Advances in Secure IoT Data Sharing

Other titles in Foundations and Trends® in Privacy and Security

Navigating the Soundscape of Deception: A Comprehensive Survey on Audio Deepfake Generation, Detection, and Future Horizons
Taiba Majid Wani, Syed Asif Ahmad Qadri, Farooq Ahmad Wani and Irene Amerini
ISBN: 978-1-63828-492-5

Reverse Engineering of Deceptions on Machine- and Human-Centric Attacks
Yuguang Yao, Xiao Guo, Vishal Asnani, Yifan Gong, Jiancheng Liu, Xue Lin, Xiaoming Liu and Sijia Liu
ISBN: 978-1-63828-340-9

Identifying and Mitigating the Security Risks of Generative AI
Clark Barrett, Brad Boyd, Elie Bursztein, Nicholas Carlini, Brad Chen, Jihye Choi, Amrita Roy Chowdhury, Mihai Christodorescu, Anupam Datta, Soheil Feizi, Kathleen Fisher, Tatsunori Hashimoto, Dan Hendrycks, Somesh Jha, Daniel Kang, Florian Kerschbaum, Eric Mitchell, John Mitchell, Zulfikar Ramzan, Khawaja Shams, Dawn Song, Ankur Taly and Diyi Yang
ISBN: 978-1-63828-312-6

Cybersecurity for Modern Smart Grid Against Emerging Threats
Daisuke Mashima, Yao Chen, Muhammad M. Roomi, Subhash Lakshminarayana and Deming Chen
ISBN: 978-1-63828-294-5

Advances in Secure IoT Data Sharing

Phu Nguyen
SINTEF
phu.nguyen@sintef.no

Arda Goknil
SINTEF
arda.goknil@sintef.no

Gencer Erdogan
SINTEF
gencer.erdogan@sintef.no

Shukun Tokas
SINTEF
shukun.tokas@sintef.no

Nicolas Ferry
Université Côte d'Azur
Nicolas.FERRY@univ-cotedazur.fr

Thanh Thao Thi Tran
DnB
thaotran98@hotmail.com

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Privacy and Security

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

P. Nguyen *et al.*. *Advances in Secure IoT Data Sharing*. Foundations and Trends® in Privacy and Security, vol. 7, no. 1, pp. 1–73, 2024.

ISBN: 978-1-63828-423-9

Foundations and Trends® in Privacy and Security

Volume 7, Issue 1, 2024

Editorial Scope

Foundations and Trends® in Privacy and Security publishes survey and tutorial articles in the following topics:

- Access control
- Accountability
- Anonymity
- Application security
- Artifical intelligence methods in security and privacy
- Authentication
- Big data analytics and privacy
- Cloud security
- Cyber-physical systems security and privacy
- Distributed systems security and privacy
- Embedded systems security and privacy
- Forensics
- Hardware security
- Human factors in security and privacy
- Information flow
- Intrusion detection
- Malware
- Metrics
- Mobile security and privacy
- Language-based security and privacy
- Network security
- Privacy-preserving systems
- Protocol security
- Security and privacy policies
- Security architectures
- System security
- Web security and privacy

Information for Librarians

Foundations and Trends® in Privacy and Security, 2024, Volume 7, 4 issues. ISSN paper version 2474-1558. ISSN online version 2474-1566. Also available as a combined paper and online subscription.

Contents

Advances in Secure IoT Data Sharing

Phu Nguyen[1], Arda Goknil[1], Gencer Erdogan[1], Shukun Tokas[1], Nicolas Ferry[2] and Thanh Thao Thi Tran[3]

[1] *SINTEF, Norway; phu.nguyen@sintef.no, arda.goknil@sintef.no, gencer.erdogan@sintef.no, shukun.tokas@sintef.no*
[2] *I3S/INRIA Kairos, Université Côte d'Azur, France; Nicolas.FERRY@univ-cotedazur.fr*
[3] *DnB, Norway; thaotran98@hotmail.com*

ABSTRACT

The proliferation of IoT devices on the Internet is currently in the billions, and projections anticipate that there will be 50 billion connected IoT devices in the IoT market by 2030. This rapid expansion will result in a substantial increase in data, which includes personal data, generated by these IoT devices. It is estimated that the data volume will reach 73.1 zettabytes by 2025. To fully realize the substantial benefits of the IoT, it is imperative to facilitate the responsible utilization and sharing of this data among various stakeholders. However, it is crucial to establish robust security and trust mechanisms to ensure data integrity and privacy during data sharing. Our objective is to summarize and assess the research efforts that address secure IoT data sharing. We systematically review the state-of-the-art techniques ensuring and preserving security in the IoT data-sharing environment through a systematic literature review (SLR) study. We pose three research questions, define selection

Phu Nguyen, Arda Goknil, Gencer Erdogan, Shukun Tokas, Nicolas Ferry and Thanh Thao Thi Tran (2024), "Advances in Secure IoT Data Sharing", Foundations and Trends® in Privacy and Security: Vol. 7, No. 1, pp 1–73. DOI: 10.1561/3300000042.

and exclusion criteria for primary studies, and extract and synthesize data from these studies to answer our research questions. Our SLR results can help readers to obtain (i) an overview of existing secure IoT data-sharing approaches and related issues, (ii) a deep-dive into Edge-focused secure IoT data sharing solutions, and (iii) research directions that require attention from the research community for follow-up work.

1

Introduction

In recent years, the Internet of Things (IoT) has achieved pervasive ubiquity, driven by its capacity to interconnect commonplace items such as automobiles, household appliances, and infant surveillance devices to the Internet, facilitating seamless communication across processes, individuals, and objects. At present, the global landscape boasts billions of IoT devices in active connection, and it is foreseen that the IoT market will witness the integration of 30 billion connected devices by 2023, as anticipated by Cisco (Grossetete, 2018). IoT technology empowers the creation of intelligent, interoperable entities encompassing both the digital and physical realms, individuals and services, and thereby giving rise to diverse ecosystems primed for secure cross-domain interactions.

Nonetheless, as the IoT ecosystem undergoes continued expansion and diversification, it renders the vast data reservoir vulnerable to various security and privacy risks. The inherently interconnected nature of IoT networks, coupled with the multifaceted spectrum of stakeholders engaged, has precipitated an urgent imperative for establishing resilient data management and governance protocols. The assurance of secure sharing and judicious utilization of data generated within the IoT framework assumes paramount significance in upholding the sanctity of sensitive information, encompassing aspects of confidentiality, integrity, and accessibility.

The management and governance of data sharing securely within the context of the Internet of Things (IoT) present challenges that are multifaceted. These challenges lie first in the intrinsic complexity and multifaceted nature of IoT systems. On the one hand, IoT systems typically perform distributed sensing, actuating, and processing across multiple layers composed of Thing, Edge, and Cloud resources. Things and Edge devices are operating in the midst of the physical world to sense and collect environmental data, including sensitive data. This creates novel opportunities for bad actors as (i) the devices can be physically accessible and (ii) it is not possible for security experts to anticipate all the possible environmental situations under which the system will operate. On the other hand, these challenges extend beyond the technical facets of data security, encompassing a rich tapestry of regulatory, ethical, and societal dimensions pertinent to data handling. The data generated by IoT systems may traverse organizational demarcations, transcend international borders, and become ensnared in a complex web of legal and compliance prerequisites. Furthermore, IoT ecosystems frequently comprise several stakeholders, ranging from device manufacturers to end-users, each carrying their unique entitlements and obligations about data.

Although several surveys study and classify research on secure IoT data sharing, they do not provide a detailed account and unified analysis of existing solutions (i.e., secure IoT data sharing techniques) for secure IoT data sharing research, the security and trust aspects of these solutions, and their limitations and potential future work (open issues to be further investigated). Few existing studies (Lo *et al.*, 2019; Al-Ruithe *et al.*, 2019; De Prieëlle *et al.*, 2020) have examined related topics of secure IoT data sharing such as data governance and blockchain solutions, but none has done a Systematic Literature Review (SLR) on secure IoT data sharing. We answer three main research questions (also detailed in sub research questions) to address the research on secure IoT data sharing for theoretical and practical implications.

- **RQ1:** *What is the current landscape of solutions for secure IoT data sharing in general?*

- **RQ2:** *What are the specific technical aspects of Edge-focused online IoT data sharing approaches?*
- **RQ3:** *What are the current limitations of the IoT data sharing, and what are the open issues to be further investigated?*

We follow a typical four-step SLR process (Kitchenham and Charters, 2007): (i) the definition of research questions, (ii) a search strategy including the selection of online repositories and search strings, (iii) inclusion and exclusion criteria, and (iv) a data synthesis and extraction procedure. This work is an extension of Tran *et al.* (2023). We conducted an extensive snowballing process (Wohlin, 2014) to enrich and update the list of primary studies. Moreover, with the importance of Edge computing, we deep-dived into the primary studies that have Edge-focused IoT data sharing approaches.

We analyzed the primary studies using our taxonomy of IoT data sharing to provide the answers to our three research questions. Following a top-down approach, we present first a high-level summary of our results. Then, we discuss in more detail the primary studies that have Edge-focused IoT data sharing approaches. Researchers can use this summary and the taxonomy to classify and compare future secure IoT data sharing studies.

The remainder of this monograph is structured as follows. We provide some background concepts in Section 2. Then, Section 3 gives the details of our approach and Section 4 shows our taxonomy for extracting data to answer our RQs. Next, we present the results of our SLR in Section 5. In Section 6, we discuss some possible threats to validity. We compare our study with related work in Section 7 and give our conclusions in Section 8.

References

Abbas, K., L. Tawalbeh, A. Rafiq, A. Muthanna, I. Elgendy, and A. Abd El-Latif. (2021). "Convergence of Blockchain and IoT for secure transportation systems in smart cities. Secur. Commun. Netw. 2021, 1–13 (2021)".

Akkaoui, R., X. Hei, and W. Cheng. (2020). "EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange". *IEEE Access*. 8: 113467–113486. DOI: 10.1109/ACCESS.2020.3003575.

Alaba, F. A., M. Othman, I. A. T. Hashem, and F. Alotaibi. (2017). "Internet of Things security: A survey". *Journal of Network and Computer Applications*. 88: 10–28.

Alshehri, S., O. Bamasaq, D. Alghazzawi, and A. Jamjoom. (2023). "Dynamic Secure Access Control and Data Sharing Through Trusted Delegation and Revocation in a Blockchain-Enabled Cloud-IoT Environment". *IEEE Internet of Things Journal*. 10(5): 4239–4256. DOI: 10.1109/JIOT.2022.3217087.

Association, I. D. S. (2024). "Reference Architecture Model". URL: https://internationaldataspaces.org/wp-content/uploads/IDS-RAM-3.0-2019.pdf.

Bai, L., M. Hu, M. Liu, and J. Wang. (2019). "BPIIoT: A Light-Weighted Blockchain-Based Platform for Industrial IoT". *IEEE Access*. 7: 58381–58393. DOI: 10.1109/ACCESS.2019.2914223.

Banavathu, R. and S. Meruva. (2023). "Efficient secure data storage based on novel blockchain model over IoT-based smart computing systems". *Measurement: Sensors*. 27: 100741. DOI: https://doi.org/10.1016/j.measen.2023.100741.

Byabazaire, J., G. O'Hare, and D. Delaney. (2020). "Data Quality and Trust: Review of Challenges and Opportunities for Data Sharing in IoT". *Electronics*. 9(12). DOI: 10.3390/electronics9122083.

Cheikhrouhou, O., K. Mershad, F. Jamil, R. Mahmud, A. Koubaa, and S. R. Moosavi. (2023). "A lightweight blockchain and fog-enabled secure remote patient monitoring system". *Internet of Things*. 22: 100691. DOI: https://doi.org/10.1016/j.iot.2023.100691.

Cisco. (2024). "Fast Innovation require Fast IT". URL: https://www.cisco.com/c/dam/global/en_ph/assets/ciscoconnect/pdf/bigdata/jim_green_cisco_connect.pdf.

Daidone, F., B. Carminati, and E. Ferrari. (2022). "Blockchain-Based Privacy Enforcement in the IoT Domain". *IEEE Transactions on Dependable and Secure Computing*. 19(6): 3887–3898. DOI: 10.1109/TDSC.2021.3110181.

De Prieëlle, F., M. De Reuver, and J. Rezaei. (2020). "The Role of Ecosystem Data Governance in Adoption of Data Platforms by Internet-of-Things Data Providers: Case of Dutch Horticulture Industry". *IEEE Transactions on Engineering Management*: 1–11.

Dorri, A., S. S. Kanhere, R. Jurdak, and P. Gauravaram. (2017). "Blockchain for IoT security and privacy: The case study of a smart home". In: *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. 618–623. DOI: 10.1109/PERCOMW.2017.7917634.

Dubovitskaya, A., P. Novotny, Z. Xu, and F. Wang. (2020). "Applications of blockchain technology for data-sharing in oncology: Results from a systematic literature review". *Oncology*. 98(6): 403–411. DOI: 10.1159/000504325.

Dwivedi, A. D., G. Srivastava, S. Dhar, and R. Singh. (2019). "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT". *Sensors*. 19(2). DOI: 10.3390/s19020326.

Egala, B. S., A. K. Pradhan, V. Badarla, and S. P. Mohanty. (2021). "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control". *IEEE Internet of Things Journal*. 8(14): 11717–11731. DOI: 10.1109/JIOT.2021.3058946.

Firouzi, F., B. Farahani, M. Barzegari, and M. Daneshmand. (2022). "AI-Driven Data Monetization: The Other Face of Data in IoT-Based Smart and Connected Health". *IEEE Internet of Things Journal*. 9(8): 5581–5599. DOI: 10.1109/JIOT.2020.3027971.

Fu, J.-S., Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang. (2018). "Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing". *IEEE Transactions on Industrial Informatics*. 14(10): 4519–4528. DOI: 10.1109/TII.2018.2793350.

Gaia-X. (2024). "Gaia-X: A Federated Data Infrastructure for Europe". URL: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

Gimenez, P., M. Llop, E. Olivares, C. Palau, M. Montesinos, and M. Llorente. (2020). "Interoperability of IoT platforms in the port sector". *Proceedings of 8th Transport Research Arena TRA*: 27–30.

Goknil, A., P. Nguyen, S. Sen, D. Politaki, H. Niavis, K. J. Pedersen, A. Suyuthi, A. Anand, and A. Ziegenbein. (2023). "A Systematic Review of Data Quality in CPS and IoT for Industry 4.0". *ACM Computing Surveys*.

Griggs, K. N., O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh. (2018). "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring". *Journal of medical systems*. 42: 1–7.

Grossetete, P. (2018). "IoT and the Network: What is the future?" Cisco. URL: https://blogs.cisco.com/networking/iot-and-the-network-what-is-the-future.

Guan, Q., J. Lei, C. Wang, G. Geng, Y. Zhong, L. Fang, X. Huang, and W. Luo. (2023). "BI-FERH: Blockchain-IoT based framework for securing smart hotel". *Computer Science and Information Systems*. 20(4): 1541–1568.

Hang, L., I. Ullah, and D.-H. Kim. (2020). "A secure fish farm platform based on blockchain for agriculture data integrity". *Computers and Electronics in Agriculture*. 170: 105251. DOI: https://doi.org/10.1016/j.compag.2020.105251.

Hao, X., W. Ren, Y. Fei, T. Zhu, and K.-K. R. Choo. (2023). "A Blockchain-Based Cross-Domain and Autonomous Access Control Scheme for Internet of Things". *IEEE Transactions on Services Computing*. 16(2): 773–786. DOI: 10.1109/TSC.2022.3179727.

IBM. (2024a). "What are smart contracts on blockchain?" URL: https://www.ibm.com/topics/smart-contracts.

IBM. (2024b). "What is blockchain technology?" URL: https://www.ibm.com/topics/what-is-blockchain.

IDSA. (2024a). "IDSA is at the forefront of Europe's digital future". URL: https://internationaldataspaces.org/we/ids-in-europe/.

IDSA. (2024b). "Innovating the future of daa exchange in Europe and beyond". URL: https://internationaldataspaces.org/we/.

Isaja, M., P. Nguyen, A. Goknil, S. Sen, E. J. Husom, S. Tverdal, A. Anand, Y. Jiang, K. J. Pedersen, P. Myrseth, J. Stang, H. Niavis, S. Pfeifhofer, and P. Lamplmair. (2023). "A blockchain-based framework for trusted quality data sharing towards zero-defect manufacturing". *Computers in Industry*. 146: 103853. DOI: https://doi.org/10.1016/j.compind.2023.103853.

Jeoung, J., S. Jung, T. Hong, and J.-K. Choi. (2022). "Blockchain-based IoT system for personalized indoor temperature control". *Automation in Construction*. 140: 104339. DOI: https://doi.org/10.1016/j.autcon.2022.104339.

Kang, J., R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang. (2019). "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks". *IEEE Internet of Things Journal*. 6(3): 4660–4670. DOI: 10.1109/JIOT.2018.2875542.

Kitchenham, B. A. and S. Charters. (2007). "Guidelines for performing Systematic Literature Reviews in Software Engineering". *Tech. rep.* No. EBSE 2007-001. Software Engineering Group. URL: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf.

Li, C., R. Chen, Y. Wang, Q. Xing, and B. Wang. (2024). "REEDS: An Efficient Revocable End-to-End Encrypted Message Distribution System for IoT". *IEEE Transactions on Dependable and Secure Computing*: 1–18. DOI: 10.1109/TDSC.2024.3353811.

Li, Z., J. Zhang, J. Zhang, Y. Zheng, and X. Zong. (2023). "Integrated Edge Computing and Blockchain: A General Medical Data Sharing Framework". *IEEE Transactions on Emerging Topics in Computing*: 1–14. DOI: 10.1109/TETC.2023.3344655.

Lo, S. K., Y. Liu, S. Y. Chia, X. Xu, Q. Lu, L. Zhu, and H. Ning. (2019). "Analysis of Blockchain Solutions for IoT: A Systematic Literature Review". *IEEE Access*: 58822–58835.

Ma, Z., L. Wang, and W. Zhao. (2021). "Blockchain-Driven Trusted Data Sharing With Privacy Protection in IoT Sensor Network". *IEEE Sensors Journal*. 21(22): 25472–25479. DOI: 10.1109/JSEN.2020.3046752.

Makhdoom, I., I. Zhou, M. Abolhasan, J. Lipman, and W. Ni. (2020). "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities". *Computers & Security*. 88: 101653. DOI: https://doi.org/10.1016/j.cose.2019.101653.

Manoj, T., K. Makkithaya, and N. V.G. (2023). "A trusted IoT data sharing and secure oracle based access for agricultural production risk management". *Computers and Electronics in Agriculture*. 204: 107544. DOI: https://doi.org/10.1016/j.compag.2022.107544.

Matsas, M. (2024). "Data Space Radar". URL: https://internationaldataspaces.org/adopt/data-space-radar/.

Mayer, A. H., V. F. Rodrigues, C. A. d. Costa, R. d. R. Righi, A. Roehrs, and R. S. Antunes. (2021). "FogChain: A Fog Computing Architecture Integrating Blockchain and Internet of Things for Personal Health Records". *IEEE Access*. 9: 122723–122737. DOI: 10.1109/ACCESS.2021.3109822.

Medium. (2024). "Manageing Complexity Of IoT Sensors, Endpoints, Gateways, And Network Bottlenecks". Medium.

Mollah, M. B., M. A. K. Azad, and A. Vasilakos. (2017). "Secure Data Sharing and Searching at the Edge of Cloud-Assisted Internet of Things". *IEEE Cloud Computing*. 4(1): 34–42. DOI: 10.1109/MCC.2017.9.

Nawaz, A., J. Peña Queralta, J. Guan, M. Awais, T. N. Gia, A. K. Bashir, H. Kan, and T. Westerlund. (2020). "Edge Computing to Secure IoT Data Ownership and Trade with the Ethereum Blockchain". *Sensors*. 20(14). DOI: 10.3390/s20143965.

Nguyen, D. C., P. N. Pathirana, M. Ding, and A. Seneviratne. (2021). "A Cooperative Architecture of Data Offloading and Sharing for Smart Healthcare with Blockchain". In: *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 1–8. DOI: 10.1109/ICBC51069.2021.9461063.

Nguyen, H.-H., P. H. Phung, P. H. Nguyen, and H.-L. Truong. (2022). "Context-driven Policies Enforcement for Edge-based IoT Data Sharing-as-a-Service". In: *2022 IEEE International Conference on Services Computing (SCC)*. 221–230. DOI: 10.1109/SCC55611.2022.00041.

Oracle. (2024). "What Is Data Management?" URL: https://www.oracle.com/database/what-is-data-management/.

Özyilmaz, K. R., M. Doğan, and A. Yurdakul. (2018). "IDMoB: IoT Data Marketplace on Blockchain". In: *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. 11–19. DOI: 10.1109/CVCBT.2018.00007.

Patel, H. and B. Shrimali. (2023). "AgriOnBlock: Secured data harvesting for agriculture sector using blockchain technology". *ICT Express*. 9(2): 150–159. DOI: https://doi.org/10.1016/j.icte.2021.07.003.

Petersen, K., S. Vakkalanka, and L. Kuzniarz. (2015). "Guidelines for conducting systematic mapping studies in software engineering: An update". *Information and Software Technology*. 64: 1–18.

Pham, H.-A., T.-K. Le, T.-N.-M. Pham, H.-Q.-T. Nguyen, and T.-V. Le. (2019). "Enhanced Security of IoT Data Sharing Management by Smart Contracts and Blockchain". In: *2019 19th International Symposium on Communications and Information Technologies (ISCIT)*. 398–403. DOI: 10.1109/ISCIT.2019.8905219.

Preuveneers, D. and W. Joosen. (2019). “Towards Multi-party Policy-based Access Control in Federations of Cloud and Edge Microservices”. In: *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 29–38. DOI: 10.1109/EuroSPW.2019.00010.

Rajmohan, T., P. H. Nguyen, and N. Ferry. (2022). “A decade of research on patterns and architectures for IoT security”. *Cybersecurity*. 5(1): 1–29.

Al-Ruithe, M., E. Benkhelifa, and K. Hameed. (2019). “A systematic literature review of data governance and cloud data governance”. *Personal and Ubiquitous Computing*.

Samuel, O., A. B. Omojo, S. M. Mohsin, P. Tiwari, D. Gupta, and S. S. Band. (2023). “An Anonymous IoT-Based E-Health Monitoring System Using Blockchain Technology”. *IEEE Systems Journal*. 17(2): 2422–2433. DOI: 10.1109/JSYST.2022.3170406.

Sarabia-Jácome, D., I. Lacalle, C. E. Palau, and M. Esteve. (2019). “Enabling Industrial Data Space Architecture for Seaport Scenario”. In: *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. 101–106. DOI: 10.1109/WF-IoT.2019.8767216.

Seiner, R. S. (2024). “Data Governance and the Internet of Things”. URL: https://www.slideshare.net/Dataversity/data-governance-and-the-internet-of-things.

Sengupta, J., S. Ruj, and S. D. Bit. (2020). “A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT”. *Journal of network and computer applications*. 149: 102481.

Sengupta, J., S. Ruj, and S. Das Bit. (2023). “FairShare: Blockchain Enabled Fair, Accountable and Secure Data Sharing for Industrial IoT”. *IEEE Transactions on Network and Service Management*. 20(3): 2929–2941. DOI: 10.1109/TNSM.2023.3239832.

Shang, J., R. Guan, Y. Tong, *et al.* (2022). “Microgrid data security sharing method based on blockchain under Internet of Things architecture”. *Wireless Communications and Mobile Computing*. 2022.

Sharma, A., S. Kaur, and M. Singh. (2024). "A secure blockchain framework for the internet of medical things". *Transactions on Emerging Telecommunications Technologies*. 35(1): e4917. DOI: https://doi.org/10.1002/ett.4917.

Singh, P., M. Masud, M. S. Hossain, and A. Kaur. (2021). "Cross-domain secure data sharing using blockchain for industrial IoT". *Journal of Parallel and Distributed Computing*. 156: 176–184. DOI: https://doi.org/10.1016/j.jpdc.2021.05.007.

Song, R., B. Xiao, Y. Song, S. Guo, and Y. Yang. (2023). "A Survey of Blockchain-Based Schemes for Data Sharing and Exchange". *IEEE Transactions on Big Data*. 9(6): 1477–1495. DOI: 10.1109/TBDATA.2023.3293279.

Tang, B., H. Kang, J. Fan, Q. Li, and R. Sandhu. (2019). "IoT Passport: A Blockchain-Based Trust Framework for Collaborative Internet-of-Things". In: *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies. SACMAT '19*. Toronto ON, Canada: Association for Computing Machinery. 83–92. DOI: 10.1145/3322431.3326327.

Tran, T., P. Nguyen., and G. Erdogan. (2023). "A Systematic Review of Secure IoT Data Sharing". In: *Proceedings of the 9th International Conference on Information Systems Security and Privacy - ICISSP*. INSTICC. SciTePress. 95–105. DOI: 10.5220/0011674200003405.

Umran, S. M., S. Lu, Z. A. Abduljabbar, and V. O. Nyangaresi. (2023). "Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry". *Internet of Things*. 24: 100969. DOI: https://doi.org/10.1016/j.iot.2023.100969.

Ur Rahman, M., F. Baiardi, and L. Ricci. (2020). "Blockchain Smart Contract for Scalable Data Sharing in IoT: A Case Study of Smart Agriculture". In: *2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT)*. 1–7. DOI: 10.1109/GCAIoT51063.2020.9345874.

Wan, P. K., L. Huang, and H. Holtskog. (2020). "Blockchain-Enabled Information Sharing Within a Supply Chain: A Systematic Literature Review". *IEEE Access*. 8: 49645–49656. DOI: 10.1109/ACCESS.2020.2980142.

Wang, F., J. Cui, Q. Zhang, D. He, C. Gu, and H. Zhong. (2023). "Lightweight and Secure Data Sharing Based On Proxy Re-Encryption for Blockchain-Enabled Industrial Internet of Things". *IEEE Internet of Things Journal*: 1–1. DOI: 10.1109/JIOT.2023.3340567.

Wei, X., Y. Yan, S. Guo, X. Qiu, and F. Qi. (2022). "Secure Data Sharing: Blockchain-Enabled Data Access Control Framework for IoT". *IEEE Internet of Things Journal*. 9(11): 8143–8153. DOI: 10.1109/JIOT.2021.3111012.

Wohlin, C. (2014). "Guidelines for snowballing in systematic literature studies and a replication in software engineering". In: *EASE'14*. 38.

Xu, R., S. Y. Nikouei, Y. Chen, E. Blasch, and A. Aved. (2019). "BlendMAS: A Blockchain-Enabled Decentralized Microservices Architecture for Smart Public Safety". In: *2019 IEEE International Conference on Blockchain (Blockchain)*. 564–571. DOI: 10.1109/Blockchain.2019.00082.

Yu, J., B. Yan, H. Qi, S. Wang, and W. Cheng. (2024). "An Efficient and Secure Data Sharing Scheme for Edge-Enabled IoT". *IEEE Transactions on Computers*. 73(1): 178–191. DOI: 10.1109/TC.2023.3325668.

Zaabar, B., O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid. (2021). "HealthBlock: A secure blockchain-based healthcare data management system". *Computer Networks*. 200: 108500. DOI: https://doi.org/10.1016/j.comnet.2021.108500.

Al-Zahrani, F. A. (2020). "Subscription-Based Data-Sharing Model Using Blockchain and Data as a Service". *IEEE Access*. 8: 115966–115981. DOI: 10.1109/ACCESS.2020.3002823.

Zhang, L., M. Peng, W. Wang, Z. Jin, Y. Su, and H. Chen. (2021). "Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing". *Transactions on Emerging Telecommunications Technologies*. 32(10): e4315. DOI: https://doi.org/10.1002/ett.4315.

Zheng, X., S. Sun, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Meré. (2019). "Accelerating Health Data Sharing: A Solution Based on the Internet of Things and Distributed Ledger Technologies". *J Med Internet Res*. 21(6): e13583. DOI: 10.2196/13583.

Zichichi, M., S. Ferretti, and G. D'angelo. (2020). "A Framework Based on Distributed Ledger Technologies for Data Management and Services in Intelligent Transportation Systems". *IEEE Access*. 8: 100384–100402. DOI: 10.1109/ACCESS.2020.2998012.

Zuo, Y. and Z. Qi. (2022). "A Blockchain-Based IoT Framework for Oil Field Remote Monitoring and Control". *IEEE Access*. 10: 2497–2514. DOI: 10.1109/ACCESS.2021.3139582.