INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

OPEN ACCESS

Received: 03/03/2025

Accepted: 03/03/2025

Published: 30/05/2025

Citation: Sathya K, Saraswathi A (2025) Design of Privacy Preserving Model for Academic Documents Issuance and Verification Using Distributed Hyperledger Fabric Approach (PACIV) and SSI. Indian Journal of Science and Technology 18(20): 1554-1564. https://doi.org/10.17485/IJST/v18i20.358

* **Corresponding author**.

kssathyacs3@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Design of Privacy Preserving Model for Academic Documents Issuance and Verification Using Distributed Hyperledger Fabric Approach (PACIV) and SSI

K. Sathya[1]*, **A. Saraswathi**[2]

1 Research Scholar(PT), PG and Research Department of Computer Science, Government Arts College (Autonomous), (Affiliated to Bharathidasan University, Tiruchirappalli), Karur – 639 005, Tamil Nadu, India
2 Associate Professor, PG and Research Department of Computer Science, Government Arts College (Autonomous), (Affiliated to Bharathidasan University, Tiruchirappalli), Karur – 639 005, Tamil Nadu, India

Abstract

Objectives: The challenges faced towards issuance of academic documents, verification of documents and moderation by authorities in comparison to traditional methods. Academic certificates issuance and verification can benefit greatly from blockchain-based privacy-preserving models, which offers a promising alternative to traditional paper-based methods. Primary objective of this research work PACIV is to establish a secure and decentralized network for managing academic certificates, the underlying technology used is the Hyperledger Fabric blockchain. **Methods:** Proposed PACIV platform connects student community, faculty members and academic members from multiple universities to different verifiers, as well limiting number of verifiers to whom students can present their certificates. The Hyperledger fabric and self-sovereign Identity model used for preserving the privacy of academic certificates issuance and verification. **Findings:** Performance evaluation assesses the system's speed, throughput, and latency. Observed time taken for a transaction to complete is found to be 320ms for 100 peers to 479 ms for 400 peers in use. **Novelty:** PACIV approach is implemented in this research to secure academic university certificates access from unauthorized access and providing more improved privacy and security with the practical implementation by applying SSI model.

Keywords: Hyperledger Fabric; Blockchain; Privacy protection; SSI; Academic documents

1 Introduction

Any academic organization [1] is considered to be a valuable and trustworthy on the creation and maintenance of Academic certificates and maintenance of academic documents a part of major record keeping task. Trust [2] is lost on an academic certificate if its personal identity is lost or mishandled by any micreants.

In order to achieve Hyperledger Fabric, a blockchain platform specifically designed for enterprise use cases, in combination with self-sovereign identity (SSI) [3] and verifiable credentials (VC) is vital for design. Blockchain technology [4] has potential to revolutionize the challenge of providing distributed security way academic certificates are issued and verified. By utilizing a decentralized and tamper-proof system, blockchain technology can ensure the integrity and authenticity of academic certificates while also preserving the privacy of the individuals involved. SSI allows individuals to control their own digital identities, while VCs provide a secure way to store and share information such as academic qualifications [5]. In this paper, blockchain-based privacy preserving model for academic certificate issuance and verification using Hyperledger Fabric using Edward curve key generation using Elliptic Key generation approach is elaborated. The primary aim of this research work is to design a blockchain-based privacy-preserving academic certificate issuance and verification system using Hyperledger Fabric and SSI, VC, and DID technologies by taking into account the key design considerations and trade-offs. Conceptual model for academic certificate system with appropriate algorithms, protocols [6], and evaluation metrics needed to achieve the goal of secure and privacy-preserving certificate issuance and verification needs to be shared. Additionally, SSI negotiation for providing security which aligns along standards and regulations is discussed. Challenges, limitations of the proposed model and suggest possible future work to improve its performance and security is discussed. The primary objective of this research work is to establish a secure and decentralized network for managing academic certificates, the underlying technology used is the Hyperledger Fabric blockchain.

The platform connects student community, faculty members and academic members from multiple universities to different verifiers, as well limiting number of verifiers to whom students can present their certificates. While creating a consortium of universities and verifiers provides a private and secure platform for sharing data, it is not a scalable solution. Verifiers cannot practically invest in joining numerous consortiums to verify students from multiple universities.

Research Gap:

This research work discusses on the challenges faced towards issuance of academic documents [7], verification of documents and moderation by authorities in comparison to traditional methods. Academic certificates issuance and verification can benefit greatly from blockchain-based privacy-preserving models, which offer a promising alternative to traditional paper-based methods [8]. By utilizing blockchain technology, these models create a secure, transparent, and tamper-proof system for issuing and verifying academic certificates, as demonstrated by the work of [2], [3]. With the increasing demand for higher education and the growing number of graduates, traditional paper-based methods are no longer sustainable. They are time-consuming, prone to fraud, and have limited access to verification. In contrast, blockchain-based models offer greater security, transparency, and accessibility. The research topic at hand is significant due to its potential to improve the credibility and authenticity of academic certificates [9], mitigate the risks of fraud and data breaches, and give students and graduates more agency over their academic records and credentials. Blockchain technology, which is a decentralized digital ledger that enables secure and transparent transactions without the need for intermediaries, underpins this research. In essence, blockchain technology functions as a database that logs transactions in chronological order, allowing multiple parties to simultaneously maintain and update the ledger [10]. Each block on the chain contains a unique hash, timestamp, and transaction data, all of which must be verified by network participants before being added to chain [2]. Blockchain technology possesses several fundamental characteristics, such as decentralization, immutability, and transparency, which render it an excellent solution for a range of industries, including finance, supply chain management, education, and healthcare [11]. Decentralization of a blockchain system means that it does not rely on a central authority to control it, enhancing its resilience to hacking and fraudulent activities. Immutability, on the other hand, ensures that any transaction recorded on the blockchain remains unalterable and cannot be deleted, providing a high level of data security. Additionally, transparency is another key characteristic of blockchain, where the ledger is open and visible to everyone, thereby promoting greater accountability and trust. Blockchain technology has numerous potential applications in various fields, including education [12]. For example, academic institutions can leverage blockchain technology to create a secure, transparent, and tamper-proof system for issuing and verifying academic certificates. This can reduce the risks of fraud and data breaches, while also making the verification process more efficient and accessible. By creating a digital record of academic achievements, students and graduates can have greater control over their academic records and credentials [7], which can enhance their employability and career prospects. In addition, blockchain technology has the potential to facilitate secure and efficient micropayments for education-related services like online courses and tutoring, thus broadening access to education for individuals who may not have the financial means to pay for conventional education services. Additionally, the use of blockchain technology could enable the establishment of digital identity management systems for students and graduates,

which could furnish employers with a dependable and trustworthy source of information [13]. Traditional academic certificates issuance and verification systems have several challenges and limitations [14], [3].

The paper is organized with Section-1 focusing on introduction to Blockchain and need for providing security on academic certificates. Section-2 focuses on design and development of proposed model PACIV using privacy preservation using Hyperledger fabric. The experimental approach with performance analysis is elaborated in Section-3 and conclusion with need for future work discussed in section-4.

2 Methodology

2.1 Model Description

2.1.1. Overview of Blockchain approach Hyperledger approach

To ensure sensitive data's security and confidentiality, blockchain-based academic certificate issuance and verification necessitate strong privacy techniques [15]. A high level of security is provided by additional privacy techniques which are necessary to prevent unauthorized access and data breaches using blockchain technology which inherently supports on privacy. Hyperledger Fabric, Verifiable Credentials (VC), Decentralized Identifiers (DID), and Self-Sovereign Identity (SSI) are some of the most effective techniques that can enhance the security and privacy of blockchain-based academic certificate issuance and verification [6], [9], [11]. Hyperledger Fabric provides a private and permissioned blockchain network that restricts access to authorized users only. VC enables the creation of digital credentials that can be easily verified without compromising the privacy of the credential holder.

2.1.2. Key Stakeholders of handling Academic certificates with user's role Identification

There are number of key stakeholders of the proposed model Figure 1 to legitimate with the roles for academic certificate verification as 1. Verifying credential in the certificates by job agents, companies, Governance body (a) Issuers – Universities Authority who will issue certificates (in the form of Verifiable Credential) to the students; (b) Verifiers – Job agents such as Organizations who support on providing different tasks/Jobs to students) etc., who verifies academic certificates (c) Holders/Owners – Students who get Certificates from Universities and provides these to the Companies/Other-Organizations to get the Job/different-services. (d) Governance Body – Ministry of Higher Education who authenticate and validate Issuers and confirm that Issuer is genuine or suggests on validation.

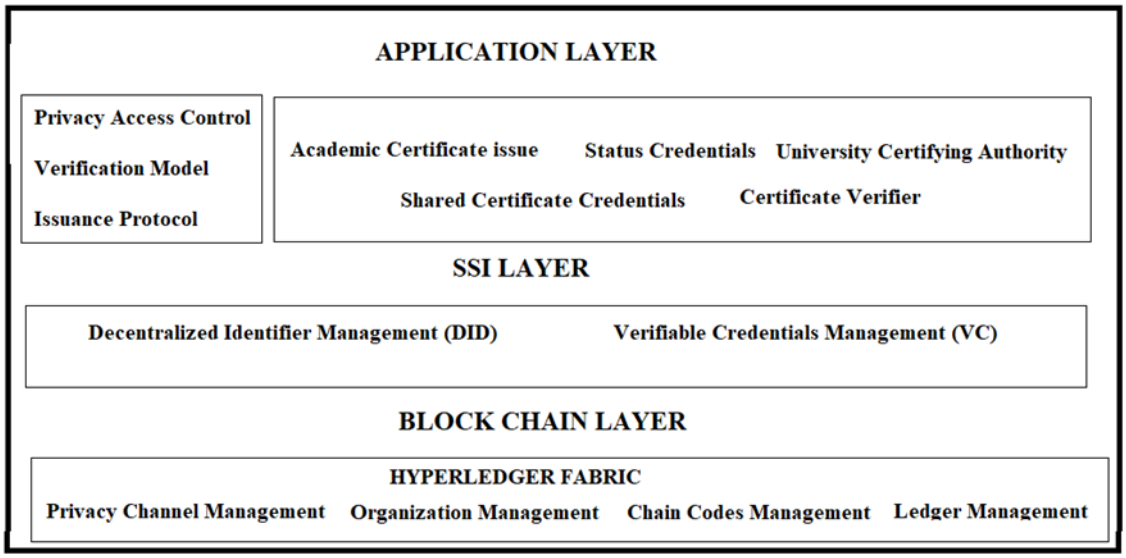

Fig 1. Layered system architecture of block chain over HyperLedger Fabric

2.1.3. Privacy Preserving Model for Academic Certificates Issuance and Verification Using Hyperledger Fabric and Self-sovereign Identity Model (PACIV)

A detailed description of the proposed system, includes multiple nodes such as the endorser, orderer, committer, and certificate. The endorser verifies transaction plans, simulates execution, and endorses. The orderer sorts transactions, determines sequence, reaches consensus, and saves them in the ledger. The committer checks transaction legitimacy and updates/maintains the data and ledger status of the blockchain. The certificate provides member identity via digital certificates, enabling authority control of the blockchain system. The channel ensures privacy protection for members by creating an independent communication pathway between network members.

This section elaborates on the system design of the proposed model, which includes the key stakeholder and role identification, system architecture, cryptography primitives, and system operations. The basis of the model which proposed in this work is VCs, DIDs and the Hyperledger fabric blockchain.

The layered system architecture of the proposed model is shown in Figure 1, the system is divided into three layers, which are described below:

1. Application layer: provides the proposed protocols for academic certificates issuance and verification while preserving the privacy.
2. Self-Sovereign Identity layer provides secure and reliable certificates management features and maintains the identities and schemas.
3. Blockchain layer provides blockchain-based immutable transaction distributed ledger and state database, which are maintained via a consensus of authorized peer nodes in the network. This layer provides an operating environment for running smart contracts.

SSI refers to a group of technologies that give individuals direct control over their digital identity, as opposed to relying on third parties. The traditional centralized and federated identity models place control with issuers and verifiers in the network, while the decentralized SSI model shifts control to individual users, enabling them to interact with others as peers. Decentralized identifiers (DIDs) and verifiable credentials (VCs) by the W3C are the two fundamental base standards for self-sovereign identities to date.

The proposed PACIV model includes a privacy channel designed and implemented within the Hyperledger Fabric blockchain to preserve privacy while allowing educational institutions to know each other. It is important to note that anonymity should not be the primary focus of the system, as universities should be known entities in the real world. Anonymity and privacy must also be differentiated to avoid confusion. The ministry has its universities, and it is crucial that they are not anonymous to each other. It is also important that other universities and ministries have relationships with each other. Thus, the privacy channel allows for these relationships to exist within the network. The proposed academic certificate issuance and verification is PACIV, which involves several steps, including generating a unique Decentralized Identifier (DID) for each student, creating a DID document, registering the DID on the blockchain, and issuing academic certificates as a transaction on the blockchain. The verifier can then access the blockchain and verify the academic certificate by querying DID and DID document. By following this protocol, the academic certificate issuance and verification process can be secured and decentralized.

Step 1: The network administrator, who is the higher authority, creates organizations within the network.

Step 2: Each education authority creates a channel that connects the universities, which is authenticated by the governance body.

Step 3: Each university creates its own peers under its organization.

Step 4: Peers within a university organization host a copy of the ledger and validate transactions before committing them to the ledger.

Step 5: Only universities can host the ledger to ensure trust and accountability in the system.

Step 6: Each university organization generates identities for students to control their own identity information using Self-Sovereign Identity (SSI) and Verifiable Credentials (VC).

Step 7: The university organization's admin is the only entity authorized to issue certificates on the network.

Step 8: The education authority, responsible for supervising schools at all levels, is hard-coded in the initial genesis state of the Hyperledger Fabric network to ensure trust and accountability.

Step 9: Third-party entities only need the certificate ID, keys, and owner's name to validate and authenticate the certificate, preserving privacy while ensuring that entities know each other.

By following these steps, the network can ensure the authenticity of academic certificates while preserving privacy and security. It is essential to acknowledge the critical role played by education authorities in the issuance and verification of academic credentials, and to ensure that they are hard-coded in the initial genesis state of the network to ensure trust and

accountability. The use of SSI and VC allows students as users to control their own identity information while maintaining privacy. The network design ensures that only universities can host the ledger, adding to the trust and accountability of the system. Finally, third-party entities can authenticate certificates with minimal information, preserving privacy while ensuring that entities know each other.

Algorithm 1 : Procedure of building PACIV Protocol

1. Each Govt_N has *{University*$_1$*,.....,University*$_i$ *| i >0, i = identification of university}*
2. $\text{Govt}_N \rightarrow \text{Channel}_M$, M = Govt_N
3. $\text{Govt}_N \rightarrow \text{University}_{Mi}$| $\text{University}_{Mi} \in \{\text{Govt}_N\}$, M = Govt_N, i={identification of university},
4. $\forall\ \text{University}_{Mi} \exists\ \text{Govt}_M$
5. $\{\text{University}_{M1}.....,\text{University}_M\} \subseteq \text{Channel}_M$, M = Govt_N
6. $\text{University}_{Mi} \rightarrow \text{Peer}_i$, {i ∈ N}
7. Ledger $\subseteq$ Peer_0,.....,Peer_i
8. $\text{University}_{admin} \rightarrow \text{Identity}_s$, {s ∈ Students}
9. $\text{University}_{admin} \rightarrow \text{Certificate}_s$, {s ∈ Students}

PACIV permit full control over entities to exist within the Hyperledger fabric. Universities can be combined using a channel allowing them to have their own private environment; this gives flexibility to allow sharing of information and full control of privacy on each entity. The channels are created by governance body to ensure no shady organization to exist in the midst of the network. Students are generated by universities limiting random users to exist in the network. Peers generated by universities are the only entities to host the ledger limiting the amount of access to the ledger hence reducing any chance for any type of attack, as an added measure. Since with the decentralized solution final commits happen only when most connected peers approve.

University DID management involves four entities: the university, the education authority, the Fabric CA, and the verifiable data registry. Two main processes are taken into account in this module: 1) registering the university on the Hyperledger Fabric blockchain, and 2) updating the DID and DID Doc. In the registration process, the university is registered on the Hyperledger Fabric by sending its name to the education authority, then approves and adds it to the Hyperledger Fabric. After the university is enrolled on the blockchain, the blockchain sends a public-private key and cryptographic material to the university. In return, the university is registered on the verifiable registry using the identity issued by the CA and publishes the DID and associated DID Doc to prove control. The process is represented by the following steps:

1. The university obtains a public key certificate from the Fabric CA.
2. The university sends a ”DID Anchor Request,” which is added to the ledger.
3. The ”university endorser” reads the ”DID Anchor Request.”
4. The university endorses the ”DID Anchor Request” and creates a NYM.
5. The contents of the NYM include:

    (a) DID of the university
    (b) Public key of the university in PEM format
    (c) Public key of the university in 58base encoding
    (d) Endorser name

The management of the University DID on the ledger is developed based on Algorithm 1.

Algorithm 2 outlines the process for managing the registration of a university's Decentralized Identifier (DID) on the ledger in a Hyperledger Fabric-based system. The algorithm takes n number of requests for registering the university DID on the ledger as input, and outputs the approval to register the university DID. The algorithm begins by iterating through each request using a counter. On each iteration, the algorithm reads the request of registering DID from the university. The education authority then checks the request to ensure that it meets the necessary requirements. If the request is approved, the fabric Certificate Authority (CA) sends the public-private key pair to the university. The university is then registered on the ledger using the identity issued by the fabric CA. Finally, the university publishes the DID on the ledger to prove control. If the request is not approved, the transaction is rejected. The algorithm continues to iterate through each request until all requests have been processed. Overall, Algorithm 2 ensures that the process of registering a university DID on the ledger is carefully managed and meets the necessary requirements for security and privacy.

Algorithm 2: Management of University DID on the ledger

Input: n request for registering university DID on the ledger

Output: approval to register University DID

1. for counter = 1 to n do
2. read the request of registering DID from the university
3. the education authority checks the request
4. if (the request) approved
5. the fabric CA send the public-private key to the university
6. the university is registered using the identity issued by fabric CA
7. the university published the DID on the leger.
8. end if
9. else
10. reject the transaction
11. end if
12. end for

Algorithm 3: Updating University DID on the Ledger

Input: New public-private key pair of the University

Output: Update University DID and DID Doc on the verifiable registry

1. University generates a new public-private key pair on the Hyperledger fabric
2. University updates its DID Doc to include new public key
3. University creates a signature for the new DID Doc
4. University sends the signature and the new DID Doc to the verifiable registry
5. Verifiable registry verifies the signature and updates the University's DID and DID Doc

Algorithm 3 describes the process of updating the University's DID and DID Doc on the verifiable registry by generating a new public-private key pair on the Hyperledger fabric. It outlines the process for creating a Decentralized Identifier (DID) for users involved in the academic certificate issuance and verification process based on Hyperledger Fabric blockchain. DID provides a unique identity for each user, which can be used for authentication and authorization purposes. The algorithm takes user's role as input and outputs a unique DID.

To design a Decentralized Identifier (DID) system for users participate in academic certificate issuance and verification using Hyperledger Fabric blockchain, unique DIDs need to be assigned based on user roles are identified and verified. For DID registry, which is a decentralized service that allows for the management of DIDs and the resolution of their associated DID Documents. Each document includes information such as associated public key, service endpoint to access the DID, and its related details. The DID document storage and maintenance of its safety must be regulated on Hyperledger Fabric blockchain. This can be accomplished by creating a private data collection on the blockchain, which allows for the storage of private data which should be made accessible to specific network members. DID document resolution and consistent update should be permitted from DID registry, based on a smart contract responsible for the resolution of DIDs can be implemented. The functionality to update DID documents as required, such as when a user changes their public key or service endpoint should be supported.

2.2 Workflow of Proposed Model PACIV

The Figure 3 represents a decentralized and secure system for issuing and verifying academic certificates using Hyperledger Fabric blockchain and integrating various digital identity technologies, such as Decentralized Identifiers (DID), Self-Sovereign Identity (SSI), and Verifiable Credentials (VC).The entities involved in this system include: (a)Issuer: This could be an educational institution or organization that issues academic certificates; (b) Owner: Represents the individual who receives the academic certificate and is the rightful owner of the credential; (c) Verifier: Defines the employer or a third-party organization that needs to verify the authenticity of the academic certificate; (d) Education authority: Defines government or regulatory body responsible for overseeing the education sector;

The key components of Hyperledger Fabric that enable this network are the Fabric CA (Certificate Authority) and the ledger management system. All entities involved in the system are registered using Fabric CA, which provides them with public and private keys. After being approved by Fabric CA, entities can publish schemas and DID (Decentralized Identifiers) on the ledger, enabling them to interact with the system based on their specific roles. The issuer and verifier use suggested protocols to issue and verify VC (Verifiable Credentials) based on SSI (Self-Sovereign Identity) principles. SSI allows individuals to control their identity information and share it securely with others without relying on third-party intermediaries. VC is a cryptographic proof that represents a credential, such as an academic certificate, that has been issued by an issuer and can be verified by a verifier. To issue an academic certificate, the issuer creates a VC containing the necessary information, such as the name of the owner, the name of the issuing institution, the type of degree or certificate, and the date of issuance. The owner then receives the VC and stores it securely in their digital wallet. Once owner needs to provide proof of their academic credential, they can share the VC with the verifier. The verifier can then verify the authenticity of the VC using the cryptographic proofs and information contained within it. The proposed model for managing academic certificates, defines multiple steps. Issuer, defines typically a university, generates academic certificates in the form of Verifiable Credentials (VCs). The VCs contain a set of tamper-evident claims about the student and metadata that cryptographically prove the issuer's identity. Upon issuing a VC, the organization attaches its public Decentralized Identifier (DID) to the credential. This public DID is also registered on the Hyperledger Fabric blockchain, which acts as a verifiable data registry. Therefore, anyone can verify the organization associated with a specific public DID without contacting the issuer. The next step involves the holder, i.e., the student, consenting to accept or reject the issued credential. If accepted, the holder can receive the credential and store it in their digital wallet, which could be a web or mobile wallet. The holder stores the private key for the DID in their wallet, while the public keys are registered on the blockchain by the issuing authority. Subsequently, the issuer registers their information and corresponding public key on the Hyperledger Fabric ledger. When the holder presents the certificate in the form of a VC to a verifier, the verifier requests the public key of the university from the blockchain to verify its validity. Once the verifier receives the university's public key and cryptographic materials from the blockchain, the certificate can be cryptographically verified. In summary, the workflow of this model involves issuing academic certificates as Verifiable Credentials, associating a public DID with the credential, registering the public DID on the Hyperledger Fabric blockchain, and having the holder store the private key for the DID in their digital wallet. The issuer registers their details and corresponding public key on the blockchain, and the verifier requests the public key of the university from the blockchain to verify the authenticity of the credential.

3 Results and Discussion

3.1 Issuance and Verification Protocols for Academic Certificates Issuance and Verification

This section details with protocols developed for issuing and verifying academic credentials with a focus on preserving privacy. To ensure consistency, as per W3C Verifiable Credentials Data Model v1.0, various terms are defined and adopted. (a) "credential" refers to a certificate issued by an educational institution in the name of a student; (b) "issuer" denotes the educational institution responsible for issuing academic credentials. In this context, we use the terms "issuer" and "university" interchangeably; (c) "holder" is the recipient of academic credentials, and we use the terms "holder" and "student" interchangeably; (d) "verifier" represents entities or individuals seeking to verify credentials.

To design SSI (Self-Sovereign Identity) model over the Hyperledger Fabric blockchain is adopted various protocols need to be followed as part of design and implementation. This model consists of two primary processes: ledger management and verifiable credential workflows. Previous section discusses on the components of ledger management, and this section proposes on protocols for academic credential issuance and verification. Figure 2 provides an illustration of the SSI-based approach for certificate issuance and verification on Hyperledger Fabric.

To establish a secure and decentralized network for managing academic certificates, Hyperledger Fabric blockchain technology can be adopted. The key components of Hyperledger Fabric that enable this network are the Fabric CA (Certificate Authority) and the ledger management system. All entities involved in the system are registered using Fabric CA, which provides them with public and private keys. After being approved by Fabric CA, entities can publish schemas and DID (Decentralized Identifiers) on the ledger, enabling them to interact with the system based on their specific roles. The issuer and verifier use suggested protocols to issue and verify VC (Verifiable Credentials) based on SSI (Self-Sovereign Identity) principles. SSI allows individuals to control their identity information and share it securely with others without relying on third-party intermediaries. VC is a cryptographic proof that represents a credential, such as an academic certificate, that has been issued by an issuer and can be verified by a verifier. To issue an academic certificate, the issuer creates a VC containing the necessary information, such as the name of the owner, the name of the issuing institution, the type of degree or certificate, and the date of issuance. The owner then receives the VC and stores it securely in their digital wallet. When the owner needs to provide proof of their academic

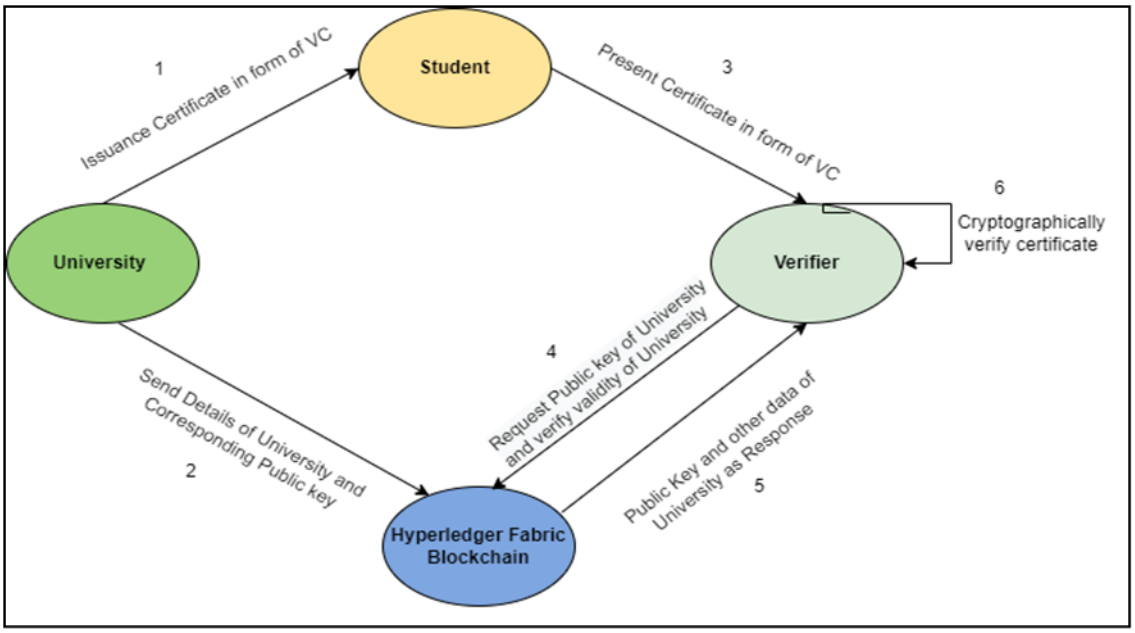

Fig 2. SSI-based approach for certificate issuance and verification on Hyperledger fabric

credential, which can share the VC and verifier. The verifier can then verify the authenticity of the VC using the cryptographic proofs and information contained within it. The proposed model for managing academic certificates, consists of several steps. Firstly, the issuer, which is typically a university, generates academic certificates in the form of Verifiable Credentials (VCs). The VCs contain a set of tamper-evident claims about the student and metadata that cryptographically prove the issuer's identity. Upon issuing a VC, the organization attaches its public Decentralized Identifier (DID) to the credential. This public DID is also registered on the Hyperledger Fabric blockchain, which acts as a verifiable data registry. Therefore, anyone can verify the organization associated with a specific public DID without contacting the issuer. The next step involves the holder, i.e., the student, consenting to accept or reject the issued credential. If accepted, the holder can receive the credential and store it in their digital wallet, which could be a web or mobile wallet. The holder stores the private key for the DID in their wallet, while the public keys are registered on the blockchain by the issuing authority. Subsequently, the issuer registers their information and corresponding public key on the Hyperledger Fabric ledger. When the holder presents the certificate in the form of a VC to a verifier, the verifier requests the public key of the university from the blockchain to verify its validity. Once the verifier receives the university's public key and cryptographic materials from the blockchain, the certificate can be cryptographically verified. In summary, the workflow of this model involves issuing academic certificates as Verifiable Credentials, associating a public DID with the credential, registering the public DID on the Hyperledger Fabric blockchain, and having the holder store the private key for the DID in their digital wallet. The issuer registers their details and corresponding public key on the blockchain, and the verifier requests the public key of the university from the blockchain to verify the authenticity of the credential.

3.2 Performance Analysis and test bed

Fabric blockchain test bed is set up with five organizations carrying one peer each. PACIV approach is used with three order to avoid any delay even when one order is down. The endorsement policy requires at least one peer to be an endorser from each organization. The network is set up on a virtual machine with Linux Ubuntu 20.04 with 12 CPU cores at different instances to check the performance with 64 GB RAM. Test bed was implemented as an "infrastructure" to integrate monitoring tools. Each experiment that carried out uses fixed and variable rate controllers and recorded.

Performance evaluation assesses the system's speed, throughput, and latency. The number of transactions per second (TPS) and the response time of the system can be used to measure performance. Transaction throughput is the number of transactions that can be processed per second by the system, calculated as shown in (1.1) and (1.2).

$$Transaction\ throughput = Number\ of\ transactions\ processed\ /\ Time \tag{1.1}$$

Confirmation time is the time it takes for a transaction to be confirmed and included in the blockchain. It can be calculated using the following formula:

$$Confirmation\ time = Time\ when\ the\ transaction\ is\ confirmed - Time\ when\ the\ transaction\ is\ initiated \quad (1.2)$$

Security features, such as encryption, hashing, and access control, can be evaluated based on their implementation and effectiveness. Privacy features, such as zero-knowledge proofs and self-sovereign identity, can be evaluated based on their ability to protect users' privacy. Experiment carried out for proposed PACIV can be observed throughput and latency.

Performance of PACIV shows an average throughput of 476 Mbps, for variable peer loads and blocks in use, with observed throughput (Figure 3) of 371 Mbps for blocks of 10 with peers in use up to 10 peers and increases to average of 579 Mbps for higher peers. Observed time taken (Figure 4) for a transaction to complete is found to be 320ms for 100 peers to 479ms for 400 peers in use. PACIV is able to show optimally improved thorough put taken for a transaction process in comparison to SPChain[11] proposed by Renpeng Zou et al as shown in Figure 5. This study and its performance analysis demonstrates that PACIV is able to manage high throughput for 100 Peers and 200 block of Peers adaptively in comparison to SPChain[11] approach. Hence for controlled adaptive throughput PACIV with SSI model is novel in terms of optimized execution.

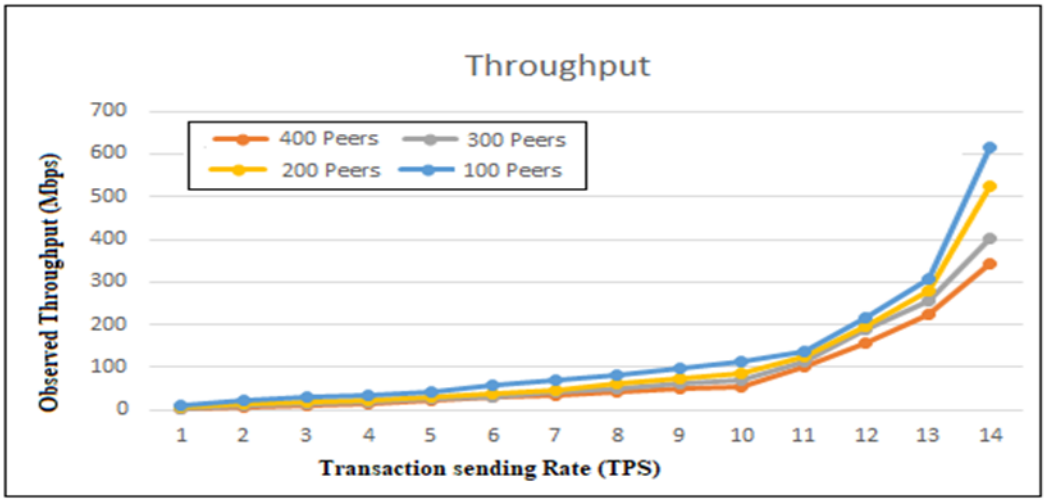

Fig 3. Observed Throughput for execution of process with variable number of nodes

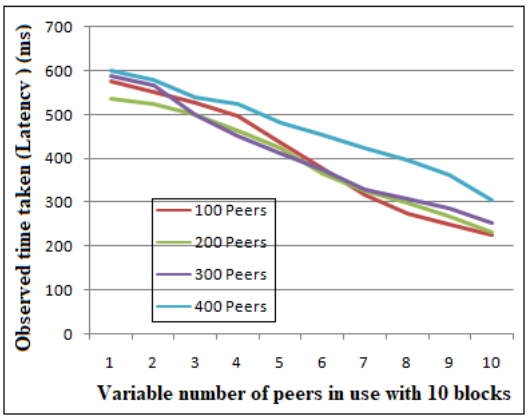

Fig 4. Observed Time taken for execution of process with variable number of nodes

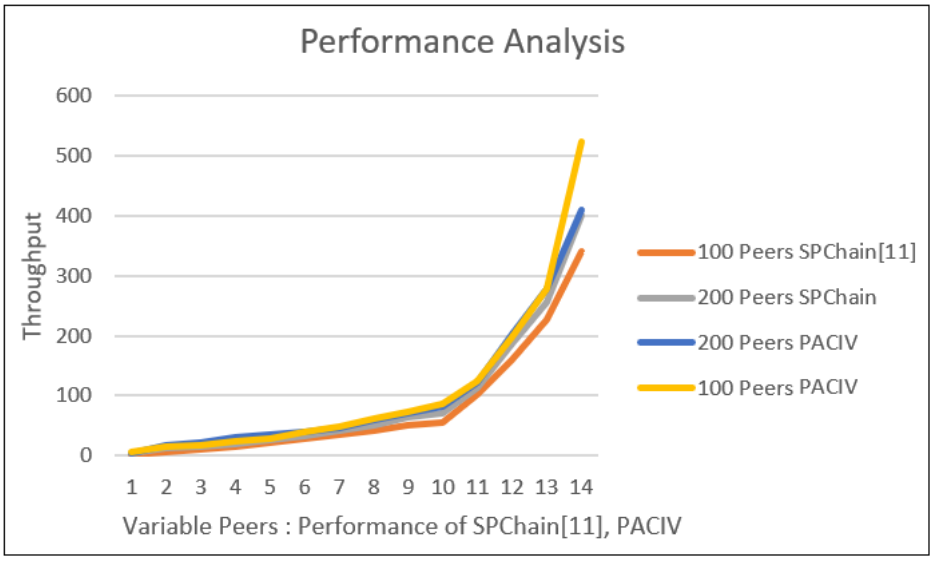

Fig 5. Comparison and Analysis of proposed PACIV with SPChain [11] approach

4 Conclusion

An academic organization [6] adopts different role and responsibilities towards issuance and providing academic certificates to student community and being handled by competent authority. Using blockchain-based applications for academic certificate issuance and verification poses a significant challenge for privacy preservation, particularly when it comes to public blockchains. A Decentralized Control Verification Privacy-Centered (PACIV) proposed in this research work, works on Hyperledger Fabric over blockchain to preserve and control the privacy of academic certificates using SSI approach. The proposed PACIV approach preserves the privacy of academic data, including student personal records, academic certificates, and related documents handling cost of scalability as well. This is achieved by providing complete authority over all network nodes, establishing private cloud based environment for academic institutes as well limiting access to the ledger.

PACIV approach emphasis on security which is resistant to different attacks as well restricting access to ledger entry and requiring approval from most connected peers before committing any changes. SSI method is incorporated to propose PACIV as well designed with a Hyperledger log report which measures the user activity consistently which is novel as part of research work defined. PACIV is proposed to predict attacks as well minimal time taken for multiple levels of security to be incorporated. This novel approach is proved in terms of preventing unauthorized access and providing a trusted and reliable verification process. In addition Hyperledger Fabric blockchain technology improves user interoperability and automation in the certificate verification process.

By utilizing Hyperledger Fabric blockchain technology and digital identities, our proposed protocol presents a significant step towards achieving a transparent and trustworthy academic certificate management system. Therefore, while the PACIV approach provides improved privacy and security, it also provides practical implementation and scalability for a large number of universities and verifiers. PACIV also can be adopted to securely manage and verify digital information as per user demand. Applications in the field of block chain for academic trust and management can be related to academic certificate management, verifying student's competencies and learning outcomes management. Additional applications can be extended to evaluating students' professional ability, protecting learning objects, securing collaborative learning environment, fees and credits transfer, obtaining digital guardianship consent. With regard to exams conduct and learning, competitive management, copyrights management, enhancing students' interactions in e-learning, examination review and supporting lifelong learning.

References

1) Khairwa A, Thangavelu A. Moving object detection for surveillance video frames using two stage multi-scale residual convolution neural networks. *International Journal of Grid and Utility Computing*. 2024;15(3-4):253–262. https://doi.org/10.1504/ijguc.2024.140124.
2) K DK, Senthil P, Kumar DSM. Educational Certificate Verification System Using Blockchain. *International Journal of Scientific & Technology Research*. 2020;9(3). Available from: https://www.ijstr.org/final-print/mar2020/Educational-Certificate-Verification-System-Using-Blockchain.pdf.

3) Liu M. Performance optimization for blockchain-enabled industrial internet of things (IIoT) systems: A deep reinforcement learning approach. *IEEE Transactions on Industrial Informatics*. 2019. https://doi.org/10.1109/TII.2019.2897805.
4) Zou R, Lv X, Zhao J. SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. *Information Processing & Management*. 2021;58(4):102604. (10-26). https://doi.org/10.1016/j.ipm.2021.102604.
5) Hu T, Liu X, Chen T, Zhang X, Huang X, Niu W, et al. Transaction-based classification and detection approach for Ethereum smart contract. *Information Processing & Management*. 2021;58(2):102462. https://doi.org/10.1016/j.ipm.2020.102462.
6) Salunkhe, Rajkumar S. Protection of Electronic Health Records (EHRs) on the Ethereum Blockchain: Identifying and Preventing Active Threats to Smart Contracts. *KSII Transactions on Internet and Information Systems*. 2025;19(1). https://doi.org/10.3837/tiis.2025.01.010.
7) Kolokotronis N. Secured by blockchain: Safeguarding internet of things devices. *IEEE Consumer Electronics Magazine*. 2019;8(3):28–34. https://doi.org/10.1109/MCE.2019.2892221.
8) Chaudhari S, Mohite S, Kumbhakarn S, Rathod V, Khairnar S. Blockchain based solution for academic certificate management system using smart contract. *International Journal of Science and Research Archive*. 2023;8(1):291–297. https://doi.org/10.30574/ijsra.2023.8.1.0037.
9) Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. *Future Gener Comput Syst*. 2020;107:841–853. https://doi.org/10.1016/j.future.2017.08.020.
10) Huynh-The T, Gadekallu TR, Wang W, Yenduri G, Ranaweera P, Pham QV, et al. Blockchain for the metaverse: A Review. *Future Generation Computer Systems*. 2023;143:401–419. https://doi.org/10.1016/j.future.2023.02.008.
11) Ma C. The privacy protection mechanism of hyperledger fabric and its application in supply chain finance. *Cybersecurity*. 2019;2(1):1–9. https://doi.org/10.1186/s42400-019-0022-2.
12) Shala B. Blockchain and trust for secure, end-user-based and decentralized iot service provision. *IEEE Access*. 2020;8:119961–119979. https://doi.org/10.1109/ACCESS.2020.3005541.
13) Pajooh H, Rashid M, Alam F, Demidenko S. Hyperledger Fabric Blockchain for Securing the Edge Internet of Things. *Sensors*. 2021;21:359. https://doi.org/10.3390/s21020359.
14) Bellini E, Iraqi Y, Damiani E. Blockchain-based distributed trust and reputation management systems: A survey. *IEEE Access*. 2020;8:21127–21151. https://doi.org/10.1109/ACCESS.2020.2969820.
15) Ghani F, Salman AA, Khudhair AB, Aljobouri L. Blockchain-based student certificate management and system sharing using hyperledger fabric platform. *Periodicals of Engineering and Natural Sciences*. 2022;10(2):207–218. https://doi.org/10.21533/pen.v10i2.2839.