

IT risks associated with information theft in the financial system - a systematic review

Frank Cabanillas-Alca, Sebastian Chaquila-Muñoz, Orlando Iparraguirre-Villanueva

Facultad de Ingeniería y Arquitectura, Universidad Autónoma del Perú, Lima, Perú

Article Info

Article history:

Received Jun 21, 2024

Revised Sep 6, 2024

Accepted Sep 30, 2024

Keywords:

Attack
Banking
Information
Security
System

ABSTRACT

This research paper systematically reviews the financial system's computer security risks associated with information theft. The objective is to explore the security risks and their implications concerning information theft in the economic system. Three research questions were formulated to identify these risks, their nature, and potential consequences to achieve this objective. Fifty-five articles obtained from reliable databases linked to both study variables were analyzed using the PRISMA methodology. To ensure the validity and reliability of the information, various filters were applied, such as year, keywords, and elimination of duplicate articles. In addition, an exhaustive reading of the content of each article was carried out, organizing all the information through a systematization matrix. After a thorough review of the research articles, mostly written in English and representing 34.55% of the total in 2023, risks associated with the financial sector were identified, including malware, ransomware, phishing, distributed denial of service (DDoS), hybrid XSS, eavesdropping, and social engineering. Geographically, India leads with 14.55% of the articles, followed by South Korea and the United States, with 12.72% each, while the other countries have lower percentages. In conclusion, these risks coincide with previous research and the consequences they generate, highlighting the importance of this type of study for the basis of scientific research.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Orlando Iparraguirre-Villanueva

Facultad de Ingeniería y Arquitectura, Universidad Autónoma del Perú

Lima, Perú

Email: oiparraguirre@ieee.org

1. INTRODUCTION

Currently, the issue of security problems or computer vulnerabilities continues to be a major concern for the development [1] of the financial system, giving way to data access violations and data theft [2]. Therefore, using a username and password would not be enough to cover all the risks of these systems, causing a security risk of critical information for the customer [3]. For this reason, such financial institutions must implement appropriate technologies to ensure an adequate and secure environment [4]. However, it is essential to consider these vulnerabilities that could represent an IT risk, as they refer to flaws in the system that can be exploited by attackers and could cause fatal consequences [5]. According to the aforementioned, these risks could compromise security and privacy [6]. Given that the information handled in the financial sector is susceptible and critical, this situation entails a significant information security risk [7], in which any exposure or breach could be used to cause economic damage, compromise data, affect personal security, or directly harm others [8]. Therefore, information theft becomes an IT risk to be considered in the financial sector [9].

The research plays on the critical need to address security risks and computer vulnerabilities in the financial system. Closely exploring the threats related to information theft highlights the urgent need to analyze these cyber threats [10]. Although the article does not seek to implement solutions, it will provide a broader view of these risks, which will help guide future research and development projects to ensure the protection of data from potential online attacks [11].

Regarding the above, these research results would be accurate and reliable, as they are based on a wide range of studies and data, which will be collected from academic repositories to gain a deeper understanding of these risks and their implications in the financial system. This will provide an up-to-date and comprehensive view of these risks in the financial system [12]; they are also directly related to the most important issues of the ISO 27001 standard [13], which covers the confidentiality and integrity of information by financial systems.

Furthermore, the main objective of this paper is to explore the security risks and their implications related to information theft in the financial system. Following the central idea of the review article, questions will be addressed that seek to identify these risks, what they consist of, and what types of consequences would negatively affect the financial system. A systematic literature review will be carried out through a comprehensive analysis of 55 articles. To achieve this, articles from reliable databases linked to both study variables were identified and analyzed, thus making it possible to acquire up-to-date scientific knowledge. From a methodological perspective, the systematization is elaborated using the PRISMA methodology, ensuring information filtering to obtain valid and reliable data.

2. RELATED WORK

2.1. General risks in the financial system

This section explores how cyber attacks affect the financial sector, followed by related work. For example, the article [14] explored the challenges faced by Ecuador's financial sector. To achieve this purpose, they had to interview financial security managers, security officers, authorities, and managers of internet service providers. The findings indicate that Ecuador's financial sector faces cybersecurity risks caused by external and internal actors, which can result in fraud and operational failures. Furthermore, in [15] they implemented an Internet of things (IoT)-based risk monitoring in the financial industry. They collected IoT-related data, improving reliability and efficiency. The results show a 7.1% reduction in risk measurement. Similarly, the study [16] strengthened cyber security in environments where the banking infrastructure is highly distributed. Advanced algorithms and techniques for intrusion detection and security event correlation were implemented to achieve this. Implementing improved intrusion detection strengthened cyber security and protected the banking infrastructure by identifying and mitigating threats more effectively.

2.2. Data and privacy risks

For the present area, it focuses on how cyber-attacks affect users' data and put their privacy at risk. For example, in [17] they discussed security and privacy issues in big data. To do so, they analyzed the implications of massive data's velocity, volume, and variety. They identified several security and privacy issues in big data, including unauthorized access, data loss, and data misuse. In addition, Schyff *et al.* [18] conducted a comprehensive review of online privacy fatigue. For this purpose, they conducted a scoping review based on the PRISMA-ScR check. The response to this is the identification of five categories of antecedents of privacy fatigue: privacy risk, privacy control and management, knowledge and information, individual differences, and privacy policy characteristics. On the other hand, Rodrigues *et al.* [19] They presented PTMOL to analyze the privacy threats faced by OSN users. To realize the objective, they conducted two studies in which they evaluated the use of PTMOL for the design stages. The result mentions that PTMOL can be effectively incorporated into software development during the design phase of OSNs.

2.3. Financial management and transaction risks

For example, Riad and Elhoseny [20] proposed a new access control scheme that uses blockchain technology for the key revocation process, and they performed a security analysis to evaluate the scheme's robustness against known attacks in open banking systems. For this purpose, they conducted a security analysis to evaluate the scheme's robustness against known attacks in open banking systems. The research indicates that the proposed BKR-AC scheme has a faster response time. In turn, in the study [21], they addressed the problem of corruption and money laundering in non-governmental organizations and governmental fundraising organizations. They presented a blockchain-based transaction system that uses smart contracts to prevent illegitimate block changes during financial transactions. The results of this system show that this approach is much more secure and less susceptible to scams than traditional financial transaction systems. Furthermore, Choithani *et al.* [22] explored the relationship between artificial

intelligence, cybersecurity, and cryptocurrencies. Specific artificial intelligence techniques were reviewed and analyzed, such as support vector machines and neural networks of the artificial, short-term memory, and recurrence unit type. The result is that the impact and potential of artificial intelligence transform how cryptocurrencies and the financial system interact.

2.4. Risk assessment and risk management in the financial system

Finally, the next area highlights the risks faced by the financial sector, including a predictive model of threats in mobile money services and techniques to mitigate these risks. In line with the above, the research [23] delved into the growing threat of cybercrime in mobile money services. To achieve this, they gathered information through interviews with mobile money practitioners and applied the Synthetic Minority Oversampling Technique. The results mention that machine learning algorithms are effective in modelling and automating the prediction of cyber threats. Also, Asher *et al.* [24], they evaluated the capability of tools for reverse engineering mobile applications. They collected a dataset to be evaluated through these tools and compared the execution times. The results revealed that none of the existing tools could independently complete the reverse engineering process. Similarly, Swetha and Dara [25] they implemented LAN security to protect the data center of an organization in the BFSI industry. To achieve this, they configured the security functions in LANenforcer and added an intrusion prevention system for all traffic to pass through. In response, they found that implementing LAN security successfully protected the organization's data center. However, in the study [26] They proposed a new digital risk assessment framework. They identified 17 types of digital risks and quantified the probability of loss and impact of each risk using the Bernoulli distribution.

3. METHOD

The article uses a qualitative approach, like a systematic review, as existing knowledge on the proposed topic was collected and analyzed [27]. This will help to understand the present topic better and to answer the questions posed. Systematic review involves a methodical and transparent process of locating, selecting, and critically evaluating the relevant literature in each field. This process involves clearly defining research questions, identifying key terms and search strategies, selecting relevant data sources, evaluating included studies, and synthesizing results [28].

For this case, articles on the risks of financial systems in the period 2018-2023 have been collected. For this process, searching for and selecting information based on the parameters established by the Prisma methodology was necessary. The following aspects were considered for the acceptance of these articles in this systematic review:

In this case, articles on the risks of financial systems were collected during the period from 2018 to 2023. The search and selection of information based on the requirements given by the Prisma methodology was necessary for this specific process. In this systematic review, the following aspects were considered for the acceptance of such articles:

- It needs to be written in English, as it will have a greater source of international information related to the variables of this systematic review.
- It must be from reliable databases because it guarantees a clear review of this article.
- Publication date belonging to the year 2018 - 2023, given that adequate and updated information about the proposed article can be obtained in this period of antiquity.
- Filters for the article, such as "engineering" and "computer science," should be considered for the correct relationship in this systematic review.
- The selected articles are required to be open access
- The existence of statements about the risk of financial systems in their security would ensure congruence between the objectives of this systematic review and the articles found.

To discard the articles, the following aspects were considered:

- The articles obtained must not be duplicated to have repeated information.
- The date of publication must be older than 2018.
- The selected documents must not be of the book, thesis, or proceedings type.
- The information obtained from the articles should not be distant because the information described will not be related to this systematic review.

The following databases were considered for the search process: IEEE, Science Direct, Scopus, Springer, and ProQuest.

For the first step, the search is carried out using key terms such as "banking," "system," "attack," "information," and "security," as well as their translation into Spanish as "banca," "Sistema," "ataque," "información" and "Seguridad." After performing this search, the filter was applied according to the year of publication, excluding those that did not comply with the 2018 and 2023 years of publication. According to Figure 1, the articles included in the systematic review were distributed as follows:

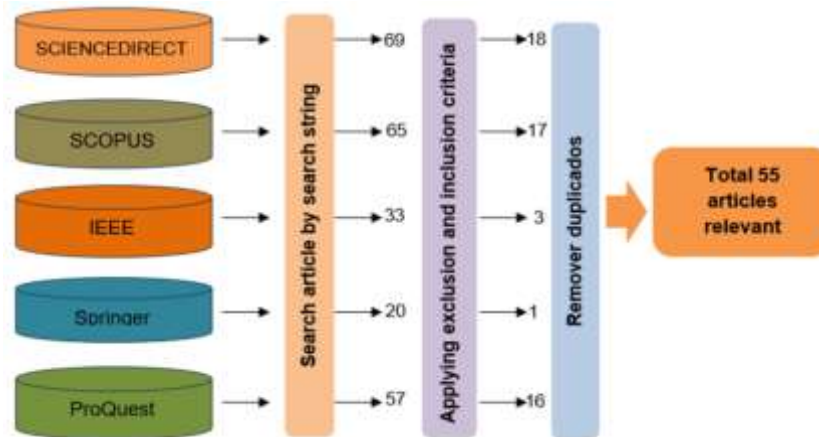


Figure 1. Number of studies identified by each database

Then we proceeded to a review of duplicates, which consisted of checking with the Mendeley tool if any article was duplicated; then to verify, we downloaded the articles for each database in XML format so that when imported into Microsoft Excel, we could make a complete filter, where the result was that there were 33 duplicates. The quantities identified in the search for information from the databases are described in Figure 2, according to the parameters of the PRISMA methodology.

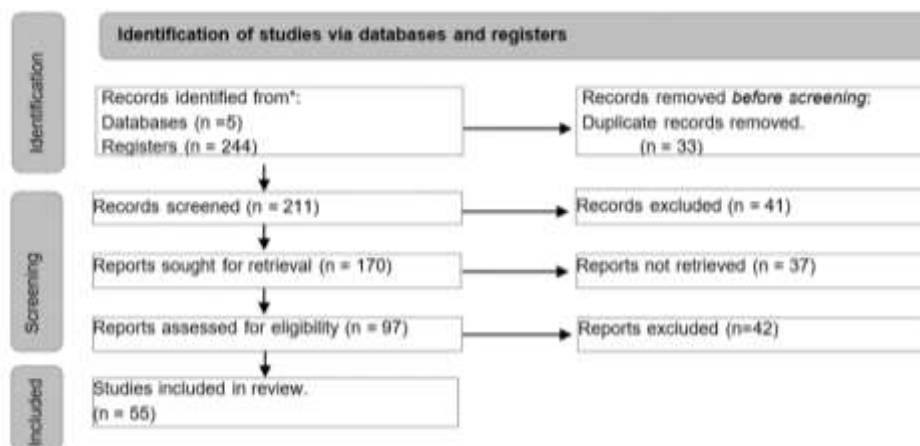


Figure 2. PRISMA methodology

4. RESULTS

Based on the database of 244 scans, the results were structured. In addition, during a rigorous analysis, according to the established filters, they were passed on to another database with methodological data of 55 studies. The PRISMA method was applied to clarify the results from the literature review. Starting with the identification of five bibliographic sources, specifically Science Direct, Scopus, IEEE Xplore, Springer, and ProQuest, the first selection was based on the search for keywords and phrases, of which 28.28% corresponded to Science Direct, 8.20% to Springer, 26.64% to Scopus, 23.36% to ProQuest, and 13.52% to IEEE.

During the second phase, the review of duplicates was carried out using the Mendeley tool to check if any article was duplicated; in addition, the articles were downloaded for each database in XML format so that when imported into Microsoft Excel, a complete filter could be made, from which 74 studies were removed, where the results showed 28.44% corresponded to Science Direct, 7.58% to Springer, 26.07% to Scopus, 26.07% to ProQuest, and 11.85% to IEEE.

During the third phase, the year of publication is considered; in this case, from 2018 to 2023, 37 studies were removed, of which 28.82% corresponded to Science Direct, 7.65% to Springer, 25.88% to

Scopus, 26.47% to ProQuest, and 11.18% to IEEE. During the fourth stage, eligibility, words, or phrases related to this systematic review’s subject matter were considered. Of the latter, 78 studies were removed, 18.75% corresponded to Science Direct, 4.46% to Springer, 20.53% to Scopus, 24.92% to ProQuest, and 6.25% to IEEE. In the fifth phase, we considered whether the studies were open access, where 36 studies were removed, giving 25.77% for Science Direct, 6.19% for Springer, 27.84% for Scopus, 30.93% for ProQuest, and 9.28% for IEEE.

The criterion of reading the summary was finally incorporated in the sixth phase, where identification by components such as methodology and results found was used to explain the relevance of the study and relationship with the objective of the study, considering that it has the same unit of analysis and variables or constructs addressed; and the correct access link, which involves identifying an access link to the document. This resulted in 42 excluded documents and 55 selected documents. Figure 3 shows the selection procedure of studies found in the databases.

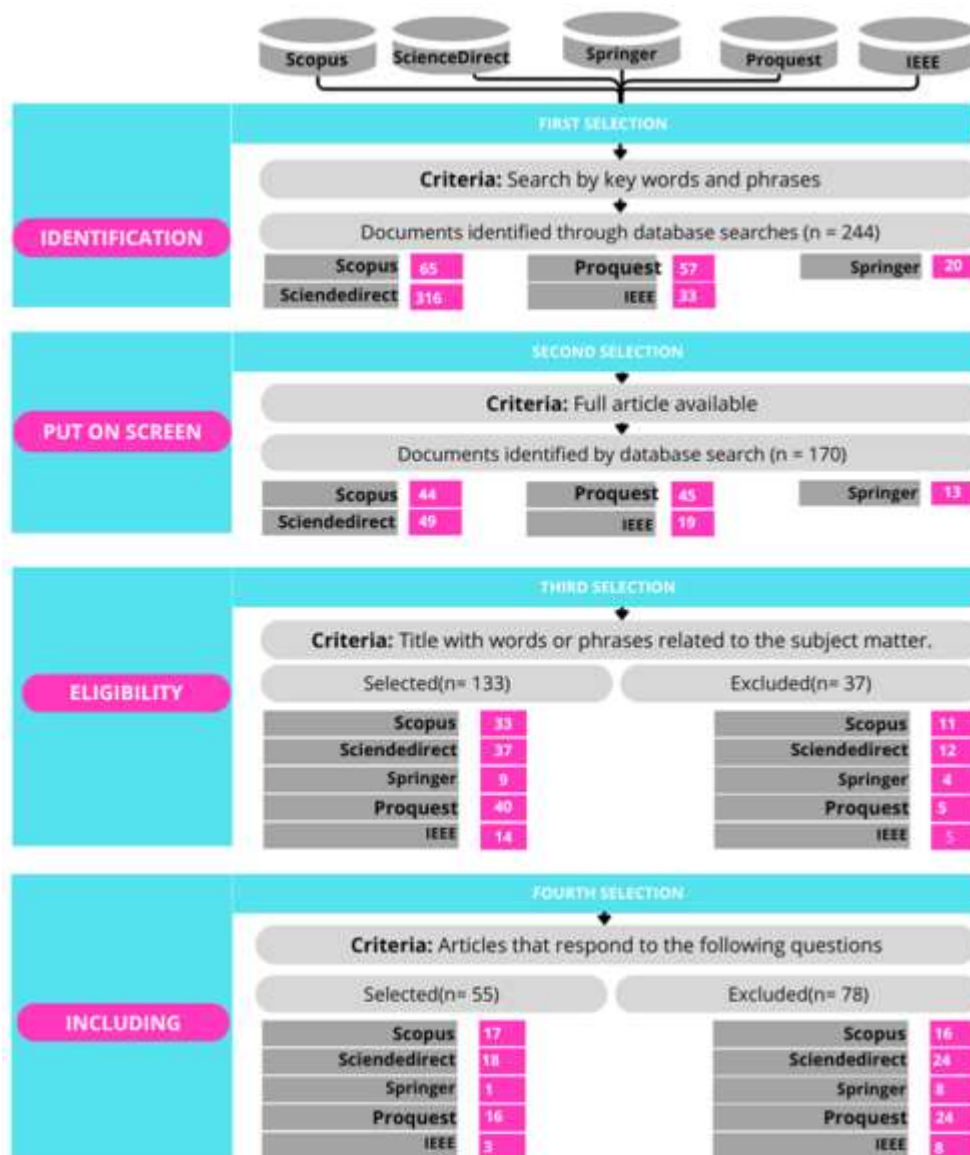


Figure 3. Selection procedure for studies found in databases

Figure 4 shows that 17 articles (30.91%) come from Scopus, 1 article (1.82%) from Springer, 18 (32.73%) from Science Direct, 16 (29.09%) from ProQuest and 3 (5.45%) from IEEE. Therefore, the Springer database is the least used database, with only a 1.82% share. ScienceDirect is the most predominant database in this research, with a 32.73% share.

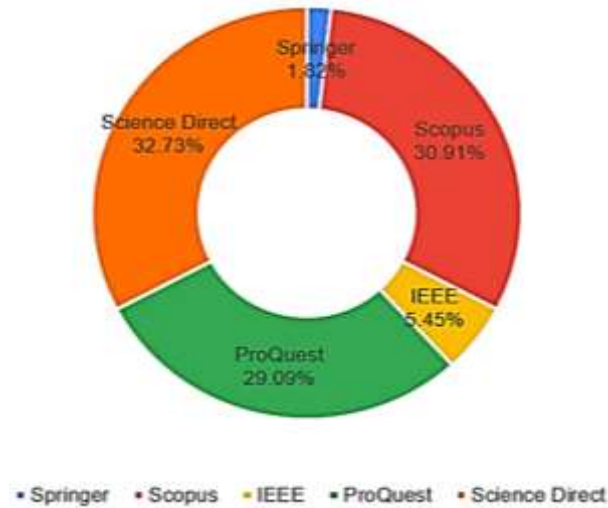


Figure 4. Percentages of data in the databases

The distribution of documents in the research by year of publication is shown in Figure 5, which includes 2018 to 2023. There is a steady increase in the number of newly created papers. In 2018 they represented 3.64% of the total; in 2019, they represented 7.27%; in 2020, they represented 7.27%; in 2021, they represented 21.82%; in 2022, they represented 25.45%; and finally, in 2023, they represented 34.55% of the total. A total of 55 documents will be added to the research.

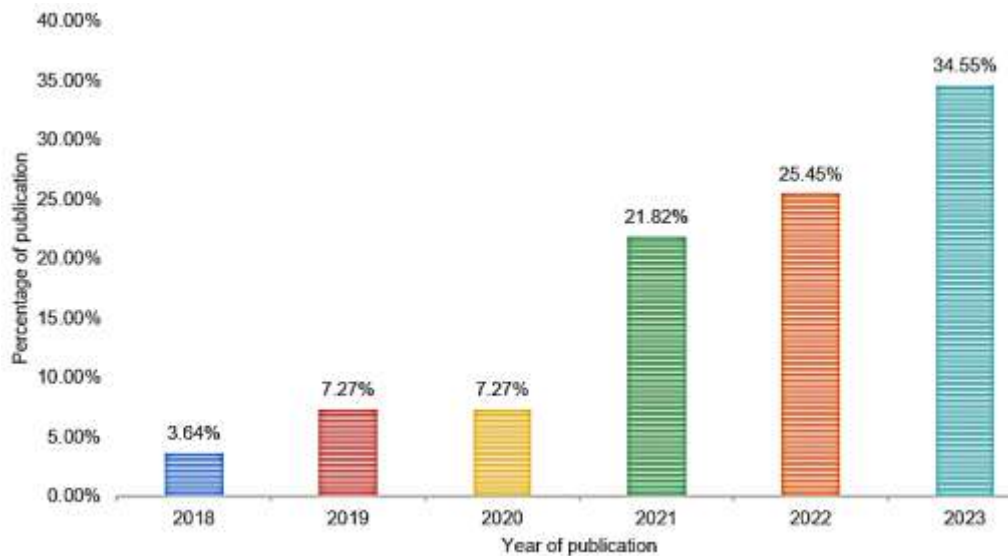


Figure 5. Documents covered in the year of publication of the investigation

Figure 6 shows that India leads the list, representing 14.55% of the total (8 articles), which indicates a significant contribution to this study. Then, the country of South Korea, which represents 12.72% of the total (7 articles), and the country of the United States, with 7 articles, represents 12.72%, which indicates its importance in this project.

In addition, other countries that contribute less to the total number of documents are mainly South Africa, Ethiopia, Saudi Arabia, Algeria, Yemen, and Ecuador, with one document each, and Indonesia and Malaysia, with two documents each. Despite their lower numerical contribution, these countries still add geographical diversity to the project. Figure 7 presents the research by country and continent.

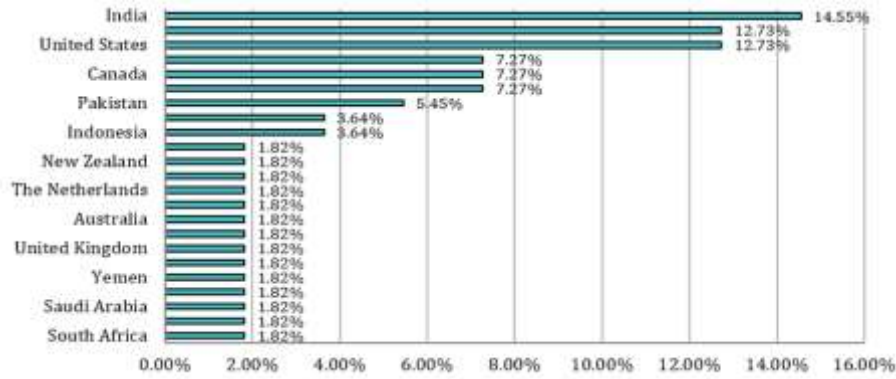


Figure 6. Research papers are grouped by continent and sorted by country of origin

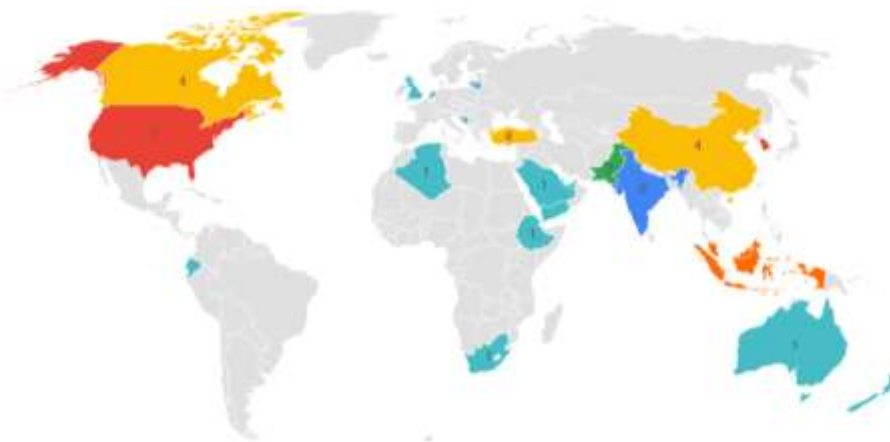


Figure 7. Documents grouped at a continental level according to country of origin

On the other hand, the distribution of articles in 5 academic databases classified as “Quantitative” and “Qualitative” is shown in Figure 8. 60% of the articles focus on qualitative research, while the remaining 40% fall into the quantitative category. Springer has 0 (0%) quantitative articles and 1 (1.82%) qualitative article, Scopus has 6 (10.91%) quantitative articles and 11 (20%) qualitative articles, Science Direct has 3 (5.45%) quantitative articles and 15 (27, 27%) of qualitative articles, IEEE offers 1 (1.82%) quantitative article and 2 (3.64%) qualitative articles. ProQuest has 12 (21.82%) quantitative articles and 4 (7.27%) qualitative articles.

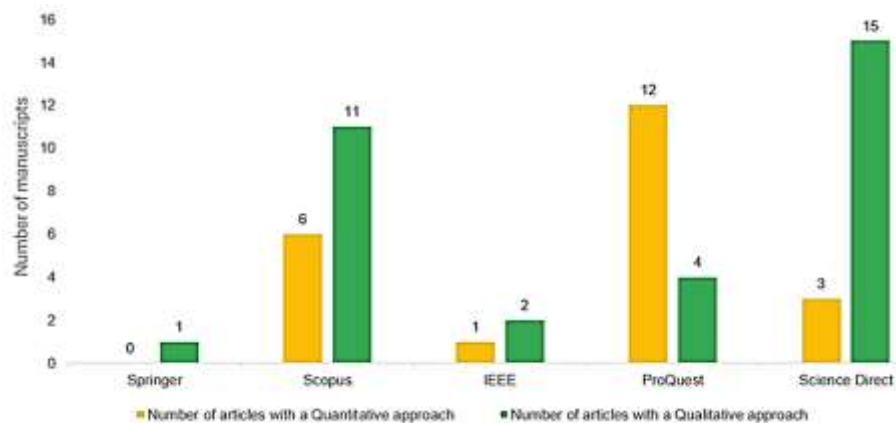


Figure 8. Documents incorporated into the research based on the research approach

Visualizing the network of documents available in databases is presented using bibliometric analysis. This quantitative tool displayed the keywords, highlighting their importance (Occurrences) and relationship strength with other keywords (Total strength of connection). In Figure 9, keywords with larger circles indicate greater importance, and those with more connections represent greater strength in relationships with other keywords.

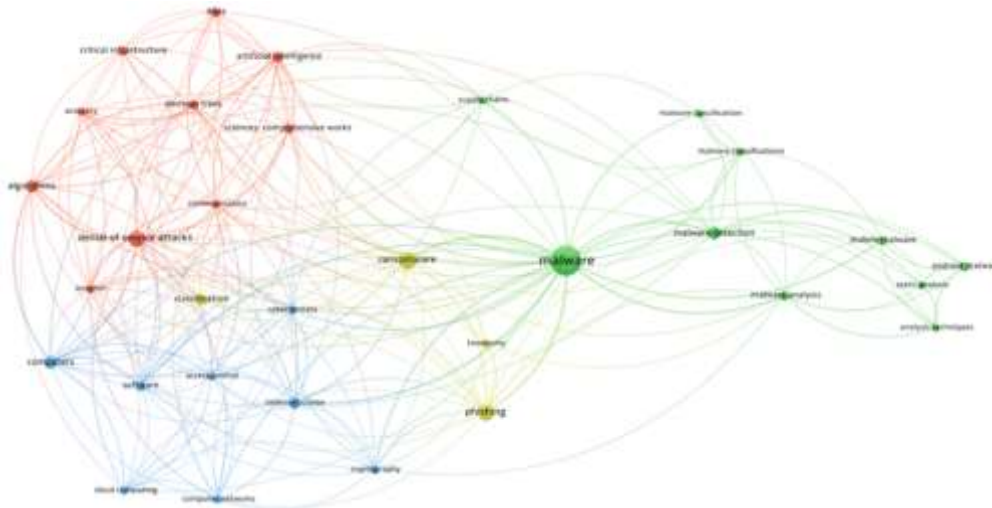


Figure 9. Network visualization of documents available in databases based on bibliometric analysis

5. DISCUSSION

5.1. RQ1: What risks affect the financial sector?

Several risks significantly affect the financial sector; among those identified in Table 1, one of the main ones is malware, considered a critical risk that requires special attention due to its ability to compromise cyber security. This statement supports the work [14], stating that the predominant risks in the financial sector are mostly external, highlighting malware as a threat that can trigger operational problems and information theft. Specifically, ransomware, a malware variant, is presented as a unique risk as it can encrypt financial information, causing system unavailability and demanding a ransom to unlock files. It also correlates with the study [26], which identifies 17 types of digital risks, highlighting among them ransomware, which can negatively affect the financial sector, generating vulnerabilities through external attacks by encrypting data. On the other hand, distributed denial of service (DDoS), which is considered a risk that can aggravate the attacks above since it would compromise security systems in the financial sector, is supported by Swetha and Dara [25], which mentions that these DDoS attacks lead to an interruption of services, which would negatively affect the financial sector.

Table 1. Risks affecting the financial system

No	Risks affect the financial sector	Quantity	References
1	Malware	10	[26]-[47]
2	Ransomware	8	[48]-[55]
3	Phishing	8	[56]-[63]
4	DDoS	17	[64]-[80]
5	XSS híbrido	1	[81]
6	Eavesdropping.	1	[82]
7	Social engineering	1	[83]

5.2. RQ2: What are these risks affecting the financial sector?

The risk affecting the financial sector manifests itself through various cyber threats, each with its own method of attack. According to Table 2, Malware, in the form of malicious software, is designed to evade security detection, as the study supports. Which mentions that malware is used to damage or take control of a computer system [15]. It is like ransomware in that it can compromise the integrity of financial systems. Both act as infiltrators that can trigger serious consequences by compromising the confidentiality and availability of information. On the other hand, the psychological manipulation associated with Social Engineering shares similarities with Phishing in its deceptive approach to obtaining confidential information.

Both techniques exploit users' trust, either through identity fraud in the case of Phishing or through psychological manipulation in Social Engineering. In turn, [17] mentions that Phishing is common technique cybercriminals use to obtain confidential information from users and is not necessarily related to large datasets.

Table 2. Concept of each risk affecting the financial system

No.	Risk	What is this risk affecting the financial sector?	Quantity	References
1	Ransomware	Secuestro de datos por medio del cifrado	5	[48]-[51], [55]
2	Phishing	Engaño para obtener información sensible mediante falsificación de identidad.	6	[56]-[58], [60]-[63]
3	DDOS	Inundar un servidor o red con una gran cantidad de solicitudes falsas	7	[64]-[67], [69], [72], [74]
4	Malware	Software malicioso para evadir la detección de seguridad	10	[31]-[34], [36]-[39],
5	XSS híbrido	Serie de inyecciones maliciosas en las vulnerabilidades de aplicaciones web.	1	[81]
6	Social engineering	Manipulación psicológica para obtener información confidencial.	1	[82]
7	Eavesdropping	Escuchar conversaciones privadas sin el consentimiento de la persona	1	[83]

5.3. What are the consequences of these risks for the financial sector?

A comparison of these risks' main implications and consequences for the financial industry is mentioned. According to the review of all the articles, it is analyzed that the main ones correspond to the loss of financial data and the theft of confidential/banking information. Regarding the former, it affects the integrity and confidentiality of data. However, it is important to highlight the theft of banking information, as it compromises the financial security of the affected individuals and can lead to fraudulent transactions. This is supported by the article [23]. It points out that, thanks to these vulnerabilities, cybercriminals are finding gaps in the new security controls and increasing cybercrime. All of the above relates significantly to research [25] Malicious access and insider attacks can include attempts to steal confidential information and disrupt the organization's services, such as DDoS attacks or packet flooding attacks. Table 3 shows the consequences of IT risks in the financial sector.

Table 3. Consequences caused by risks in the financial system

No	What are the consequences of this risk for the financial sector?	Quantity	References
1	Exposure of personal/financial information	6	[29], [30], [35], [44], [59], [77]
2	Financial fraud	3	[32], [56], [58]
3	Loss of banking/personal data	26	[29]-[31], [35], [38], [40]-[45], [47], [48], [52]-[54], [59], [62], [66], [73], [75], [76], [77], [79], [80], [81]
4	Theft of confidential/banking information	9	[29], [31], [41], [44], [45], [48], [56], [58], [82]
5	Data privacy breach	5	[41]-[43], [54], [68]
6	Disruption to security services	4	[43], [71], [73], [80]

6. CONCLUSION

The present systematic review examined theoretical and practical studies on IT risks associated with information theft in the financial system. By applying inclusion and exclusion criteria, 55 out of 244 articles were selected using the PRISMA methodology. These articles were distributed as follows: 17 (30.91%) from Scopus, 1 (1.82%) from Springer, 18 (32.73%) from Science Direct, 16 (29.09%) from ProQuest, and 3 (5.45%) from IEEE. The studies identified specific IT risks in the financial sector and the consequences associated with them. Geographically, India leads with 14.55% of articles, which represents a significant contribution to the study, followed by South Korea and the United States with 12.72% of articles each, and the rest are distributed across the other countries with smaller percentages.

Finally, the development of this review provided a comprehensive exploration of the various studies that explain and analyze the knowledge about IT risks and the consequences they generate, such as information theft in the financial system, including exposure of personal/financial information, financial fraud, loss of banking/personal data, theft of confidential/banking information, breach of data privacy and disruption of security services. All these aspects will help to guide future research and development projects to ensure data protection against possible online attacks. Regarding limitations, it is important to note that it was impossible to identify all the risks that could exist or be related to the financial sector. This limits the ability to cross-check information on these risks comprehensively.

ACKNOWLEDGEMENTS

I want to express my sincere thanks to my fellow researchers, whose collaboration and support were fundamental to this project's success. Your contributions significantly enriched our work.

REFERENCES





- [1] C. Fei and J. Shen, "Machine learning for securing cyber-physical systems under cyber attacks: a survey," *Franklin Open*, p. 100041, Oct. 2023, doi: 10.1016/J.FRAOPE.2023.100041.
- [2] M. Dib and S. Pierre, "Insider attack model against HSM-based architecture," *IEEE Access*, vol. 11, pp. 86848–86858, 2023, doi: 10.1109/ACCESS.2023.3304994.
- [3] P. Suba, M. Mailsamy, and S. Sinduja, "Secure internet banking authentication," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 8, no. 6 Special issue, pp. 139–140, 2019, doi: 10.35940/ijeat.F1029.0886S19.
- [4] Q. Z. Abdulla and M. D. Al-Hassani, "Consumer use of E-Banking in Iraq: security breaches and offered solution," *Iraqi Journal of Science*, vol. 63, no. 8, pp. 3662–3670, 2022, doi: 10.24996/ij.s.2022.63.8.40.
- [5] W. Cai, J. Chen, J. Yu, and L. Gao, "A software vulnerability detection method based on deep learning with complex network analysis and subgraph partition," *Information and Software Technology (IST)*, vol. 164, p. 107328, Dec. 2023, doi: 10.1016/J.INFSOF.2023.107328.
- [6] O. Tanga, O. Akinradewo, C. Aigbavboa, and D. Thwala, "Cyber attack risks to construction data management in the fourth industrial revolution era: a case of gauteng province, South Africa," *Journal of Information Technology in Construction*, vol. 27, pp. 845–863, 2022, doi: 10.36680/j.itcon.2022.041.
- [7] S. E. A. Ali, F. W. Lai, P. D. D. Dominic, N. J. Brown, P. B. B. Lowry, and R. F. Ali, "Stock market reactions to favorable and unfavorable information security events: A systematic literature review," *Computers and Security*, vol. 110, p. 102451, Nov. 2021, doi: 10.1016/J.COSE.2021.102451.
- [8] T. J. Holt, "Understanding the state of criminological scholarship on cybercrimes," *Computers in Human Behavior*, vol. 139, p. 107493, 2023, doi: 10.1016/j.chb.2022.107493.
- [9] A. Aparicio, M. M. Martínez-González, and V. Cardeñoso-Payo, "App-based detection of vulnerable implementations of OTP SMS APIs in the banking sector," *Wireless Networks*, 2023, doi: 10.1007/s11276-023-03455-w.
- [10] W. Boungou, "Cyber-attacks and banking intermediation," *Economics Letters*, vol. 233, p. 111354, 2023, doi: 10.1016/j.econlet.2023.111354.
- [11] H. U. Khan, M. Z. Malik, S. Nazir, and F. Khan, "Utilizing bio metric system for enhancing cyber security in banking sector: a systematic analysis," *IEEE Access*, vol. 11, pp. 80181–80198, 2023, doi: 10.1109/ACCESS.2023.3298824.
- [12] P. Hou *et al.*, "Technology and practice of intelligent governance for financial data security," *Chinese Journal of Network and Information Security*, vol. 9, no. 3, pp. 174–187, 2023, doi: 10.11959/j.issn.2096-109x.2023048.
- [13] ISO.org, "ISO/IEC 27001 Standard – Information Security Management Systems." Accessed: Oct. 11, 2023. [Online]. Available: <https://www.iso.org/standard/27001>
- [14] F. E. Catota, M. Granger Morgan, and D. C. Sicker, "Cybersecurity incident response capabilities in the ecuadorian financial sector," *Journal Cybersecur*, vol. 4, no. 1, 2018, doi: 10.1093/cybsec/tyy002.
- [15] Y. Li, "Security and risk analysis of financial industry based on the internet of things," *Wireless Communications and Mobile Computing*, vol. 2022, 2022, doi: 10.1155/2022/6343468.
- [16] S. Eswaran, V. Rani, D. Daniel, J. Ramakrishnan, and S. Selvakumar, "An enhanced network intrusion detection system for malicious crawler detection and security event correlations in ubiquitous banking infrastructure," *International Journal of Pervasive Computing and Communications*, vol. 18, no. 1, pp. 59–78, 2022, doi: 10.1108/IJPC-04-2021-0102.
- [17] F. M. Abdullah, "Privacy, security and legal challenges in big data," *International Journal of Civil Engineering and Technology*, vol. 9, no. 13, pp. 1682–1690, 2018, [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85061119724&partnerID=40&md5=d6eb4c7e63cef4363ae2aa72d1fd615c>
- [18] K. V. D. Schyff, G. Foster, K. Renaud, and S. Flowerday, "Online privacy fatigue: a scoping review and research agenda," *Future Internet*, vol. 15, no. 5, 2023, doi: 10.3390/fi15050164.
- [19] A. Rodrigues, M. L. B. Villela, and E. L. Feitosa, "Privacy threat modeling language," *IEEE Access*, vol. 11, pp. 24448–24471, 2023, doi: 10.1109/ACCESS.2023.3255548.
- [20] K. Riad and M. Elhoseny, "A blockchain-based key-revocation access control for open banking," *Wireless Communications and Mobile Computing*, vol. 2022, 2022, doi: 10.1155/2022/3200891.
- [21] M. Jain, S. Kaswan, and D. Pandey, "A blockchain based fund management scheme for financial transactions in NGOs," *Recent Patents on Engineering*, vol. 16, no. 2, 2022, doi: 10.2174/1872212115666210615155447.
- [22] T. Choithani, A. Chowdhury, S. Patel, P. Patel, D. Patel, and M. Shah, "A comprehensive study of artificial intelligence and cybersecurity on bitcoin, crypto currency and banking system," *Annals of Data Science*, 2022, doi: 10.1007/s40745-022-00433-5.
- [23] M. L. Sanni, B. O. Akinyemi, D. A. Olalere, E. A. Olajubu, and G. A. Aderounmu, "A predictive cyber threat model for mobile money services," *Annals of Emerging Technologies in Computing*, vol. 7, no. 1, pp. 40–60, 2023, doi: 10.33166/AETIC.2023.01.004.
- [24] S. W. Asher, S. Jan, G. Tsaramiris, F. Q. Khan, A. Khalil, and M. Obaidullah, "Reverse engineering of mobile banking applications," *Computer Systems Science and Engineering*, vol. 38, no. 3, pp. 265–278, 2021, doi: 10.32604/CSSE.2021.016787.
- [25] K. V. Swetha and R. Dara, "Deployment of intrusion prevention system on multi-core processor based security hardware," *International Journal of Computer Networks and Communications*, vol. 10, no. 3, pp. 13–25, 2018, doi: 10.5121/IJCNC.2018.10302.
- [26] S. Muammar, D. Shehada, and W. Mansoor, "Digital risk assessment framework for individuals: analysis and recommendations," *IEEE Access*, vol. 11, pp. 85561–85570, 2023, doi: 10.1109/ACCESS.2023.3293062.
- [27] T. M. Gulotta, R. Salomone, G. Mondello, and B. Ricca, "FLAVIA-LCT - Framework for systematic literature review to analyse vast InformAtion in life cycle thinking studies," *Heliyon*, vol. 9, no. 5, p. e15547, 2023, doi: 10.1016/j.heliyon.2023.e15547.
- [28] A. Ilic, Y. Sievers, K. Roser, K. Scheinemann, and G. Michel, "The information needs of relatives of childhood cancer patients and survivors: A systematic review of qualitative evidence," *Patient Education and Counseling*, vol. 114, p. 107840, 2023, doi: 10.1016/j.pec.2023.107840.

- [29] O. Flor-Unda, F. Simbaña, X. Larriva-Novo, Á. Acuña, R. Tipán, and P. Acosta-Vargas, "A comprehensive analysis of the worst cybersecurity vulnerabilities in Latin America," *Informatics*, vol. 10, no. 3, p. 71, 2023, doi: <https://doi.org/10.3390/informatics10030071>.
- [30] S. Huh, S. Cho, J. Choi, S. Shin, and H. Lee, "A comprehensive analysis of today's malware and its distribution network: common adversary strategies and implications," *IEEE Access*, vol. 10, pp. 49566–49584, 2022, doi: 10.1109/ACCESS.2022.3171226.
- [31] S. A. Roseline and S. Geetha, "A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks," *Computers and Electrical Engineering*, vol. 92, p. 107143, 2021, doi: 10.1016/j.compeleceng.2021.107143.
- [32] M. Alrammal, M. Naveed, S. Sallam, and G. Tsaramirsis, "A critical analysis on android vulnerabilities, malware, anti-malware and anti-malware bypassing," *Journal of Internet Technology*, vol. 23, no. 7, pp. 1651–1661, 2022, doi: 10.53106/160792642022122307019.
- [33] M. Dhalaria and E. Gandotra, "A hybrid approach for android malware detection and family classification," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 6, no. 6, pp. 174–188, 2021, doi: 10.9781/ijimai.2020.09.001.
- [34] S. Yang, Y. Wang, H. Xu, F. Xu, and M. Chen, "An android malware detection and classification approach based on contrastive learning," *Computers and Security*, vol. 123, p. 102915, 2022, doi: 10.1016/j.cose.2022.102915.
- [35] Sudhakar and S. Kumar, "An emerging threat fileless malware: a survey and research challenges," *Cybersecurity*, vol. 3, no. 1, pp. 1–12, Dec. 2020, doi: 10.1186/S42400-019-0043-X/TABLES/5.
- [36] A. Djenna, A. Bouridane, S. Rubab, and I. M. Marou, "Artificial intelligence-based malware detection, analysis, and mitigation," *Symmetry (Basel)*, vol. 15, no. 3, p. 677, 2023, doi: 10.3390/sym15030677.
- [37] S. Chen *et al.*, "Automated poisoning attacks and defenses in malware detection systems: An adversarial machine learning approach," *Computers and Security*, vol. 73, pp. 326–344, 2018, doi: 10.1016/j.cose.2017.11.007.
- [38] A. Yeboah-Ofori *et al.*, "Cyber threat predictive analytics for improving cyber supply chain security," *IEEE Access*, vol. 9, pp. 94318–94337, 2021, doi: 10.1109/ACCESS.2021.3087109.
- [39] R. Korine and D. Hendler, "DAEMON: Dataset/platform-agnostic explainable malware classification using multi-stage feature mining," *IEEE Access*, vol. 9, pp. 78382–78399, 2021, doi: 10.1109/ACCESS.2021.3082173.
- [40] A. Singh, R. A. Ikuesan, and H. Venter, "MalFe—malware feature engineering generation platform," *Computers*, vol. 12, no. 10, p. 201, 2023, doi: 10.3390/computers12100201.
- [41] A. K. Pandey and F. Alsolami, "Malware analysis in web application security: An investigation and suggestion," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 7, pp. 191–201, 2020, doi: 10.14569/IJACSA.2020.0110725.
- [42] A. Abusitta, M. Q. Li, and B. C. M. Fung, "Malware classification and composition analysis: A survey of recent developments," *Journal of Information Security and Applications*, vol. 59, 2021, doi: 10.1016/j.jisa.2021.102828.
- [43] I. Gulatas, H. H. Kilinc, A. H. Zaim, and M. A. Aydin, "Malware threat on edge/fog computing environments from internet of things devices perspective," *IEEE Access*, vol. 11, pp. 33584–33606, 2023, doi: 10.1109/ACCESS.2023.3262614.
- [44] A. Qamar, A. Karim, and V. Chang, "Mobile malware attacks: Review, taxonomy and future directions," *Future Generation Computer Systems*, vol. 97, pp. 887–909, 2019, doi: 10.1016/j.future.2019.03.007.
- [45] N. A. Anuar, M. Z. Mas'ud, N. Bahaman, and N. A. Mat Ariff, "Mobile malware behavior through opcode analysis," *International Journal of Communication Networks and Information Security*, vol. 12, no. 3, pp. 345–354, 2020, [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85100188047&partnerID=40&md5=b40aaf91007889c408a9475428424b5e>
- [46] M. A. Husainiamer, M. M. Saudi, A. Ahmad, and A. S. M. Syafiq, "Mobile malware classification for iOS inspired by phylogenetics," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 8, pp. 99–105, 2021, doi: 10.14569/IJACSA.2021.0120812.
- [47] D. Ö. Şahin, O. E. Kural, S. Akleyek, and E. Kılıç, "Permission-based Android malware analysis by using dimension reduction with PCA and LDA," *Journal of Information Security and Applications*, vol. 63, 2021, doi: 10.1016/j.jisa.2021.102995.
- [48] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics (Basel)*, vol. 12, no. 6, p. 1333, 2023, doi: 10.3390/electronics12061333.
- [49] S. Poudyal and Di. Dasgupta, "Analysis of crypto-ransomware using ML-based multi-level profiling," *IEEE Access*, vol. 9, pp. 122532–122547, 2021, doi: 10.1109/ACCESS.2021.3109260.
- [50] T. Yin, A. Sarabi, and M. Liu, "Deterrence, backup, or insurance: game-theoretic modeling of ransomware," *Games (Basel)*, vol. 14, no. 2, p. 20, 2023, doi: 10.3390/g14020020.
- [51] C. Lee and K. Lee, "Impact analysis of resilience against malicious code attacks via emails," *Computers, Materials and Continua*, vol. 72, no. 3, pp. 4803–4816, 2022, doi: 10.32604/cmc.2022.025310.
- [52] H. Riggs *et al.*, "Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure," *Sensors*, vol. 23, no. 8, p. 4060, 2023, doi: 10.3390/s23084060.
- [53] T. R. Reshmi, "Information security breaches due to ransomware attacks - a systematic literature review," *International Journal of Information Management Data Insights*, vol. 1, no. 2, p. 100013, 2021, doi: 10.1016/j.jjime.2021.100013.
- [54] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," *Computers and Security*, vol. 111, 2021, doi: 10.1016/j.cose.2021.102490.
- [55] S. Razaulla *et al.*, "The age of ransomware: a survey on the evolution, taxonomy, and research directions," *IEEE Access*, 2023, doi: 10.1109/ACCESS.2023.3268535.
- [56] S. Chanti and T. Chithralekha, "A literature review on classification of phishing attacks," *International Journal of Advanced Technology and Engineering Exploration*, vol. 9, no. 89, pp. 446–476, Apr. 2022, doi: 10.19101/IJATEE.2021.875031.
- [57] X. Wang, Z. Yan, R. Zhang, and P. Zhang, "Attacks and defenses in user authentication systems: A survey," *Journal of Network and Computer Applications*, vol. 188, p. 103080, 2021, doi: 10.1016/j.jnca.2021.103080.
- [58] M. A. Ali, M. A. Azad, M. Parreno Centeno, F. Hao, and A. van Moorsel, "Consumer-facing technology fraud: Economics, attack methods and potential solutions," *Future Generation Computer Systems*, vol. 100, pp. 408–427, 2019, doi: 10.1016/j.future.2019.03.041.
- [59] S. R. Zahra, M. A. Chishti, A. I. Baba, and F. Wu, "Detecting COVID-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system," *Egyptian Informatics Journal*, vol. 23, no. 2, pp. 197–214, 2022, doi: 10.1016/j.eij.2021.12.003.
- [60] J. Rastenis, S. Ramanauskaitė, J. Janulevičius, A. Čenys, A. Slotkiene, and K. Pakrijauskas, "E-mail-based phishing attack taxonomy," *Applied Sciences (Switzerland)*, vol. 10, no. 7, 2020, doi: 10.3390/app10072363.





- [61] T. V. N. Rao and S. Reddy, "Investigation of phishing attacks and means to utilize anti phishing techniques," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 7, no. 2, pp. 5–10, 2019, doi: 10.17762/ijritcc.v7i2.5224.
- [62] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," *Computers and Security*, vol. 73, pp. 519–544, 2018, doi: 10.1016/j.cose.2017.12.006.
- [63] F. Hassandoust, H. Singh, and J. Williams, "The role of contextualization in users' vulnerability to phishing attempts," *Australasian Journal of Information Systems*, vol. 24, 2020, doi: 10.3127/AJIS.V24I0.2693.
- [64] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Systems Research*, vol. 215, p. 108975, 2023, doi: 10.1016/j.epr.2022.108975.
- [65] E. Söğüt and O. A. Erdem, "A multi-model proposal for classification and detection of DDoS attacks on SCADA systems," *Applied Sciences*, vol. 13, no. 10, p. 5993, 2023, doi: 10.3390/app13105993.
- [66] Maniah, B. Soewito, F. L. Gaol, and E. Abdurachman, "A systematic literature review: risk analysis in cloud migration," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, Part B, pp. 3111–3120, 2022, doi: 10.1016/j.jksuci.2021.01.008.
- [67] A. Bashaiwath, H. Binsalleeh, and B. AsSadhan, "An explanation of the LSTM model used for DDoS attacks classification," *Applied Sciences*, vol. 13, no. 15, p. 8820, 2023, doi: 10.3390/app13158820.
- [68] R. Prakash, V. S. Anoop, and S. Asharaf, "Blockchain technology for cybersecurity: A text mining literature analysis," *International Journal of Information Management Data Insights*, vol. 2, no. 2, p. 100112, 2022, doi: https://doi.org/10.1016/j.ijime.2022.100112.
- [69] G. Cascavilla, D. A. Tamburri, and W.-J. Van Den Heuvel, "Cybercrime threat intelligence: A systematic multi-vocal literature review," *Computers and Security*, vol. 105, p. 102258, 2021, doi: 10.1016/j.cose.2021.102258.
- [70] E. A. Al-Qarni, "Cybersecurity in healthcare: a review of recent attacks and mitigation strategies," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 5, 2023, doi: 10.14569/IJACSA.2023.0140513.
- [71] T. G. Gebremeskel, K. A. Gameda, T. G. Krishna, and J. R. Perumalla, "DDoS attack detection and classification using hybrid model for multicontroller SDN," *Wireless Communications and Mobile Computing (Online)*, vol. 2023, 2023, doi: 10.1155/2023/9965945.
- [72] R. Gunawan, H. Ab Ghani, N. Khamis, J. Al Amien, and E. Ismanto, "Deep learning approach to DDoS attack with imbalanced data at the application layer," *TELKOMNIKA*, vol. 21, no. 5, pp. 1060–1067, Oct. 2023, doi: 10.12928/TELKOMNIKA.v21i5.24857.
- [73] L. F. Eliyan and R. Di Pietro, "DoS and DDoS attacks in software defined networks: a survey of existing solutions and research challenges," *Future Generation Computer Systems*, vol. 122, pp. 149–171, 2021, doi: 10.1016/j.future.2021.03.011.
- [74] P. Vargas and I. Tien, "Impacts of 5G on cyber-physical risks for interdependent connected smart critical infrastructure systems," *International Journal of Critical Infrastructure Protection*, vol. 42, p. 100617, 2023, doi: 10.1016/j.ijcip.2023.100617.
- [75] S. Ullah, Z. Mahmood, N. Ali, A. Tahir, and A. Buriro, "Machine learning-based dynamic attribute selection technique for DDoS attack classification in IoT networks," *Computers*, vol. 12, no. 6, p. 115, 2023, doi: 10.3390/computers12060115.
- [76] S. Balasubramaniam *et al.*, "Optimization enabled deep learning-based DDoS attack detection in cloud computing," *International Journal of Intelligent Systems*, vol. 2023, 2023, doi: 10.1155/2023/2039217.
- [77] C. Lee and S. Lee, "Overcoming the DDoS attack vulnerability of an ISO 19847 shipboard data server," *Journal of Marine Science and Engineering (JMSE)*, vol. 11, no. 5, p. 1000, 2023, doi: 10.3390/jmse11051000.
- [78] R. U. Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, and J. Qadir, "Security and privacy of internet of medical things: a contemporary review in the age of surveillance, botnets, and adversarial ML," *Journal of Network and Computer Applications*, vol. 201, p. 103332, 2022, doi: 10.1016/j.jnca.2022.103332.
- [79] J. Choi *et al.*, "Understanding internet of things malware by analyzing endpoints in their static artifacts," *Computer Networks*, vol. 206, 2022, doi: 10.1016/j.comnet.2022.108768.
- [80] M. R. Haque *et al.*, "Unprecedented smart algorithm for uninterrupted SDN services during DDoS attack," *Computers, Materials, and Continua*, vol. 70, no. 1, pp. 875–894, 2022, doi: 10.32604/cmc.2022.018505.
- [81] D. Korać, B. Damjanović, D. Simić, and K.-K. R. Choo, "A hybrid XSS attack (HYXSSA) based on fusion approach: Challenges, threats and implications in cybersecurity," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, Part B, pp. 9284–9300, 2022, doi: 10.1016/j.jksuci.2022.09.008.
- [82] K. Lee and K. Yim, "Vulnerability analysis and security assessment of secure keyboard software to prevent PS/2 interface keyboard sniffing," *Sensors*, vol. 23, no. 7, 2023, doi: 10.3390/s23073501.
- [83] N. Tariq, M. Asim, and F. A. Khan, "Securing SCADA-based critical infrastructures: challenges and open issues," *Procedia Comput Sci*, vol. 155, pp. 612–617, 2019, doi: 10.1016/j.procs.2019.08.086.

BIOGRAPHIES OF AUTHORS







Frank Cabanillas-Allica     a system engineering graduate, he a data analyst, seeking excellence and innovation in data analysis and interpretation. I possess strong skills in extracting valuable information and creating predictive models. He focus on continuous improvement and delivering exceptional results drives me to seek growth in environments that value accuracy and innovation, where I also explore cloud solutions to optimize processes and drive business impact. He can be contacted at email: fcabanillas@autonoma.edu.pe.



Sebastián Chaquila-Muñoz     systems engineering graduate, with experience in software development (Front End) and information security, committed to excellence and innovation. I possess strong skills in intuitive design and robust backend functionality. He focus on continuous improvement and delivering exceptional results drives me to seek growth in environments that value excellence, where I also explore cloud solutions. He can be contacted at email: schaquila@autonoma.edu.pe.



Orlando Iparraguirre-Villanueva     systems engineer with a master's degree in information technology management, and a Ph.D. in Systems Engineering from the Universidad Nacional Federico Villarreal - Peru. ITIL® Certified, Specialization in Business Continuity Management (SBCM), SCRUM Certified. National and international speaker/panelist (Panama, Colombia, Ecuador, Venezuela, México). Extensive experience in undergraduate and postgraduate teaching in different universities in the country. Thesis advisor and jury in different universities. Professional experience in management positions in the field of Information Technology. Research professor with publications in Scopus and WoS-indexed journals (Q1, Q2, Q3, and Q4) of high impact. Topics of interest: open-source software, IoT, augmented reality, machine learning, AI, CNN, text mining, virtual environments, scientific research methodology, and thesis. He can be contacted at email: oiparraguirre@ieee.org.