16 July 2021 Study · Digital Identity · Web & Cloud · 25 min read

Enhancing the Internet-of-Things (IoT) by utilizing Self-Sovereign-Identity (SSI)

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/enhancing-the-internet-of-things-iot-by-utilizing-self-sovereign-identity-ssi/

Self-Sovereign Identity (SSI) represents a recent identity model that enhances the user-centric identity model. SSI utilizes distributed ledger technoloy to address the central trusted party. Devices of the Internet-of-Things (IoT) can also have digital identities. Thus, questions emerge such as how SSI can enhance the internet of things. This work investigates interoperability and data sharing problems in IoT by reviewing the literature in the related field. Next, based on our analysis, we propose an architecture that addresses the identified problems. Next, we evaluate and discuss our concept.

1. Introduction

Digital identities play a more and more important role in our daily life since the number of online services is permanently increasing provided by so-called Service Providers (SPs). These identities, in particular, the identity data, are being used to perform identification and authentication towards an SP in order to grant or deny access to a service. Digital identities are often directly related to natural persons but should not be limited to these because also legal persons can have a digital identity.

Digital identities require management the so-called Identity Management (IdM). IdM includes processes covering the whole identity lifecycle, including issuing, managing, usage, support and deactivation as well as the needed governance and policies. Different IdM models evolved over time, focusing on different aspects, such as putting the user in the center as in the user-centric IdM model.

With the emergence of Blockchain technology, new opportunities also arose for IdM. Thus, a new IdM model emerged the so-called Self-Sovereign Identity model, which can be seen as a further evolvement of the user-centric model. It differs from the user-centric model by addressing the central trusted party by utilizing Blockchain technology.

1.1. Internet of Things (IoT)

With the rise of the Internet of Things (IoT), a new area began offering huge potential for new use cases. Gartner (Gartner, 2014) and IBM (IBM, 2015) predicted already in 2015 and 2014 that there will be soon millions and billions of IoT devices connected and reporting tons of data. These devices include starting from simple sensors, such as temperature sensors, to more advanced devices such as smart traffic lights. Gartner and IBM also included smartphones in their report, which is not always the case. Further, these reports predicted that with this enormous amount of connected devices, new opportunities would arise, elevating our species to a new level.

The beginning of IoT devices started with simple sensors that were pushing their data to a storage or processing location and used for monitoring systems or analyzing them. Today, IoT devices include smart meters, smart traffic lights, smart vehicles, and many more, to name a few. These devices are either interconnected with each other or to other devices, or to platforms where they report their data. Due to this huge amount of data, many new use cases can be realized, like having a smart traffic system in cities to prevent traffic jams or to decrease air pollution. Another use case could be the monitoring of a power grid, which involved many different aspects and factors. These are just two out of a countless number of use cases that these devices make possible. Dorsemaine et al. (Dorsemaine et al. 2016) defined the IoT as:

Sensors and/or actuators carrying out a specific function and that are able to communicate with other equipment. It is part of an infrastructure allowing the transport, storage, processing and access to the generated data by users or other systems. Then, a definition for the IoT would be: Group of infrastructures interconnecting connected objects and allowing their management, data mining and the access to the data they generate. All of these devices report data to their corresponding platform. Like for example, a smart fridge could provide data about the temperature on the inside, energy consumption to the end-user. This fridge could order missing items like milk at a connected store whenever they are getting under a previously defined threshold. Additionally, the fridge can also report usage data, error messages to the hardware manufacturer used to analyze user's behavior in order to enhance and costume the manufacturer's products. Another example would be a sensing device in a parking lot that reports information about if a specific parking spot is free or occupied to the corresponding platform. The city government could host this platform in order to provide a smart parking system. Currently, many different IoT devices, manufactured by a variety of companies, were created and installed, providing data and services for various purposes and run by many different organizations. All of these devices create a massive amount of data. These data were not created with the thought in mind that they are going to be used together for something bigger.

Page: 2 out of 11 Combining these data opens up new possibilities for novel use cases such as smart energy grid or smart cities. To achieve these new use cases, the data of various sensors will have to be taken into account. For instance, when looking at the smart city use case, to realize a smart traffic system that is used to prevent traffic jams and decrease pollution. This system would rely on data from traffic lights to count the cars, etc., possibly from smart cars to measure the progress within the traffic and also other systems and devices. Since these devices were not created to work together with each other, problems are emerging. Besides the previously mentioned use cases, there is a lot more potential when combining IoT data, as described in the previous paragraph. For simplicity, we will focus on this work on the smart city use case since this is, on the one hand, a complex use case but, on the other hand, still easy to follow and understand.

1.2. Outline

In this report, we are investigating the related literature in the field of IoT which is related to data exchange and interoperability aiming to identify common problems of data exchange in IoT. Additionally, we identity the reasons of data exchange problem in IoT as well as cluster the found problems into generic categories. Based on these findings, we introduce the related work in which SSI based solutions try to address some of the before mentioned issues. Finally, we introduce a concept how SSI could enrich IoT devices.

2. Background

2.1. Self-Sovereign Identity

Self-sovereign identity (SSI) is a new model that presents a new identity management (IdM) concept, which gives the owners of digital identities full control over the related identity data. When following the evolution of identity models, SSI can be interpreted as the next model in the evolution after the user-centric model providing advantages such as not having to trust a central authority. A basic SSI architecture is depicted in Figure 1.

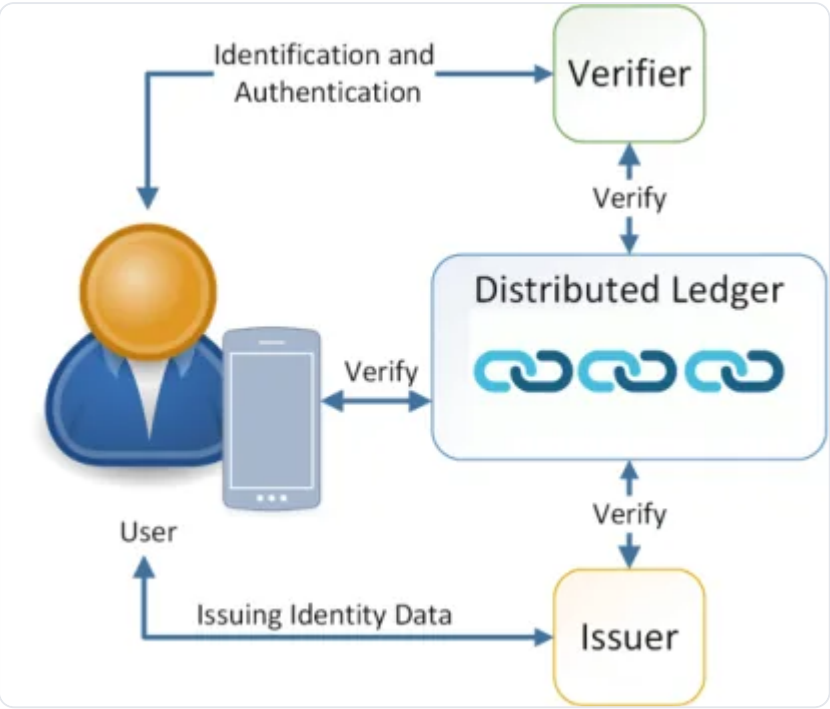


Figure 1: Basic Architecture of an SSI System (Abraham, Schinnerl, and More 2021) Page: 3 out of 11

2.1.1. Conceptual Requirements

SSI is a recent concept that does not provide an architectural definition but rather conceptional requirements. According to the Sovrin Foundation (Sovrin Foundation 2018), an SSI system satisfies four main requirements: governance to ensure the system is trusted by all stakeholders, performance at internet scale, accessibility, and privacy. Allen (Allen Christopher 2016) defined the ten principles of SSI: existence, control, access, transparency, persistence, portability, interoperability, consent, minimization, and

protection. Mühle et al. (Mühle et al. 2018) have presented the architecture of such an SSI system and surveyed essential components of SSI, and identified identification, authentication, verifiable claims, and attribute storage as these components.

2.1.2. Technical Concept

One of the core building blocks of an SSI system is the distributed ledger (DL), which serves as a decentralized public key infrastructure (DPKI) and provides properties such as immutability and transparency. Besides the DL, an SSI system requires identifiers that do not depend on an issuing party, such as a decentralized identifier (DID). Users create such identifiers and register them at the DL. Then, trusted claim issuers (or attesters) attest attributes of a user. As users in such an SSI system should be in full control, the users' identity data, DIDs, and private key material are stored in the users' domain. In contrast, a user's public information is stored on the ledger, including public keys and revocation information. When performing authentication at a service provider (SP), this SP can then verify the users' claims ownership and attestations.

2.2. Decentralized Identifier (DID)

Decentralized Identifiers (DIDs) (Community Group 2018) were designed and are used to create self-sovereign digital identities. They are URLs that provide a way for trustworthy interactions with their subject. A DID subject is the identifier that the DID describes, and DIDs redirect to DID Documents.

DID Documents contain three major sections: proof purposes, verification methods, and service endpoints. Service endpoints are URIs pointing to a service provided by a DID subject. Verification methods describe cryptographic methods that can be used with proof purposes to prove things such as the integrity of the DID Document or the relationship of an entity to the DID. DID Documents optionally contain public key(s) of the DID subject, and the proof of the public key ownership can be done statically or dynamically. Static proof of ownership requires that a DID Document is signed with the private key and later verified with the public key, whereas the dynamic proof requires a challengeresponse protocol sent to the responsible service endpoint.

The following DID example "did:method:123456789" resolves to the corresponding DID document stored on the DL. It contains a context property that maps a valid string to an Internationalized Resource Identifier or a JSON Object. The *id* property identifies the DID subject; an *authentication* property defines the subject, authentication type, controller of the corresponding private key, the public key, and the public key format needed for the authentication; a *service* property that defines the service type and the service endpoint. We refer interested readers to the extensive online documentation (Community Group 2018).

3. Problems in IoT

When trying to achieve the smart city use case, information of different IoT devices and platforms are necessary to predict events calculate solutions and monitor the current situation. Nevertheless, combining IoT data is not as simply as it seems on the first view. The following list contains reasons that create problems when sharing IoT data. The following paper were including in our literature research: (Bröring et al.

2017; Broring et al. 2018; Jangid and Chauhan 2019; Zarko et al. 2018; Kazmi, Serrano, and Lenis 2019; Daliya and Ramesh 2018; Kalatzis et al. 2018; Dorsemaine et al. 2016; Sonune and Kalbande 2018; Sasaki 2020).

1. **Purpose of Deployment:** The same IoT device could possibly be deployed for different purposes. For example, while an optical barrier could report how many people are entering or leaving a building this sensor could also be used for parking lots counting the cars entering and leaving.
2. **Service Provider:** The same IoT device could be deployed for the same purpose but possibly from different service providers, which can be competitors. Thus, these service providers do not want to interchange their information since they are competing parties.
3. **Manufacturers:** IoT devices with similar or even the same functionality are often created by various manufacturers. It is in most of the cases not in the interest of these manufactures that the IoT devices are interchangeable. For some cases it is, but for most of the cases it is not. Manufacturers generally try to keep customers in their" world" to further buy products from the same manufacturer since these devices are compatible with each other. This is the so-called" vendor-lock-in".
4. **Device Model Version:** But even if one is using the same IoT device, manufactured by the same company there is also the possibility of missing interoperability due to the version of the device. Often, when devices climb up the lather of evolution, the newer models are not compatible with older versions anymore.

According to the previous mentioned differentiation of IoT devices, and by reviewing the literature in this field, we have identified problems and clustered them into generic categories described as follows:

1. **Missing Interoperability:** IoT devices and the data they are producing are often not interoperable due to the differentiation facts. Either the data format or the communication protocol lack interoperability. Also, different device versions or protocol versions can also create problems.
2. **Missing access to the Data:** Just because a system would require the data of various IoT devices, does not mean that the service provider that plans to implement this use case can also access all these data. Whereas some of the IoT data are pushed to clouds or computing platforms, other devices store them on the device itself and have to be collected manually.
3. **Lack of Knowledge:** Since there is no general map or list of all the possible IoT devices and data deployed in the world, there is also a lack of knowledge about what kind of data and devices are available. Sometimes, it might even be the case that devices and the data they are creating should even stay secret.
4. **Lack of Motivation:** Manufacturers often try to create a vendor-lock-in to" force" the customers to stay within the specific manufacturer’s world. Also, when competing companies deploy the same system, they would rather not share their data with others to not weaken up their market position. Moreover, for others, it is simply not interesting for them to make their data available for others because it comes with extra effort and often no real benefit. Thus, there is a lack of motivation for these parties to make the data available to others.
5. **Missing Data Governance:** Even though parties would like to open their IoT data to others, data governance could hinder them in doing so. For example, when a smart car sensor measures using GPS the way the driver takes to work, these data should then not be used by the police to evaluate the average speed and send him a speeding ticket. The privacy of the users has to be preserved.

Additionally, if data were created by a certain party, it might not be allowed actually Page: 5 out of 11 to share these data with others. Data governance describes a possibly huge problem when combing or sharing data.

6. **Big Data Analysis:** After overcoming all other problems, there is still the challenge of the actual data analysis. Big data analysis is its own big research field dealing with the huge amount of data and how to analyze them. The problem lies in correctly interpreting both the input data as well as the calculated results. This problem is also not a small one and should be considered when trying to combine device data as well.

When combining or sharing data in order to achieve new uses, like the smart city use case, our identified problems have to be taken into account in order to be successful.

4. SSI Concept for IoT

This chapter introduces both, the related work in the field of SSI and IoT as well as our proposed concept.

4.1. Related Work

Since SSI is a relatively recent IdM concept, the related work especially with the focus on enhancing IoT, nevertheless, we have performed research in this field and briefly introduce the related work as follows.

The work of Bartolomeu (Bartolomeu et al. 2019) reviews the concept of SSI and further presents the possible use-cases and opportunities for industrial IoT applications utilizing SSI. Further, potential advantages and challenges were briefly discussed. In contrast, our work contains a proposed architecture, whereas Bartolomeu only discusses use-cases, challenges and advantages.

A similar view on the topic of SSI and IoT is presented by Kulabukhova (Kulabukhova et al. 2019). This work starts with an overview of approaches used within SSI systems. Next, the paper discusses SSI infrastructures, including communication and authentication protocols. An architecture on how to integrate SSI in a classic service architecture is presented as well. Finally, a summary of existing solutions is presented that implement SSI systems. In contrast, we proposed an architecture for SSI enhanced IoT based on a problem analysis performed beforehand.

In the work of Gebresilassie (Gebresilassie et al. 2020), a new concept for SSI-based IoT is presented and discussed. The proposed idea utilizes IOTA as distributed ledger platform, which limits their contribution since its focusing only on this ledger and relies on provided functionality. In contrast, our concept is presented in a generic way so that our system does not rely on one ledger implementation. Additionally, our work has a wider view addressing more aspects like various data storage options.

The work of Fedrecheski (Fedrecheski et al. 2020) first presents an overview of SSI systems, including its building blocks like DIDs and VCs. Next, a comparison of data models for identity data is presented, followed by a discussion about the benefits and challenges of SSI for IoT. In contrast, our work presents a concept including architecture that enhances IoT by utilizing SSI.

Page: 6 out of 11

4.2. Concept

This section introduces our concept in which IoT data can be combined and reused for data analysis. It contains subsections introducing the actors and one to introduce the architecture.

4.2.1. Actors

The actors involved in our concept are detailed as follows.

- **IoT Device:** In this concept, we differentiate between two kinds of IoT devices. First, the devices with low computational power such as simple sensors for measuring the temperature. To the second group count IoT devices with more computational power like surveillance cameras or IoT fridge. Devices with low computational power might not be able to perform cryptographic operations like digital signing the data before pushing these data to a receiver. In contrast, devices with more computational power might be able to sign data as well as securely store related key material.

- **Computation Middleware:** In case of an IoT device with low computational power, the computation middleware will be utilized both the storage of key material as well as perform cryptographic operations such as signing the measured data before pushing those. The advantage of such middleware lies in the fact that it will be operated directly on site of the IoT device to prevent man-in-the-middle attacks and securing data before sending it e.g. over the internet to the user's device. Besides this main task can the computational middleware be utilized for an additional task like bringing the data in the right format. Not every hardware manufacturer will support our proposed data format, utilizing JSON VCs (Sporny, Longley, and Chadwick 2019), thus, the middleware can before signing put the data in the right format and only pushes the data afterwards, which will increase the interoperability.

- **User with Mobile Device:** In our concept, the user is the registered owner of IoT devices and thus in full control over the data created by these devices and send to the user. To manage devices like adding new ones, removing old ones or using the produced data, the user takes advantage of, in our concept, a mobile device that includes an application to manage the devices. Nevertheless, utilizing a mobile phone app is only one way to achieve this, another way would be to use e.g. an online service.

- **Secure and/or Distributed Data Storage** : A secure and distributed data storage is applied in our concept to store the data, which belong to a related user. A distributed storage provides benefits such as data redundancy addressing the possible data loss of a central data storage. As second option as secure data storage is the usage of an encrypted cloud storage which utilizes cryptography such as proxy re-encryption to encrypt and re-encrypt data when sharing those.

- **SSI Network** : The SSI network serves as decentralized public key infrastructure (DPKI), which is responsible to provide verification information. This kind of information contains public keys and identifier, all personal identifiable information (PII) are stored off-ledger. The user can register public information of the device including its ownership to the ledger. This way, a service prover (SP) that is interested in combining data to perform e.g. an analysis can be sure that the data are being authentic and its integrity is protected.

- **Data Consumer** : The data consumer represents a party that is interested combining data from various users and devices in order to run an analysis on these data. Data are being delivered to the SP directly or indirectly. Indirect represents the flow in which the user is fetching the data from the secure storage and forwards it to the SP, whereas in the direct flow the user grants the SP permissions to fetch the data directly. Permissions to data should only granted for a limited period and renewed if needed to minimize the data access.

Page: 7 out of 11

4.2.2. Architecture

This subsection details the architecture of our concept in which we introduce SSI for IoT. Figure 2 illustrates the involved actors as well as the main interaction flows.

Second, the user's mobile phone receives the data from the sensors etc. and can be used for the supposed purpose. Additionally, the mobile phone app sends the data to a secure storage location. The way this is implemented depends on the used storage as well as cryptographic operations. We propose to either choose a secure and distributed data storage like IPFS [1] or select secure cloud storage that utilizes cryptographic primitives such as proxy re-encryption. In case cloud storage was used, only encrypted data are stored on the cloud. They can further re-encrypt these data 1 https://ipfs.io/, accessed 12.07.2021 Page: 8 out of 11

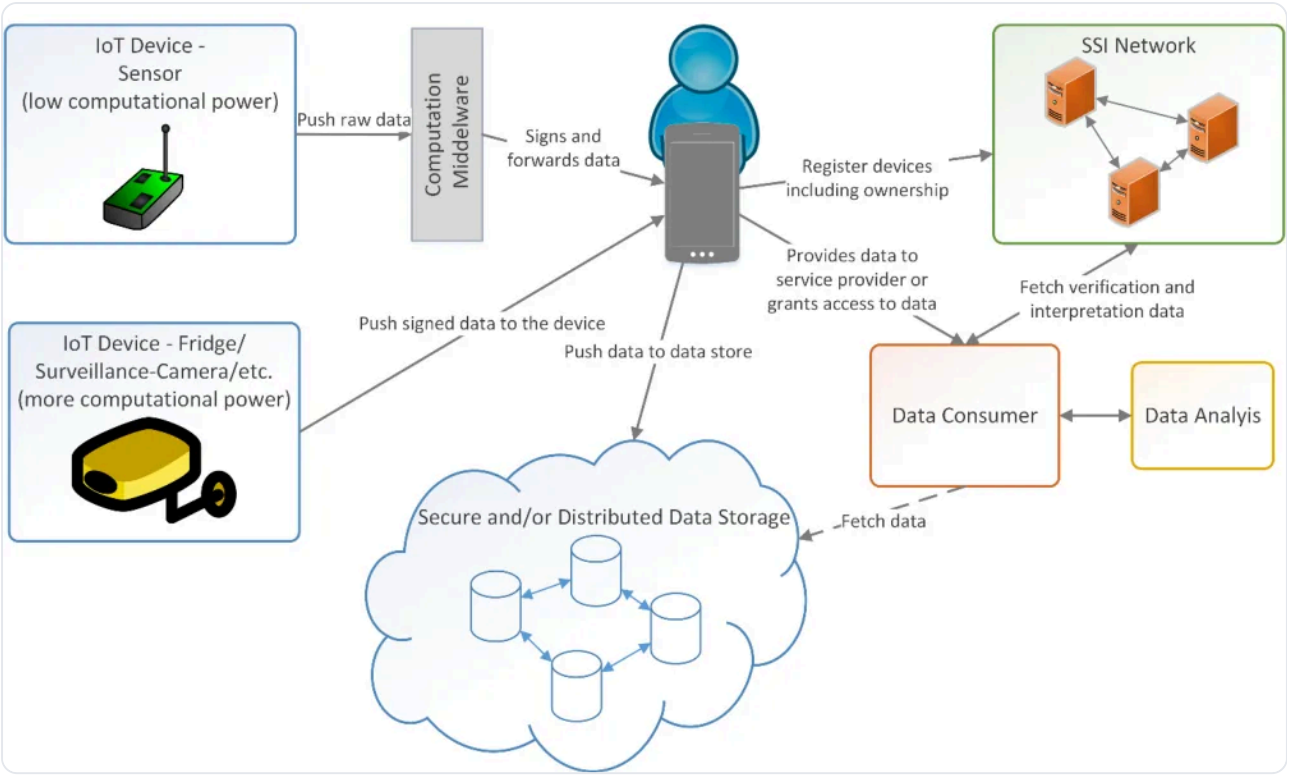


Figure 2: Architectural Overview of our Concept including Main Interaction Flows between the Actors In our architecture, the user utilizes a mobile phone, including a dedicated application to manage on the one hand the devices and, on the other hand, the data and sharing capabilities. First, the user adds her devices to its membership. In particular, we are taking advantage of DIDs and VCs identified in the preliminaries. Each device will get its own cryptographic key pair used for signing the data as well as a DID. The corresponding DID document is registered by the user to the SSI network. In case that the device does not fulfill the computational power to perform cryptographic operations or the sufficient secure storage possibility for the related key material, a so-called computational middleware is utilized on-site of the IoT device and is responsible for signing the data as well as storing the related key material. Other devices that have sufficient capabilities to store key material and perform cryptographic operations perform those directly. The created DID document corresponding to an IoT device will contain a field claiming the owner of this device which states the user's DID. The SP can at a later point fetch this document and use the contained information to validate the signature as well as the ownership of the device. Additional information like service endpoints etc., can be added to the device's DID document as well as long as it does not reveal any sensitive information.

Next, users can go to data consumers and advertise data that a user wants to share coming from a related IoT devices. After receiving the data, the data consumer can interpret and combine the data, followed by possible data analysis or conclusion. This way, complex use-cases that rely on a combination of data coming from many sensors and IoT devices can be achieved, such as a smart city or smart traffic light system.

5. Discussion and Evaluation

5.1.1. Evaluation

In the following subsection, we present an evaluation in which we detail how our system addresses the issues found in our IoT assessment.

1. **Missing Interoperability:** Since our system is built upon VCs that rely on public available contexts and schemas, it is simple to interpret this data correctly. This way, interoperability is increased heavily. For devices that do not use the proposed data format we propose to use the middleware that formats and signs the data.
2. **Missing access to the Data:** Our concept considers the storage of the data in a public storage location protected through e.g., access control. As soon as the user either provides the data or grants access to the data, the data consumer can utilize these data for the consumer's purpose.
3. **Lack of Knowledge:** Our system does not fully address this issue since the user has to actively advertise the available data towards the data consumer or to some kind of online data catalog. Nevertheless, our system does not consider some kind of broadcasting available data for the data consumer to look up.
4. **Lack of Motivation:** Motivating the user to share his/her data is not in the scope of our concept. Nevertheless, data monetization could be a good motivator for users to share their data.

5.1.2. Discussion

The work presented, including concept and evaluation, might raise some questions or discussion points which are addressed in this section.

Computation Middleware : Instead of having a middleware in place responsible for storing key material and performing cryptographic operations, the mobile phone app could perform these operations as well. Nevertheless, since the middleware is operated directly on the site of the IoT device, data integrity can be ensured.

DIDs and VCs: Our concept utilizes standardized SSI concepts, which is on the one hand DIDs and, on the other hand VCs, a JSON-based lightweight data format. VCs can be interpreted by utilizing the concept of contexts and schemas. Thus, the interoperability is increased and vendor lock-in is prevented.

User consent for data sharing: In our system, the user fully controls the data created by her devices. Only by providing explicit consent that a user is willing to share the data these are actually shared. This further leads to the fact that the user also actively has to advertise her data at a data consumer and the data consumer not automatically has the knowledge of available data.

Data monetization : The possibility of data monetization could strongly increase the motivation of user actually to share their data with a data consumer. This could be achieved by e.g., implementing an online catalog where the user can register the data they are willing to share. Data consumers can look up available data sets in this catalog.

6. Conclusion

In this work, we have assessed related work related to IoT and interoperability in IoT. Through the assessment, we were able to identify reasons for problems in IoT and further to identify the actual problems as well. Next, we proposed an IoT concept enriched by SSI in order to address the before identified problems. We start our concept by introducing the involved actors, followed by a description of our

envisioned architecture. The architecture also details the main interactions between the actors. Finally, we present an evaluation of our system based on the before mentioned problems. Additionally, a discussion describes design decisions as well as other views on our work.

We conclude that SSI has the potential to enrich IoT systems and can help to increase interoperability as well as data sharing capabilities. Nevertheless, each use-case IoT use-case which is considered to apply SSI to it has to be separately evaluated due to the SSI overhead that might come with it. We further propose to increase the research in this direction since there are still open questions related to the identified problems that have not been addressed.

7. Bibliography

Abraham, Andreas, Christopher Schinnerl, and Stefan More. 2021. "SSI Strong Authentication Using a Mobile-Phone Based Identity Wallet." *SECRYPT 2021*. Allen Christopher. 2016. "The Path to Self-Sovereign Identity." April 25. 2016.

http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. Bartolomeu, Paulo C., Emanuel Vieira, Seyed M. Hosseini, and Joaquim Ferreira. 2019. "Self Sovereign Identity: Use-Cases, Technologies, and Challenges for Industrial IoT." *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA* 2019-Septe: 1173–80. https://doi.org/10.1109/ETFA.2019.8869262. Bröring, Arne, Stefan Schmid, Corina Kim Schindhelm, Abdelmajid Khelil, Sebastian Käbisch, Denis Kramer, Danh Le Phuoc, Jelena Mitic, Darko Anicic, and Ernest Teniente. 2017. "Enabling IoT Ecosystems through Platform Interoperability." *IEEE Software* 34 (1): 54–61. https://doi.org/10.1109/MS.2017.2. Broring, Arne, Andreas Ziller, Victor Charpenay, Aparna S. Thuluva, Darko Anicic, Stefan Schmid, Achille Zappa, Mari Paz Linares, Lars Mikkelsen, and Christian Seidel. 2018. "The BIG IoTAPI-Semantically Enabling IoT Interoperability." *IEEE Pervasive Computing* 17 (4): 41–51. https://doi.org/10.1109/MPRV.2018.2873566. Community Group, W3C. 2018. "Decentralized Identifiers (DIDs) v0.11." 2018. https://w3c ccg.github.io/did-spec/. Daliya, V. K., and T. K. Ramesh. 2018. "A Survey on Enhancing the Interoperability Aspect of IoT Based Systems." *Proceedings of the 2017 International Conference On Smart Technology for Smart Nation, SmartTechCon 2017*, 581–86. https://doi.org/10.1109/SmartTechCon.2017.8358438. IBM, 2014. "Device Democracy Saving the Future of the Internet of Things IBM Institute for Business Value." Dorsemaine, Bruno, Jean Philippe Gaulier, Jean Philippe Wary, Nizar Kheir, and Pascal Urien.

2016. "Internet of Things: A Definition and Taxonomy." *Proceedings - NGMAST 2015: The 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, January, 72–77. https://doi.org/10.1109/NGMAST.2015.71.

 Fedrecheski, Geovane, Jan M. Rabaey, Laisa C.P. Costa, Pablo C. Calcina Ccori, William T.

Pereira, and Marcelo K. Zuffo. 2020. "Self-Sovereign Identity for IoT Environments: A Perspective." *ArXiv* . Gebresilassie, Samson Kahsay, Joseph Rafferty, Philip Morrow, Liming Luke Chen, Mamun Abu Tair, and Zhan Cui. 2020. "Distributed, Secure, Self-Sovereign Identity for IoT Devices." *IEEE World Forum on Internet of Things, WF-IoT 2020 - Symposium Proceedings*, 1–6. https://doi.org/10.1109/WF-IoT48130.2020.9221144. Jangid, Aarti, and Parul Chauhan. 2019. "A Survey and Challenges in IoT Networks." *Proceedings of the International Conference on Intelligent Sustainable Systems, ICISS 2019*, no. Iciss: 516–21. https://doi.org/10.1109/ISS1.2019.8908079. Kalatzis, Nikos, George Routis, Ioanna Roussaki, and Symeon Papavassiliou. 2018. "Enabling Data Interoperability for Federated IoT Experimentation Infrastructures." *2018*

Global Internet of Things Summit, GIoTS 2018, 1–6. https://doi.org/10.1109/GIOTS.2018.8534555. Kazmi, Aqeel, Martin Serrano, and Angelos Lenis. 2019. "Smart Governance of Heterogeneous Internet of Things for Smart Cities." *Proceedings of the International Conference on Sensing Technology, ICST* 2018-Decem: 58–64. https://doi.org/10.1109/ICSensT.2018.8603657. Kulabukhova, Nataliia, Andrei Ivashchenko, Iurii Tipikin, and Igor Minin. 2019. *Self-Sovereign Identity for IoT Devices* . *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* . Vol. 11620 LNCS. Springer International Publishing. https://doi.org/10.1007/978-3-030-24296-1_37. Gartner, 2014. "Mass Adoption of the Internet of Things Will Create New Opportunities and Challenges for Enterprises." Accessed July 16, 2021. https://www.gartner.com/en/documents/2994817/mass-adoption-of-the-internet-of-things-willcreate-new-. Mühle, Alexander, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. 2018. "A Survey on Essential Components of a Self-Sovereign Identity." *Computer Science Review* 30: 80–86. https://doi.org/https://doi.org/10.1016/j.cosrev.2018.10.002. Sasaki, Yuya. 2020. "We Do Not Have Systems for Analysing IoT Big-Data." *10th Annual Conference on Innovative Data Systems Research (CIDR '20)*, 1. Sonune, Suvarnamala, and Dhananjay Kalbande. 2018. "IoT Enabled API for Secure Transfer of Medical Data." *Proceedings of 2017 International Conference on Intelligent Computing and Control, I2C2 2017* 2018-Janua: 1–6. https://doi.org/10.1109/I2C2.2017.8321934. Sovrin Foundation. 2018. "Sovrin [TM] : A Protocol and Token for Self- Sovereign Identity and Decentralized Trust." *Sovrin*, no. January: 1–41. Sporny, Manu, Dave Longley, and David Chadwick. 2019. "Verifiable Credentials Data Model 1.0."

19 November 2019. 2019. https://www.w3.org/TR/vc-data-model/. Zarko, Ivana Podnar, Joaquin Iranzo, Christoph Ruggenthaler, Jose Antonio Sanchez Murillo, Joao Garcia, Pavle Skocir, and Sergios Soursos. 2018. "Collaboration Mechanisms for IoT Platform Federations Fostering Organizational Interoperability." *2018 Global Internet of Things Summit, GIoTS 2018* . https://doi.org/10.1109/GIOTS.2018.8534547.