INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

Analysis and Implementation of Academic Documents Privacy-Preserving Management Model using Dynamic VC and DID Over Hyperledger Fabric Blockchain Technology - PADV

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

OPEN ACCESS

Received: 16/09/2025
Accepted: 27/10/2025
Published: 23/11/2025

Citation: Sathya K, Saraswathi A (2025) Analysis and Implementation of Academic Documents Privacy-Preserving Management Model using Dynamic VC and DID Over Hyperledger Fabric Blockchain Technology - PADV. Indian Journal of Science and Technology 18(42): 3370-3382. https://doi.org/10.17485/IJST/v18i42.1410

* **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

Abstract

Objectives: Providing an efficient privacy preservation approach of academic documents is the primary objective of this research work. **Methods:** Proposed privacy-preserving of academic documents verification model for academic certificate issuance and verification using Hyperledger Fabric over dynamic VC and DID blockchain technology. It can handle privacy and security challenges present in existing academic document's issuance and verification systems, while also enhancing their efficiency and accuracy among different users. **Findings:** PADV proposed approach is tested over a cloud for different users from academic coordinator, student, executive or issuer perspective over 200 peers up to 400 peers to generate multiple blocks of document. The performance of PADV for 200 and 400 Peers engaged in generating and providing privacy / protection for academic documents which shows maximum of 760 Mbps for 400 peers and 587 Mbps for 200 Peers. SP-Chain shows a maximum of 515 Mbps for 400 Peers and 378 Mbps for 200 Peers. The performance of proposed work PADV is verified over real-time elastic cloud environment running on multiple peers. PADV performs with an optimal higher throughput and minimal latency time compared to other models. **Novelty:** Creating dynamic verification credentials (VC) assigned to academic documents as unique credits along with DID adds more privacy and security to document.

Keywords: Hyperledger Fabric; Blockchain; Dynamic Verification Credential; DID; Latency time

1 Introduction

Providing security over documents relies on trust in the platform and faces the risk of a single point of failure [1]. Furthermore, verifiers have to trust that the issuer was correctly verified by the platform, and credential holders [2] have to trust that the platform's database and identity system will not tamper with their data. To address these challenges, this research aims to explore blockchain-based academic certificate issuance and verification systems. Academic certificates [3], [4] are formal documents issued by educational institutions that represent a student's completion of a degree program or other educational training. They typically contain information such as the student's name, institution name, student id, type of degree or training received, date of completion, and other relevant details. The credibility and integrity of academic documents are essential [5], as they help build trust and confidence in the education system. It is important to preserve the privacy and security of academic certificates once issued and verified, as they contain sensitive information about the recipient and are often used for employment, continuing education, and other purposes. The use of blockchain technology and other privacy-preserving techniques can help ensure the authenticity and privacy of academic certificates, protecting them from fraud and misuse.

When a student presents an academic certificate to a verifier, the verifier can use various components, such as the issuer's legitimacy and the signature's authenticity, to verify the certificate's authenticity. However, due to technological support and advancements fake academic certificates are created [6], manipulated, which causes managers verifiers to lose trust in academic certificates [2] and users with improved skill set. Verifiers follow different models, approaches, which is challenging to manually examine the academic documents for tampering or inconsistency, or contacting universities for proof / update. However, these methods are time-consuming [7], costly, and not entirely authenticated. Several solutions to generate trust between the user as a student and verifier, such as using legal systems to create laws [8] that punish the presentation of tampered documents, trusted third parties to verify the certificate, and embedding proof of authenticity such as watermarks or holograms that do not support authentication solution. However, these solutions have drawbacks, such as laws being hard to enforce, technical solutions being necessary [9], and the possibility of abuse of power by third parties or data breaches. Therefore, preserving the privacy and security of academic documents is essential to maintain trust between students and verifiers [10].

Authorized Academic certificates issuance and verification system can be implemented [11] using least cost and time required models such as privacy-preserving models using blockchain. This approach suggests a promising alternative to traditional paper-based methods [9]. 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 [12] [13]. Dynamic Consent Management Systems (DCMS) [14] utilizes blockchain technology with privacy support for documents in addition to security as well decentralization of abstract entity data controller models to support consent privacy. This approach supports assess of dynamic content effectiveness of decentralized system settings, along with a dynamic overview of DCMS, to suggest electronic forms usage and its overall implementation. Research work proposed by Liu et al [15] suggests a secure blockchain-supported for a privacy-preserving ACS (access control scheme) over IoT system, which adopts the fully homomorphic encryption (FHE) model.

This model is supposed to support confidentiality of publishing events and utilize ledger mechanism to store volumes of large data over a cross domain access of information. The proposed study aims to create and assess a privacy-preserving model for academic certificate issuance and verification using Hyperledger Fabric [16] over dynamic VC and DID blockchain technology. This study aims to handle privacy and security challenges present in existing academic document's issuance and verification systems, while also enhancing their efficiency and accuracy among different users.

Research Gap: On analysis of literature work carried out in this domain of research towards improved security for academic certificate issuance and utilization over different variable users is primary research gap identified. The research paper provides a thorough explanation of the design of dynamic verifiable credentials (VC) and digital identifiers (DID), which are integrated through a smart contract on the created Hyperledger network. Additionally, a privacy channel is established on the network, and an off-chain verification schema has been developed to preserve the privacy of students' data and verifiers' identities. This paper offers a comprehensive overview of the model's design and implementation, emphasizing the key components and their integration to ensure privacy and security in academic certificate issuance and verification on the blockchain. Though existing research works suggest providing security as a major metric, this proposed work PADV analyses its performance using throughput (Mbps) along with time taken for analysis as shown in Section-3.4

2 Methodology

2.1 Model Description

2.1.1. Academic Documents Issuance and Verification Model

The process of issuance and verification of academic documents involve a system or method that approves enabling academic documents such as qualification degrees, such as diplomas, degrees, and documents. This model is explained in detail by[6],[17] and consists of several elements, including the issuer, recipient, verifier, certificate, issuance process, and verification process. The issuer is responsible for providing the certificate to the recipient who has completed the required coursework or training. The verifier then authenticates the certificate by confirming the issuer's records and the recipient's identity. The academic certificate issuance and verification model[3] is crucial in preserving the credibility and integrity of academic qualifications, which promotes trust and confidence in the education system. The model follows a standard process that involves the recipient submitting transcripts or other documentation to the issuer. The issuer then reviews the documentation and issues the academic certificate to the recipient if satisfied. Finally, the recipient presents the certificate to a verifier, who checks its authenticity by verifying the issuer's records.

2.1.2. Design and Analysis of PADV

Block chain design and implementation (ref Figure 1) is a decentralized[2], secure, and tamper-proof ledger that stores information in a way that cannot be altered or deleted. When the student needs to prove the authenticity of their certificate, they present it to verifier. The verifier module (Refer Section 4.2-(b)) then checks the certificate's authenticity by verifying it with the blockchain ledger created each instance[5]. The verifier accesses the blockchain to retrieve the certificate, and the blockchain confirms the authenticity of the certificate. If the certificate is verified successfully, the verifier approves it. However, if the verification process fails, verifier rejects the certificate. Using blockchain technology for academic certificate verification eliminates the need for physical documents, which can be lost or forged. It also makes the verification process more efficient, reliable, and secure. The blockchain provides a tamper-proof, decentralized storage solution for academic documents, ensuring that they cannot be altered or deleted without proper authorization. Overall, this approach provides a more secure and efficient way of verifying academic certificates, reducing the risk of fraud and increasing trust in the certificate issuance and verification process. Section-3.1 discuss and analyze the functional and non-functional requirements for a digital academic documents management system. Understanding these requirements is crucial for developing a system that meets the needs of all stakeholders involved in the certificate issuance and verification process.

2.1.3. Functional Requirements for academic documents verification system

A blockchain-based academic documents issuance and verification system, functional requirements might include the ability to issue, verify, and store academic, the required documents on cloud of blockchain. It may also include the capability to integrate with other systems such as student information management systems and academic databases. Additionally, the system may need to have features such as user authentication, document instance revocation, and documents transfer[1]. Proposed system PADV should prove its credibility and security enough to prevent unauthorized access and tampering of documents. Approach should be scalable enough to handle a large number of certificate issuances and verifications.

2.1.4. Design of Hyper Ledger based Academic Documents Issuance and Verification system (PADV) for privacy and authentication involves the following steps

1. Determine the system requirements: Before designing and developing the system, it's important to determine the requirements. This includes both functional and non-functional requirements, such as the type of academic documents that the system will handle, the expected number of users, the level of privacy and security required, and the desired performance metrics.
2. Choose the appropriate blockchain platform: In this case, Hyperledger Fabric is a suitable blockchain platform for implementing a privacy-preserving academic certificate issuance and verification system. It provides a permissioned blockchain network, which allows for greater control over access and security.
3. Implement Self-Sovereign Identity (SSI) and Decentralized Identifiers (DIDs): SSI and DIDs are important components of a privacy-preserving system. SSI allows individuals to control their own identities, while DIDs provide a way to uniquely identify entities on the blockchain. These technologies can help protect the privacy of users and ensure that only authorized individuals have access to academic documents.

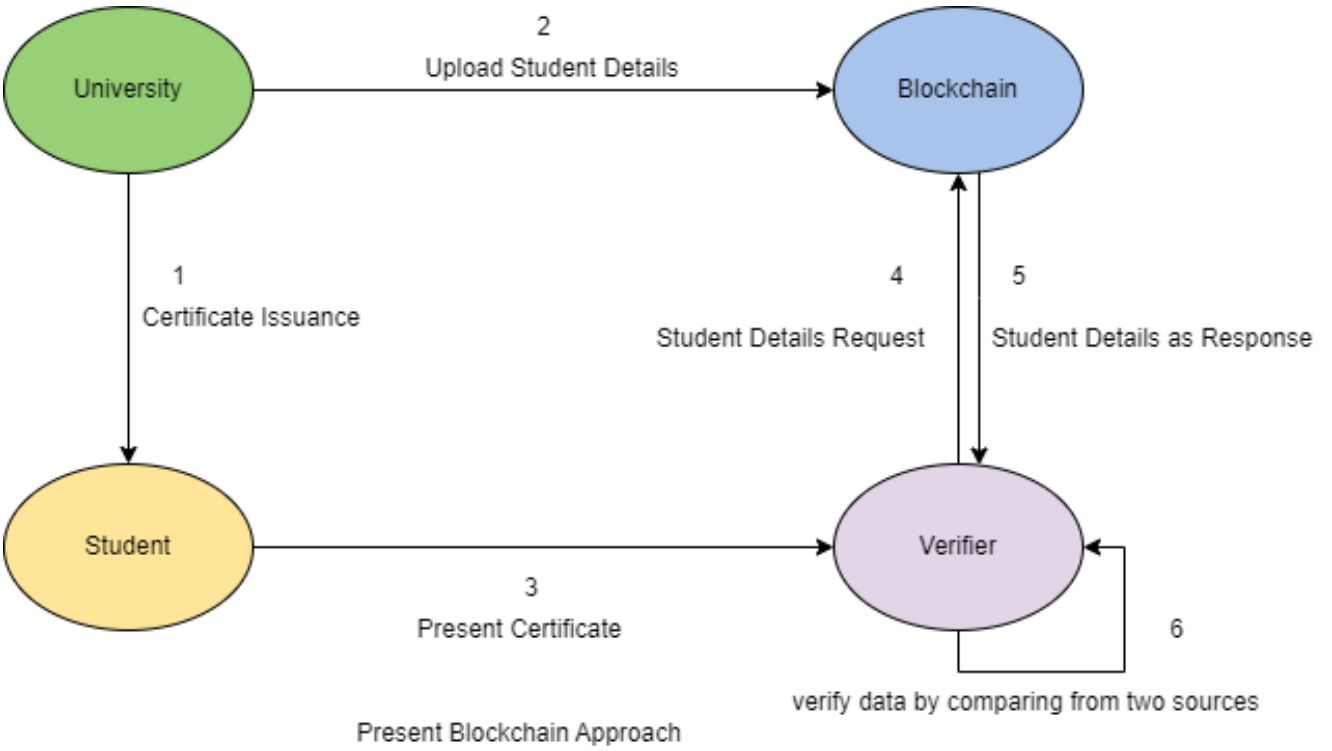

Fig 1. Generic block chain academic documents verification model

4. Using dynamic Verifiable Credentials (VCs)[7] to issue and verify academic documents: Dynamic VCs provide a way to issue and verify credentials in a decentralized manner, without the need for a central authority. This can help improve the security and privacy of academic certificate issuance and verification.
5. Implement privacy-preserving techniques: There are various privacy-preserving techniques that can be implemented in a blockchain-based system, such as zero-knowledge proofs, ring signatures, and homomorphic encryption. These techniques can help ensure that sensitive data is kept confidential and secure.
6. Test and deploy the system: Once the system has been designed and developed, it needs to be thoroughly tested to ensure that it meets the desired requirements. This includes testing the performance, security, and privacy of the system. Once testing is complete, the system can be deployed and made available to users.

When designing an academic document credentialing system that utilizes blockchain technology, there are several key components that must be considered. These components include the SSI, DID, VC, verification process, and system testing and deployment as shown in Figure 2. The SSI, or self-sovereign identity, is a crucial element of the system, as it provides individuals with control over their personal data and credentials. DID must be designed with security in mind to provide a tamper-proof identity[16]. Dynamic Verifiable credentials, or VCs, are digital representations of academic documents that can be issued, stored, and verified on the blockchain. It is essential to include all necessary information, such as the name of the institution, student name, degree earned, time of access, access system details and date of issuance. VCs should also comply with industry standards such as the W3C Verifiable Credentials Data Model[7]. Dynamic verifiable credentials are a type of Verifiable Credential (VC) which can change or update instantly over time. Unlike static VCs which hold a fixed piece of information, dynamic VCs allow for changes to be reflected within the credential itself. Verification is critical in any academic credentialing system, and the verification process must be designed to ensure the authenticity of the VC. Utilizing cryptographic techniques such as digital signatures and hashes can help ensure that the VC has not been tampered with. Finally, the system should be thoroughly tested to ensure that it meets the requirements and functions as intended. Once testing is complete, the system can be deployed to the production environment. **Algorithm 1** outlines the major steps involved in Hyperledger Fabric-based DID and VC Certificate Issuance Algorithm.

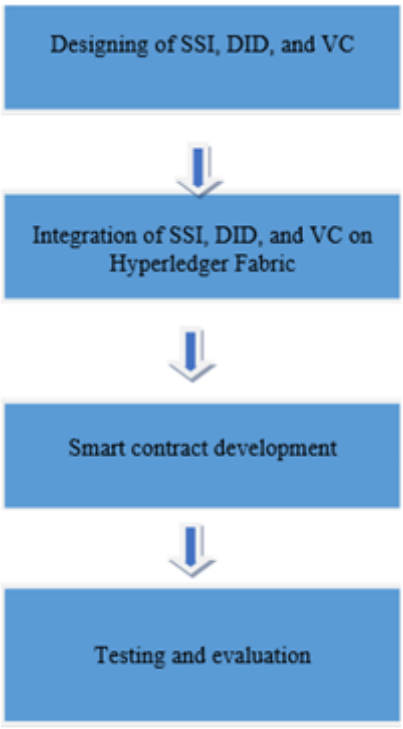

Fig 2. Overview of Proposed model – PADV

2.1.5. Algorithm and approach

Algorithm 1: Hyperledger Fabric-based DID and Dynamic VC Certificate Issuance
Input: individualId (string), certificateCriteria (object), dynaVC (string)
Output: certificateTransaction (object)
1. Define the certificate issuance process and criteria.
2. Define ***certificateCriteria*** as an object with relevant certificate information such as the type of certificate, course, and institution.
3. Create a unique decentralized identifier (DID) ***individualId*** for the individual using a DID method of your choice.
4. Use the DID to create a digital wallet that stores the individual's credentials.
5. Generate new dynamic verifiable credential (VC) transaction ***dynaVC*** using the Hyperledger Fabric blockchain.
6. Use the institution's private key to digitally sign the transaction.
7. Embed individual's DID with document information to the transaction data, time of access, user-id, system-details as Dynamic VC.
8. Submit the transaction ***certificateTransaction*** to the Hyperledger Fabric blockchain for verification and validation.
9. Once the transaction is validated and confirmed, the certificate is issued to the individual's digital wallet.

The Hyperledger Fabric-based DID and dynamic VC certificate issuance algorithm given in **Algorithm (1)** is a set of steps that outlines how to issue academic documents securely and efficiently using blockchain technology. The algorithm takes individualId, a unique identifier for the recipient, and certificateCriteria, an object that defines the certificate issuance criteria, as input. The algorithm then creates a unique decentralized identifier (DID) for the individual and uses it to create a digital wallet that stores the individual's credentials. Next, the algorithm creates a new dynamic verifiable credential (VC) transaction on the Hyperledger Fabric blockchain using the certificate criteria defined in the input. The institution's private key is used to digitally sign the transaction, ensuring that it is tamper-proof and authentic. The individual's DID, relevant certificate information, time of access, system-id are then embedded to transaction data as a dynamic VC. Finally, the transaction is submitted to the Hyperledger Fabric blockchain for verification and validation. Once the transaction is validated and confirmed, the certificate is issued to the individual's digital wallet. This algorithm enhances the security and ownership of academic documents by using

self-sovereign identity (SSI) principles, blockchain technology, and industry standards such as the W3C Verifiable Credentials Data Model.

An improved and efficient authenticated model PADV (Privacy control and verification system for Academic Documents) has been developed and integrated with Hyperledger Fabric blockchain. This protocol ensures that universities can collaborate without compromising data privacy and security. The PADV protocol involves the following steps:

1. An admin, who is occupying role of higher authority of organization can create and manage, control group, creates organizations.
2. Each education authority creates a channel that connects the universities. The channel is authenticated by the governance body.
3. Each university creates its own peers as members.
4. The peers of a given university host a copy of the ledger and validate transactions before committing to the ledger.
5. Approved educational institutions can host the ledger.
6. The university organization generates identities for each student as a authorized user.
7. The university organization (admin) is the only entity that can issue documents in the network.

By following these steps, the PADV protocol ensures that data privacy and security are maintained while collaboration between universities is facilitated. It is important to note that anonymity is not preferred in the educational environment as it is essential for universities to be known entities. In Hyperledger Fabric, a channel is a mechanism for forming a communication path between multiple organizations. In this scenario, a channel named ACM has been created as shown in Figure 3, which contains two organizations, Education Authority and Validator. The channel is set up to enable collaboration between the organizations while maintaining data privacy and security. Only members of the Education Authority organization have permission to write the blockchain, and they do not write student data directly. Instead, they write metadata such as the credential format containing attributes present in the credential, details of the entity that added the credential format, the public key of the university, and details of the entity that approved the university. This metadata will facilitate verification of the credentials. The University will declare a statement containing meta details that will be used to issue credentials. These meta details will be read by the verifier to cryptographically verify the credentials. Since no student data is added to the blockchain/ledger, this system is called a ”metasystem” It stores only cryptographic details and their provenance that will be needed to dynamic verify credentials. The Validator organization will have a copy of the blockchain/ledger and will serve as a watchdog to ensure that the Education Authority is not tampering with the data and working according to the rules and laws. The Validator also provides read access to the verifiers who will use the data to verify the credentials. The ACM channel has been set up to enhance privacy control in the educational environment by ensuring that universities and educational organizations can collaborate while maintaining data privacy and security.

3 Results and Discussion

3.1 Implementation of PADV

Academic documents are created in the form of verifiable data using the verifiable credential data model proposed by W3C. This enables documents to be converted into dynamic verifiable credentials, which can accommodate cryptographic operations. Verifiable credentials are created in JSON format, which is the most widely used format for data exchange on the web. To ensure privacy and security, the proposed verifiable credential workflow consists of three stages for PADV as shown in Figure 3:

1. Certificate issuance: The university or issuer issues verifiable credentials to students/owners. Additionally, the university sends the details of the university and the corresponding public key to the blockchain.
2. Certificate sharing: Students present their documents in the form of verifiable credentials to the verifier.
3. Certificate verification: The verifier requests the public key of the university and verifies the university's validity from the blockchain. The verifier then receives the public key and other data of the university as a response from the blockchain. The verifier then cryptographically verifies the certificate.

(a) Issuance protocol proposed in this research consists of four steps:

1. Bharathidasan University creates the credential definition for issuing a particular certificate and issues multiple certificates such as degree sheets to different students. The issuance process occurs off-chain, and no student data is added to the blockchain.

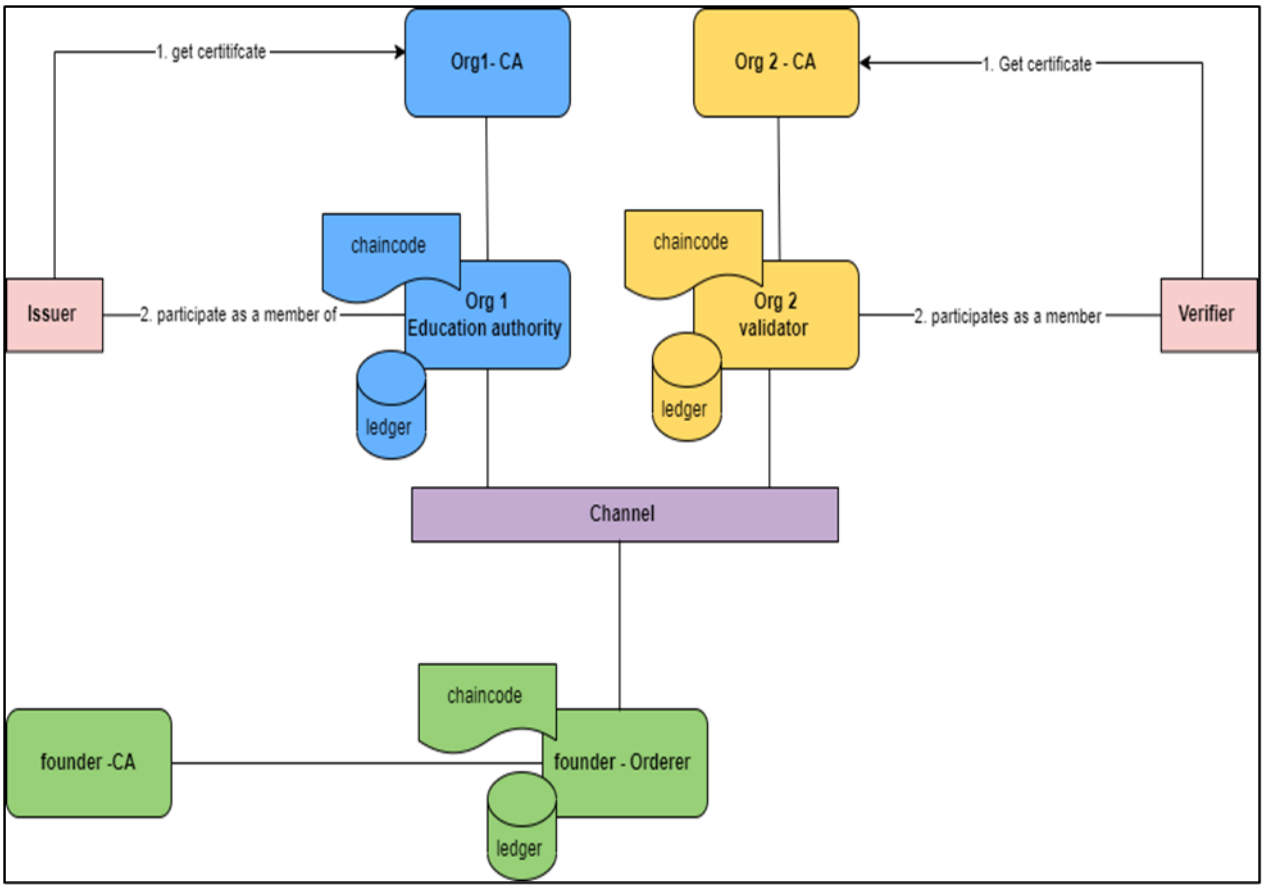

Fig 3. Hyperledger fabric-based blockchain channel for issuing and verifying academic documents: PADV design overview

2. A document such as Degree Certificate issued as a verifiable credential with attributes { Name, RegNo, Year of Passing_InstitutionName } declared in schema.
3. Verifiable credentials are signed by the public key.
4. Public key and schema are referenced in the ”credential definition.”

(b) Verification protocol proposed in this research includes the following steps:

1. Verifier module reads and understands the schema.
2. Verifier sends a request to the student user to understand the values of document attributes referenced in the schema.
3. Student sends a ”Verifiable Presentation” created from dynamic verifiable credential.
4. Verifiable Presentation contains a link to the credential definition, values of the attributes requested, and signature of the university authority
5. The verifier receives the Verifiable Presentation.
6. Using the Verifiable Presentation, the verifier constructs a verifiable credential. The verifier creates a JSON object with attributes from the schema and adds the values received from the student.
7. Verifier cryptographically verifies if the signature sent by the student matches the verifiable credential decrypted using the public key of the university referenced in the ”credential definition” created by the university.

Figure 4 shows the proposed approach for privacy-preserving academic certificate issuance and verification using dynamic verifiable credentials. PADV approach supports leveraging the immutable nature of blockchain to store, issue, and verify credentials which can change over time thus supporting the transparent nature of document standards as well ZKP (Zero Knowledge Proof).

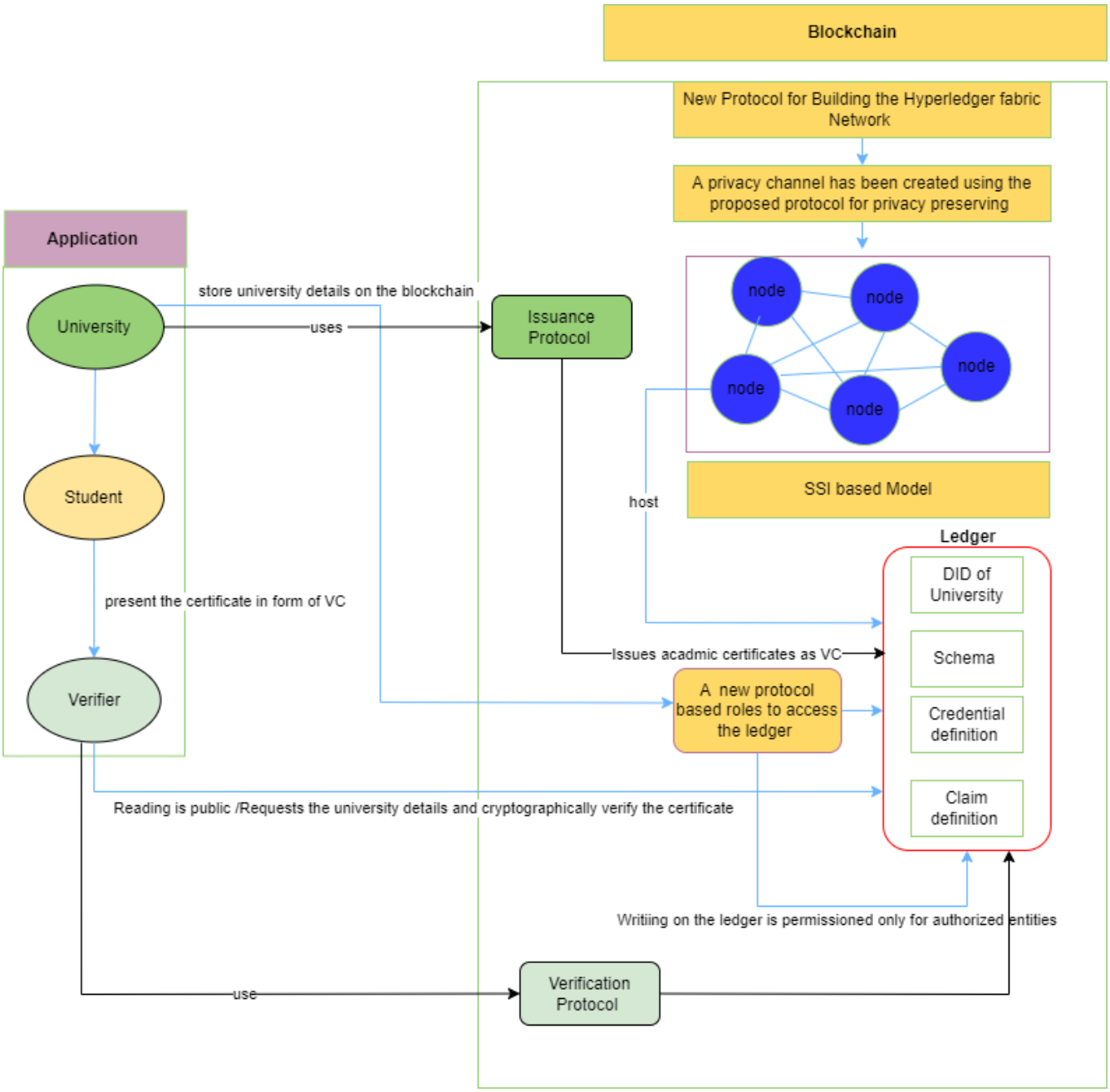

Fig 4. Proposed PADV model for privacy-preserving academic documents using certificate issuance and verification using dynamic verifiable credentials (VC)

3.2 Case Study

This research presents an example of a DID document design for a particular use case, illustrated in Listing 1 and encoded in the JSON-LD format. The DID document is uniquely identifiable by its ”id: issuerID” property, which in this case is set to ”1KoR4pzD59gfD2eUPvFp91KxCFy638EWhS” on line 3. Lines 2-3 define the DID method type, issuer identifier, and issuance timestamp. The subsequent lines, 4-9, describe the public key and its corresponding identifier, verification type, and key-value in multiple bases. Lines 10-20 specify the claims regarding the DID holder, including personal information and affiliations. The authentication method is defined in lines 25-28, outlining the method type, public key, and signature value. Lastly, lines 29-42 specify the proof method, which determines the verification type, creation timestamp, creator, verification method, and signature value used to sign the DID document. The example showcases how a DID document can be structured to include identifying information, personal information, and proof of authenticity. The JSON-LD format enables machine-readability and interoperability with other systems that use semantic web technologies.

Listing 1. Design of a DID document schema in JSON-LD 1 format.

```
1. {”context”: ”https://www.w3.org/ns/did/v1”,
2. ”issuer”: {
3. ”issuerID”: ”1KoR4pzD59gfD2eUPvFp91KxCFy638EWhS”,
4. ”publicKey”: {
5. ”type”: ”Ed25519VerificationKey”,
6. ”value”//16-bits ”9d45579de90a05d9a91cabab4cd379b1c2ac3cf7771fd9555ae87eadc48a0a81”
7. },
8. ”issuanceDate”: ”2025-07-01 20:37:19” },
9. ”student”: {
10. ”studentID”: ”1BoBiew5dkyZmAJF5XQApHBrHfrkyCocJw”,
11. ”fullName”: ”SathyaPriya”,
12. ”email”: ”sathya003@gmail.com”,
13. ”profileURL”: [
14. ”https://www.bdu.ac.in/”,
15. “https://linkedin.com/sathyaphd”],
16. ”affliation”: {
17. ”institutionID”: ”BhuG5QSWjPhD2025”,
18. ”institutionName”: ”GovtArtsCollege”,
19. “locationPlace”: “Karur,TN,India”
20. ”degree”: ”PhD_ComputerScience”,
21. ”department”: ”Department of Computer Science”,
22. ”regOnRoll”: ”P2019200”},
23. ”personalInfo”: {
24. ”type”: ”Ed25519Encryption”, // encryption type
25. ”phone”: ”+91######009”,
26. ”address”: ”################################################” },
27. ”publicKey”: {
28. ”type”: ”Ed25519VerificationKey”,
```

29. ”value”: ”75bfab0b5a43a1ab46370b97d49da713eaee19636c2ff847fe62efa81a6dd285”
30. } },
31. ”authentication”: {
32. ”type”: ”EdDSA”,
33. ”signature”: ”8b83c71c8c5a874e29bef72562d5a8d81b58cf8bceed97e04963bad3f37279dd5d0aed29de8f700b9fd86 381eef961a3bcba9bc0770de484a37e311e4ae01b03” },
34. }

3.2.1. Experimental Approach

To analyze and investigate performance of PADV with other block chain computational models such as SP-Chain[10] and CredChain[4], experiments had been proposed. CloudJoin model[6] of Computing Research Infrastructures (CRI) for deployment of large blockchain testbeds using hybrid dynamic cloud computing systems is used in this approach for variable set of resources and users. Experimental test-bed consists of varying number of resources, for every increase of 4 peers variable from number of peers 100 to 400 Table 1. The impact of the varying number of cloud nodes needs to be observed, based on five different tasks varying between 100,200, 250, 300, and 400 Mbytes. Experiment is conducted for variable iterations from 1 to 15 numbers to determine the throughput and latency effect as shown in Table 2.

Table 1. Cloud resource settings

Parameter Value	Type	Unit
Size	[1000, 3500]	[MI]
Required memory	[50,200]	[MB]
Input file size	[0.3,1.5]	[MB]
Output file size	[0.1,1]	[MB]
Deadline	[500, 2500]	[ms]
No of Peers	[200,400]	[nos]

Table 2. Attribute of cloud node settings for block chain

Parameter	Cloud	Unit
CPU processing rate	[3000, 10000]	[MIPS]
CPU usage cost	[1, 2.1]	[$/second]
Memory usage cost	[0.02,0.05]	[$/MB]
Bandwidth usage cost	[0.05,0.1]	[$/MB]
Memory	[256,4096]	[MB]
Delay	[50,250]	[ms]

Experiments are conducted using CloudJoin emulation model which interconnects on CloudLab using 2 VMs and different cloud resources supported 15 iterations so that values get saturated. This work is built using Amazon Managed Blockchain (AMB) which supports setting up and scale multiple blockchain networks. The basic building block interacts on chain code using the Hyperledger Fabric Command Line Interface (CLI). The designed **Java** supported blockchain application interacts with block network using Hyperledger Fabric SDK. This approach investigates the impact of the number of client user nodes; verification nodes being interconnected. Document requests are assigned to scheduler across multiple VMs with resources such that users may support the consume as per demand. The activities need to be tracked and credits to be exchanged between client nodes based on resource utilization.

3.3 Performance Analysis

The performance analysis of PADV is shown in Figure 5 and Figure 6, which shows the observed throughput and latency time (Delay) for variable number of peers engaged in communication for securing an academic certificate. The cloud bandwidth required for establishing a secured session to generate and access an academic document when a user makes a request and

creates a block chain of secured document between different cloud nodes engaged in communication. Hence throughput is considered as a major metric to define the efficiency and reliability of secured number of blocks or peers engaged to generate an academic certificate. Figure 5 shows the performance of PADV for 200 and 400 Peers engaged in generating and providing privacy / protection for academic documents which shows maximum of 760 Mbps for 400 peers and 587 Mbps for 200 Peers. SP-Chain shows a maximum of 515 Mbps for 400 Peers and 378 Mbps for 200 Peers. X axis indicates the saturation point (number of runs / iterations) required to achieve an optimal privacy limit as per blockchain standards using Fabric Hyper Ledger approach. Y-axis in graph indicates the observed latency – time taken (ms) to approach the optimal privacy limit of 400 peers of blocks involved in communication. Figure 6: Observed Latency Time (ms) for PADV for 400 number of peers engaged in providing privacy and protection for PADV as 567 ms, while SPChain shows 346 ms and CredChain shows 429ms.

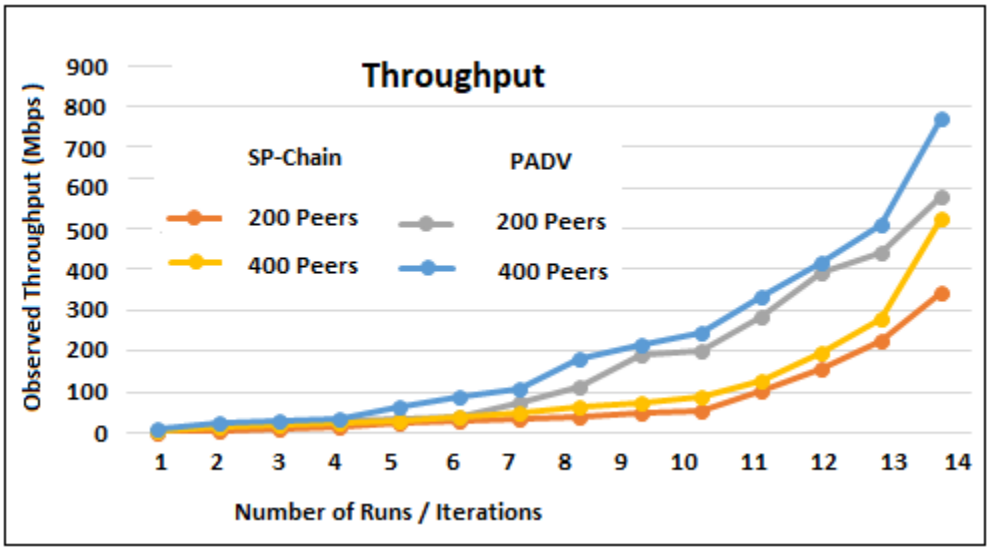

Fig 5. Observed Throughput of PADV

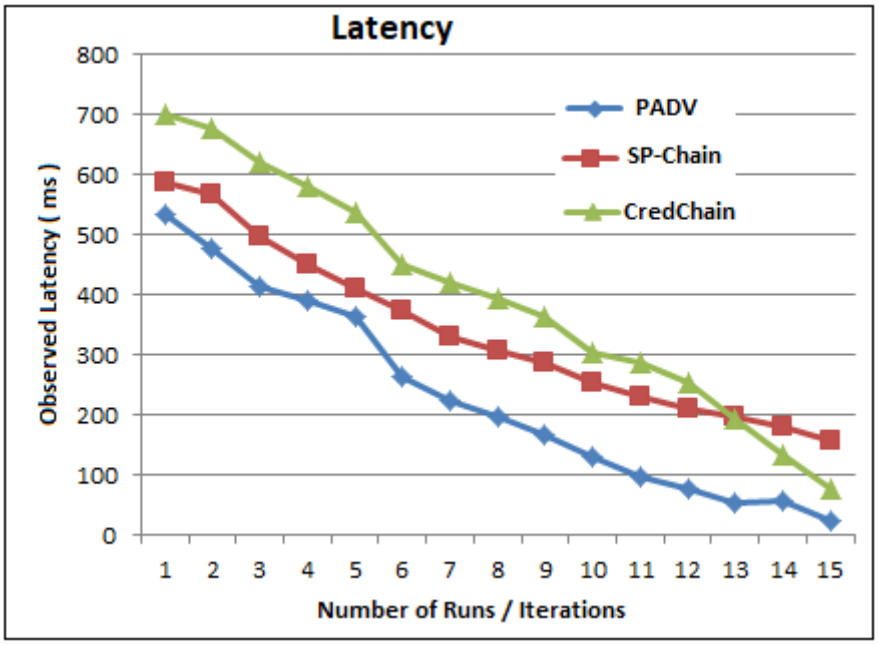

Fig 6. Observed latency (ms) for variable number of peers

The performance of proposed approach PADV is compared with existing models as shown in Figure 6 and Figure 7. Analysis of observed throughput for transmitted data as number of blocks over SPChain and proposed PADV suggests that observed throughput achieves a maximum of 82.6 % in comparison to DCMS approach which shows 67.8% while SPChain shows 64.8%. PADV attributes its efficient throughput due to dynamic VC implementation at terminal ends of proposed architecture.

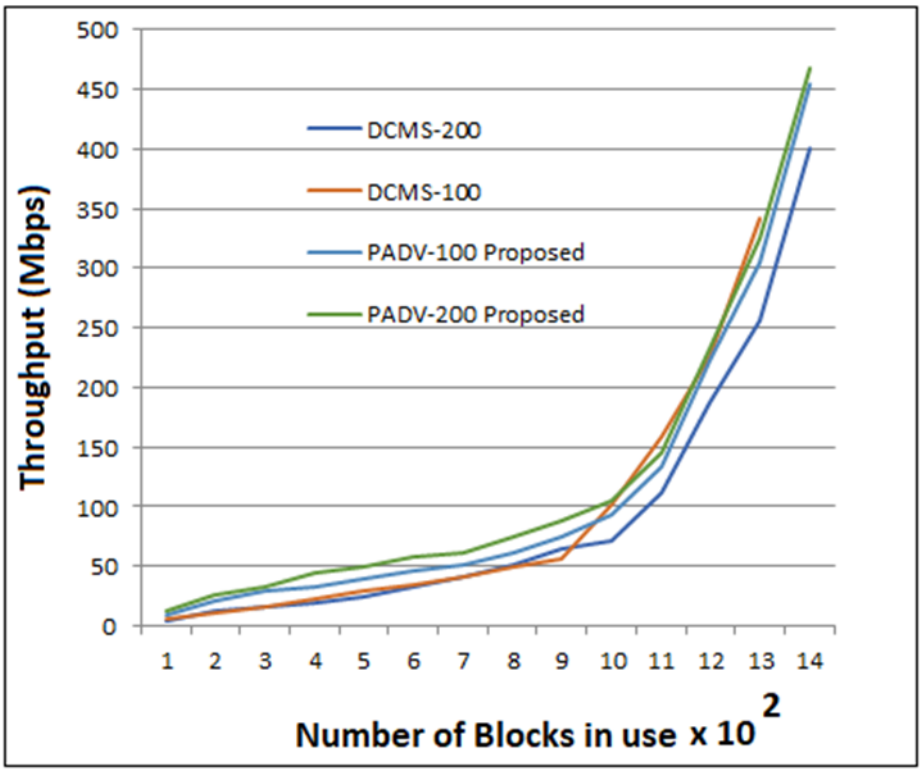

Fig 7. Comparison of Proposed PADV approach with other approaches

4 Conclusion

This study has proposed an efficient privacy and protection approach for academic documents using Fabric Hyper Ledger block chain approach. The proposed PADV approach is tested over a cloud for different users from academic coordinator, student, executive or issuer perspective over 200 peers up to 400 peers to generate multiple blocks of document. which showed an improved throughput of an average of 78.5 Mbps compared to 67.4Mbps in DCMS and SPChain models with minimal latency and efficient security applied with faster time taken to achieve in comparison to existing models as discussed in Figure 6.

To summarize design and implementation of proposed PADV, the authors have suggested definition of dynamic verification credentials and SSI for providing privacy among multiple users engaged in document with improved security by generating dynamic VC as key parameter which is novelty of proposed work and hence recommended for academic certificate verification and issuance model. Proposed PADV is found to prove its performance in terms of time taken for execution as well addressing key privacy and security challenges in the current academic certificate issuance and verification systems, while also ensuring data confidentiality, integrity, and authenticity. Though PADV suggests higher autonomy is achieving security model lacks in delayed latency when block transmission rate exceeds 200Mbps for recurring chain of blocks of data. Hence an improved version of PADV could support relative block of data verified such that large block of data can be supported.

References

1) El-Hindi M, Binning C, Arasu A, Kossmann D, Ramamurthy R. BlockchainDB: A shared database on blockchains. *Proceedings of the VLDB Endowment*. 2019;12(11):1597–1609. https://doi.org/10.14778/3342263.3342636.
2) Huang H, Lin J, Zheng B, Zheng Z, Bian J. When blockchain meets distributed file systems: An overview, challenges, and open issues. *IEEE Access*. 2020;8:50574–50586. https://doi.org/10.1109/ACCESS.2020.2979881.

3) Awaji B, Solaiman E, Albshri A. Blockchain-based applications in higher education: A systematic mapping study. *Proceedings of the 5th International Conference on Information and Education Innovations*. 2020;p. 96–104. https://doi.org/10.1145/3411681.3411688.
4) Harika G, Hareesh, Harshitha BH, Akash GA, Hema ND. Academic Credential Verification System Using Blockchain. *International Journal of Innovative Science and Research Technology*. 2024;9(11). https://doi.org/10.38124/ijisrt/IJISRT24NOV1597.
5) de Ocáriz Borde HS. An overview of trees in blockchain technology: merkle trees and merkle patricia tries. *University of Cambridge: Cambridge, UK*. 2022. https://doi.org/10.1145/3708622.3708624.
6) Ahmad RW, Salah K, Jayaraman R, Yaqoob I, Omar M. Blockchain in oil and gas industry: Applications, challenges, and future trends. *Technology in Society*. 2022;68. https://doi.org/10.1016/j.techsoc.2022.101941.
7) Krishna ESP, Arunkumar T. An improved security approach for attack detection and mitigation over IoT networks using HACABO and Merkle signatures. *International Journal of Internet Technology and Secured Transactions*. 2021;11(5-6):494–517. https://doi.org/10.1504/IJITST.2021.117419.
8) Shalaby S, Abdellatif AA, Al-Ali A, Mohamed A, Erbad A, Guizani M. Performance evaluation of Hyperledger Fabric. *Proc IEEE Int Conf Inform, IoT, Enabling Technol (ICIoT)*. 2020;p. 608–613. https://doi.org/10.1109/ICIoT48696.2020.9089614.
9) Zhang Y, Xu C, Lin X, Shen X. Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors. *IEEE Transactions on Cloud Computing*. 2021;9(3):923–937. https://doi.org/10.1109/TCC.2019.2908400.
10) Liang W, Zhang D, Lei X, Tang M, Li KC, Zomaya AY. Circuit copyright blockchain: Blockchain-based homomorphic encryption for IP circuit protection. *IEEE Transactions on Emerging Topics in Computing*. 2021;9(3):1411–1420. https://doi.org/10.1109/TETC.2020.2993032.
11) Xu Y, Zhang C, Wang G, Qin Z, Zeng Q. A Blockchain-Enabled Deduplicatable Data Auditing Mechanism for Network Storage Services. *IEEE Transactions on Emerging Topics in Computing*. 2021;9(3):1421–1432. https://doi.org/10.1109/TETC.2020.3005610.
12) Joshi AP, Han M, Wang Y. A survey on security and privacy issues of blockchain technology. *Math Found Comput*. 2018;1(2):121–147. https://doi.org/10.3934/mfc.2018007.
13) Uddin M. Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *Int J Pharm*. 2021;597. https://doi.org/10.1016/j.ijpharm.2021.120235.
14) Khalid MI, Ahmed M, Helfert M, Kim J. Privacy-First Paradigm for Dynamic Consent Management Systems: Empowering Data Subjects through Decentralized Data Controllers and Privacy-Preserving Techniques. *Electronics*. 2023;12(24):4973. https://doi.org/10.3390/electronics12244973.
15) Liu Z, Meng L, Zhao Q, Li F, Song M, Dai D, et al. A Blockchain-Based Privacy-Preserving Publish-Subscribe Model in IoT Multidomain Data Sharing. *Wireless Communications and Mobile Computing*. 2022;2022:2381365–13. https://doi.org/10.1155/2022/2381365.
16) Soelman M, Andrikopoulos V, Perez JA, Theodosiadis V, Goense K, Rutjes A. Hyperledger Fabric: Evaluating endorsement policy strategies in supply chains. *Proc IEEE Int Conf Decentralized Appl Infrastructures (DAPPS)*. 2020;p. 145–152. https://doi.org/10.1109/DAPPS49028.2020.00019.
17) Castro RQ, Au-Yong-Oliveira M. Blockchain and higher education diplomas. *European Journal of Investigation in Health, Psychology and Education*. 2021;11(1):154–167. https://doi.org/10.3390/ejihpe11010013.