Inter-Organizational Data Sharing: What Issues Should Be Considered?

1st Dewi Puspasari
Computer Science Faculty
Universitas Indonesia
Depok, Indonesia
dewi.puspasari81@ui.ac.id

2nd Ahmad Nizar Hadiyanto
Computer Science Faculty
Universitas Indonesia
Depok, Indonesia
nizar@cs.ui.ac.id

3rd Suryana Setiawan
Computer Science Faculty
Universitas Indonesia
Depok, Indonesia
setiawan@cs.ui.ac.id

2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS) | 978-1-6654-2733-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICIMCIS53775.2021.9699333

***Abstract*—Currently, data sharing activities between agencies have been done in many ways. This provides benefits but behind it there are also threats. Therefore, we explore what needs to be considered in sharing current data based on previously published research results. This research was conducted with a systematic literature review approach to 34 articles entered in the Scopus electronic database in 2017-2021. From the results of this study, we then propose six domains that need to be considered when sharing data, namely Security; access control; data privacy; confidentiality, integrity, and availability of data; compliance and trust; also data audit capabilities.**

Keywords—data sharing, systematic literature review, data sharing consideration

I. INTRODUCTION

In this data age and the connectivity era, data sharing cannot be avoided. A data that is owned by an organization, maybe data that is also needed by various other organizations as a basis for decision making. Population data, for example, it becomes input data for social security data, data on projections for food supply needs, and so on. Therefore, data owned by organization, especially current government institutions, are rarely only exclusively owned by these organizations, but are also needed by other organizations.

The importance of this data sharing was tested during this covid-19 pandemic[1]. Some people think that there is a lot of data from various sources that are not in sync with each other, making it difficult to handle and make decisions during this pandemic.

Data sharing is a data exchange process where data formats are open and available, as well as known process patterns and standards. Thus, organizations or individuals who have the right to access it can use the data and metadata [2].

Along connectivity with the internet and applications that support interoperability, organizations are increasingly easier to exchange data or use shared data. They also can use cloud storage that can be accessed by various organizations by applying layered access methods, and so on.

However, beyond these benefits, there are threats that lurk. A common problem when sharing data is related to the lack of control over the data, namely issues of security, accountability, data privacy and data integrity [3]–[7]. Another problem is the presence of certain parties that are not invited, who can manipulate data and the user activities that are not recorded well [5], [8]–[10].

At this time, data sharing technology continues to expand following the development of digital technology. The data sharing process is also faster and can involve more parties [11], [12]. The threat can be more diverse. With these numerous threats, there are varied things that need to be considered when two or more organizations agree to share and exchange data. [5], [10], [13].

Research on data sharing continues to grow, but no one specifically discusses what factors still need to be considered when sharing data between units in organizations or inter-organizations. Therefore in this study, there are several problems that we want to explore with a explanatory method with systematic literature review approach. We have made only one question, because we believe that in the course of conducting this research, other issues will be found that enrich the results of this study. The research question of this study is "What are the issues that are still need consideration around data sharing activities?"

To make it easier for readers to get an overview of the results of this study, we begin this paper with an abstract which is a summary of the paper, an introduction that contains our background to do the research and research questions that we set. Then, we review related works. In the next section, we describe in detail the research methodology that we are doing and the results we have obtained. From the analysis of the results, we then conclude and propose the future work.

II. RELATED WORKS

Research using the systematic literature review (SLR) method has now been carried out. Initially, this method was widely used in the realm of medicine and health, before then it was used in various fields of science. This research method is suitable for explanatory preliminary research, to find out trends in research in a scientific discipline or to identify and interpret the results of state of the art on a topic [14].

SLR according to [15], is one form of secondary study by conducting a series of activities, ranging from identification, analysis, and interpretation of all the evidence obtained associated with certain research questions that are not biased and the stages can be repeated. Whereas according to [16], SLR is a literature review method that identifies, assesses, and interprets all findings on a research topic, to answer previously defined research questions.

This method is necessary for those who want to know the latest issues conveyed by various researchers in a field and aim to synthesize these findings [14], [15]. This method also avoids researchers from subjectivity and bias.

In the field of information systems, the SLR method also began to be widely used, including in the field of data governance. The research conducted by [17] findings the distinguish between traditional data governance where data is stored on company servers and cloud data governance.

A. Majid [17] conducted a literature review of papers and journals that have been published in the field of data governance since 2007. After conducting a series of screening, 52 study results were found that met the criteria. After

conducting a study and synthesis of 52 study results it was found that there were similarities and differences between non-cloud (traditional) data governance and those using cloud data governance.

The similar from both are discussing policy and process, also technology. The difference is that traditional data governance in addition to the two domains only addresses people and organizational bodies. While, cloud data governance discusses eight other domains, namely data governance structures, cloud deployment models, service delivery models, cloud actors, organizational, service level agreements, monitor matrices, and legal contexts.

III. METHODOLOGY

In this paper, we conduct explanatory research using the systematic literature review (SLR) method proposed by Kitchenham [14]. The selection using the SLR method is because the research we conducted aims to find out the latest issues about data sharing activities, given that the information technology sector continues to grow. By doing SLR, we hope to get a state of the art from the results of research that has been done for data sharing topics that are part of data management [14], [15].

Because our research question is to find state of the art from current issues related to data sharing, we use the term "data sharing" when conducting SLRs on published research results. This data sharing is more focused on sharing and exchanging data carried out by an institution or organization, not by individuals.

In this study we conducted a literature review of the results of publications in the Scopus electronic database. Our literature search comes from conference proceedings and book chapters. Based on the search, it was found that research in the data sharing domain was quite popular with the number of publications recorded on Scopus reaching 112.534. The amount of research for this topic has increased since 1990 with 325 articles. The increase in research on this topic is increasingly visible after 2010. In 2010 there were 4.340 results of research indexed by Scopus and the number continued to increase with a peak in 2020, namely 10.418. In 2021 there were 6.461 published research results. The number of publications can be seen in Fig. 1.

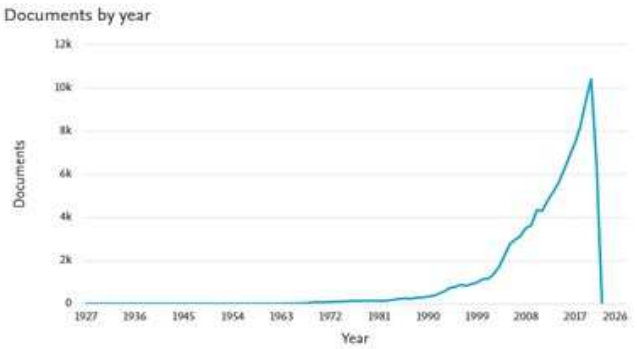

Fig. 1. The Number of Publications on Data Sharing in Scopus Based on Issuance Year

This SLR process then is carried by providing various criteria and limitations. We then conduct a search and screening process by determining the criteria for inclusion and exclusion as seen in Table I. We choose data sharing that is applied in organizations in the form of the latest publications, based on 2017-2021. Furthermore, we conducted screening, only selecting English-language publications, the results of publications in the form of conference paper and book chapters, also were in the subject area of "computer science".

Next, screening for conference paper and book chapter is carried out, and based on 2017-2021, so that 10.389 is filtered. We do keyword filtering in the form of "data sharing" to 1.603 results of publication. From this amount, the first filter is carried out in the form of a title. From this screening process 145 articles were produced.

TABLE I. CRITERIA FOR INCLUSION AND EXCEPTIONS IN SLRS

Entry Criteria Publication	Exclusion Criteria
Data sharing activities are implemented in the organization or multi-organizations	Not relevant, for example data sharing activities per individual
2017-2021 range	Duplicated publication
Written in English	Not written in English
Publications in the form of conference papers and book chapters	Lecture note, and publications cannot be accessed online with institutional access.
Being in the subject area of computer science	

The next iteration is selection based on abstract, obtained 63 articles. In the fourth iteration is done by reading the contents of the results of the publication one by one. This stage produced 34 published studies. The stages of SLR can be seen in the Fig.2.

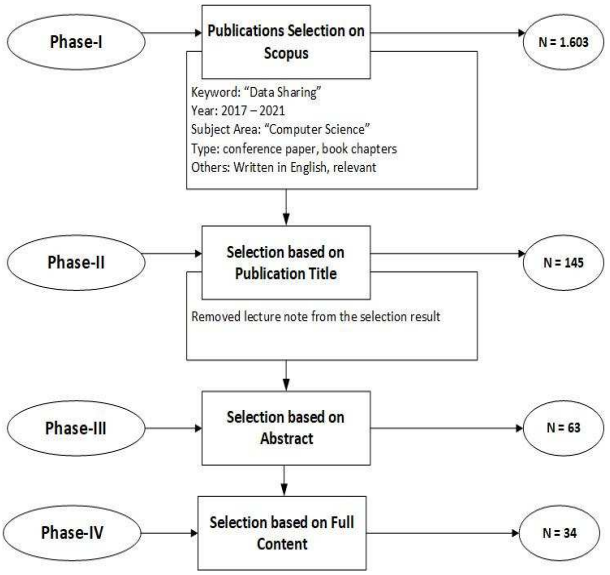

Fig. 2. Stages of the Systematic Literature Review

IV. RESULT

This section describes the description of demographics and the results of an analysis of 34 articles obtained from the process of a systematic literature review. Most of the articles, 17 paper (50%) were published in 2020, followed by 7 publications in 2021 (20,6%), then 5 publications in 2019 (14,7%), 3 publications in 2018 (8,8%), and 2017 as many as 2 publications (5,9%).

Of the 34 publications all in the form of proceeding papers. Based on research data, it is seen that quite a lot of research in the field of health, namely eight papers (23,5%), others in the field of agriculture, energy, advertising, government sector, and so on. The amount of research in the health field is also

influenced by the global pandemic situation and more and more are aware of the importance of patient data privacy [8], [11].

With the proliferation of cryptocurrency, blockchain technology which was initially widely used by financial transaction then began to be widely used in other fields, especially the field of healthcare [1], [18], [19]. This technology is believed to have many advantages over just storing and sharing data through the cloud [3]. Therefore, here we find many papers with specific topics leading to the blockchain that is 16 papers (47,5%). While only five papers (14,7%) specifically discuss cloud technology. Other papers do not explicitly mention the technology and location of data storage.

In addition to technology, other topics discussed related to security, namely access control and authentication mechanism; encryption; data privacy, compliance, and other topics, such as data sharing agreements and trust, data; auditability and traceability; also data confidentiality. integrity and availability. One paper can consist of two or more discussion topics, such as encryption also discussed in the cloud environment. After we categorized the issues, then we synthesize them. Matters that are issues in each category/subcategory will be summarized can be seen in Table II.

A. Data Sharing Issue Related Technology and Storage Location

Technology related to data sharing is very diverse. Nowadays the popular technology is blockchain. The technology is also began to be widely used in various sectors, not just financial transactions [5], [8]–[11], [18]–[25]. As for data sharing storage, more and more people are using cloud systems [6], [7], [13], [26], [27].

B. Blockchain

Blockchain technology was initially widely used in finance because it was considered more secure, then began to be widely applied in healthcare and other fields transactions [5], [8]–[11], [18]–[25], [28]. This technology has the advantages of maintaining data integrity, minimizing security risks and data loss, ease of search, protecting data privacy, protecting data confidentiality, data access control, user data privacy, and data availability [3], [20], [29].

Despite having many advantages, there are still issues related to this technology. The issues are a matter of trust, data privacy, data confidentiality, data agreement, authentication, of users relating to access control policies with the abundant conditions of transaction data [3], [8], [9], [11], [18], [19], [21]–[25], [30]. For that there are a variety of solutions offered, namely using anonymous identities to ensure user data privacy [9], maintaining access control and authentication mechanisms [10], increasing trust and maintaining data agreement among organizations and users of the system [23], [24]. Paper [8] develop risk model with four scenarios to avoid the vulnerability in authentication mechanism.Whereas, paper [24], [25] suggest use a privacy preserving blockchain based data sharing platform for InterPlenary File System.

C. Cloud Storage

Cloud is an alternative storage media that is currently widely used by organizations. More and more organizations are now storing and sharing data in the cloud [6], [7], [13], [26], [27]. This is because cloud storage provides advantages in sharing data, namely from the side of interoperability, saving costs, and can be used to share data with various remote organizations [6], [7]

However, there is concern that the owner has lost his physical control and that there are cloud providers that cannot be trusted, allowing data leakage to occur [6], [7].

Therefore, the main challenge of sharing data in a cloud environment is how to secure and share data efficiently and maintain access control on the data, so that it is clear who can access data with dynamic membership [6], [26]. The system should also have a trace element and monitor compliance mechanism [6].

To address the issue, it is proposed to use group signature, ciphertext-policy attribute-based encryption and broadcast encryption, which supports both intra-group and cross-group data sharing with anonymous access [7].

D. Data Sharing Issue Related to Security

Data security is an important element in data sharing. This is also referred to in the previous category with regard to storage in the cloud, and also systems with blockchain.

E. Access Control & Authentication Mechanism

The issue of access rights is also considered in collaborative cloud and blockchain technology. This is because there is concern of an unauthorized user [1], [8], [10], [19], [24]–[26], [28], [30]. Paper [8] propose password can be using pictorial and authenticating user can be use Flexxpass with multi-factor authentication (mFA). The define of access rule also significant. Paper [10] sugest a blockchain-based multidimensial user authorization and role based access control mechanism. While the paper suggests to use Kerberos based time to live [26] to improve the performance of the authentication mechanism.

F. Encryption Method

Sharing data, especially in the cloud environment, has risks especially for protect data confidentiality[4], [7], [18], [25], [28], [30], [31]. There is concern and lack of trust in third-party providers, so it is feared that important and privacy data is leaked in the hands of those who do not have access rights [1], [30].

With the various risks, a variety of methods for encryption are proposed. Paper [4] suggest to maintain confidentiality over the transmission combination steganography using genetic algorithm and visual crytography using pseudorandom number. Paper [19], [30] propose uses identity-based proxy reencryption technology and distributed key generation technology. Other suggest ciphertext-policy attribute-based encryption and broadcast encryption [7]. While paper [26] suggests a cloud system using elliptic curve cryptography with a secure hashing algorithm.

G. Other Security Issues

Security issues are generally about access control and authentication mechanisms. However, we also need other security systems such as behavior monitor systems to detect if there is an attack, as well as physical security. In the paper a unified model is proposed to improve security and improve the performance of mission-critical cloud systems [6]. Paper [23] propose a secure design that first stores order forms in

Distributed Database, after that UI records in Contract Account.

H. Data Privacy

The issue of data privacy is increasingly important, especially with the load of digital applications and the current pandemic conditions where patient data in medical systems and user private data in other systems are prone to misuse [5], [8], [9], [11], [22], [24]. This is also supported by the application of the General Data Protection Regulation (GDPR) in the European Union [32], [33].

Paper [11] propose design two different sharing protocols and blockchain based multi-role healthcare data sharing system to manage data privacy. Paper [9] suggest to use anonymous identities to ensure user's privacy.

I. Policy and Compliance

The implementation of policies such as private data sharing policies is necessary because the protection of data privacy is required in the GDPR [32], [33]. Any organization that manages and shares data must comply with these policies and rules. Policy can also be born from the points of agreement of groups involved in the data sharing process [12], [28], [34], [35].

However, there are challenges in translating and lowering high-level sharing policies into infrastructure architectures so that data sharing platforms are secure [34], [36].

J. Other Issues

There are also other issues that are issues in the data sharing process. These are related to trust and data sharing agreement; data confidentiality, integrity, and availability; and data auditability & traceablity. Following the results of each subcategory:

K. Trust & Data Sharing Agreement

Current data is generally shared between organizations. Current data sharing challenges include sensitive data, risk of privacy, data access, the purpose of sharing data between organizations. Therefore, it is necessary for the participating institution to agree on the points and translate them into an agreement or policy [35]. In addition, the content of the policy is known to all involved so that a trust emerges. [12], [23], [34], [36], [37].

L. Data Confidentiality, Integrity, and Availability

In data sharing, the concern is the loss of data, theft of sensitive data, or changes to unauthorized data [1], [3], [4], [11], [13], [18], [20], [24], [29]–[31], [38], [39]. For this, the security system on the data sharing platform is very important. Papers [1], [3], [21] propose a smart contract to anticipate this. Others propose modern encryption, two different sharing protocols [4], [11]. While the paper [24] proposed using the InterPlenary File System platform.

M. Traceability and Auditability

Audit plays an important role in keeping activities running in accordance with regulations, including in data sharing activities [10], [25]. Data such as health records are very important data, so it is natural that there will be concern when sharing data in a cloud environment to can be traced with the user that access them [1], [24].

TABLE II. SUMMARY OF EACH CATEGORY

Topic	Paper	Issues
Blockhain	[1], [3], [8]–[11], [18]–[25], [30]	Access control and authentication mechanisms are often mentioned still have gaps. In addition, the issue of data privacy must be considered. Blockchain is also expected to have audit mechanisms, traceability, and also protect data confidentiality and ensure data availability.
Cloud Storage	[6], [7], [13], [26]	There are still concerns about data confidentiality leaks and data privacy abuse, as well as data integrity issues and data confidentiality protection. Therefore, in the cloud, a good control mechanism is needed.
Security		
• Encryption	[1], [4], [7], [18], [19], [25], [26], [28], [30], [31]	Encryption is important to protect data confidentiality from unauthorized access.
• Access Control & Authentication	[1], [8], [10], [19], [24]–[26], [28], [30]	Need to identify the user's authority and provide access control in data sharing platform
• Other Issue	[6], [23]	About monitoring suspicious behavior and attacks
Data Privacy	[5], [8], [9], [11], [22], [24], [32], [33]	Since the implementation of the GDPR and the misuse of privacy data, privacy data has become a spotlight.
Policy & Compliance	[5], [28], [32]–[36]	Any organization that collects, manages, and shares data needs to comply with regulations and policies, including data privacy protection.
Other Issues		
• Trust & Data Sharing Agreement	[12], [23], [34]–[37]	Data agreements and trusts among members involved in the data sharing process are also grown. Trusts can also come through with a secure and trusted platform system.
• Data Confidentiality, Integrity, Availability	[1], [3], [4], [11], [13], [18], [20], [21], [24], [29]–[31], [38], [39]	Loss of data, theft of sensitive data, or changes to the data sharing platform are still worth noting even though the security technology is considered advanced.
• Traceability & Auditability	[1], [10], [24], [25]	Blockchain need to provide auditability and traceability mechanism.

From the summary results, it can be seen that there are several issues that are repeated and included in several categories, such as privacy, data confidentiality data integrity, and data availability, also access control. In addition, there are also other issues implicitly and explicitly important in each category that are important for governance in sharing data.

Manage access control is often alluded to in papers that discuss blockchain, cloud storage, also to protect data confidentiality, integrity, and availability. Manage access control is also related to encryption.

Protect data confidentiality, integrity, and availability has been discussed in blockchain, cloud storage, control access, and auditability & traceability. Then, security and infrastructure has been reviewed in cloud, encryption method, and blockchain topics.

Data sharing agreement has been discussed in data sharing agreement, trust, policy, and data privacy topics. Policy can be formed from the data agreement in addition to the regulations that must be complied with. But what is no less important is compliance with the regulations so that it creates trust.

While, protect data privacy is widely discussed in blockchain, cloud, access control, and policy. In addition, which is also widely discussed is auditability and traceability, which are also discussed in the blockchain. The results of this brainstorm can be seen in the Figure 3.

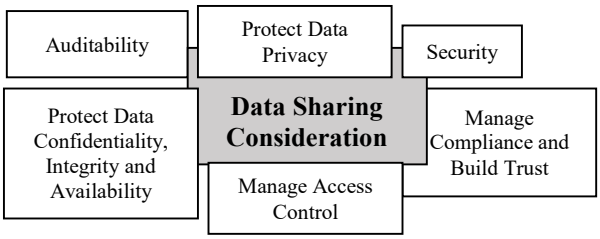

Fig. 3. Data Sharing Consideration

There are six domains that need to be considered in data sharing activities. Security includes encryption method, physical security and software to monitor abnormal behavior to ensure the organizations have secure data sharing channel. Since there could be a violation, it is necessary to manage access control using encryption methods to guarantee confidential data is safe. In addition, to ensure of the integrity, the parties must comply with the policy and and build trust relationship. Data sharing platforms also need to be audited periodically, if there are any suspicions a search needs to be done. In addition, no less important is the protection of data privacy.

V. Conclusion and Future Work

Currently data sharing activities are often carried out in organizations or between organizations. The platforms and technologies used in data sharing are diverse, such as blockchain and storage locations can also be distributed in a cloud environment. There are several causes of data sharing failure such as lack of trust in third party service providers, and data leakage cases.

Therefore in this study based on the SLR method, we carried out analysis and synthesis of 34 papers. We then propose six domains that need to be considered when sharing data, namely security; manage access access control; protect data confidentiality, integrity, and availability; protect data privacy; compliance and trust; and auditability.

In the future work, we will do case studies in meta-organizations for assesing data sharing activities.

References

[1] K. Christodoulou, P. Christodoulou, Z. Zinonos, E. G. Carayannis, and S. A. Chatzichristofis, "Health Information Exchange with Blockchain amid Covid-19-like Pandemics," Proc. - 16th Annu. Int. Conf. Distrib. Comput. Sens. Syst. DCOSS 2020, no. October, pp. 412–417, 2020.

[2] D. Sharing, I. G. I. Global, K. Pangan, D. Sh, B. Clouds, and H. Technologies, "InfoSci-OnDemand," pp. 6–8.

[3] S. Wang and J. Liu, "Blockchain Based Secure Data Sharing Model." IEEE 23th International Conference on Computer Supported Cooperative Work in Design, p. 6, 2021.

[4] H. Vig, G. D. Singh, T. Choudhury, and T. Sarkar, "An Efficient and Secured Data Sharing Approach through Image Transmission." 2021 International onference on Emerging Smart Computing and Informatics, p. 5, 2021.

[5] K. Martiny, L. Briesemeister, G. Denker, M. S. John, and R. Moore, "Protecting Privacy during a Pandemic Outbreak," ICISSP 2021 - Proc. 7th Int. Conf. Inf. Syst. Secur. Priv., no. Icissp, pp. 308–318, 2021.

[6] B. Bhargava, P. Angin, and R. Ranchal, "Privacy-Perserving Data Sharing and Adaptable Service Compositions in Mission-Critical Clouds." International Semantic Intelligence Conference, 2021.

[7] L. Rao, Qingqing Xie, and Hui Zhao, "Data Sharing for Multiple Groups with Privacy Preservation in The Cloud." 2020 International Conference on Internet of Things and Intelligent Applications, 2020.

[8] M. Banton, J. Bowles, A. Silvina, and T. Webber, "On the Benefits and Security Risks of a User-Centric Data Sharing Platform for Healthcare Provision," UMAP 2021 - Adjun. Publ. 29th ACM Conf. User Model. Adapt. Pers., no. grant 826278, pp. 351–356, 2021.

[9] M. U. Rahman, B. Fabrizio, and Laura Ricci, "Blockchain Smart Contract for Scalable Data Sharing in IoT: A Case Study of Smart Agriculture." 2020 IEEE Global Conference on Artificial Intelligence and Internet of Things, 2020.

[10] Y. Ding et al., "Blockchain Based Access Control Mechanism of Federated Data Sharing System." 2020 IEEE International Conference on Parallel & Distributed Processig with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking, 2020.

[11] Y. Yu, Q. Li, Q. Zhang, W. Hu, and S. Liu, "Blockchain-based Multi-role Healthcare Data Sharing System." 2020 IEEE International Conference on E-health Networking, Application & Services, 2020.

[12] X. Zhou et al., "Policy Enforcement for Secure and Trustworthy Data Sharing in Multi-domain Infrastructures." IEEE 14th International Conference on Big Data Science and Engineering, 2020.

[13] A. V. Deorankar and K. T. Khobragade, "A Review on Various Data Sharing Strategies for Privacy of Cloud Storage." Proceedings of The Fourth International Conference On Computing Methodologies and Communication, 2020.

[14] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering - A systematic literature review," Inf. Softw. Technol., vol. 51, no. 1, pp. 7–15, 2009.

[15] D. Friday, S. Ryan, R. Sridharan, and D. Collins, "Collaborative risk management: a systematic literature review," Int. J. Phys. Distrib. Logist. Manag., vol. 48, no. 3, pp. 231–253, 2018.

[16] R. Roller, J. Roes, and E. Verbree, "Benefits of linked data for interoperability during crisis management," Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci. - ISPRS Arch., vol. 40, no. 3W3, pp. 211–218, 2015.

[17] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "A systematic literature review of data governance and cloud data governance," Pers. Ubiquitous Comput., vol. c, pp. 1–21, 2018.

[18] Y. Rui-jun, H. Jin-bo, and C. Yan, "Design of Data Sharing Module Based on Medical Blockchain." ICIIBMS 2019 - 4th International Conference on Intelligent Informatics and Biomedical Sciences, 2019.

[19] H. A. Sudarsono, A., Yuliana, M., Darwito, "A Secure Data Sharing Using Identity-Base Encyption Scheme for e-Healthcare System." Proceeding - 2017 3rd International Conference on Science in Information Technology: Theory and Application of IT for Education, Industry and Society in Big Data Era, ICSITech 2017 2018-January, pp. 429-434, 2017.

[20] Y. Luo, J. Fan, C. Deng, Y. Li, Y. Zheng, and J. Ding, "Accountable Data Sharing Scheme Based on Blockchain and SGX." Proceedings - 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2019, 2019.

[21] L. Desai, Harsh Liu, Kevin Kantarcioglu, Murat Kagal, "Adjudicating Violations in Data Sharing Agreements Using Smart Contracts." Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data,

Blockchain, Computer and Information Technology, iThings/Gree, 2018.

[22] A. G. Alzahrani, A. Alenezi, H. F. Atlam, and G. Wills, "A Framework for Data Sharing Between Healthcare Providers Using Blockchain," IoTBDS 2020 - Proc. 5th Int. Conf. Internet Things, Big Data Secur., no. IoTBDS, pp. 349–358, 2020.

[23] G. Le, Q. Gu, Q. Jiang, and W. Lin, "TrustedChain: A Blockchain-based Data Sharing Scheme for Supply Chain." 2020 International Conference on Data Mining Workshops, 2020.

[24] V.-H. Hoang, E. Lehtihet, and Y. Ghamri-Doudane, "Privacy-Preserving Blockchain-Based Data Sharing Platform for Decentralized Storage Systems." IFIP, 2020.

[25] T. Chen, Y. Yu, and Z. Duan, "Data Access & Sharing Approach for Trade Documentations Based on Blockchain Technology." 2019 IEEE 3rd International Conference on Electronic Information Technology and Computer Engineering, EITCE 2019, 2018.

[26] S. Pachaghare and P. Patil, "Improving Authentication and Data Sharing Capabilities of Cloud using a Fusion of Kerberos and TTL-based Group Sharing." Proceedings of The Fifth International Conference on Communication and Electronics Sysems, 2020.

[27] "30-secure data sharing.pdf." .

[28] L. Lucking, Markus Manke, Raphael Schinle, Markus Kohout and W. Nickel, Stefan Stork, "Decentralized Patient-Centric Data Management for Sharing IoT Data Streams." 2020 International Conference on Omni-Layer Intelligent Systems, COINS 2020, 2020.

[29] S. Lin, X. Wang, N. Shaotao, W. Kou, and J. Du, "Research on The Sharing of Equipment Data Based on Blockchain." 6th International Conference on Smart Grid and Electrical Automation, 2021.

[30] Z. Su, H. Wang, H. Wang, and X. Shi, "A Financial Data Security Sharing Solution Based on Blockchain Technology and Proxy Re-encryption Technology," Proceedings of 2020 IEEE 3rd International Conference of Safe Production and Informatization, IICSPI 2020. pp. 462–465, 2020.

[31] K. Fan, Q. Pan, J. Wang, T. Liu, H. Li, and Y. Yang, "Cross-Domain based Data Sharing Scheme in Cooperative Edge Computing." Proceedings - 2018 IEEE International Conference on Edge Computing, EDGE 2018 - Part of the 2018 IEEE World Congress on Services, 2018.

[32] T. Urban, D. Tatang, M. Degeling, T. Holz, and N. Pohlmann, "Measuring The Impact of The GDPR on Data Sharing in Ad Networks," Proc. 15th ACM Asia Conf. Comput. Commun. Secur. ASIA CCS 2020, no. November 2019, pp. 222–235, 2020.

[33] Y. Nam, E. Shin, S. Lee, S. Jung, Y. Bae, and J. Kim, "Global-scale GDPR Compliant Data Sharing System." 2020 International Conference on Electronics, Information, and Communication, ICEIC 2020, 2020.

[34] S. Shakeri, L. Veen, and P. Grosso, "Evaluation of Container Overlays for Secure Data Sharing." 2020 IEEE 45th LCN Symposium of Emerging Topics in Networking, 2020.

[35] G. Costantino, F. Martinelli, I. Matteucci, and M. Petrocchi, "Efficient Detection of Conflicts in Data Sharing Agreements," Commun. Comput. Inf. Sci., vol. 867, no. June, pp. 148–172, 2018.

[36] E. Karafili, E. C. Lupu, A. Cullen, B. Williams, S. Arunkumar, and S. Calo, "Improving Data Sharing in Data Rich Environments," Proc. - 2017 IEEE Int. Conf. Big Data, Big Data 2017, vol. 2018–Janua, pp. 2998–3005, 2017.

[37] J. Gelhaar and B. Otto, "Challenges in the Emergence of Data Ecosystems," Proc. 24th Pacific Asia Conf. Inf. Syst. Inf. Syst. Futur. PACIS 2020, no. June, 2020.

[38] M. Sun, Y. Zhan, and X. Sun, "Analyzing The Cross-Sector Sharing of Government Data Based on the Niche Theory." Proceedings - 2019 IEEE 4th International Conference on Data Science in Cyberspace, DSC 2019, 2019.

[39] T. Nokkala, H. Salmela, and J. Toivonen, "Data Governance in Digital Platforms," 25th Am. Conf. Inf. Syst. AMCIS 2019, 2019.