Blockchain-Enabled User Authentication in Zero Trust Internet of Things

Shanshan Zhao[1], Shancang Li[1](✉), Fuzhong Li[2], Wuping Zhang[2], and Muddesar Iqbal[3]

[1] Department of Engineering Design and Mathematics,
University of the West England, Bristol, UK
shancang.li@uwe.ac.uk

[2] School of Software, Shanxi Agricultural University,
Taigu, Jinzhong 030801, China

[3] London South Bank University, London, UK
m.iqbal@lsbu.ac.uk

Abstract. The Internet of Things (IoT) connects increasing number of smart devices, which makes the central authorities or third parties (e.g., cloud, fog, firewall, etc.) based authentication scheme very challenging. In recent, the blockchain shows great promises in IoT to provide secure and flexible authentication schemes. In this work, a blockchain enabled authentication scheme is proposed for IoT devices, which ensures a more secure and easily interoperable alternative to IoT systems. It makes it possible to switch smart devices from an untrust to a trusted data using blockchain.

Keywords: Internet of Things · Security · Blockchain · Authentication · Public key infrastructure

1 Introduction

The Internet of Things (IoT) is expected to have a strong influence on many areas (*e.g.*, smart city, smart home, healthcare industry, smart manufacturing, *etc.*) by providing interconnection and information exchanging [1,2]. Increasing number of smart devices are connected by the IoT, which makes the IoT become a growing complicated system and leads to many challenges, like security, privacy, authentications, *etc.* In existing IoT systems, the security requirements mainly relies on the type of applications it serves [3,4]. The authentication scheme in IoT ensures a more secure and easily interoperable alternative to IoT systems. However, the unprecedented number of smart devices makes it very challenge to guarantee every device connected to the IoT system is authenticated and certified. In existing systems, such as smart home [5], healthcare, industrial critical system (ICS), industrial IoT [6], supervisory control and data acquisition (SCADA) systems, public key infrastructure-based schemes have been widely used [7,8]. Most existing IoT systems are secured through following techniques:

D. Wang et al. (Eds.): SPNCE 2020, LNICST 344, pp. 265–274, 2021.
https://doi.org/10.1007/978-3-030-66922-5_18

– Authentication, ensure connected devices in the IoT can access the resource.
– Encryption, encrypt the data before transmission and passed to the storage device, ensure to protect the data from eavesdropping.
– Integrity, guarantee the genuine device and operating correctly, together with conformity and malware free for data in IoT.

1.1 IoT Authentication

This work focuses on the authentication of user and devices in IoT, which can help IoT system to manage smart devices that are mutually authenticated and verified. In may existing IoT systems, resource access control techniques are widely used to secure data and resources in the system. However, due to the diversity of devices in the growing IoT system, it is becoming difficult to use access control techniques due to the security principles and levels might be different for devices.

An IoT system usually contains diverse devices with different communication protocols, security levels, *etc.* A smart home system might use multiple connectivity techniques, like Low energy Bluetooth (BLE), RFID (radio frequency identification), WiFi, 3G/4G/5G, *etc.* Connecting devices using above techniques are usually not difficult due to most IoT devices supports one or more connectivity, and devices are usually authenticated using user-password or multi-factor authentication to verify device and access. The current trends suggest that many IoT systems requires IoT devices should be able to support secure socket layer and public key infrastructure (PKI), where the authenticity of users/devices were proven using digital certificates [9].

PKI based solution would ensure a level of trust of a user/device. In recent, the emerging blockchain technologies show promises in device authentication, which makes it possible to manage users/devices authentication and integrity of messaging between them using blockchain. The blockchain technology, can be seen as a decentralised ledger system, could enhance the security and ensure identity and access management. Devices can potentially be considered as an autonomous node in the system and every access attempt is verified and traced automatically.

On the other hand, the diversity of IoT devices makes it very challenging to run secure PKI. Authentication schemes, such as user-password based, multiple factor authentication, or Azure IoT, can be used to manage all devices. The MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol for smart devices in IoT using a publish/subscribe model, which is widely used in energy sensitive IoT applications. Different IoT applications require one or more protocols. However, the overhead generated by the protocol could be too much for resource constrained IoT devices, or device might not support the protocol.

In existing IoT systems, a number of authentication solutions have been developed, most of them significantly rely on application scenarios [10]. It is very challenging to support different types of devices in an authentication scheme that is also secure. However, it is possible to ensure devices are designed by following some security standards in design. To provide IoT systems with strong secure authentication, each devices needs to be authenticated before grantee the access.

1.2 Blockchain

The blockchain technology is a decentralised ledger system that maintains a growing chain of verified blocks, which records generated transactions and data. The blockchain technology can provide excellent traceability, immutability, and transparency, which can well help in verification the authenticity of access in IoT.

Basically, a blockchain system computes a cryptographic hash as unique identification for each record or transactions. The one-way hash function cryptographically generates the same hash value when given the same input, which is a perfect way to verify the authenticity of the input. When slight change is made on the input, it will cause dramatically different hash value. The blockchain can be distributed across all participants and each participant keeps an identical copy of the ledger. In each block, the records were verified and immutable.

The blockchain can further enhance the trustworthiness of users/devices, and data in an IoT system. The blockchain can offer user to anonymously perform secure. Meanwhile, the integrity of it is continuously being verified by the entire network as opposed to a central entity such as a central server or authority. This way, each participant do not have to trust a central entity but security is guaranteed by the strength and computing power of the entire system participating in the blockchain.

2 Blockchain-Enabled Device Mutual Authentication

In blockchain system, each participant holds a public key pair as their address. The network will validate the transaction and after that will start to add the transaction to the blockchain. The blockchain technology can be used for many areas, including e-voting, supply chain, *etc.* In zero trust IoT (zIoT) environment, blockchain can be used to authenticate every individual device without a central authority. Each individual entity can use its key information, such as name, unique identity, id, serial number, *etc.*, to register its identity on the blockchain that can be verified based on its hash value earlier registered on the blockchain.

One challenge is that the blockchain requires all participants to reach a consensus result to make sure it is trustworthy and independent of controlling organisations. In zIoT scenarios, users or devices need to be motivated in a blockchain which can be used for authentication tasks.

For dynamic access, such as a device joining/leaving the zIoT system, its identity need to be well dealt with in blockchain. In case of leaving the system, the decentralised authentication provider based on blockchain technology.

As a good counterpart to the identity authentication/verification protocol, the blockchain technology can verify its own data integrity without requiring for a third party. In a blockchain network, the validity and security can be guaranteed using hash values, while the access control can be coordinated using smart contracts.

In a blockchain based authentication system, only the device/user owns the private key, which can be used to verify its ownership when an IoT service/application needs a proof of identity. The generated data can be stored on a blockchain, the IoT service/application do not have to worry about correctness and ownership of the data.

In this work, we propose a blockchain-enabled device authentication solution for zero trust IoT (BazIoT), which provides a new way to manage device/identity authentication with following features:

- BazIoT utilises blockchain in zIoT by enabling user to verify user/devices and their data without the need for a central entity, which can help reduce the use of third-part validation and further reduce the data breaches or incidents.
- It provides impeccable security, by storing data in blockchain and eliminating single points of failure inherent to centralised system.
- The BazIoT follows 'never trust, always verify' principle to stop malicious access to the data, which verifies each attempt of access to the resources.
- Unlike existing solutions, the BazIoT enables user/device owners fully control their data, in which blockchain network helps users to be in charge of their data and control the access right to these data.

However, in BazIoT, there are still a number concerns need to be addressed

- Incentivising the node, the BazIoT requires different participants, which requires extra computation resources;
- Permanent loss of access, in BazIoT the only way to gain access to the data is through a private key. If a user lose the key, there would be no way to get a new private key used for data access.
- Scalability, the BazIoT tends to get rather complex and fact, scalability could be a huge hurdle for public blockchains.
- Alterability of the data, the nature of immutability of blockchain guarantees the data validity but in IoT scenarios, extra option is needed to make the data owner be able to alter their data.

2.1 Self-sovereign Security

As mentioned above, the blockchain-based authentication system could significantly reduce the identity theft and data breaches. Meanwhile, it can also offer self-sovereign identities and security, enable device/user to fully control their own identity and data.

Self-sovereign security means in the sub IoT system (e.g., smart home), the user holds control of their security and all its attributes (including authentication, encryption, integration, privacy, etc.) and is not dependent on any single issuer or versifier to be online or available at the time of using the device. The self-sovereign security can ensure that device/user control their identity and data and share minimised attributes in the system.

The self-sovereign security system puts the users and device at the heart of the centre of security and its own data, in which smart contract can be used for device/user identity registration on blockchain network, and therefore resilient to censorship and server failure. It enable user/device fully control their identity data and access of their owned resources.

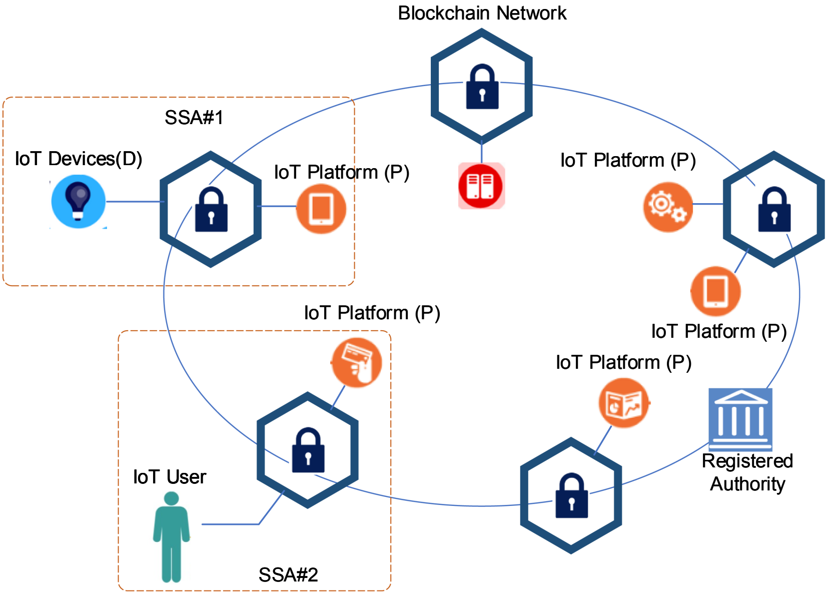


Fig. 1. Blockchain enabled zero trust IoT architecture.

The self-sovereign security can help to give back to the user/device full control on its identity and data, which enable user/device be the central of their own identity and data. There is no central authority needed for the entire IoT system.

2.2 Challenges

The main challenge that authentication of identity by blockchain faces is the involvement of different independent participants to calculate the blockchain to make it trustworthy and decentralised. How to implement consensus of participation is yet to be seen. In recent, the mutual distributed ledger identity schemes have been developed to enable secure the data storage, management, secure access in financial, healthcare, industrial sectors, as shown in Table 1.

New requirements for IoT device is *serverless, paswordless, self-sovereign security*, the decentralised blockchain technology is a perfectly tool to guarantee identity, trust, interoperability. It can also implement decentralised platform that enable secure cryptographic identity management. On the other hand, the blockchain can make the self-sovereign identity/security become a reality.

Table 1. Existing blockchain-based authentication schemes

Solution	Description
Civic [11]	Blockchain enabled biometrics identity manage system on mobile device, supporting multi-factor, without user-password
Helix [12]	Blockchain enabled digital identity system, supporting multiple participants share both self-asserted and verified information
Vida identity [2]	Identity authentication enables distributed key revocation and re-issuance
Spidchain [13]	Self-sovereigh identity, allow individuals to create, recover, revoke identifier, to sign and verify files and claims, etc.
BitID [14]	Bitcoin based authentication protocol, authenticates addresses by signing cryptographic challenge
Clear.me	Verified identity claims are signed by issuers, encrypted, and stored via the blockchain
Digi-ID [15]	DigiByte blockchain based authentication method allowing user to log in to a site, app by simply scanning or tapping on a QR code
CerCoin [16]	Namecoin-based blockchain authentication system that maintains a public ledger of domains and associated public keys
Trusted key [17]	Self-sovereign identity platform based on Ethereum, which offers mobile identity, id verification, password-less login, supports IoT
Ockam [18]	ERC20 based blockchain that registers IoT devices to solve systemic security and interoperability problems

3 Proposed Device Authentication in zIoT

As mentioned in Table 1, a number Blockchain based authentication has been developed and most of them focus on the identity authentication in cloud, blockchain systems. In this work, we will introduce a mutual authentication scheme for devices in the zIoT, in which all devices need to be verified before granting access to the zIoT by following the principle of "never trust, always verify".

In zIoT, the self-sovereign security area (SSA) is dynamic, as shown in Fig. 1, the IoT user/device A belongs SSA #1 and IoT user/device B belongs SSA #2. When A finishes the access session, the SSA #1 will be dismissed and new SSA will be established for new successful access. Actually, the roles of devices can be switched from resource owner to resources requester depends the application scenarios. All key events will be recorded in blockchain and the procedure is coordinated using smart contract.

The proposed protocol verifies to both the authentication participants. The user is the entity attempting to gain access to the protected resource in zIoT [19].

1. The user/device logs with a password-less scheme, with a authentication request ask authentication for accessing resources in an IoT systems.
2. The authentication request would simply encode the $\{blockchain\ address\}$ using public key of the resource owner in zIoT.
3. The resource owner verifies the request and send back a response.

The blockchain enabled protocol can prevents critical cyber attacks in zIoT, including, spoofing attack, phishing attack, the main-in-the-middle, replay attack, *etc.* In this solution, the verification and encryption (AES) keys are stored on the blockchain and the signing and decryption keys are stored on the device, which can enable the devices can fully control its resources and data.

In a zIoT system, at the IoT device/user side:

(1) The device retrieve the RSA public key P of the verifier in zIoT, which will be used to encrypt blockchain address of the IoT device/user as $(addr, P)$ and then send to the IoT platform;
(2) When the verifier receives the request, it will extract the $addr$ using the P, then the zIoT retrieve the RSA public key D of the device/user from the blockchain, and then generate a random string and timestamp *nonce* that then will be sent to the device/user;
(3) The device/user decrypts the received *hash* and then and sends back to verifier in a encrypted envelope.
(4) The verifier verifies the digital signature and confirm the authentic of the access.

As shown in Fig. 2. The identity addresses private key is derived from user keychain phrase that user chooses to use to sign in to the app. It never leaves the user's instance of the browser. This private key signs the authentication response token for an app to indicate that the user approves sign in to that system. The BazIoT is designed to protect enterprise-level zIoT from potential security breaches using blockchain-enabled mutual verification.

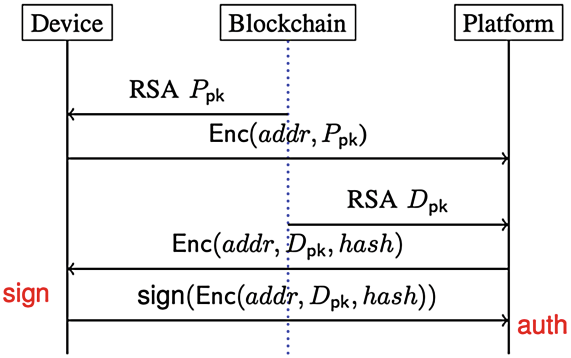
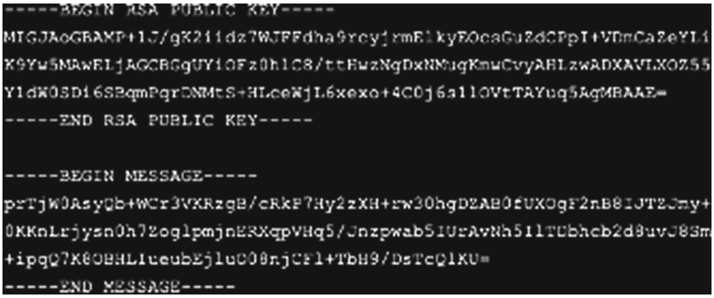


Fig. 2. BazIoT authentication flow

4 Evaluation

Decentralised authentication is more efficient. The BazIoT eliminates the need for reliance on third parties for document authentication and allows users to select their own solution based on their needs. In this work, we use a very simple blockchain to implement the proposed BazIoT.

In BazIoT, the identifier of a device/user could be one or combination of *name, account number, imei number, address, serial number, etc.* In this work, we use device *serial number* as their identifier, as {“device_id”: “test-id-z2832”}, the keys generated as shown in Fig. 3.



```
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAMP+1J/gK2iidz7WJFFdha9rcyjrmE1kyEOcaGu2dCPpI+VDmCa2eYLi
K9YwSMAwELjAGCBGgUYiOFz0h1C8/ttHwzNqDxNMugKmwCvyAHLzwADXAVLXOZ55
Y1dW0SDi6SBqmPqrDNMtS+HLceNjL6xexo+4C0j6s11OVtTAYuq5AqMBAAE=
-----END RSA PUBLIC KEY-----

-----BEGIN MESSAGE-----
prTjW0AsyQb+WCr3VXRzgB/cRkF7Hy2zXH+rw30hgDZAB0fUXOgF2nB8IJTZJmy+
0KKnLrjysn0h7Zog1pmjnERXqpVHq5/JnzpwabSIUrAvNh5I1TUbhcb2d8uvJ8Sm
+ipqQ7K8OBHLIueubEj1uO08njCFl+TbH9/DsTcQ1KU=
-----END MESSAGE-----
```

Fig. 3. Keys generated in BazIoT

In the blockchain, we assume IoT platform is the verifier that verifies an IoT device. The blockchain addresses of device and platform are: ‘0xdf1256d ffa2342ef9da8ed5862ebf732b12972a3', and '0xce1473fdea4235db9ce83d28721bf7 b2d12982c5', respectively. In this work, AES symmetric encryption is used to encrypt data transmission.

In practical systems, the procedure of BazIoT consists three main steps:

Initialise. This stage the BazIoT creates initialisation for a device that wants to access the resource in IoT, key parameters include {*device-id, blockchain address, , , authentication-id, RSA-, RSA-*}, and AES parameters $\mathsf{dpk}, \mathsf{iv}, \mathsf{tag}$;

Authentication. An IoT device first extract the RSA public key of the platform (IoT resources) P, and then encrypts its blockchain address using (P, add), which then will be sent to the resource holder (platform). The platform can decrypts the cipher using (P, add), and then create a 4096-bit *nonce*,

$$H_{nonce} = sha512(nonce \mid\mid timestamp) \tag{1}$$

The hash then will be encrypted using the public key of device D as (D, H_{nonce}). When receives the encrytped message, the device is able to decrypt and then sign the hash value using its private key. Together with the blockchain address and hash value, the digital signature then will be enveloped into a encrypted envelope using P, which then is sent back to platform.

Verification. When receives the encrypted envelope, the platform can decrypt it using P and extract the $\{address, hash, signature\}$, if the signature is valid, then returns 'accept', else returns 'reject'.

5 Conclusion

This work investigated the device/user authentication in zero trust IoT environments. A passwordless device authentication scheme is proposed that can provide enhanced security for IoT, meanwhile, it supports the dynamic authentication of IoT devices like joining/leaving. All access to the resource in the IoT system will be verified before granting access.

References

1. Sharma, V.: An energy-efficient transaction model for the blockchain-enabled Internet of vehicles (IoV). IEEE Commun. Lett. **23**(2), 246–249 (2019)
2. Li, S., Choo, K.R., Sun, Q., Buchanan, W.J., Cao, J.: IoT forensics: Amazon echo as a use case. IEEE Internet Things J. **6**(4), 6487–6497 (2019)
3. Xu, L., He, W., Li, S.: Internet of Things in industries: a survey. IEEE Trans. Ind. Inform. **10**(4), 2233–2243 (2014)
4. Yazdinejad, A., Parizi, R.M., Dehghantanha, A., Choo, K.R.: Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks. IEEE Trans. Netw. Sci. Eng. 1 (2019, in press)

5. Jangirala, S., Das, A.K., Vasilakos, A.V.: Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment. IEEE Trans. Ind. Inform. **16**, 7081–7093 (2019)
6. Li, S., Xu, L.D., Zhao, S.: The Internet of Things: a survey. Inf. Syst. Front. **17**(2), 243–259 (2015)
7. Yang, D., Jeon, S., Doh, I., Chae, K.: Randomly elected blockchain system based on grouping verifiers for efficiency and security. In: 2020 22nd International Conference on Advanced Communication Technology (ICACT), pp. 159–165 (2020)
8. Haddad, Z., Fouda, M.M., Mahmoud, M., Abdallah, M.: Blockchain-based authentication for 5G networks. In: 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), pp. 189–194 (2020)
9. Li, S., Qin, T., Min, G.: Blockchain-based digital forensics investigation framework in the Internet of Things and social systems. IEEE Trans. Comput. Soc. Syst. **6**(6), 1433–1441 (2019)
10. Li, S., Zhao, S., Yang, P., Andriotis, P., Xu, L., Sun, Q.: Distributed consensus algorithm for events detection in cyber-physical systems. IEEE Internet Things J. **6**(2), 2299–2308 (2019)
11. Civic: Flexibility without oversharing your identity (2020). https://www.civic.com/wallet/
12. Helix: Building trusted digital identity (2020). https://blockchain-helix.com/
13. Spidchan: Spidchain (2020). https://gomedici.com/companies/spidchain
14. BitID: Bitcoin authentication open protocol (2020). https://github.com/bitid/bitid
15. Digi-ID: Authentication at its best (2020). https://www.digi-id.io/
16. Feng, T., Chen, W., Zhang, D., Liu, C.: One-stop efficient PKI authentication service model based on blockchain. In: Si, X., et al. (eds.) CBCC 2019. CCIS, vol. 1176, pp. 31–47. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-3278-8_3
17. Wood, M.: Blockchain digital identity startup trusted key acquired by workday (2020). https://www.ledgerinsights.com/workday-blockchain-digital-identity-trusted-key/
18. Simone, S.D.: Ockam brings blockchain serverless identification to IoT devices (2020). https://www.infoq.com/news/2019/01/ockam-blockchain-iot-identity/
19. Nagpal, R.: Blockchain-based authentication of devices and people (2018). https://medium.com/blockchain-blog/blockchain-based-authentication-of-devices-and-people-c7efcfcf0b32