The University of Texas at Austin
Center for Identity

An Identity Asset Sensitivity Model in Self-Sovereign Identities

Kai Chih Chang
Razieh Nokhbeh Zaeem
K. Suzanne Barber

UTCID Report #21-07

August 2021

An Identity Asset Sensitivity Model in Self-Sovereign Identities

Kai Chih Chang
kaichih@identity.utexas.edu
The University of Texas at Austin
Austin, Texas, USA

Razieh Nokhbeh Zaeem
razieh@identity.utexas.edu
The University of Texas at Austin
Austin, Texas, USA

K. Suzanne Barber
sbarber@identity.utexas.edu
The University of Texas at Austin
Austin, Texas, USA

ABSTRACT

Due to the emergence of new paradigms such as social media and the Internet of Things (IoT), the use of the Internet has ushered in further challenges. After years of research, there is still no complete layer of identity on the Internet. In order to provide identity management, self-sovereign identity has become a popular choice. Self-sovereign identities provide users with complete autonomy and immutability for personal identities, as well as complete control for their identity owners. Like any type of identity, a self-sovereign identity also processes the Personally Identifiable Information (PII) of the identity holder and faces privacy and security risks common to identity management. This research proposes a model of determining PII sensitivity by a score to measure what attributes or combination thereof is sensitive to share. Our work highlights that while it is important to improve *how* PII attributes are shared, it is paramount to identify *which* PII attributes are safer to share to achieve the same identity management goals.

KEYWORDS

Self-Sovereign Identity, Privacy, Internet of Things, Identity

ACM Reference Format:
Kai Chih Chang, Razieh Nokhbeh Zaeem, and K. Suzanne Barber. 2021. An Identity Asset Sensitivity Model in Self-Sovereign Identities. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Due to the massive increase in online services, the number of users, and the rapid growth of devices, digital identities have become complex and more difficult to manage than ever. The Internet of Things (IoT) continues to expand in scale and scope, resulting in different interactions between devices, services, and people. This leads to low communication privacy in the IoT ecosystem and insufficient authenticity of information. Therefore, the IoT ecosystem is facing various new challenges. A key pillar of digital identity security and privacy is a powerful identity management system, of which Self-Sovereign Identity is a brand new solution.

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Self-Sovereign Identity (SSI) is emerging as the new paradigm for digital identity and privacy. In contrast to most previous identity management systems where the service provider was at the center of the identity model, SSI is user centric [18]. An identity holder has full control on what data to disclose to the verifier and can also prove to a verifier the knowledge of an attribute without revealing the attribute itself using zero-knowledge proofs [14].

As with any type of identity, self-sovereign identities too deal with Personally Identifiable Information (PII), or identity assets, of the identity holders and come with the usual risks of privacy and security. This study explored self-sovereign identities with respect to privacy alongside its credential verification process. By proposing a model of determining identity asset sensitivity by a score, a program for SSI agent is made to arbitrate what attributes or combination thereof is sensitive to share.

This paper makes the following contributions:

(1) We make an identity model for agents of SSI solutions to arrive at a decision on sharing attributes for proof requests.
(2) Having access to UT CID probabilistic models and Bayesian inference tool Ecosystem [20], we take advantage of Bayesian inference to help calculate sensitivity score of identity assets.

The remainder of the paper is arranged as follows: Section 2 describes the SSI process in general. Section 3 introduces our background work and methodology. Section 4 shows an analysis of our solution. Section 5 describes related work of SSI. Section 6 provides a conclusion.

2 SELF-SOVEREIGN IDENTITY

Self-Sovereign Identity (SSI) is an approach in which users have full control of their own digital identities. There are three core actors in SSI: Holder , Issuer, and Verifier. The holder is the person possessing their own identity assets and accessing an online service. The verifier is the online service (relying party) that needs to know something about the holder. The issuer is an entity that can hold and state information about the holder. In this section, we give a high-level introduction of how SSI works.

2.1 Decentralized Identifiers

Decentralized Identifiers (DIDs), a new type of unique identifier, is being developed with the support of the W3C [23].

They are designed to enable users to generate their own identifiers using systems they trust. An example of DID URL is

```
did:method:112233445566778899
```

The *did* above shows that it is a DID. The *method* indicates the DID method which defines how implementers can realize the features described by this specification. 112233445566778899 is the DID

method-specific identifier which identifies the DID subject. In order to communicate securely with the DID controller, a designated service endpoint must be used. At the same time, it is necessary to realize the attribute certification process by combining the certification purpose and the verification method [3]. A DID document (DDO) can define a given verification method (eg, an encrypted public key) to evaluate a specific proof created with a unique purpose (eg, identity verification). A common storage mechanism for DDOs are blockchains [2], from which they can be resolved using the referred DID.

2.2 Verifiable Credentials

Verifiable Credentials (VCs) is a W3C recommendation for portable and provable claims about a subject [24]. For example, a person can claim to be 18 years old and a device can claim to be type of a censor. VCs provide us with a digital equivalent of credentials we use in our daily lives like a driver's license or a passport. It also supports selective disclosure, so end users can prove claims about their identity without revealing more information than they intend to. VCs can express information that a physical credential contains, but the usage of digital signatures from both the issuer and holder make them tamper-evident and more trustworthy to the verifier [17].

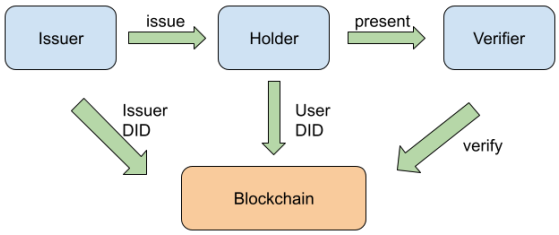

Figure 1: A simple graph that shows the high level architecture of SSI.

2.3 Process

Like what is shown figure 1, at a high level, an issuer publishes and validates themselves to blockchain. Credentials issued are signed with the issuer's private key corresponding to the public key in the DID. Verifiers construct proof the request which is then presented to the holder. Holders construct verifiable presentation using credentials issue. Verifiers check the presentation against the issuer's public key from the DID.

To verify any credential, a verifier makes a proof request to the holder (prover) requesting certain attributes and predicates. Some of these are mandatorily required to be verifiable (e.g. social security number.) while some can be self-asserted by the identity holder (e.g. name.) [4]. To be able to discern between proof requests that requests sensitive data versus ordinary disclosable data by an agent, we propose a model that provides a novel way for agents to arrive at a decision on sharing attributes for proof requests between communicating DIDs.

3 DATA AND METHODOLOGY

In this section, we briefly introduce the background work that we are using and also the details of our risk measurement model.

3.1 UT CID ITAP Dataset

The Identity Threat Assessment and Prediction (ITAP) [25–29] is a research project at the Center for Identity at the University of Texas at Austin that enhances fundamental understanding of identity processes, valuation, and vulnerabilities. The purpose of ITAP is to identify mechanisms and resources that are actually used to implement identity breach. ITAP cares about the exploited vulnerabilities, types of identity attributes exposed, and the impact of these events on the victims.

Between years 2000 and 2020, about 6,000 incidents have been captured [1]. ITAP gathers details of media news stories (e.g., the identity assets exposed, the location and date of the event, the age and annual income of the victims, and the perpetrators' methods) about identity theft with two methods. First, it monitored a number of Web sites that report on cases of identity theft. Second, it created a Google Alert to provide notifications when any new report of identity theft appears. By *manually* analyzing these cases, ITAP has generated a list of identity attributes with each of them being assigned identity-related vulnerabilities, values, risk of exposure, and other characteristics depending on their properties, such as, whether or not an attribute is unique to a person, whether or not an attribute is widely used, how accurately it can be verified, etc. To date, ITAP has generated a list including over 600 identity assets, which is the list of identity assets we are referring to in this research.

Each identity asset in the UT CID ITAP dataset has a group of properties, including, but not limited to the following properties:

Risk: indicates the probability of this identity asset being misused in identity theft and fraud incidents.
Value: indicates the monetary value of this identity asset when misused in identity theft and fraud incidents.

3.1.1 Overlap with the Internet of Things. While ITAP data is collected from all sorts of PII, we believe—based on our prior research—that there is a good overlap between ITAP and PII stored in IoT. People continue to store their sensitive information in their smart-phone applications. A great body of research is dedicated to the sensitive data storing on mobile phones including our prior work [5]. Whether the applications are installed by the phone manufacturer or downloaded by the user, each app has a privacy policy explaining how that app collects, uses and protects identity assets. We analyzed those privacy policies to begin to uncover just how much of our identity assets is on our phones and potentially shared/traded on the internet. We investigated about 200 mobile apps and from these apps, our results indicated that 35% of the identity assets in the UT CID ITAP dataset were being collected by our mobile phone. Therefore, we took the UT CID ITAP dataset as a reference to help with our sensitivity scores.

3.2 UT CID Identity Ecosystem

Taking UT CID ITAP dataset as input, the UT CID Identity Ecosystem [6, 7, 9, 15, 16, 20, 21] developed at the Center for Identity at the University of Texas at Austin models identity relationships, analyzes identity thefts and breaches, and answers several questions about identity management. It transforms the dataset into identity assets and relationships, and performs Bayesian network-based inference to calculate the posterior effects on each attribute. The UT CID Identity Ecosystem Graphical User Interface (GUI) can color and size attribute nodes based on various properties as shown in Figure 2.

We represent UT CID Identity Ecosystem as a graph $G(V, E)$ consisting of N identity assets $A_1, ..., A_N$ and a set of directed edges as a tuple $e_{ij} =< i, j >$ where A_i is the originating node and A_j is the target node such that $1 \leq i, j \leq N$. Each edge e_{ij} represents a possible path by which A_j can be breached given that A_i is breached.

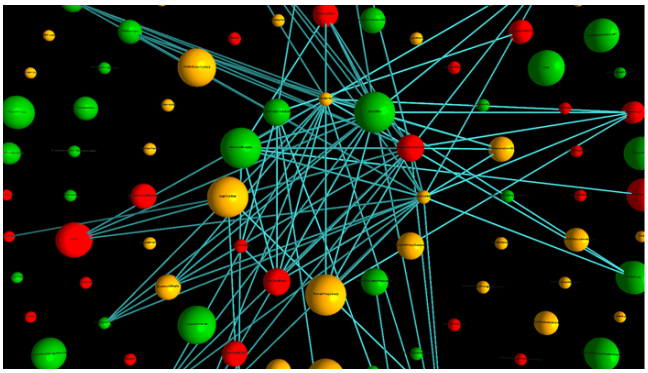

Figure 2: A snapshot of the UT CID Identity Ecosystem. The color of nodes is determined based on its risk and the size of nodes is decided based on its value.

3.3 Calculating the Sensitivity Score

In this model, the score should reflect the sensitivity level of the set of identity assets. The higher the score is, the more sensitive this set is and the more dangerous to one's privacy when this set is exposed. Dangerous here means the danger of monetary loss one would encounter when the identity asset of this person is exposed. We leverage the UT CID ITAP and Identity Ecosystem to help with the measurement of sensitivity scores.

Recall that ITAP associates monetary values to identity assets. Each identity asset also has a prior probability, meaning the probability this node is likely to be exposed on its own before the breach evidence set is given. Given N identity assets in UT CID ITAP dataset, each identity asset A_i is labeled with a monetary value $V(A_i)$ and a prior probability $P(A_i)$. We could have simply used the monetary loss and the prior probability for our model but then many of the numbers end up being zero. Thus, we leverage two more parameters which we introduced in previous work [6] to refine risk and value of identity assets.

There are many identity assets that have the monetary value 0 reported from UT CID ITAP, because the monetary loss of the identity asset's exposure was not reported in the UT CID ITAP news stories. The two parameters can increment the value of risk and loss by a small amount which can lead to the result of elimination of some zero outcomes. We have shown that these two parameters have reduced around 10% (50 identity assets) of the number of identity assets in the lowest rank [8]. Therefore, we are using them here to refine risk and value as well.

The first parameter we reuse from our previous work is called *Accessibility*. We analyzed identity asset's ancestors (in the UT CID Identity Ecosystem graph) to assess the probability and likelihood of discovering this node from other nodes. Let, $Anc(A_i)$ be the set of ancestors of A_i. By performing Bayesian network-based inference on each element in $Anc(A_i)$, we can derive our accessibility of A_i as

$$AC(A_i) = \Sigma(\Delta P(Anc(A_i))) \tag{1}$$

where ΔV denotes the value difference for risk. Low values of accessibility indicate that it is more difficult to discover to this attribute from others. An identity asset with low accessibility is harder to breach or discover (discoverability).

Therefore, given a set S of K identity assets sharing for proof request between communicating DIDs, the probability of being exposure of set S after refining with accessibility can be shown as

$$\begin{aligned} P'(S) &= P(S) + AC(S) \\ &= \frac{\Sigma P(A_i)}{K} + \Sigma(\Delta P(\bigcup_{i=1}^{k} Anc(A_i))) \end{aligned} \tag{2}$$

where $P(S)$ is the mean value of risk for S.

The other parameter from our previous work is called *Post Effect*. For a target identity asset, we analyze its descendants in the UT CID Identity Ecosystem graph. Let, $Des(A_i)$ be the set of descendants of A_i. By performing Bayesian network-based inference on A_i, we can derive our post effect of A_i as

$$PE(A_i) = \Sigma(\Delta V(Des(A_i))) \tag{3}$$

where ΔP denotes the value difference for monetary loss. The post effect measures how much the respective identity asset would influence others. The low value of post effect of an identity asset indicates that the damage or loss one would encounter is smaller after this identity asset is exposed to fraudsters.

Hence, given a set S of K identity assets sharing for proof request between communicating DIDs, the value of set S after refining with post effect can be shown as

$$\begin{aligned} V'(S) &= V(S) + PE(S) \\ &= \frac{\Sigma V(A_i)}{K} + \Sigma(\Delta V(\bigcup_{i=1}^{k} Des(A_i))) \end{aligned} \tag{4}$$

where $V(S)$ is the mean value of monetary loss for S.

Then the expected loss of S can be shown as

$$Exp(S) = P'(S) \cdot V'(S) \tag{5}$$

The score of S is then derived by normalizing the expected loss to get a value between 0.0 and 1.0, with 1.0 being the most sensitive dataset to share. As a result, the score can be shown as

$$score(S) = \frac{ln(Exp(S))}{Total} \tag{6}$$

where *Total* denotes the sum of expected loss of the entire UT CID ITAP dataset.

4 COMPARATIVE ANALYSIS

Rana et al. [21] have shown the set of high frequently-used identity assets used in popular blockchain-based identity verification solutions. We are applying our approach on this set of identity assets and give some results and analysis in this section.

The identity assets used in these solutions are Email Address and Phone Number for account creation or enrollment and either of these government issued identity cards: Social Security Number(SSN), Driver's License Number, Passport Information, and National Identity Card. Table 1 shows this set of identity asset, their statistics, and their scores. National Identity Card on the last row has the value 0 of loss. If we were to simply use loss and risk, the score would have been 0, but we can see that its score is still greater than 0 due to our refinement with acceccibility and post effect. Social Security Number has the highest score in the entire UT CID ITAP dataset.

We have made email address and phone number as the base case, since in many blockchain-based IdM solutions, email address and phone number are used to set up accounts. Then we have listed down each of the set of identity asset shared for verification and apply our approach for that set. We have listed the the set and its score in Table 2. We observe the maximum score is for SSN along with email address and phone number and also that the score of National Identity Card along with email address and phone number is merely the same as the base case. The reason is that National Identity Card actually does not have that many ancestors and descendants in the UT CID Identity Ecosystem graphic model. Hence, using National Identity Card for identity verification process is recommended for SSI solutions as it is less sensitive and minimizes risk and liability.

5 RELATED WORK

5.1 Overview

The future Internet of Things will require users to be the root of trust in their devices, leading to a user-centric Internet of Things. With the increasing importance of privacy issues, solutions that minimize the sharing of personal data have become critical. The comprehensive realization of these will require innovative and open IoT authentication standards.

Fedrecheski et al. [11] discussed aspects of self-sovereign identity that are likely to improve decentralized IoT security and privacy, while also pointing out the factors that will require innovation to bring SSI to IoT, such as support for constrained devices.

Dai et al. [10] discussed several challenges for these devices such as suffering from limited resources including computing resource, storage resource, and battery power. They also showed that it is challenging to preserve data privacy in IoT due to the complexity and the decentralization of IoT systems.

Therefore, some researches have started focusing on enhancing identity privacy for SSI. Grüner et al. [12] proposed a universal quantifiable trust model and a specific implementation variant of blockchain-based identity management. In the paper they described functions to calculate the specific trust values and present the corresponding algorithm. Trust can be derived in a decentralized manner from the proof of claims and applied to the associated digital identity by using this model. Bhattacharya et al. [4] proposed a novel attribute sensitivity score model for self-sovereign identity agents to ascertain the sensitivity of attributes shared in credential exchanges. This model is created by first manually assigning scores to identity attributes and then feeding facts to an expert system to determine how sensitive the requested attributes are. However, those scores relied on expert estimation. On the other hand, we constructed our privacy risk model by leveraging the probabilistic model in the UT CID Identity Ecosystem and taking the dataset from empirical UTCID ITAP as our input.

5.2 Frameworks

In this section, we introduce some popular self-sovereign identity identity management systems (IDMs). All of the frameworks leverage some blockchain technology, which lets them take advantage of the blockchain's decentralized, secure, private and immutability characteristics. Existing IDMs can be classified into traditional and decentralized identity domain models. Traditional IDMs mainly rely on a centralized identity provider (IDP). The program performs all operations to create, update, manage and delete identities throughout the user's life cycle. The recently developed decentralized IDMs uses Distributed Ledger Technology (DLT) as its enabling technology. Features of the blockchain can address the requirements of the IoT ecosystem.

5.2.1 Sovrin. The Sovrin SSI is based entirely on open source projects––the Hyperledger Indy Project [22]. It performed Privacy by Design which includes pairwise pseudonymous identifiers, peer-to-peer private agents, and selective disclosure of personal data using zero-knowledge proof cryptography.

5.2.2 uPort. uPort is based on the SSI concept implemented on the Ethereum blockchain technology [19]. It uses Ethereum smart contracts by addressing them with unique persistent identifiers. A smart contract is a program written to automatically observe, accomplish and implement an agreement. Any user can call the smart contract to execute its code so that developers can build and deploy arbitrarily complex user-facing apps and services.

5.2.3 Jolocom. Jolocom [13] also stores decentralized identities (DIDs) on the public permissionless Ethereum blockchain. Its DID documents (DDO) describe how to use a specifc DID and may contain additional attributes. Jolocom allows for the generation of child DIDs that can hide that credentials concern the same person.

Blockchain is the most widely used technology among the DLT types that led to many innovations beyond the financial industry. Thus, there are plenty of blackchain-based IDMs existing in the current IoT society. As a contribution, our work is made for SSI agents to arbitrate what identity assets or combination thereof is sensitive to share.

6 CONCLUSION

In this paper, we sought to understand the sensitivity of the set of Personally Identifiable Information (PII), or identity assets, used and shared for Self Self-Sovereign Identity (SSI) solutions. Most

Table 1: Sensitivity score of identity assets.

Identity Asset Name	Prior Probability	Loss (USD)	Score
Email Address	0.027526	18105024	0.613
Phone Number	0.017439	4405490	0.605
Social Security Number	0.096598	27465086	0.938
Driver's License Number	0.008719	2314811	0.688
Passport Information	0.002565	1252465	0.652
National Identity Card	0.000342	0	0.125

Table 2: Combination of different identity assets.

Verification Set	Score
Email Address, Phone Number	0.665
Email Address, Phone Number, SSN	0.957
Email Address, Phone Number, Passport	0.765
Email Address, Phone Number, Driver's License	0.750
Email Address, Phone Number, National Identity Card	0.687

solutions are using similar SSI architectures. Therefore, we sought to construct a model of determining identity asset sensitivity by a score—applicable on most SSI solutions.

Our approaches leveraged the identity assets collected from these mobile apps and cross-referenced these PII to a list of over 600 identity assets collected in the Identity Theft Assessment and Prediction (ITAP) project at The University of Texas at Austin. The ITAP project investigates theft and fraud user stories to assess how identity assets are monetized and the risk (likelihood) of respective identity assets to be stolen and/or fraudulently used.

In this work, we utilized two parameters that resulted from UT CID probabilistic models and Bayesian inference tool to refine the original risk of exposure and value of monetary loss. Our comparison of different set of identity asset that used for verification process in Blockchain-based solutions shows that National Identity Card for identity verification process is recommended for SSI solutions as it is less sensitive and minimizes risk and liability.

This work was the first to provide a program to generate sensitivity score of the set of identity assets for giving a novel way for agents to arrive at a decision on sharing attributes for proof requests between communicating DIDs by leveraging the personal data reference model built by the UT CID Identity Ecosystem and ITAP projects.

REFERENCES

[1] 2019. *ITAP Report 2019.* Technical Report. Center for Identity, University of Texas at Austin.

[2] D.S. Baars. 2016. Towards self-sovereign identity using blockchain technology. http://essay.utwente.nl/71274/

[3] Paulo C Bartolomeu, Emanuel Vieira, Seyed M Hosseini, and Joaquim Ferreira. 2019. Self-sovereign identity: Use-cases, technologies, and challenges for industrial iot. In *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 1173–1180.

[4] Manas Pratim Bhattacharya, Pavol Zavarsky, and Sergey Butakov. 2020. Enhancing the Security and Privacy of Self-Sovereign Identities on Hyperledger Indy Blockchain. In *2020 International Symposium on Networks, Computers and Communications (ISNCC)*. 1–7. https://doi.org/10.1109/ISNCC49221.2020.9297357

[5] Kai Chih Chang, Razieh Nokhbeh Zaeem, and K. Suzanne Barber. 2020. Is Your Phone You? How Privacy Policies of Mobile Apps Allow the Use of Your Personally Identifiable Information. In *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. 256–262. https://doi.org/10.1109/TPS-ISA50397.2020.00041

[6] Kai Chih Chang, Razieh Nokhbeh Zaeem, and K Suzanne Barber. 2018. Enhancing and Evaluating Identity Privacy and Authentication Strength by Utilizing the Identity Ecosystem. In *Proceedings of the 2018 Workshop on Privacy in the Electronic Society*. ACM, 114–120.

[7] Kai Chih Chang, Razieh Nokhbeh Zaeem, and K Suzanne Barber. 2018. Internet of things: Securing the identity by analyzing ecosystem models of devices and organizations. In *2018 AAAI Spring Symposium Series*.

[8] Kai Chih Chang, Razieh Nokhbeh Zaeem, and K Suzanne Barber. 2020. A Framework for Estimating Privacy Risk Scores of Mobile Apps. In *International Conference on Information Security*. Springer, 217–233.

[9] Chia-Ju Chen, Razieh Nokhbeh Zaeem, and K Suzanne Barber. 2019. Statistical Analysis of Identity Risk of Exposure and Cost Using the Ecosystem of Identity Attributes. In *2019 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, 32–39.

[10] Hong-Ning Dai, Zibin Zheng, and Yan Zhang. 2019. Blockchain for Internet of Things: A Survey. *IEEE Internet of Things Journal* 6, 5 (2019), 8076–8094. https://doi.org/10.1109/JIOT.2019.2920987

[11] Geovane Fedrecheski, 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. *2020 Global Internet of Things Summit (GIoTS)* (Jun 2020). https://doi.org/10.1109/giots49054.2020.9119664

[12] Andreas Grüner, Alexander Mühle, Tatiana Gayvoronskaya, and Christoph Meinel. 2018. A Quantifiable Trust Model for Blockchain-Based Identity Management. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. 1475–1482. https://doi.org/10.1109/Cybermatics_2018.2018.00250

[13] Jolocom. 2019. A Decentralized, Open Source Solution for Digital Identity and Access Management. *Whitepaper 2.1* (2019).

[14] NV Kulabukhova. 2019. Zero-knowledge proof in self-sovereign identity. In *Proceedings of the 27th International Symposium Nuclear Electronics and Computing (NEC'2019)*. 381–385.

[15] David Liau, Razieh Nokhbeh Zaeem, and K Suzanne Barber. 2019. Evaluation Framework for Future Privacy Protection Systems: A Dynamic Identity Ecosystem Approach. In *2019 17th International Conference on Privacy, Security and Trust (PST)*. IEEE, 1–3.

[16] David Liau, Razieh Nokhbeh Zaeem, and K Suzanne Barber. 2020. A Survival Game Analysis to Personal Identity Protection Strategies. In *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE, 209–217.

[17] Zoltán András Lux, Dirk Thatmann, Sebastian Zickau, and Felix Beierle. 2020. Distributed-Ledger-based Authentication with Decentralized Identifiers and Verifiable Credentials. In *2020 2nd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS)*. 71–78. https://doi.org/10.1109/BRAINS49436.2020.9223292

[18] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. 2018. A survey on essential components of a self-sovereign identity. *Computer Science Review* 30 (2018), 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

[19] Nitin Naik and Paul Jenkins. 2020. uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain. In *2020 IEEE International Symposium on Systems Engineering (ISSE)*. 1–7. https://doi.org/10.1109/ISSE49799.2020.9272223

[20] Razieh Nokhbeh Zaeem, Suratna Budalakoti, K Suzanne Barber, Muhibur Rasheed, and Chandrajit Bajaj. 2016. Predicting and explaining identity risk, exposure and cost using the ecosystem of identity attributes. In *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*. IEEE, 1–8.

[21] Rima Rana, Razieh Nokhbeh Zaeem, and K Suzanne Barber. 2018. US-Centric vs. International Personally Identifiable Information: A Comparison Using the UT CID Identity Ecosystem. In *2018 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 1–5.

[22] Drummond Reed, Jason Law, and Daniel Hardman. 2016. The technical foundations of sovrin. *The Technical Foundations of Sovrin* (2016).

[23] Drummond Reed, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, and Markus Sabadello. 2021. *Decentralized Identifiers (DIDs) v1.0.* Technical Report.

[24] Mannu Sporny, Dave Longley, and David Chadwick. 2019. *Verifiable Credentials Data Model 1.0.* Technical Report.

[25] Razieh Nokhbeh Zaeem and K Suzanne Barber. 2020. How Much Identity Management with Blockchain Would Have Saved Us? A Longitudinal Study of Identity Theft. In *International Conference on Business Information Systems*. Springer, 158–168.

[26] Razieh Nokhbeh Zaeem, Monisha Manoharan, and K Suzanne Barber. 2016. Risk kit: Highlighting vulnerable identity assets for specific age groups. In *2016 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, 32–38.

[27] Razieh Nokhbeh Zaeem, Monisha Manoharan, Yongpeng Yang, and K Suzanne Barber. 2017. Modeling and analysis of identity threat behaviors through text mining of identity theft stories. *Computers & Security* 65 (2017), 50–63.

[28] Jim Zaiss, Razieh Nokhbeh Zaeem, and K. Suzanne Barber. 2019. Identity Threat Assessment and Prediction. *Journal of Consumer Affairs* 53, 1 (2019), 58–70. https://doi.org/10.1111/joca.12191 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1111/joca.12191

[29] Jim Zaiss, Razieh Nokhbeh Zaeem, and K Suzanne Barber. 2019. Identity threat assessment and prediction. *Journal of Consumer Affairs* 53, 1 (2019), 58–70.

WWW.IDENTITY.UTEXAS.EDU