SHORT TERM SCIENTIFIC MISSION (STSM) – SCIENTIFIC REPORT

Action number: CA15127 (Resilient communication services protecting end-user applications from disaster-based failures (RECODIS))

STSM title: Blockchain based Secure Identity management for mobile users

STSM start and end date: 27/01/2020 to 07/02/2020

HOST: Dr. Madhusanka Liyanage - School of Computer Science, University College Dublin, Ireland

PURPOSE OF THE STSM

In this modern age of competition, reduction in leakages can help operators to marginally increase their revenues. With convergence, the number of points of connectivity or touchpoints will be more, which will increase the chances of revenue leakages. With the increase in the risks and frauds, new solutions providing technologies are always admired by organizations, one such ledger trending technology is Blockchain.

Blockchain, a distributed ledger technology has gained a lot of attention in areas beyond the cryptocurrency. Blockchains can help telecom operators much more effectively within their business network because they support consensus, provenance, immutability, and finality. Some operators have already started the journey with blockchain. For example, in 2015, Orange launched its ChainForce initiative to support collaboration between corporate partners and startups exploring new blockchain technology and use cases [1]. Other CSPs exploring and piloting blockchain programs include Verizon and Du [2].

Data is the new natural resource of the digital economy. This resource continues to rapidly grow in volume as the use of smart devices increases and the IoT expands. And thanks to their networks, CSPs are in the middle of all the data transport and transactions. Recognizing the importance of data integrity, CSPs expect blockchains to help ensure data quality and accuracy as well as increase trust in transactions from end to end. Blockchain can provide a secure platform, the possibility to omit third-party intermediaries, and security measures against fraud and cybercrime.

Blockchain can help create new sources of revenue by providing data management and identity authentication solutions to enhance their user base. Cellular Service Providers (CSPs) could utilize their relevant customer data to provide a dynamic platform for identity transactions, such a system establishment would involve a multi-step process where first the subscriber creates a digital identity similar to a digital signature which would be placed on the eSIM. Operators could provide their subscribers with an app that creates unique virtual identities for each subscriber which are encrypted and stored in a Blockchain.

DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

During this research visit, we focused on developing the architecture of the framework based on blockchain to securely generate the decentralized identity (DID) of the subscriber and stored locally on the device to prevent the cyberattacks. The framework which we developed has the following features:

- Virtual identity based on Decentralized identity (DID) to mask real user identity.
- User Profile creation based on DIDs.
- Live monitoring of permissions granted and revoke access to profile data.
- Complete logging of the use of subscriber data using blockchain.
- Mobile and web application for easy-to-use identity management.
- Any entity can request for the generation of DID.
- Companies can request users for their profile data
- Users can access or revoke permissions given.
- Users can request all details of the interaction with their profile (logs).

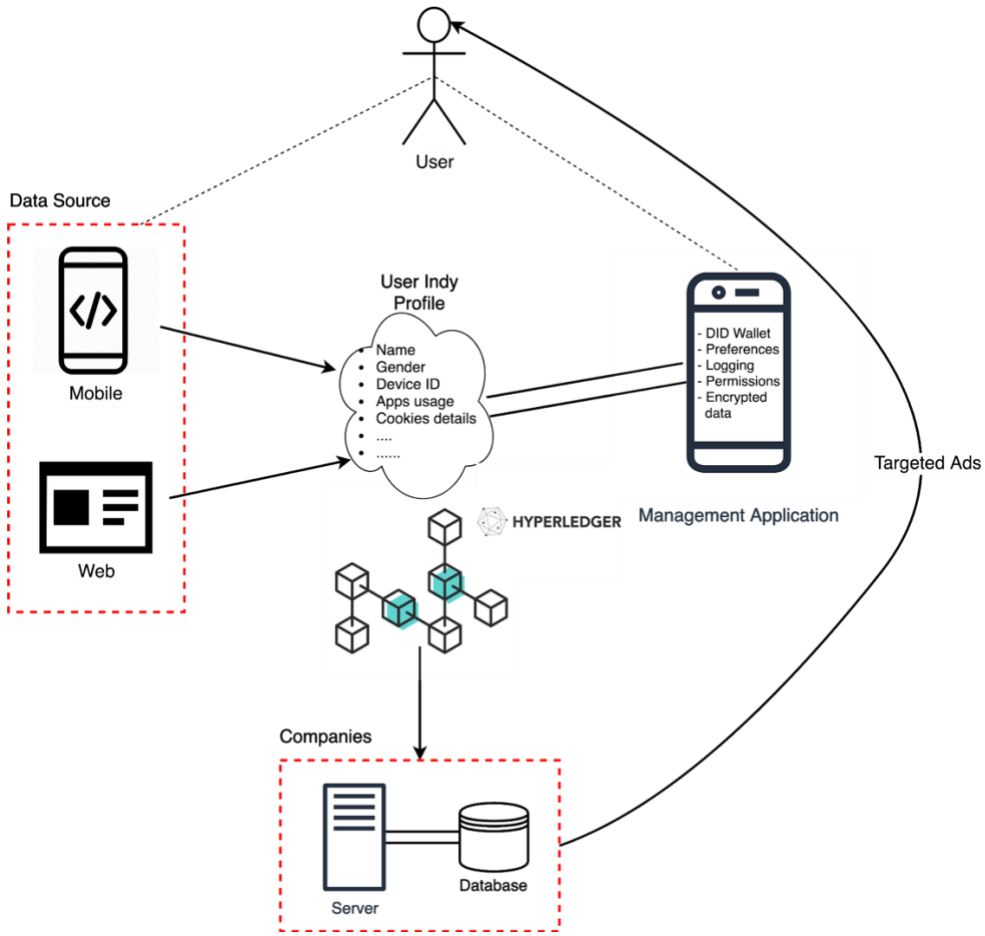

Fig.1 Proposed Architecture

DESCRIPTION OF THE MAIN RESULTS OBTAINED

After finalizing the architecture details, we focused on the implementation of the proof of concept. We divided the roles into three parts namely, Agency (who sets up the network), User, and Advertising companies.

The Government or an organization that sets up the framework provides the application for Decentralized Identifiers management. They also act as the Trust Anchor i.e. assign roles to new joining participants, node pools, maintaining the network, etc. The agency should also be responsible for setting up the schema for the user profile.

The users should be able to create their profile on the framework using the apps provided by the agency. The first set up Credential Definition for their profile which also supports revocation. After creating the keys, they can update their profiles e.g. Personal information, linking Advertising IDs, preferences e.t.c. Users will be able to control their Identity that is stored on the ledger. The user will be able to map one identity record to multiple Decentralized Identifiers.

The advertisement companies join the network with the permission of the agency. After joining they can send proof requests i.e. the data or information, they require from the users. After the approval of access from User, companies can start tracking using DIDs and provide targeted ads.

The benefits of using such a platform provide a Private and powerful identity which is secured using the Industry-standard cryptography. Distributed Ledger also provides redundancy for the data stored. On the other hand, Users are completely anonymous and secure their data using the platform. They are in control of their personal information and can view logs of who accesses their data. Users can revoke access to any company who uses their data. By revoking a new DID will be generated that links to the same profile. Users are also in control of revealing specific information to specific requesters and can easily manage their identity from the web and mobile.

In the end, the Advertisement Companies can benefit from Detailed information i.e. both Mobile and web for better-targeted ads. They also get Verified information directly from the user and it can save them cost as now there is the only single source for data which helps for tracking.

For the proof of Concept, we will be implementing the following things: -

- Blockchain technologies
    - Hyperledger Indy : Distributed ledger built for decentralized identity, Indy nodes
    - Hyperledger Aries : Agent protocol and cryptographic wallets, Zero-knowledge proof, DKMS, High-level APIs
    - Hyperledger Ursa : Crypto Library for Indy and Aries
- Android Application for Management
    - Wallet for DID

    - Easy-to-use profile management
    - Logging
- Web Application for Indy profile
- Indy nodes on Dockers
    - 1 Trust Anchor
    - 2 Identity Owner
    - 2 Companies

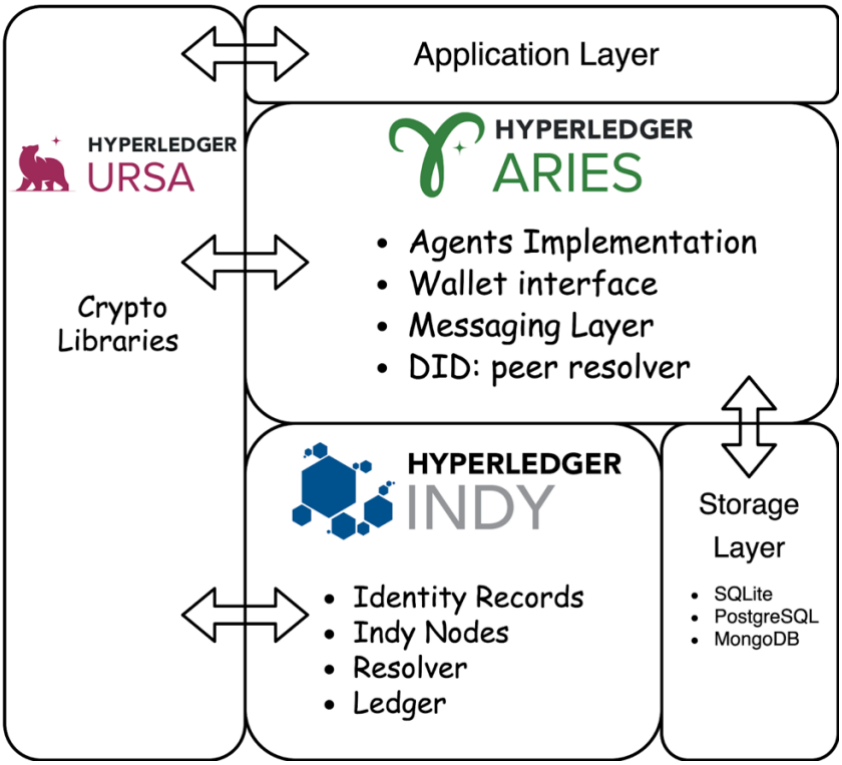

Fig.2 Implementation Details

FUTURE COLLABORATIONS

The main focus will be to publish the work in a renowned conference targeting IEEE GLOBECOM 2020. After the successful implementation and evaluation of the idea, we will publish a journal paper. In the future, more features can be added to the proposed framework such as

- Monetization of the user data
- Integration of the framework with the EU Self Sovereign Identity framework