ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

A NOVEL DATA FOR AUTHORITY ACCESS DATA DELEGATION BY UTILIZING SELF-SOVEREIGN IDENTITY AND VERIFIABLE CREDENTIALS

PRIYA RANJAN RAJ[1], ILENI ANUDEEP REDDDY[2], CHITTI AJAY REDDY[3], NAINI HARSHA VARDHAN REDDY[4], GADADASU SATEESH[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5]B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT – Users can take charge of their digital identities and data with Self-Sovereign Identity (SSI), a decentralized, user-centric approach to Identity Management (IdM). It lessens the drawbacks of conventional, centralized IdM systems and offers numerous benefits. Notwithstanding its advantages, SSI primarily emphasizes direct communication between two separate entities. When the identity holders are the verified bearers of their credentials, it permits direct identification, authentication, authorization, and access to resources and services. However, it mainly ignores indirect identity control, like delegation, which is a necessary component of everyday life and interpersonal relationships. In organizational settings, delegation is especially prevalent. It typically results from the need for increased productivity, relief, or distribution of work, as well as from the incapacity to carry out tasks, responsibilities, and duties for a variety of reasons. It needs more research and the creation of fresh strategies, though, as it is comparatively understudied within the SSI framework. Therefore, our study sought to close the previously mentioned gap and provide a thorough analysis of delegation in the SSI ecosystem.

Index Terms – Access delegation, authority delegation, delegation, self-sovereign identity, verifiable credential, verifiable mandate.

I. INTRODUCTION

Self-Sovereign Identity (SSI) is a decentralized, user-centric concept representing a paradigm shift in how digital identity is perceived and managed. It presents a shift of power and control from centralized authorities, such as the Certificate Authority (CA) and Identity and Service Providers (IdPs and SPs), to end-users or identity holders within the SSI's scope in the center of digital interactions. Therefore, they are responsible for identity provisioning and management; for creating, storing, and managing their Decentralized Identifiers (DIDs) and cryptographic material; obtaining (identity) attributes in the form of Verifiable Credentials (VCs) from various sources, storing them, and transmitting them as proof of identity when required. Consequently, SSI addresses the shortcomings of traditional, centralized approaches, such as Single Point Of Failure (SPOF), centralization of power and control by IdPs and SPs, centralized data storage of Personally Identifiable Information (PII), and reliance on intermediaries to provide identity (IdPs, CAs), which can lead to personal data misuse, data leakage, identity theft, and other security and privacy-connected risks. On the other hand, it brings many advantages to the field of Identity Management (IdM), as it follows modern technological principles and approaches, such as the decentralization of power, control, and data, usercentrism, enhanced security and privacy data sovereignty, minimal or selective data disclosure, interoperability, mobile-first design, and digital wallets, that present a crucial component in the SSI ecosystem and are consistent with the efforts of the European Commission. Despite its advantages and positive features, SSI focuses predominantly on direct, one-to-one interactions between two independent entities. It facilitates direct identification, authentication, authorization, and access to resources and services where the identity holder is the authenticating bearer of their credentials. Therefore, it supports primarily cases where identity holders use and manage their digital identifiers (DID), cryptographic material, and credentials (VC). In this regard, SSI does not address Indirect Identity Control (IIC) primarily, essential to everyday life situations and natural human relationships in the physical world, such as guardianship, controllership, and delegation.

Consequently, SSI excludes individuals who, due to social, legal, mental, physical, or other limitations, are unable to act independently in the digital environment. These include children, the elderly, the homeless, animals, and other entities needing proxies to manage their identity.

Furthermore, current SSI models do not address situations where a delegation of tasks, rights, responsibilities, or permissions is required effectively, either due to the need for increased efficiency, relief from work, cooperation, and collaboration, or due to the temporary or permanent inability of an entity (e.g., an individual) to perform certain activities or tasks. The aforementioned situations are prevalent in an organizational context for companies and organizations where delegation plays a key role. It enables flexible management of resources, access, and responsibilities. In hierarchical structures, it is crucial for transferring access rights, making decisions, or performing tasks to subordinate entities, which allows for increased efficiency, instilling trust, reducing overload, and promoting collaboration. It is important within (among employees) and across organizational boundaries (partners). In addition, it enables security policy optimization and the expansion of Access Control (AC) mechanisms, by enabling shared or time-limited access to critical systems and data. While delegation is an essential and often necessary feature for companies and organizations, it is beneficial for their end users, as it represents added value, and allows users to empower third parties (other identity holders) to act or access services and resources on their behalf. This is especially relevant when accessing and managing health, financial, or personal data, and services when users cannot perform specific actions due to illness, travel, or other limitations.

II. RELATED WORKS

1) Towards the classification of self-sovereign identity properties

Self-Sovereign Identity (SSI) is a novel and emerging, decentralized digital identity approach that enables entities to control and manage their digital identifiers and associated identity data while enhancing trust, privacy, security, and the many other properties identified and analyzed in this paper. The paper provides an overview and classification of the SSI properties, focusing on an in-depth analysis, furthermore, presenting a comprehensive collection of SSI properties that are important for the implementation of the SSI system. In addition, it explores the general SSI process flow, and highlights the steps in which individual properties are important. After the initial purification and classification phase, we then validated properties among experts in the field of Decentralized and Self-Sovereign Identity Management using an online questionnaire, which resulted in a final set of classified and verified SSI properties. The results can be

used for further work on definition and standardization of the SSI field.

2) Revocable and offline-verifiable self-sovereign identities

Identity management systems enable users (i.e., provers) to authenticate and provide attributes to verifiers by using certified credentials obtained from an authority. To accept such a credential, verifiers require information on whether the presented credentials are still valid or if they have been revoked. Up-to-date revocation information can be obtained from a revocation database; however, this requires that the verifier or prover is online. The problem becomes more interesting in the offline case when the prover (e.g., citizen) and verifier (e.g., police officer) do not have an Internet connection to query the revocation status of the presented credential (e.g., digital driver's license). In this paper, we extend the Self-Sovereign Identity (SSI) model to support both revocation as well as offline-verification.

3) Privacy preserving eID derivation to self-sovereign identity systems with offline revocation.

Digital identities play a vital role in an increasingly digital world. These identities often rely on central authorities to issue and manage them. Central authorities have the drawback of being a central trusted party, representing a bottleneck and single point of failure with exclusive control of identity-related data. Self-sovereign identity (SSI) tackles those problems by utilizing distributed ledger technology and making users the sovereign owners of their identity data. Nevertheless, SSI, as recent technology, still lacks qualified identity data. This is especially a problem since sensitive services like eGovernment or banking services require identity data issued by a qualified identity provider; thus, SSI - based identities cannot be used for these services. In this paper, we propose a concept for deriving identity data from an existing identity system into an SSI in a fully privacy-preserving way by additionally supporting offline verification. This way, we enable a chain of trust from the existing identity system to the SSI system by introducing a novel trust model. Our concept utilizes novel cryptographic primitives to support efficient and privacy-preserving identity showing as well as revocation. To underline the feasibility of our concept, we implement a proof system and benchmark the related use cases.

4) Distributed Attestation Revocation in Self-Sovereign Identity

Self-Sovereign Identity (SSI) aspires to create a standardised identity layer for the Internet by placing citizens at the centre of their data, thereby weakening the grip of

big tech on current digital identities. However, as millions of both physical and digital identities are lost annually, it is also necessary for SSIs to possibly be revoked to prevent misuse. Previous attempts at designing a revocation mechanism typically violate the principles of SSI by relying on central trusted components. This lack of a distributed revocation mechanism hampers the development of SSI. In this paper, we address this limitation and present the first fully distributed SSI revocation mechanism that does not rely on specialised trusted nodes. Our novel gossip-based propagation algorithm disseminates revocations throughout the network and provides nodes with a proof of revocation that enables offline verification of revocations. We demonstrate through simulations that our protocol adequately scales to national levels.

III. PROPOSEED METHODOLOGY

We also limited ourselves to the SSI approach, utilizing SSI principles and properties, highlighting the importance of decentralization, autonomy, user-centrism, control over data and interactions, privacy, data minimization, and security, among others, presented. In addition to the above concepts, SSI is consistent with the mobile-first approach, it emphasizes the importance of GDPR, and it is also aligned with the efforts of the European Commission, which aims to provide digital identity wallets enabling digital identification for every citizen, resident, and business within the EU. Thus, (A1) we assume the utilization of basic SSI building blocks to extend the SSI model and support delegation.Within the SSI ecosystem, formal delegation can be achieved through a DID document (DDO) andVCdelegation. The first, typically, focuses on identity control capabilities and DID governance, while the second enables entities to delegate roles, rights, permissions, or claims, providing more flexible and granular delegation. Hence, (L4) we limited ourselves to the VC delegation.

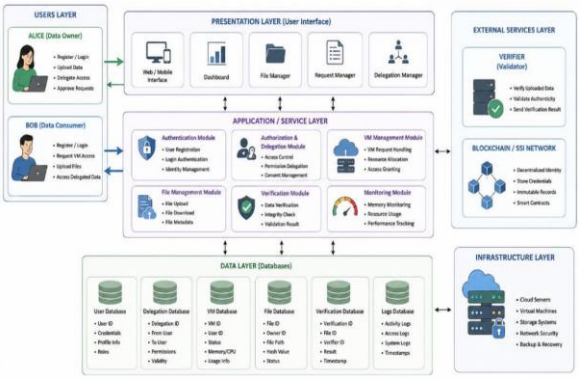


Fig. 1: System Architecture

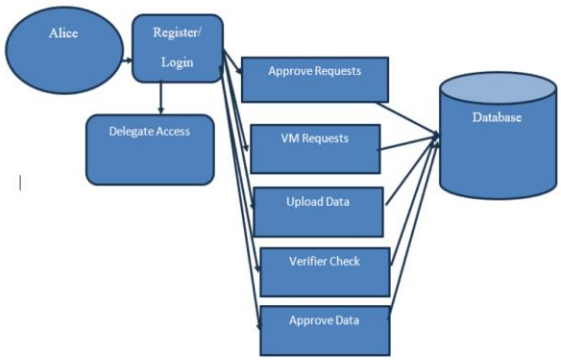
The system architecture of the Self-Sovereign Identity (SSI) cloud system represents the overall structure and interaction between different modules, users, servers, and security components. The architecture is divided into multiple layers, including the user layer, presentation layer, application layer, data

layer, security layer, and infrastructure layer. In the user layer, Alice and Bob interact with the system through web or mobile interfaces. Alice acts as the data owner who uploads files, delegates access permissions, and approves requests, while Bob requests virtual machine access and uploads files. The presentation layer provides dashboards, request management, and file management interfaces for user interaction.

Implementation Modules

Alice

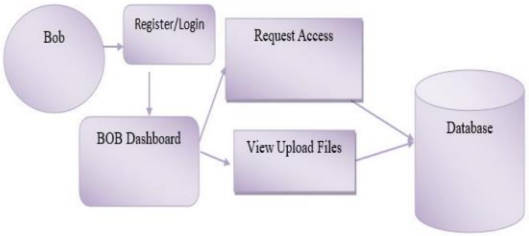
Alice is a registered data owner in the cloud-based system. After completing the registration process, Alice can securely log in using her user ID and password. She has the authority to upload and manage her data in the cloud environment. Alice delegates access permissions to authorized users, allowing them to request resources such as virtual machines for data processing and storage. Whenever a request is made, Alice carefully reviews and approves the access request to ensure data security and privacy. After approval, the requested virtual machine resources are provided to the user. Alice then uploads her data to the cloud server for secure storage and sharing. To maintain integrity and trust, the uploaded data is verified by a verifier who checks the authenticity and correctness of the information. Once the verification process is completed successfully, Alice grants final approval, ensuring that only verified and secure data is available within the system.



Bob

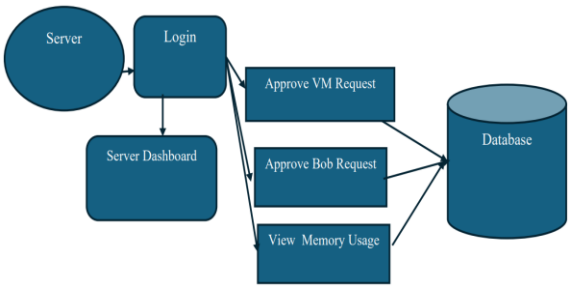
Bob is a valid user of the cloud-based system who first completes the registration process by providing the required personal and account details. After successful registration, Bob receives a unique user ID and password, which he uses to securely log in to the system. Once authenticated, Bob can access the available services and resources provided by the cloud environment. Bob submits a request for access to a virtual machine in order to perform data storage, processing, or other computing tasks. The request is reviewed and approved by the authorized owner or administrator before access is granted. After receiving permission, Bob can browse the cloud storage system and view the files that are available to him based on his access rights. He is also allowed to upload files securely into the system for

storage and sharing purposes. This process ensures secure authentication, controlled resource allocation, and safe file management within the cloud platform.



Server

The server plays an important role in managing authentication, virtual machine allocation, and resource monitoring within the cloud computing environment. Users can securely connect to the server by entering their valid user ID and password. After successful login, users are allowed to access cloud services based on their permissions. When a user submits a request for a virtual machine, the server reviews the request and verifies the availability of resources. Once the request satisfies the required conditions, the server approves and allocates the virtual machine to the user. The server is also responsible for controlling and managing all approval processes to ensure secure and authorized access to resources. In addition, the server continuously monitors system performance and resource usage. It can display the amount of memory currently consumed as well as the free memory available in the system. This helps maintain efficient resource utilization, improves system performance, and ensures smooth operation of cloud services for all users.



Proposed Algorithm

Self-Sovereign Identity (SSI) is a user-centric, decentralized approach to identity management that enables entities, i.e., identity holders, to control their digital identities (identifiers and identity data) fully without relying on any external, central authority for identity provisioning, management, and storage. Thus, it strives to minimize or even eliminate entirely, reliance on intermediaries acting as CAs or IdPs in digital interactions, tackling the challenges and concerns of traditional, centralized approaches, such as SPOF, centralized control and data storage, vendor locking, personal data misuse, connected to data breaches, leaks, and identity thefts, as well as other privacy and security threats It empowers entities to be in control of their identity and data flow during digital interactions, and presents a means for digital identification, authentication, and authorization. It allows entities to (1) create

and manage an unlimited number of unique Decentralized Identifiers (DIDs) for different interactions independently of any external entity, i.e., centralized authority, (2) establish relationships (i.e., peer-to-peer connections) with different stakeholders (i.e., service and resource providers, SP and RP, providing value to the end users) within the SSI ecosystem, (3) obtain identity data/attributes/claims in the form of Verifiable Credentials (VCs) from various sources (i.e., third-party credential issuers).

IV. EXPERIMENATAL RESULTS

This project is implements like web application using COREJAVA and the Server process is maintained using the SOCKET & SERVERSOCKET and the Design part is played by Cascading Style Sheet.

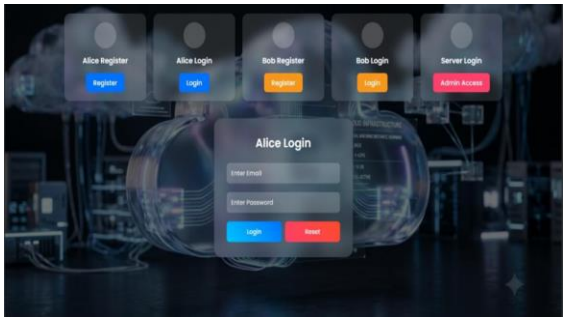


Fig. 2: Alice Login

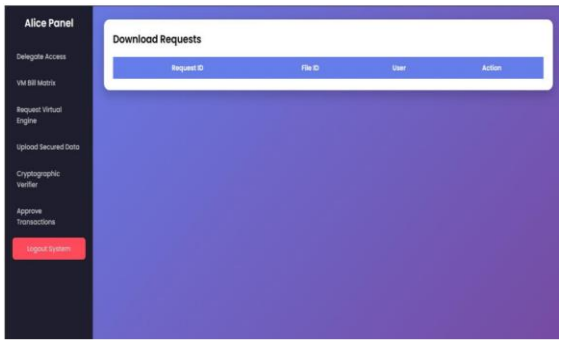


Fig. 2: Alice Panel



Fig. 3: Upload File

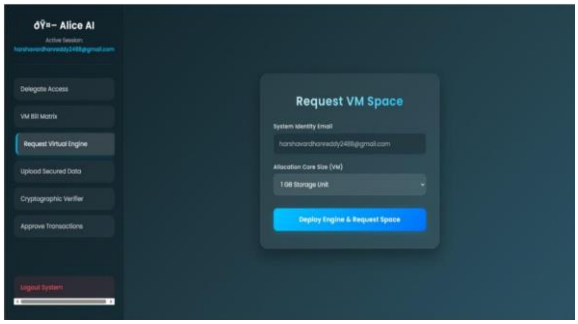


Fig. 4: Request VM Space



Fig. 5: Server Login

V. CONCLUSION

Digital identification, authentication, and authorization are important aspects of ensuring the security and reliability of digital interactions. By utilizing the SSI approach, we can simplify these processes and enable users, i.e., identity holders, to gain control over their digital identity and data. SSI brings many advantages, and reduces the shortcomings of the traditional, centralized Identity and Access Management (IAM) system that we highlighted in the introductory sections (Section I - II), e.g., centralization, intermediaries, SPOF, identity abuse and theft, security and privacy issues, etc. It represents a significant leap in the field of IAM, and it brings many advantages, such as decentralization, control, user-centricity, improved security, privacy, sovereignty, data minimization, selective disclosure, interoperability, and mobile-first design.

REFERENCES

[1] Q. Pham, J. Reid, A. McCullagh, and E. Dawson, ‘‘On a taxonomy of delegation,’’ Comput. Secur., vol. 29, no. 5, pp. 565–579, Jul. 2010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404809001473

[2] A. Ali, U. Habiba, and M. A. Shibli, ‘‘Taxonomy of delegation model,’’ in Proc. 12th Int. Conf. Inf. Technol. - New Generat., Apr. 2015, pp. 218–223. [Online]. Available: https://ieeexplore.ieee.org/document/7113476

[3] G. Yin, D. Shi, M. Guo, and H. Wang, ‘‘SRDL: A simple rolebased delegation logic,’’ in IEEE MTT-S Int. Microw. Symp. Dig., Aug. 2009, pp. 913–916. [Online]. Available: https://ieeexplore.ieee.org/document/5331636

[4] Š. Čučko, Š. Bećirović, A. Kamišalić, S. Mrdovic, and M. Turkanović, ‘‘Towards the classification of self-sovereign identity properties,’’ IEEE Access, vol. 10, pp. 88306–88329, 2022. [Online]. Available:https://ieeexplore.ieee.org/document/9858139

[5] E. Commission. (2024). A Digital Id and Personal Digital Wallet for Eu Citizens, Residents and Businesses. [Online]. Available: https://ec.europa.eu/digitalbuildingblocks/sites/display/EUDIGITALIDENTITYWALLET

[6] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen. (2022). Decentralized Identifiers (DIDS) V1.0. [Online]. Available: https://www.w3.org/TR/didcore

[7] M. Sporny, D. Longley, and D. Chadwick. (2022). Verifiable Credentials Data Model 1.1. [Online]. Available: https://www.w3.org/TR/vc-datamodel- 1.1

[8] M. Sporny, D. Longley, D. Chadwick, and O. Steele. (2024). Verifiable Credentials Data Model 2.0. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0

[9] A. Abraham, S. More, C. Rabensteiner, and F. Hörandner, ‘‘Revocable and offlineverifiable self-sovereign identities,’’ in Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom), Dec. 2020, pp. 1020–1027. [Online]. Available: https://ieeexplore.ieee.org/document/9343191

AUTHORS Profile



Mr. PRIYA RANJAN RAJ has received his B.Tech in Computer Science from MIT University, Meghalaya in 2019, M.Tech in Computer science from Chandigarh University, Mohali, Punjab in 2021 and Pursuing Ph.D degree in Computer Science from Chandigarh University, Mohali, Punjab . He is dedicated to teaching field from the last 4 years. His research area Networking, Edge Computing and IOT. At present He is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus ,Ibrahimpatnam, Telangana, India.



Mr. ILENI ANUDEEP REDDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. CHITTI AJAY REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. NAINI HARSHA VARDHAN REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. GADADASU SATEESH pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.