PrivySharing: A Blockchain-based Framework for Integrity and Privacy-preserving Data Sharing in Smart Cities

Imran Makhdoom[1][a], Ian Zhou[1][b], Mehran Abolhasan[1][c], Justin Lipman[1][d] and Wei Ni[2][e]
[1]*University of Technology Sydney, New South Wales, Australia*
[2]*Data61-CSIRO, Marsfield, New South Wales, Australia*

Keywords: Internet of Things, Smart City, Security and Privacy, Blockchain, EU GDPR Compliance.

Abstract: The ubiquitous use of Internet of Things (IoT) ranges from industrial control systems to e-Health, e-commerce, smart cities, supply chain management, smart cars, cyber-physical systems and a lot more. However, the data collected and processed by IoT systems especially the ones with centralized control are vulnerable to availability, integrity, and privacy threats. Hence, we present "PrivySharing," a blockchain-based innovative framework for integrity and privacy-preserving IoT data sharing in a smart city environment. The proposed scheme is distinct from existing technologies on many aspects. The data privacy is preserved by dividing the blockchain network into various channels, where every channel processes a specific type of data such as health, smart car, smart energy or financial data. Moreover, access to user data within a channel is controlled by embedding access control rules in the smart contracts. In addition, users' data within a channel is further isolated and secured by using private data collection. Likewise, the REST API that enables clients to interact with the blockchain network has dual security in the form of an API Key and OAuth 2.0. The proposed solution also conforms to some of the significant requirements outlined in the European Union General Data Protection Regulation. Lastly, we present a system of reward in the form of a digital token "PrivyCoin" for the users for sharing their data with the stakeholders/third parties.

1 INTRODUCTION

IoT-based services are expected to connect 30 billion devices by 2020 (Lund et al., 2014). Use of IoT technologies will not only improve the quality of life of people but also contribute to the world economy. However, at the same time global urban population is also predicted to reach 5 billion by 2030. This rapid urbanization demands effective, and optimum use of city resources as well as smart governance and efficient service delivery (Moustaka et al., 2018; Zhang et al., 2017). It is believed that the solution to the rapid urbanization problems lies in creating smart cities that utilize IoT technologies to monitor the physical world in real-time and provide intelligent services. These services may include eToll, smart parking (Zhang et al., 2017), smart health, and police assistance (Moustaka et al., 2018).

Concurrently, IoT devices are vulnerable to a vast number of security and privacy attacks (Makhdoom et al., 2018). Although, these threats are known to the manufacturers but security in IoT devices is either neglected or treated as an afterthought (Wurm et al., 2016). Sequel to this, a smart city network also suffers from numerous security and privacy issues (Moustaka et al., 2018; Bartoli et al., 2011), such as threats to privacy, integrity, and availability of user data, false data injection (Zhang et al., 2017), vulnerability to Sybil Attack (Cui et al., 2018), and single point of failure due to centralized control.

If we look at Figure-1, the user data collected by numerous sensors is stored and processed by various OSN (Online Social Networks), smart city control centre or various other smart city components such as Intelligent Transportation Systems (ITS), health emergency response, fire and rescue etc., These components with mostly centralized control process user data for provision of various services to the users and third parties. Although such a centralized control may look effective from the outside, yet it has some signif-

[a] https://orcid.org/ 0000-0002-6205-5897
[b] https://orcid.org/0000-0002-7154-4561
[c] https://orcid.org/0000-0002-4282-6666
[d] https://orcid.org/0000-0003-2877-1168
[e] https://orcid.org/0000-0002-4933-594X

Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J. and Ni, W.
PrivySharing: A Blockchain-based Framework for Integrity and Privacy-preserving Data Sharing in Smart Cities.
DOI: 10.5220/0007829803630371
In *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (ICETE 2019)*, pages 363-371
ISBN: 978-989-758-378-0

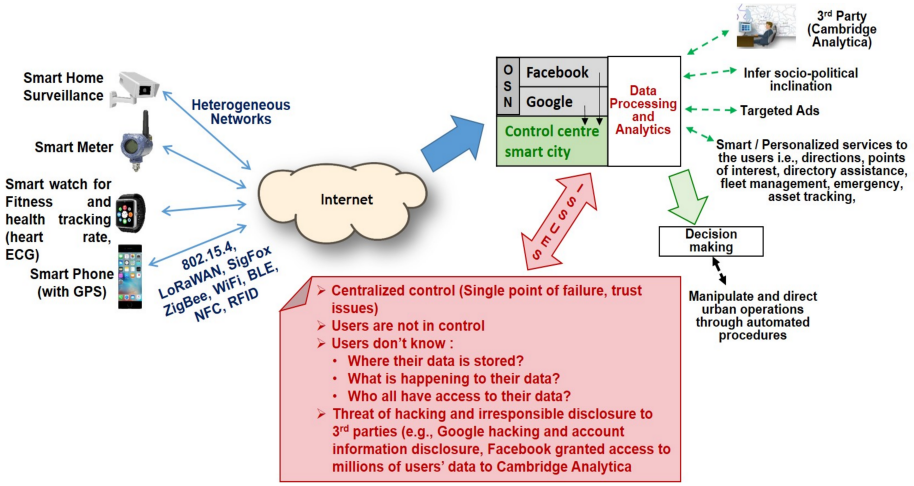

Figure 1: Issues in the smart city environment.

icant security concerns.

Centralized control is subject to a single point of failure in case of a cyber-attack or other technical malfunctions (Puthal et al., 2016). Moreover, it also has trust issues, as the users have to put their trust in the entity that is handling their data. Hence, users have no control over their data assets. Further concerns for user data include: Users do not know where their data is stored? Who has access to it? Is their any unauthorized disclosure to the third parties? These concerns are very realistic as the disclosure of personal data leakage concerning 87 million users by Facebook Inc. in April 2018 (Sara and Michael, 2018) and a bug in Google Plus (Sara, 2018) that resulted in the exposure of personal information of approx 500,000 users is a candid example of one of cloud/OSN vulnerabilities.

Moreover, any smart city application is believed to store, process and analyze users' data. Hence, every security solution developed for a smart city environment must comply with the undermentioned key requirements of European Union General Data Protection Regulation (EU GDPR) (GDPR, 2018) while handling users' data:

- Personal data should be gathered and processed only with the consent of the data owner based on a contract.
- Any technology dependent on user data must preserve user privacy by design.
- The owner of data has the right to know, as to who has access to his data?
- User data be erased immediately once it is no longer required.
- The system should be transparent and must log all the activities concerning user data.

As far as IoT security is concerned, though blockchain was initially conceived as a financial transaction (TX) protocol in the form of Bitcoin, but due to its cryptographic security benefits, researchers and security analysts are focusing on the blockchain to resolve security and privacy issues of IoT. Hence, we believe that a carefully selected blockchain technology with an insightful business network design can resolve most of the data integrity and privacy issues of a smart city.

1.1 Related Work

Security researchers around the world are developing and investigating ingenious ways to implement blockchain in the IoT environment. These use cases aim to take advantage of the inherent benefits of the blockchain such as decentralized control, immutability, cryptographic security, fault tolerance, and capability to run smart contracts. Recently, researchers (Michelin et al., 2018) presented a blockchain-based data sharing framework for a smart city environment. The framework called "SpeedyChain" focuses on reducing the TX settlement time for real-time applications such as smart cars and also aims to ensure user privacy. Moreover, it ensures data integrity, tamper-resistance, and non-repudiation that are some of the intrinsic benefits of the blockchain. In another work, Pradip Kumar and Jong Hyuk proposed a Software Defined Networking (SDN) and blockchain-based hybrid network architecture for a smart city (Sharma and Park, 2018). The proposed architecture addresses usual smart city issues including high TX latency, security and privacy, bandwidth bottlenecks, and requirement of high computational resources. Authors claim that the proposed model limits the effects of

node compromise to the local area.

Additionally, researchers (Rahman et al., 2019) proposed smart contract based sharing economy services in a smart city. The proposed model uses Artificial Intelligence (AI) for data analytics and uses blockchain to store the results. Similarly, Biswas and Muthukkumarasamy (Biswas and Muthukkumarasamy, 2016) presented an overview of a blockchain-based security framework for secure communication between smart city entities. However, it is not clear that which blockchain platform, and consensus protocol is used in the smart city application?

In another endeavor (Kountché et al., 2017; Haidar et al., 2017), security researchers have proposed solutions to address various user privacy issues in ITS. Nonetheless, they do not cater for the challenges of the smart cities such as trustless data sharing among multiple organizations. Similarly, Ali Dorri and Raja Jurdak proposed a secure, private and lightweight architecture of a blockchain-based smart home application (Dorri et al., 2016; Dorri et al., 2017). It aims to solve certain blockchain issues such as computational intensiveness, latency in TX confirmation and energy consumption. However, there are many security concerns that need further explanation (Makhdoom et al., 2018b). Likewise, authors (Buterin et al., 2014) proposed an Ethereum Blockchain based mechanism to manage IoT devices (Huh et al., 2017). Nevertheless, Ethereum Blockchain does not provide data privacy. Correspondingly, Yu Zhang and Jiangtao Wen proposed an Ethereum Blockchain based decentralized electronic business model for the IoT (Zhang and Wen, 2016). Whereas, the proposed solution mostly focused on the working of the e-business model, and thus lacking technical aspects.

Though the research work discussed above has certainly made some significant contributions towards blockchain and IoT domain. However, still, there are many open issues such as preserving data privacy in a smart city environment, user-defined fine-grained access control, fast TX settlement, users' right to forget (concerning data deletion), an incentive for users to share their data, etc. Therefore, to fill the respective research gaps, we propose "PrivySharing," a blockchain-based secure and privacy-preserving framework. The experimental results have shown that a carefully designed blockchain solution can ensure user data privacy and integrity in various network settings as per the wishes of the data owner. It also effectively protects against false data injection and Sybil Attacks. Moreover, PrivySharing complies with some of the significant data security and privacy requirements of the European Union General Data Protection Regulation (EU GDPR). The major contributions of this paper are:

1. Protection against most of the smart city threats concerning user data integrity and privacy.
2. Compliance with some of the essential requirements of EU GDPR.
3. A blockchain-based solution providing the "right to forget" concerning user data.
4. A scalable (concerning blockchain size), secure and an efficient (in terms of energy consumption and computational requirements) data sharing framework.
5. User-defined fine-grained access control to his/her data.
6. Providing a transparent and auditable network operation and simultaneously preserving user data privacy.
7. Secure client access to the blockchain network through a REST API.
8. A reward system for the users for sharing their data with the stakeholders/third parties.

1.2 Organization of the Paper

The paper is organized into four sections. Section-2 presents the detailed architecture, working, reward mechanism and security analysis of "PrivySharing." Experimental results including Access Control List (ACL) rules and some limitations of the proposed solution are illustrated in Section-3. Finally, the paper is concluded in Section-4, with a gist of future work.

2 PRIVYSHARING: BLOCKCHAIN-BASED SECURE DATA SHARING

By leveraging data integrity and smart contract features of the blockchain, various operations in a smart city environment can be securely and autonomously performed. Moreover, blockchain also protects against the adverse effects of server hacking and falsification/modification of permissions (Cui et al., 2018). No doubt, people in a smart city environment feel safe when they have the assurance that their personal and sensitive data collected by various devices is fully protected and they have the control over it (Mazhelis et al., 2016). Such assurance can only be provided by none other than the blockchain technology.

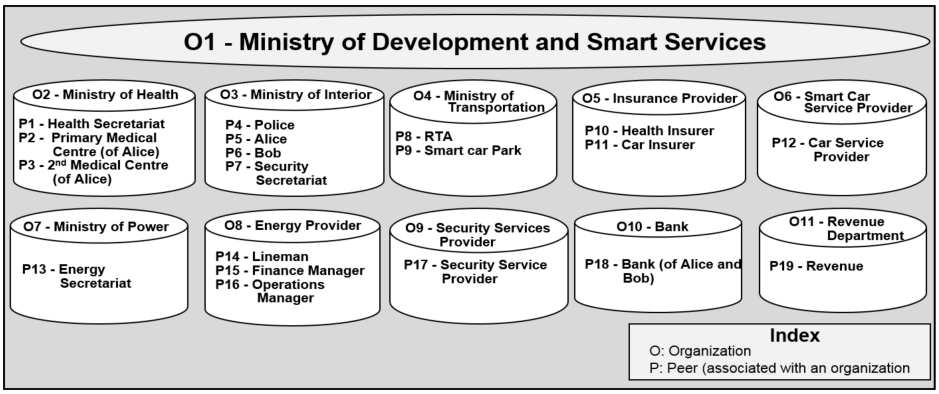

Figure 2: Network participants.

Table 1: List of assets.

Data Types	Assets
Health Data	Health Alert (Heart rate, blood sugar, blood alcohol etc.) Full Health History Insurance Cover Health Payment Claims Type of Disease Current Disease History
Smart Car Data	GPS Data Accident Alert Damage Assessment Servicing and Auto Payments
Smart Meter Data	Line Status Units Consumed and Bill Consumption Pattern
Surveillance Data	Equipment Status and Servicing Security Breach Alert CCTV Recording
Financial Transactions	Income Expenses Tax

2.1 Smart City Scenario

Let's assume that Alice is living in a smart city where every aspect of her life is being monitored and controlled through numerous sensors and smart devices. The critical aspects include personal health, smart living, smart car, performance of security apparatus, and financial TXs to keep the services running. For better understanding, we have formulated a list of numerous assets (associated with a specific type of data) that Alice owns (as shown in Table-1). Based on these assets, Alice can easily decide as to which stakeholder/third-party needs access to which asset? and what operation he can perform on that asset? Such a distinction among the stakeholders/third-parties further assists Alice to plan and control the access to her data.

To implement above mentioned smart city use case we have used Hyperledger-Fabric (Androulaki et al., 2018) as the underlying blockchain platform due to its effective data security and privacy preserving capabilities as compared to other blockchain platforms (Makhdoom et al., 2018a; Makhdoom et al., 2018b). The key feature that distinguishes Hyperledger-Fabric from other blockchain technologies is that the blockchain ledger consists of two distinct but related parts, i.e., a blockchain to log the TXs and a world state (a database such as CouchDB, and LevelDB) to keep track of the ledger states.

2.2 Basic Terminologies

Some terminologies specific to Hyperledger-Fabric are:

- **Committing Peers.** Every peer node in the Hyperledger-Fabric blockchain is a committing peer. However, a Committing Peer does not have a smart contract installed. It just validates and commits a new block of TXs sent by the Ordering Service to its copy of the ledger.
- **Endorsing Peers.** These are special committing peers with the capability to run the smart contracts. They prepare, sign and endorse the responses to the TX proposals sent by the clients, in line with the endorsement policy of the respective channel (Ch).
- **Ordering Service.** It is a collection of some peer nodes that arrange the new TXs in a block and then broadcast that block to all the peers of the concerned Ch.
- **Membership Service Provider (MSP).** On the one hand, Certificate Authorities (CAs) issue X.509 certificates to the network entities, while, on the other, an MSP states that which peer nodes are members of which organization. Different MSPs can be used to represent various organizations or multiple groups within an organization. Usually, the MSPs are defined at the network, Ch and local/peer level.

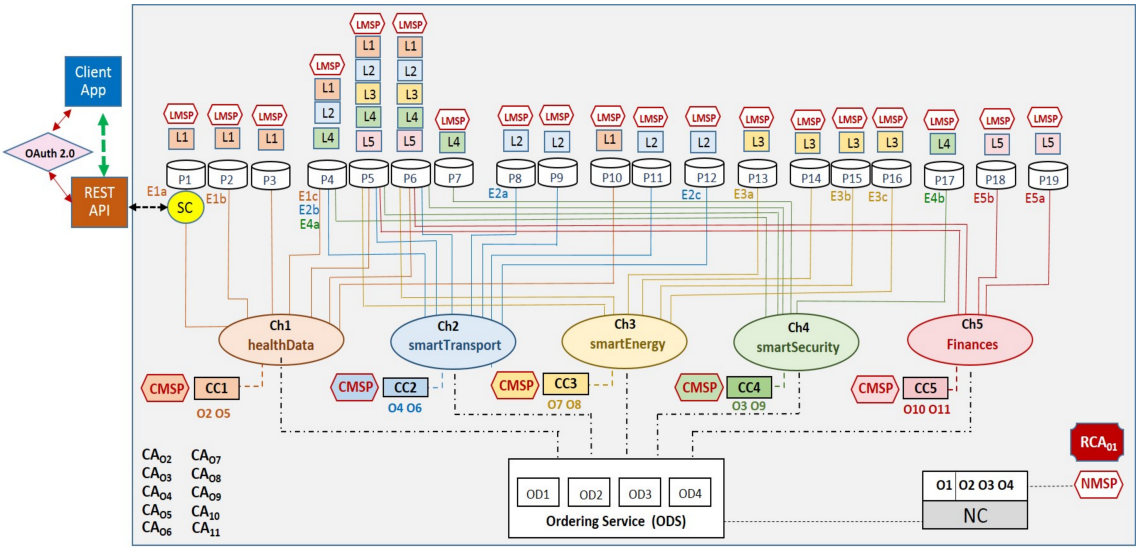

Figure 3: Smart city blockchain-network architecture.

2.3 Network Architecture

As shown in Figure-2, we have designed a smart city blockchain network comprising eleven organizations and their associated peer nodes. Keeping in view the sharing of different categories of users' data with different stakeholders and the requirement to ensure user data privacy and security, the blockchain network shown in Figure-3 comprises five different data Chs. Where, Ch1 is used for the sharing of users' health data, and similarly, Ch2 for smart transportation, Ch3 for smart energy, Ch4 for smart security and Ch5 handles financial data. Hence, these Chs serve to preserve the privacy of user data by securely sharing a particular type of data with authorized entities only. The network is initiated by organization-1 (O1), and is governed by the policy rules specified in the network configuration (NC). NC also controls access to the smart city network. Similarly, every Ch is regulated by the policy rules specified in the respective Channel Configuration (CC). In this setting, Ch1 is under the control of O2 and O5 and is governed by CC1. Correspondingly, Ch2 is regulated by CC2, and so on.

The CC is essential for Ch security, e.g., if the client application (clientApp) wants to access a SC on P1, then P1 consults its copy of CC1 to determine the operations that clientApp can perform. Moreover, there is a separate ledger for every Ch, and all the peer nodes have to maintain a copy of the ledger concerning every Ch they are member of. Data in a Ch is isolated from the rest of the network including other Chs. Another important aspect of smart city blockchain network is the ordering service (ODS), which is common to all the Chs. Each node in the ordering service keeps a record of every Ch created through NC. Regarding CAs, every organization in the network can have its own CA. But there is one Root CA (RCA) in the network to establish the root of trust. As a Proof of Concept (PoC) for PrivySharing, we are using Hyperledger-Fabric RCA to issue X.509 certificates to all the network entities. These certificates serve to authenticate the network entities and to digitally sign the client application TX proposals and smart contract TX responses. A user accesses the network through a clientApp with a specific X.509 ID, using a smart contract (SC). It is imperative to mention that only the endorsing peers can see the SC logic as they have to run the users' TX proposals to prepare the responses.

To ensure the privacy of critical user data within a Ch, we adopted a methodology of "Private Data Collection," in which the critical private data is sent directly to the authorized organizations/stakeholders only. This data is stored in a private database (a.k.a sideDB) on the authorized nodes, and only the hash of this data is processed, i.e., endorsed, ordered and written to the ledgers of every peer on the Ch. The hash of the data serves as an evidence of the TX, and it also helps in the validation of the world state. An important data security feature here is that the ordering nodes do not see the private data.

Another important feature of the proposed network architecture is the use of Membership Service Provider (MSP) at various levels such as network, Ch and local/peer. The network MSP (NMSP) defines the members of the network and their admin rights. Additionally, an NMSP also defines that which RCAs/CAs

are trusted. On the other hand, the Ch MSPs (CMSP) outline admin and participatory rights at the Ch level. A use case for the CMSP is that, e.g., an admin of an organization wants to instantiate a SC on Ch1, then by looking at the CMSP the other Ch members can verify that whether that admin is a part of a specific organization or not and whether he is authorized to instantiate the SC on Ch1 or not.

Similarly, a local MSP (LMSP) is defined for every client-node/peer. The LMSP associates a peer with its organization. Here a question may arise that, what is the difference between CC and a CMSP? A CC contains the policies that govern that Ch, i.e., which all organizations regulate that Ch? Who can add new members to the Ch? Whereas, a CMSP establishes the linkage between the nodes and their respective organizations.

Another question may arise that what advantages do we get by using multiple Chs for different data types? There are two aspects to this selection; one is scalability and second is increased privacy of user data. From the scalability point of view, if there is only one Ch for all data types, then it means that all the users will have to store the ledger comprising all TXs that are not even related to them. Hence, the ledger size will be increasing rapidly thus putting more strain on storage resources of all the users/peers. Whereas, in the case of "PrivySharing," the users will maintain a ledger that stores only that data which concerns all the users of that particular Ch. As far as the privacy of user data is concerned, a data specific Ch shared only by some of the stakeholders provides more privacy than a single Ch comprising all the stakeholders sharing multiple data types.

2.4 Reward Mechanism

PrivySharing incentivizes the users to share their data with other users, stakeholders or third parties by rewarding them with a local digital token named "PrivyCoin." The users get the incentive based on the number of days their data is shared with the stakeholders/third parties, as soon as the TX for data sharing is committed. In this context, if a stakeholder does not have requisite coins in their account, the TX will fail (shown in Figure-4). The coins are issued to the users and the stakeholders by the network admin only.

2.5 Security Analysis

The security, being the core objective of this work has been assessed at every level of the network operation. The key aspects are as under:

When the blockchain network is first created, all

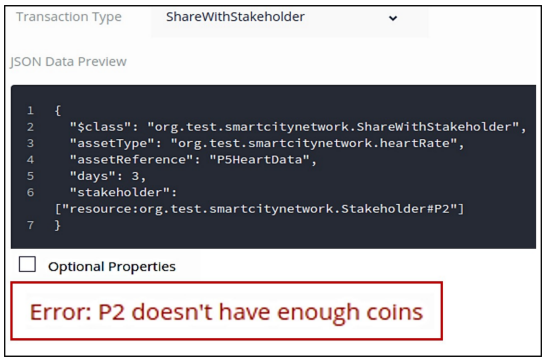

Figure 4: Error for not having enough coins.

the peers and orderer organizations are issued with certificates from respective RCA, or other trusted CAs. Then, a connection profile is created for all the network entities including Chs, ODS, organizations, peers, and CAs. The connection profile defines the complete blockchain network setup. The key point here is that no other peer (with the intention of endorsing the TXs on a Ch) can join the network if it is not defined in the connection profile. It is clarified that by peers, we mean committing, endorsing or ODS peer nodes that maintain the blockchain network. Whereas, the users/clients access the blockchain network through REST API or clientApps.

To deploy the business network model (PrivySharing in this case) comprising asset definitions, TX logic, and ACL rules, on the blockchain, the admin of responsible organization (O1 in this scenario) requires a Business Network Card (BNC). BNC is created using the connection profile of the organization and the valid public and private key for that admin issued by the authorized CA, as defined in the connection profile.

The TXs initiated by the clientApps on a specific Ch are endorsed as per the endorsement policy defined before the start of the business network. The endorsement policy may include, e.g., which all peers (with endorsing ability) are required to endorse a TX on a Ch concerning health data? Correspondingly, a TX is considered valid, only if the responses of all the required endorsing peers are same. Hence, only a valid TX will update the world state.

Another security feature is that before the start of the business network on the blockchain, business network admins have to be defined and issued with the certificates by the respective organizations with admin rights on a Ch. These certificates are later used to create the BNCs for the said admins to access the business network. Without a valid BNC, no one can add participants (clients/peers) for an organization. Moreover, every new client/peer added under an or-

Figure 5: Validation of assets access control.

ganization is also issued with an ID by the respective CA with the approval of the business network admin. These IDs are further used to control access to the users' profile and assets as per the ACL rules defined for the specific Ch.

Access to the REST API is secured using the API key which is required to launch the REST API. In addition to the API Key, OAuth 2.0 authorization protocol is also deployed to authenticate the users/stakeholders, authorize access to the REST server instance, and allow the stakeholders/users to interact with the business network deployed on the blockchain. Furthermore, due to the distributed nature of the smart contracts, the integrity of any business network deployed on the blockchain is guaranteed. Similarly, it also protects against hacking of servers, where, the attackers can change the policy rules, escalate access rights, etc. Correspondingly, protection against application and web vulnerabilities can also be guaranteed with high probability, as any change in the smart contract requires installing and instantiating a new version of the contract on all the endorsing peers. However, it can not be done discretely. Additionally, due to a distinction between blockchain and the world state, an auditable log of TXs and events is maintained without compromising the privacy of the users' data.

Considering decentralization aspect, the use of a dedicated trusted CA, a blockchain admin, and a business network admin by every organization in the blockchain network, provides some degree of decentralization as compared to all the admin rights resting with a single organization.

3 EXPERIMENTAL RESULTS

To validate the security effectiveness of the proposed solution, we developed a business network model of health data sharing in a smart city environment (PrivySharing), i.e., the operation of Ch1 (as shown in Figure-3), in Hyperledger Composer-Playground version 0.20. As a PoC, we deployed the business network architecture of PrivySharing on Hyperledger Fabric ver 1.2 with one Ch, four committing peers with endorsing powers and two ordering nodes. We have used CouchDB as a world state because of its support for rich queries. It is also validated that access to users' health data assets is effectively regulated by numerous ACL rules.

3.1 ACL Rules

These rules enforce that the data asset owners have access to their assets only, i.e., no user can see data assets of any other user, and only the data owners can initiate a TX to share their data assets with other users/stakeholders. Similarly, the data owner has the right to revoke the sharing of his assets, and he can also delete his assets when no longer required without affecting the TX history stored on the blockchain. Moreover, as all the TXs are recorded on the blockchain, hence, to increase privacy, a data owner can see the TX history concerning his own assets only. Additionally, the valid users can read and update their own profiles only, and other users/stakeholders cannot see each other's profile. Users can also delegate the stakeholders to create assets for the respective users. E.g., Alice (P5) delegates

her primary medical centre (P2) to create a health data asset for her. Accordingly, the stakeholders can only see the data assets that are shared with them or created by them. Lastly, all the users/stakeholders can view their coins only.

The validity of the ACL rules was checked on both, the Hyperledger Composer-Playground and the REST API. E.g., As shown in Figure-5a and Figure-5b, to compare the access rights we have created a user with admin rights that can view assets of all the users (blood alcohol level), i.e., P5 and P6 in this case. Whereas, the user P5 with ID Pid5 can see his assets only. Moreover, Figure-5c and Figure-5d show that initially, a user P4 with id Pid4 cannot see any asset, as no asset is currently shared with him. However, once user P5 shares his blood alcohol level with P4, he can see P5's blood alcohol level. Similarly, only P5 can initiate a TX to share its assets. Whereas, if P4 tries to share the asset of P5 with any other entity then he will get an error (as shown in Figure-6) as he currently does not have the right to initiate a data sharing TX.

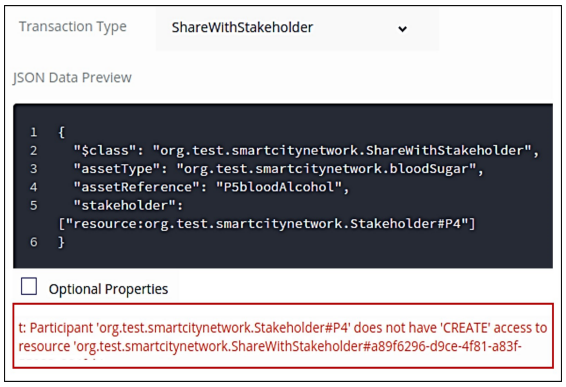

Figure 6: Validation of TX initiation rights.

3.2 Performance Efficiency

As far as the performance efficiency matters, the use of multiple Chs to process different data types instead of a single Ch facilitates simultaneous TX processing, thus resulting in reduced network latency. Similarly, Hyperledger-Fabric provides instant TX confirmation with varying throughput ranging from 1838 to 3560 TXs per second (Androulaki et al., 2018). The TX throughput depends upon number of factors, such as, block size, TX size, peer CPU, and number of peers in the network. Moreover, Hyperledger-Fabric uses Kafka consensus algorithm which is a voting-based protocol, that provides consensus finality without any risk of forks (Hyperledger, 2019). In addition, it has very low computational and energy requirements as compared to the PoW-based consensus protocols.

3.3 Limitations and Open Challenges

- **Multiple Ledger Storage by the Peers.** The committing peers have to maintain multiple ledgers, as per the number of channels they are a member of. This can infer a massive resource requirement for such nodes in a large smart city network.
- **IoT Device Integrity.** IoT data, being the basic element to provide various seamless services in a smart city environment necessitates that the device initially generating and processing that data should be credible, i.e., only a legitimate and clean device should be able to input data to the blockchain. Whereas, currently there is no such mechanism to test the integrity of the IoT devices at run time.

4 CONCLUSIONS AND FUTURE WORK

User data generated by today's smart devices ranging from smart watches to smart cars, smart homes, auto-pay systems, ITS, etc., is vulnerable to privacy and security threats. Moreover, users also reserve the right to manage and control access to the data they own. Therefore, in this paper, we introduced "PrivySharing,", an innovative blockchain-based integrity and privacy-preserving data sharing mechanism for smart cities. The proposed strategy ensures that personal/critical user data is kept confidential, securely processed and is exposed to the stakeholders on the need to know basis as per user-defined ACL rules embedded in the smart-contracts. Moreover, the data owners are rewarded for sharing their data with the stakeholders/third parties. PrivySharing also complies with some of the significant EU GDPR requirements.

Though we have presented all the details of the proposed network architecture and security mechanism, however, as a PoC for this paper, we implemented a part of it. In the future, we aim to extend this work and incorporate the concept of edge computing to relieve end nodes from storing multiple ledgers. We also plan to devise a mechanism for secure integration of IoT devices with the blockchain.

REFERENCES

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A. D., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolic, M., Cocco, S. W., and Yellick, J. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. *CoRR*, abs/1801.10228.

Bartoli, A., Hernández-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., and Barthel, D. (2011). Security and privacy in your smart city. In *Proceedings of the Barcelona smart cities congress*, volume 292.

Biswas, K. and Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. In *Proceedings of the 14th IEEE International Conference on Smart City High Performance Computing and Communications*, pages 1392–1393.

Buterin, V. et al. (2014). A next-generation smart contract and decentralized application platform. *Whitepaper*.

Cui, L., Xie, G., Qu, Y., Gao, L., and Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. *IEEE Access*, 6:46134–46145.

Dorri, A., Kanhere, S., Jurdak, R., and Gauravaram, P. (2017). Blockchain for iot security and privacy: The case study of a smart home. In *Proceedings of the 2nd IEEE Workshop on Security, Privacy, and Trust in the Internet of Things (PERCOM), Hawaii, USA*.

Dorri, A., Kanhere, S. S., and Jurdak, R. (2016). Blockchain in internet of things: Challenges and solutions. *arXiv preprint arXiv:1608.05187*.

GDPR (2018). General data protection regulation. Available at https://gdpr-info.eu/, Viewed 03 January 2019.

Haidar, F., Kaiser, A., and Lonc, B. (2017). On the performance evaluation of vehicular pki protocol for v2x communications security. In *Proceedings of the 86th IEEE Vehicular Technology Conference (VTC-Fall)*, pages 1–5.

Huh, S., Cho, S., and Kim, S. (2017). Managing iot devices using blockchain platform. In *Proceedings of the 19th International Conference on Advanced Communication Technology (ICACT)*, pages 464–467. IEEE.

Hyperledger (2019). Hyperledger architecture, volume 1. Available at https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf, Viewed 21 February 2019.

Kountché, D. A., Bonnin, J.-M., and Labiod, H. (2017). The problem of privacy in cooperative intelligent transportation systems (c-its). In *Proceedings of IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 482–486.

Lund, D., MacGillivray, C., Turner, V., and Morales, M. (2014). Worldwide and regional Internet of Things (IoT) 2014–2020 forecast: A virtuous circle of proven value and demand. *International Data Corporation (IDC), Tech. Rep*.

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., and Ni, W. (2018). Anatomy of threats to the internet of things. *IEEE Communications Surveys Tutorials*.

Makhdoom, I., Abolhasan, M., and Ni, W. (2018a). Blockchain for iot: The challenges and a way forward. In *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications - Volume 2: SECRYPT*, pages 428–439. INSTICC, SciTePress.

Makhdoom, I., Abolhasan, M., and Ni, W. (2018b). Blockchain's adoption in iot: The challenges, and a way forward. *Journal of Network and Computer Applications*, 125:251 – 279.

Mazhelis, O., Hämäläinen, A., Asp, T., and Tyrväinen, P. (2016). Towards enabling privacy preserving smart city apps. In *International Smart Cities Conference (ISC2)*, pages 1–7. IEEE.

Michelin, R. A., Dorri, A., Steger, M., Lunardi, R. C., Kanhere, S. S., Jurdak, R., and Zorzo, A. F. (2018). Speedychain: A framework for decoupling data from blockchain for smart cities. In *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pages 145–154. ACM.

Moustaka, V., Theodosiou, Z., Vakali, A., and Kounoudes, A. (2018). Smart cities at risk!: Privacy and security borderlines from social networking in cities. *Athena*, 357:905–910.

Puthal, D., Nepal, S., Ranjan, R., and Chen, J. (2016). Threats to networking cloud and edge datacenters in the internet of things. *IEEE Cloud Computing*, 3(3):64–71.

Rahman, M. A., Rashid, M. M., Hossain, M. S., Hassanain, E., Alhamid, M. F., and Guizani, M. (2019). Blockchain and iot-based cognitive edge framework for sharing economy services in a smart city. *IEEE Access*, 7:18611–18621.

Sara, S. (2018). A Google bug exposed the information of up to 500,000 users. Available at https://www.cnbc.com/2018/10/08/google-bug-exposed-the-information-of-up-to-500000-users.html, Viewed 15 February 2018.

Sara, S. and Michael, N. (2018). Facebook has been worried about data leaks like this since it went public in 2012. Available at https://www.cnbc.com/2018/04/12/facebook-warned-of-data-breaches-years-ago-when-it-went-public-in-2012.html, Viewed 15 February 2018.

Sharma, P. K. and Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems*, 86:650–655.

Wurm, J., Hoang, K., Arias, O., Sadeghi, A.-R., and Jin, Y. (2016). Security analysis on consumer and industrial iot devices. In *Proceedings of the 21st IEEE Asia and South Pacific Design Automation Conference (ASP-DAC)*, pages 519–524.

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., and Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. *IEEE Communications Magazine*, 55(1):122–129.

Zhang, Y. and Wen, J. (2016). The iot electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications*, pages 1–12.