IOTA-Based Access Control Framework for the Internet of Things

Ruka Nakanishi, Yuanyu Zhang, Masahiro Sasabe and Shoji Kasahara
Graduate School of Science and Technology, Nara Institute of Science and Technology,
8916-5 Takayama-cho, Ikoma, Nara 630-0192, Japan.
Email: nakanishi.ruka.nm0@is.naist.jp, {yy90zhang, m-sasabe, kasahara}@ieee.org

***Abstract*—With the rapid dissemination of the Internet of Things (IoT), the number of resources deployed in IoT systems such as devices and data is growing explosively. Since IoT systems often handle private information, it is essential to enforce appropriate access control to prevent unauthorized access. However, conventional access control schemes in which access rights are stored in a centralized server are prone to load concentration and a single point of failure. Although distributed access control schemes leveraging blockchain technologies have been proposed to deal with such problems, they inherit the drawbacks of the blockchain technologies, such as high transaction fee and low throughput. This paper proposes a novel access control framework based on IOTA, an emerging distributed ledger technology which enables free micro transactions with high throughput. This framework provides scalable and fine-grained access control by encrypting access rights using the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) technology and storing them on the distributed ledger of IOTA, called Tangle.**

***Index Terms*—Internet of Things, IOTA, Blockchain, Access Control, Ciphertext-Policy Attribute-Based Encryption (CP-ABE)**

I. Introduction

Thanks to the dissemination of the Internet of Things (IoT), an explosively growing amount of IoT resources (e.g., devices and data) are deployed in the Internet nowadays. These resources serve as fundamental components for decision making and task execution, and are thus extremely crucial for developing various smart applications, like intelligent logistics, smart healthcare and smart manufacturing [1].

On the other hand, IoT devices, especially sensors, are usually designed without much security consideration, resulting in critical security issues. One of the representative security issues is unauthorized access to the IoT resources, which has been extensively reported [2]. As IoT data usually contain personal information and IoT devices are often deployed physically close to human bodies, without appropriate *access control* to the IoT resources, our property and safety would be significantly threatened.

Access control is referred to as restricting the access to resources (i.e., objects) to only the authorized users (i.e., subjects). In prevailing access control frameworks, access policies stating "who can access what resources" are stored in a centralized server for ease of management. However, the centralized server turns out to be a single point of failure, when destroyed by disasters or compromised by malicious users. Moreover, in large-scale systems like the IoT, centralized servers can suffer from load concentration. Thus, access control in IoT systems requires the properties of reliability and scalability as well as distributed backups for access policies.

To meet these requirements, distributed access control frameworks leveraging the blockchain technology have been proposed [3]–[5]. Blockchain, one of the building blocks of cryptocurrencies such as Bitcoin [6], can be considered as a database, which is managed over Peer-to-Peer (P2P) networks in a distributed manner. Each peer stores a copy of the blockchain and also verifies the validity of the stored data, such that no peers can tamper with the data. Such distributed and tamper-resistant features make the blockchain a perfect option for storing access rights and policies.

Recently, another noticeable functionality called smart contract has also been implemented in some blockchains like the Ethereum [7]. Smart contracts are executable codes that are deployed in the blockchain and can be executed by any peer, and thus provide distributed computing with high reliability by storing both the code and the execution results in the blockchain. This makes smart contracts the prevailing mechanisms for managing access rights/policies and conducting access verification in recent blockchain-based access control schemes for the IoT, like [3]–[5].

Although blockchain-based schemes are distributed and reliable, they inherit two main drawbacks from the blockchains. First, they incur monetary cost to users, since users need to pay some fee to the peers who verify the validity of the stored access rights/policies and execute smart contracts to process access requests. Second, they have low scalability/throughput of processing access requests. In most blockchains, newly issued transactions are verified and included into the blockchain at regular intervals. However, the number of transactions which can be included in each interval is limited, lowering the throughput. These two drawbacks may hinder the application of blockchain-based schemes to large-scale IoT systems.

To overcome these drawbacks, an access control framework based on the IOTA technology [8] has been proposed [9]. IOTA is a next-generation distributed ledger technology which tackles the issues of transaction fees and scalability of the blockchain by changing the data structure of the distributed ledger and the consensus protocol. Although the scheme in [9] has shown some advantages over blockchain-based schemes, it still has some limitations, like requiring pre-established secure

subject-object communication links, heavy burden of token management and unclear implementation of authorization, as introduced in greater details in Section II. To address these limitations, this paper combines the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) technology and the IOTA technology to propose a novel distributed access control scheme with higher flexibility, finer granularity and higher scalability. More specifically, the proposed scheme exploits the CP-ABE technology to encrypt the access rights and then stores the encrypted rights in the IOTA distributed ledger, called Tangle. By properly fining the policies of the CP-ABE, we can achieve more flexible and fine-grained access control. In addition, the CP-ABE provides one-to-many (i.e., one object and multiple subjects) access control, reducing the burden of token management and improving the scalability.

The remainder of this paper is structured as follows. In Section II, we introduce some related work. We then describe the CP-ABE technology in Section III. We introduce our scheme in Section IV and its implementation in Section V. Finally, we summarize the paper in Section VI.

II. Related Work

A. Conventional Access Control Frameworks

Representative access control models include Access Control List (ACL), Role-Based Access Control (RBAC) Attribute-Based Access Control (ABAC) and Capability-Based Access Control (CapBAC) [10]. ACL is a list kept by an object to record the granted access rights of subjects. In RBAC, roles (e.g., guest and administrator) are assigned to subjects and access rights are decided for each role. In ABAC, attributes (e.g., age and affiliation) are assigned to subjects and objects, and logic formulas of attributes called policies are used to specify the access rights granted to the subjects. In CapBAC, tokens are issued to subjects as proof of possessing certain access rights (capabilities). To access the objects, subjects are required to present the corresponding tokens to the object owners. Based on these models, centralized access control schemes have been proposed [11], [12], which are not suitable for large-scale IoT systems as introduced in Section I.

B. Blockchain-Based Access Control Frameworks

In [3], an Ethereum-based distributed CapBAC scheme was proposed, which stores the tokens of subjects using Ethereum smart contracts. When receiving an access request from a subject, object owners can decide to permit or deny the request by referring to the token on the blockchain and verifying the subject's access rights. In this way, access rights can be stored in a distributed and tamper-resistant fashion, and each object owner can enforce access control independently without relying on a specific authority.

In [4], an Ethereum-based distributed ABAC scheme was proposed, where the subjects' attributes, the objects' attributes and access control policies are recorded to smart contracts by respective administrators. On receiving an access request from a subject, object owners trigger the corresponding smart contract to verify the subject's access rights. The smart contract refers to the attributes and policies to perform the access control and returns the verification result to the object owner. The use of smart contracts provides trustworthy management of access rights and decision making. In addition, access control can be enforced even if some peers behave abnormally since the functions are decentralized.

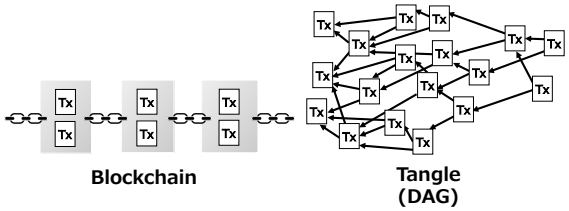

Fig. 1. Comparison of blockchain and Tangle.

As seen above, drawbacks in conventional schemes can be solved by utilizing blockchains. However, these schemes inherit the shortcomings of blockchains such as high transaction fees and low throughput, both of which may hinder their application to practical IoT systems.

C. IOTA-Based Access Control Framework

To mitigate the drawbacks of blockchain-based schemes, an IOTA-based access control scheme has been proposed [9]. IOTA is a next-generation distributed ledger technology designed for machine-to-machine (M2M) micro payments. Unlike Bitcoin and Ethereum, the distributed ledger of IOTA, called the Tangle, forms a directed acyclic graph (DAG) as shown in Fig. 1. Transactions (Tx) are linked together directly using one-way hash functions, instead of being encapsulated in blocks. Another significant characteristic of IOTA is the removal of mining. In IOTA, the consistency of the Tangle is maintained by requiring every peer to verify and approve two existing transactions to issue a new transaction. This not only eliminates the need of transaction fees but also accelerates the speed at which new transactions are approved, because the increase in the number of incoming transactions leads to more existing transactions being approved. For these reasons, IOTA is considered to have higher throughput and scalability.

Although smart contracts have not been implemented in IOTA, a novel data communication protocol called Masked Authenticated Messaging (MAM) [13] is available. Using MAM, peers can record data to and retrieve data from the Tangle in a tamper-resistant fashion. Peers can record data to the Tangle by masking (i.e., encrypting) them and issuing them as special transactions (MAM transactions). Each MAM transaction is associated with an address with which any peer can refer to the transaction. MAM transactions issued by the same peer are linked together chronologically, forming a channel (i.e., a chain of transactions). In addition, a signature of the issuer is attached to every MAM transaction, which enables subscribers to verify the authenticity of the issuer (authenticated messaging). Using MAM, peers can safely exchange data via the Tangle by subscribing to each other's channel.

In [9], an IOTA-based CapBAC framework called the Decentralized Capability-Based Access Control framework using IOTA (DCACI) was proposed. In DCACI, access tokens are stored on the Tangle using MAM. During the initial authorization process, a subject first sends a request for access rights to an object owner. The owner decides the access rights to grant based on local authorization policies and issues the subject an access token. At the same time, the owner records the token to the Tangle as the original copy. To access an object, the subject sends the owner an access request along with the token. The owner checks the presented token against the original one on the Tangle to verify its authenticity.

Although DCACI has achieved fee-less distributed access control, the framework still suffers from three drawbacks. First, it requires pre-established secure communication links between subjects and object owners. Requests and tokens are sent without being encrypted, facing the risk of being leaked to malicious users when an insecure channel is used. Second, it supports only one-to-one access control, which means that one token must be recorded for each subject, i.e., one token per subject, increasing the burden of token management for large-scale IoT systems. Finally, it provides no concrete implementation of the authorization process at the owner sides, i.e., the way/model used to decide what access rights should be granted to the subjects before issuing tokens.

To overcome the above drawbacks, we propose a novel access control framework based on IOTA and the CP-ABE technology to realize more flexible and scalable access control.

III. Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

CP-ABE [14] is a type of public-key cryptosystems. Unlike common public-key cryptosystems in which each user possesses a pair of public and private keys, there is only one public key (the master public key) in CP-ABE and private keys are associated with a set of attributes. The master public key and private keys are issued to users by a key-issuing authority, which associates each private key with the attributes of the corresponding user. For example, the authority may issue a student in the division of Information Science (IS) a private key corresponding to the set of attributes {Division: IS, Role: Student}, and a staff a private key corresponding to the set of attributes {Division: IS, Role: Staff}.

Another difference from common cryptosystems is the introduction of logic formulas called policies into the encryption process. Policies state the conditions of attributes that need to be satisfied to decrypt the ciphertext. The decryption succeeds if and only if the set of attributes associated with the private key satisfies the policy. For instance, given a ciphertext encrypted using the policy "Division: IS AND Role: Staff", users with the private key corresponding to the set of attributes {Division: IS, Role: Staff} can decrypt it, while users with the private key corresponding to the set of attributes {Division: IS, Role: Student} cannot.

As seen above, CP-ABE enables fine-grained ABAC by restricting the successful decryption to a specific group of users using policies. In our scheme, we encrypt tokens using CP-ABE and store them on the Tangle to achieve flexible access right authorization.

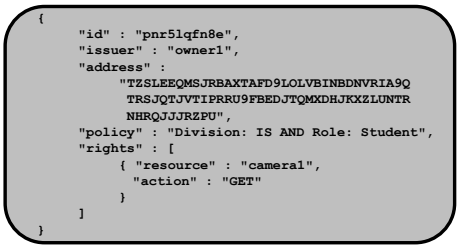

Fig. 2. Example of a token.

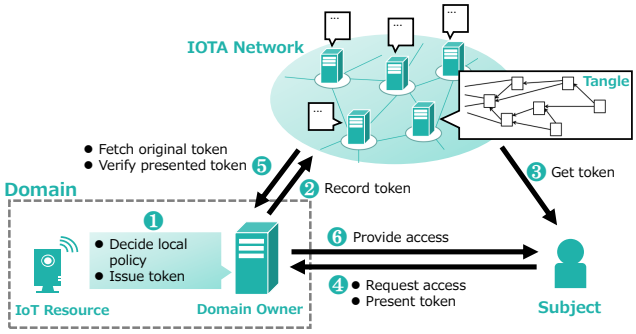

Fig. 3. Proposed scheme.

IV. Proposed Scheme

We combine CP-ABE with IOTA to solve the issues mentioned in Section II. The scheme is thus a hybrid of CapBAC and ABAC, and access rights are managed by encrypting tokens using CP-ABE and recording them on the Tangle as MAM transactions.

A. Token Structure

As shown in Fig. 2, a token is a JSON object which is issued by object owners. A token contains a unique ID, the issuer, the address it is associated with on the Tangle, the policy that must be satisfied to decrypt the token, and a list of access rights. This indicates that only the subjects whose attributes satisfy the policy in the token can decrypt the token and are thus granted the access rights recorded in the token. For instance, the token shown in Fig. 2 has been issued by `owner1` and is associated with the address `TZS..U` on the Tangle. Only subjects whose attributes satisfy the policy `Division:IS AND Role:Student` can perform the action `GET` on the resource `camera1`. Using this token structure, we design the overall architecture of the proposed scheme, which is illustrated in Fig. 3.

B. Access Right Authorization

In the authorization phase (i.e., Step 1 in Fig. 3), the object owner first decides the policy embedded into the token and the corresponding access rights to specify which group of subjects can perform what actions to the object. Examples of policies and access rights are shown in Fig. 4. The first example implies that subjects satisfying the policy "Division: IS AND Role: Student" will be authorized to perform the action "GET" on

Policy	Access Rights
Division: IS AND Role: Student	'GET' access to 'camera1'
Division: IS AND Role: Staff	'LOCK' access to 'smart key1' 'UNLOCK' access to 'smart key1'

Fig. 4. Examples of policies and access rights.

the resource "camera1". After deciding the policy and access rights, the object owner prepares a token according to predefined structure and encrypts it under the policy using CP-ABE. For the first example in Fig. 4, the object owner will issue a token as shown in Fig. 2, and then encrypt it under the policy "Division: IS AND Role: Student".

The owner then records the encrypted token to the Tangle as an MAM transaction (Step 2 in Fig. 3). Although the MAM transaction itself is public and visible to any peer, the token can be decrypted only by those with a private key associated with a set of attributes satisfying the policy. Subjects can obtain the encrypted token from the Tangle and decrypt it using the private keys issued by the authority (Step 3 in Fig. 3). In this way, once the owner has recorded an encrypted token to the Tangle, all subjects satisfying the policy can obtain the token and are authorized the access rights. On the contrary, in DCACI, the owner has to conduct the authorization (although the implementation is not provided) and token issuance processes once for every subject, which increases the burden of object owners. Our scheme not only alleviates the burden of the owner but also enables one-to-many access control. This means that one token is responsible for the access control of a group of subjects, while, in DCACI, one token is only for one subject.

C. Access Right Verification

After successfully decrypting the token, a subject can send the object owner an access request (Step 4 in Fig. 3). An access request is a JSON object consisting of the object to access, the action to perform, the token to present and the corresponding policy. The request is also encrypted using CP-ABE, so that there is no need to establish a secure communication channel between the subject and the object owner. The subject encrypts the request under some policy that allows only the object owner to decrypt it (e.g., "Role: Owner").

On receiving an access request, the owner decrypts it using the private key issued by the authority and verifies it. The verification process consists of two steps, token verification and request evaluation. In the token verification step, the owner fetches the original token (i.e., the one issued during authorization) from the Tangle (Step 5 in Fig. 3). The presented token is checked against the original token to verify its authenticity. Since the Tangle is tamper-proof, any modification in the token can be detected in this process. The access request is rejected if the token verification fails. Having passed the token verification, the request evaluation is performed based on the list of access rights contained in the token. If the requested action does not exist in the list, the request is rejected because it is an attempt of unauthorized access.

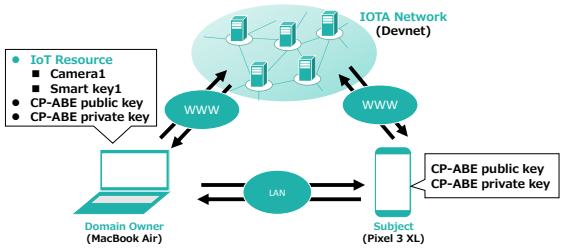

Fig. 5. System configuration of the prototype.

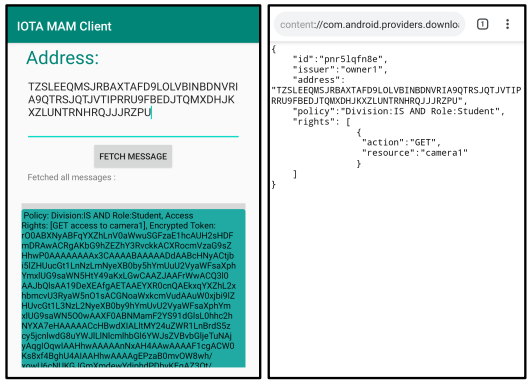

Fig. 6. Token fetching from Tangle (left) and token decryption (right).

V. Implementation

To show the feasibility of our scheme, we have implemented a proof-of-concept prototype using the IOTA Devnet [15].

A. System Configuration

As shown in Fig. 5, we used a MacBook Air (CPU: 1.8 GHz Intel Core i5, RAM: 8GB) as the object owner, and a Google Pixel 3 XL as the subject. The owner manages two IoT resources, "camera1" and "smart key1". The official JavaScript API [16] was used to issue and fetch MAM transactions, and implementation based on [17] was used to handle CP-ABE encryption and decryption. The owner service was implemented by an HTTP server which listens for requests from the subject. In addition, we integrated the CP-ABE key-issuing authority into the service. We developed a native Android application at the subject side, which can fetch MAM transactions from the Tangle, handle CP-ABE and fire access requests. Both the owner and the subject participate in the IOTA Devnet as clients and communicate with a full node (`https://nodes.devnet.iota.org`) to issue and fetch MAM transactions.

B. Access Right Authorization

For simplicity, we limited the tokens to the two illustrated in Fig. 4 (i.e., the student token and the staff token), and issued the subject a private key associated with the set of attributes {Division: IS, Role: Student}. Fig. 6 shows the result of fetching and decrypting the student token using the private key. We can see that the access right is successfully authorized via the Tangle to the subject.

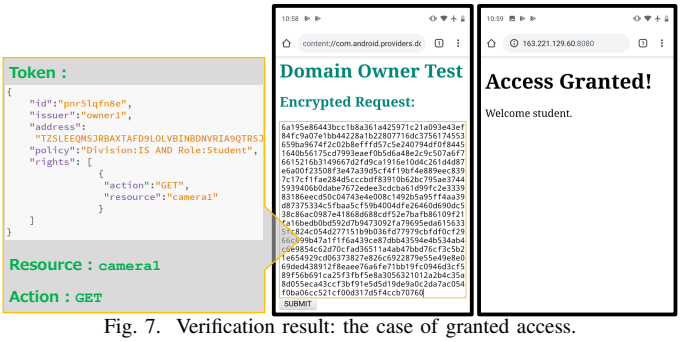

Fig. 7. Verification result: the case of granted access.

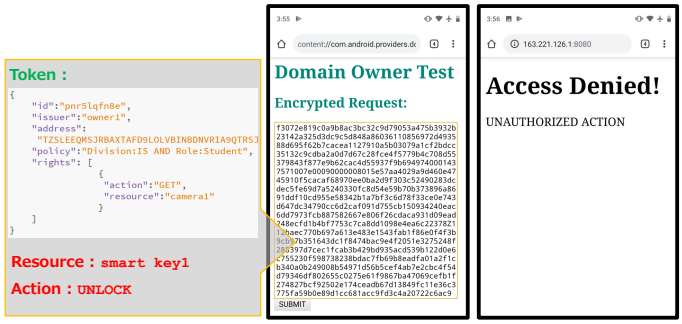

Fig. 8. Verification result: the case of denied access due to unauthorized action.

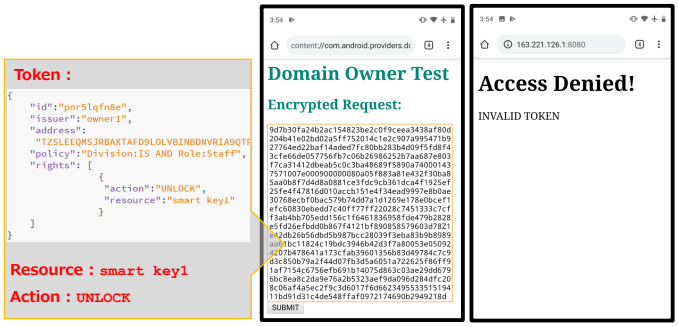

Fig. 9. Verification result: the case of denied access due to tampered token.

C. Access Right Verification

Fig. 7 shows the result of sending an access request containing "camera1" as the resource, "GET" as the action and the student token. In this case, the subject is authorized to perform the action "GET" on the resource "camera1", and the presented token is authentic. Therefore, access is granted.

On the other hand, Fig. 8 shows the result of sending an access request with "smart key1" as the resource, "UNLOCK" as the action and the student token. Although the token is valid, it does not contain the access right to the resource "smart key1". The owner thus rejects the request for unauthorized access.

Moreover, Fig. 9 shows the result of an attempt to perform the action "UNLOCK" on the resource "smart key1" using a tampered token. Based on the student token, its resource field, action field and the policy field were modified to "smart key1", "UNLOCK" and "Division: IS AND Role: Staff", respectively. The owner detects the falsification by checking the presented token against the original token fetched from the Tangle and rejects the request.

VI. Conclusions

In this paper, we have proposed an IOTA-based access control framework in which ABAC and CapBAC are combined by leveraging the CP-ABE technology. Thanks to CP-ABE, our scheme overcomes the drawbacks that exist in the previous framework named DCACI and provides more fine-grained and scalable access control. We have also shown the feasibility of our scheme by implementing a proof-of-concept prototype using the IOTA Devnet.

Acknowledgment

This work was supported in part by the Japan Society for the Promotion of Science (JSPS) KAKENHI (A) under Grant 19H01103, the Support Center for Advanced Telecommunications (SCAT) Technology Research Foundation and the Telecommunications Advancement Foundation.

References

[1] Gartner identifies top 10 strategic iot technologies and trends. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends/

[2] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying iot security: an exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[3] Y. Nakamura, Y. Zhang, M. Sasabe, and S. Kasahara, "Capability-Based Access Control for the Internet of Things: An Ethereum Blockchain-Based Scheme," in *Proc. of IEEE GLOBECOM 2019*, December 2019.

[4] M. Yutaka, Y. Zhang, M. Sasabe, and S. Kasahara, "Using Ethereum Blockchain for Distributed Attribute-Based Access Control in the Internet of Things," in *Proc. of IEEE GLOBECOM 2019*, December 2019.

[5] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, April 2019.

[6] Bitcoin - open source p2p money. [Online]. Available: https://bitcoin.org/en/

[7] Smart contracts. [Online]. Available: https://ethereum.org/developers/#smart-contract-languages

[8] The next generation of distributed ledger technology — iota. [Online]. Available: https://www.iota.org/

[9] S. K. Pinjala and K. M. Sivalingam, "Dcaci: A decentralized lightweight capability based access control framework using iota for internet of things," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, April 2019, pp. 13–18.

[10] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the internet of things: Big challenges and new opportunities," *Computer Networks*, vol. 112, pp. 237–262, 2017.

[11] S. Bhatt, F. Patwa, and R. Sandhu, "Access control model for aws internet of things," in *International Conference on Network and System Security*. Springer, 2017, pp. 721–736.

[12] S. Gusmeroli, S. Piccione, and D. Rotondi, "Iot access control issues: a capability based approach," in *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. IEEE, 2012, pp. 787–792.

[13] Introducing masked authenticated messaging-iota. [Online]. Available: https://blog.iota.org/introducing-masked-authenticated-messaging-e55c1822d50e/

[14] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, May 2007, pp. 321–334.

[15] Devnet - iota documentation. [Online]. Available: https://docs.iota.org/docs/getting-started/0.1/network/iota-networks/

[16] Masked authentication messaging wrapper for javascript (browser and node). [Online]. Available: https://github.com/iotaledger/mam.client.js/

[17] zlwen/cpabe-java: The implementation of ciphertext policy attribute based encryption in java. [Online]. Available: https://github.com/zlwen/cpabe-java/