Self-sovereign Identity framework development in compliance with Self sovereign Identity principles using components

Mohammed Shuaib[1], Salwani Mohd Daud [1], (Member, IEEE), Shadab Alam[2]

[1] Razak Faculty of Technology and Informatics (RFTI), Universiti Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia

[2] Department of CS & IT, Jazan University, Saudi Arabia

Corresponding author Salwani Mohd Daud (e-mail: salwani.kl@utm.my).

Abstract

Digital identity is the need of the hour, but the existing digital identity solutions are susceptible to different malicious attacks and manipulations. Also, these identity solutions can leak the personal identity information (PII) of the users, and users have no control over them. Another issue of the current identity solutions is that no user data is stored in a centralised manner, and users have no control over them, making them vulnerable. A new phenomenon, Self-sovereign identity (SSI), is gaining popularity to provide a secure and reliable identity solution to the users. SSI solutions provide a reliable and secure identity solution based on identity principles. SSI provides a mechanism for the users to control their identity information and give consent for its use. Also, the identity details are stored in a decentralised fashion with the users that help counter the issues of digital identity solutions. This paper highlights the advantages of SSI adaptation, reviews the existing SSI solutions and evaluate them based on SSI principles. Also, it evaluates the SSI components needed for developing SSI frameworks to fully comply with the SSI principles. It further highlights the steps for adopting an SSI ecosystem and discussed various digital identity governing laws to be undertaken by the governments, and highlights SSI applications in different domains.

Index Terms: *Blockchain, SSI compliance, Self-sovereign identity, Identity principle, SSI component*

I. INTRODUCTION

A recent survey highlighted that 37 % of employees in US firms reset their passwords more than 50 times every year and losses around 426 USD annually due to password glitches apart from the effect on their working efficacy [1]. Also, a world bank survey revealed that around 14 % of the global population lacks proof of identity in any form [2]. Providing identity to individuals and maintaining secure and reliable identity storage is a big challenge. After providing the identity to the individuals, the secure and reliable management of identity is a far more significant challenge. A recent incident of the Cambridge Analytica leaked the 87 million Facebook user's password details due to a security breach in the system of a third-party service provider [3]. There are many such examples of data breaches due to the centralised nature of these records and the use of third-party service providers. Digital identity and its security are becoming more critical with the advancement and adaptations of online services.

Self-sovereign identity (SSI) is the next-generation identity management model that secure and reliable identity record management. The identity records are stored in a decentralised manner and provide control to the users over their identity details [4]. In this way, the SSI is capable of handling the shortcomings of traditional identity solutions. Users of the SSI solutions have full control over their personal identity information (PII), and consent of users is required for using the PII. Thus the issue of centralised storage and identity theft is resolved [5][6]. SSI is a new paradigm, and several researchers are working in this domain to review it and analyse its applications, but the academic literature is still limited. Some of the related literature can be found in these articles [7][8][9][10][11].

The SSI is based on the ten identity principles outlined by Christopher Allen. The SSI solutions have to follow these ten principles of Self-sovereign identity. Several initiatives and government agencies are currently active to develop SSI solution on the blockchain platform. Several blockchain-based SSI frameworks like Sovrin [1], Uport [12] , Civic [13], Blockstack [14], Selfkey [15], ShoCard [16] are available and being used in various domains. In order to have a successful SSI solution, it needs to comply with all the SSI principles [9][17][18][19][20][21]. None of the existing SSI frameworks fully comply with the SSI principles. There are several building blocks for developing an SSI framework. These building blocks are also referred as SSI components. To identify SSI components for the SSI framework in compliance with SSI principles, the major contributions of this research work are:

1. To compare the current SSI solution on the principles of SSI
2. To identify the steps and requirements for the SSI adoptions.
3. To identify the Components of SSI to comply with the principles of SSI

Further on, this study will describe the SSI concept and SSI principles in section II and compare four available prominent SSI solutions based on SSI principles in section III. It highlights the steps and requirements for adopting SSI solutions in section IV. Section V presents a brief description and visualisation of the SSI framework and component architecture, and various SSI components have been explained in section VI. A very detailed critical analysis of SSI components and how they are useful for developing SSI solutions in compliance with each SSI principle is given in section VII. Finally, section VIII give a brief overview of possible use cases for SSI application, followed by the conclusion.

II. SELF-SOVEREIGN IDENTITY (SSI)

Self-sovereign identity solutions allow users to get control over their personal identity. Users will decide precisely what information they need to reveal about themselves, who and in what contexts. Under the self-sovereign identity model, no one can prohibit a person from exercising basic human rights, such as the right to be expression and privacy. Individuals do not need to retain their identities. They can choose any identity operator. The pre-requisite for SSI is that digital identities must be scalable and interoperable across different platforms. Individuals are free to choose the identity operator and switch from one operator to another [22]. While no clear definition of self-sovereign identity exists, a set of requirements have been defined as the key principles needed to function as a self-sovereign identity [21]. These principles can be regarded as a criterion to check the existing identity solution to comply with these principles.

- *Existence:* Users have an independent existence and are not dependent on the details found in their digital identifiers.
- *Control:* Users should control their identities and be able to transform, update, refer and hide them. User has full authority to disclose or choose privacy on their identity details.

- *Access:* Individuals should have access to their data and should have the ability to be able to retrieve it when necessary.
- *Transparency:* Systems and algorithms used to handle and run digital identities must be accessible and transparent. The public must be able to track the operation and maintenance of the system.
- *Persistence:* The identity must be long-lived, and the individual's identity must be preserved for as long as the individual wants.
- *Portability:* information and resources concerning identity must be transportable, and not owned by a single third-party, even though they are trusted.
- *Interoperability:* identities are available for common use in all contexts instead of restricted to a one siloed environment.
- *Consent:* individuals should give consent to use their identities. The data sharing by third-parties must occur with the consent of the data subject.
- *Minimisation:* The disclosure of claims should be kept to a minimum and should only be disclosed when necessary to perform a task.
- *Protection:* The user's right to privacy must be protected at all costs, even though this would go against the identity providers' interests.

These principles benefit the user and form the basis of the SSI solution and need compliance in order to provide an SSI solution to the user [21]. None of the SSI solutions today comply with all these principles[20]. Several competing SSI solutions have emerged during the development process, adopting different ideas and using different blockchain . In [23], review the available SSI solutions based on blockchain and discuss their implementations concerning the SSI principles. An analysis of the SSI concept's potential and evaluation of blockchain-based SSI solution Sovrin, Multichain, Blockstack & Uport has been done [24]. Comparative analyses of UPort and Sovrin are performed by [25]. A detailed analysis of the ShoCard Sovrin, Civic and UPort is carried out. These systems use certain decentralisation techniques based on the author's criteria and principles, none of which comply with the SSI requirements [20]. However, it is still rare for SSI systems to be compared with the SSI design principles. Therefore, to fill this gap in the next section, we have compared the existing blockchain-based self-sovereign identity(BC-SSI) solution Uport, Sovrin, Civic and Shocard on the principle of SSI to identify that if the existing BC-SSI solution complies with the SSI principles or not.

III. COMPARISON OF SELF-SOVEREIGN IDENTITY SOLUTIONS ON SSI PRINCIPLE

There are several SSI solutions available based on the blockchain platform. Still, in this section, only UPort, Civic, Shocard, and Sovrin have been shortlisted for comparison because of their innovative SSI identity management approaches. Together these SSI solutions cover the broader landscape of BC-SSI solutions. The analysis for each selected SSI solution to comply with the SSI principles is shown in Table 1. First, we began the analysis with uPort, which is an identity and communication platform based on the Ethereum blockchain [12]. Second, the Sovrin Foundation, which has set out to standardise and implement the Self-Sovereign Identity architecture using blockchain so that anyone can issue and verify it [1]. Third, Civic offers an SSI ecosystem to allow low-cost and reliable access to identity verification and customer KYC processes [13]. Finally, the ShoCard-based identity ecosystem provides authentication, an attestation to the credentials, and proper authentication [16].

1) UPORT

uPort enables users to manage their online network of identities by utilising an ethereum blockchain [12]. The uPort mobile app creates keys and creating the corresponding three smart contracts for each identity. The uPort registry stores identity information in a cryptographically secure manner and securely links it to an identifier.

Analysis: UPort is developed with open international standards and open source applications (3). The user's key identity is stored on the Ethereum blockchain and then distributed on thousands of computers worldwide (4). Individual build and control their own personal identity (1). Personal identity information is stored securely on the computer and in IPFS and is not open to the user (2). Users may share information with the third party at their own choice (7). Private data is stored locally on the user computer and uses JSON instead of XML (5). UPort has a "Selective Disclosure Request" regarding confidential inf. However, the JSON user profile for the registry is public, which compromises the user's privacy (8). Some centralised components include a message server that allows the transfer of attributes, an application manager, and a push notification centre (9). UPort can validate your identity with various attributes and generate JWT tokens to verify your claims (6). The cost of using Ether is directly related to the price of Ether on the Ethereum network (10).

2) SOVRIN

The Sovrin Foundation has come together to standardise and develop an environment to store the self-sovereign Identities on a blockchain so that everyone can use and verify them [1]. Sovrin has developed a specific framework built on top of Hyperledger Indy. Sovrin uses a permissioned blockchain called Stewards to achieve global consensus.

Analysis: In Sovrin, the Identity Owner's cryptographic key pairs are the only way to access and do all the user has permission to do (1). Personal data is collected on the user's device or preferred agents who are not the third-party service providers (2). Sovrin and agents are used to store attributes associated with the identity (6). The code that runs, validates, and gives access to the ledgers is open source (3). An encrypted and private local container with an agent can be used to maintain and backup storage (4). The datasets can be accessed using system-independent semantic Web formats such as JSON-LD to ensure data portability (5). Identity Attributes are exchanged only by obtaining consent from the Identity Owner (7). For each relationship, Sovrin utilises decentralised identifiers and public keys to provide selective disclosure of verifiable statements using zero information proof (8). Although the ledger itself has a decentralised framework and has several nodes, the permissioned ledger requires a governing body (9). Identity owners will have unrestricted access to their identities, but Sovrin supports "Premium Claims" to create identity issuers' economic opportunities (10).

3) CIVIC

Civic is developing a single identity verification ecosystem where anyone can quickly request identity verification services at a low cost [13]. Civic is built on an ERC20 token based on the ethereum blockchain that generates keys on a third-party platform. All personal information is set to own by the user, and only the hash of the personal information is stored on the blockchain.

Analysis: Civic enables Identity data is stored on the user's computer to access and control its identity information (1). The user's control and access are guaranteed as long as the device controls the user (2). In Civic, the Ethereum network is likely to be available in the future in which real data relies on the user-maintained long-term storage (3). The information may be used in Civic applications but is not portable outside such Civic applications (4). Identity information is accessible in the civic environment but is not portable beyond the civic ecosystem (5). Civic will enable password-less access to services as well as self-declared and checked identity attributes (6). When data is stored on the user's device, the data owner must determine who can access the identity information (7). Selective parts of the Merkle tree can be revealed with hashes for any elements that the user prefers not to reveal (8). Information held on the Civic Network can be used to carry out applications within the Civic Ecosystem. Information should be revealed selectively as per the request of the customer (9). The fees are calculated by Ether's cost on Ethereum and the likelihood of CVC tokens for some services (10).

4) SHOCARD

ShoCard was created in 2015 to provide a more reliable authentication mechanism than conventional methods [16]. ShoCard utilises alternative security methods such as the blockchain, which guarantees authenticity and does not require any personal data. It supports Zero-knowledge proof as well as the complete KYC process.

Analysis: ShoCard is partially centralised and dependent on ShoCard infrastructure. It creates a future existence problem for ShoCard (4). Users construct, maintain and control their digital ID (1). The public blockchain is generally open to the public, but issues can compromise identity data with the ShoCard service (2). ShoCard has received four patents and nine patents pending and now shares its inventions & algorithms on open-source and open-source standards (3). ShoCard can use multiple blockchains at the same time to better support future blockchain (5). Through the use of ShoCard, there is a couple of different choices for identification and authorisation, such as KYC and attesting credentials (6). Users will determine how and with whom they want to share their identity information (7). Users will decide which data they want to share and did not need to share irrelevant data (8). The central server partly centralises the ShoCard (9). ShoCard is an independent blockchain, theoretically operating on the public ledger, with transaction fees (10).

TABLE 1 Comparison of SSI solutions based on SSI principles

SSI principle	SSI solutions			
	Uport	Shocard	Sovrin	Civic
Control	✓	✓	✓	✓
Access	✓	×	✓	×
Transparency	✓	✓	✓	✓
Persistence	×	×	×	×
Portability	✓	✓	✓	×
Interoperability	✓	✓	✓	✓
Consent	✓	✓	✓	✓
Minimalization	✓	✓	✓	✓
Protection	✓	×	×	×
Existence	×	✓	✓	×

IV. STEPS AND REQUIREMENTS FOR SSI ADOPTION

For adopting and standardising any new technology, there are several guidelines and regulations are prescribed by Government agencies and autonomous institutions authorised for standardising such technologies. There is a range of guidelines for developing a digital identity framework. Some of the sources are International Telecommunication Union (ITU) [26], Financial Action Task Force (FATF) [27], European Union [28] and the Open Identity Exchange (OIX) [29]. Although these guidelines were not exclusive to self-sovereign identity, they also refer to the application of self-sovereign identity. Identity systems may be classified into three groups, depending on the legislation's origins that defines liability. There are three types of identity structures [29]. The Digital Identity Level I scheme is the law applicable to all digital identity solutions. Tier II is a public law applicable only to particular jurisdictions. Tier III is a contract law that many businesses are complying with. The type of digital identity scheme, according to the OIX, is shown in Table 2.

Table 2 Digital identity scheme and governing laws as per OIX

Source for rules regulating liability	General Law	Identity-Specific Law	Contract-based rules
Level	1	2	3
Type of rule	Public Law	Public Law	Private Law
Usefulness	Everyone within the jurisdiction.	Persons in ID system jurisdiction covered by the statute	Entities that adhere to the terms of the contract

Numerous steps are required to create a fully scalable, fully operational and fully autonomous self-sovereign identity ecosystem. Such measures can differ based on the amount of government involvement. Table 3 shows the requirements for the governments to adopt the SSI model. Many governments allow users to use digital identities at the national level. In Estonia, the national ID card system offers access to all electronic facilities, such as banking and used by 98% of the population [30].

The self-sovereign identity approach would allow governments to issue digital IDs that can be used to access any digital services without significant infrastructure and additional obligations. Governments register identity records in blockchain and trust lists using a self-sovereignty strategy. The government will no longer have the responsibility of verifying to make sure that the certificates are valid. In the SSI system, the government only needs to issue digital certificates and register cryptographic proofs in certificates in a public and decentralised network, removing the government's need to maintain additional Infrastructure [31]. Individuals will have full control over the sharing of data. The government does not require to validate and authorise digital credentials isued by government agencies explicitly.

Table 3 Requirement for the adoption of SSI by governments

S.No.	Requirements	Description
1	Creating a trustworthy registry	The government shall establish and manage the public register. If people want to use a blockchain network, they need to define who can join the network and who can't.
2	Build new digital wallets	Certain government organisations have been granted the authority to trusted digital wallets providers.
3	Attractions of	The government would allow its citizens to register their digital

	individuals	IDs for government-based services to promote e-government services.
4	Development of DIDs	The government would require one DID method and allow wallet providers to use it.
5	Identification of standards	Recognition of decentralised identifiers and verifiable credentials must be adopted by world leaders such as ISO, ITU, IEEE or NIST.
6	Issuing of verifiable credentials/certifications	The government will develop relevant systems and protocols for issuing digital ID documents (e.g. a digital passport)
7	Acceptance by service providers	The authentication of SSI-compliant digital identities is more convenient for service providers because they can verify customers more easily, more effectively and with higher security levels.

V. SSI FRAMEWORK AND COMPONENT ARCHITECTURE

There are three main layers in the SSI framework: regulations layer, components layer, and trust framework layer. This layered SSI framework has been presented in Figure 1. Further, the interaction among SSI components has been explicitly defined in the form of SSI component architecture.

The objective of SSI architecture is to give the user a visualisation of the components and how they interact with each other. The SSI component architecture is shown in Figure 2.

The SSI components architecture consists of three layers of functionality. The first layer is a DPKI where different ledgers with different DID methods contain DIDs for an organisation to make it publicly recognisable at this level. The second layer is a decentralised key management system (DKMS). A DID is a public key that contains one or more private keys. DKMS handles all of these keys using a structured structure. The third layer is characterised by verifiable credentials such as a driver's license, a degree, or residency proof. These verifiable credentials contribute to additional personal information about other individuals. Any user can create, verify and hold the credentials. The fourth and final stage uses verifiable presentations to create verifiable statements and verifiable credential. They are designed to securely show personal identity data of an individual to third parties, sharing only as much information as required, thus maintaining the owner's privacy.

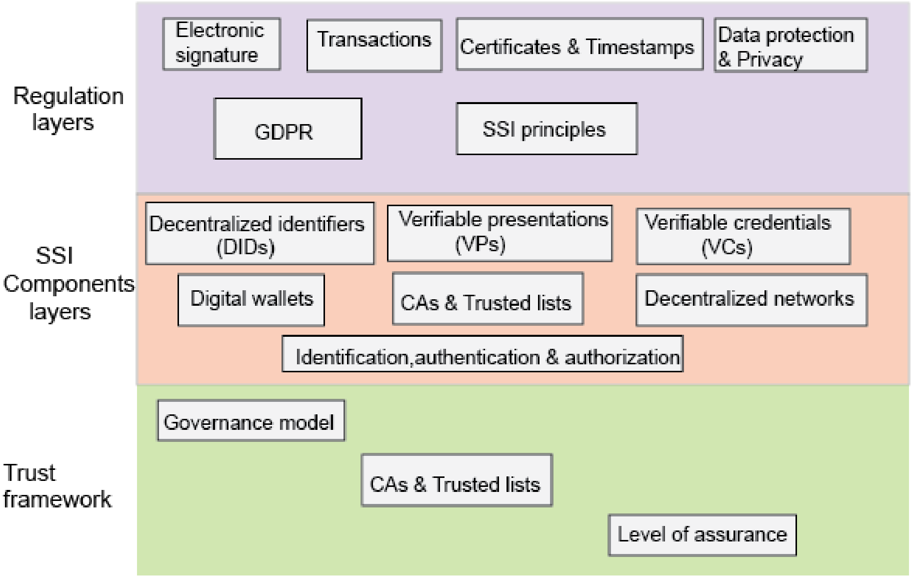

Figure 1 SSI framework

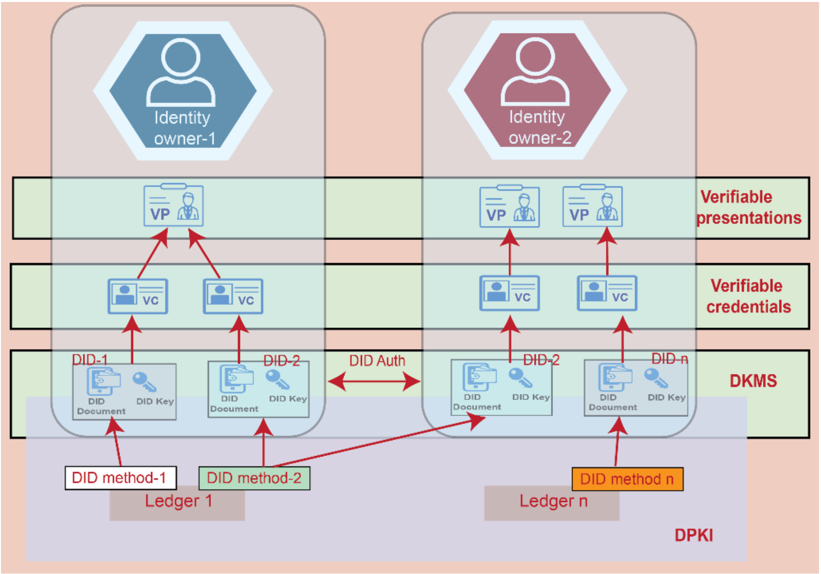

Figure 2 SSI components architecture

VI. COMPONENTS OF SSI

There are various SSI components available to develop an SSI solution and comply with SSI principles. These SSI components have been briefly in this section. A graphical representation of different SSI components has been given in Figure 3.

A. DECENTRALISED IDENTIFIERS (DIDS)

A global working group has been set up to develop the Decentralised Identifiers (DIDs) standard [32]. A DID is a digital identity that facilitates to have a verifiable and decentralised identity. A DID is an identifier associated with a subject (e.g. a person, an agency, an object, a data model, an abstract entity, etc.) that the DID controller considers to be defined. The various types of DID standards to be followed shall be known as DID methods.

- *DID Documents:* The DID refers to the DID document that provides specific information about the authentication mechanisms to prove that the DID, endpoints, and other attributes.
- *DID Registries:* The number of DID implementations with DIDs is required to have a DID registry. Due to the decentralised existence of DIDs, centralised and autonomous DID registries are not feasible. DID registries are intended to act as identifiers for a variety of purposes.
- *DID Methods:* The DID standard is made using DID methods. DID methods differ concerning the mechanisms for establishing and validating DIDs, the authentication systems. Currently, there is no officially recognised list of DID methods. However, the W3C42 and DIF43 maintain unofficial lists.

B. VERIFIABLE CREDENTIALS (VCS)

The first step to have a self-sovereign identity solution is to provide a trustworthy signing issuer that issues verifiable credentials (VC). A credential is a digital file that contains one or more credentials about a person from another source, authenticated by the verifier. The W3C working group is currently developing standards related to Verifiable Credentials (VC). The claims and the proof shall support the Verifiable Credential(VC). The proof is what determines the legitimacy of one's credentials. A claim is a statement about the topic of research on which claims could be made.

- *Credential Registry Exchange*: There are three methods for exchanging credential. In the first instance, the credential is sent from the issuer to the holder. Second, the credential is passed from the requester to the holder. Finally, the credential is transmitted from the holder to the verifier. It is essential that the credential exchange between the credential repository (i.e. the digital wallet) and the service that creates or utilises the credential be secured.
- *Revocation*: Credentials represent the individual's status and can be revoked or suspended at the consent of the person who holds them. A specific guideline should be required regarding revoking a credential and modifying the credential status.

C. VERIFIABLE PRESENTATIONS (VPS)

The W3C facilitated the concept of Verifiable Presentations within the Verifiable Credentials specification [33]. The verifiable presentation is presented through verifiable credentials and has been packaged so that its authorship is verifiable. When the Verifiable credentials presented expressly will become verifiable presentations.

- *Selective Disclosure Mechanisms and Zero-Knowledge Proofs (ZKP)*: In self-sovereign identification systems, individuals regulate both their identity and credentials. Therefore, they have the right to present themselves. Individuals have an option on how much details they should share. They have multiple verifiable credentials provided by various issuers and build a presentation with explicit statements from such credentials so that it may not disclose any other claims included in it.
- *Traceability and Monitoring*: The sharing of credential takes place off-chain, which means that the credential is not registered. Verification of the certificate ensures that there is no traceable record of the transaction. It helps to reduce data privacy issues. However, in certain situations, the sharing and verification of credentials are supposed to be transparent. It is mainly the case when measuring and providing feedback on solutions is essential.

D. DIGITAL REPOSITORIES AND WALLETS

In the sense of Self sovereign identity, a digital wallet enables private repositories of users to secure information such as keys, identities and credentials. A digital wallet can protect access to the holder by ensuring that only authorised individuals have access to the wallet. It secures and protects data with encryption. It also verifies the transfer of DID documents, trustworthy lists, and cryptographic proof of DID documents. Provide a mechanism for individuals to update their credentials.

- *Key Recovery*: The first layer to establish a digital identity contains a private key and an authenticator. It protects us from unexpected events and inappropriate uses of our identifiers and credentials. Therefore, It is essential to ensure digital wallets' recovery due to the loss or misuse of digital wallets.
- *Recovery of Credentials*: Digital wallet allows for storing and managing digital credentials. If the wallet is lost or passwords are compromised, it is possible to retrieve the password using a digital wallet. Essential recovery methods should be in place for the backing up of credentials in both cloud and offline computers. Cloud back-ups or other back-ups facilitated by the wallet provider should describe how or when the users can retrieve the credentials. The recovery process of credentials must be a balance between usability and security.

E. IDENTITY PROOFING, AUTHENTICATION, AND AUTHORISATION

Authentication, proof of identity and authorisation occur when an electronic transfer of knowledge by the service provider takes place. Identity proof relies on the verifiability of the requester. Authentication is a way of ensuring that the service has already been delivered and consumed securely. Authorisation requires that the requester have the necessary authorisation to use the service, allowing them access to the service.

- *Identity Proofing*: The Identity proofing process begins with the requesting entity requesting identity credentials. Next, the identity issuer authenticates the user's identity. The customer then receives a digital identity certificate from the issuer. Finally, the credential is saved in the secure repository.
- *Authentication*: Authentication is dependent on three distinct factors. Firstly, the password is essential. Second, the credential you have can include a mobile, ID card, or cryptographic key. Third, biometric data source like figure print
- *Authorisation*: When applying for a service, the service provider shall check that the credential issued is legitimate. The issuer is acknowledged, and that the presenter is authorised to request the credential. When a verifiable certification is issued, Two different behaviours toward providing certificates is observed, namely Authorization for the Presenter and Authorisation of purpose.

F. CERTIFICATE AUTHORITIES (CAS) AND TRUSTED LISTS (TLS)

In the digital identity system of public key infrastructure, the certificate authority issues identity credentials accepted by others with a relative degree of assurance. Others can trust multiple profit and non-profit organisations as CAs for various purposes. Currently, there is a range of trustworthy lists (TLs). The first trust list is the CAs approved by the trusted authority that individuals may trust. The second trust list is the certificates provided by the CAs that each person owns and the certificates' status. It allows us to verify that a digital certificate issued by an agency that we do not recognise or trust is certified by an entity that we fully trust.

G. DISTRIBUTED LEDGER TECHNOLOGY (DLT)

SSI must use decentralised ledgers to store cryptographic proofs for DIDs, verifiable credentials and presentations. Blockchain enables SSI to achieve the highest degree of security and scalability required. Blockchain uses public ledgers that are distinguished by the use of smart contracts. Distributed ledger technology is better suited than most other decentralised technologies for establishing Proof of Identity, blockchain address can be used as DIDs, and smart contracts can be used as trusted lists.

- *Permissionless*: Permissionless DLT allows users to access the network at any time, such as Bitcoin and Ethereum. Many networks use cryptographic technology. They have access to the system, but with high transaction fees and anonymity, every individual is anonymous.
- *Permissioned private*: Permissioned DLT consist of a finite network of well-defined entities which deploy, run, and manage all of the nodes. Generally, such networks are developed and managed by a blockchain provider.
- *Permissioned public*: For permissioned public access to the network, it provides participants with access to the network and asks that they comply with specific laws and regulations. Publicly accessible networks are open, transparent, decentralised and do not require any fees. At the same time, the identity of everyone guarantees not only anonymity but also regulatory compliance.

VII. COMPONENTS OF SSI IN COMPLIANCE WITH SSI PRINCIPLES

The explanation principles of digital identity are extensive. Some of these principles may be more specific. For example, the first concept can be divided into user control and consent. Some identity solutions may satisfy one but not the other. Given that at the time of writing these principles, there was no self-sovereign identification. It was all the more remarkable to have the majority of principles adopted from "The Evolution of Digital Identity Concepts guiding principles" by Christopher Allen [21]. In a well-known post, "The Path to Self-Sovereign Identity," Allen outlined SSI principles, including specific guidelines from other sources such as Kim Cameron and the W3C Verifiable Statements Task Force [34]. These ten principles are taken from Allen's paper [21] and serve as guidelines for SSI-adapting participants. A concise description of these SSI principles and which SSI component can be used to comply with these principles have been presented in Table 4.

1. *Control*: Users must control their identities. The user is the ultimate authority of his identity, subject to well-understood and safe algorithms that ensure that the identity and its arguments remain valid. He should be able to identify, update, or even hide it. The user is free to pick actors or privacy as he wishes. The user does not regulate all identity claims: other users can make claims about a user, but they should not be central to its identity.
2. *Access*: Users must have access to their own data. A user must always be able to easily access and recover all the claims and other identification details. There must be no hidden data and no gatekeepers.
3. *Transparency*: Transparent systems and algorithms. The systems for managing and running an identity network must be transparent in terms of their functioning, management and updating. The algorithms should be open source, well-documented and autonomous from any particular architecture.
4. *Persistence*: Identities must be long-lived. The user can only remove identities. Claims can be updated and removed, but the identity that belongs to these claims should be long-lived. Identities can ideally remain permanently, or probably as long as the consumer wants. Although private keys could have to be rotated and data need to be changed, the identity remains. In the rapidly evolving

world of the Internet, this goal may not be entirely feasible, but identities at least remain until new identity systems outdate them.

5. *Portability*: Identity information and services must be transportable. A trusted third-party entity party should not hold the identity. It should be transportable, although a trusted entity behaves in the best interests of the customer. Transportable identities ensure that the individual stays in charge of their identity, which can increase identity persistence over time.
6. *Interoperability*: Identities should be used as widely as possible. Identity is of little benefit if used only in small niches. A modern-day digital identity system aims to access identity information widely and across international borders to create global identities without relinquishing user control.
7. *Consent*: Users must agree to the use of their identity. Any identity system is designed to share identity and claims, and an interoperable system improves the number of shares occurring. However, data sharing must only occur with user consent. While other users such as an employer, credit office, or spouse can make claims, the user must also confirm consent.
8. *Existence*: Users must have an independent existence. An SSI fundamentally depends on the ineffable "I" at the core of identity. It will never fully exist in digital form. It needs to be the self-supporting kernel to support this.
9. *Minimalisation*: Disclosure of claims must be minimised. When sharing data, it should include the least amount of data required to perform the task. It is supported by selective disclosure and zero-knowledge proof. However, non-corruptibility is a difficult task .the best possible way to solve this is to use minimisation to promote privacy.
10. *Protection*: The rights of users must be protected. If the identity network priorities vary from those of individuals' rights, the network should protect users' rights and freedom over the network.

Table 4 Overview of SSI principles and required SSI components for its compliance

SSI Principle	Description	SSI Components
Control	The user controls and has authority over identity and personal data. Files are kept in a decentralised manner to the fullest extent.	Asymmetric cryptography authentication protocol DPKI (DID holder)
Access	User can access their data and identities quickly and directly.	DID naming system Digital credential wallet
Transparency	The operation and system used need to be transparent. Additionally, how an identity scheme operates, managed and maintained should be publicly available and easily understood.	open protocols and open standards
Persistence	The identity will last long since user identities will exist from birth to death.	Time revocation Revocation list Proof of non-revocation DKMS key recovery
Portability	The services of the identity system must be transportable. The user identification is not limited to any particular network. Additionally, users should be able to move their names, certificates and proofs, from one network to another.	Open standard DID

Interoperability	Identities should be as universally accepted. The organisations, databases or registries can interact internationally easily and securely via an identity system.	JSON-LD universal resolver DID Auth protocol
Consent	Users can explicitly authorise other entity to use their identity data.	verifiable credential asymmetric cryptography authentication protocol
Existence	Users must have an independent existence	DID documents verifiable presentation Multiple identifiers Anonymous credentials
Minimalization	Prevents detailed disclosure of identity information as minimising the disclosure of identity information will enhance privacy.	ZK capable verifiable credentials
Protection	The rights of user privacy need to be protected. The identity solution must include the "privacy by design" principle.	pairwise-pseudonymous DIDs Verifiable presentations DKMS endpoints

A. *Control*

Every user has an identity and knows the secret that only he knows. The possession of the secret is equivalent to the possession of the credential or the right to use the credential. It needs identity owners to keep private keys on their computers.

1. ***DPKI***: DPKI does not require a centralised authority to create keys for actors since actors themselves create them in a decentralised manner. The DID holder has a private key that allows them to control their DID [35][36]. User keys are generated on the client-side without relying on a central authority.
2. ***Asymmetric cryptography authentication protocol***: Zero-knowledge proof of asymmetric cryptography protocol enables the identity owner to prove the identity ownership by using the private key stored on the blockchain. Most of the SSI system uses the asymmetric cryptography authentication protocol for authentication [35].

B. *Access:*

1. ***DID naming***: A DID naming system is required to add human identifiers to the DID. the DID naming system develops a single-layer above the DID layer. DID documents should be registered in the blockchain and verified with the corresponding DID. In the same way, DID documents are linked to DID [37].
2. ***Digital credentials***: Mobile devices are useful as they provide user to have full control and always available. To store and retrieve keys, a mobile device can be installed with a secure wallet account. We can create more links by scanning the codes with a smartphone. The links help establishes that credentials were issued to the user and to store the digital credentials [38].

C. *Transparency*

1. ***Open protocols and open standards***: The Internet is an open network. Web, DNS, and applications are open-source software. The solutions build using open source software can be used by anyone but is not owned by anyone. Also, Everyone can improve them. An identity system based on a public blockchain needs to function the same way to provide all identities. The Sovrin is build using open source software and will provide open governance. Sovrin and the Stewards operate with complete openness and transparency [39]. Additionally, personal information should be cryptographically encrypted to prevent unauthorised access.

D. *Persistence*

Credential holders have complete power over how their credential should be used, whereas credential issuers have the right to revoke them for unauthorised usage. If the conditions for the credential are not fulfilled, the issuer shall revoke the credential. The identifier attached to the credential, or any other form of credential, will be included in the revocation list. The revocation list is kept on the ledger and can be reviewed by the verifiers if the credential presented to them has been revoked. The following approaches revoke the credential of the [40] .

1. ***Time-revocation***: expired part of credential data.
2. ***Revocation list***: Mapping the credential ID with the revocation list.
3. ***Proof of non-revocation***: ZKP of a credential that has not been revoked is contained in Hyperledger Indy.
4. ***DKMS Key recovery***: The recovery process requires users to make backups of their wallets. DKMS can provide the requisite features to retrieve passwords safely. Users must maintain several backups of their wallets and store them in secure digital storage, such as a cloud-based agent [35][36].

E. *Portability*

An identity using open standards makes a Portable Identity available to multiple standards [39].

1. ***Open standard DID***: is a portable DID develop using an open standard, and which is described and addressed by a private key on a ledge

F. *Interoperability*

1. ***JSON-LD***: the DID documents is developed using the JSON-LD. The JSON-LD will share data in a consistent format that can be understood by both systems [41].
2. ***Universal resolver***: A community-based project of the "Decentralised Identifier Foundation" (DIF) was formed to develop a universal resolver to create an interoperable system. It can resolve any DID form on the underlying ledgers of any DID method that can be used to resolve the DID method in the SSI ecosystem. It offers details regarding DIDs recorded with the DID method based on the DID. DID methods are linked with each other to make cross-border interactions easier. One of the most important parts of interoperability is DKMS, which describes how DIDs interact with one another and the ledger. It also includes offering useful tools for key management, like key recovery [42].
3. ***DID Auth protocol:*** utilises open standard, Secure Quick Reliable Login(SQRL) and the Web Auth protocol that present the challenge to authenticate the user. The standardising of

specification using open Standardising using SQRL will ensure all DIDs perform according to the designed specifications and enable interoperability[35][36] .

G. *Consent*

1. ***Verifiable credential:*** It allows users to save their identity credentials in wallets installed on personal devices and make them accessible via the Internet. It provides the user with full control & consent of the credentials stored in the wallet so that Users can also choose with whom users share information and how long the information is shared. [32].
2. ***Asymmetric cryptography authentication protocol***: It allows a given user to fully control and possess all their personal information with the public key stored in blockchain through the zero-knowledge proof(ZKP) feature of asymmetric cryptography. [36][35] .

H. *Existence*

1. ***Decentralised identifiers:*** are persistent, ensuring that the holder is authenticated to be cryptographically secure as long as the private key is present with the identity holder [36]. The domain also has several services that include a website and an agent service. The identity holder will probably have multiple data points, such as a mailing address, telephone number, or other information which might be used to develop a relationship [43].
2. ***Verifiable presentation***: A Verified credential contains evidence of authenticity from the identity issuer. It enables the identity issuer to verify the identity owner digitally [32]. A verified presentation is made by the identity owner and eventually forwarded to the verifier who verifies it.
3. ***Multiple identifiers***: An identity owner may get multiple identifiers and build a new identity when required .the ID claims may not depend on an identifier. The identifiers and credentials will continue to be separate. It impacts the combination of credentials with any identifier. Also, the DID will be shared with the verifier whenever necessary.
4. ***Anonymous credentials***: The identity owner that gives credential to the verifier does not wish to reveal his ID. alternatively. Identity ownership is shown in a one-way using zero-knowledge proof [40].

I. *Minimalization*

1. ***Zero-knowledge capable verifiable credentials***: It helps users keep their claims of credentials hidden and proves only the existence of those claims that can be used to compare claims against numbers without disclosing the actual information. ZKPs is an effective cryptographic technique that can prove claims without disclosing the actual value. The user should be able to access their credential on their personal device. The use of ZKPs based credentials presentations is required. Consequently, the user is forced to rely on a third-party for storing the credentials. [44][32].

J. *Protection*

1. ***Pairwise-pseudonymous DIDs***: It preserves privacy by preventing the linkage of identities. Whenever two services want to analyse their users' interests, the better solution is to compare a DID, which only recognises a particular connection. Additionally, there is only one information service provider that will be stored in the DID. However, the file's information is difficult to

trace as it is not assigned to a user's account. The pairwise pseudonym DID, with public and private keys, is created on the user side [36].

2. ***Verifiable presentations***: It promises enhanced privacy and balances individual integrity using ZKP cryptography techniques by verifying proof of one's identity without revealing actual private information [32].
3. ***DKMS Endpoint***: It enhances privacy by providing a way for endpoints to protect their data and establish trust with other endpoints. Endpoints are used as DIDs and DID keys that provide the anonymity of identity to prove a person's identity [35] [36].

VIII. USE CASES OF SSI

Designing and implementing Self-Sovereign Identity Solutions will open up a new world of opportunities and use cases across industries. In the next paragraphs, we discussed some of these opportunities to maximise social and financial development internationally.

- *Education*: As per IDB's study, children lacking legal documentation in Latin America and the Caribbean are up to 17.7% less likely to enrol in school than their recorded peers. It increases the chance of admission to primary education by as much as 25.3 per cent and high school by 19.5 per cent [45]. Smoother access to identification and authentication through SSI would help to reduce these numbers.
- *Government services*: Digital ID systems affect different countries based on differing capabilities for accessing government services. According to official government figures, 98% of Estonians have a national ID card and use it to travel, access bank accounts, create digital signatures, verify medical records, or e-voting [46]. The SSI model will allow all governments to upgrade to a more secure form of identity management and provide an opportunity for those without it [47][48][49].
- *Healthcare*: Healthcare will benefit significantly from the use of SSI. Healthcare is most at risk of data breaches, with 49 per cent of the total number of data breaches happening in 2018. Having more control of your medical records will help solve this issue [50][51][52]. Medical centres would minimise patients' personal identification information, from identifying people with their pseudonymous identifiers and eventually eliminating all medical information from their databases. Another possible benefit of SSI is the potential increase in how many patients will have access to healthcare. Because of ease of identification, they may qualify for the provision of healthcare services, like vaccinations [45].
- *Natural disasters*: The digitisation of documents is the best way to help keep user information confidential in a natural disaster. Decentralised registries and SSI solutions provide users with greater control over their digital identifiers and knowledge, which the user can retrieve in the event of loss or theft. In 2015, FEMA started working on how the Agency responds to disasters and handles grants and relief funds[53][54][55]. They argued that FEMA might issue blockchain identities to individuals seeking help and assistance in the event of a natural disaster [56].
- *Public safety and gender equality*: Using SSI and immutable blockchain networks will drastically improve law enforcement and public safety. Domestic violence against women, which is a public health issue, could be resolved by implementing smart contract action protocols. The action is activated automatically in the smart contract as soon as the violence has been reported [57].

V. CONCLUSION

This paper has highlighted the importance of SSI and reviewed the UPort, Civic, Shocard, and Sovrin SSI solutions based on SSI principles. This comparison concludes that none of the existing SSI solutions is fully complying with SSI principles. It further highlights the steps for adopting a fully scalable, fully operational and fully autonomous self-sovereign identity ecosystem and discussed various digital identity governing laws to be undertaken by the governments. The major contribution of this paper is to review the SSI components required for developing any SSI solution and how these SSI components are fulfilling the requirements of SSI principles compliance individually. Lastly, the applications of SSI in the domain of education, government sector, natural disaster, public safety and gender equality have been highlighted.

ACKNOWLEDGMENT

The preferred spelling of the word "acknowledgement" in American English is without an "e" after the "g." Use the singular

REFERENCES

[1] Sovrin Foundation. Sovrin^{TM}: A Protocol and Token for Self- Sovereign Identity and Decentralized Trust. 2018.

[2] World bank. ID4D 2018 Global Dataset 2018. https://id4d.worldbank.org/global-dataset (accessed December 21, 2020).

[3] Isaak J, Hanna MJ. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. Computer (Long Beach Calif) 2018;51:56–9. https://doi.org/10.1109/MC.2018.3191268.

[4] Stokkink Q, Pouwelse J. Deployment of a Blockchain-Based Self-Sovereign Identity. 2018 IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, IEEE; 2018, p. 1336–42. https://doi.org/10.1109/Cybermatics_2018.2018.00230.

[5] European Commission. Trends in electronic identification: An overview. vol. 1.1. 2018.

[6] ESSIF. European Self-Sovereign Identity Framework. Eur Comm 2021. https://essif-lab.eu/ (accessed February 25, 2021).

[7] Der U, Jahnichen S, Sürmeli J. Self-sovereign Identity $-$ Opportunities and Challenges for the Digital Revolution. ArXiv 2017:6.

[8] Muhle A, Gruner A, Gayvoronskaya T, Meinel C. A survey on essential components of a self-sovereign identity. Comput Sci Rev 2018;30:80–6. https://doi.org/10.1016/j.cosrev.2018.10.002.

[9] Baars D. Towards Self-Sovereign Identity using Blockchain Technology. University of Twente, 2016.

[10] Stokkink Q, Pouwelse J. Deployment of a Blockchain-Based Self-Sovereign Identity. 2018 IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, IEEE; 2018, p. 1336–42. https://doi.org/10.1109/Cybermatics_2018.2018.00230.

[11] Coelho P, Zúquete A, Gomes H. Federation of Attribute Providers for User Self-Sovereign Identity. J Inf Syst Eng Manag 2018;3. https://doi.org/10.20897/jisem/3943.

[12] Lundkvist C, Heck R, Torstensson J, Mitton Z. Uport: A platform for self-sovereign identity. 2016.

[13] Civic Technologies Inc. Civic Whitepaper. 2017.

[14] Ali M, Shea R, Nelson J, Freedman MJ. Blockstack: A New Internet for Decentralized Applications. vol. 41. 2017.

[15] SelfKey Foundation. Self-Sovereign Identity for more Freedom and Privacy - SelfKey 2017.

https://selfkey.org/ (accessed April 13, 2020).

[16] ShoCard. ShoCard 2020. https://shocard.com/wp-content/uploads/2019/02/ShoCard-Whitepaper-2019.pdf (accessed April 13, 2020).

[17] Mehendale DK, Reshma S. Masurekar, Harsha V. Patil. Implications of Block Chain in Real Estate Industry. Int J Recent Technol Eng 2019;8:500–3.

[18] Adam Nagy, Kwadjo Anobaah Nyante, Andreas Peter, Zoltán Hattyasy. Secure identity management on the Blockchain. University of Twente, 2018.

[19] Abraham A, Theuermann K, Kirchengast E. Qualified eID Derivation Into a Distributed Ledger Based IdM System. 2018 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng., IEEE; 2018, p. 1406–12. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00195.

[20] Ellingsen J. Self-Sovereign Identity Systems. Opportunities and challenges. Norwegian University of Science and Technology, 2019.

[21] Christopher Allen. The path to self-sovereign identity. Coin Desk 2016. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (accessed May 18, 2020).

[22] Wang F, De Filippi P. Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. Front Blockchain 2020;2. https://doi.org/10.3389/fbloc.2019.00028.

[23] van Bokkem D, Hageman R, Koning G, Nguyen L, Zarin N. Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology. ArxivOrg 2019:1–8.

[24] Schaffner M. Analysis and Evaluation of Blockchain-based Self-Sovereign Identity Systems. Technical University of Munich, 2020.

[25] Naik N, Jenkins P. Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems. 2020 IEEE Int. Symp. Syst. Eng., IEEE; 2020, p. 1–6. https://doi.org/10.1109/ISSE49799.2020.9272212.

[26] Hani Eskandar, Xhixho D, Sundberg N, Obiso M, Huseinovic K, Sharma S, et al. Digital Identity Roadmap Guide. Geneva: International Telecommunications Union; 2019.

[27] The National Archives. Guidance on Digital Preservation 2013:11–55. http://www.nationalarchives.gov.uk/information-management/projects-and-work/guidance.htm (accessed January 13, 2021).

[28] Lyons T, Courcelas L, Timsit K. Blockchain for Government and Public Services. 2018.

[29] OIX. The Open Identity Exchange 2019. https://openidentityexchange.org/members/anon/new.html?destination=%2Findex.html (accessed January 13, 2021).

[30] e-Estonia. e-identity 2019. https://e-estonia.com/solutions/e-identity/id-card/ (accessed January 13, 2021).

[31] Allende López M. Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain. Inter-American Development Bank; 2020. https://doi.org/10.18235/0002635.

[32] Sporny M, Longley D, Chadwick D. Verifiable Credentials Data Model 1.0. 19 Novemb 2019 2019:1. https://www.w3.org/TR/vc-data-model/ (accessed August 2, 2020).

[33] Reed D, Sporny M, Longley D, Allen C, Grant R, Sabadello M. Decentralized Identifiers (DIDs) v1.0 Properties id. WwwW3cOrg 2021. https://w3c.github.io/did-core/ (accessed August 19,

2020).

[34] W3C Credentials Community Group. Verifiable Claims Task Force 2017. https://w3c.github.io/vctf/ (accessed August 2, 2020).

[35] Allen C, Brock A, Buterin V, Callas J, Dorje D, Lundkvist C, et al. Decentralized Public Key Infrastructure. 2015.

[36] Reed D, Sporny M, Longley D, Allen C, Grant R, Sabadello M. Decentralized identifiers (DIDs): data model and syntaxes for decentralized identifiers. 2019.

[37] Gerard V. Designing the future identity: authentication and authorization through self-sovereign identity. Delft Univ Technol 2019:1–75.

[38] Government of Canada. Pan-Canadian Trust Framework Overview. Github n.d. https://canada-ca.github.io/PCTF-CCP/ (accessed February 25, 2021).

[39] Phil Windley DR. Sovrin : A Protocol and Token for Self-Sovereign Identity and Decentralized Trust A White Paper from the Sovrin Foundation. 2018.

[40] Hyperledger. MSP Implementation with Identity Mixer — hyperledger-fabricdocs master documentation 2018. https://hyperledger-fabric.readthedocs.io/en/release-1.3/idemix.html#what-is-idemix (accessed March 23, 2021).

[41] M. Sporny, D. Longley, G. Kellogg, M. Lanthaler, N. Lindström. JSON-LD 1.1 2020. https://www.w3.org/TR/json-ld/ (accessed August 19, 2020).

[42] Markus Sabadello. A Universal Resolver for self-sovereign identifiers. Medium 2017. https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c (accessed August 19, 2020).

[43] Tobin A, Reed D. The Inevitable Rise of Self-Sovereign Identity A white paper from the Sovrin Foundation. Provo,Utah: 2017.

[44] Glauser R. Self-Sovereign Identities in Cardossier. ETH Zürich, 2019.

[45] Brito S, Corbacho A OR. El registro de nacimientos. La llave para la inclusión social en América Latina y el Caribe. New York, USA: 2013.

[46] Sullivan C, Burger E. E-residency and blockchain. Comput Law Secur Rev 2017;33:470–81. https://doi.org/10.1016/j.clsr.2017.03.016.

[47] Alam S, Shuaib M, Samad A. A Collaborative Study of Intrusion Detection and Prevention Techniques in Cloud Computing. In: Bhattacharyya S, Hassanien AE, Gupta D, Khanna A, Pan I, editors. Int. Conf. Innov. Comput. Commun., vol. 55, Springer; 2019, p. 231–40. https://doi.org/10.1007/978-981-13-2324-9_23.

[48] Abdus S, Shadab A, Mohammed S, Mohammad.Ubaidullah B. Internet of Vehicles (IoV) Requirements, Attacks and Countermeasures. 5 Int. Conf. "Co mputing Sustain. Glob. Dev., 2018, p. 4037–40.

[49] Shuaib M, Daud SM, Alam S, Khan WZ. Blockchain-based framework for secure and reliable land registry system. TELKOMNIKA (Telecommunication Comput Electron Control 2020;18:2560. https://doi.org/10.12928/telkomnika.v18i5.15787.

[50] Shuaib M, Alam S, Daud SM. Improving the Authenticity of Real Estate Land Transaction Data Using Blockchain-Based Security Scheme, Springer, Singapore; 2021, p. 3–10. https://doi.org/10.1007/978-981-33-6835-4_1.

[51] Raghuvanshi A, Kumar Singh U, Shuaib M, Alam S. An investigation of various applications and related security challenges of Internet of things. Mater Today Proc 2021. https://doi.org/10.1016/j.matpr.2021.01.821.

[52] Shuaib M, Alam S, Daud S, Ahmad S. Blockchain-Based Initiatives in Social Security Sector. Proc. 2nd Int. Conf. ICT Digit. Smart, Sustain. Dev. ICIDSSD 2020, 27-28 Febr. 2020, Jamia Hamdard, New Delhi, India, New Delhi: EAI; 2021, p. 8. https://doi.org/10.4108/eai.27-2-2020.2303256.

[53] Shuaib M, Alam S, Shahnawaz Nasir M, Shabbir Alam M. Immunity Credentials using Self-Sovereign Identity for combating COVID-19 Pandemic. Mater Today Proc 2021. https://doi.org/10.1016/j.matpr.2021.03.096.

[54] Shuaib M, Alam S, Shabbir Alam M, Shahnawaz Nasir M. Compliance with HIPAA and GDPR in blockchain-based electronic health record. Mater Today Proc 2021. https://doi.org/10.1016/j.matpr.2021.03.059.

[55] Shuaib M, Alam S, Shabbir Alam M, Shahnawaz Nasir M. Self-sovereign identity for healthcare using blockchain. Mater Today Proc 2021. https://doi.org/10.1016/j.matpr.2021.03.083.

[56] Lewis LA. A Consideration of a National Approach: The US Planetary Impact Emergency Response Working Group (PIERWG); A Joint Effort Between NASA and FEMA, Springer, Cham; 2019, p. 151–62. https://doi.org/10.1007/978-3-030-01000-3_10.

[57] Lacchain. Blockchangel Challenge 2020. https://blockchangel.webintra.net/ (accessed January 13, 2021).