi.org/10.1108/10662240410542652

Puschmann, T. (2017). Fintech. *Business and Information Systems Engineering*, *59*(1), 69–76. https://doi.org/10.1007/s12599-017-0464-6

Qu, G., and Michael, M. N. (2010). RAPiD: An indirect rogue access points detection system. *??International Performance Computing and Communications Conference, Pp*, 9–16.

Ravikumar, T. (2019). Digital financial inclusion: A payoff of financial technology and digital finance uprising in India. *International Journal of Scientific and Technology Research*, *8*(11), 3434–3438. www.ijstr.org

Rehman, A., Haseeb, K., Saba, T., Lloret, J., and Sendra, S. (2021). An Optimization Model with Network Edges for Multimedia Sensors Using Artificial Intelligence of Things. *Sensors*, *21*, 7103. https://doi.org/10.3390/s21217103

Sahi, A. M., Khalid, H., Abbas, A. F., Zedan, K., and Khatib, S. F. A. (2022). *The Research Trend of Security and Privacy in Digital Payment*.

Saied, Y. Ben. (2013). Collaborative security for the internet of things. Economics and Finance. *Institut National Des T?L?Communications English*, *2013*.

Saksonova, S., and Kuzmina-Merlino, I. (2017). Fintech as financial innovation - The possibilities and problems of implementation. *European Research Studies Journal*, *20*(3), 961–973. https://doi.org/10.35808/ersj/757

Schmidt, A., Bye, R., Schmidt, H., Clausen, J., Kiraz, O., and Y, K. A. (n.d.). *Static Analysis of Executables for Collaborative Malware Detection on Android*.

Suryono, R. R., Budi, I., and Purwandari, B. (2020). Challenges and Trends of Financial Technology (Fintech): A Systematic Literature Review. *Information*, *11*, 12. https://doi.org/http://dx.doi.org/10.3390/info11120590

Urke, A. R. (2022). Kure, ?.; ?vsthus, K. *A Survey Of*, *802*, 15. https://doi.org/10.3390/s22010015

Wu, H., Fan, Y. ;Wan., Ma, Y. ., Xing, H. ., and A, L. (2021). Comprehensive Review on Edge Caching from the Perspective of Total Process: Placement, Policy and Delivery. *Sensors*, *21*, 5033. https://doi.org/10.3390/s21155033

Yang, N., Wang, L., Geraci, G., Elkashlan, M., Yuan, J., and Renzo, M. Di. (2015). *Safeguarding 5G Wireless Communication Networks Using Physical Layer Security*. *April*, 20–27.

Zhou, Y. (2012). *Dissecting Android Malware : Characterization and Evolution*. *4*. https://doi.org/10.1109/SP.2012.16