Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.061733

ARTICLE

P2V-Fabric: Privacy-Preserving Video Using Hyperledger Fabric

Muhammad Saad and Ki-Woong Park*

SysCore Lab, Sejong University, Seoul, 05006, Republic of Korea

*Corresponding Author: Ki-Woong Park. Email: woongbak@sejong.ac.kr

Received: 02 December 2024; Accepted: 20 March 2025; Published: 16 April 2025

ABSTRACT: The proliferation of Internet of Things (IoT) devices introduces substantial security challenges. Currently, privacy constitutes a significant concern for individuals. While maintaining privacy within these systems is an essential characteristic, it often necessitates certain compromises, such as complexity and scalability, thereby complicating management efforts. The principal challenge lies in ensuring confidentiality while simultaneously preserving individuals' anonymity within the system. To address this, we present our proposed architecture for managing IoT devices using blockchain technology. Our proposed architecture works on and off blockchain and is integrated with dashcams and closed-circuit television (CCTV) security cameras. In this work, the videos recorded by the dashcams and CCTV security cameras are hashed through the InterPlanetary File System (IPFS) and this hash is stored in the blockchain. When the accessors want to access the video, they must pass through multiple authentications which include web token authentication and verifiable credentials, to mitigate the risk of malicious users. Our contributions include the proposition of the framework, which works on the single key for every new video, and a novel chaincode algorithm that incorporates verifiable credentials. Analyses are made to show the system's throughput and latency through stress testing. Significant advantages of the proposed architecture are shown by comparing them to existing schemes. The proposed architecture features a robust design that significantly enhances the security of blockchain-enabled Internet of Things (IoT) devices while effectively mitigating the risk of a single point of failure, which provides a reliable solution for security concerns in the IoT landscape. Our future endeavors will focus on scaling the system by integrating innovative methods to enhance security measures further.

KEYWORDS: Blockchain; IoT; hyperledger fabric; verifiable credentials; privacy

1 Introduction

Using dashcams and CCTV security systems within the IoT has changed how we approach surveillance and data collection. These technologies enhance security and awareness in various situations. Dashcams record videos of the road and surroundings while driving, making them useful for documenting accidents and preventing crime. Similarly, CCTV security systems monitor public spaces to watch activities and discourage criminal behavior. However, the widespread use of these tools raises privacy concerns, especially regarding how we manage and store sensitive video data. As dashcams and CCTV security systems connect more through IoT, the risk of unauthorized access and data breaches grows. It is essential to protect personally identifiable information in the recorded footage to avoid privacy violations.

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 significant obstacles in this transformation that requires careful consideration when devising new methods [4].

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 [5]. The blockchain concept was announced in 2008 alongside the creation of Bitcoin by Satoshi Nakamoto. It has since been utilized in many domains outside of cryptocurrency and payment verification systems [6]. Thanks to its decentralized structure and intrinsic transparency, blockchain technology is currently being harnessed in healthcare, transportation, and education. Blockchain serves as a decentralized ledger technology for reliable resource management, ensuring the security of all transactions. The development of resource trading for blockchain-based computing further enhances this security. Smart contracts, a crucial aspect of blockchain technology, have sparked substantial research across various fields, reinforcing the reliability and security of this innovative technology.

Implementing Hyperledger Fabric technology within Internet of Things (IoT) systems is becoming increasingly prevalent. Hyperledger Fabric is constructed on the foundational principles of blockchain technology and features an open architecture that permits modifications to the consensus mechanism, thus enhancing overall performance [7]. Its modular design allows users to tailor the system to meet their requirements, incorporating functionalities to attain desired outcomes. As a permissioned blockchain framework, Hyperledger Fabric restricts registration to authorized participants, who must undergo a process facilitated by a Membership Service Provider (MSP). A certificate authority is responsible for issuing certificates to the participants during this process. The private data collection (PDC) feature allows for the creation of channels among blockchain participants, ensuring the desired level of privacy. This feature eliminates the need for establishing separate channels, unlike in public blockchains. Additionally, many mobile IoT devices can be integrated with Hyperledger Fabric for authentication, similar to how they are utilized in public blockchains.

Sharing credentials could raise privacy concerns and for digital credentials to be widely accepted, a system is required that provides secure verification of the participant identities [8]. Verifiable credentials are the standardized digital credential with cryptographic security, privacy protection, and machine readability and is one of the promising evolutions supporting decentralized identity authentication [9]. They enable the system to issue verifiable credentials and then verify the validity of these credentials [10]. In [11], a blockchain based platform is proposed which provides a distributed and secure system where every individual can store their verified credentials and share them with all potential employers. This system also empowers the employers to verify the credentials instantaneously. Another system to discover and recruit reputable talent using blockchain technology is proposed in [12]. This system enables trustless networks and allows entities to conduct transactions without mutual trust.

Combining blockchain technology with CCTV security camera systems and dashcams transforms data management. When integrated with artificial intelligence, these systems offer enhanced analytical capabilities, real-time threat detection, and rapid responses to various incidents. This combination has the potential to significantly improve safety and security, especially in urban areas such as smart cities, where interconnected surveillance networks are prevalent. However, it is essential to balance the advantages of enhanced surveillance with the need to protect individuals' privacy.

Implementing Hyperledger Fabric in smart grids is increasingly recognized for its potential to enhance privacy measures. In [13], the authors executed a comprehensive empirical study focusing on validator peers within Hyperledger Fabric to improve the energy efficiency of permissioned blockchains by utilizing FPGAs. Moreover, reference [14] delineates a framework designed to secure data aggregation schemes in smart grids, offering a decentralized and secure approach to safeguarding individual privacy and confidentiality.

Hyperledger Fabric is also frequently applied in land registration and rental agreements. In [15], the authors introduced a system that facilitates secure and transparent land transactions, encompassing all phases from planning to certificate issuance, while integrating land sale management to diminish reliance on intermediaries notably. Additionally, the General Data Protection Regulation (GDPR) has designed an innovative residential rental platform, enabling secure rental contracts and payment transactions between landlords and tenants, as detailed in [16].

Online voting systems have been developed utilizing Hyperledger Fabric to ensure voter anonymity and confidentiality. In [17], the authors examine various drawbacks and limitations inherent in current voting systems, while assessing several established blockchain frameworks for the purpose of constructing a robust blockchain-based electronic voting system. In [18], the authors focus on enhancing the security and reliability of online voting systems through the application of Hyperledger Fabric, thereby ensuring the protection of each vote cast against potential risks. Furthermore, in [19], the authors introduce a sophisticated method for the transmission of transaction data, which is encrypted using homomorphic encryption. This approach facilitates secure data transfer through a protected channel, with the encrypted information subsequently recorded on the blockchain following the conclusion of the voting process.

A significant amount of research has been conducted in the healthcare field utilizing Hyperledger Fabric. In [20], the authors propose a COVID-19 pandemic-focused framework to enhance the management of patients in the healthcare system. The access control mechanism using chaincode is detailed in [21]. The authors of [22] introduce a healthcare monitoring system using blockchain architecture. This system utilizes Hyperledger fabric for monitoring, leveraging its privacy features. To ensure the integrity of stored security recordings in smart cities and decide whether the data has been changed is proposed in [23]. Additionally, the authors of [24] propose a methodology for ensuring secure networks through vehicle-mounted cameras integrated with blockchain technology for access control and data integrity. A multi-tier blockchain system is proposed in [25], which is designed to manage crime scenarios and store the evidence.

To achieve privacy in this system, we propose a blockchain-based design for the video sharing system using Hyperledger fabric as a backbone. Different types of authentications are incorporated to achieve the desired goal of privacy enhancement. Key contributions of our work are outlined as below:

- Our framework formulates an innovative chaincode algorithm that guarantees the system's efficient operation. The endorsement policies are meticulously crafted to reflect real-world scenarios.
- Our system enhances privacy by generating a unique key for each recorded video. This method strengthens security and makes it significantly harder for malicious users to gain unauthorized access or control over the recordings.
- Implementing multi-factor authentication techniques significantly enhances the security of systems. Alongside web tokens that serve as temporary access keys, verifiable credentials provide a strong barrier against unauthorized access, ensuring only authorized individuals can enter.

The remainder of this paper is organized as follows: Section 2 reviews the related work. The proposed framework architecture is explained in Section 3. Theoretical analyses are discussed in Section 4 along with the comparisons, while Section 5 concludes the paper with future research directions.

2 Related Works

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 and surveillance systems. Numerous surveillance systems are utilizing Hyperledger Fabric due to its privacy

features. In [26], a blockchain-based personal data trading system using decentralized identifiers and verifiable credentials is proposed. This system allows users to collect personal data in their own data storage provided by the system. Hyperledger fabric is used to ensure the integrity of the traded data and the history of transactions. Fig. 1 shows the system's overall architecture consisting of a mobile app, DID agent, data agent, trade agent, and Hyperledger fabric. The DID, data, and trade agent work together to ensure data management by category, authenticating the user ownership of personal data and taking care of all the metadata for trading. The system ensures personal data trading without the centralized service providers. This system has a limitation concerning the risk of a single point of failure in case the mobile phone is lost or stolen, which is used to manage all the personal data. Compared to this, our system focuses on multiple authentication options, which mitigates this issue.

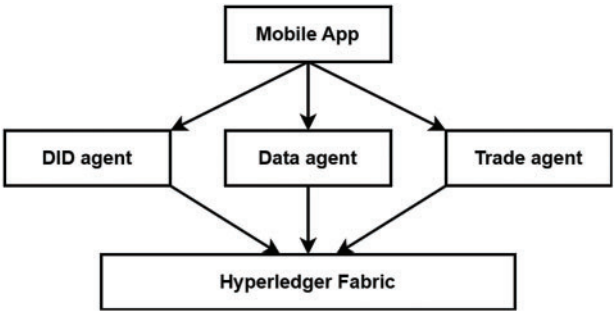

Figure 1: Architecture of blockchain-based personal data trading system

In Fig. 2 [27], the authors present a credentials verifier system using blockchain. They use blockchain as a backbone for the entire system. To upload the credentials, different types of certificates are initially stored in the temporary database. The admin on receiving the notification verifies the certificates. After verification, the certificates are uploaded to the IPFS, making it impervious for any further amendments. The systems work on different use cases depending on the nature of the system in use. The limitation of the system is the scalability of the system to bigger systems when it comes to very large systems on a global scale. In our system, we accommodate this limitation by using Hyperledger fabric's modular architecture.

In [28], a framework for secure privacy and anonymity setup using Hyperledger fabric is proposed. The system is called SPAS-H. This system is the steppingstone for our work. Fig. 3 shows the architecture of SPAS-H. In this system, the feed from the CCTV security camera is redirected to the renter when they rent a property. Simultaneously, the old access keys for the CCTV camera are invalidated, and the feed to the property owner is terminated. The renter generates a web token for the owner and sends it, allowing the owner to verify it on a web portal. Though this scheme has enhanced privacy preservation, the shortcoming comes from using just one authentication technique. Our current work incorporates multiple authentication schemes to enhance the system's privacy.

This paper presents an efficient setup for privacy of Hyperledger fabric, building upon the original SPAS-H architecture introduced in [28]. Our proposed system effectively enhances privacy while addressing essential requirements such as independence from third parties, reduced computational complexity, and immutable transactions. The modular design of Hyperledger fabric enables us to integrate various entities, allowing for the seamless incorporation of our core components. This system offers a comparable level of security enhancement to other mentioned systems.

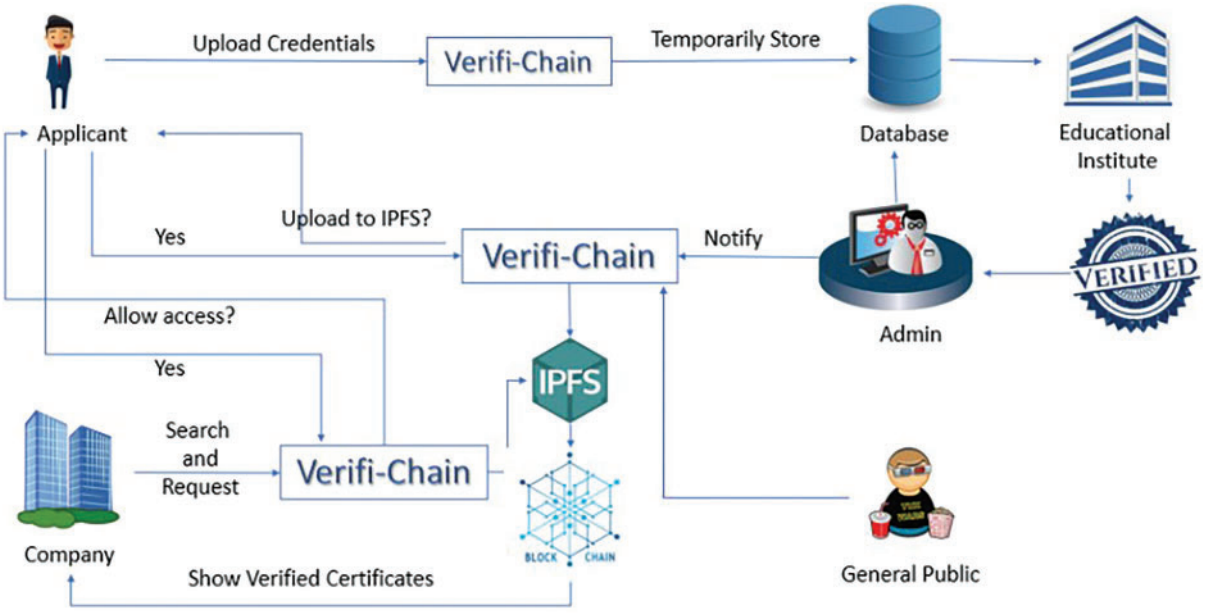

Figure 2: Workflow of verifi-chain architecture [27]

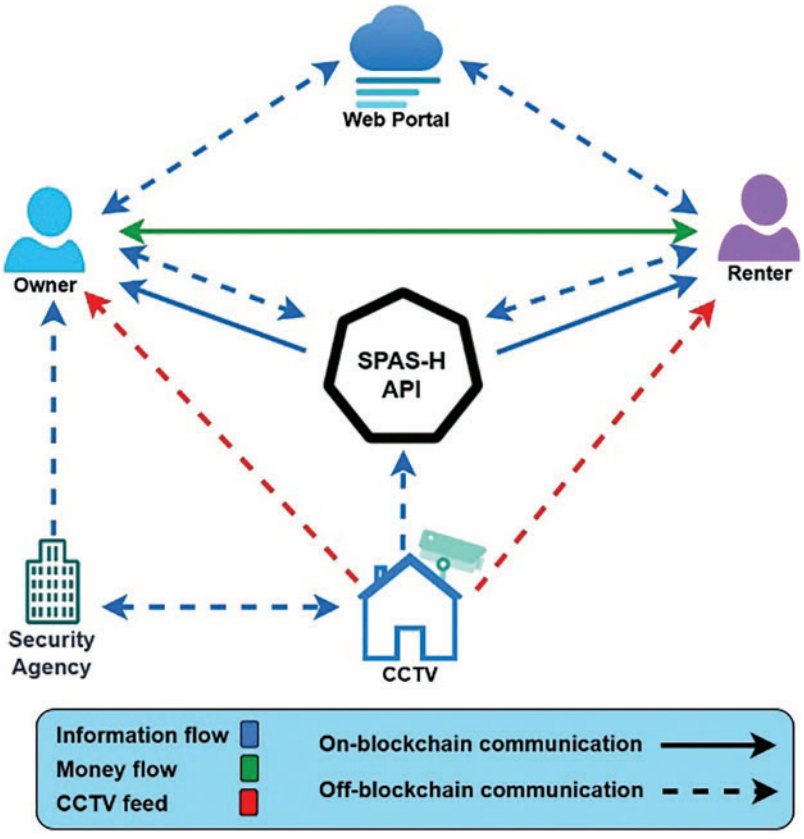

Figure 3: Architecture of secure privacy and anonymity setup using hyperledger fabric (SPAS-H)

3 Proposed Architecture

We focus on a system that includes multiple cameras, such as car dash cams and CCTV security cameras. The videos recorded by these devices serve various purposes, from entertaining viewers on social media to assisting in investigations of theft or accidents. It is crucial to ensure a high level of privacy in these situations. Moreover, dash cam footage plays a vital role in maintaining data integrity and provenance, as it is used for traffic management, location sharing, and enhancing situational awareness. CCTV security cameras can capture community events, such as cultural parades and festivals, with footage available for viewing or rental. There are also rare occurrences, like meteor showers or planetary alignments, where recorded footage is in high demand. However, those renting this footage often prefer to remain anonymous. Across all these scenarios, the importance of privacy is a common concern.

3.1 Basic Architecture of the Proposed System

We call our system the Privacy-Centric System (PCS). The highlight of Hyperledger fabric is its architecture, which is based on modules. This feature helped us customize and align it with our system's requirements. The permissioned architecture restricts unauthorized access. Moreover, the channel support ensures confidentiality among the entities involved. Given that our system necessitates the fulfillment of multiple conditions prior to granting access, we employ Fabric's customizable endorsement policies. These policies facilitate the appropriate validation and authorization of transactions based on our distinct needs. Furthermore, our system leverages various fundamental characteristics of blockchain technology, including reducing reliance on third parties for central operations, providing complete database access and historical data for every node, and guaranteeing immutability.

PCS system is composed of different components. These components collaborate to produce the desired results for the system. They include:

- **Cam:** This includes car dashcams and CCTV security cameras. These devices record videos.
- **Cam owner:** The authorized owner of multiple dashcams and CCTV security cameras across various properties.
- **Accessor:** The person who accesses the video content. This person is divided into categories according to the access rights.
- **IPFS:** The Interplanetary File System module is used to hash the encrypted video.
- **Web portal:** The platform for authorization and validation.
- **PCS:** The connection between the Hyperledger fabric network and different involved entities.
- **Keys management:** Platform for keys generation.
- **Trusted manager:** This is the internal authority which authenticates the verifiable credentials.
- **Chain code:** A smart contract with trigger conditions.
- **Blockchain network:** A Hyperledger fabric network.
- **CDN:** Network for delivery of the video content to the accessors after all verifications.

Fig. 4 provides an overview of the basic architecture of the PCS. The system's core feature is the on-blockchain and the off-blockchain communication between the entities. The camera serves as a video recording device, which can either be a dashcam or a CCTV security camera. The ownership of these cameras lies solely with the cam owner, who may own multiple cameras, including both dashcams and CCTV security cameras. However, each camera can only be owned by one individual.

Cam owners encrypt the videos through their private keys and categorize them into various types, such as infotainment, theft, and accidents, to facilitate easier searching for those who need to access the footage. The individuals who access the videos are referred to as accessors, and they are classified into

different categories based on their video access rights. These rights can include the ability to view or copy the videos. Communication between the cam owner and accessors occurs through the PCS. Additionally, financial transactions are processed via on-blockchain communication, while off-blockchain interactions for authentication take place through a web portal. There is also off-blockchain communication between the cam owners and trusted manager and accessors and trusted manager for the verifiable credentials. An IPFS node generates hashes of the encrypted videos received from the cam owners, and a Content Delivery Network (CDN) is utilized to deliver the requested videos to the accessors off-blockchain.

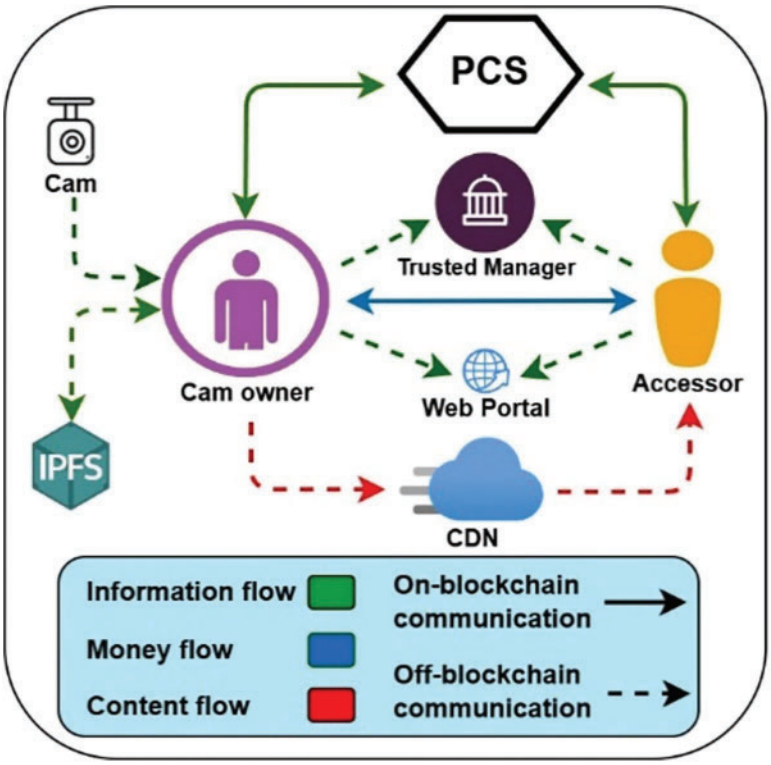

Figure 4: Privacy-Centric System (PCS) architecture

3.2 The Flow of PCS Working

The PCS operates in two main phases: storing and accessing video content. The storing video process involves recording, encrypting, and hashing the video, while the accessing video phase involves authentication, transfer and decrypting of the video. Both main phases incorporate blockchain communication elements, ensuring that transactions are immutable.

The first phase of storing the video is relatively straightforward, while the second phase requires thorough verification processes for accessing the video. In the first phase the video is recorded by the cameras, which can be a dashcam or the CCTV security camera. The video is then encrypted by the cam owner and is hashed by the IPFS node. The hash of the video is then stored in the blockchain which becomes an immutable transaction. In the second phase, the accessor must go through the authentication process through the web token generated through the web portal. Additional authentication is the presentation of the verifiable credentials to the trusted manager. On successful authentications, the accessor receives the encrypted video. The decryption process is taken over at the end. Both the phases are analyzed in detail below.

3.2.1 Phase 1: Storing the Video

This is the starting phase of the framework, where the video recorded from the cameras is encrypted, hashed, and stored. The records of all transactions are stored in blockchain to become tamper-proof.

1. The process of cam specification and recording.
    a. There are two types of cameras: car dash cams and CCTV security cameras on buildings. Both types of cameras are connected to the cam owners and can record the video. The camera records video V.
2. The process of communication to and from the cam owner.
    a. The camera sends recorded video V to the cam owner.
    b. The cam owner generates its keys pair through the keys management.
    c. The cam owner encrypts video V. Encrypted video $EV = Ek(V)$.
    d. The cam owner transfers the encrypted video EV to the IPFS node.
3. The process of hash code production.
    a. The video's hash is denoted by h. This contains many videos from different cam owners who are part of the blockchain network, so the videos are denoted by h_1, h_2, h_3, . . ., h_n. This hash is calculated using the SHA-256 algorithm.
    h = Hash (EV)
    b. IPFS node sends the h of the EV to the cam owner.
4. The process of an authorized cam owner to join the network.
    a. The cam owner signs up on the PCS.
    b. Through the MSP, the authorized cam owner joins the network.
    c. The CA issues the membership certificate to the cam owner, thus making it a member of the blockchain network.
    d. The cam owner now has the key pairs, PCS ID, EV, and h.
5. The process of entering details on the PCS.
    a. The cam owner enters the details on the PCS which includes their blockchain address and the metadata of the video. The metadata is comprised of the time, date, location and tag of the video. The tag is categorized according to the nature of the video like infotainment, crime or accident video.
    b. The cam owner uploads the hash of the encrypted video to the blockchain.
6. The process of ledger updation.
    a. PCS sends 'upload hash' proposal. The endorsing peers start simulating the upload chaincode.
    b. PCS receives the proposal response through the endorsing peer.
    c. Ordering service, on receiving the transaction from PCS, generates a block and send it to the committing peers.
    d. The block is committed to the blockchain after each transaction is validated and the endorsement policy is verified by the committing peer. Fig. 5 shows the sequence of the workflow in phase 1.

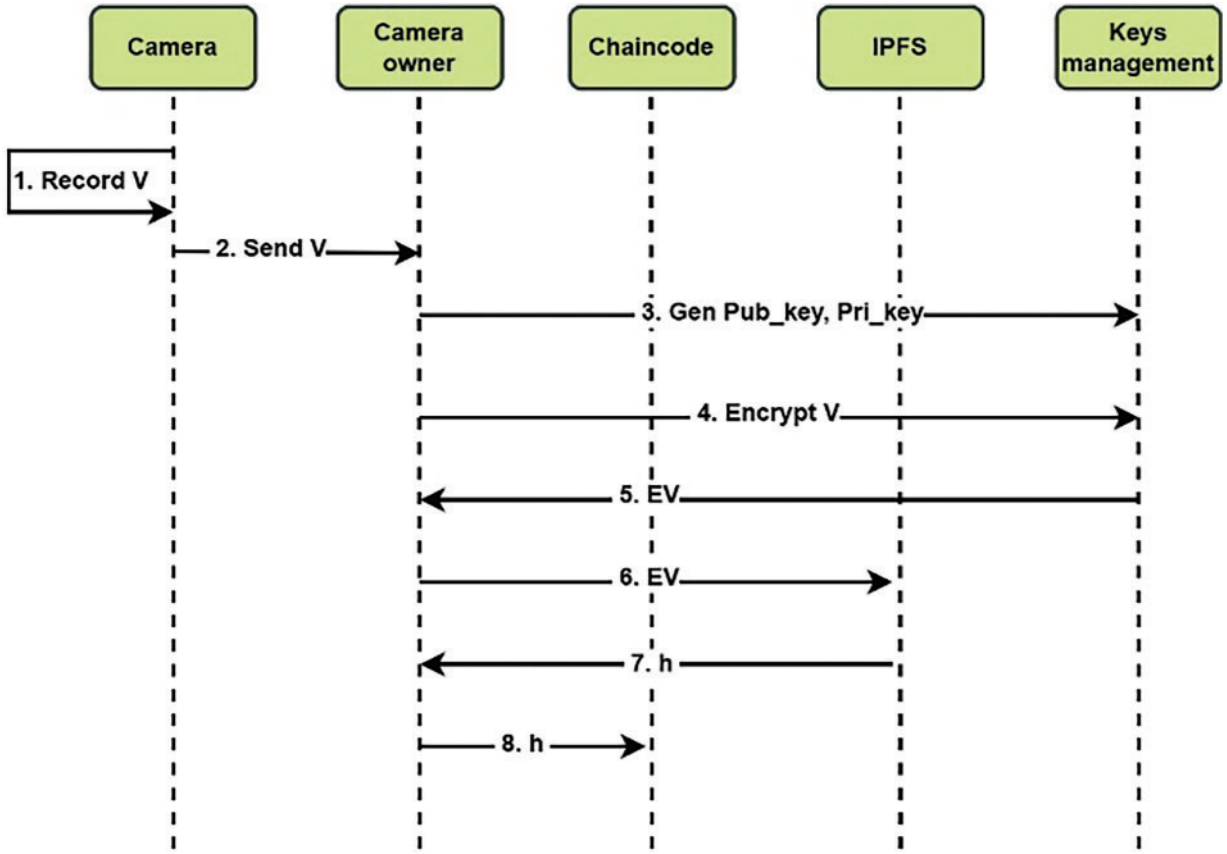

Figure 5: Workflow sequence of phase 1

3.2.2 Phase 2: Accessing the Video

This phase of the framework deals with the transfer of the required video from the cam owner to the accessor. It includes the web token authentication of the accessor on the web portal and the verifiable credentials play their part. The trusted managers also feature in this phase, which are an important part of the transfer of the video. The stepwise description of the phase is given as follows:

1. The process of accessor joining the PCS and the blockchain.
   a. The accessor signs up on the PCS app and joins the blockchain network.
   b. The accessor enters the blockchain address in the PCS app. The accessor now has the PCS ID and blockchain address. The accessor is categorized according to the rights for video, e.g., right to view only, right to copy, etc. This access is based on the accessor input at the time of signing up on the PCS.
2. The process of accessing the required video.
   a. The accessor looks for the required video on the PCS.
   b. The accessor asks for the required video on the PCS through video id (*V_ID*).
   c. PCS triggers the cam owner about the *V_ID*.
   d. The cam owner asks the accessor about the duration the video is required for through the PCS. This helps in deciding the fee for the video which the accessor must pay to the cam owner.
   e. The accessor informs the cam owner about the duration.

3. The process of composing verifiable credentials and transfer to trusted manager.
    a. Upon receiving the duration of the required video, the cam owner composes the verifiable credentials. This contains the context, ID, type, issuer and validity.
    b. After composing the verifiable credentials, the cam owner sends them to the trusted manager.
    c. The cam owner sends the verifiable credentials to the accessor through the PCS.

Table 1 shows the example of a sample verifiable credential composition which contains the context of the video, the video ID, the type of video (infotainment, crime, accident, etc.), the issuer of the video and the validity of the video based on the duration provided by the accessor.

Table 1: Verifiable credentials example

Context	**www.video.com**
ID	3195a
Type	crime
Issuer	bob
Validity	20241130 17:55

4. The process of web token generation and authentication.
    a. The cam owner generates the JSON web token (JWT) through the web portal.
    b. The cam owner sends the JWT to the PCS against the accessor's ID.
    c. The PCS notifies the accessor about the JWT.
    d. The accessor authenticates the JWT on the web portal.
    e. If the JWT is authenticated, the PCS sends notification to the cam owner and the trusted manager.
5. The process of verifiable credentials presentation.
    a. The trusted manager on receiving the JWT authentication successful notification from the PCS, sends message to the accessor about presenting the verifiable credentials.
    b. The accessor starts the verifiable credentials presentation to the trusted manager. The trusted manager verifies all the credentials with the credentials sent by the cam owner earlier.
    c. If the presented credentials are successfully verified, the trusted manager sends notification to the PCS to initiate the blockchain transactions of producing the hash of the required video asked for by the accessor.

Algorithm 1 shows the chaincode.

Algorithm 1: Accessor wants to access the video

Definitions: $O_i \ \epsilon \ O$: Set of Cam owner
$A_i \ \epsilon \ A$: Set of Accessors
$CC_i \ \epsilon \ CC$: Set of Chaincodes
$V_i \ \epsilon \ V$: Set of Videos
TM: Trusted Manager
Input: Blockchain address, public key, JWT and VC
Output: Video access to the accessor
1 **Initialization:** CC.expiry = false

(Continued)

Algorithm 1 (continued)

CC.duration = accessor defined
CC.V_i_access = false
for each *Video* V_i, *CamOwner* O_i **do**
    Send O_i *[BC_addr, pub_key, EV and h]* to PCS
for each *Accessor* A_i *after choosing video V* do
    Send *V_id* to O_i.
    O_i.*CC.duration* ← *getRentDuration( )*
    O_i send VC to *TM*
        then generate JWT
        return O_i.*JWT*
    End
for each *Owner* O_i *after generating JWT* **do**
    Send O_i *[JWT]* to A_i
        A_i verifies JWT on web portal
    if *Oi. token == Ai.token then*
        Send PCS *JWT.success* to *TM*
        Send *TM [present VC]* to A_i
for each *Accessor* A_i receiving *[present VC]*
        Present A_i.*VC* to *TM*
    If A_i.*VC* == O_i.*VC*
            Send *PCS [h]* to A_i
            Send A_i*[h]* to O_i
            return O_i.*EV to* A_i
    End
End
End

After the initialization and video recording, both the cam owner and accessor are required to enter details into the chaincode, as shown in Lines 4–7. The accessor selects the video and sends the video ID to the PCS. Following this, the authentication procedure occurs from Lines 8–20. The cam owner asks the accessor how long they need the video. Based on the response, the cam owner creates the verifiable credentials and sends them to the trusted manager. Afterward, the cam owner generates a JWT and sends it to the accessor. The accessor then verifies the JWT on the web portal. The trusted manager requests the accessor to present the verifiable credentials. Once the accessor provides the VCs, the trusted manager verifies them, and the process of sending the encrypted video begins, as detailed in Lines 21–27.

6. The process of ledger updation.
    a. PCS sends 'upload hash' proposal. The endorsing peers start simulating the upload chaincode.
    b. PCS receives the proposal response through the endorsing peer.
    c. Ordering service, on receiving the transaction from PCS, generates a block and send it to the committing peers.
    d. The block is committed to the blockchain after each transaction is validated and the endorsement policy is verified by the committing peer. The endorsement policy used in this case is briefly described in Table 2.
    e. The PCS gets the hash produced by the blockchain network and notifies the cam owner.

7. The process of transferring the video.
   a. As the PCS receives the *h* of the *V* from the blockchain, it forwards it to the accessor.
   b. The accessor sends the *h* to the cam owner.
   c. The cam owner h, the *h*, sends the *EV* to the accessor.
   d. The accessor generates their keys pair through the keys management.
   e. The accessor receives the encrypted video through CDN.
   f. The accessor decrypts the video through their private key.

Table 2: Endorsement policy

Configuration	Accessor wants to access the video
Peer nodes	P1, P2, P3
Orderer node	O
Endorsement policy	3/3 (P1.P2.P3) for crime videos 3/3 (P1.P2.P3) for accident videos 2/3 [(P1.P2)|(P1.P3)|(P2.P3)] for infotainment videos

Fig. 6 shows the workflow of phase 2.

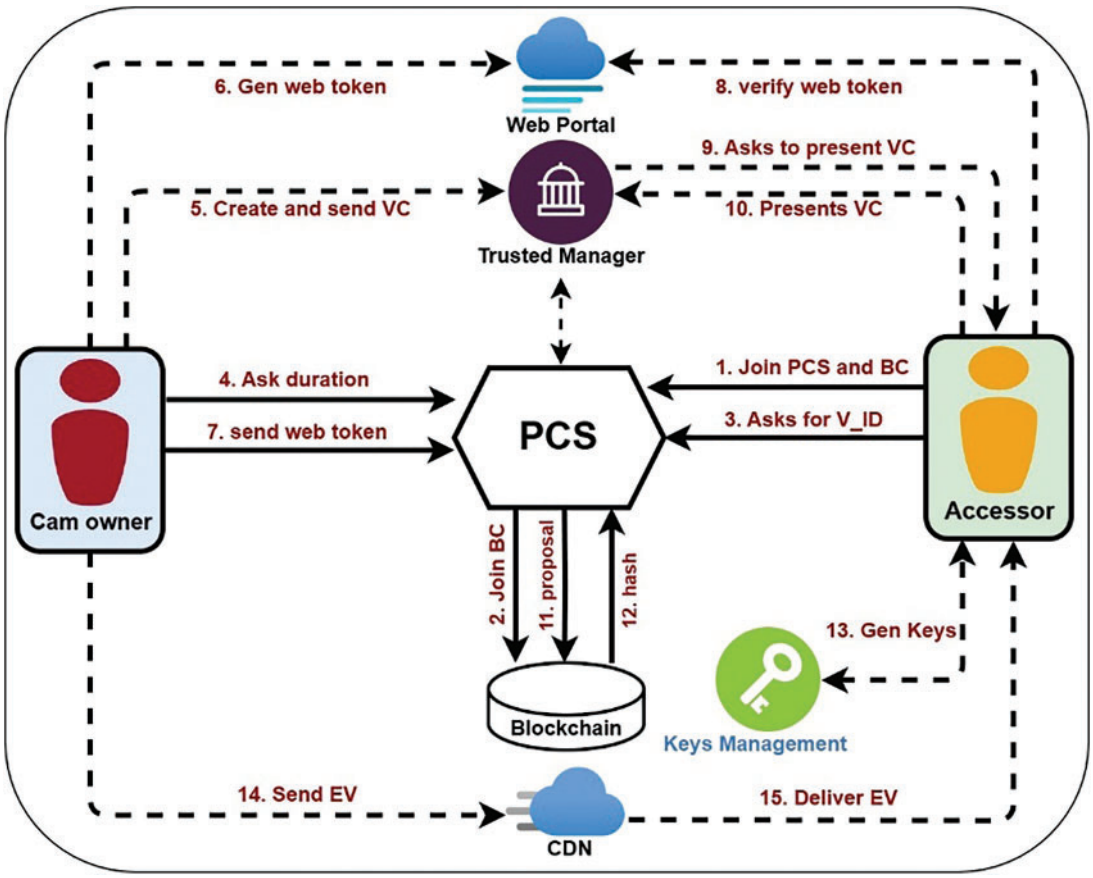

Figure 6: Workflow of phase 2

Fig. 7 shows the activity diagram of the PCS.

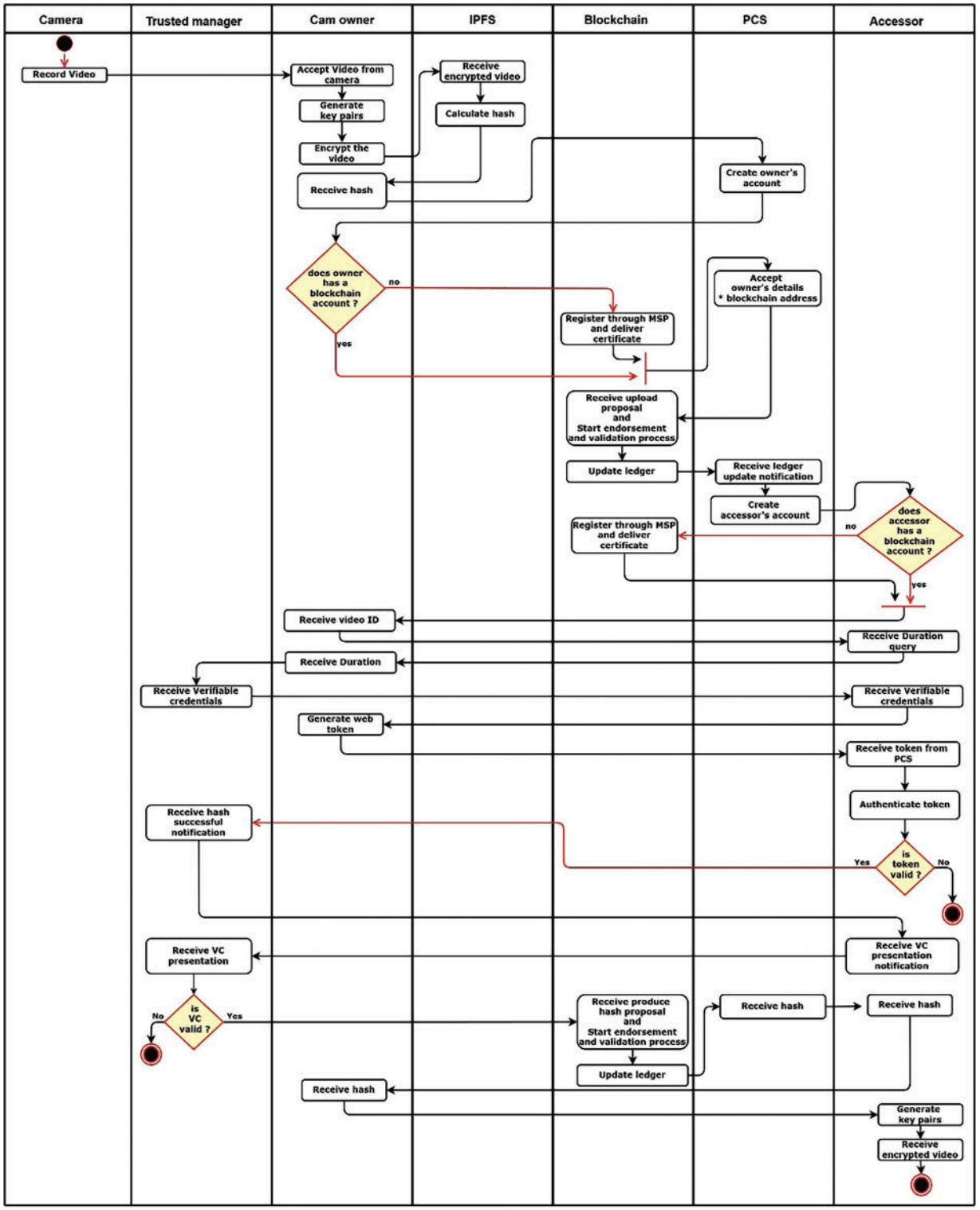

Figure 7: Activity diagram of Privacy-Centric System (PCS)

4 Discussion and Analysis

Our proposed scheme strongly emphasizes the critical importance of preserving user privacy in our digital interactions. To achieve this goal, we have developed and implemented a novel chain code algorithm that stands out due to its innovative approach of utilizing a unique key for each data instance. This means that a new and distinct key is generated for every recorded video captured by our camera system, and no keys are reused throughout the process. This method significantly reduces the risk of unauthorized access or data breaches, as each video is secured with its own tailored cryptographic key. In addition to our key management strategy, we further enhance the privacy of collected data by integrating verifiable credentials and web tokens. These technologies provide a robust framework for ensuring only authorized users can access sensitive information. By implementing these mechanisms, we actively mitigate various security threats that could compromise the system, such as the risks associated with key reuse, single points of failure, the potential for blockchain collapse, and the overarching threat of system hacking. Another vital consideration in our scheme is the solution's scalability. We address this issue by employing a modular architectural approach utilizing Hyperledger Fabric. This framework is particularly advantageous because it allows for the seamless addition of new modules or functionalities as the system grows or new requirements arise. This flexibility ensures that our solution can adapt without significant limitations.

From a security point of view, different types of security threats are handled in this system utilizing the core features of blockchain technology. Unauthorized access issues have been taken care of by introducing the multi-factor authentication in the system. This multi-factor authentication not only restricts the users but also the trusted managers for unauthorized access in the system. This unauthorized access also restricts the information disclosure of the users through the blockchain system. The denial-of-service issue is mitigated by the removal of a single point-of-failure in the system.

During the implementation phase of our scheme, we encountered several challenges that required careful consideration and proactive problem-solving. One notable challenge was integrating communication between on-chain transactions and off-chain data sources. We successfully addressed this issue by utilizing oracles—specialized third-party services capable of retrieving data from external systems and then inputting that data into the blockchain. This approach facilitated effective communication between on-chain and off-chain components. It ensured that our system remained responsive to real-time data while maintaining the integrity and security of the blockchain. The off-blockchain communication is carried out by the front-end development for the users which is implemented by Python3 and Web3 libraries.

4.1 Implementation

The Hyperledger Fabric is recognized as a powerful solution for organizations seeking to implement internal blockchain applications while mitigating concerns regarding external interference due to its permissioned architecture. Table 3 shows the implementation parameters used in this work.

Table 3: Implementation parameters

Fabric version	2.5.7
Server RAM	4 GB
Endorsing peer	1
Committing peer	2
Orderer	1

A significant advantage of Hyperledger Fabric lies in its high degree of configurability, which is attributable to its modular architecture and the flexible deployment of chaincodes. The chaincode performs

a critical role in the operational functionality of the blockchain, encapsulating the essential logic required for the proposed solution. Unlike many other blockchain platforms that necessitate the use of domain-specific languages for the execution of smart contracts, Hyperledger Fabric permits the use of general-purpose programming languages, including Java, Go, and Node.js. For this application, the chaincode was developed using Node.js.

4.2 Evaluation

The evaluation is carried out by overloading the system with varying operations performed every second. Thorough monitoring was done to see the effects of reaction and response times. The first evaluation metric is the delay in read-and-write operations. Transaction latency is the time it takes for a transaction to pass through all the phases of proposing, endorsing, ordering, and committing successfully. A decrease in latency is shown in Fig. 8, which indicates the system's working efficiency when scalability is considered in terms of several varying operations. The interval between querying the ledger and receiving a response is known as the read latency. Fig. 9 shows a significant decrease, indicating rapid responses when the volume of operations increases.

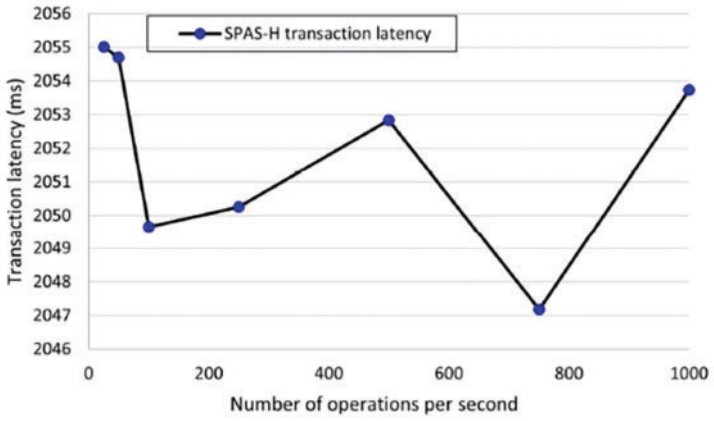

Figure 8: Transaction latency

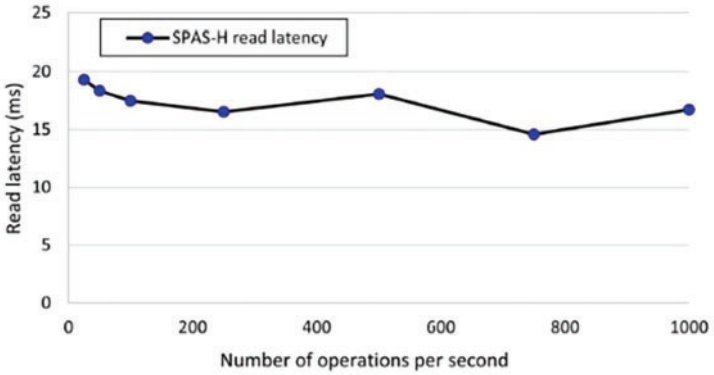

Figure 9: Read latency

Transaction throughput denotes the rate at which a blockchain system validates and commits transactions over a specified duration. This metric is representative of the entire network of nodes, rather than an individual node. Fig. 10 depicts the system's transaction throughput, which remains constant irrespective of the volume of operations executed per second.

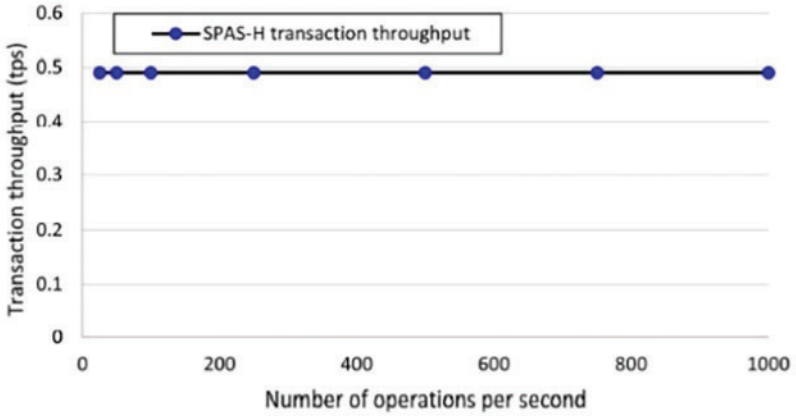

Figure 10: Transaction throughput

Read throughput is a metric that quantifies the number of read operations executed over a specified time interval, expressed as reads per second. Fig. 11 shows the system's progressive enhancement in read throughput, underscoring its efficiency and resilience in high-demand environments. This observation indicates that the system is capable of meeting operational requirements when managing extensive systems with an increasing volume of transactions.

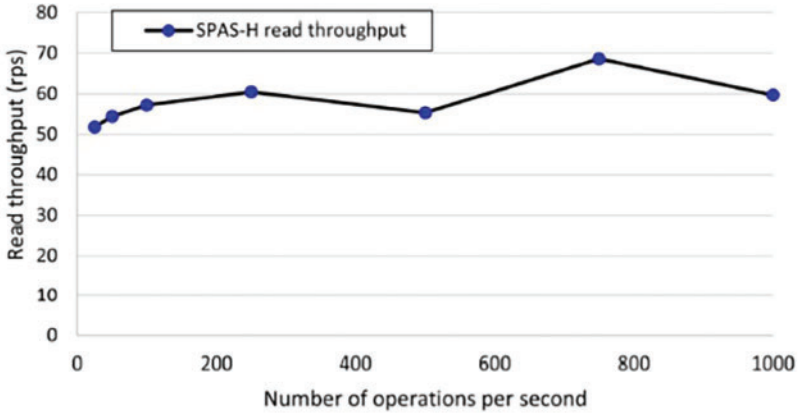

Figure 11: Read throughput

Fig. 12 shows the qualitative comparison of PCS with SPAS-H which does not have empirical parameters. Computational overhead of PCS is more than SPAS-H because of the multi-factor authentication scheme while PCS has more traceability resistance, confidentiality and smart contract integration. Due to the multi-factor authentication including verifiable credentials, PCS has more proof complexity in comparison with SPAS-H.

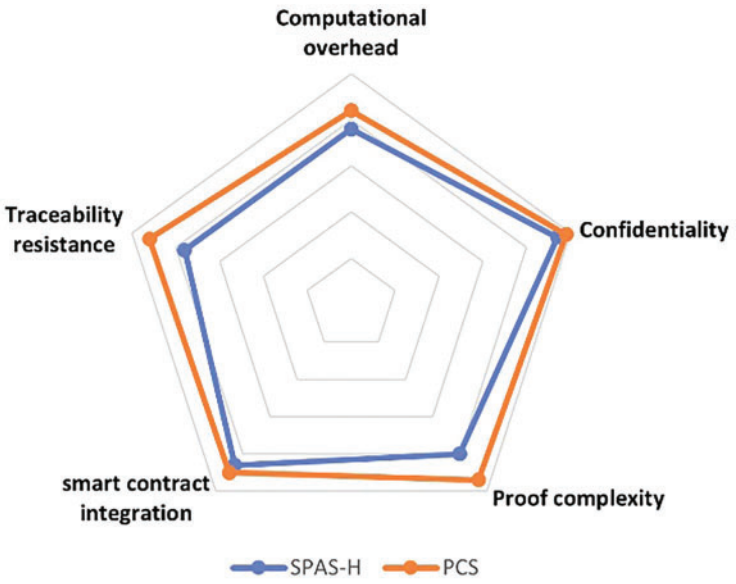

Figure 12: Qualitative comparison

Table 4 shows a comparative analysis of PCS with existing solutions given in Section 2. The parameters include privacy, authentication, smart contract usage, confidentiality, keys usage and single point of failure.

Table 4: Comparative analysis

Categories	Verifi-Chain	SPAS-H	PCS
Privacy	Partially achieved	Achieved	Achieved
Smart contract	Yes	Yes	Yes
Confidentiality	High	High	High
Keys usage	Re-used	Always new	Always new
Single Point-of-Failure	Yes	No	No
Authentication	Credentials	Web tokens	Multi-factor

5 Conclusion

The PCS system offers an innovative solution to address privacy concerns within the existing framework while effectively overcoming challenges associated with traceability. This system employs a sophisticated mechanism that integrates verifiable credentials and Web Token authentication. This distinctive combination significantly enhances the robustness of our approach in safeguarding individual privacy. The architecture is applicable beyond its current implementation, extending its relevance to various Internet of Things (IoT) domains where privacy-sensitive data may be exposed to potential risks. For instance, in smart home environments, the system protects data generated by IoT devices—such as facial and voice recognition technologies—by securely storing this information on a blockchain.

The practical implications of this architectural framework are particularly significant within the automotive industry. The use of chaincodes enables functionalities such as intelligent parking solutions and fuel payment systems while safeguarding the confidentiality of identity-sensitive and financial transactions. A critical advancement in our research is the formulation of a novel chaincode algorithm distinguished by its

incorporation of verifiable credentials and web token authentication. This integration enhances the overall operational efficiency of our system. The scalability of our solution across various domains that depend on sensitive data, where the protection of privacy is paramount, highlights the versatility and applicability of our approach. Hyperledger Fabric offers modular scalability, thereby facilitating the streamlined expansion of the system. Beyond Internet of Things (IoT) applications, this architectural design also presents substantial potential within the pharmaceutical sector, especially concerning the development and distribution of medications among wholesalers, dispensers, and end consumers.

PCS works in an efficient way but there are some limitations. These include the existence of trusted management in the system. Though we consider them to be trusted, there can be malicious users which become trusted managers at some point. We plan to resolve this limitation in our future work. Another limitation is the throughput in scalability of the system. Till this point, we have established that the system is scalable enough to cater to big systems, but the trends in the graphs show that if the system is overburdened with transactions, there can be a point of scalability issues. The resolution of this issue is another agenda in our future work.

Acknowledgement: The authors wish to express their appreciation to the reviewers for their helpful suggestions which greatly improved the quality of this paper.

Funding Statement: This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) (Project Nos. RS-2024-00438551, 30%; 2022-11220701, 30%; 2021-0-01816, 30%), and the National Research Foundation of Korea (NRF) grant funded by the Korean Government (Project No. RS-2023-00208460, 10%).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Muhammad Saad; data collection: Muhammad Saad; analysis and interpretation of results: Muhammad Saad and Ki-Woong Park; draft manuscript preparation: Muhammad Saad and Ki-Woong Park. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Agarwal R, Verma P, Sonanis R, Goel U, De A, Kondaveeti SA, et al. Continuous security in IoT using blockchain. In: 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP); 2018 Apr 15–20; Calgary, AB, Canada. p. 6423–7.
2. Khor JH, Sidorov M, Woon PY. Public blockchains for resource-constrained IoT devices—a state-of-the-art survey. IEEE Internet Things. 2021;8(15):11960–82.
3. Hwang D, Choi J, Kim KH. Dynamic access control scheme for IoT devices using blockchain. In: 2018 International Conference on Information and Communication Technology Convergence (ICTC); 2018 Oct 17–19; Jeju Island, Republic of Korea. p. 713–5. doi:10.1109/ictc.2018.8539659.
4. Xu L, Shah N, Chen L, Diallo N, Gao Z, Lu Y, et al. Enabling the sharing economy: privacy respecting contract based on public blockchain. In: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts; 2017 Apr 2–6; Abu Dhabi, United Arab Emirates. p. 15–21. doi:10.1145/3055518.3055527.
5. Pouraghily A, Wolf T. A lightweight payment verification protocol for blockchain transactions on IoT. In: 2019 International Conference on Computing, Networking and Communications (ICNC); 2019 Feb 18–21; Honolulu, HI, USA. p. 617–23.

6. Saberhagen N. CryptoNote v 2.0, white paper. [cited 2025 Jan 1]. Available from: https://cryptopapers.info/cryptonote/.
7. Klaokliang N, Teawtim P, Aimtongkham P, So-In C, Niruntasukrat A. A novel IoT authorization architecture on hyperledger fabric with optimal consensus using genetic algorithm. In: 2018 Seventh ICT International Student Project Conference (ICT-ISPC); 2018 Jul 11–13; Nakhonpathom, Thailand. p. 1–5. doi:10.1109/ICT-ISPC.2018.8523942.
8. Mukta R, Martens J, Paik HY, Lu Q, Kanhere SS. Blockchain-based verifiable credential sharing with selective disclosure. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); 2021 Dec 29–Jan 1; Guangzhou, China. p. 959–66. doi:10.1109/TrustCom50675.2020.00128.
9. Fang J, Feng T, Guo X, Ma R, Lu Y. Blockchain-cloud privacy-enhanced distributed industrial data trading based on verifiable credentials. J Cloud Comput. 2024;13(1):30. doi:10.1186/s13677-023-00530-7.
10. Doğan Ö, Karacan H. A blockchain-based e-commerce reputation system built with verifiable credentials. IEEE Access. 2023;11:47080–97. doi:10.1109/ACCESS.2023.3274707.
11. Taha A, Zakaria A. Truver: a blockchain for verifying credentials: poster. In: Proceedings of the 35th Annual ACM Symposium on Applied Computing; 2020 Mar 30–Apr 3; Brno, Czech Republic. p. 346–8. doi:10.1145/3341105.3374067.
12. Sulaiman R, Alamsyah A, Wulansari P. Reshaping the future of recruitment through talent reputation and verifiable credentials using blockchain technology. In: 2022 10th International Conference on Information and Communication Technology (ICoICT); 2022 Aug 2–3; Bandung, Indonesia. p. 316–21. doi:10.1109/ICoICT55009.2022.9914891.
13. Santoso N, Javaid H. Improving energy efficiency of permissioned blockchain using FPGAs. In: 2022 IEEE 28th International Conference on Parallel and Distributed Systems (ICPADS); 2023 Jan 10–12; Nanjing, China. p. 177–84.
14. Mahmood A, Khan A, Anjum A, Maple C, Jeon G. An efficient and privacy-preserving blockchain-based secure data aggregation in smart grids. Sustain Energy Technol Assess. 2023;60:103414. doi:10.1016/j.seta.2023.103414.
15. Zein RM, Twinomurinzi H. Information sharing in land registration using hyperledger fabric blockchain. Blockchains. 2024;2(2):107–33. doi:10.3390/blockchains2020006.
16. Proenca AS, Dias TR, Correia MP. Blockchain-based residential smart rent. arXiv:2402.05737. 2024.
17. Singh S, Singh A, Verma S, Dwivedi RK. Designing a blockchain-enabled methodology for secure online voting system. In: 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT); 2023 Jan 5–7; Bengaluru, India. p. 178–84. doi:10.1109/IDCIoT56793.2023.10053410.
18. Chovancová E, Chovanec M, Ádám N, Hurtuk J. Online voting management system based on blockchain. In: 2023 IEEE 27th International Conference on Intelligent Engineering Systems (INES); 2023 Jul 26–28; Nairobi, Kenya. p. 169–74. doi:10.1109/INES59282.2023.10297916.
19. Tang B, Tan M, Liu M, Liu Z, Tian W. A privacy protection method of blockchain-based E-voting using homomorphic encryption and order-preserving encryption. In: 2023 5th International Conference on Artificial Intelligence and Computer Applications (ICAICA); 2023 Nov 28–30; Dalian, China. p. 86–90. doi:10.1109/ICAICA58456.2023.10405563.
20. Khatri S, al-Sulbi K, Attaallah A, Ansari MTJ, Agrawal A, Kumar R. Enhancing healthcare management during COVID-19: a patient-centric architectural framework enabled by hyperledger fabric blockchain. Information. 2023;14(8):425. doi:10.3390/info14080425.
21. Mohan MS, Sujihelen L. An efficient chain code for access control in hyper ledger fabric healthcare system. E Prime Adv Electr Eng Electron Energy. 2023;5:100204. doi:10.1016/j.prime.2023.100204.
22. Attia O, Khoufi I, Laouiti A, Adjih C. An IoT-blockchain architecture based on hyperledger framework for healthcare monitoring application. In: 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS); 2019 Jun 24–26; Canary Islands, Spain. p. 1–5. doi:10.1109/ntms.2019.8763849.
23. Khan P, Byun YC, Park N. A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. Electronics. 2020;9(3):484. doi:10.3390/electronics9030484.

24. Moolikagedara K, Nguyen M, Yan WQ, Li XJ. Video blockchain: a decentralized approach for secure and sustainable networks with distributed video footage from vehicle-mounted cameras in smart cities. Electronics. 2023;12(17):3621. doi:10.3390/electronics12173621.
25. Kim D, Ihm SY, Son Y. Two-level blockchain system for digital crime evidence management. Sensors. 2021;21(9):3051. doi:10.3390/s21093051.
26. Yoon D, Moon S, Park K, Noh S. Blockchain-based personal data trading system using decentralized identifiers and verifiable credentials. In: 2021 International Conference on Information and Communication Technology Convergence (ICTC); 2021 Oct 20–22; Jeju Island, Republic of Korea. p. 150–4. doi:10.1109/ictc52510.2021.9621153.
27. Rahman T, Mouno SI, Raatul AM, Azad AKA. Verifi-chain: a credentials verifier using blockchain and IPFS. In: International Conference on Information, Communication and Computing Technology; 2023 May 27; New Delhi, India. p. 361–71.
28. Saad M, Haidery SA, Bhandari A, Bhutta MR, Park DJ, Chung TS. An efficient privacy and anonymity setup of Hyperledger Fabric for blockchain-enabled Internet of Things (IoT) devices. Electronics. 2024;13(13):2652.