Enhanced Privacy Setup for Blockchain-Enable IoT Devices Using Multi-Factor Authentication

Muhammad Saad
SysCore Lab
Sejong University
Seoul, South Korea
muhammadsaad11@gmail.com

Ki-Woong Park
SysCore Lab
Sejong University
Seoul, South Korea
woongbak@sejong.ac.kr

***Abstract*— As the number of Internet of Things (IoT) devices keeps growing, security has become a major concern. With trade-offs like complexity and scalability, maintaining privacy in the system is a highly desired characteristic. This work presents an architecture for the management of IoT devices with Hyperledger Fabric. We incorporated our system with blockchain and Closed Circuit Television (CCTV) surveillance camera at a rental property. When new renters arrive, the CCTV security camera automatically reroutes its stream. We implemented multi-factor authentication via push notifications and web tokens to enhance security between renters and property owners. One of our contributions is an effective architectural framework that makes use of multi-factor authentication and key invalidation circumstances. Our proposed scheme enhances the security of IoT devices with blockchain technology and mitigates the risk of a single point of failure, providing a robust and reliable solution.**

Keywords—privacy, blockchain, Hyperledger, IoT, authentication

I. Introduction

The Internet of Things (IoT) constitutes a sophisticated network wherein numerous gadgets and entities engage with one another. These systems, frequently centralized, depend on trust [1]. They connect many devices to exchange and update data for smart cities, homes, cars, and healthcare [2]. As the use of IoT has grown, attempts have been made to switch from centralized access control to distributed solutions [3]. Ensuring security is one of the major obstacles in this transformation [4].

The blockchain concept was announced in 2008 alongside the creation of Bitcoin by Satoshi Nakamoto. It has since been utilized in a number of domains outside of cryptocurrency and payment verification systems [5]. Due to its decentralized structure and intrinsic transparency, blockchain technology is currently employed in the healthcare, transportation, and education sectors.

Traditionally, systems that rely on a third party often incur high costs and allow these intermediaries access to all data. However, there is a noticeable shift toward using blockchain in these areas [6]. Blockchain functions as a decentralized ledger technology for reliable resource management. Resource trading for blockchain-based computing has been developed to guarantee further security. Smart contracts, an essential aspect of blockchain technology, have generated substantial research across various fields.

Hyperledger Fabric technology deployment in IoT systems is becoming common nowadays. Hyperledger Fabric is based on the principles of blockchain technology and features an open architecture that allows for modifications to the consensus mechanism to enhance performance [7]. Its modular approach enables users to customize the system according to their specific needs, adding functionalities that help achieve desired outcomes. As a permissioned blockchain architecture, Hyperledger Fabric restricts registration to participants who go through the Membership Service Provider (MSP). During this process, the certificate authority issues a certificate to the participants. The private data collection (PDC) feature allows for the creation of channels among blockchain participants, ensuring the desired level of privacy. Unlike public blockchains, this feature eliminates the need for establishing separate channels. Additionally, many mobile IoT devices can be integrated with Hyperledger Fabric for authentication, similar to how they are utilized in public blockchains.

CCTV security camera feed is the primary focus of our system, and they require a high degree of user privacy. The system enables the property owner and the renter to access the CCTV security camera feed independently. Multi-factor authentication utilizing push notifications and web tokens enhances the privacy aspect of our solution. Although these features increase the system's complexity, they effectively accomplish the objective of utmost anonymity.

The remainder of this paper is organized as follows: Section 2 reviews the related work. In Section 3, we present our proposed framework architecture. Section 4 discusses analyses and comparisons while Section 5 concludes the papers with future research direction.

II. Related Work

Since the introduction of Hyperledger Fabric, researchers have conducted numerous studies across various domains. Privacy is a fundamental goal for everyone, and as a result, it has garnered considerable attention. Fields such as healthcare, electoral systems, and intelligent grids have prioritized privacy, along with surveillance systems.

Numerous surveillance systems are utilizing Hyperledger Fabric due to its enhanced privacy features. In [8], the authors propose a data verification method specifically for CCTV surveillance cameras in smart cities. The authors propose a mechanism that ensures the integrity of recorded video footage, allowing authorities to verify whether a video has been altered. In [9], the authors discuss a decentralized approach for creating safe and sustainable networks that use distributed video feeds from cameras mounted on vehicles in smart cities. The authors integrate vehicle cameras, blockchain technology, and a certification authority to ensure the secure and sequential storage of video data, protecting it from unauthorized modification and access. In [10], the authors introduced a dual tier blockchain framework designed to manage digital crime evidence. This system

979-8-3315-0412-0/25/$31.00 ©2025 IEEE

categorizes the evidence into two types: hot and cold blockchains, facilitating better organization and security.

In [11], the authors present a framework for ensuring privacy in blockchain-enabled IoT devices. They provide an overview of a rental room system in which the CCTV camera feed is kept private and directed solely to the renter rather than the property owner. In this context, the third-party acts as a manufacturer, and the authors implement smart contracts to automate the system. Similarly, in [12], a framework for a secure privacy and anonymity system for blockchain-enabled IoT devices is proposed. In this case, the CCTV security camera feed is also redirected to the renter when renting a property. This architecture is the foundation for our improved work, presented in this paper.

III. Privacy Secure System

The modular architecture of Hyperledger Fabric enabled us to leverage its functionalities to fulfill our specific requirements. The permissioned network functionality allowed us to limit the number of anonymous users in the network and retain control over scalability. Our approach improves anonymity among participating entities due to channel support within the fabric. Our system necessitates the fulfillment of multiple conditions prior to granting access; thus, the endorsement rules of Fabric are applicable, as they can be tailored to meet specific requirements, ensuring appropriate validation and authorization of transactions. The solution leverages the intrinsic characteristics of blockchain technology, including the reduction of dependence on a central authority, providing each node with access to the complete database, and ensuring the preservation of its historical integrity and immutability.

Fig 1. shows the working architecture of our framework which we call Privacy Secure System (PSS). PSS comprises of different entities which are defined as follows:

- **Owner**: A property owner can have multiple properties, each with one CCTV camera.
- **Renter**: The person who rents the available property will receive access to the CCTV security camera feed.
- **CCTV security camera**: The device for transmitting video output.
- **Security Agency**: Responsible for installing CCTV security cameras at property owners' locations. It possesses a blockchain network that includes all transactions and records.
- **Registered device**: The device that the owners register to get push notifications.
- **Web portal**: This platform is used for authentication purposes both at the owner's and the renters' end.
- **PSS API**: The interface between the entities and the Hyperledger fabric.

The architecture illustrates both on-chain and off-chain blockchain connectivity. The security agency installs the CCTV camera and awaits the public key, thereafter, transmitting it to the property owner. The CCTV security camera feed is oriented towards the owner. Communication between the owner and renter occurs through the PSS interface utilizing blockchain technology, which involves monetary transactions. Additionally, on-blockchain communication occurs between the owner and the PSS interface, as well as between the renter and the PSS interface. The owner and renter additionally engage in off-blockchain communication via the web portal for authentication purposes, which falls under the scope of authentication. Another authentication factor is the push notification which is sent off-blockchain from PSS to the owner's registered device. The CCTV security camera interfaces with the PSS off-blockchain to transmit public key information to the renter.

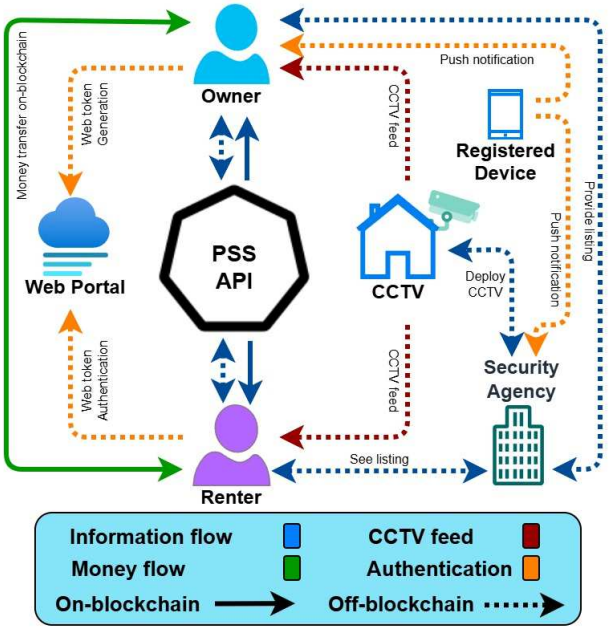

Fig 1. Architecture of the Privacy Secure System (PSS)

The property owner initiates the process by providing the listing to the security agency. The list comprises the owners' unoccupied homes available for rent. The security agency installs CCTV security cameras at vacant houses. The security agency operates a private blockchain network on Hyperledger Fabric, with several channels, each containing several peers. The peers serve as endorsers and committers within the system, as well as the owners or renters of certain properties. The owner and renter enroll via the membership service provider and acquire the certificate from the certificate authority. Subsequently, they produce their public and private keys via symmetric key encryption and input the public keys together with the requisite specific information into the PSS and the chain code. The owner registers a device with the PSS API to receive push notifications.

The handover of the CCTV security camera feed from the owner to the renter takes place subsequently. Prior to this, the funds are remitted to the owner. The renter chooses the property for rental, triggering a push notification to the owner. Upon confirmation from the owner, the renter may proceed; otherwise, an additional push notice is dispatched to the owner. The renter is unable to proceed without receiving a response. The renter creates a web token via the web portal and transmits it to the owner through the PSS API for the chosen property. The owner verifies the web token on the

web portal. Upon successful authentication, blockchain operations commence. Figure 2 illustrates the flow of the PSS, highlighting the critical procedures of key generation, authentication, and endorsement. The procedural steps are outlined as follows:

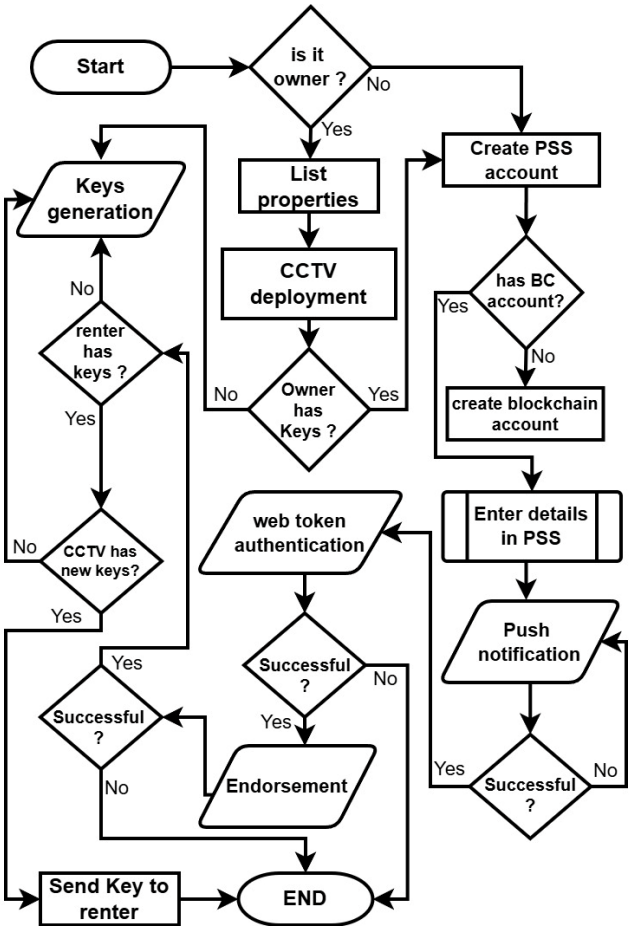

Fig 2. Flowchart of Privacy Secure System (PSS)

1- The property owner shares a detailed list of all properties, both vacant and occupied, with the security agency to help future renters make informed choices.
2- CCTV security cameras are installed at all properties. The security agency asks the CCTV security camera owner to generate the key pair. Through key management and asymmetric key encryption, CCTV security cameras generate public and private keys. The security agency gives the public key to the CCTV security camera owner. Owner generates key pairs. The owner uses private keys to access the CCTV security camera feed. CCTV cameras begin transmitting video feed to the owner.
3- The security agency requests the owner to join PSS and blockchain. After registration, the owner logs in with their credentials. A certificate is issued when they connect to the security agency's blockchain network via MSP. The owner then has a PSS ID, blockchain address, and certificate and submits their information in the chain code, linking their data to properties within PSS. The owner also registers a device with the
4- The renter registers for PSS, logs in, and browses properties. A push notification is sent on the owners registered device and security agency. If the push notification is passed, the renter is allowed to proceed. A certificate authority issues a certificate after joining the security agency's blockchain network via MSP. The renter possesses a PSS ID, blockchain address, and certificate.
5- The renter creates a web token using their blockchain address and certificate on the web interface, stores it on PSS for the selected property, and notifies the owner of updates. The owner authenticates the web token and verifies property details on PSS, maps the renter's PSS ID to their CCTV ID, and requests the rental period. After the renter pays, they request the CCTV camera key from PSS.
6- PSS proposes redirecting CCTV security camera feeds to the endorsing peer, which simulates this proposal through the chain code. After execution, the endorsing peer responds to PSS. The ordering service creates transaction blocks and sends them to the committing peer, which verifies the transactions and endorsement policy before submitting the block to the blockchain.
7- After updating the ledger, PSS asks for the CCTV security camera's public key. CCTV security camera generates new key pairs and sends PSS the public key. Video transmission to the owner is stopped after the old CCTV security camera key is invalidated. PSS sends the renter the CCTV security camera's public key. The renter generates key pairs and uses their private key to view the video feed.

Algorithm 1: Redirection of CCTV security camera feed

Input: Blockchain address, public key and web token
Output: CCTV Camera feed redirection

Initialization: SC.expiry = false
SC.duration = renter defined
SA.CCTV_access = false
SA.CCTV_key = generate ( )
for each *Property P_i, Owner O_i* **do**
    Send *O_i [BC_addr, pub_key]* to *SA*
    SA.P_i ← **NULL**
for each *Renter R_i after choosing property P* do
    Send push notification to *O_i.registered_device*
        if *O_i.push notification == true*
            then generate web token
            return *R_i.token*
        end
for each *Renter R_i after generating token* **do**
    Send *R_i [BC_addr, pub_key, PSS_id, token]* to *O_i*
        O_i verifies token on web portal
    if *Oi. token == Ri.token then*
        O_i.P_i.CCTV == R_i.PSS_ID
        Set *SA.CCTV_access == true*
        Set *SC.expiry == true*
        SC.duration ← *getRentDuration( )*
        return *SA.CCTV_key to R_i*
    End
End

Algorithm 1 shows the chaincode procedure and the conditions that need to be met. After initialization, the owner registers the device for push notifications and enters details in the PSS API. The renter joins the PSS which triggers a push notification to the owner. The web token is generated by the renter if the push notification is authenticated by the owner. The renter sends the web token to the owner through the PSS API and this web token is authenticated by the owner on the web portal.

IV. Security Analysis

The primary objective of our proposed architecture is to ensure robust privacy for all participants involved. We achieve this by incorporating advanced chaincode approaches, which facilitate secure interactions on the blockchain, and by utilizing unique cryptographic keys assigned to the assets' owner and renter. This key differentiation enhances security by ensuring only authorized individuals can access or modify the data relevant to their transactions. Our system also addresses several potential security risks that may arise in decentralized environments, including double spending attacks, which can undermine the integrity of transactions, single points of failure that can lead to system-wide vulnerabilities and threats related to the mishandling or theft of private keys. By proactively restricting these risks compared to existing frameworks, we aim to demonstrate our architecture's enhanced resilience and reliability.

We are also aware of the unique security issues that arise when you combine (IoT) devices with blockchain technology. These include concerns about data privacy and the chance of centralized points of failure that could weaken the system's integrity. Our system incorporates a CCTV security camera network designed to use cutting-edge IoT-enabled technologies to mitigate these risks. Central to our framework is a multiple key generation process critical to minimizing security vulnerabilities. This process ensures that the previously issued keys are rendered obsolete and no longer valid when a rental contract is concluded. This design choice significantly reduces the necessity for third-party involvement, thus streamlining the transition and enhancing the security of overall architecture. By employing these innovative strategies, we aim to create a more secure and private ecosystem for all users involved in the rental process

V. Conclusion

The PSS represents an innovative approach to addressing prevalent privacy concerns in today's digital landscape. One of the primary advantages of this system is its ability to significantly reduce the challenges associated with traceability and link-ability, which are critical issues in maintaining user anonymity and data confidentiality. At the core of our solution is a sophisticated methodology that combines push notifications with web token authentication. This integration not only enhances user experience by providing timely updates but also ensures that access to sensitive information is tightly controlled. Each interaction within the system is securely authenticated, preventing unauthorized access and safeguarding user data.

Moreover, the versatility of our architecture is a standout feature, as it extends beyond its current application. The principles and technologies behind the PSS have the potential to be applicable across various sectors within the IoT. This is especially crucial in environments where personal and privacy-sensitive data is at risk of exposure. In the context of smart homes, for instance, our system plays a vital role in protecting data generated by IoT devices. These devices often include advanced technologies such as facial and voice recognition systems, which can be particularly vulnerable to data breaches. By leveraging blockchain technology, we ensure that all sensitive information is not only securely stored but also immutably recorded, enhancing overall security and trustworthiness. Thus, the PSS offers a comprehensive solution that addresses the multifaceted challenge of privacy in an increasingly interconnected world.

Acknowledgment

This work was supported by the Information and Communication Technology Planning Evaluation (IITP) grant funded by the Ministry of Science and ICT (Project No. RS-2024-00438551, 10%; RS-2022-00165794, 20%; 2022-11220701, 10%; IITP-2024-2021-0-01816, 10%), the National Research Foundation of Korea (NRF) grant funded by the Ministry of Science and ICT (Project No. RS-2023-00208460, 20%), the Korea Research Institute for Defense Technology Planning and Advancement (KRIT) (Project No. 21-107-A00-009, 10%), and the Ministry of Science and ICT grant through the Information Technology Research Center (ITRC) Program (Project No. RS-2023-00228996, 20%).

References

[1] R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S.A. Kondaveeti and S. Shekar, "Continuous security in IoT using blockchain," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, 2018, pp. 6423-6427.

[2] J.H. Khor, M. Sidorov and P.Y. Woon, "Public blockchains for resource-constrained IoT devices – A state-of-the-art survey*," IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 11960-11982, 2021.

[3] D.Y. Hwang, J.Y. Choi and K.H. Kim, "Dynamic access control scheme for IoT devices using blockchain," in *Proceedings of the International Conference on Information and Communication Technology Convergence*, 2018, pp. 713-715.

[4] L. Xu, N. Shah, L. Chen, N. Diallo, Z. Gao, Y. Lu and W. Shi, "Enabling the sharing economy: Privacy respecting contract based on public blockchain," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, 2017, pp. 15-21.

[5] A. Pouraghily and T. Wolf, "A lightweight payment verification protocol for blockchain transactions on IoT devices," in *Proceedings of the IEEE International Conference on Computing, Networking and Communications*, 2019, pp. 617-623.

[6] N. V. Saberhagen, "CryptoNote 2.0," 2013. [Online]. Available: https://decred.org/research/saberhagen2013.pdf

[7] N. Klaokliang, P. Teawtim, P. Aimtongkham, C. So-In and A. Niruntasukrat, "A novel IoT authorization architecture on hyperledger fabric with optimum consensus using genetic algorithm," in *Proceedings of the International Student Project Conference*, 2018, pp. 1-5.

[8] P.W. Khan, Y.C. Byun and N. Park, "A data verification system for CCTV surveillance cameras using blockchain technology in smart cities," *Electronics*, vol. 9, no. 3, pp. 484, 2020.

[9] K. Moolikagedara, M. Nguyen, W.Q. Yan and X.J. Li, "Video blockchain: a decentralized approach for secure and sustainable networks with distributed video footage from vehicle-mounted cameras in smart cities," *Electronics*, vol. 12, no. 17, pp. 3621, 2023.

[10] D. Kim, S.Y. Ihm and Y. Son, "Two-level blockchain system for digital crime evidence management," *Sensors*, vol. 21, no. 9, pp. 3051, 2021.

[11] M.N. Islam and S. Kundu, "Poster Abstract: Preserving IoT Privacy in sharing economy via smart contract," in *Proceedings of the IEEE/ACM International Conference on Internet-of-Things Design and Implementation*, 2018, pp. 296-297.

[12] M. Saad, M.R. Bhutta, J. Kim and T.S. Chung, "A framework for enhancing privacy and anonymity in blockchain-enabled IoT devices," *Computers, Materials and Continua*, vol. 78, no. 3, pp. 4263-4282, 2024.