Journal of Applied Business, Taxation and Economics Research (JABTER)
Vol. 5, No. 2, December 2025 (Page: 255-264) P-ISSN 2828-4976
DOI: 10.54408/jabter.v5i2.475 E-ISSN 2808-263X

SLR PRISMA: Information Security's Role in Banking Data Integrity

Novian Tika Melati[1*], Kurnia Ekasari[1], Kartika Dewi Sri Susilowati[1]

[1*] State Polytechnic of Malang, Indonesia

Corresponding Author: noviantikam25@gmail.com [1)]*

Keywords **:** *Information Security, Banking, Data Integrity, SLR, PRISMA*

Abstract: This study aims to explore the role of information security in maintaining banking data integrity in the digital era through a Systematic Literature Review (SLR) guided by the PRISMA protocol. A total of 55 relevant journal articles were analyzed using VOSviewer for bibliometric analysis and Taguette for thematic synthesis. The co-occurrence analysis revealed frequently used keywords such as internet banking, information security, technology, electronic banking, and customers, indicating a strong research focus on digital banking systems. Meanwhile, the co-authorship analysis showed limited collaboration among scholars, suggesting that the topic of information system security in the banking sector remains relatively underexplored. The thematic analysis identified key areas of concern, including the implementation of firewalls and intrusion detection systems, the development of secure integration models using OAuth 2.0, cryptographic measures such as AES-256 encryption, tokenization, and the Vigenère cipher, as well as the adoption of cloud computing and blockchain technology. Various cyber threats were also discussed, including data theft, transaction manipulation, credential misuse, malware, phishing, insider threats, and ransomware attacks. Furthermore, the importance of customer data protection was emphasized, particularly in relation to the Consumer Protection Law (UUPK). The findings underscore the need for enhanced technological solutions and stronger research collaboration to strengthen data integrity and security in the banking industry amid growing digital challenges.

Introduction

The banking sector is undergoing rapid digital transformation, reshaping operations and customer interactions (Saputri & Zulkarnain, 2024). Digitalization enhances transaction speed, service accessibility, and operational efficiency, yet it also introduces significant risks in the form of cyber threats, such as data theft and system manipulation (Hassandi &

Pangestu, 2025). Cyberattacks on banking institutions remain frequent and costly, often due to insufficient security measures and policy enforcement (Wisuda, 2022; Febriyanto et al., 2023). While many banks adopt formal security systems, their effectiveness is often undermined by limited staff awareness and inadequate internal audits (Nurhaliza et al., 2025). These challenges compromise banking integrity, damage public trust, and threaten financial stability. Information security is critical for safeguarding data integrity and maintaining customer trust. Beyond technical protection, it serves as an ethical and legal foundation for financial operations (Almadira et al., 2024). Addressing cyber threats requires robust, well-integrated security systems supported by strong governance and a proactive security culture. This study examines the interplay between information security and banking integrity by conducting a Systematic Literature Review (SLR) guided by the PRISMA protocol. It offers strategic recommendations for banks and regulators to develop sustainable security systems, highlighting best practices and addressing policy-implementation gaps (Suryawijaya, 2023; Wahana, 2025). The goal is to support a resilient, trusted, and secure digital banking ecosystem in the face of evolving cyber threats.

Research Method

This research is a qualitative research using the Systematic Literature Review (SLR) approach. This research was conducted by following the Systematic Literature Review (SLR) stages referring to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocol, which consists of four main stages: identification, screening, eligibility evaluation, and inclusion. To support the literature collection process, an auxiliary tool was used, namely Publish or Perish (PoP).

From the results of the literature search using Publish or Perish, 980 journals have been found. Based on these results, the next step is to create a PRISMA diagram, a PRISMA diagram is a framework to show that researchers have filtered literature objectively, transparently, and logically. (Mishra & Mishra, 2023) . So it meets the requirements of *a Systematic Literature Review.* The following is a PRISMA diagram image:

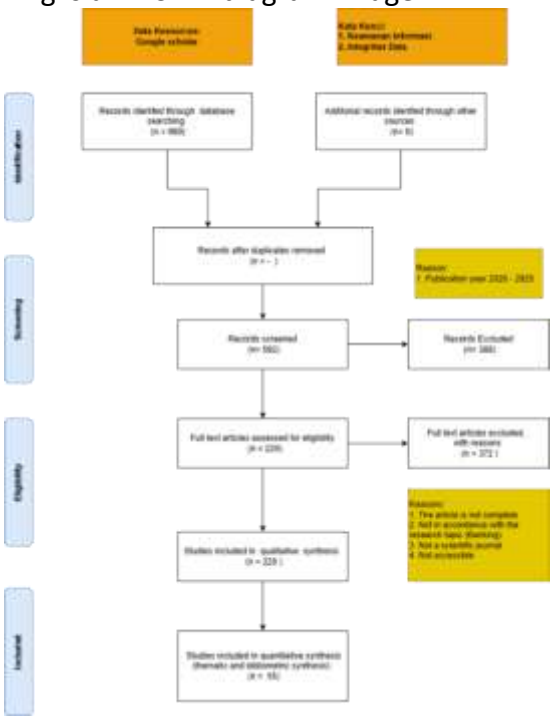


Figure 1. PRISMA DIAGRAM

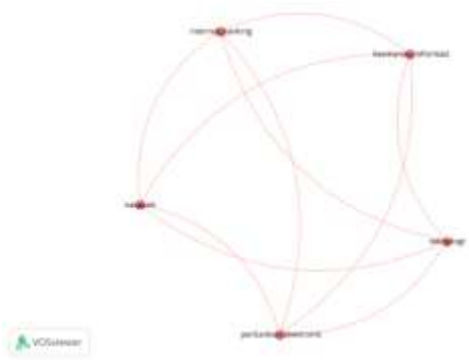
P-ISSN 2828-4976
E-ISSN 2808-263X

From the PRISMA flow diagram, 55 journals have been obtained that will proceed to the next stage, namely bibliometric analysis using VOSViewer and thematic analysis. From the 55 journals, it has been confirmed by the researcher that these journals have met the inclusion criteria and are in accordance with the research topic.

Result and Discussion

Co-Occurance Visualization Analysis

This analysis aims to identify the most frequently appearing keywords and their relationship to each other in scientific publications. Using VOSviewer software, this visualization provides a graphical representation of the thematic relationships that are built based on the frequency of co-occurrence of keywords in the analyzed documents.



Source : Processed data (2025)
Figure 1Co-Occurance Visualization

Visualization in Figure 2. Co-Occurrence Visualization has shown the results of *co-occurrence analysis* using VOSviewer software, which illustrates the relationship between keywords that often appear together in the analyzed documents. There are six main keywords identified, namely *internet banking* , *information security* , *technology* , *electronic banking* , and *customers* . Each keyword is represented in the form of a node , where the size of the node indicates the frequency of its occurrence. Meanwhile, the connecting line between nodes (*edge*) indicates a relationship or connection based on co-occurrence in one document, which in this context describes the thematic relationship between one concept and another.

The keyword *internet banking* occupies a central position in the network, because it has high connectivity with other keywords, such as *information security* , *customers* , *technology* , and *electronic banking* . This shows that *internet banking* is a major topic that is widely discussed in the related literature, and is closely related to issues such as information protection, technological developments, and customer experience and satisfaction. The keyword *information security* also has a strong relationship with *technology* and *customers* , indicating that the security aspect is a major concern in the development of digital banking services. In addition, *electronic banking* has a broad relationship with all other keywords, reflecting its role as an umbrella concept that covers various forms of digital services in the banking world, including *internet banking* itself.

Overall, this visualization shows that research in the field of digital banking, especially *internet banking* , is multidisciplinary, combining aspects of technology, information security, and customer service. The strong relationship between keywords indicates that each concept is interrelated and forms a comprehensive study framework in understanding the dynamics of digital-based banking services. These findings also provide an in-depth understanding of the developing research focus, and can be a basis for formulating policy directions or developing a safer electronic banking system that is oriented towards customer satisfaction.

In addition to providing a thematic overview, the results of this *co-occurrence analysis* can also be used to identify dominant focuses and potential research gaps *that* can still be explored further. For example, although keywords such as *technology* and *information security* already have a significant relationship with *internet banking* , there has been no deeper exploration of further issues such as *user experience* , *trust* , or *cyber threat mitigation* which are also relevant in the digital banking ecosystem. This suggests that future research can be directed to integrating aspects of user behavior and a more comprehensive security approach, especially in facing new challenges such as cyber attacks and the development of AI-based technology in banking services.

Furthermore, this analysis also has important practical implications for the banking industry. The finding that *customers* are nodes that are directly related to almost all of the main keywords indicates that the user or customer perspective is a central factor in the development of *internet banking services* . Therefore, banks need to pay attention to factors that influence customer trust and comfort in using digital services, such as personal data security, ease of access, and the reliability of the technology used. Thus, *co-occurrence visualization* not only functions as a bibliometric analysis tool, but also as a strategic basis for formulating policies and innovations in information technology-based banking services.

Co-Authorship Visualization Analysis

Therefore, a *co-authorship analysis is carried out* , which aims to identify patterns of scientific collaboration between authors in research related to the topic being studied. VOSviewer is used to visualize this collaborative network, by showing which authors frequently collaborate and how they are related.

Source : Processed data (2025)
Figure 2Visualization of Co-Authorship

Figure 3. Co-Authorship Visualization has displayed a visualization of the *co-authorship network* or author collaboration which was also generated using VOSviewer. In this visualization, each node represents an author, and the connecting lines indicate the existence of a collaborative relationship in one or more co-authored documents. There are five authors

P-ISSN 2828-4976
E-ISSN 2808-263X

identified as having collaborative relationships, namely: Herdianto, Tedi; Febri Syawaludin, Dwi; Oga Laksana, Medika; and Elan Maulani, Isma.

From the visualization, it can be seen that the collaboration structure between authors is still relatively simple and not too complex. There is one main group that is connected through collaborative channels, but there has not been a large or strong cross-disciplinary collaboration *cluster* . This shows that although there is cooperation between authors, it is still limited and tends to be centralized in a small scope or certain institutions.

The strongest collaboration is seen between Herdianto, Tedi with other authors such as Febri Syawaludin, Dwi and Oga Laksana, Medika, indicating that Herdianto plays an important role as a liaison in this scientific writing network. Meanwhile, authors Elan Maulani, Isma are in a more separate position but remain connected through relationships with other authors, reflecting collaboration across small groups.

These findings have several important implications. First, this *co-authorship analysis* shows that there is room for strengthening collaboration between researchers, especially in increasing joint publications that are cross-institutional and multidisciplinary. Second, broader collaboration can increase the richness of perspectives in research, as well as expand academic networks that have an impact on the quality and visibility of scientific publications. Therefore, encouraging synergy between authors is an important strategy in developing strategic research in the fields of technology and digital banking.

Implications of Findings

The results of the data visualization analysis using VOSviewer in the previous sub-chapter provide a number of significant implications, both in academic and practical contexts. From an academic perspective, these findings strengthen the understanding of the focus of emerging studies in the literature on digital banking, especially on topics such as internet banking, information security, and technology. The close relationship between these keywords indicates that research in this field is interdisciplinary and requires a holistic approach, covering technical, managerial, and consumer behavior aspects. Therefore, researchers need to consider the integration of various scientific perspectives, such as information technology, security systems, risk management, and organizational and consumer behavior in developing a framework for further research.

In a practical context, the results of this visualization provide a clear picture to banking industry players that information security issues and the use of technology are not just supporting aspects, but are core components of customer-oriented digital banking services. Successful internet banking services are those that are able to align security, ease of access, and user experience simultaneously. Therefore, the strategic implication of this finding is the need to strengthen technological infrastructure and improve cybersecurity systems to maintain customer trust, while encouraging wider adoption of digital services.

Meanwhile, the analysis of collaboration between authors also has implications for the research ecosystem. The lack of a broad collaborative network indicates the need for increased interaction and cooperation between researchers from various institutions and disciplines. Cross-institutional collaboration can be a means to produce more comprehensive, high-impact research, and contribute to the development of innovative theories and practical solutions in facing the challenges of digital banking in an era of increasingly complex technology. Therefore, encouraging scientific collaboration and strengthening the research community is an important strategy to develop science in this field sustainably.

Qualitative Thematic Analysis

As a complement to the quantitative analysis in the form of bibliometric visualization and author networks, this study also implements a qualitative approach through thematic analysis using Taguette software. This tool allows researchers to mark and group text sections from scientific articles into a number of themes based on similarities in meaning and issues contained. Thematic analysis aims to reveal hidden or deep meanings from textual data that has been collected and reviewed.

Table 1. Article Tagging

tags	content
Firewall & IDS	developing Secure Integration Model based on OAuth 2.0, Greybox penetration testing, Cryptography, cloud computing, Sangfor Cyber Command
Encryption & Authentication	AES-256 encryption, Unique Code tokenization, Vigenere cipher
Cyber Threats	data theft, transaction manipulation, credential abuse, malware attacks, phishing, and insider threats, ransomware attacks
Blockchain Technology	blockchain technology
Customer Data Security	Consumer Protection Act (UUPK)

Source : Processed data (2025)

Through the process of *highlighting* and *coding* , five main themes were obtained that represent central issues in the study of information security and digital technology in the banking sector. The following is an explanation of each theme:

1. Firewall & Intrusion Detection System (IDS)

This theme covers content related to system defense technology from external attacks, such as the use of the OAuth 2.0 model, *Greybox penetration testing techniques* , *cryptography* , *cloud computing* , and the implementation of the *Sangfor Cyber Command system* . This tag emphasizes devices and methods of active protection of information systems from external threats.

2. Encryption & Authentication

This theme covers various data security techniques such as AES-256 encryption, *Unique Code tokenization* , and *Vigenère cipher* . The main focus of this theme is on how data is encrypted and authenticated to maintain its integrity and confidentiality in the digital transaction process.

3. Cyber Threats

This theme covers important issues such as *data theft* , *transaction manipulation* , *credential abuse* , to malware-based attacks , *phishing,* and *ransomware* . This theme highlights various types of attacks and vulnerabilities that pose a threat to the digital ecosystem.

4. Blockchain Technology

This tag indicates a focus on *blockchain technology* as a potential solution in financial systems and data security, offering transparency, integrity, and decentralization of data.

P-ISSN 2828-4976
E-ISSN 2808-263X

5. Customer Data Security

This theme covers aspects of regulation and protection of consumers or users of the banking system, as reflected in the quote regarding *the Consumer Protection Law (UUPK)* . This aspect emphasizes the importance of governance and compliance with the rule of law in guaranteeing user rights.

The findings of this analysis show that the issue of information security and digital technology in banking has a variety of focuses, ranging from the technical side such as encryption and firewalls, to socio-legal aspects such as user data protection. This shows that a multidisciplinary approach is very important in responding to information security challenges in today's digital era.

Thus, this qualitative thematic analysis successfully provides a strong initial mapping of relevant content, while supporting the results of the visualization of co-occurrence and co-authorship that have been discussed previously. The integration of quantitative and qualitative approaches strengthens the final conclusions of the study, and provides a more focused direction for further research development.

Conclusion

This study aims to evaluate the trends and focus of research related to information security in the digital banking sector through a bibliometric approach and thematic analysis. Based on the results of the bibliometric analysis using VOSviewer software, two main visualizations were obtained, namely the analysis of co-occurrence keywords and the analysis of the author collaboration network (co-authorship).

From the analysis of co-occurrence keywords, it was found that there were only a small number of keywords that often appeared and were interconnected. Keywords such as internet banking, customers, technology, electronic banking, and information security formed a simple network with connectivity that was not too complex. This shows that themes related to information security in the banking sector have not yet become the main focus in previous studies in a broad and in-depth manner.

Furthermore, the results of the co-authorship visualization show that the collaboration network between researchers is still limited. There are several groups of authors working in small teams, but there has been no significant collaboration between these groups, either in terms of number or diversity of institutions or geographic areas. This indicates that there are not many research communities that are organized and consistently developing studies on information security in the banking sector.

To strengthen the findings, a qualitative thematic analysis was also conducted using the Taguette tool. From the tagging results, five main themes were obtained: (1) Firewall & Intrusion Detection System (IDS), (2) Encryption & Authentication, (3) Cyber Threats, (4) Blockchain Technology, and (5) Customer Data Security. These themes show that the research focuses more on the technical aspects of information security, such as AES-256 encryption, tokenization, cryptography, and system penetration testing (greybox testing). However, non-technical themes such as legal aspects, regulations, customer education, and organizational risk management have not yet emerged significantly.

The combined results of this bibliometric and thematic analysis reinforce the conclusion that research on information security in digital banking is still limited, both in terms of quantity, range of themes, and academic collaboration. Thus, this topic holds great potential

for further exploration, especially in the face of increasing cyber threats to the digital financial industry.

Suggestion

Based on the results of the bibliometric and thematic analysis that has been conducted, there are several suggestions that can be put forward for further research development. First, future research is suggested to expand the focus of the study, not only limited to technical aspects such as firewalls, encryption, and intrusion detection systems, but also include other strategic dimensions such as information security governance, data protection policies, security education for customers, and more comprehensive risk analysis. This is important considering the complexity of information security challenges in the digital banking industry which are not only technical, but also involve social, legal, and managerial aspects.

Second, collaboration between researchers needs to be strengthened, both nationally and internationally. The results of the co-authorship analysis show that the connectivity between authors is still limited and small-group in nature. Therefore, encouragement is needed to form a broader and more inclusive research network, which is able to bring together academics from various institutions and disciplines to explore information security issues in the financial sector more systematically. This collaboration can also be expanded by involving industry practitioners, regulatory institutions, and information technology solution providers so that the research produced is more applicable and relevant to the needs in the field.

Third, the use of the latest technology in banking information security systems needs to be further explored in future research. Technologies such as blockchain, artificial intelligence, and biometric authentication have great potential in strengthening digital security systems that are more adaptive to various types of threats. In addition, a multidisciplinary research approach needs to be encouraged so that information security issues can be studied holistically, involving technological, legal, social, economic, and public policy aspects.

By combining these approaches, it is hoped that future research can provide a more meaningful contribution in building a digital banking information security system that is robust, sustainable, and responsive to developments in the era.

References

Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2024). Information security risk assessment methods in cloud computing: Comprehensive review. *Journal of Computer Information …*. https://doi.org/10.1080/08874417.2024.2329985

Alkadrie, S. A. (2024). Keamanan Cloud Computing di Era Industri 4.0: Systematic Literature Review. *KONSTELASI: Konvergensi Teknologi Dan Sistem …*. https://ojs.uajy.ac.id/index.php/konstelasi/article/view/10277

Almadira, A., Pratama, Y., & Purwani, F. (2024). MELINDUNGI DATA DI DUNIA DIGITAL: PERAN STATEGIS ENKRIPSI DALAM KEAMANAN DATA. *Journal of Scientech Research and …*. https://www.idm.or.id/JSCR/index.php/JSCR/article/view/608

Alonge, E. O., Eyo-Udo, N. L., Ubanadu, B. C., & ... (2024). Developing an Advanced Machine Learning Decision-Making Model for Banking: Balancing Risk, Speed, and Precision in Credit Assessments. In *Journal details …*. researchgate.net. https://www.researchgate.net/profile/Enoch-Alonge/publication/390165834_Real-Time_Data_Analytics_for_Enhancing_Supply_Chain_Efficiency/links/67e3f71c35f7044c

P-ISSN 2828-4976
E-ISSN 2808-263X

9288b0c8/Real-Time-Data-Analytics-for-Enhancing-Supply-Chain-Efficiency.pdf

Aziza, N., & Wardhani, D. F. (2025). Evaluasi Keamanan Aplikasi Mobile Banking: Ancaman, Perlindungan dan Studi Kasus Pada Sistem Perbankan Digital. *Jurnal Ilmiah Teknologi Informasi Dan …*. https://jifti.upnjatim.ac.id/index.php/jifti/article/view/184

Febriyanto, G. A., Purnamasari, S. R., & ... (2023). Penertiban Dokumen Kredit Dalam Meminimalisir Risiko Kehilangan Data Nasabah Di Bank Bri Unit Wirolegi Jember. *EJOIN: Jurnal …*. https://ejournal.nusantaraglobal.ac.id/index.php/ejoin/article/view/1607

Ha-Kyung, Y. O. U. (2025). The Prisma Statement Analysis: Research on the Key Elements of Information Security Standard. *The Journal of Industrial Distribution &Business*. https://koreascience.kr/article/JAKO202513432402517.page

Hassandi, I., & Pangestu, M. G. (2025). Identifikasi Resiko Dalam Era Digital: Studi Kasus Resiko Teknologi Pada PT Bank Syariah Indonesia. *Jurnal Manajemen Teknologi …*. https://ejournal.unama.ac.id/index.php/jms/article/view/1997

Hutapea, Y., Fauzi, A., Dwiyanti, A., Alifah, F. A., & ... (2024). Peran Manajemen Sekuriti Dalam Mencegah Resiko Kerugian Terhadap Keuangan Digital. *… Dan Multi Talenta*. https://siberpublisher.org/index.php/JKMT/article/view/162

IBM X-Force. (2022).

Kurniawan, R., Septiono, T. R., & Saputra, D. A. R. (n.d.). Analisis Pengaruh Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking BRI. In *ojs.udb.ac.id*. https://ojs.udb.ac.id/index.php/Senatib/article/view/4644/3101

Lame, G. (2019). Systematic literature reviews: An introduction. *Proceedings of the International Conference on Engineering Design, ICED*, *2019-August*(August), 1633–1642. https://doi.org/10.1017/dsi.2019.169

Mishra, V., & Mishra, M. P. (2023). Prisma for Review of Management Literature – Method, Merits, and Limitations – an Academic Review. *Review of Management Literature*, *2*, 125–136. https://doi.org/10.1108/S2754-586520230000002007

Mujahidah, N., Raudhah, P. N., & ... (2025). Responsibility Accounting Di Era Digital: Tantangan Dan Peluang Dalam Manajemen Modern. *Jurnal Semesta …*. https://jurnalpustakacendekia.com/index.php/J-SIME/article/view/410

Munira, M. S. K. (2025). … THE INFLUENCE OF CYBERSECURITY THREATS AND RISKS ON THE ADOPTION AND GROWTH OF DIGITAL BANKING: A SYSTEMATIC LITERATURE REVIEW. *Available at SSRN 5229868*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5229868

Nurhaliza, S., Ningsih, A. S., & ... (2025). KEAMANAN DATA NASABAH BANK SYARIAH. *Jurnal …*. https://ejurnal.kampusakademik.co.id/index.php/jmia/article/view/3907

Restika, R., & Sonita, E. (2023). Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah: Menjaga Stabilitas Keuangan Di Era Digital. *Krigan: Journal of Management …*. http://ejournal.uinbukittinggi.ac.id/index.php/krigan/article/view/7929

Saputri, C. S., & Zulkarnain, Z. (2024). Dampak Teknologi Informasi Mengenai Proses Audit: Teknologi Informasi. *Jurnal Teknik …*. https://ejurnal.politeknikpratama.ac.id/index.php/jtmei/article/view/3206

Sianturi, C. G. P., Nababan, R., & Siregar, R. J. (2024). Peran Hukum Dalam Melindungi Data Pribadi. *Innovative: Journal Of Social …*. http://j-innovative.org/index.php/Innovative/article/view/15192

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum*. https://journal.undiknas.ac.id/index.php/JAH/article/view/4484

Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*. http://jurnal.kemendagri.go.id/index.php/jskp/article/view/1682

Wahana, A. (2025). Peran Teknologi Transparansi dan Keamanan dalam Ekonomi 5.0 pada Blockchain. *Indonesian Research Journal on Education*. http://irje.org/irje/article/view/2322

Wisuda, S. (2022). Perlindungan Hukum Konsumen Pengguna e-Banking: Ditinjau dari Undang-Undang Perlindungan Konsumen dan Undang-Undang Perbankan. In *MLJ Merdeka Law Journal*. pdfs.semanticscholar.org. https://pdfs.semanticscholar.org/8557/be17fc99c9e8b6ad66462e356e6f7c272a0c.pdf

Zhang, J., Tan, R., Su, C., & Si, W. (2020). Design and application of a personal credit information sharing platform based on consortium blockchain. *Journal of Information Security and …*. https://www.sciencedirect.com/science/article/pii/S2214212620308139