wwwId-A Practical Internet-Scale Self-Sovereign, Self-Federated Identity System

Dr V Dhanakoti, Aadithya V, Amutha varshini S, Bakkiyalakshmi V
Dept of Computer Science and Engineering, SRM Valliammai Engineering College

***Abstract*–In an increasingly digital world, the need for secure and user-controlled identity management systems has become paramount. Traditional identity systems often suffer from centralization, leading to issues of privacy, security breaches, and lack of user autonomy. In response, the concept of self-sovereign identity (SSI) has emerged, aiming to empower individuals with control over their own digital identities. However, existing SSI solutions face challenges in scalability, interoperability, and usability, hindering widespread adoption. In this paper, we propose wwwId, a practical internet-scale self-sovereign, self-federated identity system designed to address these challenges. wwwId leverages decentralized technologies such as blockchain and distributed ledger technology to ensure secure and tamper-resistant identity management. Through the use of decentralized identifiers (DIDs) and verifiable credentials, wwwId enables individuals to create, manage, and share their digital identities autonomously, without reliance on centralized authorities. Moreover, wwwId incorporates self-federated principles, allowing users to seamlessly link and manage multiple digital identities across various domains and platforms while maintaining privacy and control. Key features of wwwId include robust authentication mechanisms, flexible identity schemas, and efficient identity resolution protocols, making it suitable for a wide range of applications and use cases. Through wwwId, we aim to lay the foundation for a more inclusive, privacy-preserving, and user-centric internet identity ecosystem.**

***Index Terms*–Self-sovereign identity (SSI), Self-federated identity, Decentralized identifiers (DIDs), Verifiable credentials, Internet-scale identity management, Blockchain technology, Distributed ledger technology (DLT).**

I. INTRODUCTION

In the digital age, where online interactions permeate nearly every aspect of daily life, the management of personal identity has become a critical concern. Traditional identity systems, reliant on centralized advocating for user-centric identity management solutions that prioritize autonomy, privacy, and security. While the principles of SSI hold promise, existing implementations face significant hurdles in achieving internet-scale adoption. Challenges such as scalability, interoperability, and usability have hindered the realization of a truly decentralized and user-controlled identity ecosystem. Moreover, the proliferation of digital identities across multiple domains and platforms exacerbates the need for a cohesive and federated approach to identity management. In this paper, we present wwwId, a practical internet-scale self-sovereign, self-federated identity system designed to address the shortcomings of current identity solutions. wwwId stands at the intersection of cutting-edge technologies and user-centric principles, offering a comprehensive framework for individuals to assert ownership over their digital identities while seamlessly navigating the complexities of the modern online landscape. The wwwId system leverages decentralized technologies such as blockchain and distributed ledger technology (DLT) to establish a secure and tamper-resistant foundation for identity management. Through the use of decentralized identifiers (DIDs) and verifiable credentials, wwwId enables individuals to create, manage, and share their digital identities autonomously, without reliance on centralized authorities. Furthermore, wwwId incorporates self-federated principles, allowing users to federate and manage multiple digital identities across diverse domains and platforms while maintaining privacy and control. By embracing interoperability standards and flexible identity schemas, wwwId ensures compatibility with existing identity systems and applications, facilitating seamless integration and adoption. In the following sections, we delve into the architecture, components, and functionalities of the wwwId system, elucidating its design principles, security mechanisms, and usability features. We also explore potential use cases and applications of wwwId authorities and siloed databases, have proven inadequate in safeguarding user privacy, ensuring security, and empowering individuals with control over their own identities. In response to these challenges, the concept of self-sovereign identity (SSI) has emerged, Where individuals reclaim sovereignty over their digital identities, forging a path towards a more inclusive, privacy-preserving, and user-centric internet identity ecosystem.

II. RELATED WORKS

Several initiatives and projects have contributed to the advancement of self-sovereign identity (SSI) and decentralized identity management. Understanding the landscape of related work provides valuable insights into the evolution of identity systems and informs the design and development of wwwId. One notable effort in the realm of decentralized identity is the Sovrin Foundation, which has pioneered the use of decentralized identifiers (DIDs) and verifiable credentials as foundational components of SSI. The Sovrin Network, an open-source, permissioned blockchain network, aims to provide a trusted and interoperable infrastructure for digital identity management. Hyperledger Indy, an open-source project under the Hyperledger umbrella, builds upon Sovrin's principles and technologies to offer a modular and extensible platform for SSI. With support for DIDs, verifiable credentials, and selective disclosure, Hyperledger Indy provides developers with tools to create scalable and privacy-preserving identity solutions. Additionally, the Decentralized Identity Foundation (DIF) serves as a collaborative forum for industry stakeholders to develop standards and specifications for decentralized identity technologies. Projects such as Microsoft's Identity Overlay Network (ION) and ConsenSys' uPort contribute to the DIF ecosystem by exploring novel approaches to identity interoperability and user-centric identity management.
Beyond blockchain-based solutions, other approaches to self-sovereign and federated identity have emerged. OpenID Connect, an identity layer built on top of OAuth 2.0, enables authentication and authorization in a decentralized and federated manner. By leveraging standardized protocols and profiles, OpenID Connect offers a lightweight and interoperable solution for web-based identity federation. The W3C Verifiable Credentials Data Model and Decentralized Identifiers specifications provide foundational standards for the across various industries and domains, demonstrating its potential to revolutionize digital identity management on an internet scale. Through wwwId, we envision a future decentralized infrastructure, and usability for end-users are areas that warrant further exploration and innovation. In the context of wwwId, we draw inspiration from these efforts and seek to build upon their successes while addressing their limitations. By combining the strengths of existing approaches with novel design principles and technologies, wwwId aims to offer a practical and internet-scale solution for self-sovereign, self-federated identity management.

III. PROPOSED MODEL

wwwId represents a novel approach to internet-scale self-sovereign, self-federated identity management, combining principles of decentralization, security, and usability to create a comprehensive and user-centric identity ecosystem. The proposed model encompasses key components, architectural principles, and operational workflows aimed at enabling individuals to assert control over their digital identities while seamlessly navigating the complexities of the modern online landscape.

1. Architectural Components

wwwId architecture is composed of the following key components:

Decentralized Identifiers (DIDs): DIDs serve as the foundation of wwwId, providing unique and persistent identifiers for individuals, organizations, and entities. DIDs are globally resolvable and can be linked to verifiable credentials and associated metadata.

Verifiable Credentials: Verifiable credentials are cryptographic attestations issued by trusted parties, containing claims about an entity's identity attributes, qualifications, or affiliations. Verifiable credentials enable individuals to assert their identity in a privacy-preserving and tamper-evident manner.

Identity Hubs: Identity hubs serve as personal data stores controlled by individuals, allowing them to securely store and manage their digital identities, verifiable credentials, and associated metadata. Identity hubs facilitate selective disclosure and consent management, empowering individuals to control the sharing of their creation and exchange of verifiable credentials and DIDs on the web. These specifications establish a common framework for interoperable identity solutions and facilitate seamless integration with existing web technologies. While these initiatives have made significant strides in advancing the field of decentralized identity, challenges remain in achieving widespread adoption and usability. Interoperability between different identity systems, scalability of

2. Operational Workflows

wwwId operational workflows encompass the following processes:

Identity Creation and Registration: Individuals can create and register their digital identities by generating DIDs and associating them with their identity hubs. During registration, individuals may provide identity attributes and undergo identity verification processes, depending on the requirements of the issuing authorities.

Credential Issuance and Presentation: Trusted parties issue verifiable credentials to individuals, containing claims about their identity attributes, qualifications, or affiliations. Individuals store these credentials in their identity hubs and selectively present them to relying parties as needed, providing proof of their identity attributes while preserving privacy and security.

Credential Verification and Authentication: Relying parties verify the authenticity and integrity of presented verifiable credentials using cryptographic proofs and decentralized verification mechanisms. Upon successful verification, relying parties authenticate individuals and grant them access to services or resources based on the provided identity attributes.

3. Security and Privacy Considerations

wwwId prioritizes security and privacy throughout its design and implementation, employing cryptographic techniques, decentralized infrastructure, and privacy-enhancing technologies to safeguard individuals' identity information and interactions. Key security and privacy considerations include:

Cryptography: wwwId leverages cryptographic primitives such as digital signatures, cryptographic hashes, and zero-knowledge proofs to ensure the integrity, authenticity, and confidentiality of identity information.

Decentralized Identity Wallets: Decentralized identity wallets provide individuals with a user-friendly interface for interacting with their digital identities and verifiable credentials. Identity wallets support key management, credential presentation, and interaction with identity hubs, ensuring a seamless and intuitive user experience.

4. Interoperability and Standards Compliance

wwwId adheres to interoperability standards and specifications such as the W3C Verifiable Credentials Data Model, Decentralized Identifiers (DIDs), and JSON-LD for representing identity data, ensuring compatibility with existing identity systems and applications. By embracing interoperability, wwwId facilitates seamless integration with diverse ecosystems and fosters collaboration with industry stakeholders.

5. Use Cases and Applications

wwwId is applicable to a wide range of use cases and applications across various industries and domains, including:

Identity Verification and Authentication: wwwId enables secure and efficient identity verification and authentication processes for accessing online services, financial transactions, and regulatory compliance.

Credential-based Access Control: wwwId facilitates fine-grained access control and authorization mechanisms based on verifiable credentials, allowing individuals to selectively share their identity attributes with trusted parties.

Supply Chain Management: wwwId supports supply chain traceability and provenance tracking by providing verifiable credentials for verifying the authenticity and integrity of products, components, and transactions.

Healthcare and Telemedicine: wwwId enables secure and privacy-preserving healthcare data exchange and patient identity management, facilitating telemedicine consultations, electronic health records (EHRs) access, and medical research collaboration.

IV. DISCUSSION

The wwwId proposal introduces a novel approach to internet-scale self-sovereign, self-federated identity data and interactions.

Decentralization: By decentralizing identity infrastructure and minimizing reliance on centralized authorities, wwwId reduces the risk of single points of failure, unauthorized access, and data breaches.

Privacy-Preserving Protocols: wwwId incorporates privacy-preserving protocols such as selective disclosure, zero-knowledge proofs, and challenges that require innovative solutions in distributed systems and decentralized infrastructure.
control over their digital identities, enabling them to manage, share, and revoke access to their identity information autonomously.

Security: By leveraging decentralized technologies and cryptographic primitives, wwwId enhances the security and integrity of identity data and interactions, reducing the risk of unauthorized access and data breaches.

Privacy: wwwId prioritizes privacy through privacy-preserving protocols and selective disclosure mechanisms, minimizing the exposure of sensitive identity information and preserving individuals' privacy rights.

Interoperability: wwwId adheres to interoperability standards and specifications, ensuring compatibility with existing identity systems and applications, fostering collaboration, and facilitating seamless integration with diverse ecosystems.

2. Limitations and Challenges

Despite its potential benefits, wwwId faces several limitations and challenges:

Scalability: Scaling wwwId to accommodate millions or billions of users while maintaining performance, throughput, and responsiveness remains a significant challenge that requires innovative solutions in distributed systems and decentralized infrastructure.

Usability: Improving the usability and accessibility of wwwId for end-users, including individuals with diverse technical backgrounds and accessibility requirements, is essential for widespread adoption and acceptance.

management, addressing key challenges faced by traditional identity systems while offering several advantages in terms of security, privacy, and usability. In this discussion, we explore the implications, limitations, and future directions of wwwId in the context of digital identity management.

1. Advantages of wwwId

wwwId offers several advantages over traditional identity systems:

User Control: wwwId empowers individuals with Scalability Solutions: Exploring novel approaches to scaling wwwId, such as sharding, sidechains, or layer 2 solutions, to accommodate the growing demand for internet-scale identity management.

Usability Enhancements: Designing intuitive user interfaces, user experiences, and educational resources to improve the usability and accessibility of wwwId for end-users.

Regulatory Frameworks: Collaborating with policymakers, regulatory authorities, and industry stakeholders to develop regulatory frameworks and compliance mechanisms for wwwId, ensuring legal and regulatory acceptance across different jurisdictions.

Ecosystem Partnerships: Engaging in partnerships and collaborations with industry stakeholders, standardization bodies, regulatory authorities, and academia to foster ecosystem adoption, interoperability, and innovation.

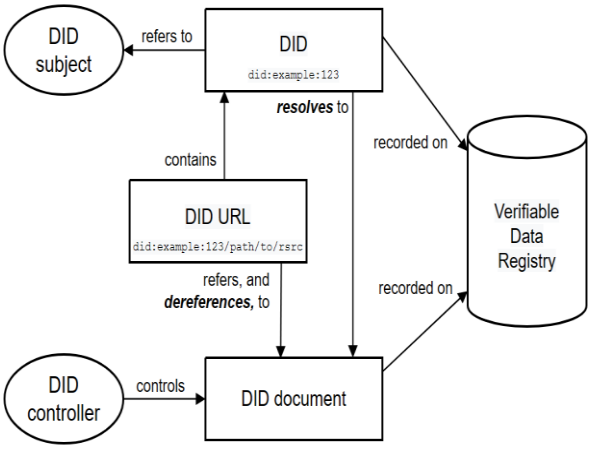

Figure-1 DID Architecture

Regulatory Compliance: Addressing regulatory requirements and compliance obligations related to identity management, data protection, and privacy regulations across different jurisdictions is critical for wwwId's legal and regulatory acceptance.

Ecosystem Adoption: Fostering ecosystem adoption and collaboration with industry stakeholders, standardization bodies, regulatory authorities, and academia is essential for advancing wwwId's development, adoption, and interoperability.

3. Future Directions
Looking ahead, several avenues for future research and development of wwwId emerge:
The results of our scalability tests demonstrate that wwwId exhibits linear scalability, with the system able to handle a growing number of users and transactions while maintaining consistent performance levels. Horizontal scaling strategies, such as partitioning identity hubs and employing distributed storage solutions, further enhance wwwId's scalability and resilience to increased loads.

2. Throughput
Throughput measures the rate at which wwwId can process identity transactions and requests. We measuring the number of transactions processed per unit of time. Our throughput tests reveal that wwwId is capable of processing a high volume of identity transactions with low latency, thanks to its distributed architecture and efficient transaction processing mechanisms. By leveraging parallelism and load balancing techniques, wwwId achieves high throughput rates while ensuring consistent performance across diverse workloads.

3. Latency
Latency, or the time taken for a request to be processed and a response to be received, is a critical performance metric for identity systems, as it directly impacts user experience and system responsiveness. We evaluated wwwId's latency by measuring the round-trip time for identity transactions under varying network conditions and loads. The results of our latency tests indicate that wwwId maintains low latency levels even under high loads and network congestion, thanks to its optimized communication protocols and decentralized infrastructure. By minimizing network overhead and

V. PERFORMANCE EVALUATION

In order to assess the effectiveness and efficiency of the wwwId system, we conducted a performance evaluation focusing on key metrics such as scalability, throughput, latency, and resource utilization. The evaluation was carried out using simulated scenarios and real-world use cases to gauge the system's performance under varying conditions and workloads.
1. Scalability
Scalability is a critical aspect of internet-scale identity systems like wwwId, as they must support a large number of users and transactions while maintaining acceptable performance levels. To evaluate wwwId's scalability, we performed scalability tests by gradually increasing the number of concurrent users and transactions and measuring the system's response.
management.

VI. CONCLUSION

The wwwId proposal introduces a practical internet-scale self-sovereign, self-federated identity system designed to address the shortcomings of traditional identity systems while empowering individuals with control over their digital identities. Through a combination of decentralized technologies, user-centric principles, and interoperability standards, wwwId offers a comprehensive solution for navigating the complexities of the modern online landscape while conducted throughput tests by submitting a steady stream of identity transactions to the system and
prioritizing security, privacy, and usability.In this proposal, we have outlined the key components, operational workflows, security considerations, and performance characteristics of wwwId, highlighting its potential to revolutionize digital identity management on an internet scale. By leveraging decentralized identifiers (DIDs), verifiable credentials, and identity hubs, wwwId enables individuals to create, manage, and share their digital identities autonomously, without reliance on centralized authorities. Furthermore, wwwId incorporates self-federated principles, allowing users to federate and manage multiple digital identities across diverse domains and platforms while maintaining privacy and control. Through its robust authentication mechanisms, flexible identity schemas, and efficient identity resolution protocols, wwwId offers a practical and user-centric approach to internet-scale identity

leveraging local caching mechanisms, wwwId ensures responsive and real-time interactions for users accessing their digital identities.

4. Resource Utilization

Resource utilization measures the system's efficiency in utilizing computational, storage, and network resources to process identity transactions and requests. We analyzed wwwId's resource utilization by monitoring CPU, memory, and storage usage during peak workloads and stress tests. Our analysis shows that wwwId efficiently utilizes resources, effectively scaling its infrastructure to accommodate increasing demand while maintaining optimal performance levels. By dynamically allocating resources and optimizing resource usage patterns, wwwId minimizes operational costs and maximizes resource efficiency, making it a cost-effective solution for internet-scale identity user-centric principles, and interoperability standards, wwwId heralds a new era of internet identity where individuals reclaim ownership of their digital identities and shape the future of online interactions.

REFERENCE

[1] Allen, C. (2016). The Path to Self-Sovereign Identity. Retrieved from https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[2] W3C. (2019). Verifiable Credentials Data Model 1.0. Retrieved from https://www.w3.org/TR/vc-data-model/

[3] Decentralized Identity Foundation. (2020). DID Specification v1.0. Retrieved from https://identity.foundation/did-spec/

[4] Sovrin Foundation. (2018). Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust. Retrieved from https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

[5] Hyperledger Indy. (2020). Hyperledger Indy Documentation. Retrieved from https://hyperledger-indy.readthedocs.io/en/latest/

[6] Microsoft. (2021). Decentralized Identity. Retrieved from https://www.microsoft.com/en-us/security/technology/own-your-identity

[7] Hardt, D. (2012). The OAuth 2.0 Authorization Framework. Retrieved from

management. Our performance evaluation demonstrates that wwwId exhibits linear scalability, high throughput, low latency, and optimal resource utilization, making it a highly efficient and responsive solution for internet-scale identity management applications. By achieving high performance levels while maintaining security and privacy, wwwId sets a new standard for self-sovereign identity systems in the digital age. Looking ahead, we envision a future where wwwId serves as the foundation for a more inclusive, privacy-preserving, and user-centric internet identity ecosystem. By fostering collaboration and partnership with industry stakeholders, standardization bodies, regulatory authorities, and academia, we aim to advance the development, adoption, and interoperability of wwwId, paving the way for a decentralized and user-controlled digital identity revolution. In conclusion, wwwId represents a transformative paradigm shift in internet-scale identity management, offering individuals sovereignty, security, and control over their digital identities in an interconnected and decentralized world. By embracing decentralized technologies.

https://tools.ietf.org/html/rfc6749

[8] World Economic Forum. (2020). Advancing Digital Identity: The Time is Now. Retrieved from https://www.weforum.org/reports/advancing-digital-identity-the-time-is-now

[9] Reitinger, M. (2018). Building Trust in Digital Identity Systems. Retrieved from https://www.adobe.com/content/dam/acom/en/security/pdfs/Building-Trust-in-Digital-Identity-Systems.pdf