A proposed approach for Digital Identity management using Self Sovereign Identity

Shailaja Lohar
Research Scholar, SKNCOE's Research Centre, Pune
snl.sit@sinhgad.edu
Sachin Babar
Department of Computer Engineering, Sinhgad Institute of Technology, Lonavala, Pune
Hodce.sit@sinhgad.edu
Parikshit Mahalle
Department of Computer Engineering, Smt.Kashibai Navale College of Engineering, Vadgaon, Pune
Alborg.pnm@gmail.com

Identity of a virtual entity must be as secure just like it is in the real world. These virtual entities are the numerous users who access the internet-based services. These services always need some digital identification to comply with the user's request. More number of users are opting for online services daily for variety of applications. The existing digital identity management systems take care of this process. A single sign on identity management system allows same credential to access different systems whereas user centric where the user's identification is stored on a secured device owned by the user. But none of the systems are giving user, the complete control of their digital identity. Self-sovereign identity management system is one of the promising identity management system which will make the user, the complete owner of his identity by eliminating the centralized approach of managing the identity. This paper gives an overview of existing identity management systems based on self-sovereign identity and a proposed approach for secure identity management using self-sovereign identity management system.

Keywords: Software maintenance, automated regression analysis, application baselining.

1. INTRODUCTION

Identification and verification of a person, organization, entity in real world is supported by three main steps, claim, proofs, verification as shown in figure 1. These same are applicable to a digital identity to ensure uniqueness and secure verification of users. Maintaining the proofs of these claims for authentication is a tedious task handled by different types of identity management systems. The increase in number of internet users has given rise to digital identity management concerns. Identity thefts have increased with the increase in usage of Internet of Things based applications. Many authentication systems face the challenges of compromised identity and exposure of user's important credentials to systems which are not trustworthy. Such systems add to the worst case scenario of compromised credentials which can be misused for malicious purpose also. The use of federated identity systems like Facebook or Google are having secure policies for digital identities, solving the authorization problems, but users have to completely trust these systems thereby losing their own control over their identity.The verification, authentication and claims of user must be secured from third party entities and should be stored in a de-centralized manner. This section gives a brief overview of the evolution of digital identity systems. The comparison among these systems is also summarized.

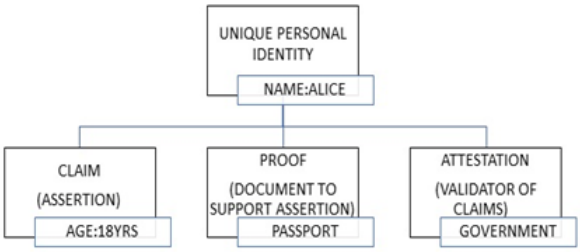

Figure 1. Identity Management in Real World

The paper is organized as follows. Section II gives a brief description of existing Identity Management Systems which is summarized in table I. In Section III the implemented and existing systems are studied and a review of the same is presented along with its summary of comparisons in table 2. The proposed approach is detailed in Section IV, Section VI discusses the results along with further study approach and Section V concludes the paper.

2. TYPES OF IDENTITY MANAGEMENT SYSTEMS

2.1 Centralized Model

Fett et al. [2017] The verified credentials are stored and controlled by a single central authority. This information can be shared with multiple service providers. This model is suitable for managing a big number of users. Identities of each service provider are stored with the identity provider. When the service provider needs to authenticate a user, it will send the user information to the Identity provider to complete the process of verification. The main disadvantage is the centralized identity provider's vulnerability to data breach and central point of failure. A separate entity acts as an exclusive user identifier and credentials provider for all service providers. User accesses all service providers using same set of credentials. User authenticates himself only once and can access all the services. A third party is responsible for authenticating, allocating and verifying the credentials. Authentications solutions like Kerberos are used and the Kerberos authentication server is used as the centralised authority for verification.

2.2 Federated Model

E.Birrell and F.Schneider [2013] The federation is a set of agreements, standards and technologies that a group of service providers can use to identify the users from other domains. Different identifiers owned by the same user are mapped together in different domains. This allows the user to work in cross domains without the need of repeated authentication. This model also supports single-sign-on across multiple domains. Every Service Provider can store user identities locally and have its own identity database. Policies and requirements of different groups vary, this may cause a disagreement among the group of service providers. This model resembles the user centric model because the power to the centralized authority is given to multiple central authorities.

2.3 User Centric Model

Dunphy and Petitcolas [2018] To overcome the limitations like maintaining only a single domain in federated system, User centric model was introduced. Wherein the user can store credentials and identifiers from different service providers in a single hardware device like a smart card or a portable personal device. The personal identification device should be under the control of the user, and not under the control of the identifier providers, the credential issuers or the service providers. Example Google Sign-in.

2.4 Self-Sovereign Identity Model

Bokkem et al. [2019] This model gives user the complete authority over his identity. No administrative authority, or third party is involved in the authentication, verification or validation of the user. The complete process is decentralized adding the benefit of trust among all the participating entities, user. It gives user control of their own identity Fett et al. [2017].

Efficiency parameters → / Type of Idm ↓	User Centric	Centralized	De-centralized	Examples	Privacy Protection
Centralized	Yes	Yes	No	FacebookConnect	Weak
Federated	Yes	Yes	No	Liberty Alliance.	Strong
User Centric	Yes	No	Yes	Mozilla Web browser	Strong
Self Sovereign Identity	Yes	No	Yes	uPort,Sovrin	Strong

Table 1. Summary of Comparison between Identity Management Systems

Sovereign Identity. Every system has their own specification of parameters which can be compared to determine performance of the systems. Accordingly, the table II gives an insight into the systems with summary of their specifications. The above systems address the identity management in best ways possible but there are very few approaches which adhere to Self-Sovereign Identity criteria. The challenges faced by these systems include:

- X Designing an identity establishment system for IoT based scenarios.
- X Implementing Distributed ledger for constrained devices.
- X Eliminating the need of centralized identity.

3. RELATED WORK

The summary of identity management systems Dunphy and Petitcolas [2018] discussed in the above section clearly instigates the need of complete ownership of the user over his digital identity. In traditional identity systems this identity was either stored on a centralized repository or shared among all the systems that needed the claim verification from users. This posed as a threat to the user's credentials and attacks like spoofing, spear phishing attacks, credential stuffing, Man in middle attacks. The systems which have implemented the SSI are giving some promising results. Like uPort Dunphy and Petitcolas [2018] makes use of smart contracts to assess the digital identity and uses Ethereum as the repository for identity storage. Liberty Haddouti and Ech-Cherif El Kettani [2019] is a user centric identity management system which gives mobility, security and privacy. OpenId Dunphy and Petitcolas [2018] provides a single-sign-on solution by allowing users with multiple application authentication using single OpenId authentication. ShoCard Bernal Bernabe et al. [2019] uses a distributed ledger a blockchain to store the verification data whereas identification related data is stored locally. Civic Haddouti and Ech-Cherif El Kettani [2019] uses Identity partners to verify users claims. The identity data is encrypted and stored on user's device and verification is done through the blockchain. Cryptid Haddouti and Ech-Cherif El Kettani [2019] uses blockchain for storing the record which is timestamped. No local

or central server is required, all the data is de-centralized and can be accessed from anywhere. It implements authentications for ensuring the security of user credentials. Uniquid Bernal Bernabe et al. [2019] uses biometrics like fingerprint to provide secure identity management on personal devices. The uniquid supervisor API's are responsible for creating, inspecting, revoking the connections between devices thus providing tools to manage digital identity. A private blockchain is used to save the devices which are connected through secure authentications. Sora Takemiya and Vanieiev [2018] uses a hyperledger Iroha Dunphy and Petitcolas [2018]e. This system uses DID (Decentralized Identifier) for issuing a verifiable claim, these claims are split into two parts. First part is public and stored on blockchain in form of hashes, digital signature and issuer information. Second part is shared with the verifier and is private. These existing systems show the widespread acceptance and use of Self Sovereign Identity. The table 2 gives a detailed

PARAMETERS → SYSTEM ↓	Integrity & Confidentiality	Identity Provider Type	Identity Storage	Cross domain access	User control over identity
Liberty	Both	Central Server	Domain specific	Yes	Partial
OpenId	Both	OIXnet Registry	Openid Provider	Yes	Yes
ShoCard	Both	Blockchain	User device	Yes	Yes
Uport	Both	Smart Contract	IPFS (Inter Planetary File System)	Yes	Yes
BlockAuth	Only Integrity	Identity Registrar	franchise partner	Yes	Yes
Civic	Both	Civic Secure Identity Platform (SIP)	Civic API's	Yes	Partial
CryptId	Confidentiality	Identity Registry	Blockchain	Yes	Yes
UniquId	Both	Blockchain	User Device	Yes	Yes
Sora Identity	Both	Central Server	Blockchain	Yes	Yes

Table 2. Summarized view of the existing Identity Management Systems as per working parameter

summarized view of the systems mentioned in table I. Most of the systems are not giving the user, complete authority of their identity. The study also shows some following research gaps.

- X The distributed ledger implemented through blockchain cd has an overhead of storage.
- X The complexity of maintaining multiple identities for multiple domains increases with number of nodes in the ledger.
- X Some systems which store the data temporarily do not encrypt it which is a major privacy concern.
- X The mutual identification of two entities in an IoT based scenario requires addressing of secure, user-controlled verification.
- X IoT being a constrained ?] network, the overhead of distributed ledgers should be reduced for faster and secure identification and verification of identity.

PARAMETERS / SYSTEM	Advantages	Limitations	Type of Identity Management System
Liberty	Permission Based Attribute Sharing Ensures privacy protection & confidentiality between service providers	Access to only their respective set of domains User creates different accounts to access non-federated domains.	Federated
OpenId	Provides trustworthy, simple and effective identification to multiple applications & service providers.	No encryption of id_tokens. Limited signature algorithms. Vulnerable to phishing attacks.	User Centric
ShoCard	Central server manages distribution of certifications among users and domains. Bears less risk of data breach in comparison with distributed plain text data.	In case of company termination, ShoCard Users loses the acquired certifications. Set up of ShoCard is expensive due to time consumption in mining.	User Centric
Uport	Flexible and easy to use. Abstraction of public key cryptography from end user.	Data stored temporarily on the server is not encrypted raising a privacy concern. Uport id may be compromised by a phishing attack.	Self-Sovereign Identity
BlockAuth	Saves time of authentication by ensuring validity of user by reducing the cost of repeated requests of verification.	Relies on building acceptance from a number of existing open-source communities and integrating into a variety of libraries	User Centric
Civic	The need of username, password, third party and hardware tokens are eliminated. Use of single identity requestor for multi-purpose authentications	Adoption by a greater number of users is yet to happen. Competing technologies are ahead	User Centric
CryptId	Data distribution across multiple systems prevents data corruption.User data need not be saved to a photo ID card. It can be stored on anything that can store a few kilobytes of	No control of user after issuance verification by centralized server.	De-centralised

Table 3. Summary of the systems as per types limitations

4. INTRODUCTION TO SELF-SOVEREIGN IDENTITY

The Self Sovereign Identity Geoff and Tomaso [2019] is a promising approach towards digital identity management. The main aspects of this approach are Verifiable Claims (VC) and Distributed identifiers (DID) Xiaoyang and Youakim [2018]. Figure 2 shows the relation between the VC and DID. The user is the owner of his identity, the issuer gives proof for user's claim and the verifier uses verifiable credentials (VC) to attest the claim ¡]jl. The user, issuer, verifier sign a claim of id proof with the de-centralized identifier (DID) residing in a distributed ledger. An identifier is assigned to a specific user. The claim verification and the Decentralised Identifier **?**] are stored on a distributed ledger or simply can be termed as a distributed register. The DID's allow the user to manage, create or discard identifiers as and when needed.

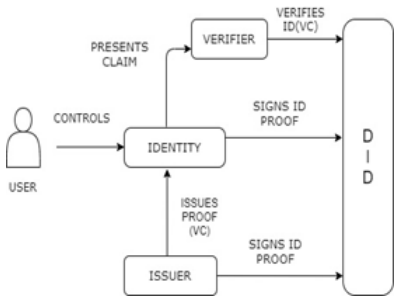

Figure 2. Identity verification based on Self Sovereign Identity

Thus, the figure indicates 3 main entities of the Self Sovereign Identity System: User, Issuer and Verifier Toth and Anderson-Priddy [2019]. The verification of the user is done without any intermediary with the help of decentralized ledger, DID and VC.

5. PROPOSED APPROACH

Addressing the need of user's control over his own identity as mentioned in the above related work, the building blocks of proposed work are mentioned below.

a) **Creating Identifier**

Current identifiers on internet are controlled by specific organizations. For example, our email address is under Google's control. DID (Decentralised Identifier) is W3C proposed standard, which is not dependent on any centralized registry or identity provider. DID method have its own set of rules to control the linkage of DID to a ledger. Thus, the identifier related document is created, updated or deactivated on a distributed ledger.

b) **Storage of the identities**

DID will be the mechanism to create unique identifier but, its storage will be on blockchain Alfonso et al. [2018]. The verification of DID from issuer should ensure integrity throughout as well as eliminate centralized storage of credentials. Storing the credentials on blockchain will ensure that no one had tampered with the data.

c) **Verifiable Credential**

In real world example of passport, the credential will consist of information of the passport holder, issuing authority government, data related to how the passport was issued, information of date of renewal. All these types of attributes can be digitally represented using a verifiable credential (VC). The proposed approach has been implemented with the use of DID and VC for user credential verification. The frameworks used leverage different types of blockchain and DID retrieval mechanisms. The phases in the identity verification process are shown with a simple sequence diagram. The verification system with the phases is shown in Figure 3. The basic functionalities of the approach will include following processes:

- Issue a credential to the user.
- Share a credential only with the demanding entity, authority.
- Discard or update the credential
- Associate the entity with identifier

The DID format from W3C, World Wide Web Consortium[1] standard is used in the approach. It includes the format for DID document and standard for Verifiable credentials.

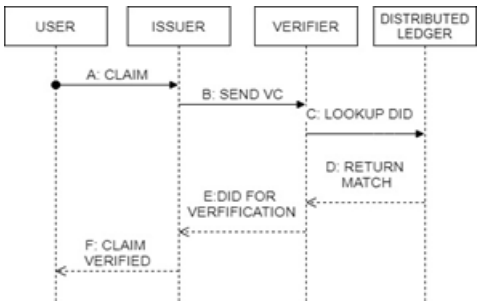

Figure 3. Working of the approach among the entities

As shown in the figure 3, the following steps are considered for identity verification.

[1]https://w3c.github.io/webpayments-ig/VCTF/charter/faq.html

A) User claims his identity

B) Issuer sends this veri able credential to veri er

C) Veri er looks up in the distributed ledger for the matching DID

D) Matched DID is returned to the veri er

E) Issuer receives the DID corresponding to the VC

F) Claim is veri ed for the user

The system will eliminate the centralized entities in establishing the mutual identity ¡]ba. As per the requirements assessed from the studied survey, we plan to explore and implement the de-centralization with the following approach.The distributed ledger ¡]au includes the following benefits with respect to the constrained resources in IoT based scenarios.

X Distributed storage of data, in our case, it's the identity.

X No intermediary required for identity verification.

X Immutable, since no third party can tamper the data.

The above processes use the decentralized identifiers and verifiable claims through smart contractsvan Thuan et al. [2014]. The holder of the digital identity will have a unique identifier which he will share only with the required entity without sharing all the personal identification details giving him the sole ownership of his identity. Smart contracts will ensure the validation of identification is only between Claimer and the issuer. The repository for acting as a registry will be the distributed ledger thus eliminating the centralized storage of the credentials.Using the ledger and the smart contract can give a solution to de-centralize the identity of a user or an entity.

Issue to be Addressed	*Approach for new solution*
Storing the Identity /Claims	Distributed Ledger (Blockchain)
Authorization to access the stored Identity	Smart Contract
Standardizing the process of de-centralized identities	Decentralized Identifiers (DID), Verifiable Claims(VC)

Table 4. Proposed Solution's broad plan with new approach

6. RESULTS AND DISCUSSION

To assess the use of distributed ledger Q.Stokkink and J.A [2018] in managing identities, we evaluated some identity management frameworks. Each has its own mechanism of handling the verification process to authenticate identity of the user. Trinsic[2] is a full stack self-sovereign identity platform built for developers. It gives a digital wallet to users for maintaining the verifiable credential. The VC that is created can be stored with any verifier organization. Also, the credential can be revoked by the user. The distributed ledger IndyScan is used with Sovrin Stagingnet[3] which gives details of transactions, timestamps, transaction id and very important, the DID (De-centralized identifier). User registers through a verifier application and it is stored by scanning the QR code in Trinsic wallet mobile app. The following figures shows a credential created by us and stored in out mobile and also shared with another verifier.

[2]https://Studio.Trinsic.Id

[3]https://Indyscan.Io/Txs/Sovrin$_S tagingnet/Domain$

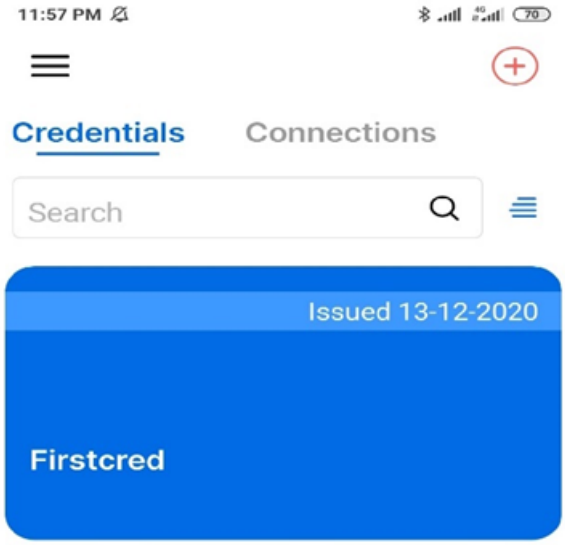

Figure 4. Credential created from Trinsic framework

Figure 5.Transaction details on IndyScan Stagingnet

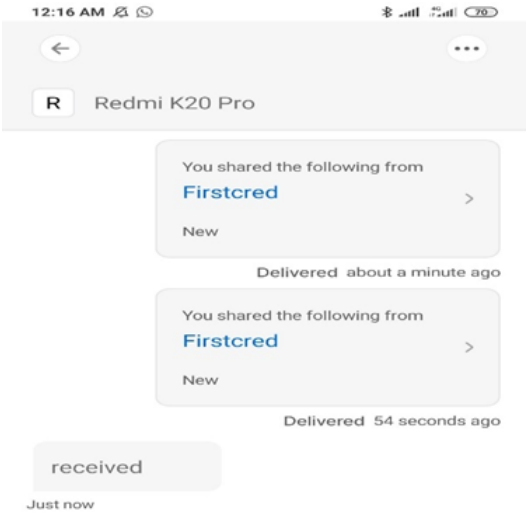

Figure 6. Sharing the credential with third party

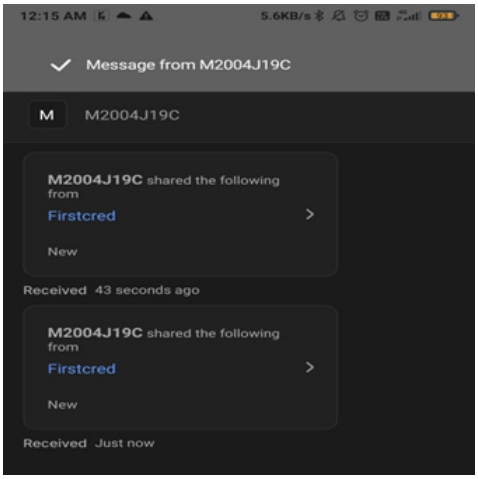

Figure 7. Receiving the credential from owner

The next framework id Dock[4], which uses the decentralized Ethereum blockchain for issuing verifiable credentials. The issuer can create his own identity and through DID on blockchain which also makes backtracking of the origin easier. This information can be shared with third party to verify authenticity. Another framework from Ockam[5] was studied. It gives an approach to implement the DID document to store the entity registration claim. The blockchain gives storage for namespace which is unique to each device. If the device has it private key, it can cryptographically prove its identity ownership. The tests and study performed on these frameworks supports the concept of SSI principles. The results show a promising foundation for our proposed approach with respect to SSI for Internet of Things. Taking the study further, our

[4]https://www.dock.io
[5]https://ssimeetup.org/machine-identity-dids-verifiable-credentials-trust-interoperability-iot-mrinal-wadhwa/

next investigation and approach will be to analyse if same SSI principles[6] can be applied to any device, entity in use cases related to Internet of things.

7. CONCLUSION

In the growing network of things and online interactions, securing the digital identity is also becoming an important issue. Self-Sovereign identity is the most promising approach towards securing digital identities and giving user the complete control of his identity. As compared to the existing or previous approaches of identity management, the SSI provides a de-centralised storage, verification and processing of the user credentials. It assures the users more control and more security of their identity. The discussed and presented work provides analysis of the existing systems which supports the proposed approach and works as an input which makes use of Verifiable Claims, De-centralized Identifier and Blockchain for managing the digital identity in Internet of things uses cases. Security and Identity management of Internet of Things, both are crucial factors in the growing world of Internet. The Self Sovereign Identity can is a promising approach for identity verification and authentication in Internet of Things scenario.

References

Alfonso, P., Nachiket, T., Giovanni, M., Francesco, L., and Antonio, P. 2018. Blockchain and iot integration: A systematic survey. *Sensors 18,* 8.

Bernal Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., and Skarmeta, A. 2019. Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access 7*, 164908–164940.

Bokkem, D. V., Hageman, R., Koning, G., Nguyen, L., and Zarin, N. 2019. Self-sovereign identity solutions: The necessity of blockchain technology. *ArXiv abs/1904.12816*.

Dunphy, P. and Petitcolas, F. A. P. 2018. A first look at identity management schemes on the blockchain. *CoRR abs/1801.03294*.

E.Birrell and F.Schneider. 2013. Federated identity management systems: A privacy-based characterization. *IEEE Security Privacy 11,* 05 (sep), 36–48.

Fett, D., Küsters, R., and Schmitz, G. 2017. The web sso standard openid connect: In-depth formal security analysis and security guidelines. *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, 189–202.

Geoff, G. and Tomaso, A. 2019. A decentralized digital identity architecture. *Frontiers in Blockchain 2*, 17.

Haddouti, S. E. and Ech-Cherif El Kettani, M. D. 2019. Analysis of identity management systems using blockchain technology. In *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*. 1–7.

Q.Stokkink and J.A, P. 2018. Deployment of a blockchain-based self-sovereign identity. *IEEE International Conference On Internet Of Things*, pp.1336–1342.

Takemiya, M. and Vanieiev, B. 2018. Sora identity: Secure, digital identity on the blockchain. In *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*. Vol. 02. 582–587.

Toth, K. C. and Anderson-Priddy, A. 2019. Self-sovereign digital identity: A paradigm shift for identity. *IEEE Security Privacy 17*, 17–27.

van Thuan, D., Butkus, P., and van Thanh, D. 2014. A user centric identity management for internet of things. In *2014 International Conference on IT Convergence and Security (ICITCS)*. 1–4.

Xiaoyang, Z. and Youakim, B. 2018. Identity management systems for the internet of things: A survey towards blockchain solutions. *Sensors 18,* 12.

[6]http://www.Lifewithalacrity.Com/2016/04/The-Path-To-Self-Soverereignidentity