

TrustNShare – Data Trust Model Balancing Privacy Risk, Reputation, and Incentives

Cord SPRECKEISEN^{a,1}, Tim SCHNEIDER^a, Sven FESTAG^a,
Sebastian USCHMANN^a, Hamza MAATOUK^b, Stephan JONAS^b, Anna WEBER^c,
Sven BOCK^c, and Friederike KLAN^c

^a*Institute of Medical Statistics, Computer and Data Sciences (IMSID), Jena University Hospital, Jena, Germany*

^b*Institute of Digital Medicine, University Hospital Bonn, Bonn, Germany*

^c*German Aerospace Center (DLR), Institute of Data Science, Jena, Germany*

ORCID ID: C. Spreckelsen <https://orcid.org/0000-0002-7301-1566>, T. Schneider <https://orcid.org/0009-0006-9817-8369>, S. Festag <https://orcid.org/0000-0002-2507-5901>, S. Uschmann <https://orcid.org/0000-0003-3108-6495>, S. Jonas <https://orcid.org/0000-0002-3687-6165>, H. Maatouk <https://orcid.org/0009-0009-9136-9471>, F. Klan <https://orcid.org/0000-0002-1856-7334>, S. Bock <https://orcid.org/0000-0002-9931-9569>, A. L. Weber <https://orcid.org/0009-0000-0538-4160>

Abstract. The TrustNShare project aims to facilitate health data exchange by creating a framework that balances privacy, reputation, and incentives. The approach allows for flexible privacy levels while mitigating the risks of data re-identification, supported by blockchain-based tamper-proof logging. Through a participatory development process involving stakeholders, a reputation model and incentives were established. The data trust enhances data sharing negotiations by informing participants of key factors like user reputation and privacy risks.

Keywords. Data trust model; blockchain; privacy; re-identification; participation

1. Introduction and Methodology

Data trusts serve as neutral intermediaries that establish legal, technical, and organizational frameworks to facilitate data sharing [1]. Several approaches for privacy-protecting data sharing in the highly regulated health domain have been proposed, while many disregard the possibility of privacy breach despite the use of privacy-preserving procedures [2,3]. TrustNShare addresses health data exchange and focuses on the relative influence of reputation, incentives, and privacy standards in facilitating the initiation of data sharing, as well as ensuring tamper-proof logging throughout the data sharing process based on blockchain technology [4].

Current methods for technical data privacy, such as differential privacy, often allow the level of privacy to be freely chosen. In all these methods, the level of privacy can be determined by choosing a function parameter. The goal of TrustNShare is to develop a model that mediates between the incentives offered to share data and the expected

¹ Corresponding Author: Cord Spreckelsen, Institute of Medical Statistics, Computer and Data Sciences, Jena University Hospital, Bachstr. 18, 07743 Jena, Germany; E-Mail: cord.spreckelsen@med.uni-jena.de.

compensation for remaining re-identification risks, given a flexibly selectable level of privacy and the reputation of data users.

The project established a participatory process involving stakeholders in the creation of a reputation model and the specification of incentive factors. The process included guideline-based interviews, online surveys as well as co-creative activities. Influencing factors identified in this way are combined with concepts of prospect theory [5].

A technical core element for fostering trust is tamper-proof transaction logging, implemented using blockchain technology, namely Hyperledger Fabric. The software project is built on a MERN stack (MongoDB, Express, React, and Node) and a blockchain framework (Hyperledger Firefly) and is deployed via container images.

2. Results

TrustNShare has identified specific drivers that influence the willingness to share data through the reputation of data users and the compensation of privacy risks. The TrustNShare transmission model, which mediates between expected risk compensation and incentives, also employs quantitative concepts of risk aversion and perceived probability. The platform of the data trust specifically queries these factors, infers areas of potential agreement, and then informs the parties involved. Performance and usability of the platform were systematically evaluated, and on this basis a revision cycle was carried out for both the underlying model and the supporting application.

3. Discussion and Conclusions

The TrustNShare data trust model fills a gap: It supports the negotiation of data sharing in the face of fine-grained privacy levels. The biggest challenge has been to communicate the underlying concepts to users. This is crucial for building trust. Equipped with explanatory text and graphical representations, the technical implementation of the model is not simply a data exchange platform, but a supporting mediator.

References

- [1] Stalla-Bourdillon S, Thuermer G, Walker J, Carmichael, Simperl E. Data protection by design: Building the foundations of trustworthy data sharing. *Data & Policy*. 2020 Jan;2:e4, doi: 10.1017/dap.2020.1.
- [2] Raab R, Küderle A, Zakreuskaya A, Stern AD, Klucken J, Kaissis G, et al. Federated electronic health records for the European Health Data Space. *The Lancet Digital Health*. 2023 Nov;5(11):e840-e847.
- [3] Wirth, F.N., Meurers, T., Johns, M. et al. Privacy-preserving data sharing infrastructures for medical research: systematization and comparison. *BMC Med Inform Decis Mak*. 2021; 21:242
- [4] Maatouk H, Uschmann S, Festag S, Schneider T, Weber A, Khoi NM, et al. TrustNShare: Development of a Blockchain-Based Data Trust Model for Secure and Controlled Health Data Sharing Grounded on Empirical Research. *Stud Health Technol Inform*. 2023 Jun 29;305:2389, doi: 10.3233/SHTI230472.
- [5] Gisbert-Pérez J, Martí-Vilar M, González-Sala F. Prospect Theory: A Bibliometric and Systematic Review in the Categories of Psychology in Web of Science. *Healthcare*. 2022 Oct;10(10):2098, doi: [10.3390/healthcare10102098](https://doi.org/10.3390/healthcare10102098)