Secure Backup and Recovery of SSI Wallets using Solid Pod Technology

Authors: Mohammad **Farhad**

Gourab **Saha**

Masum Alam **Nahid**

Fairuz Rahaman **Chowdhury**

Partha Pritom **Paul**

Mohammad Raihan **Ullah**

Md Sadek **Ferdous**

1 July 2024

Analytical Presentation

CONTENTS

- Introduction
- Research Objectives
- Background
- Related Work
- Proposal
- Architecture and Protocol Flows
- Discussion and Conclusion

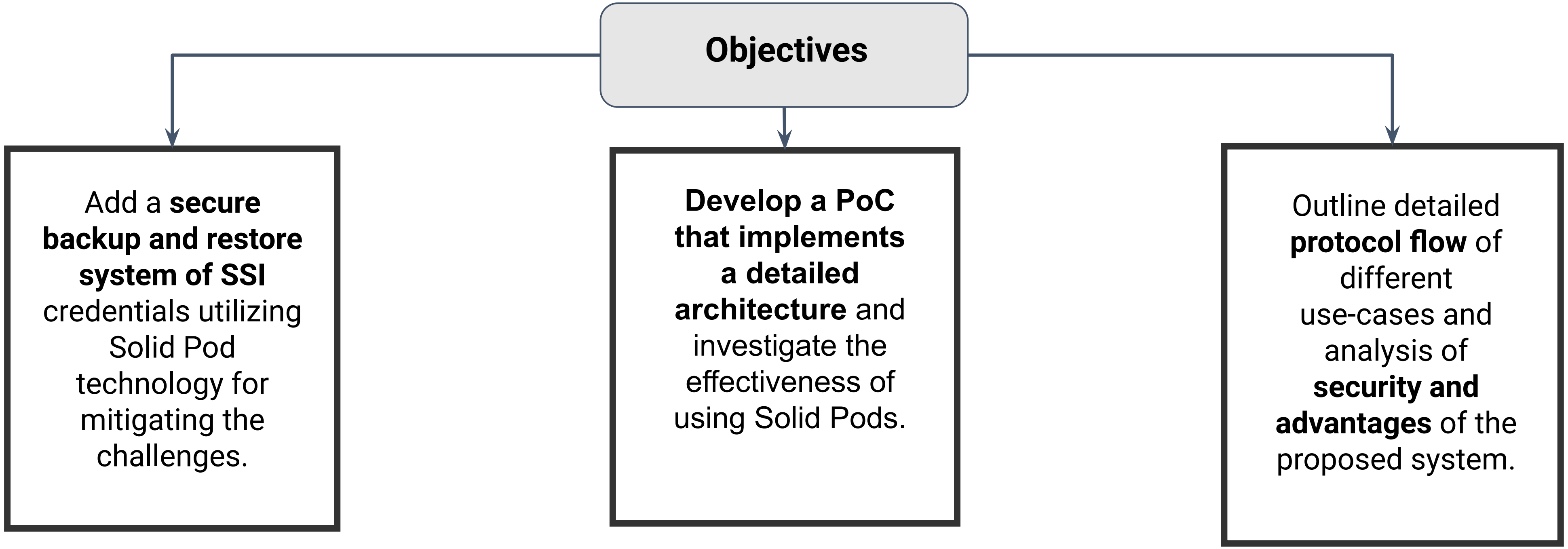
Introduction

Self-Sovereign Identity (SSI) empowers users with **control over their identity data**. A critical component of SSI is the wallet, which store cryptographic keys and identity data, often lack secure backup and recovery methods. To address this, we propose using Solid Pods, a technology by Tim Berners-Lee, for secure and decentralized storage. This research outlines the architecture, implementation, use-case protocols, and security analysis of using Solid Pods for SSI wallet backup and recovery.

Research Objectives

Motivation

- The motivation behind this research is to **address the security concerns associated with storing SSI credentials**.
- Another reason behind this research aims to **investigate the possibility of this emerging technology Solid Pod** for the secure storage of SSI credentials.



Objectives

Add a **secure backup and restore system of SSI** credentials utilizing Solid Pod technology for mitigating the challenges.

Develop a PoC that implements a detailed architecture and investigate the effectiveness of using Solid Pods.

Outline detailed **protocol flow** of different use-cases and analysis of **security and advantages** of the proposed system.

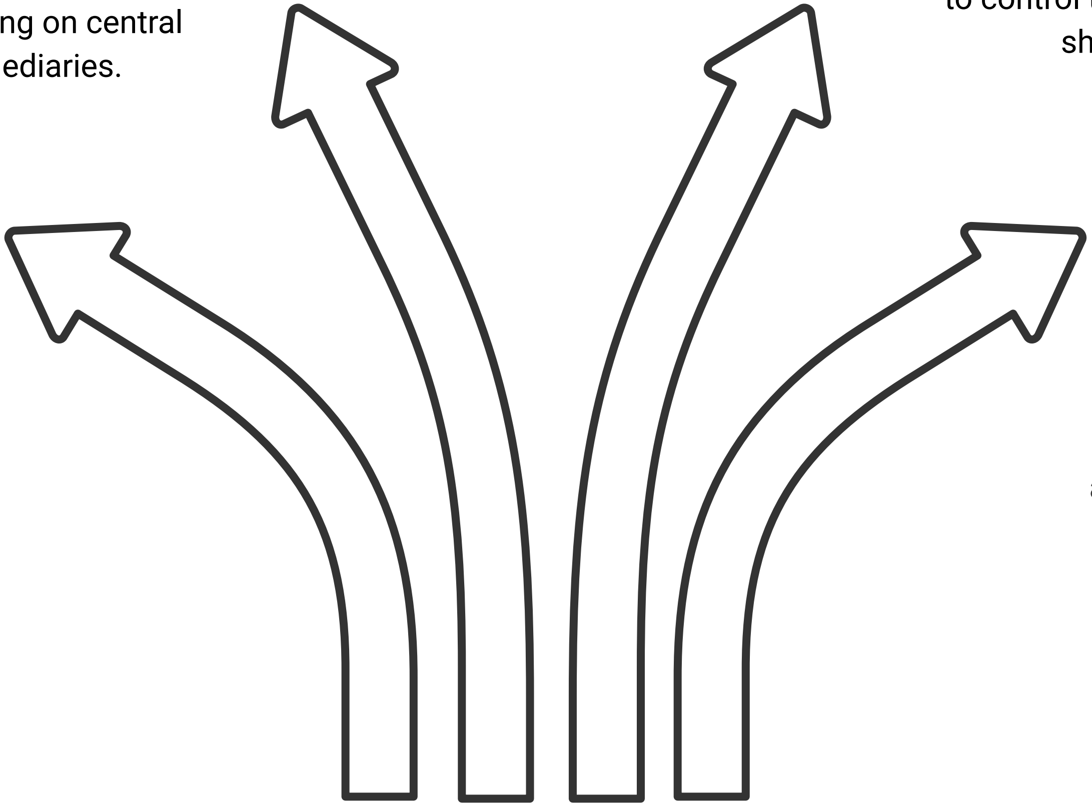
Background

Self-Sovereign Identity

Self-Sovereign Identity, a digital identity model that allows individuals to own, control, and share their personal identity information without relying on central authorities or intermediaries.

Solid Pod

Solid Pod is a decentralized data storage technology that enables users to control their personal data and share it securely.



Blockchain

Blockchain is a decentralized, distributed ledger technology that makes it possible to record transactions in a way that is safe, transparent, and impervious to manipulation.

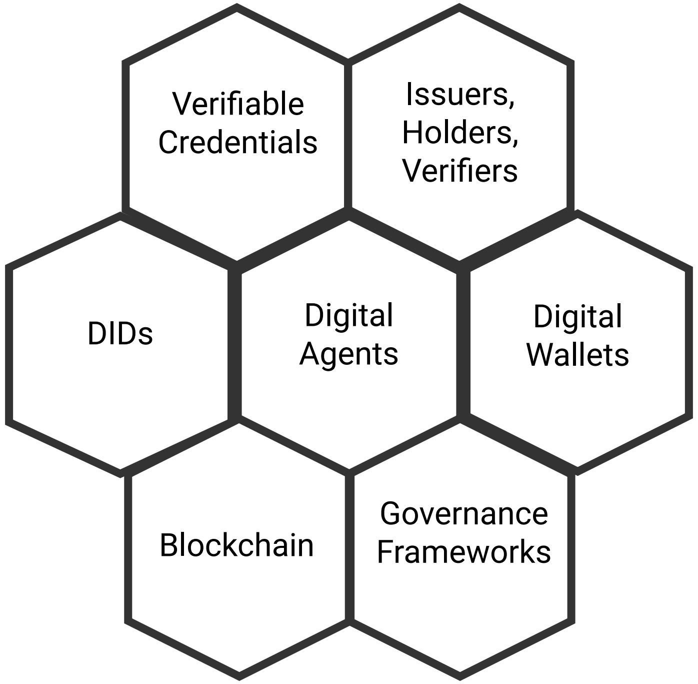
Digital Wallet

A digital wallet is a software application that allows users to store, manage, and use digital assets such as cryptocurrency and digital identity credentials.

What is Self-Sovereign Identity?

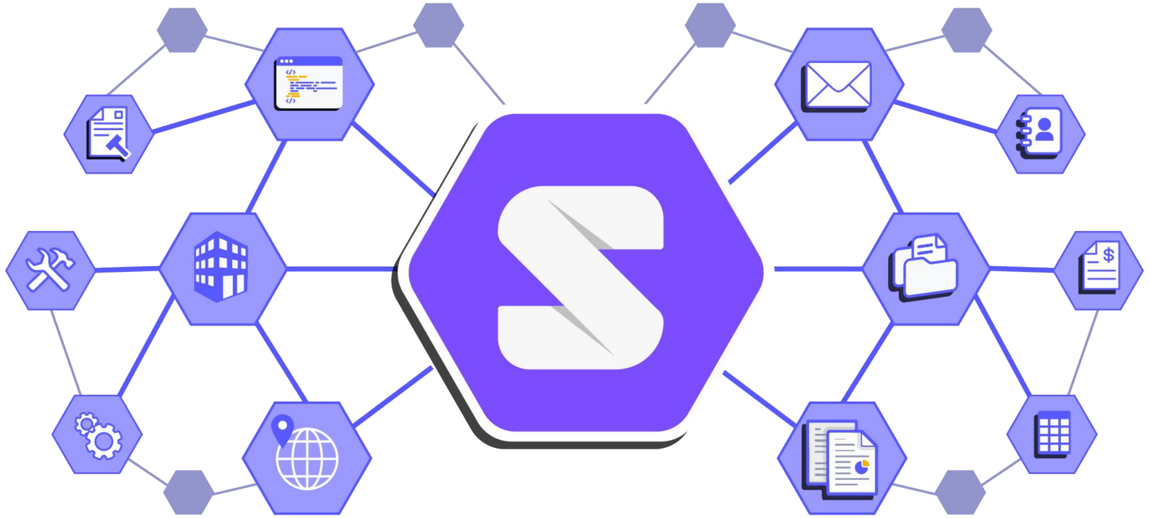
- ➢ Self-Sovereign Identity, also known as SSI, is a new paradigm for **digital identity on the internet**. SSI is for providing web services in a **secure passwordless** manner with much more **user control** and greater flexibility.

"There are **seven** building blocks of Self-Sovereign Identity."



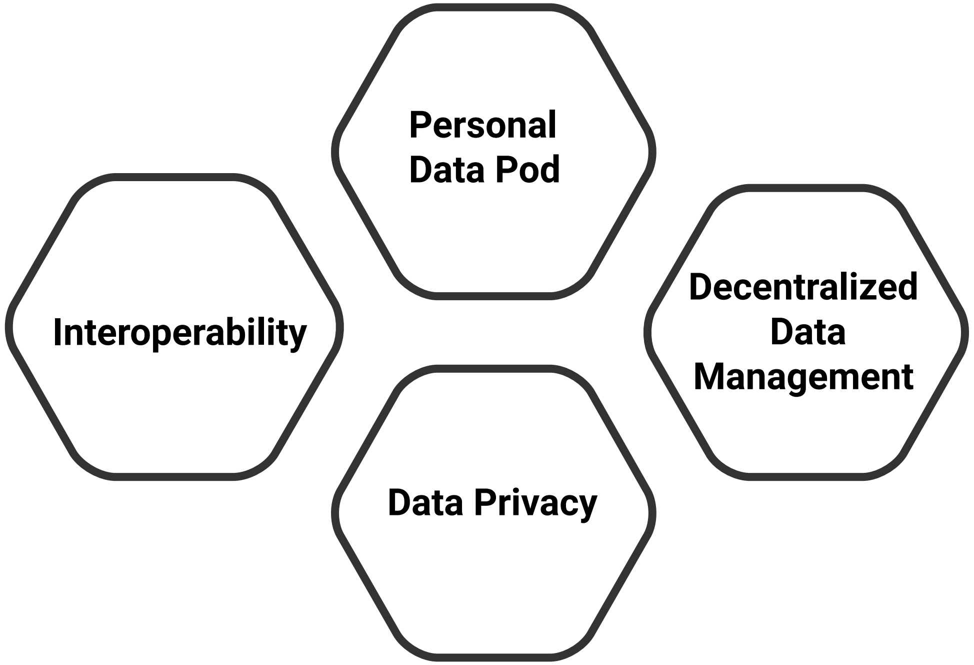
What is Solid Pod?

- ➢ Solid Pod is a technology developed by Sir Tim Berners-Lee for **decentralized** and **secure storage** of personal data in a **Personal Online Data (POD)** server, providing users with greater control over their data and **enhanced privacy and security**.



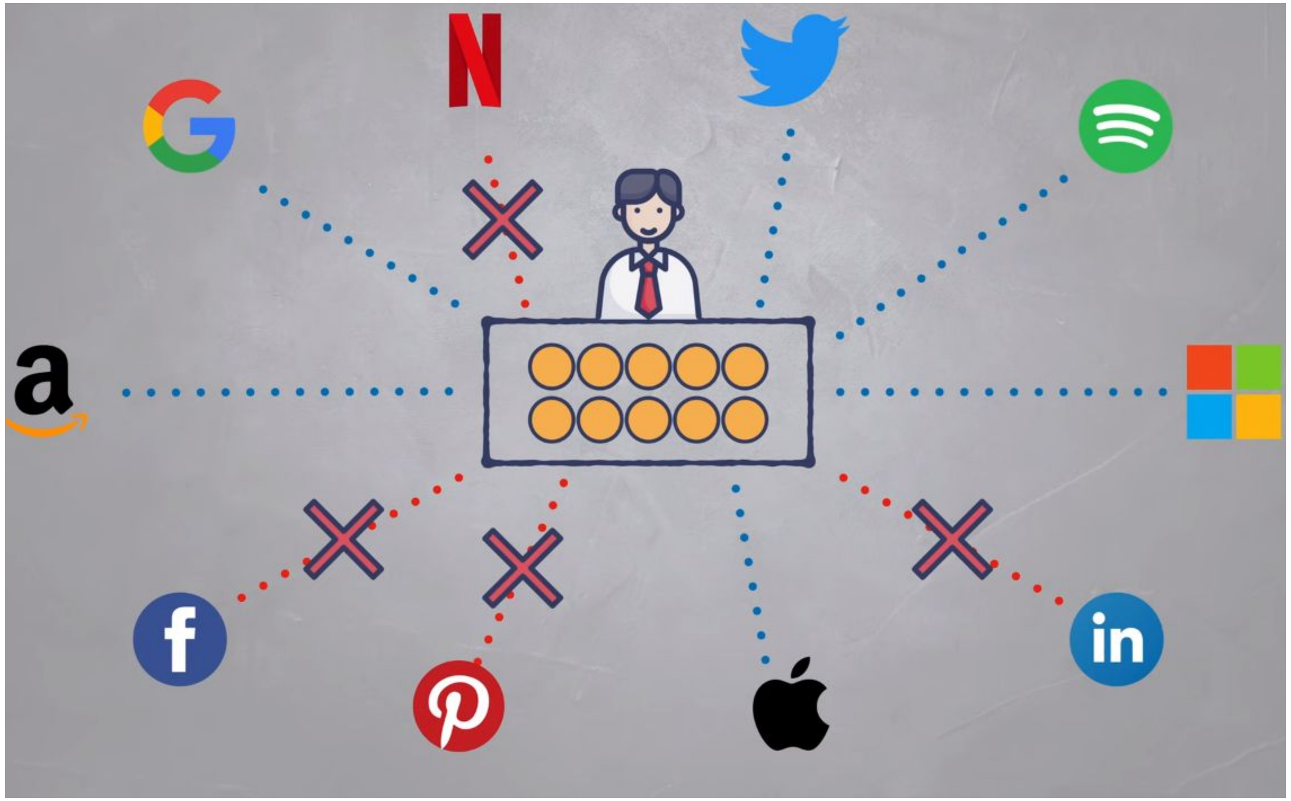
Why Solid Pod?

- ➢ **Key features of Solid Pod**



Why Solid Pod?

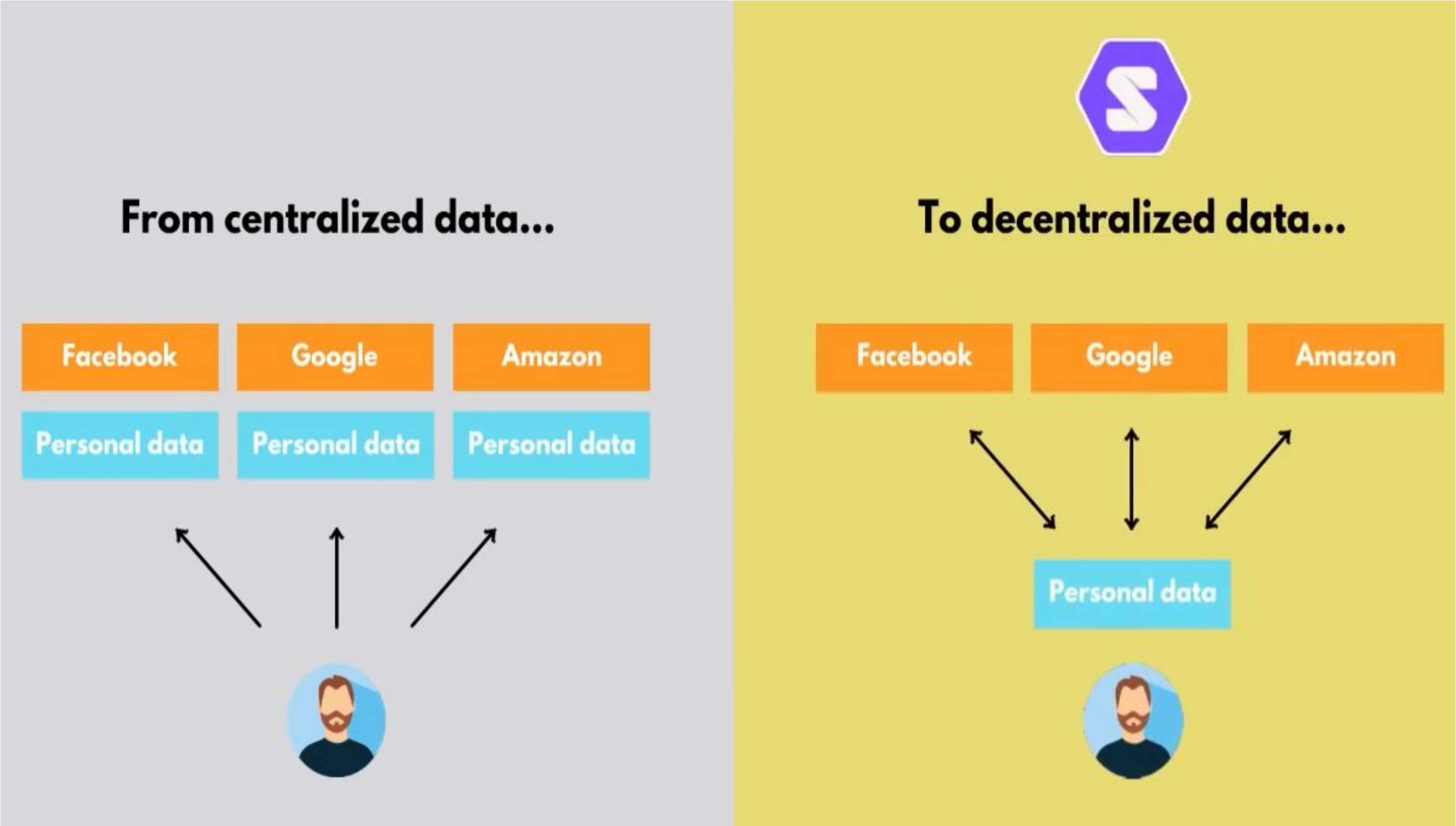
Personal Data Pod



➢ **Personal Data Pod:** Solid offers a personal data pod that serves as a **secure and private storage space for individuals' data**, granting them full control over access and sharing permissions.

Why Solid Pod?

Decentralized Data Management



- **Decentralized Data Management:** Solid provides a decentralized data management model, where individuals can store their data in a personal data pod, rather than relying on a centralized third party to store it for them.

Why Solid Pod?

Data Privacy

- **Data Privacy:** Solid provides support for secure and privacy-preserving data sharing, enabling individuals to control their data and choose what data they share and with whom they share it.

Why Solid Pod?

Interoperability

- **Interoperability:** Solid is designed to be interoperable with other web-based technologies and data formats, enabling it to work seamlessly with existing infrastructure and systems.

Related Work

❑ Authors of “*Land registry framework based on self-sovereign identity (ssi) for environmental sustainability*” proposes SSI as a solution for secure and reliable digital identity system that allows users digital identity and they also **suggested backups but using a cloud based provider**.

❑ By analyzing the backup and restoration of the system of some wallets such as “Trinsic wallet” which deals with credentials, “Metamask wallet” for cryptocurrencies and also “Exodus wallet” those proposed **a storage option in a secure location but not in solid pod server**.

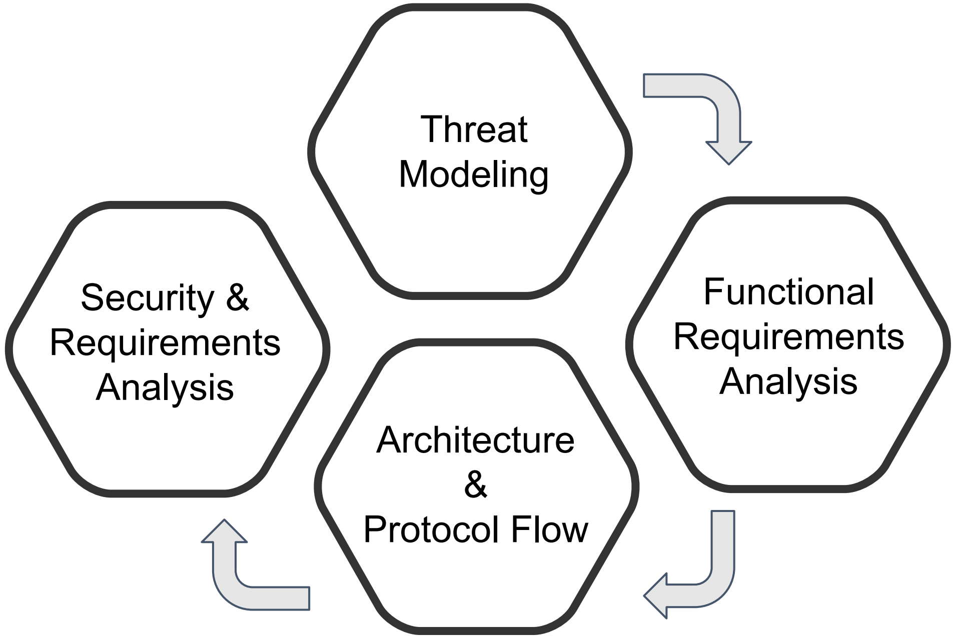
⇨ “To the best of our knowledge, there is ***limited prior research*** in the integration of SSI and Solid Pod, and **no work has been conducted on the proposed backup and restore of SSI credentials using Solid Pod in an encrypted format.** Therefore, our study aims to fill this gap by proposing a unique approach for the secure backup and restoration of SSI credentials utilizing Solid Pod technology.”

Proposal

❑ We Integrate Solid Pod that enables secure and privacy-preserving storage of SSI credentials, reducing the risk of data breaches and unauthorized access to personal data.

❑ We establish functional, security, and privacy requirements for the system along with an extensive threat model.

❑ We outline the system's architecture, integrating a digital wallet prototype and privacy-preserving data sharing using Solid Pod and its protocols.


Threat Modeling
Functional Requirements Analysis
Architecture & Protocol Flow
Security & Requirements Analysis

Threat Modeling

- Threat modeling is a structured approach to identify security risks in a software system and finding ways to mitigate them. We utilized the Microsoft **STRIDE** model for this purpose.

- The aim is to **understand security risks** and find ways to mitigate or eliminate them.

- ***T1*** involves an attacker creating a **false identity** as an authorized Pod user.

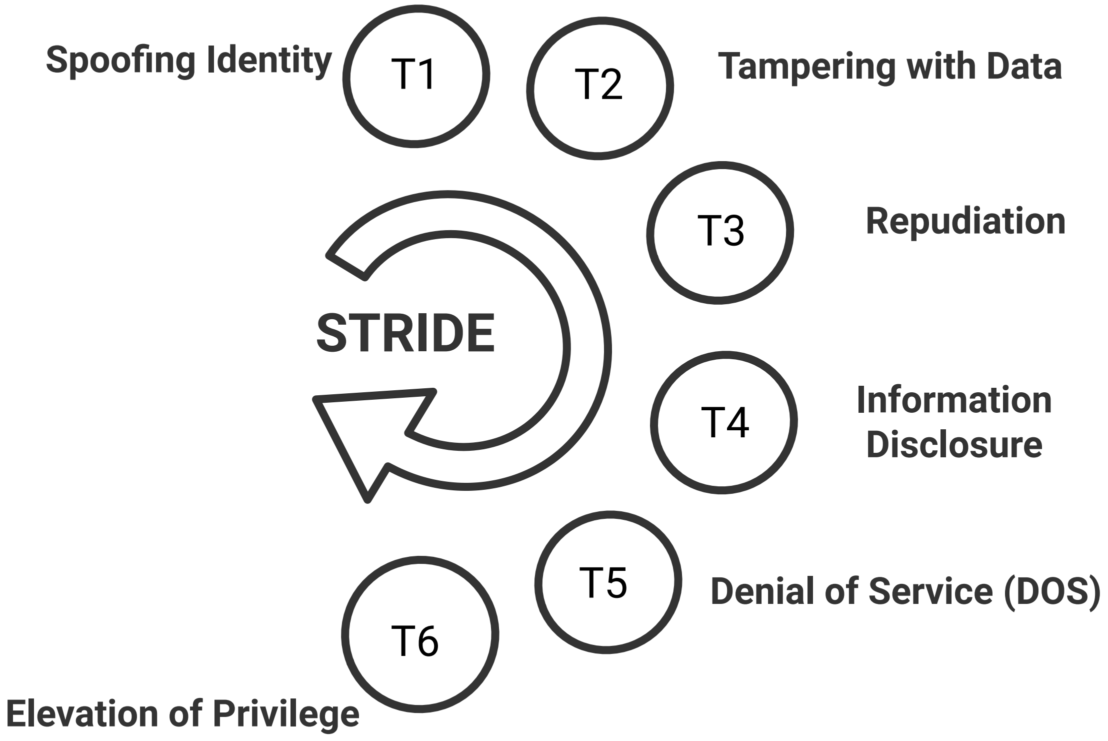
- ***T2*** indicates **corrupting** Stored Data

- ***T3*** marks act of **denying** or challenging the validity of an action.

- ***T4*** involves **exposing sensitive data** kept in the system **to an attacker**.

- ***T5*** indicates **DOS attack** to prevent legitimate users from accessing the system.

- ***T6*** marks a situation where an attacker gains **elevated access rights.**



Functional Requirements

❑ **F1:** SSI storage should have an accessible and **user-friendly interface** for easy credential management.

❑ **F2:** The system should be **compatible** with **Decentralized Identifiers** (DIDS) and **Verifiable Credentials** (VCs).

❑ **F3:** The storage solution should offer SSI credentials quick, effective access with **no/less latency** or **downtime**.

Security Requirements

❑ **S1:** By ensuring secure access to personal information on pod servers exclusively through **authorized users**, thus that can **mitigates *T1* threat**.

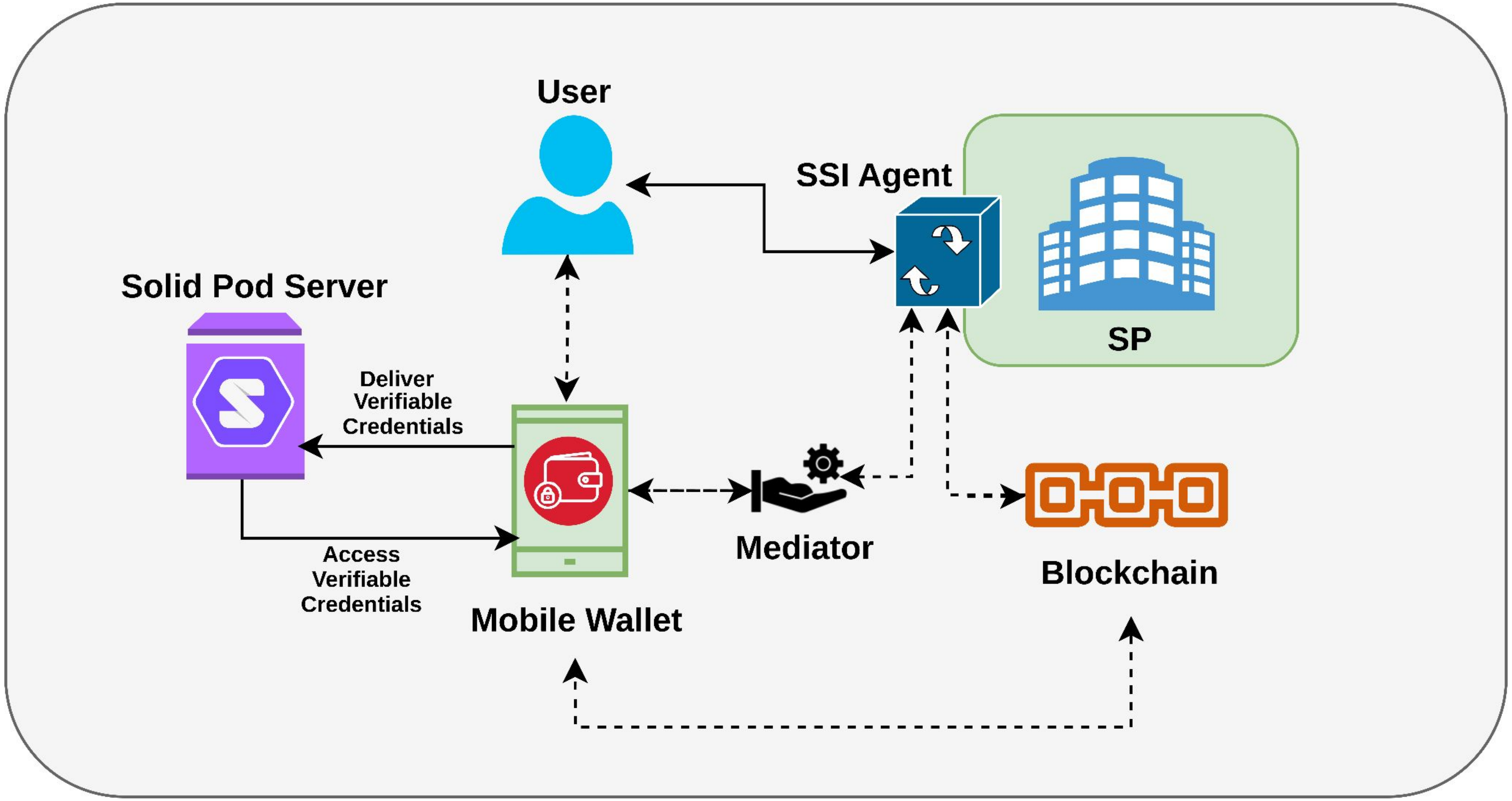
❑ **S2:** Applied **encryption** before ensuring backup and recovery, that **mitigate T2 and T3 threats**.

❑ **S3:** Includes strict access control policies, **user roles and permissions**, and monitoring and logging **to mitigate T4 threat** by limiting access to sensitive information.

❑ **S4:** Support for Notifications and Access Control Lists **to mitigate T5 threat** by informing users of content or access changes and **keeping track of information access**.

❑ **S5:** The system specification defines access control mechanisms based on Web Access Control (WAC), which enables resource owners to control **who can access their resources** which can **mitigate T6 threat**.

System Architecture



Protocol Flows

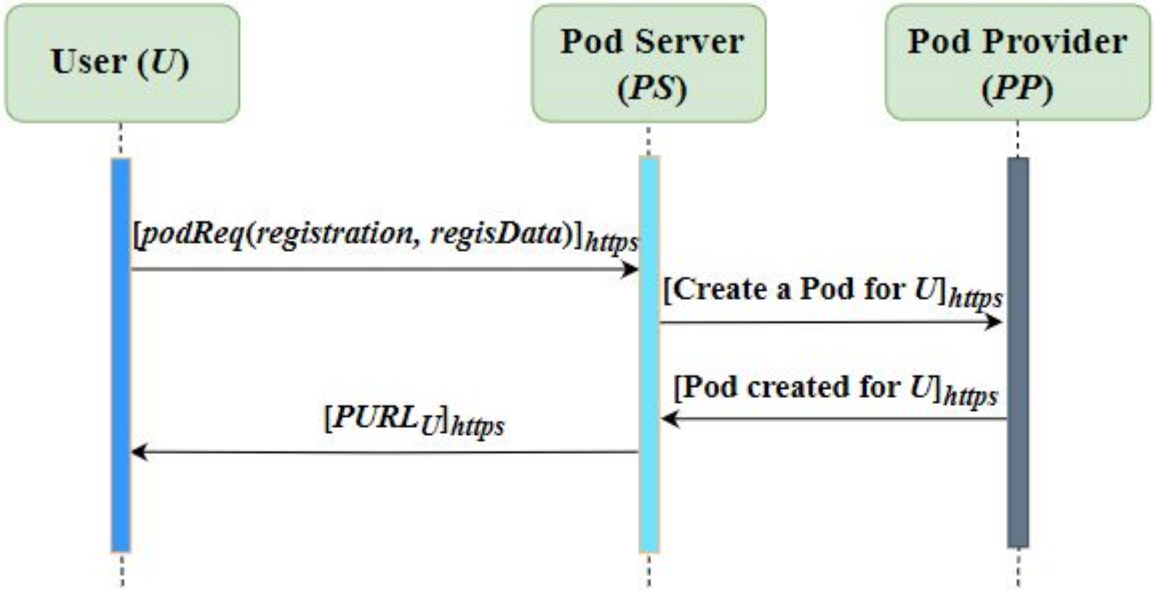


Fig. 3: Registration Protocol Flow.

- **Register and Pod creation:** Each user must register to the Pod server providing username and password. Pod server then creates a Pod storage for specific user and relay the url of the Pod denoted as **PURL$_U$** . Later users can access their pod using this PURL$_U$

Protocol Flows

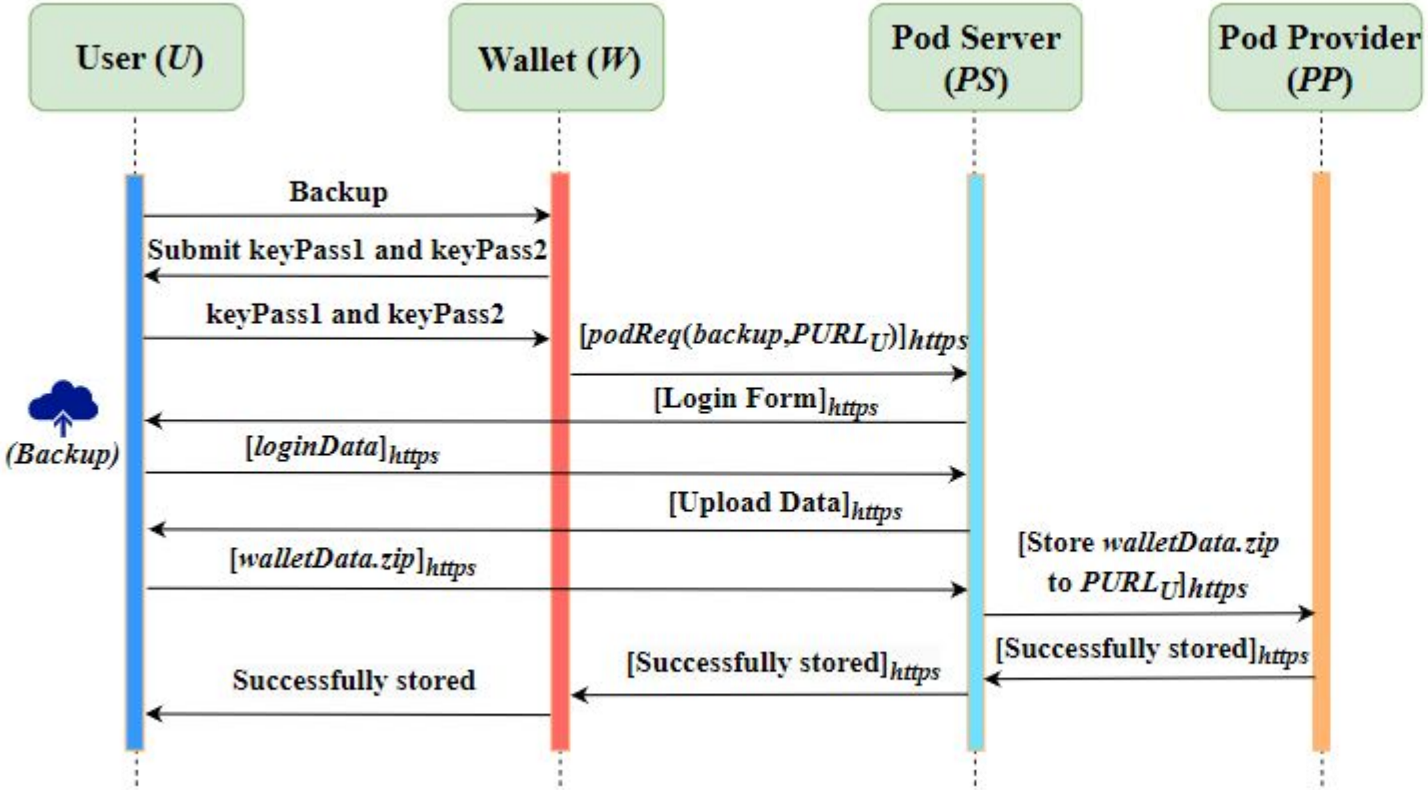

User (U)
Wallet (W)
Pod Server (PS)
Pod Provider (PP)
Backup
Submit keyPass1 and keyPass2
keyPass1 and keyPass2
[$podReq(backup,PURL_U)$]$_{https}$
[Login Form]$_{https}$
(Backup)
[$loginData$]$_{https}$
[Upload Data]$_{https}$
[$walletData.zip$]$_{https}$
[Store $walletData.zip$ to $PURL_U$]$_{https}$
[Successfully stored]$_{https}$
[Successfully stored]$_{https}$
Successfully stored

Fig. 6: Backup Protocol Flow.

- ➢ **Backup:** The process of backing up existing credentials involves the user sending their Verifiable Credential (VC) and secret key to web services for secure encryption, followed by sending a request to store the encrypted data in their Solid Pod server.

Protocol Flows

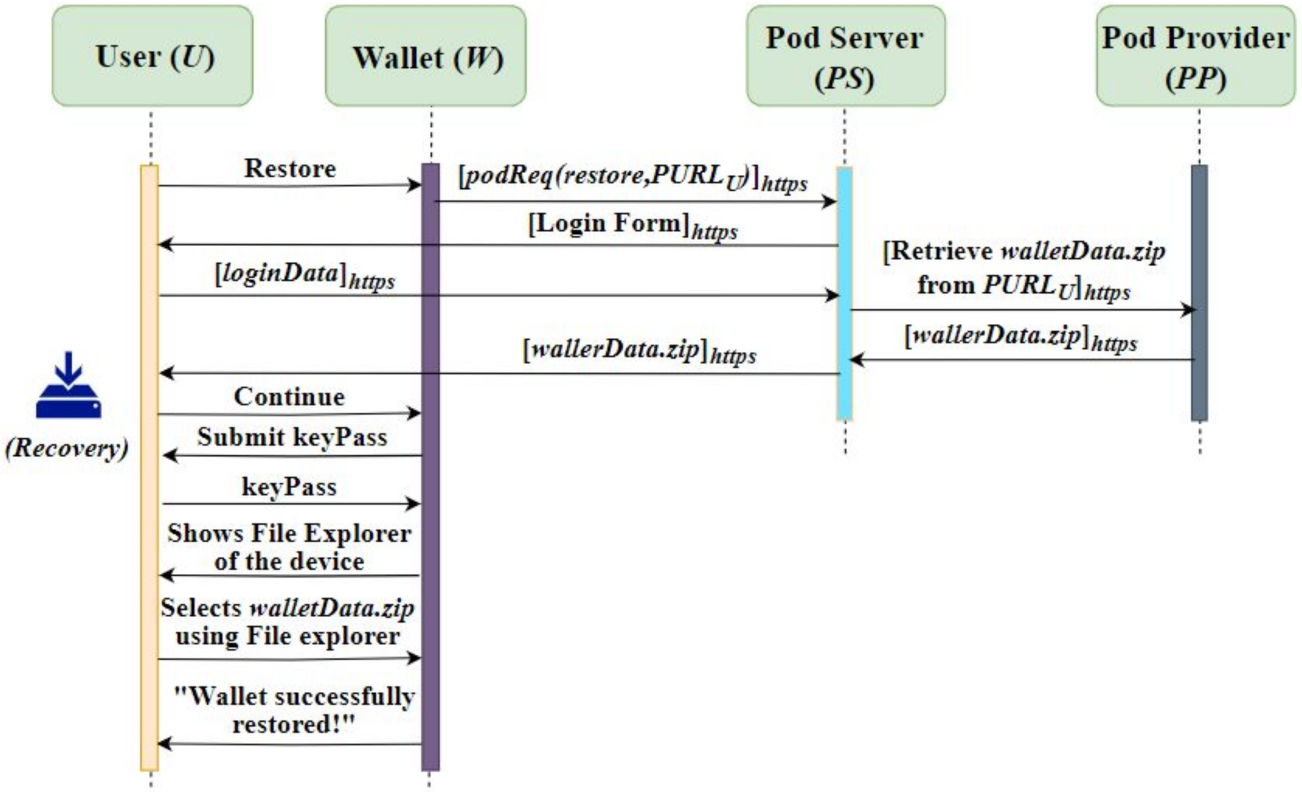

User (U)
Wallet (W)
Pod Server (PS)
Pod Provider (PP)
Restore
[$podReq(restore,PURL_U)$]$_{https}$
[Login Form]$_{https}$
[$loginData$]$_{https}$
[Retrieve $walletData.zip$ from $PURL_U$]$_{https}$
[$wallerData.zip$]$_{https}$
[$wallerData.zip$]$_{https}$
(Recovery)
Continue
Submit keyPass
keyPass
Shows File Explorer of the device
Selects $walletData.zip$ using File explorer
"Wallet successfully restored!"

Fig. 9: Recovery Protocol Flow.

- **Restore:** The process of accessing encrypted data from the pod server involves the user providing the secret key, receiving a response with stored data, decrypting it and then receiving the actual Verifiable Credential (VC) object from the web service to their wallet.

Discussion

Functional Requirement Analysis

- The system enables the user to **store, access, and manage their SSI credentials in a secure way**, with a user-friendly interface with a range of technical abilities. Our system satisfies **F1.**

- To access any SP service, **the system utilize the SSI Wallet.** That satisfies **F2.**

- The system server enables users to maintain the confidentiality of their private information by **limiting access and design for quick data retrieval**. Our system also satisfies **F3.**

Security Requirement Analysis

- The offered storage system satisfies **S1** by enabling **user access to their data and authorized** visitation to other pod servers.

- **S2** is also satisfied because data is sent in an **encrypted manner** before being backed up in a pod.

- The pod server satisfies **S3** by allowing users to manage their data and pick **what data to share and with whom to share it.**

- By limiting access to resources based on **roles and performance enhancement** by spreading traffic among several servers which satisfies **S4** and **S5** threat.

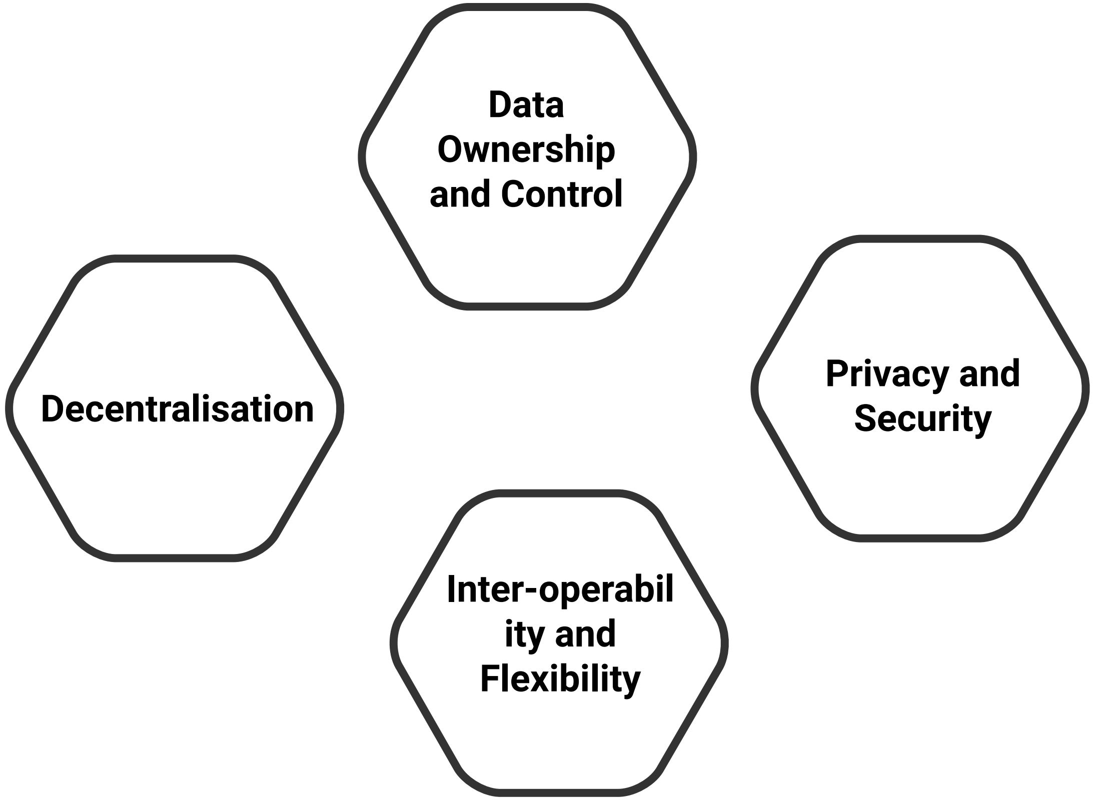
Discussion

Protocol Validation

- To evaluate the security of the system, we used the **ProVerif tool**, focusing on secrecy and authentication objectives.
- We formalized the protocol in ProVerif to **indentify potential vulnerabilities.**
- Then, we performed **a model-checking procedure** to verify specified security properties.
- The **secrecy objective** ensures that only the intended recipient can access transmitted data.
- The **authentication objective** validates the legitimacy of entities involved in the exchange.
- **Correspondence assertions** maintain proper event sequencing.
- **Injective correspondence** enforces strict one-to-one event relationships.

Discussion

Comparative Analysis between Solid Pod and Cloud



Data Ownership and Control

Decentralisation

Privacy and Security

Inter-operability and Flexibility

Discussion

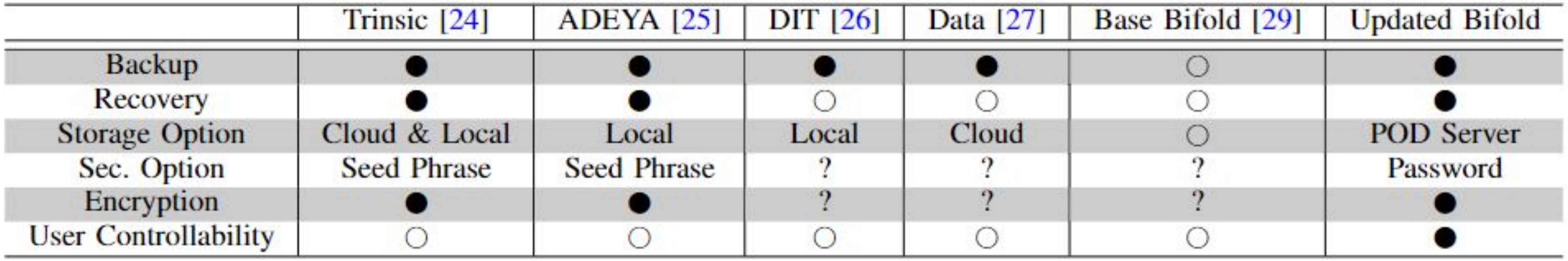
Comparative Analysis between Updated bifold and other wallets

▪ Denotes a particular feature is **present**

O Denotes a particular feature is **absent**

? Denotes a particular feature is **not explicitly specified**

TABLE III: Comparison among SSI Wallets



	Trinsic [24]	ADEYA [25]	DIT [26]	Data [27]	Base Bifold [29]	Updated Bifold
Backup	●	●	●	●	○	●
Recovery	●	●	○	○	○	●
Storage Option	Cloud & Local	Local	Local	Cloud	○	POD Server
Sec. Option	Seed Phrase	Seed Phrase	?	?	?	Password
Encryption	●	●	?	?	?	●
User Controllability	○	○	○	○	○	●

Discussion

Advantages

- ❑ Enhanced Security
- ❑ Better Privacy
- ❑ Scalability
- ❑ Flexibility
- ❑ Open Standards

Limitations

- ❑ Using a **Pod server can create a single point of failure**, such as during a DoS attack.
- ❑ Solid Pod technology is new and **lacks standardization for fundamental protocols and technologies.**

Future Work

- ❑ **Automatic SSI wallet syncing with Solid Pod** ensures up-to-date credentials, relieving users from manual synchronization and improving system usefulness.
- ❑ **Investigating blockchain for hosting Solid Pods** could open novel research avenues, and we aim to explore this in the future.

Conclusion

We propose using **Solid Pod technology for secure backup and recovery of SSI wallets**. Based on a threat model and requirements, we developed a PoC illustrating several use cases. Our PoC offers a secure, efficient way to store and restore SSI wallets, integrating with existing frameworks to enhance SSI security.

This work contributes to the field of SSI and paves the way for further research.

Thank you

Any Questions..?