Efficient Distributed Authentication and Access Control System Management for Internet of Things Using Blockchain

Hadjer Benhadj Djilali[1(✉)] and Djamel Tandjaoui[2]

[1] LSI, USTHB: University of Sciences and Technology Houari Boumediene, Algiers, Algeria
h.benhadjdjilali@usthb.dz
[2] Computer Security Division, CERIST: Research Center on Scientific and Technical Information, Algiers, Algeria
dtandjaoui@cerist.dz
http://www.usthb.dz, http://www.cerist.dz

Abstract. Internet of things (IoT) enables a huge network of connected devices inter-working and collaborating to provide relevant services and applications. This technology entered the market and is expected to grow in the upcoming years, as the critical questions related to the management and communication security continue to be challenging research problems. Current solutions of access control system management that enables communication between devices depend mainly on the use of digital certificates for authentication. However, such an approach imposes significant overhead on IoT devices since it is computationally demanding and requires validation of the certificate within a limited period. In addition, relying on a central node for deciding on issuing and revoking certificates introduces a single point of failure and could even risk the safety of personal information or physical damages related to IoT services. In this paper, we propose a new distributed authentication and access control system management for IoT by the use of Blockchain technology to keep track of the certificate of each IoT device (valid or revoked) in distributed and immutable records. In essence we replace certificate verification with a lightweight blockchain-based authentication approach. In addition, we propose a fully distributed IoT admission/revocation scheme. We show that our scheme could alleviate the computation overhead and enhance the response time while improving the overall system security.

Keywords: Internet of Things · Access control system management · Authentication · Blockchain · Security

1 Introduction

Today security and access control standards recommend the use of a Public-Key Infrastructure (PKI) with a centralized management for the creation, distribution and revocation of the digital certificates built around the notion of trust.

É. Renault et al. (Eds.): MSPN 2019, LNCS 11557, pp. 51–60, 2019.
https://doi.org/10.1007/978-3-030-22885-9_5

Typically, a PKI is mainly based on Certificate Authority (CA) that acts as a trusted third party to issue/revoke digital certificates. However, the use of a CA introduces a single point of failure in the IoT. Indeed, dramatic consequences could happen when the CA is compromised. Over the last decade, several cybersecurity attacks have been launched against CA networks [1,2] resulting into breaches, the inflicted damage includes hacking user accounts, issuing fake certificates and carrying out successful man-in-the-middle attacks [2]. Moreover, the inclusion of the certificate does not only introduce major computation overhead for performing the verification procedure but also imposes high communication overhead in terms of bandwidth. Additionally, it causes increased medium access contention and consequently longer message delivery delays. Basically, in order to include a certificate in a message an additional 145 bytes are required in every message sent as a result heavy traffic, network congestion and resource exhaustion.

To overcome the above-mentioned shortcomings, several schemes have been proposed; most of these schemes have focused on reducing the computation and communication overheads and only very, few of them have considered the single point of failure vulnerability. Although one may argue that the certificate authority can be equipped with redundant resources to make it continuously available, it may still become unreachable due to the instability of wireless links, especially when IoT devices are in motion. In this paper, we opt to overcome the shortcomings of existing solutions using the Blockchain technology.

Blockchain is one of the most revolutionizing technologies that can tremendously influence the future of various computer and communication systems [3]. Blockchain provides a secure shared database, ledger or log of transactions, without requiring a central trusted third party for its management. The consistency of the blockchain is guaranteed through a distributed consensus protocol where a set of participants (validators), in a trust-less peer-to-peer network, collaborate in a completely transparent way to accept only valid transactions. By design, every transaction is cryptographically encoded into a permanent record and it is almost impossible to modify any of them without being detected [3]. The full history of all performed transactions can be easily retrieved and checked by any entity in the network without requiring additional security mechanisms.

In this paper, we propose the use of blockchain as a mean to build a secure lightweight access control system of internet of things network, i.e., valid or revoked, in order to: (i) mitigate the single point of failure (central authority) vulnerability, and (ii) reduce the overhead of the authentication process (certificates exchanges and verification). In our proposed system, the admission/revocation of IoT device is performed in a completely distributed fashion. A set of blockchain validators, e.g., road side units, smart traffic lights panels, smart base transceiver station, smart light panels...etc any fixed smart objects that have processing and storage power, apply a distributed consensus protocol to decide about the admission/ revocation of a IoT device based on a set of predefined rules. For instance, to decide about the admission of IoT device, both the full IoT device's history that is already stored in the blockchain as well as certifi-

cates from the corresponding authorities such as the department of smart city, motor vehicle, manufacturer, insurance company, government etc. can be used. Similarly, the revocation of a particular IoT device, IoT_i, is performed by the validators based, for instance, on misbehaviour reports sent by the neighbours of such IoT device. Because the integrity and validity of the device state information in the blockchain is ensured and can be simply and securely accessed from anywhere, IoT devices no longer need to include a certificate in their messages to be authenticated by the receivers. To authenticate a sender of a message, the receiver can simply check if the sender's public key used to sign the message is already recorded in the blockchain with a valid status. This considerably reduces both the communication and computation overheads associated with the use of certificates.

The remaining of this paper is organized as follows. Section 2 provides a summary of the related work. Section 3 describes our proposed blockchain-based authentication and access control system scheme for IoT in detail. In Sect. 4, we discuss the system efficiency and evaluate its performances in comparison to traditional systems. Finally, Sect. 5 concludes the paper.

2 Related Work

Many researchers and company labs are coupling IoT technology with the blockchain technology to take advantage from each technology in purpose to improve their solutions. Indeed, a way to enhance the security of IoT networks and applications is the use of blockchain technology that is known for its high security and robustness.

Conoscenti et al. [4] conducted a systematic literature review on the blockchain for the Internet of Things. The survey described several papers that manage data collected by IoT devices. As an example, [5] describes a system to verify the identity of the data and [6] describes a method to preserve the data ownership of the IoT devices.

Cha et al. [7] proposed a design and a privacy-aware blockchain connected Gateway for Bluetooth low energy IoT devices, where the blockchain network is adopted as the underlying architecture for management of privacy preferences of the users from being tampered.

Zhang et al. [8] proposed a design of an access control policy framework based on XCAML language based on blockchain for IoT. Xu and Yu et al. [9] proposed a decentralized lightweight capability-based access scheme based on blockchain.

Reference [10], describes a cryptocurrency blockchain-based access control framework called FairAccess, a token-based access control model.

In [11], the authors propose an architecture for electronic commerce explicitly designed for IoT devices, based on the Bitcoin protocol. Distributed Autonomous Corporations (DAC) was used as a transaction entity to deal with data from IoT devices. In this model, the users can negotiate with DACs, using cryptocurrencies. Filament [12] it is a system designed to allow devices have unique identities and can discover, communicate, and interact autonomously with each other. Also, the devices involved can directly exchange value.

IOTA [13] it is a cryptocurrency explicitly developed for the selling of data from devices IoT. Instead of using a global Blockchain, the IOTA uses a DAG (Directed Acyclic Graph), the edges are the transactions, and the weights the number of times were confirmed.

Unlike the previous solutions presented in the above references, our proposed solution's goal: The design of efficient distributed authentication and access control management for internet of things using blockchain and not depending on the access control policy model implemented, Ensure a secure management access control system of IoT devices (registration, admission, misbehavior notification and revocation) in a totally decentralized manner to avoid single point of failure, A lightweight authentication scheme that eliminates the heavy computation resource to verify the digital certificate and enable authentications using simple lookup. As result we have a full control system management of the IoT network and a secure communication between the devices, furthermore our solution can be used for public government project or companies' private projects in order to secure their IoT networks from external unsafe network communications.

3 Bolckchain Based Efficient Authentication and Access Control System Management for IoT

In this paper, we propose a new blockchain-based authentication and access control system management mechanism for internet of things network. The design objective is to eliminate the single point of failure and reduce the communication and verification overheads, which exist in the centralized PKI while ensuring authentication. To achieve such an objective, the blockchain-based authentication mechanism for IoT has to ensure the following mandatory set of functionalities:

(1) Registering the public key of IoT devices.
(2) Validating the membership of IoT device's public key.
(3) Looking up/verifying the validity of IoT's public key.
(4) Revoking of IoT's public key from the network.

The detailed description of these functionalities' implementation is given in the balance of this section. Before that, we first provide an overview of our proposed system.

Due to IoT's limited characteristics features like the energy of the battery of IoT devices, we choose to implement the access control system with elliptic curve cryptography ECC [14] and Elliptic Curve Digital Signature ECDSA [15] algorithm for the digital signature to maintain the energy consumption instead pf using Public Cryptography RSA [16].

3.1 System Overview

Our goal is to enable large-scale deployment of IoT network while preserving its security. Traditional existing solution of IoT promote the use of PKI with

a centralized certification authority to ensure integrity, authentication and non-repudiation. However, such approach introduces a single point of failure and imposes heavy cost in terms of computation and communication overhead, which negatively affects the network performances and the IoT devices. Our proposed system leverages the use of blockchain technology to tackle these issues. Intrinsically, blockchain provides distributed, secure and immutable records of any kind of data. When putting the authentication information, such as certificates, on blockchain, exchanging and verifying such information becomes unnecessary. In addition, the distribution nature of blockchain eliminates the need of a trusted third party to manage and secure data, which leads to avoiding the single point of failure scenario and averting serious cyber threats (i.e., DoS attacks), which are possible in conventional PKI-based systems.

Figure 1 shows a general architecture of our system where the blockchain network is overlaid on top of the existing IoT network. In our proposed system, information about IoT admission/revocation are posted to a permissioned blockchain, where we refer to the entities writing such information as "validators". Thus, we eliminate the single point of failure by delegating decisions about IoT admission/revocation to a set of validators. We assign the validation role to a set of smart object of the city such as road side units, smart traffic light panels, base transceiver station, smart light panels...etc any fixed smart objects that have processing and storage power. As they are deployed over the whole smart cities's network, easily reachable by IoT devices and are generally interconnected by the mean of specialized link or over the Internet. In this permissioned blockchain, both IoT devices and authorities can only read from or submit transactions to the blockchain. By executing a distributed consensus algorithm, the validators decide to accept or reject the received transactions from both IoT devices and authorities.

In practice, the role of the authorities, such as the department of vehicles, e-government, manufacturers and companies ...etc. is to certify that a particular IoT conforms to membership requirements. However, instead of collecting all certificates from the different authorities into one single place for decision, in our system all certificates are pushed to the blockchain network then used by the validators for decision making in a fully distributed manner. This is very important from a security perspective, as there is no single entity controlling the admission of IoT devices to the network. In addition, for the revocation process, the decision for evicting a IoT device is performed by the set of validators instead of a single authority. IoT devices that detects misbehaviour send an embedded notification within the transaction to the blockchain, then the final decision about revoking a suspected IoT device is taken by the set of validators following some predefined rules. The admission/revocation information recorded in the blockchain are used by IoT devices to authenticate each other with a minimum communication and computation overhead.

A IoT device no longer needs to append its certificate to each message and the receiver has only to make a simple lookup to check if the sender has an entry in the blockchain with a valid status.

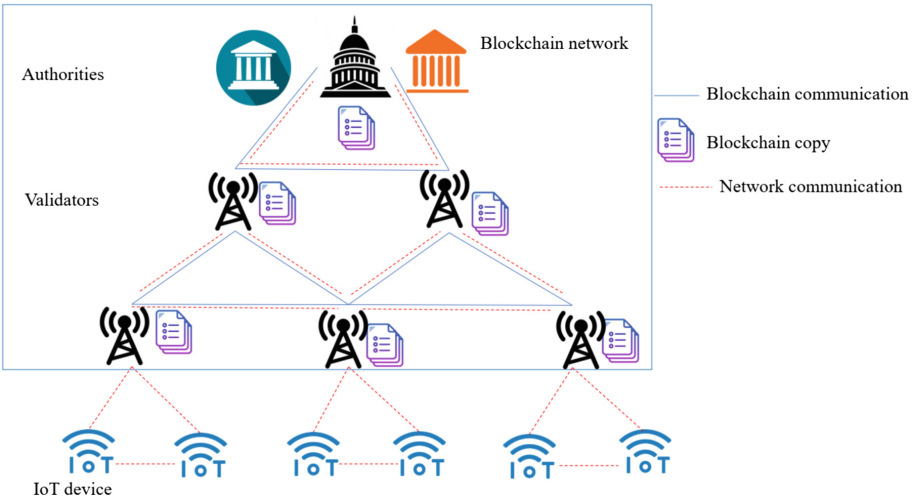

Fig. 1. General architecture of the system

3.2 IoT Device Registration

Before a IoT device IoT_i can join the network it needs first to generate a public-private key pair (pkIoT_i; skIoT_i), where the private key is kept secret and used to sign messages sent by IoT_i. The public key of IoT_i is made known to other IoT devices and is used by message recipients to verify message integrity, to authenticate the sender, and to check the membership status of IoT_i on the blockchain. To have a valid membership status on the blockchain, IoT_i needs to get enrollment certificates from corresponding authorities. Each authority a_j using its private key ska_j can issue a signed certificate to IoT_i if it is eligible. Finally, the obtained certificate is pushed to the blockchain network for validation through a registration transaction. The certificates are pushed by the according authorities and the transaction has the following format: $\langle$cert, registered, sig(sk_{a_j}, cert)$\rangle$, where cert is the generated certificate by the authority a_j, and sig is the signature of the certificate using sk_{a_j}. Mainly, the certificate contains the public key of the IoT device and the validity period.

3.3 IoT Device Admission

The blockchain network consists of a set of validators, $\text{M} = \{ \text{m}_1, \text{m}_2, \text{m}_3, .., \text{m}_k\}$, that execute a consensus algorithm to reach agreement about the state (authorization) of IoT devices. When the blockchain network receives a registration transaction from an authority to authorize a new IoT device, or reauthorize a revoked IoT device, the transaction will be accepted if it comes from an authenticated authority. When sufficient certificates for a particular IoT device IoT_i are received, one of the validators will generate a new admission transaction to add and mark the public key of the IoT device as valid in the blockchain.

The admission transaction has the following format: $\langle \text{pkIoT}_i, \text{valid}, \text{sig}(sk_{m_j}, pk_{IoT_i})\rangle$ of course the remaining validators will first check the correctness of the transaction before adding it to their local blockchain copy. The verification mainly consists of checking the validator's signature and that the concerned IoT device has sufficient certificates (registration transactions) on the blockchain.

3.4 IoT Device Authentication

Once a particular IoT device IoT_i is added and labelled in the blockchain as valid, it can join the network and start sending messages. Each IoT device that receives a message from IoT_i checks if the public key of IoT_i exists in the blockchain and is marked as valid. The receiver has to perform a simple lookup by searching the blockchain for a matching public key value. In contrast to a traditional PKI-based system, where the sender and the receiver have to include and verify a digital certificate, respectively, in our system a certificate is no longer included in the messages and the verification is replaced by a simple lookup function. The lookup function is much faster than the cryptographic signature verification of the certificate. This will considerably increase the performance of the system and improve the timeliness of incident announcements.

3.5 IoT Device Revocation

To enable a distributed revocation process, each IoT device IoT_j that detects misbehavior of IoT_i has to send a misbehavior transaction to notify the blockchain network. The misbehavior transaction has the following format: $\langle pk_{IoT_i}, \text{misbehavior}, \text{sig}(sk_{IoT_j}, Pk_{IoT_j})\rangle$, where pk_{IoT_i} is the public key of the suspected vehicle and sk_{IoT_j} is the private key of the IoT device that report the misbehavior. The validators will accept and add these transactions to the blockchain if they are originated from valid IoT device. These transactions will be later collectively considered to decide about whether revoking the membership of IoT_i is warranted. In order to revoke a suspected IoT device, a distributed revocation protocol will be executed by the blockchain validators. The revocation is generally based on rules set by a high authority and enforced by the validators. For instance, the validators can decide to revoke a particular IoT device IoT_i if more than n authentic misbehavior transactions for IoT_i are added to the blockchain in the past 24 h. If IoT_i is evicted from the network, one of the validators will create a revocation transaction and broadcast it to the blockchain network. The revocation transaction has the following format: $\langle pk_{IoT_i}, \text{revoked}, \text{sig}(sk_{m_j}, pk_{IoT_i})\rangle$, where pk_{IoT_i} is the public key of the IoT device to be evicted and sk_{m_j} is the private key of the validator. Once receiving the revocation transaction, the other validators will add it to the blockchain after checking the authenticity of its source. A summary of the different transactions used by our system is presented in Table 1.

Table 1. Summary of the used transactions

Transaction type	Sender	Transaction
Registration	Authorities	$\langle$cert, registered, sig(sk_{a_j}, cert)$\rangle$
Admission	Validators	$\langle \text{pkIoT}_i$, valid, sig(sk_{m_j}, pk_{IoT_i})$\rangle$
Misbehavior	IoT devices	$\langle pk_{IoT_i}$, misbehavior, sig(sk_{IoT_j}, Pk_{IoT_j})$\rangle$
Revocation	Validators	$\langle pk_{IoT_i}$, revoked, sig(sk_{m_j}, pk_{IoT_i})$\rangle$

4 Discussion

4.1 Storage Requirement and Optimization

1. **Multiple blockchains:** Instead of having only one blockchain that holds the different information related to IoT device registration, admission, misbehavior and revocation, each type of data can be stored in a distinct blockchain. In this case, IoT devices will use only the admission and revocation blockchains as they are sufficient to authenticate the source of any received message. Therefore, a considerable memory space can be saved.
2. **Cryptographic accumulator:** Another technique for optimizing the blockchain storage is by using cryptographic accumulator. As discussed in [12], the idea is to accumulate the set of valid IoT devices into one single digital object, where each IoT device IoTj will have a membership witness to prove that IoTj is already registered in the accumulator. In this case, only the accumulator will be saved on the blockchain, and vehicles have only to include their witness in their messages in order to allow the receiver to check the membership by applying a simple function. This will considerably decrease the size of the blockchain and can scale for very large network sizes without affecting the storage performance.

4.2 Performance Verification

By using a blockchain, the verification of IoT devices communication messages turns into a simple lookup to find whether the sender's public key exists with a valid status. In order to evaluate the verification time when using our scheme and compare it to the signature verification of digital certificate in conventional PKI, we have conducted the following experiment. To test the lookup function on a real scenario, we selected the Bitcoin blockchain as it is the largest existing one with millions of transaction entries. In Bitcoin, to speed up access and search operations, the levelDB database is used [3]. Bitcoin uses mainly two databases, the first one contains metadata about all known blocks and their location on disk. The second database contains a compact representation of all currently unspent transaction outputs (UTXO), in order to make it easier to validate a transaction for redeeming some bitcoins. It is worth noting that the database scheme can be customized to fit a specific requirement. In our experiment we calculated

the response time when searching for a particular transaction in the blockchain database. By using levelDB C++, we can access directly to the database and then search for a particular transaction by its identifier (TXID). Several queries have been issued in the experiments and the response time has been averaged. A summary of the used database and the hardware setup for the experiment is given in Table 2. The result, by averaging 1000 queries shows that the average required time to look up for a transaction is about 0:012 ms. Whereas, when verifying a digital signature, by executing the program "Openssl speed ECDSA" which gives the verification time of the ECDSA, the result is about 0:1 ms for a key size of 256. The advantage of using blockchain in this case is very clear as the verification delay is nearly dropped by a factor of 10.

Table 2. Experiment setup

CPU	8 ∗ Intel R Core(TM) i7-6700HQ 2.60 GHZ
CPU-cache	6144 KB
LevelDB	Version 1.1
Number of transactions	36328994

5 Conclusion

To sum up, using blockchain for securing authentication and access control management for internet of things is an efficient alternative to the traditional PKI-based systems. In this paper, we have presented a blockchain-based access control system management for IoT, which avoids the presence of a single point of failure and reduces both the communication and computation overhead. Our system take advantage of the distributed nature of the blockchain and the immutability of its records to provide a secure and lightweight authentication mechanism for inter IoT devices communication. Our system supports IoT devices registration, admission, misbehavior notification and revocation in a completely decentralized manner. Moreover, our system design eliminates the inherent heavy computation when verifying digital certificates and enables authentication using a simple lookup function. In summary, we believe that our proposed access system is a viable solution that offers better security and performance than the existing solutions.

References

1. Espiner, T.: Trustwave sold root certificate for surveillance (2012)
2. Fisher, D.: Final report on DigiNotar hack shows total compromise of CA servers
3. Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media Inc., Sebastopol (2015)

4. Conoscenti, M., Vetr, A., Martin, J.C.D.: Blockchain for the internet of things: a systematic literature review. In: The Third International Symposium on Internet of Things: Systems, Management and Security (IOTSMS 2016) (2016)
5. Wilson, D., Ateniese, G.: From pretty good to great: enhancing PGP using bitcoin and the blockchain. CoRR abs/1508.04868 (2015)
6. Zyskind, G., Nathan, O., Pentland, A.S.: Decentralizing privacy: using blockchain to protect personal data (2015)
7. Cha, S.-C., Chen, J.-F., Su, C., Yeh, K.-H.: A blockchain connected gateway for BLE-based devices in the internet of things. IEEE J. (2018). https://doi.org/10.1109/ACCESS.2018.2799942
8. Zhang, Y., Dukkipati, C., Cheng, L.C.: Decentralized, blockchain based access control framework for the heterogeneous internet of things. ACM (2018). https://doi.org/10.1145/3180457.3180458
9. Xu, R., Yu, C., Blasch, E., Chen, G.: A BLockchain-ENabled Decentralized Capability-Based Access Control for IoTs, BlendCAC (2018). https://arxiv.org/pdf/1804.09267.pdf
10. Ouaddah, A., Elkala, A.A., Ouahman, A.A.: Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In: Europe and MENA Cooperation Advances in Information and Communication Technologies (2017)
11. Zhang, Y., Wen, J.: An IoT electric business model based on the protocol of bitcoin. In: Proceedings of the 2015 18th International Conference on Intelligence in Next Generation Networks, ICIN 2015, pp. 184–191. IEEE, France, February 2015
12. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V.: Blockchain technology: beyond bitcoin. Appl. Innov. **2**, 6–10 (2016)
13. Popov, S.: The tangle (2016). https://iota.org/IOTAWhitepaper.pdf
14. Miller, V.S.: Use of elliptic curves in cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986). https://doi.org/10.1007/3-540-39799-X_31
15. Johnson, D., Menezes, A., Vanstone, S.: The elliptic curve digital signature algorithm (ECDSA). Int. J. Inf. Secur. **1**, 36–63 (2001)
16. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)