Towards Federated Governance and Decentralized Identities for Participatory Sensing Data Mesh

Daria Schumm[1], Bruno Rodrigues[2], Andy Aidoo[1], Tim Portmann[1], Burkhard Stiller[1]
[1]Communication Systems Group CSG, Department of Informatics IfI, University of Zurich UZH, Switzerland
[2]Embedded Sensing Group ESG, School of Computer Science SCS, University of St. Gallen HSG, Switzerland
E-mail: {schumm,stiller,aidoo}@ifi.uzh.ch, tim.portmann@uzh.ch, bruno.rodrigues@unisg.ch

***Abstract*—Sensor-driven data meshes are crucial for continuous data streams in the Industrial Internet-of-Things (IIoT). Yet establishing trust and robust governance remains a challenge in participatory and mobile crowd sensing. This paper presents a framework for automated onboarding of organizations and credential management based on federated governance and decentralized identities. The proposed design leverages federated governance, decentralized membership voting, credential issuance, and authentication to guarantee trust between coalition members in a data mesh network. As a result, the framework fosters trust, simplifies domain integration, and ensures secure collaboration in sensor-driven data mesh.**

***Index Terms*—security, data sharing, data mesh, decentralized identity**

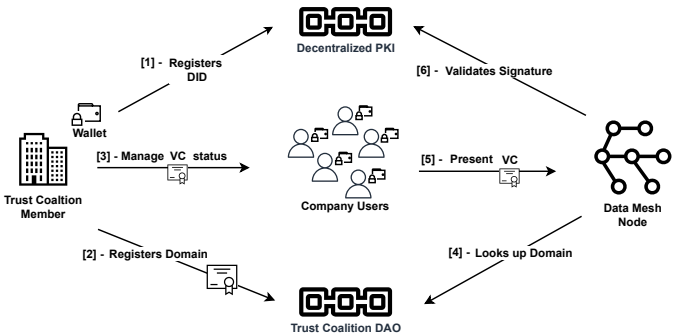

Fig. 1. Trust Coalition Network Architecture

I. Introduction

A data mesh is a decentralized data-sharing approach that enables multiple organizations to contribute and consume shared data across domains and promotes efficient resource allocation [1]. Such an approach is particularly relevant for Industrial Internet-of-Things (IIoT) and smart cities, where trust and cooperation are essential for aggregating sensor data [2]. It supports local data management within a domain while facilitating cross-domain collaboration for tasks, such as anomaly detection, disaster response, and resource optimization [3]. However, a strong trust mechanism is necessary to protect sensitive information. Furthermore, the lack of a unified identity layer complicates the authentication that is required to ensure that only authorized entities can access sensitive information [4].

Even though the data mesh concept has gained considerable interest, there is limited work that address governance models and no work considers the use of Decentralized Identity (DI) within a data mesh. Multiple tools available for data mesh architecture and can be categorized as single-tool, pre-built stacks, and custom stacks [5]. The modular approach supports a fully decentralized architecture, enabling each domain to make independent choices. Nevertheless, there is a lack of federated and decentralized governance solutions [6], [7], while some decentralized aspects for data verification, exchange, and trust are used [8]. Additionally, the use of DI is largely overlooked. This paper proposes a decentralized approach to cross-organizational information exchange, leveraging Decentralized Autonomous Organizations (DAO), smart contracts, and DI. The approach improves trust in participatory sensing, real-time IIoT, and smart city applications.

II. Proposed Design and Implementation

Governance of a decentralized data architecture requires balancing local and global policies for user authentication and authorization to ensure standardization, trust, and enforcement across independent nodes and companies. To prevent domain impersonation, new members are first verified using their Transport Layer Security (TLS) certificate and then existing coalition members vote on their approval. The DAO acts as a domain registry, managing credential definitions and membership revocations. Once a new member is validated, their Decentralized Identifier (DID) is registered in the decentralized public key infrastructure (PKI). This allows new members to issue Verifiable Credentials (VC) for identity and access rights, which data mesh nodes can verify through the PKI.

As shown in Figure 1, a trust coalition member (TCM) or an issuer, must be capable of issuing a VC to a company user or a holder. TCM must also manage the VCs they issue, allowing for updates and revocations (*e.g.*, address changes or employment termination). A data mesh node or another TCM (a verifier) require functionality to authenticate presented VC. Credential holders need a secure means of storing their VCs to prove ownership and validity when necessary. Since each TCM can issue and validate VCs, as well as manage their DID, only validated and reputable domains can join the network to minimize the risk of impersonation and maintain the integrity of the trust coalition. As shown in Figure 2, to access the information from a different domain, a user must present a VC to the relevant verifier and a TCM application that provides data product must be able to authenticate and authorize users from another TCM. The verifier checks whether the issuer domain is registered in the trust coalition via the DAO, verifies

the credential holder's access rights, and validates the VC signature. Access policies are determined by the domain owner. TCM application can delegate authentication and authorization or implement custom access control. Users requesting data are redirected to an authorization server, which verifies credentials through a mobile wallet connection. The server collects VCs, requests user consent to share the requested credentials, and enforces access based on federated governance and access control models.

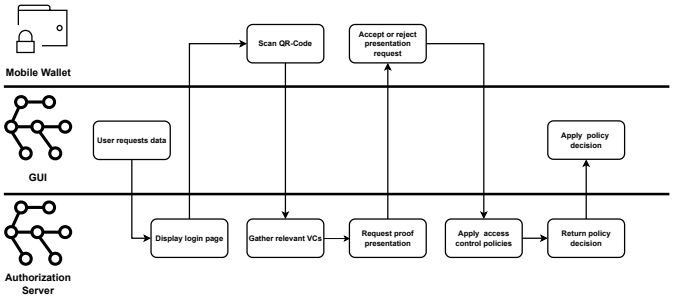

Fig. 2. Authentication and Authorization Process

A *VC service* ensures interoperability between TCM through a standard VC issuance protocol, where a credential issuer and holder establish a DIDComm connection to issue, verify, and revoke credentials. A credential schema is registered on Hyperledger Indy and revocations are managed through a tails file [9]. A web client user VC schema contains fields such as first and last name, employee ID, and their role in the organization. A *verification service* involves a verifier requesting proof from a prover. The prover responds with a zero-knowledge proof (ZKP) demonstrating data integrity and non-revocation status. After a new DIDComm is established, the verifier validates the user's VC and non-revocation proof, issuing a JSON web token (JWT) for access. To enable inspection of the authenticity of previously shown proofs, each proof is timestamped, and tampered or revoked attributes are marked as inactive, ensuring secure, privacy-preserving authentication across domains. To guarantee a flexible access control model, each domain can apply its access control policies since each of them possesses a unique identifier within the trust coalition network and is managed through the DAO. A standard identity claim VC schema contains fields such as first and last name, employee ID, and organization department. A *governance service* enables members to decide on the membership of a new domain or a company. During the onboarding process, new members provide details to register as issuers. A smart contract on the Sepolia testnet standardizing the onboarding process, allowing members to vote on applications, and ensuring secure governance through decentralized identity principles, PKI standards, and Ethereum wallets.

III. Preliminary Evaluation

The onboarding process is currently automated and supports RSA and elliptic curve algorithms. Smart contracts are used to validate the application through the use of a cryptographic challenge. Depending on the new member domain, TCM can vote for the new membership. Applications are approved or rejected based on vote thresholds, where a two-thirds approval results in acceptance. Credential definitions can be updated or invalidated by members. Domain issuers can create VCs for the users, stored securely in mobile wallets with biometric or password access. Revoked credentials are recorded in the Indy tails file. As a result, the credential holder cannot construct a valid proof of non-revocation.

Scalability, availability, and interoperability are key non-functional requirements for the proposed system. First, *scalability* depends on the SC implementation. The trust coalition membership is represented using a mapping type with the keccak256 hash function, theoretically supporting up to 2^{256} domains. Peer-to-peer communication via DIDComm ensures scalability for VC issuance, while the limitation of 32,768 revocable credentials per Indy tails file can be mitigated by publishing multiple credential definitions. Additionally, the system can theoretically support a large number of users, with verifiers managing over 3,000 concurrent proof presentations per GB of memory via the ACA-py framework. The computational burden for proof generation is minimal for modern mobile devices, requiring only a few seconds. Second, *availability* relies on the concurrent operation of verifiers, issuers, and a reachable ledger hosting DIDs. Although multiple points of failure exist, distributed ledger technology (DLT) ensures fault tolerance through redundancy. The downtime of one node does not affect the overall trust network or the Ethereum blockchain maintaining the membership list. Third, *interoperability* is achieved through Docker-based containerization, enabling the system to run on diverse hardware and software platforms. Mobile clients available for Android and iOS ensure accessibility for credential holders.

To prevent impersonation on the *security* dimension, the trust coalition utilizes Solidity SCs for membership voting on upcoming applications, enabling members to verify applicants physically if desired. Authentication is completed with a mobile wallet, which, depending on the wallet, requires the use of biometrics or password to authenticate the user. Additionally, VC design is impersonation-resistant through the use of cryptographic techniques.

IV. Considerations

This work proposed a federated governance model for a trust coalition within a participatory data mesh network. The respective model can enable coalition governance, VC lifecycle, and user authentication, providing a secure and user-centric approach to cross-domain authorization. Decentralized voting for new members ensures security through a high vote threshold, granting coalition members control over network membership. Interoperability is achieved via the standardized use of DIDs, VCs, and DAO. The prototype demonstrates the potential for a secure and decentralized collaboration, and it can be extended into a broader trust ecosystem for exchanging anonymized data, such as mobile crowd sensing information, as presented above.

REFERENCES

[1] M. W. Beall and M. S. Shephard, "A general topology-based mesh data structure," *International Journal for Numerical Methods in Engineering*, vol. 40, no. 9, pp. 1573–1596, 1997.

[2] A. Goedegebuure, I. Kumara, S. Driessen, W.-J. Van Den Heuvel, G. Monsieur, D. A. Tamburri, and D. D. Nucci, "Data mesh: a Systematic Gray Literature Review," *ACM Computing Surveys*, vol. 57, no. 1, pp. 1–36, 2024.

[3] W. Lu, Y. Gong, X. Liu, J. Wu, and H. Peng, "Collaborative energy and information transfer in green wireless sensor networks for smart cities," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1585–1593, 2017.

[4] K. Cameron, "The laws of identity," *Microsoft Corp*, vol. 12, pp. 8–11, 2005.

[5] J. Christ, L. Visengeriyeva, and S. Harrer, 2022. [Online]. Available: https://www.datamesh-architecture.com/

[6] A. Goedegebuure, I. Kumara, S. W. Driessen, D. D. Nucci, G. Monsieur, W. jan Van Den Heuvel, and D. A. Tamburri, "Data mesh: a systematic gray literature review," *ArXiv*, vol. abs/2304.01062, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:257913930

[7] A. Wider, S. Verma, and A. Akhtar, "Decentralized data governance as part of a data mesh platform: Concepts and approaches," *arXiv preprint arXiv:2307.02357*, 2023.

[8] A. Almaslukh, A. Alameer, H. Alsaleh, F. Alkadyan, N. Allheeib, A. Alhadlag, and Y. Alabdulkarim, "Data mesh meets blockchain," *International Journal of Computational Intelligence Systems*, vol. 17, no. 1, p. 27, 2024.

[9] I. T. Server. [Online]. Available: https://github.com/bcgov/indy-tails-server