IoT Passport: A Blockchain-Based Trust Framework for Collaborative Internet-of-Things

Bo Tang
Information Security Laboratory,
Sichuan Changhong Electric Co., Ltd.
bo.tang@changhong.com

Hongjuan Kang
Information Security Laboratory,
Sichuan Changhong Electric Co., Ltd.
hongjuan.kang@changhong.com

Jingwen Fan
Information Security Laboratory,
Sichuan Changhong Electric Co., Ltd.
jingwen.fan@changhong.com

Qi Li
Institute for Network Sciences and
Cyberspace, Tsinghua University
BNRist, Tsinghua University
qli01@tsinghua.edu.cn

Ravi Sandhu
Institute for Cyber Security and
Department of Computer Science,
University of Texas at San Antonio
ravi.sandhu@utsa.edu

ABSTRACT

Internet-of-Things (IoT) is a rapidly-growing transformative expansion of the Internet with increasing influence on our daily life. Since the number of "things" is expected to soon surpass human population, control and automation of IoT devices has received considerable attention from academia and industry. Cross-platform collaboration is highly desirable for better user experience due to fragmentation of user needs and vendor products with time. Centralized approaches have been used to build federated trust among platforms and devices, but limit diversity and scalability. We propose a decentralized trust framework, called IoT Passport, for cross-platform collaborations using blockchain technology. IoT Passport is motivated by the familiar use of passports for international travel but with greater dynamism. It enables platforms to establish arbitrary trust relations with each other containing specific rules for intended collaborations, enforced by a combination of smart contracts. Each interaction among devices is signed by the participants and recorded on the blockchain. The records are utilized as attributes for authorization and as proofs of incentive plans. This approach incorporates the preferences of participating platforms and end users, and opens new avenues for collaborative edge computing as well as research on blockchain-based access control mechanism for IoT environments.

CCS CONCEPTS

• **Security and privacy** → **Trust frameworks**; **Access control**; *Distributed systems security*; • **Human-centered computing** → *Ubiquitous computing*.

KEYWORDS

Internet of Things, Blockchain, Trust Framework, Access Control

SACMAT '19, June 3–6, 2019, Toronto, ON, Canada

ACM ISBN 978-1-4503-6753-0/19/06…$15.00
https://doi.org/10.1145/3322431.3326327

ACM Reference Format:
Bo Tang, Hongjuan Kang, Jingwen Fan, Qi Li, and Ravi Sandhu. 2019. IoT Passport: A Blockchain-Based Trust Framework for Collaborative Internet-of-Things. In *The 24th ACM Symposium on Access Control Models and Technologies (SACMAT '19), June 3–6, 2019, Toronto, ON, Canada.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3322431.3326327

1 INTRODUCTION

IoT connected devices are expected to exceed 25 billion globally by 2025 [25], when the human population is projected to be around 8 billion. Thereby every individual will own or engage with over a dozen IoT devices on average. With so many devices around us, how to control and beneficially use them becomes a major problem for technologists and end consumers.

This explosive growth notwithstanding, the smart life scenarios still remain a vision rather than reality. Consider that while 9 billion Micro-programmed Control Units are currently produced and installed in IoT devices annually, few are actually connected [12]. Clearly, at present, the value proposition of connecting these devices is not so compelling as one might imagine.

Since the requirements for connected devices are diverse and rapidly evolving, the IoT world has become fragmented and decentralized. All the same, centralized methods, including access control mechanisms, inherited from the traditional Internet are still used to manage and operate IoT devices. Clearly, the familiar Internet of Computers is much more homogeneous than IoT with respect to hardware, software and protocols. In order to connect the fragmented IoT devices, cross-platform collaborations become desirable and challenging. This fragmentation is holding back use of the connectivity features of IoT devices thereby limiting the potential benefit. We believe, this situation is transitional and eventually decentralized mechanisms will dominate in IoT. Blockchains have potential to be a foundation for such decentralization.

Access control mechanisms for IoT have been extensively studied [1, 2, 4–6, 16, 35–37], primarily in context of a single IoT platform. Some recent works have explored the combination of blockchain technology and IoT [19, 23, 26]. Since IoT requires multiple parties, such as manufacturers, operating platforms and users, to maintain collaborative trust with each other, blockchains have potential to build effective trust frameworks for IoT. However, an overall consensus framework for this purpose remains to be developed.

In this paper, we propose a decentralized trust framework, called IoT Passport, for collaborative IoT based on blockchain technology. A primary objective is to enable cross-platform collaboration, which is commonly required in most commodity user scenarios. The trust framework comprises blockchain-based authentication, authorization and trust as its cornerstones. It adapts the familiar concept of the modern passport, which has been successfully used for international travel for almost a century [21]. An IoT Passport is issued to each device by its operating platform under common rules enforced by smart contracts. Additional rules between platforms, including details about how collaboration should happen, which attributes should be used for authorization and how rewards should be given to incentivize participants, etc., are agreed upon and programmed in smart contracts so that the execution can be dynamically and precisely enforced during every collaborative transaction. In order to maintain a sustainable ecosystem among participating platforms, the credit management system of IoT devices and incentive management system for collaborative transactions are included. Last but not least, the data security and privacy module utilizes smart contracts and appropriate cryptography to prevent user data abuse.

The rest of this paper is divided into five sections. Section 2 discusses the background and related work, including the typical user scenario of IoT collaboration in people's daily lives, existing solutions in both industry and academia and challenges in building a trust framework for cross-platform collaborations in IoT. Section 3 analyzes the cross-platform collaboration requirements of IoT, compares the centralized and decentralized models and describes the design goals. The proposed decentralized trust framework in Section 4 consists of the design overview, the key components of the framework and their applicability in the user scenario case studies. The potential continuing research directions are presented in Section 5, followed by the conclusion in Section 6.

2 BACKGROUND AND RELATED WORK

The key problem of collaborative IoT is rooted in the trust of behaviors among connected devices and their operating platforms. To illustrate these problems, a typical real-life user scenario is presented in this section, along with an analysis of the literature to identify the gaps between the existing solutions and open issues.

2.1 Background

IoT expands from connections among people in social networks to connections among people and things [33]. Along with the development of faster wireless technologies, such as 5G [22, 27, 32], IoT is expected to be increasingly popular and convenient in people's life. It is reported that the world passed the barrier of a single connected object per person in 2008 [8] which is projected to grow to around 26 smart objects per human by 2020. IoT devices are increasingly automated with advances in artificial intelligence (AI). Numerous industry sectors are now coupled with the adjectives "smart" such as smart health, smart energy and smart cars.

The term smart life serves in this paper as a collection of user scenarios to exemplify the concept of collaborative IoT across smart devices around people, as shown in Figure 1. Currently, various types of smart devices are designed to meet people's needs through predefined collaboration protocols. With the growth of home appliance automation, many homeowners deploy cloud-connected devices. A recent study predicts home automation revenue of over $100 billion by 2020 [18] drawing even more vendors into this area.

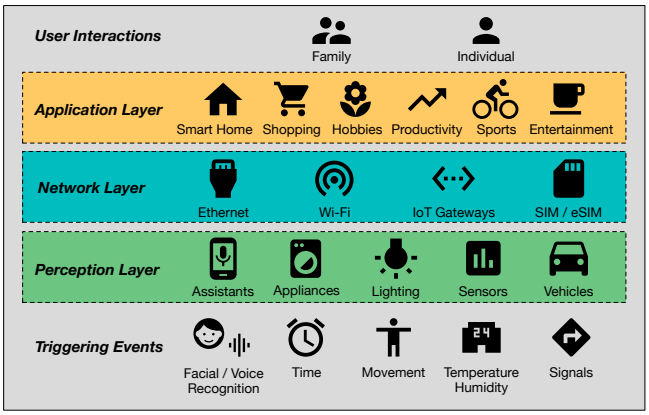


Figure 1: Smart Life Scenarios

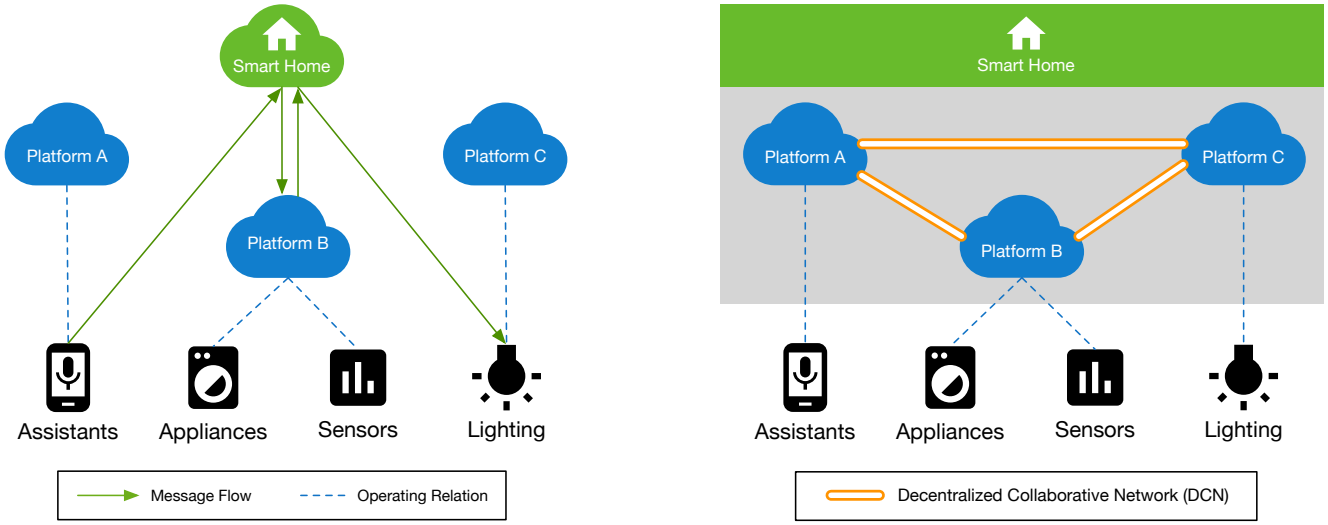
Typical smart-life scenarios are explained in Figure 1 from the perspective of layered IoT architecture. The Perception Layer, next to the bottom, consists of IoT devices including smart phones, smart home appliances and smart cars, etc., which interact with the physical world via triggering events including user interactions, environmental conditions, time and other collaborative signals. The IoT devices are connected through various protocols, as shown in the Network Layer, to the Application Layer at the top, which gives common examples of numerous user-centred smart life scenarios.

Consider Alice, as a typical smart home user who enjoys IoT conveniences as follows.

S1. On the way home, Alice converses with the AI assistant on her smart phone to check her food inventory. The smart refrigerator responds with a list and suggestions on grocery shopping. Moreover, the AI assistant provides a one-click option for same-day delivery.

S2. The facial detectors at Alice's authenticate her on arrival and further detect her mood as currently blue, so yellow lights will turn on and soft sound tracks from her favorites will play.

We assume that users will choose home appliances from various brands to cope with diverse needs along time, and that this is an important requirement for IoT trust frameworks. In order to achieve the above scenarios in this context, collaboration commands among devices are received and issued by a unified cloud platform in a typical centralized solution of a smart home application, as shown in Figure 2a. There are two options in this solution. A device either directly connects to the application cloud platform (as shown in the figure) or indirectly through its operating platform. The former requires each device to maintain connectivity with at least two cloud platforms, the application one and the operating one. The connections multiply dramatically if there is more than one smart home application provider. The latter relieves the devices from overwhelming connections however the operating platforms have to be able to adapt to all the users' favorite smart-home application platforms. Both options lead the device manufacturers, operating



(a) Centralized solution: a single application manages collaboration among the participating devices and platforms

(b) Decentralized solution: a distributed application manages collaborative commands over the DCN

Figure 2: A comparison of collaboration schemes for smart home applications

platforms and the users to a dilemma of choosing application platforms, which similarly are not likely to support all the devices at the same time.

A centralized solution not only increases the network complexity by indefinite numbers of extra connections to the collaboration management platforms, but also requires additional resources and efforts on each collaborative IoT device, including power consumption, memory space, software complexity, etc., which are extremely limited on many battery-powered devices. Moreover, data islands formed on centralized platforms tend to develop their own ecosystems instead of conforming with others. Moreover, centralized solutions have obvious drawbacks when users decide to replace smart devices from different vendors. Thus, the entire smart industry will be dispersed and drift away from the ultimate goal of bringing convenience to people's life. Hence, decentralized collaboration mechanisms motivated by these preceding facts are receiving more and more attention.

In a decentralized solution, such as shown in Figure 2b and discussed in Section 3, cross-platform collaboration becomes necessary and critical. In order to achieve the security requirements in cross-platform collaborations, a proper trust framework is essential. Its scalability is important to meet the demands of rapidly increasing amount of devices. Such a Smart Life ecosystem will be built across competitive manufacturers and service providers on the basis of collaboration. This requires a reasonable incentive mechanism to maintain its sustainable development.

2.2 Related Work

Smart device manufacturers and IoT service providers have proposed various smart home solutions, such as Samsung Smart-Things [3], Apple Home-Kit [13] and Xiaomi MIJIA [34]. Such IoT device collaboration requires judgment as to whether users or devices have the permission to use or change a certain resource, so as to prevent unauthorized usage. Thereby every collaboration request requires authentication and authorization.

Aspects of these technologies have been discussed in the research literature. Ye et al. [37] discuss an efficient authentication and access control method based on Elliptic Curve Cryptography (ECC) for perception layer. Gupte and Sandhu [9] consider an authorization framework to secure dynamic system where interactions among entities are not pre-defined. Wagner et al. discuss access control for smart locks [11]. Bouij et al. [6] propose a dynamic access control approach based on blockchain and machine learning. Kaiwen et al. [16] propose an access control model based on attribute and role to address the scenarios of large scale dynamics users. Tian et al. focus on user-centered authorization for IoT [35].

In these approaches, devices typically connect to the same cloud platform as shown in Figure 2a, where the cloud platform maintains devices identifiers [3, 13], instructions of collaboration and policies of access control. When collaboration between devices is required, initiator sends request to the cloud platform. The cloud platform send execution to responder after verifying the identification of initiator and responder and relevant policies.

Further, many works have been developed to explore the usage of trust in systems. Jøsang et al. propose the subjective logic-based trust model using elements from Dempster-Shafer belief theory [14, 15]. Liu and Issarny [17] focus on designing a reputation-based trust framework that integrates additional trust aspects, including robustness to some attacks. More recently, Durresi et al. consider the measurement-based trust model for IoT [28, 29] that gives a multi-dimensionaltrust value. These approaches are based on mathematical methodology and require a reliable third party organization. Moreover these complex schemes may not be suitable for IoT environments given the low capabilities of many IoT devices.

Recently, blockchain technology has attracted considerable attention. Blockchain comprises a distributed peer-to-peer network

where members can interact with each other in a cryptographically verifiable manner. This distributed network is compatible with a broad range of IoT features. Hammi et al. [10] propose an original decentralized system called bubbles of trust relying on the security advantages provided by blockchain. Chen [7] discusses a new hybrid blockchain technology to address IoT issues such as trustless communications and decentralized applications. Monet et al. [20] focus on a new security model and its protocol based on the blockchain technology to ensure validity and integrity of cryptographic authentication data and associate peer trust level, from the beginning to the end of a sensor network lifetime. These researches are essentially a specific implementation of traditional authentication and authorization technology on the blockchain.

Sandhu [30] discusses the Attribute-Based Access Control (ABAC) model and its evolution. ABAC is suitable for IoT. Sciancalepore et al. [31] focus on ABAC and token-based authorization for IoT platforms. Other authors [26, 36] explain the realization ABAC through smart contracts. These works are local solutions for existing technologies on blockchain. To be applicable to the Smart Home scenario, it is necessary to build an effective cross-platform IoT trust framework with ecosystem, technology and business combination that can foster sustainable development. However, this issue is not well addressed in the current literature.

3 CROSS-PLATFORM COLLABORATION

This section discusses key objectives and corresponding security requirements for building decentralized cross-platform collaboration in IoT scenarios. Traditional collaborative IoT solutions tend to isolate data exchange within central platforms, which form data islands and limit the possibilities of cross-platform collaboration. In order to connect these data islands, an infrastructure needs to be established with proper network connections, standardized APIs, data exchange mechanisms, access control policies and so on. The infrastructure, named Decentralized Collaborative Network (DCN) as shown in Figure 2b, serves as a middleware to facilitate upper layer applications, such as smart home.

3.1 Key Objectives

The goal of smart life is to make users' life easier with collaborative smart devices. To achieve this, the following critical challenges need to be addressed.

- **Agreements between Platforms:** Different platforms have different interests and tradition resulting in variety in data formats, protocols and rules, etc. Agreements between platforms is a central premise of cross-platform collaboration. Also, the agreed terms should be enforced dutifully on each collaboration between the participants, which will often be device-to-device.
- **Security and Privacy:** From the Internet to the Internet of Things, security has become increasingly important since the connected things have the ability to put people's lives and bodies in danger. Also, privacy has always been a major concern of connected devices in smart life scenarios. Both security and privacy problems become bigger in collaborative IoT scenarios. Thus, we aim at a trustworthy solution with privacy-aware mechanisms.
- **Efficiency and Scalability:** In viable IoT solutions, the response time of a user intention must be within the acceptable range or even real-time in some cases such as autonomous driving vehicles. Due to the large scale of IoT, the scalability of a cross-platform collaboration solution is essential to support a large number of participating platforms and even more numerous IoT devices.
- **Sustainable Ecosystem:** The interests of the participating platforms vary from time to time. The problem of maintaining a sustainable ecosystem meeting diverse interests is crucial. Data ownership, right of control and privacy protection are also of concern by the end-users. These need to be taken care of in the ecosystem adequately and transparently.

3.2 Security Requirements

The following requirements are essential to achieve the key goals described in Section 3.1.

- **Decentralized Trust Framework:** A secure and controlled collaboration is established among the platforms in Figure 2b through the trust mechanisms over the DCN. This requires a mechanism to issue a unique identity to each device in cross-platform collaborations, and mechanisms to establish and enforce trust.
- **Access Control and Data Security:** It is necessary to standardize and implement distributed access control protocols in order to achieve collaboration of devices under different cloud platforms. Moreover, user privacy protection and third-party auditing requirements need to be balanced.
- **Hierarchical Synchronization:** Synchronizing trust relationships across a massive global system that the IoT is expected to become is a daunting task. The concept of Hierarchical Synchronization is based on different trust domains formed at two levels by Local and Global Blockchains. A saving grace is that global synchronization need not be real-time, whereas local synchronization may need to be close to real-time.
- **Incentive Policies:** To ensure the long-term, continuous and sound operation of the trust framework, incentive mechanisms integrated with specific commercial scenarios are required.

To summarize, decentralized trust framework is critical to fulfill the collaborative service securely and automatically. From the users' perspective, they wish to realize a customized user-centered smart life by building trust within IoT collaborative devices. In which case, distributed access control plays an important role, and credit management is essential for users and platforms to check and maintain the trust relationship with their peers, as well as anomaly detection to recognize compromised peers. All the actions during collaboration must be recorded and should be traced conveniently for audit authority. For all the participants in IoT collaboration scenarios, incentive policy is important for it improves attractiveness for the participants to share their resources. All these upper-level security services call for hierarchical support from network, perception of device, and even chip-level security technology. Blockchain can take effect at different places in this hierarchical trust framework due to its programmable and enforceable character.

4 BLOCKCHAIN-BASED TRUST FRAMEWORK

In order to achieve the key objectives and correlated security requirements described in Section 3, we propose a blockchain-based trust framework for collaborative IoT scenarios. This section consists of a design overview and an introduction to the building blocks including blockchain-based trust mechanisms, blockchain-based access control approaches, hierarchical trust synchronization and incentive polices. Finally, a use case study is presented to demonstrate utility.

4.1 Design Overview

The proposed Blockchain-Based Trust Framework (BBTF) as shown in Figure 3 consists of three layers, the Perception Layer, the Network Layer and the Application Layer, which are consistent with the typical architecture of IoT.

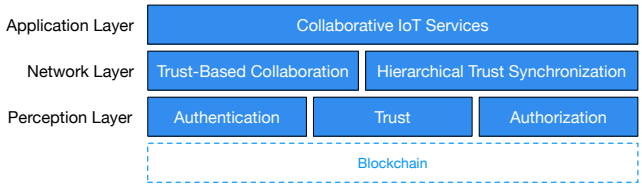


Figure 3: Blockchain-Based Trust Framework (BBTF) in Layers

The Perception Layer at the bottom provides the basic components including authentication, authorization and trust. Each of these is crucial to the collaboration process and facilitates the upper layer modules. The Network Layer in the middle contains trust-based collaboration and hierarchical trust synchronization modules using the basic components to provide middle-ware services for the applications. The Application Layer at the top includes a collection of essential services named Collaborative IoT services. The three layers comprise the core components of BBTF built upon the blockchain layer.

The core components of BBTF are described as follows.

- **Authentication.** Each device is given a unique identity across all the participating platforms over the blockchain as a representative. Authentication is decentralized so that a platform does not have to share its sensitive information of devices and users for collaboration purposes.
- **Authorization.** A suitable access control model for collaborative IoT scenarios has to be adaptable to the fragmented needs, changing contexts and arbitrary attributes. Moreover, the authorization policies are managed and enforced using smart contract with a reliable audit trail over the blockchain.
- **Trust.** In BBTF, trust guarantees that an IoT entity is capable of acting reliably and securely during collaborations by establishing trust relationships among peers via trust management. Blockchain helps synchronize this trust relationship crossing domains which are trusted at different levels. Trust degrees within the same domain can also differ from each other. Thus trust management is needed to maintain and adjust the existing trust relationships based on the credit of an IoT entity.
- **Trust-Based Collaboration.** This component provides automatic collaborations among IoT devices, triggered by a user operation or a combination of specified conditions. This is accomplished on the blockchain by using hierarchical smart contracts, which takes advantage of programmable and enforceable features, as discussed in Section 4.2.
- **Hierarchical Trust Synchronization.** Blockchain-based trust management approaches requires multi-level trust domains to achieve consensus and data synchronization. The division of trust domains and the process of consensus is described in Section 4.2.
- **Collaborative IoT Services.** These provides security audit, anomaly detection and credit management for users as well as incentive management. Incentive is important to consortium blockchain in order to improve user engagement. Incentive management not only provides incentive system for IoT collaborators, but also benefits the consortium blockchain platform by bring diversity to its application.

In order to achieve decentralized trust framework, the trust relationships between platforms need to be managed in a controllable and transparent way over the blockchain. The access control and data security requirements can be achieved by the authentication and authorization modules. Hierarchical synchronization essentially provides an approach to share the data across trust domains. Incentive policies enhances the sustainability of the collaborative IoT services.

The rest of this section discusses the core features and the design details of BBTF including the trust mechanisms, blockchain-based access control, hierarchical synchronization and incentive policies.

4.2 Trust Mechanisms

The goal of trust-based automation is to secure collaborations between IoT participants. IoT devices can control one another without a centralized facility when user gives an order or certain conditions are satisfied and perceived by sensors. Trust-based automation takes place in the perception layer. Trust management is necessary to accomplish trust-based automation. The first step of collaboration is to recognize and authenticate the device, then access control process takes place to authorize access requester to the target resource, which two steps usually happen in perception layer. With the incorporation of blockchain, we accomplish the process of collaboration mostly by using smart contracts. These smart contracts implement functions of access control for collaboration initiator to get access control permissions from the target platform. This makes authentication and authorization connected to the network layer of BBTF. All collaborators as well as their platforms can participate in access control, each by mapping to a chain node on the blockchain.

Using smart contracts to implement access control is only part of blockchain-based trust management. How to realize cross-platform collaboration automatically and efficiently remains as a crucial point. A typical centralized model, as discussed above in Section 2.2, requires high performance of computing and storage to deal with access control of IoT collaborations, making the system hard

to expand and vulnerable for attacks. In a decentralized system collaborative control messages can be transmitted by using blockchain. Once blockchain nodes reach a consensus, the nodes can share data. Collaborative rules can be written in smart contracts to make collaboration execute automatically. The process is under witness and consensus of all collaborators, which forms a trust model among participating platforms.

Cross-platform trust mechanisms are comparable with contemporary passport mechanisms. A national government issues a passport to an individual citizen as a globally unique identification. If the individual requests to visit another country, a visa with a certain category issued by the target nation may be needed according to the treaties between the two nations. During travel time, the individual has to present both the passport and the visa, as well as other supporting documents, to the customs exiting the source nation and entering the target nation for the permissions to travel. The travel history is recorded on the passport for future references by the visa and the customs officers. Inspired by the above process, we propose IoT Passport, the core mechanisms of BBTF, as shown in Figure 4, which consists of the following seven components.

- **A. IoT Passport Repository.** Like passports in the real world, IoT Passport is a universal identity for each blockchain node which represents the IoT entity. IoT Passport Repository issues an identity for each IoT entity. The identity management can be accomplished by smart contracts called IoT Passport Contracts, which consists of identity mapping, identity registration, revocation and so on. These identity management operations are recorded on blockchain so that collaborators know the identity changes of peer nodes so as to interact with each other automatically. A blockchain node uses the IoT Passport to participate in collaborations. This on-chain identity can be mapped from collaborator's physical identity. Physical identity can be device serial number, MAC address or platform register number, etc. Whether there is a need to manage global identity and how to accomplish it still requires further consideration.
- **B. User-Defined Policies.** Trust-based automation should be user-oriented, which means users are able to define collaboration scenarios based on their needs. User-Defined Policies specify the triggering conditions of collaborations and the subsequent actions to be done by the controlled devices. The triggering conditions are related to scenarios of collaborations, for example, "if temperature exceeds 40 degrees C" or "someone has passed through the door." The subsequent actions determine how the controlled devices should react in response to the triggering condition, e.g., sensors of IoT devices collect certain environment changes and report them once triggering conditions are met. The conditions and the corresponding actions are written in a smart contract called the User Scenario Contract. The input of User Scenario Contract is the triggering conditions. The smart contract analyzes the changes and selects the best matched condition entry and corresponding actions.
- **C. Access Control Policies.** Access Control Policies specify the authorization rules for device accesses. They are written in smart contracts called the Trust Rule Contracts. These contracts have the following properties. First, identity authentication should be done by devices and their platforms. Second, access control should take part when an IoT device request access permission from its target platforms. Trust value of device should be influenced by history of collaborations. Any event of trust rules contract should be recorded on blockchain and able to be traced in the future.
- **D. Cross-Platform Trust Policies.** Cross-Platform Trust Policies provide trust rules between platforms, and is written in smart contracts called the Collaborative Rule Contracts. They require the following properties to be met. Platforms should build trust prior to collaborations and subsequently observe corresponding rules. Collaborative Rules require platforms to reach the consensus of which devices and their attributes can be controlled using blockchain. Once the cross-platform trust policies between two platforms or manufacturers changes, the Collaborative Rule Contract should be changed and redeployed. Any event of Collaborative Rules should be recorded on blockchain and able to be traced in the future.
- **E. Incentive Policies.** Incentive Policies improve the engagement of platforms and the sustainability of the ecosystem by rewarding participants. Engagement is measured by the collaboration duration of platforms, number of devices involved and collaboration times, etc. The incentive topic is further discussed in Section 4.5 in detail. Incentive Agreements are written in smart contracts named the Incentive Rule Contracts. Based on a collaboration result, the Incentive Rule Contract calculates and distributes the rewards for the participating parties according to the agreed incentive rules.
- **F. Trust-Oriented Credits.** Trust-Oriented Credits (TOC) provides dynamic trust management used in access control policies. TOC reflects the reliability of trustworthiness. It is presented as credit policies in the form of a smart contract called the Credit Management Contract. It takes place when access control is completed. Based on the authorization results, it gives feedback to Access Control Policies by adjusting the trust value of IoT devices.
- **G. Provenance Data Repository.** Provenance Data Repository records the execution history of policies discussed above. It helps audit the behaviors of IoT entities and provides attributes data for authorization decisions.

The first five components are accomplished by a combination of smart contracts, while the latter two components are for the purpose of trust management and auditability. All the above mentioned smart contracts are invoked in order for each cross-platform collaboration and construct a combination of smart contracts for collaborative IoT scenarios. The IoT Passport Contract provides a universal identity for each blockchain node which represents the corresponding IoT entity. When the initiator IoT device (call it D_i) senses environment or get an command from the user, it triggers an access request to its platform. The first step is for D_i to accomplish two-way authentication between the corresponding platform and itself, which is done by the Trust Rule Contract. The platform of D_i uses User-Defined Policies to get the collaborative IoT device (call it D_r). Then the cross-platform trust polices build trust path between

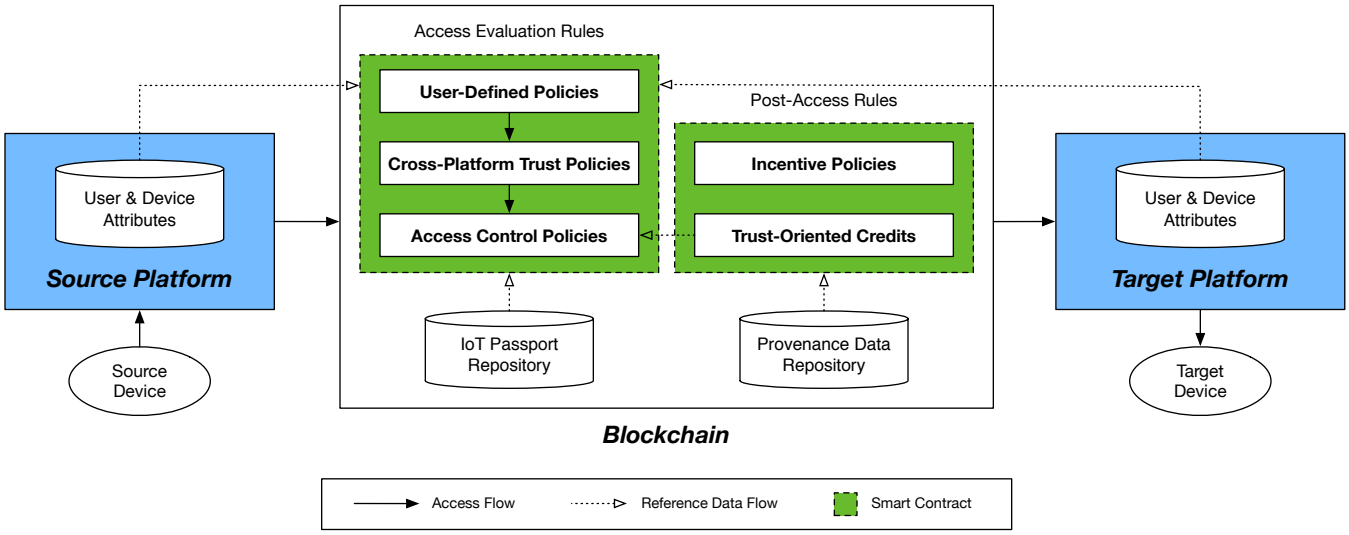


Figure 4: Cross-platform access control with Blockchain-Based Trust Framework

two collaborative platforms using Collaborative Rule Contract. If the trust path is built successfully, D_i uses Access Control Policies to get access permission from D_r. D_i is authorized once consensus of Trust Rule Contract is reached, which means a complete trust path is built between D_i and D_r, and D_i can then collaborate D_r. Since consensus of smart contract is reached among all the essential collaborative blockchain nodes, platform of D_r can send control message to its devices instead of D_i collaborating with D_r directly with the help of blockchain.

4.3 Blockchain-Based Access Control

The authentication mechanism leverages the information of the device, such as the MAC address, service number, location information and so on, to construct a globally unique device ID after hash operation. Once assigned this ID, the device is registered on the blockchain with its public key mapped to the ID. Afterwards, the device uses its private key to authenticate itself. The ID becomes its IoT passport number, while the other device information on the passport is only retrievable by the issuing platform and the device itself. In this way, the minimum necessary disclosure of the sensitive device information can be achieved during cross-platform collaboration accesses.

Having considered the trust value as one of the attributes of IoT devices, Attribute-Based Access Control (ABAC) model is suitable to apply. Since attribute is the inherent quality of IoT subject and object, no manual assignment is required, it is easy for ABAC resource owner to separate policy management and authority judgment. We believe that attribute-based model is closer to the smart life scenarios and constraint conditions can be treated as different attributes which makes the access policy changeable according to the actual situation. Besides, attribute-based encryption can protect user data from being revealed or analyzed while guaranteeing fine-grained access control.

Given the above, blockchain-based access control approaches using ABAC model can be used to realize distributed access control. Access control policies can be written in the form of smart contract and deployed in blockchain. Attribute management can also play a role as data sections of the smart contracts. By mapping these attributes into several data section of smart contract, access control policy can build a mapping from attributes to privilege. The Trust Rule Contract specifies the operations that the subject can perform on the object. First of all, subject requests an access permission to a object, then object executes the smart contract to authenticate subject and decide whether to permit the request based on the environment conditions and attributes of the subject and itself. During this step, trust is considered as one of the attributes of the subject for object to identify it, as well as one of the attributes of the object to authorize access permission to the subject.

Cross-platform access control can also be accomplished by using blockchain. Each step of collaboration is signed by a corresponding IoT entity. Platforms and devices generate blockchain key pairs and keep public keys on the blockchain as one of their attributes, leaving private key for signing collaboration message on the chain. Any device or platform can get access to the attributes of its target through access control process, which means it is trusted by its peer. If trust is built between two IoT entities, they can share public keys using blockchain. In this way, any device trusted by its platform can verify the signature of another device from a different platform, as long as trust is built between these two platforms. Since anything happened on blockchain is under the consensus of all the IoT entities on the blockchain, it is hard for a malicious node to cheat against most of the nodes, which makes the trust more reliable. Moreover, provenance data of the collaboration history is taken into consideration during a policy decision process, such as the provenance-based access control model of Park et al [24].

4.4 Hierarchical Trust Domains

As discussed in 4.3, trust attribute plays an important part in access control polices, which means a proper way to transmit trust relationships among IoT entities should be proposed to facilitate

automatic and efficient collaboration. The trust relationships of IoT entities can be shared on blockchain through consensus.

The scopes of consensus are divided by trust domains, which consist of the global trust domain and local trust domains. As the names indicate, local trust domains attain consensus and share data within local nodes while the global trust domain may contain multiple local trust domains and share data across them. This hierarchical blockchain model amplifies efficiency and scalability. The typical scale of the local trust domain is a home, a car or an office. The global trust domain usually represents an industry, an organization or a city. Basically, the local blockchain builds trust among IoT devices, while the global blockchain builds trust among operating platforms.

Local trust domain contains multiple IoT entities that share data with same degree of privacy. Each global trust domain is a relative concept since the model of trust can represent a hierarchical structure. IoT entities of local trust domain use blockchain named local blockchain to collaborate with each other. Global trust domain is formed by collaborative platforms and a blockchain named global blockchain to share data, as shown in Figure 5.

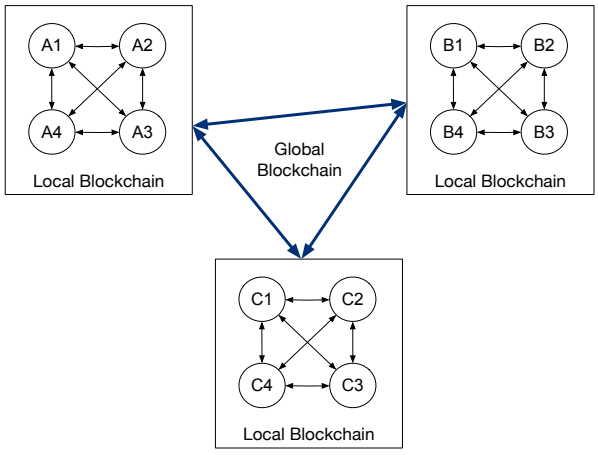


Figure 5: Hierarchical Trust Domains Synchronized across the Global Blockchain and Local Blockchains

A1 to A4 represent the blockchain nodes from the first local blockchain, B1 to B4 represent the blockchain nodes from the second local blockchain, while C1 to C4 represent the blockchain nodes from the third local blockchain. Some of the platform blockchain nodes for example, A1, B1 and C3 may be chosen from each local blockchain to compose the global blockchain.

Key components of hierarchical trust domains are discussed below. Trust relationships help build trust path between various IoT entities, and trust domains shares data among those IoT entities who trust each other.

- **A. Trust Relationship.** Trust relationship presents a way to describe the trust degree between two entities, and includes direct and indirect trust. For example, Alice trusts Bob and Bob trusts Carol does not simply means that Alice trusts Carol at the same level. Suppose A trusts B but does not trust C. However, A is willing to accept trust transmission of C from B. When B receives A's request and replies with trust between B and C, a trust path between A to C is built. Trust value is related to the duration of trust between two collaborators, the trust value of the direct trust collaborator of its peer, and the degree of satisfaction, etc. Collaborators should have the right to transmit trust or to accept it. Collaborators should decide that they should trust its indirect peer to what degree. Trust value should be changed when time lasts or specific events happen. Trust value should be easy to get but hard to change.
- **B. Trust Domain.** Trust Domain is an area in which collaborators trust each other and share data. Logically, different trust domains share different data sets.
- **C. Hierarchical Synchronization.** Hierarchical Synchronization is based on different trust domains which is formed by Local Blockchain (LB) and Global Blockchain (GB) in Figure 5. LB contains several collaborators which share the same trust domain. Besides, different LB does not share any collaborator or trust domain. GB contains at least one collaborator chosen from each LB of last level and the way of this choosing process is based on blockchain consensus. The performance of hierarchical synchronization is often a concern, since the performance of the contemporary blockchain infrastructure is limited. Nevertheless, hierarchical trust domains rarely require real-time synchronization. Also, synchronization can be achieved using other mechanisms than blockchain. Thus, the impact of blockchain performance is limited as well.

4.5 Incentive Policies

Incentive is important since it improves engagement of IoT collaborators. Incentive policies of BBTF are summarized into three different levels, including capability-based incentive policies, service-based incentive policies and ecosystem-based incentive policies. These incentive policies gain critical information from collaborations and influence the collaborations in turn. Capability-based incentive policy specifies rules of adjusting trust attributes and computational resources according to the collaborations. It helps create a closed-loop system together with the Access Evaluation Rules shown in Figure 4. Service-based incentive policy improves engagement of platforms by promising actual benefits such as critical collaborative information. Ecosystem-based incentive policy focus on the sustainable development of IoT collaboration and encourages more contribution from collaborative participants.

Capability-based incentive policy gives rewards to devices according to their engagement including contribution of computing, frequency of effective collaboration, and times of cross-platform collaboration, etc. These rewards help modify device's trust value before the next process of access control, thus brings influence on the trust relationships among IoT collaborators. Moreover, capability-based incentive policy helps balance the capability of calculation and storage among different devices in the BBTF. It keeps real-time records of the capability for each IoT entity, and evaluates consumption of computation and storage for the next time. In this way, it can distribute load of the collaboration on different devices.

Service-based incentive policy aims at improving the engagement of platforms. As the engagement of IoT devices in collaboration increases, service-based incentive policy can help the corresponding platforms to get more useful data from collaborations. That means, users and platforms should reach the agreement on which data is non-private. With these data including non-sensitive habits of user and the direction of data flow, service-based incentive policy can draw an accurate profile of users, which provides essential information for product designing and precision marketing.

Ecosystem-based incentive policy provides rankings of IoT devices and services, which helps user to reach a comprehensive understanding of habits and explore more smart life scenarios. Most important of all, more contributions means more influence of platforms. It is reflected in numerous aspects through blockchain consensus to practical benefits. Platforms on top of the ranking list have more rights in consensus like Delegated Proof of Stake (DPoS), which brings more block rewards. The block rewards vary from credits to determination of cross-platform collaboration policies.

The events of incentive policies can be recorded on blockchain, and some incentive policies such as capability-based incentive can also be written as smart contracts to execute automatically.

4.6 Use Case Study

The process of a cross-platform collaboration through the combination of smart contracts as shown in Figure 4 is demonstrated with the user scenarios in Section 2.1 as the following. Sensors at Alice's home keeps perceiving and reporting her location and movements. Once Alice is about to come home, the sensor detects the triggering conditions is met and starts to request access to the smart home IoT devices. First of all, the sensor starts to build trust between the platform with itself using Trust Rule Contracts. Let D_1 represent the sensor, and P_1 represent the platform of D_1. A_1 stands for the mood, location and moving speed attribute set of Alice that has been reported to the sensor. P_1 authenticates D_1 using identities of D_1 and A_1 as input, then it checks the user-defined policies to find out the collaborative IoT devices with the input of identity parameters set (P_1, D_1, A_1). P_1 uses User Scenario Contract to obtain controlled parties which is described in identity parameters set (P_2, D_2, A_2). Here P_2 represents the controlled platform, and D_2 the controlled devices under this condition. A_2 represents the attributes of D_2 that should be changed in this collaboration. Here in this user scenario of Alice, D_2 can be the smart lights at her home and P_2 is the platform of the smart light. A_2 represents the on-off state of the light. After deciding which IoT device to collaborate, cross-platform trust policies are checked by P_1 to identify the trust between P_1 and P_2. If success, D_1 interacts with D_2 by Trust Rule Contract again to get access permission from D_2. The smart light decides whether to authorize the sensor to control it, based on attributes that the sensor gets from Alice, and the sensor's trust value. If the sensor is authorized, P_2 can get the information of collaboration once the consensus of the corresponding smart contract is reached. Then smart light platform then may send a control order to turn on the light.

A similar collaboration could happen between Alice's smart speaker and sensor at her home so when Alice comes home the smart speaker plays her favourite music.

5 PROPOSED SECURITY FOCUSED RESEARCH AGENDA

The proposed blockchain-based trust framework aims to enable secure and transparent collaborations for connected IoT devices. Now we present opportunities for some research directions associated with the framework.

- **Context-Aware Access Control for IoT.** Even if attribute-based models are regarded as suitable for most IoT scenarios, in Smart Life scenarios some user-driven contexts for inter-device accesses need to be considered. The variety of contexts is attributed to both user-end and device-end diversity. On the user-end, the smart devices in homes or cars are shared in most use cases by multiple family members, including parents, children and guests, etc. The authorization policies and schema of different users should be distinct. For example, each inter-device transaction should correlate the provenance of the acting user's behavior and the automation policy designating user's behavior to the access decisions. On the device-end, since each transaction consists of a series of accesses across multiple devices and cloud platforms, the transaction context should be consistent in the span of its whole life cycle. In these situations, novel context-aware fine-grained access control models and their enforcement require further research.
- **Cross-Platform Trust Models.** The proposed blockchain-based trust framework enables decentralized trust among platforms and devices. Comparing to traditional trust models, this framework allows finer-grained trust models to present different types of trust relations among participants in IoT environments. The cross-platform trust models should cover arbitrary scenarios according to the dynamic business needs of all participants. For example, platform A may allow its device type A1 to be accessed by device type B1 from platform B with function F1 but not by device type C1 from platform C. In this case, the trust relations between A and B are different to those between A and C. These relations may change from time to time due to a myriad of factors in the real world. Further, the attributes associated with an individual device may also affect its trust relations with other devices. Due to the above mentioned problems and more, understanding of cross-platform trust models is critical and challenging in collaborative IoT scenarios.
- **On-Blockchain Policy Administration and Verification.** Blockchain is the foundation of the proposed trust framework. Administration and verification of trust and access policies should also be managed on blockchain. On-blockchain administration is straightforward, using a privileged smart contract to define the consensus process for administrative policies to be generated and take effect. The consensus process should include all the core stakeholders of the policy to be generated, such as the affected parties, the policy composers, the verification professionals, the administrative authority and so on. The process itself must be designed in advance and carefully changed by consensus. The verification of the proposed policy plays the gatekeeper role in the process because once the policy becomes active and enforced

in the smart contract all the transactions are affected. Analytic tools will be required to discover implementation and design issues of various policies. Typically, the verification parties should sign certifications for proposed policies on blockchain. Then, the credibility and authenticity of the verification professionals should also be managed on blockchain. The management mechanisms are not broadly discussed in this paper but deserve research attention.

- **Data on the Edge.** IoT is a typical application environment of Edge Computing, in which data security and privacy has received a lot of research attention recently. Due to the soaring market of IoT and fast-speed internet connectivity, such as 5G-enabled devices, user-generated shared data, transaction data and private data, etc. on the Edge are increasing by orders of magnitude. Data used to be free to copy in the Internet. Today, as IoT brings technology closer to the users, data becomes a valuable asset for both users and service providers, who are able to exchange their data with blockchain from the Edge. The exchange transactions need to be secure and transparent, as well as privacy-concerned in some cases. Besides the data exchange, the distributed data on the Edge of collaborative IoT also needs security and privacy protection. For example, the original meta data of a collaborative transaction may be fragmented on multiple participating devices. How to securely collect and backup this distributed data effectively becomes an open problem.

6 SUMMARY

This paper proposes a blockchain-based trust framework for collaborative IoT. In particular, we develop a layered architectural design with different key components in accordance with the layers of IoT. We present five key components associated with the smart contracts to realize the proposed framework. Furthermore, we present the details of three key mechanisms implemented in the framework, e.g., the collaboration process, hierarchical synchronization and access control models. Finally, the paper envisions future research directions beyond the trust framework for Collaborative IoT. We envision to develop context-aware access control models, cross-platform trust models, on-blockchain policy administration and verification, and data on the Edge with proposed research agenda.

REFERENCES

[1] A. Alshehri and R. Sandhu. 2016. Access Control Models for Cloud-Enabled Internet of Things: A Proposed Architecture and Research Agenda. In *CIC*. IEEE.

[2] A. Alshehri et al. 2018. Access Control Model for Virtual Objects (Shadows) Communication for AWS Internet of Things. In *ACM CODASPY*.

[3] SmartThings Inc. as a wholly owned subsidiary of Samsung Electronics. 2019. There's potential in your everyday things. Retrieved February 6, 2019 from https://www.smartthings.com/about

[4] S. Bhatt, F. Patwa, and R. Sandhu. 2017. An Access Control Framework for Cloud-Enabled Wearable Internet of Things. In *IEEE CIC*. 328–338.

[5] Smriti Bhatt, Farhan Patwa, and Ravi Sandhu. 2017. Access Control Model for AWS Internet of Things. In *Network and System Security*. Springer, 721–736.

[6] I. Bouij-Pasquier, A. Ouahman, A. El Kalam, and M. Ouabiba de Montfort. 2015. SmartOrBAC security and privacy in the Internet of Things. In *IEEE/ACS 12th Int. Conf. on Computer Systems and Applications*. IEEE, 1–8.

[7] Jollen Chen. 2018. Hybrid blockchain and pseudonymous authentication for secure and trusted IoT networks. *ACM SIGBED Review* 15, 5 (2018), 22–28.

[8] S. Elbouanani, M. El Kiram, and O. Achbarou. 2015. Introduction to the Internet of Things security: Standardization and research challenges. In *2015 11th International Conference on Information Assurance and Security*. IEEE, 32–37.

[9] Maanak Gupta and Ravi Sandhu. 2018. Authorization Framework for Secure Cloud Assisted Connected Cars and Vehicular Internet of Things. In *23rd ACM on Symposium on Access Control Models and Technologies*. ACM, 193–204.

[10] Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, and Ahmed Serhrouchni. 2018. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security* 78 (2018), 126–142.

[11] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner. 2016. Smart locks: Lessons for securing commodity internet of things devices. In *11th ACM Asia conference on computer and communications security*. ACM, 461–472.

[12] G. Hunt. 2018. Introducing Microsoft Azure Sphere: Secure and power the intelligent edge. Retrieved Feb. 17, 2019 from https://azure.microsoft.com/en-us/blog/introducing-microsoft-azure-sphere-secure-and-power-the-intelligent-edge/

[13] Apple Inc. 2019. Your home at your command. Retrieved February 6, 2019 from https://www.apple.com/ios/home/

[14] Audun Jøsang. 2001. A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 9, 03 (2001), 279–311.

[15] Audun Jøsang, Ross Hayward, and Simon Pope. 2006. Trust network analysis with subjective logic. In *Proceedings of the 29th Australasian Computer Science Conference-Volume 48*. Australian Computer Society, Inc., 85–94.

[16] Sun Kaiwen and Yin Lihua. 2014. Attribute-role-based hybrid access control in the internet of things. In *Asia-Pacific Web Conference*. Springer, 333–343.

[17] Jinshan Liu and Valérie Issarny. 2004. Enhanced reputation mechanism for mobile ad hoc networks. In *Int. Conf. on Trust Management*. Springer, 48–62.

[18] Juniper Research Ltd. 2015. Smart Home Revenues to Reach $100 Billion by 2020, Driven by Automation and Entertainment Services. Retrieved February 7, 2019 from https://www.juniperresearch.com/press/press-releases/smart-home-revenues-to-reach-\protect\T1\textdollar100-billion-by-2020

[19] Damiano Di Francesco Maesa, Paolo Mori, and Laura Ricci. 2017. Blockchain based access control. In *IFIP International Conference on Distributed Applications and Interoperable Systems*. Springer, 206–220.

[20] A. Moinet, B. Darties, and J. Baril. 2017. Blockchain based trust & authentication for decentralized sensor networks. *arXiv preprint arXiv:1706.01730* (2017).

[21] League of Nations. 1920. *Conference on passports, customs formalities and through tickets. Resolution adopted by the conference.*

[22] Afif Osseiran, Jose F Monserrat, and Patrick Marsch. 2016. *5G mobile and wireless communications technology*. Cambridge University Press.

[23] A. Outchakoucht, E. Hamza, and J. Leory. 2017. Dynamic access control policy based on blockchain and machine learning for the internet of things. *Int. J. of Advanced Computer Science and Applications* 8, 7 (2017), 417–424.

[24] Jaehong Park, Dang Nguyen, and Ravi Sandhu. 2012. A provenance-based access control model. In *Int. Conf. on Privacy, Security and Trust*. IEEE, 137–144.

[25] Christina Patsioura. 2018. *Blockchain and distributed ledger technologies: what's the value for IoT?* Technical Report. GSMA Intelligence.

[26] O. Pinno, A. Grégio, and L. De Bona. 2017. Controlchain: Blockchain as a central enabler for access control authorizations in the iot. In *GLOBECOM*. IEEE, 1–6.

[27] T. Rappaport et al. 2017. Overview of millimeter wave communications for fifth-generation (5G) wireless networks with a focus on propagation models. *IEEE Trans. on Antennas and Propagation* 65, 12 (2017), 6213–6230.

[28] Y. Ruan, A. Durresi, and L. Alfantoukh. 2016. Trust management framework for internet of things. In *IEEE Conf. on Advanced Info. Nw. and Apps*. 1013–1019.

[29] Y. Ruan et al. 2017. Measurement theory-based trust management framework for online social communities. *ACM TOIT* 17, 2 (2017), 16.

[30] Ravi Sandhu. 2012. The authorization leap from rights to attributes: maturation or chaos?. In *17th ACM SACMAT*. ACM, 69–70.

[31] S. Sciancalepore et al. 2016. Attribute-based access control scheme in federated IoT platforms. In *Wkshp. on Interoperability and Open-Source Solutions*. 123–138.

[32] H. Shariatmadari et al. 2015. Machine-type communications: current status and future perspectives toward 5G systems. *IEEE Communications* 53, 9 (2015), 10–17.

[33] Strategy and Policy Unit (SPU). 2005. *The Internet of Things*. ITU Internet Reports. International Telecommunication Union (ITU), Geneva, Switzerland.

[34] Xiaomi technology co. LTD. [n. d.]. http://www.mi.com/global/mibox/

[35] Y. Tian et al. 2017. Smartauth: User-centered authorization for the internet of things. In *USENIX Security)*. 361–378.

[36] R. Xu et al. 2018. Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the iot. *Computers* 7, 3 (2018), 39.

[37] N. Ye et al. 2014. An efficient authentication and access control scheme for perception layer of internet of things. *Appl. Math. & Info. Sci.* 8, 4 (2014), 1–8.