Blockchain-PUF-Based Secure Authentication Protocol for Internet of Things

Akash Suresh Patil, Rafik Hamza, Hongyang Yan, Alzubair Hassan, and Jin Li(✉)

School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou 51006, People's Republic of China

Abstract. Devices constituting the Internet of Things (IoT) have become widely used, therein generating a large amount of sensitive data. The communication of these data across IoT devices and over the public Internet makes them susceptible to several cyber attacks. In this paper, we propose an efficient blockchain approach based on the secret computational model of a physically unclonable function (PUF). The proposed framework aims to guarantee authentication of the devices and the miner with a faster verification process compared to existing blockchain techniques. Furthermore, the combination of the blockchain and PUF allows us to propose an efficient framework that guarantees data provenance and data integrity in IoT networks. The proposed framework employs PUFs, which provide unique hardware fingerprints for establishing data provenance. Smart contracts based on the blockchain provide a decentralized digital ledger that is able to resist data tampering attacks.

Keywords: Blockchain · Physically Unclonable Function · Authentication · Internet of Things · Data integrity

1 Introduction

The rapid development and evolution of miniaturization and electronics as well as the massive deployment of communications and networking technologies have bestowed unprecedented advances onto the world [1]. This trend has emerged in a number of electronic devices in every field of work, reducing human effort and increasing the cost of productivity. This rapid development is facilitating a shift toward the digital world.

The Internet ensures fast and efficient communication, which facilitates societal advancement. In recent decades, digitalization has seen significant progress, with developments that can be achieved and implemented through the Internet and through the concept of the Internet of Things (IoT). IoT has emerged as an encapsulate of various technologies, from radio frequency identification to wireless sensors networks to physical sensors [2]. Indeed, IoT equipment with

S. Wen et al. (Eds.): ICA3PP 2019, LNCS 11945, pp. 331–338, 2020.
https://doi.org/10.1007/978-3-030-38961-1_29

micro-controllers, digital communication transreceivers and protocol stacks that allow communication has become an integral part of the Internet. IoT devices can be applied in many research areas as electronic devices, from wearable devices to physical hardware development platforms [3,4].

Security issues have become the most challenging problem facing IoT [5]. It is essential to provide security because IoT systems are directly involved in human safety. A large number of IoT devices are connected in a system and are not managed by a single controller [6]. The design of security protocols is complicated due to the aforementioned issues.

Most security protocols are reliable for the Internet; however, they are not satisfactory for IoT systems [7–9]. Modern security protocols must be resistant to physical and side channel attacks, in addition to preserving anonymity and privacy. Additionally, modern security protocols must be efficient when used in IoT devices because they have very low computational, power and memory resources [10–12]. Thus, new security protocols and frameworks are required for establishing a secure and reliable IoT system.

In this paper, we present a blockchain-based architecture for IoT security. Moreover, we propose an authentication framework between IoT devices and miners in a blockchain network. Our work contributes to achieving identity authentication, access control, replay attack resistance, DOS attack resistance and data integrity without incurring overhead or delays. The unique features of the physically unclonable function (PUF) offer hardware security for IoT devices because a PUF carries a unique identification number for every chip at the time of manufacture, thereby offering data provenance.

In the next section, we will present the background of the presented material and challenges. In Sect. 3, we present our system architecture and the proposed framework's information work-flow. In Sect. 4, Security evaluations are discussed. Finally, the conclusions are given in Sect. 5.

2 Background and Related Works

2.1 Physical Unclonable Function (PUF)

The PUF is defined as a digital fingerprint that offers unique identification for semiconductor devices such as microprocessors. PUFs are based on unique physical variations developed during manufacturing. In short, a PUF is a physical entity embodied in a physical structure [13]. A PUF is based on the concept that even though the mask and manufacturing process are the same for every integrated circuit (IC), each IC is quite different from other ICs due to normal manufacturing variability. PUFs hold this variability to derive secret information that is unique to the chip. PUFs are promising novel primitives that can be used for secret key storage and authentication without the need for expensive hardware [14,15]. PUFs derive their secrecy from the physical characteristics of the IC. Thus, there is no need to store secrets in digital memory.

2.2 Blockchain

The first record of blockchain technology came in 2008 by mysterious founders using the name Satoshi Nakamoto [16].

Basically, a blockchain is a time-stamped chain of blocks jointly maintained by every participating node. Each block is chained together cryptographically. Blocks are digitally signed and chained to a previous block using their hash values. Blockchain technology is completely distributed, restricted to the given contractual code, autonomous and fully traceable [17].

2.3 Challenges

The IoT environment encapsulates millions of devices, and each device should be authenticated to the network before establishing communication. Because there is no human intervention in an IoT system, every IoT device should be equipped with a way to identify and authenticate themselves. However, modern techniques require secret credentials to be stored in the device memory. Unfortunately, these modern techniques are not well suited for the physically unprotected devices that are part of IoT systems [18]. An adversary may use various physical attacks to manipulate the entire IoT system.

Another issue relates to physical and cloning attacks, where an adversary may attempt to imitate a genuine and authenticated IoT device by cloning other IoT devices by extracting secret information [15]. The main intention of an attacker is to manipulate and access the IoT data sent by the other IoT devices. An attacker can eavesdrop on the communication by introducing a new message, change or replay messages, or establish other identities.

3 Proposed Framework Based on PUF Model

3.1 System Architecture

In this section, we introduce our system architecture equipped with various entities, such as the IoT devices, blockchain networks and the data owner, as shown in Fig. 1.

In our system, we have three participants: the IoT devices, the blockchain network and the data user.

- Various physical objects are merged to become smart objects, along with sensors and actuators, allowing the collection and processing of data from the real world.
- A peer-to-peer network, where every node may be a high-resource device. This network imbues our system with a distributed nature. Every node in the blockchain acts as a server/miner and maintains the history of all transactions. The blockchain is the mechanism that allows transactions to verify and provide the distributed, immutable, transparent, auditable and secure features. Additionally, every node of the blockchain network is responsible for data storage and providing the required computations.

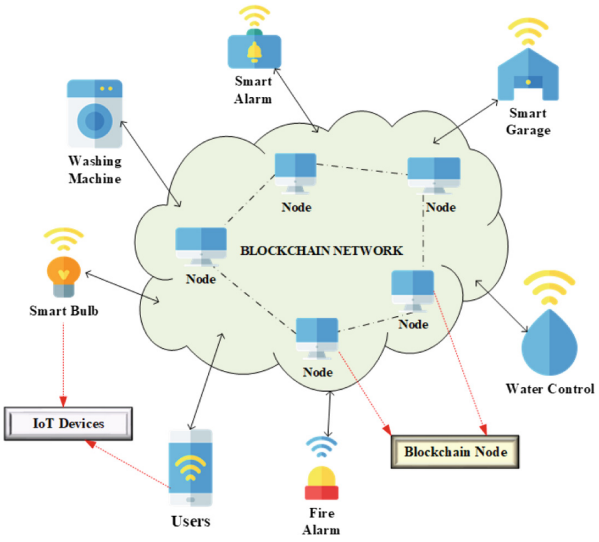

Fig. 1. The proposed system architecture

– A data user is an entity who has authority to provide their own personal data. They have full control over their data and set data access policies for intended purposes only. By adopting the blockchain and PUFs, data integrity, data provenance, and data tampering resistance can be achieved for the owner of the data.

3.2 Enrollment Phase

First, the IoT devices will request a node/miner in the blockchain network for registration. Then, this node/miner will store the registration details in local storage in a database. After successfully storing these details, the node/miner will be approved by the IoT devices (see Fig. 2). Simultaneously, the node/miner will broadcast the registration to the whole blockchain network, which will be confirmed to the user.

3.3 Verification Phase

When a user wants to interact with the node/miner, the user has to request permission; the node/miner will query this permission from local storage. Then, the node/miner will broadcast the request signed by the node/miner to the blockchain network. Once the blockchain network verifies the request, the user can interact with the IoT devices (see Fig. 3).

Our proposed work presents a unique approach to authentication using blockchain based smart contracts along with the PUF model, which offers a dense solution for secure authentication. Basically, our proposed solution will interact

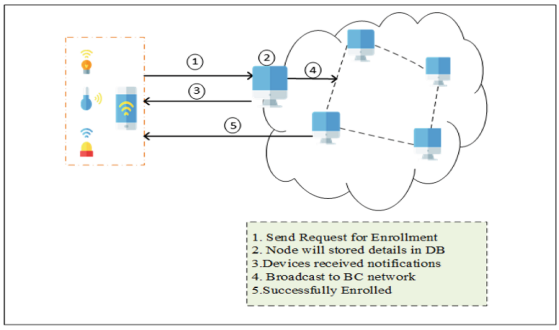

Fig. 2. Enrollment phase

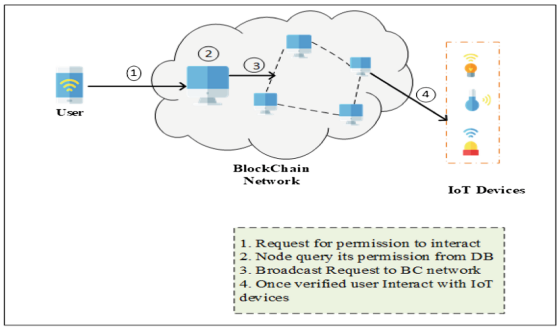

Fig. 3. Verification phase

with a blockchain based smart contract to ensure safe and secure communication. A smart contract is designed in such a way that the data coming from the IoT devices will interact with the distributed nodes in the blockchain network. Initially, all devices will need to enroll following their respective device ID and secret computational PUF model with the smart contract. Figure 4 presents the information flow of the entire IoT system.

4 Analysis

In this section, we illustrate some perspectives on evaluating the proposed PUF-based blockchain.

1. **Faster verification process**
   Existing PUF-based blockchain techniques require storing lists of challenge-response pairs (CRPs) in the database on the verifier side [19]. Therefore, collecting new CRPs from devices and storing them will become an exhaustive task and require unnecessarily storage and computations, especially under resource-constrained environments. We intend to overcome these problems by

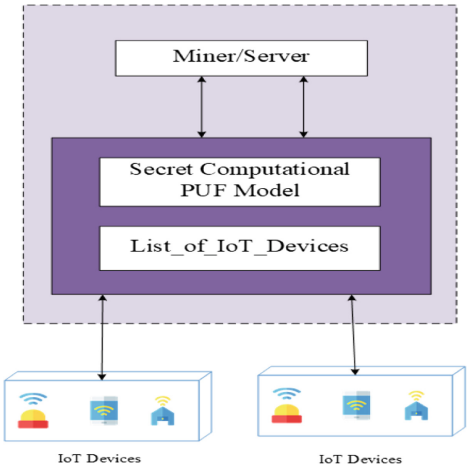

Fig. 4. The information flowchart of the IoT system.

proposing a new approach with minimally intensive processes on the database on the verifier side.

2. **Authentication of the devices and the miner**
   In the proposed PUF-blockchain model, IoT devices are authenticated with miner nodes after validating the *ID, MAC address, and secret computational model (PUF model)* parameters. The challenge-response protocol concatenation with hash ID transactions that will be verified with the stored hash *IDs* on the miner side at the time of enrollment. This guarantees a secure authentication of the devices in IoT networks.
   The server/miner will perform authentication using the device parameters that have been established in the previous transactions. The miner node will receive an *ID* from the users, and accordingly, it will send challenges or reject their requests. The parameters received from legitimate devices are checked and used to decide whether to continue or terminate the process.
3. **Data provenance and data integrity**
   The use of PUFs and the features of the blockchain ensure data provenance and data integrity for IoT environments [20]. The blockchain employs hash functions that confirm data integrity, while the unique ID in the PUF model guarantees data provenance for each IoT device. The blockchain holds a list of transactions between users, which are user data that are robust to tampering. This provides immunity from impersonation attacks. The blockchain offers an immutable chain of records; all the data transmitted previously are validated and then stored in the blockchain in such a way that these data cannot be altered by attackers.
4. **Resistance against replay attacks**
   Every step of the timestamp is used to check the data freshness, including all hash lists when transmitting the transactions. Thus, the proposed framework is well protected against replay attacks and can withstand such attacks.

5. **Resistance against man-in-the-middle attacks**
   The proposed scheme guarantees resistance against man-in-the-middle attacks. The sender is validate and verified by the receiver before processing any transactions.

Additionally, the security evaluation of the proposed framework illustrates a high level of security. The smart contract stores the full list of registered device IDs, MAC addresses and PUF models during the enrollment phase. Thus, it is nearly impossible for attackers to apply well-known attacks such as denial of service attacks, distributed denial of service attacks, and impersonation attacks. The smart contract maintains the list of registered IoT devices and the respective PUF model, along with the MAC addresses of the IoT devices, thereby offering trustworthiness for user access policies and user data usage records.

5 Conclusion

In this paper, we present an emerging technology: the PUF-based blockchain. The proposed framework ensures authentication for users and data integrity in IoT systems. Our proposed method represents an efficient and secure method for interaction between IoT devices and a miner in a blockchain network. Distributed ledgers and smart contracts carried out on the blockchain guarantee data integrity and user privacy. Cryptographic operations are implemented to enhance the blockchain protocol and ensure secure, efficient and more reliable authentication protocols. The proposed PUF-based blockchain can be employed as an efficient solution to preserve data integrity and facilitate authentication as well as reduce the computation power for IoT devices as PUF equipped in it.

Acknowledgment. This work was supported by National Natural Science Foundation of China (No. 61702125, 61702126).

References

1. Lu, Y., Xu, L.D.: Internet of Things (IoT) cybersecurity research: a review of current research topics. IEEE Internet Things J. **6**(2), 2103–2115 (2019)
2. Bedi, G., Venayagamoorthy, G.K., Singh, R., Brooks, R.R., Wang, K.: Review of Internet of Things (IoT) in electric power and energy systems. IEEE Internet Things J. **5**(2), 847–870 (2018)
3. Ikpehai, A., et al.: Low-power wide area network technologies for Internet-of-Things: a comparative review. IEEE Internet Things J. **6**(2), 2225–2240 (2019)
4. Udoh, I.S., Kotonya, G.: Developing IoT applications: challenges and frameworks. IET Cyber-Phys. Syst.: Theor. Appl. **3**(2), 65–72 (2018)
5. Frustaci, M., Pace, P., Aloi, G., Fortino, G.: Evaluating critical security issues of the iot world: present and future challenges. IEEE Internet Things J. **5**(4), 2483–2495 (2018)
6. Arif, M., Wang, G., Wang, T., Peng, T.: SDN-based secure VANETs communication with fog computing. In: Wang, G., Chen, J., Yang, L.T. (eds.) SpaCCS 2018. LNCS, vol. 11342, pp. 46–59. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-05345-1_4

7. Patil, A.S., Tama, B.A., Park, Y., Rhee, K.-H.: A framework for blockchain based secure smart green house farming. In: Park, J.J., Loia, V., Yi, G., Sung, Y. (eds.) CUTE/CSA -2017. LNEE, vol. 474, pp. 1162–1167. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-7605-3_185
8. Granjal, J., Monteiro, E., Sá Silva, J.: Security for the Internet of Things: a survey of existing protocols and open research issues. IEEE Commun. Surv. Tutorials **17**(3), 1294–1312 (2015)
9. Muhammad, K., Hamza, R., Ahmad, J., Lloret, J., Wang, H., Baik, S.W.: Secure surveillance framework for IoT systems using probabilistic image encryption. IEEE Trans. Ind. Inf. **14**(8), 3679–3689 (2018)
10. Nguyen, V., Lin, P., Hwang, R.: Energy depletion attacks in low power wireless networks. IEEE Access **7**, 51915–51932 (2019)
11. Arif, M., Wang, G., Balas, V.E.: Secure vanets: trusted communication scheme between vehicles and infrastructure based on fog computing. Stud. Inform. Control **27**(2), 235–246 (2018)
12. Hamza, R., Yan, Z., Muhammad, K., Bellavista, P., Titouna, F.: A privacy-preserving cryptosystem for IoT e-healthcare. Inf. Sci. (2019)
13. Herder, C., Yu, M., Koushanfar, F., Devadas, S.: Physical unclonable functions and applications: a tutorial. Proc. IEEE **102**(8), 1126–1141 (2014)
14. Gao, Y., Ma, H., Abbott, D., Al-Sarawi, S.F.: Puf sensor: exploiting puf unreliability for secure wireless sensing. IEEE Trans. Circ. Syst. I: Regul. Pap. **64**(9), 2532–2543 (2017)
15. Mukhopadhyay, D.: Pufs as promising tools for security in Internet of Things. IEEE Des. Test **33**(3), 103–115 (2016)
16. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf
17. Casino, F., Dasaklis, T.K., Patsakis, C.: A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics Inf. **36**, 55–81 (2019)
18. Mukherjee, A.: Physical-layer security in the Internet of Things: sensing and communication confidentiality under resource constraints. Proc. IEEE **103**(10), 1747–1761 (2015)
19. Javaid, U., Aman, M.N., Sikdar, B.: Blockpro: blockchain based data provenance and integrity for secure IoT environments. In: BlockSys@SenSys (2018)
20. Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., Njilla, L.: Provchain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), pp. 468–477, May 2017