JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 3032 - 3041
https://publishoa.com
ISSN: 1309-3452

Development of Novel Blockchain Technology for Certificate Management System using Cognitive Image Steganography Techniques

Sangeetha K.N[1], Dr. Seema Singh[2], Dr. Usha B.A[3].

Assistant Professor and Research Scholar of VTU, Dept of ECE, JSS Academy of Technical Education
(JSSATE) Bengaluru – 560060
Professor & Dean, External Relations, BMS Institute of Technology and Management, Bengaluru – 560064
Associate Professor, Dept of CSE, BMS Institute of Technology and Management, Bengaluru – 560064
Email: sangeethakn@jssateb.ac.in

ABSTRACT

The paper deals with the development of novel blockchain technology for certificate management system using cognitive image steganography techniques, in the sense, a secured approach of managing educational certificates using the blockchain and digital image steganography, providing an edge over existing systems is dealt with in greater detail. The provision for educational and governmental certificate authentication falls under the broad category of digital certificate issuance, authentication, and verification. Issuing certificates in this category can be difficult and time-consuming. Currently, existing systems for certificate management cannot guarantee data security and system trust. Using blockchain can solve this problem. This research is aimed to enhance the document verification process using blockchain technology and identify the security themes required for document verification in the blockchain. For the first time a survey of this type has been done where Blockchain and image steganography have been combined together to develop a complete backend infrastructure and the frontend application for the certificate management portal. With the proposed method PSNR & MSR of average 59 dB & 0.55 could be achieved. Exhaustive literature survey w.r.t. the recent development in the blockchain technology is also provided. The simulation results presented in the simulation results section shows the efficiency of the methodology that has been developed in the block chain field & thus has got an edge over the works done by other researchers in this field.

Keywords— Blockchain, Image Steganography, Digital certificate, Signature, Stamps, Simulation.

I. INTRODUCTION

Existing systems to manage certificates in any organizations such as schools, colleges and various government institutions to generate and store the certificates are not reliable and are not secure. There are several limitations in the existing system regarding the security of information and authenticity of certificates. Certain digital certificates and general seal and sign certificates which are only authenticated by a URL can't be trusted for issuing sensitive certificates like Birth Certificates, transfer certificates etc. Stamped and signed certificates take time to verify the authenticity. Therefore, this proposed framework can circumvent the shortcomings of the current system; it is aimed to develop a full-fledged end-to-end block chain certificate management portal for managing certificates and credentials issued by organizations. To develop this system the two technologies which are used are distributed ledger technology and image steganography.

The legitimacy of the document holder and the issuing authority are both at risk due to the rise in forgeries. Blockchain technology has recently emerged as a crucial framework for preventing document fraud and abuse as well as a workable strategy for guaranteeing the verification of documents. The proposed framework aims to use blockchain technology to improve the document verification process. By including new security themes necessary for document verification in the blockchain technique, we have created an end-to-end system in our study effort. This study also identifies the weaknesses and inadequacies in the present blockchain-based systems for verifying educational certificates. A blockchain-based architecture for authenticating educational credentials ultimately emphasizes concepts like authorization, confidentiality, the proposition of ownership, and privacy.

The issue of system trust can be resolved and data security can be ensured through the use of distributed ledger technology. Therefore, this approach will be dependable, secure, and trustworthy for creating a certificate registry for the management of certificates. The document verification process may be made better with the help of blockchain technology, which also helps prevent document fraud and abuse. Blockchain technology can be described as a distributed database that chronologically stores a chain of data in sealed blocks. Every block includes data, a cryptographic hash of the one before it, and other crucial information.

To add another layer of security, instead of distributing certificates to the end user in pdf format where the authentication hash would be specified directly and hence would compromise the hashing and authentication mechanism, the end certificate would be a digital image with embedded ledger hash and other key authentication information. This can be done by employing image steganography, which is a technique for embedding sensitive data by incorporating it inside an audio, image, video or text file. This is one of the techniques used to defend sensitive or secret data against nefarious attacks. In order to improve the execution, speed the concept of parallel programming is combined with image steganography.

In this section, an overview of the application that is being developed using the concept of image steganography using block- chain technology is presented. The entire certificate management application can be divided into the following components and these components are semi-autonomous in the system, which could be divided into end user, block chain node server & the certificatesecurity issues with the authentication generations. The high-level system design is shown in the Fig. 1, which consists of primary or secondary storage info's & the certificate management system info's. Existing systems to manage certificates in any organizations such as schools, colleges and various government institutions to generate and store the certificates are not reliable and are not secure.

There are several limitations in the existing system regarding the security of information and authenticity of certificates. Certain digital certificates and general seal and sign certificates which are only authenticated by a URL can't be trusted for issuing sensitive certificates like Birth Certificates, transfer certificates etc. Stamped and signed certificates take time to verify the authenticity. Consequently, to get around the drawbacks of the current system, it is aimed to develop a full-fledged end-to-end block chain certificate management portal for managing certificates and credentials issued by organizations. To develop this system the two technologies which are used are distributed ledger technology and image steganography technology can be used to combat document fraud, abuse and improve the document verification process. A distributed database that keeps a chain of data in sealed blocks that are organized chronologically is called blockchain technology . Each block includes data, a cryptographic hash of the previous block, and other crucial details.

The issue of system trust can be resolved by using distributed ledger technology to ensure data security. Therefore, this approach will be dependable, secure, and trustworthy for creating a certificate registry for the management of certificates. The Fig. 1 gives the high level system design which gives a brief idea of how the system is developed.

- End User application: This module will be developed using ASP.net web framework
- Blockchain Node Server: This module will be developed using .Net Network library using the concepts of C# window form theframework.
- Certificate: The user's certificate will be a digital image, with embedded information; the same image can be used to verify theauthenticity.

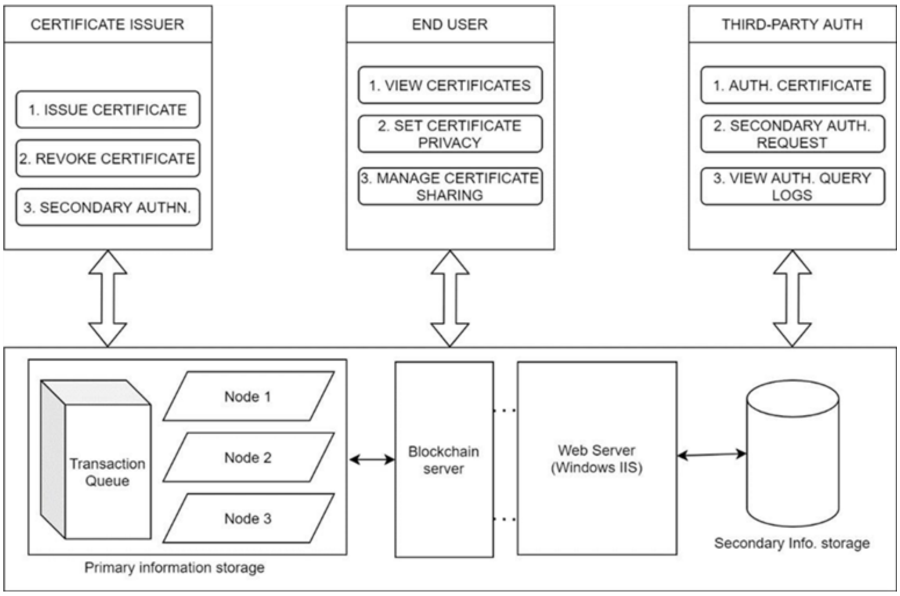


Fig. 1: High level system design

II. RELATED WORKS / LITERATURE SURVEY

A large number of researchers have worked on the topic of "Development of novel blockchain technology for certificate management system using cognitive image steganography techniques". There were a number of drawbacks & advantages in the works done by them. In this chapter, their advantages and disadvantages are discussed in a brief overview of the work done by different authors. A number of research papers were gathered from different sources, analyzed @ length & breadth with regard to the work taken up in this exciting & application-oriented area in the image steganographic field related to the security, authenticity& encryption & enhancement process with the different types of images. Here, follows a brief review of the works done by variousresearchers in the form of an exhaustive review of literature in this literature survey section. There doesn't exist any complete end- to-end block chain certificate management portal for managing certificates and credentials issued by educational organizations. From analysis of various software applications and papers on blockchain in the area of education and certificate Issual, the following ideas and implementations will be utilized in our system to develop a complete end to end and safe certificate management system.

Theoretical Aspects of Computing were taken into account when creating a High-Performance Educational Certificate Blockchain with Efficient Query [1]. Additionally, a team of academics presented a blockchain-based higher education credit network in an IEEE Access publication in [2], where the credit platform issues were discussed in greater detail there. A cutting-edge blockchain-based method for verifying educational records. Association for computing machinery was depicted in [3], scientists and engineers where the work portrayed majority of the issues that were being dealt with in the educational sector. In [4], a hybrid technique to secure e-commerce transaction with the help of AES encryption and stenography in images was discussed with new results and comparisons done w.r.t. the work done by others and showing that their method gave good results in the field of e- commerce applications. Speed up improvement using parallel approach in image steganography was discussed in [5], where a highspeed computing algorithms in the fields of black/white & color image steganographic issues were discussed in greater detail. Management, Governance and Value Creation in a Blockchain Consortium was deployed in one of the excellent references in [6]

A decentralized blockchain with high throughput and fast confirmation was discussed in [7]. A peer-to-peer electronic cash system

w.r.t. the bitcoin environment in the form of a white paper was presented in [8]. In [9] an inclusive block chain protocols was portrayed by a block chain based research group. Blockchain – a blueprint for a new economy was discussed in [10] which could be used for a host of e-commerce applications in the educational sector. A blueprint for a new economy was discussed in [11]. An overview of blockchain technology: architecture, consensus, and future trends were discussed in [12]. Blockchain as a Service (BaaS) for the company providers and trust was put form by a research group in [13] where they discussed more on the issues related to the security concepts in big companies & MNCs. Blockchain in IoT w.r.t. the current trends, challenges, and future roadmap was given in [14], where the current technologies that could be used in all types of digital scenarios was discussed. A systematic review w.r.t.the blockchain technology for the Internet of Things was discussed in [15] which provided as a ready reckoner paper for many of the researchers who wanted to pursue research in the field of image steganography. A secure sharing protocol for open blockchainsin security based certificate management system was provided by the blockchain engineers in [16].

In one of the excellent works mentioned in [17] towards blockchain-based auditable storage and sharing of IoT data was given, thisdata could be used for a number of security certificate management issues in the educational & company sectors. The IoT electric business model concepts using blockchain technology for the Internet of Things was discussed in [18] for the business applications. A high-performance educational certificate blockchain with efficient query was enunciated with some model based approaches in [19], the model being used for all general purpose activities in certificate management systems such as inserting security features inthe certificates like holograms, sim messages, etc., in [20] a blockchain-based higher education credit platform was introduced for the educational systems right from school level to the college level programs. A novel blockchain-based education records verification solution in the educational sectors was discussed in [21]. The management, governance and value creation in a blockchain consortium was discussed in [22]. In [23], a decentralized blockchain with high throughput and quick confirmation was described. The prism then took the form of disassembling the blockchain to get close to physical boundaries in [24]. Further, speed-security based trade-offs in blockchain protocols were discussed in [25].

III. PROPOSED METHODOLOGY DEVELOPED

There are five key requirements that educational certificates on a blockchain must meet, and they are authenticity, authorization, confidentiality, ownership, and privacy. These requirements are broken down one by one in the following list.

Authentication: Users must be verified through the blockchain. Students, colleges, institutes, employers, etc. are examples of users in this situation. In order to access the certificate that is recorded on a blockchain ledger, each user must be authenticated. Users can be authenticated using their username and password, although some systems may also support additional authentication methods like biometrics. For instance, the recipient will consent to the employer viewing and confirming the certificate after the recipient first joins the blockchain.

Authorization: provides people the permissions they need to conduct transactions on the blockchain. For instance, the student has the right to give his or her certificate to a potential employer. Once the certificate has been granted, the issuer will give the student complete control over it. Each of these operations must have system authorization.

Confidentiality: Private information about the student that can be kept private by the academic institution and the student is included in the confidentiality criteria. Here, the student is responsible and may disclose information to employers or other third parties as necessary for verification.

Ownership: The users of the blockchain ledger own ownership of a digital certificate. When it comes to educational certificates, the holder is the exclusive proprietor of the document. The functions of public and private keys are crucial in this situation and are accessible to all users who own a blockchain.

Privacy: Anonymity is ensured for public keys. Along with using cryptographic algorithms, hash functions must be created. The aforementioned themes are crucial to ensuring that the certificate is authentic. The credentials stated by the student on the blockchain can be verified by employers.

In this proposed system any organization can issue trusted digital certificates. As per the system, the certificates information is managed in a secured blockchain network such that once the certificate is generated and stored; its details cannot be modified. This will prevent forging of information on certificates. Also the organization can customize the certificate’s fields based on the purposeand requirement. After the certificate is issued by the organization the certificate will have all the critical information embedded init. The information is embedded using digital image steganography.

The primary technology used in this system are (i) Distributed ledger technology and (ii) Digital image steganography, which are explained as follows.

A. Distributed Ledger Technology

A blockchain, also known as a distributed ledger, is a growing collection of information referred to as blocks that are connected by cryptography. Every block includes data, a cryptographic hash of the one before it, and other crucial information. In a peer-to-peer network of computers, numerous computers are used to create a blockchain, which is a record of facts. Nodes are the anonymous individuals that make up the network. Cryptography is used in all internal communications to securely identify the source and receiver. A consensus known as a block arises in the network when a node needs to add a fact to the ledger to specify where this fact should appear in the ledger. Blockchain is essentially just a chain of blocks at its most fundamental level, but not in the conventional sense. In this context, the terms "block" and "chain" refer to digital data that is termed a block and is kept in a public database called a chain.

B. Digital Image Steganography

Digital picture Steganography is a technique for obfuscating secret information by enclosing it in a regular, non-secret file or communication, typically an image, and extracting it once it reaches its intended recipient. Steganography can be used in addition to encryption to further conceal or safeguard data. Almost any sort of digital content, such as text, images, videos, or music, can be hidden via steganography; Before being included in the seemingly innocent cover text file or data stream, the content that needs to be hidden using steganography, or hidden text, is frequently encrypted. If the hidden text is not encrypted, it is frequently altered in some way to make it more challenging to figure out what it contains.

The complete system is divided into 2 modules namely certificate issuance module & certificate verification module.

- Certificate issuance module
- Certificate verification module

I. Certificate Issuance Module

This module manages the certificate generation and authorization process by the organization. The certificate to be issued by the organization, must a valid certificate template provided as the part of system, based on the purpose and requirement all necessary fields are to be considered for certificate generation. Once the certificate markup is ready, the organization can proceed with the internal authorization of certificate and later publish the certificate information to the public blockchain record.

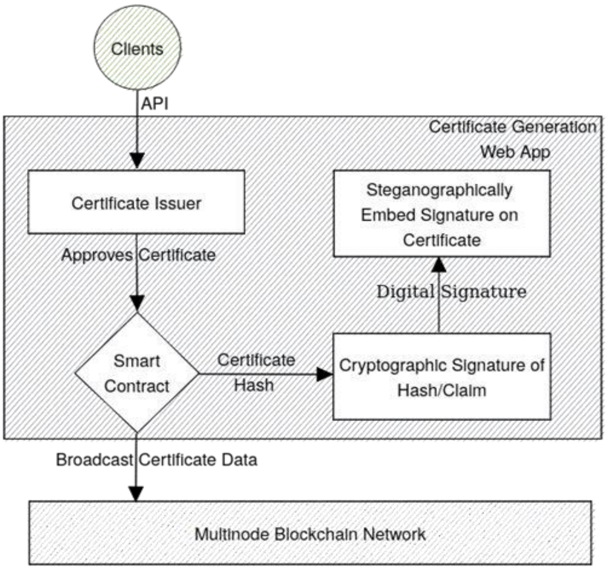
II. Certificate Verification Module

This module manages the verification of certificate authenticity from the public blockchain node. Any request of verification from a third party with valid certificate entity will be managed by the blockchain nodes. The verification process will be carried on a web portal viewing the certificate markup and other additional information like certificate query history of previous certificate viewer etc.

V. SYSTEM ARCHITECTURE

As proposed this system deals with complete end to end digital certificate management, hence it contains vast number of process and tasks related to certificate generation, verification and regular management. Various processes of this system as per proposed

architecture are divided into smaller manageable units called services. These services can be easily developed using various software architectural design patterns and are easy to maintain and deploy over any native cloud services. Fig. 2 gives the overview of the certificate issue & approval process followed by the certificate verification process in the Fig.


Clients
API
Certificate Generation Web App
Certificate Issuer
Approves Certificate
Steganographically Embed Signature on Certificate
Digital Signature
Smart Contract
Certificate Hash
Cryptographic Signature of Hash/Claim
Broadcast Certificate Data
Multinode Blockchain Network

3.

Fig. 2 : Certificate Issue & Approval

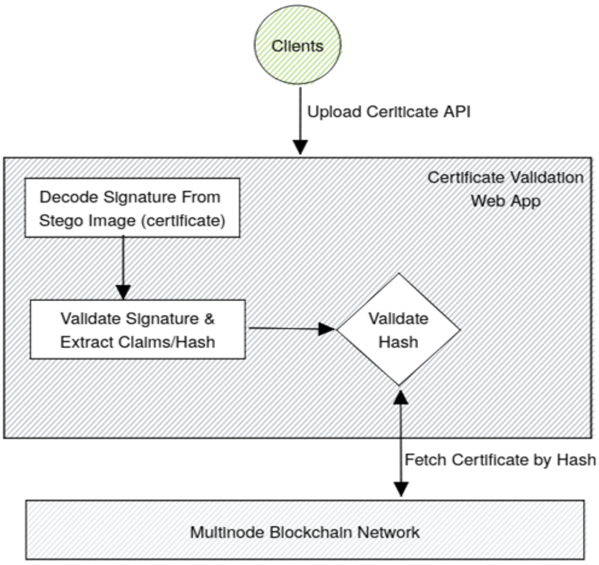

Clients
Upload Ceriticate API
Certificate Validation Web App
Decode Signature From Stego Image (certificate)
Validate Signature & Extract Claims/Hash
Validate Hash
Fetch Certificate by Hash
Multinode Blockchain Network

Fig. 3 : Certificate Verification

The architecture of the system is described as follows. The three major components of the systems are Cluster of nodes forming Blockchain, Certificate generation portal and Certificate authentication portal. All the certificate related data is stored in distributed hyper-ledger format across multiple nodes and this enables nodes sync and node verification. The certificate to be generated can be created using a web portal, which on approval by the concerned authority can be added to the blockchain network. The end certificatewhich will be provided to the user will be in form of a digital image, with encrypted certificate information embedded in it. Once the certificate is generated & approved which is in digital image form. Information about the certificated will be stored in nodes ofblockchain network which produces hash certificate value. Image steganographic algorithms were used to embed hash value inside the approved certificate with other information. The issuer private key is used to sign the certificate where it's embedded inside thecertificate.

The third-party can verify the authenticity of the certificate by using the authentication web portal. During verification phase user has to upload the authenticated image. Here the certificate information is extracted from the image and verified with at least two nodes in the blockchain network, with public key of certificate issuer for signature verification and appropriate status is provided. Once authentication process is completed authenticated certificate will be generated else an error is thrown & certificate will not begenerated. Three different types of certificates were generated degree, participation & appreciation certificate. Cognitive based image steganographic algorithm selection was used for all three types of certificates. The image steganographic algorithms used areLSB, XOR_LSB, PVD & DCT. For the proposed algorithms PSNR & MSE was calculated to select the best suitable algorithm for the selected certificate type. The system component design is shown in the Fig. 4.

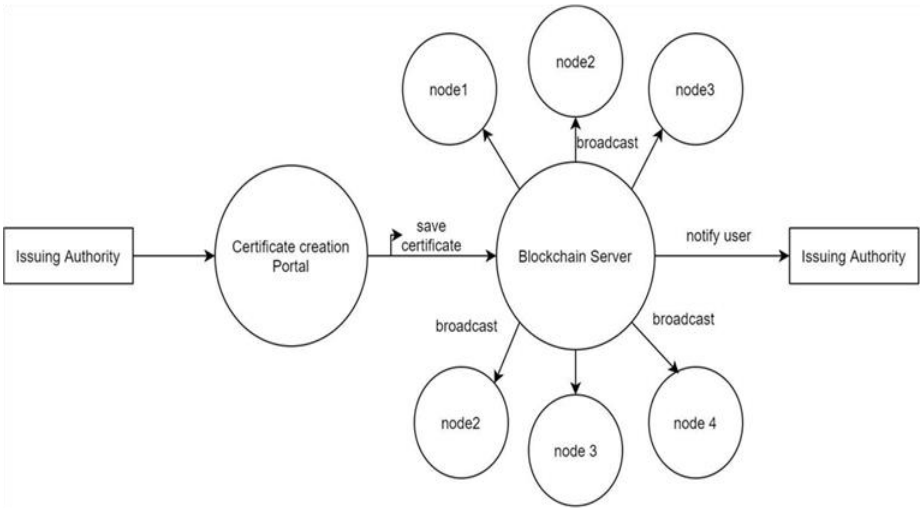


Fig. 4 : System component design using block-chain technology

VI. IMPLEMENTATION

A. Certificate entity

The end certificate which will be provided to the user will be in form of a digital image, with encrypted certificate information embedded in it. The issued certificate can be shared across digital means namely email, digital forms etc. corresponding to the embedded information, an entry in the distributed blockchain network will be made.

The blockchain block information is saved in the following format:

```
{

prev-hash: "77526b1386571………", certificate-hash: "6cd807709d9e1",timestamp: "202006101818197463",
content:

[

field1:

"description1", field2:
```

```
"description2",

]

blockhash: "c191d93b7e6cd"

}
```

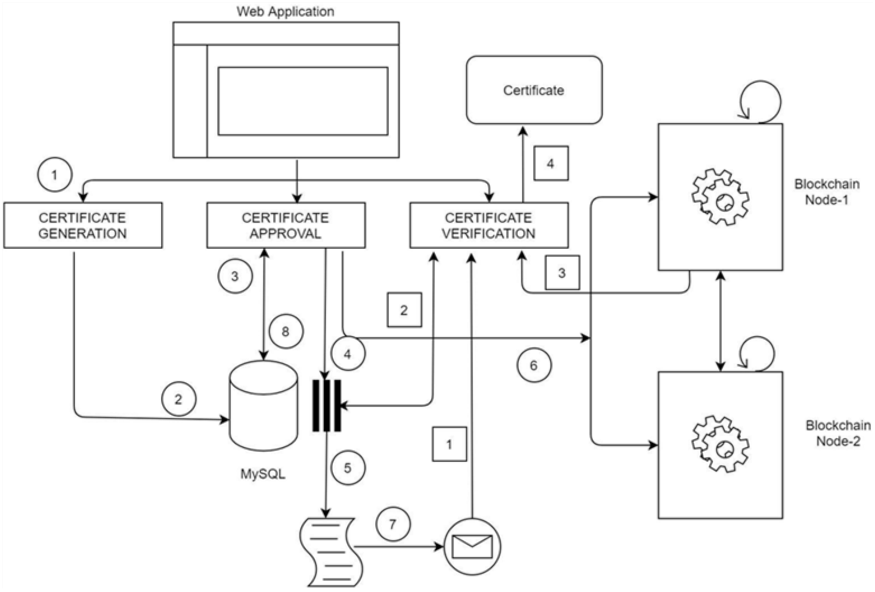


Fig. 5 : Implemented system overview

The hash values are calculated using SHA256 hashing algorithm.

The overview of the implementation procedure that is carried out in the proposed security insertion using the block-chain & stego design is shown in the Fig. 5, i.e., the system overview.

B. Verification mechanism

A digital identity reduces the bureaucracy level and increases the speed of processes within organizations by allowing for a greaterinteroperability between departments and other institutions.

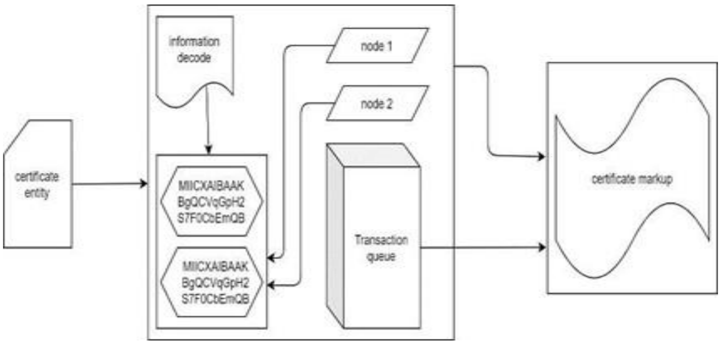


Fig 6 : Verification mechanism overview

This mechanism can be implemented using a web portal to create new authentication request, here the third-party user will upload the certificate entity of the pupil, two distinct set of nodes will be fetched for the certificate information once the hash value in the certificate matches with the information in the certificate, appropriate request response will be given. Verification mechanism overview is shown in the Fig. 6, which shows the developed protocol could be verified.

C. Image Steganography Techniques

The image steganography algorithms like LSB, XOR_LSB, PVD, and DCT are used to hide the certificate information & hash value of block chain node is implemented in sequential and parallel. The certificate information to be hidden is encrypted before being embedded in the image. Once the certificate is generated & approved from the concerned authority. At the backend certificate information will be stored in the block chain nodes & image steganographic algorithms are performed for the selected type of certificate then stego image which is certificate in digital image form will be generated for all the four algorithms. During Verification process authenticated user must select any one of the stego image. Then decoding will be done to extract the hash value & other certificate information for verification if it matches final certificate in digital form which is cover image will be generated, otherwise an error is thrown as invalid certificate.

VII. SIMULATION RESULTS

The developed algorithms are implemented using Python environment, the developed programs are run & the simulation results are observed and the security features shows the authenticity of the application developed. The testing is being carried out in BMS Institute of Technology because of the availability of high-end licensed software tools. The following are the results of the web application used by the user to generate and verify the certificate. This is the frontend which organization employees use to generate three types of certificates, approval of certificate and users use to verify the certificates. Once, the details of the certificate holder have entered. The certificate will be listed in dashboard with name of the certificate holder. Certificate has to be approved for further processing. The table 1 gives the comparison of PSNR & MSE values after the simulated results.

In the approval portal, list of certificates to be approved will be displayed. Then, the certificate has to be approved by the concerned authority. Details of the certificate will be stored in the block chain nodes in block chain application. The certificate after approval it has to be verified by third party for authentication. Verification portal has to be used for the verification. During the verification process third party should upload the authenticated image for verification as certificate generated which is in digital image form with certificate issuer signature, hash value of the block chain node & other certificate information will be embedded inside the digital image. After verification certificate will be displayed for all the four image steganography algorithms & PSNR, MSE will be generated to select the best suitable algorithm for three different types of certificates. Table 1 shows the value of PSNR & MSE values. In case, if invalid image has uploaded then an error will be thrown has no certificate will be generated.

Table 1: Comparison of PSNR & MSE values

Certificates /Algorithms	LSB	XOR- LSB	PVD	PVD
Degree	PSNR: 86.79 MSE:0.0001	50.65 0.559	48.5 0.916	49.2 0.76
Achievement	PSNR:88.95 MSE:8.263	50.58 0.568	48.5 0.916	49.25 0.772
Participation	PSNR:85.88 MSE:0.0001	50.47 0.583	48.43 0.931	49.25 0.772

VIII. CONCLUSIONS

Research was carried out how to incorporate some of the novel methods in improving the security features of embedding the data in image steganography using the block chain technology. In this survey work, we have proposed the development of a complete end-to-end certificate management system using blockchain and image steganography which would overcome the issues with the existing system such as unauthorized access to certificates, forging of documents and time-consuming verification process has been described. Blockchain technology has become a formidable tool for preventing document fraud and abuse as well as a potential way to authenticate the document verification process. The suggested method evaluates the shortcomings of the current blockchain-based solutions for documenting educational credentials and enhances document verification using blockchain technology. The proposed method for educational credential authentication focuses on challenges like authenticity, authorization, secrecy, transparency, and sovereignty. To standardize the certificate management process, all institutions must take the initiative.

REFERENCES

[1]. Yuqin Xu, Shangli Zhao, Lanju Kong, Yongqing Zheng, Shidong Zhang, Qingzhong Li, “A High-Performance Educational Certificate Blockchain with Efficient Query”, Springer International Publishing, Theoretical Aspects of Computing – ICTAC 2017, vol 10580, Springer.
[2]. M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, “EduCTX: A Blockchain-Based Higher Education Credit Platform”, IEEE Access, vol. 6, pp. 5112-5127, 2018.
[3]. Meng Han, Zhigang Li, Jing (Selena) He, Dalei Wu, Ying Xie, Asif Baba, “A Novel Blockchain-based Education Records Verification Solution. Association for Computing Machinery, SIGITE '18: Proceedings of the 19th Annual SIG Conference on Information TechnologyEducation, 2018.
[4]. Ekta Chauhan and Unmukh Datta and Maharana Pratap, “A Hybrid Technique to Secure E commerce Transaction with the Help of AES Encryption and Stenography”, Image, International Journal of Hybrid Information Technology Vol.8, No.8 (2015)
[5]. Jyothi Upadhya K., U Dinesh Acharya and Hemalatha S., “Speed Up Improvement Using Parallel Approach in Image Steganography. The Second International Conference on Information Technology Convergence and Services, 2013.
[6]. Zavolokina, Liudmila; Ziolkowski, Rafael; Bauer, Ingrid; and Schwabe, Gerhard (2020) "Management, Governance, and Value Creation in a Blockchain Consortium," MIS Quarterly Executive: Vol. 19: Iss. 1, Article 3, Management, Governance and Value Creation in a Blockchain Consortium. MIS Quarterly Executive. 2020.
[7]. Chenxing Li, Peilun Li, Dong Zhou, Zhe Yang, Ming Wu, Guang Yang, Wei Xu, Fan Long, Andrew Chi-Chih Yao, “A Decentralized Blockchain with High Throughput and Fast Confirmation”, Conflux Foundation 2020.
[8]. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system. bitcoin.org whitepaper”, Int. Conf., 2008.
[9]. Yoad Lewenberg, Yonatan Sompolinsky, and Aviv Zohar. Inclusive block chain protocols. In International Conference on Financial Cryptography and Data Security, pages 528-547. Springer, 201
[10]. Swan M., “Blockchain: Blueprint for a new economy”, O’Reilly Media Inc., 2015.
[11]. Yli-Huumo J., Ko D., Choi S., Park S., & Smolander K., “Where Is Current Research on Blockchain Technology?—A Systematic Review”, Public Library of Science, (PLOS) ONE, 11(10), e0163477, 2016.
[12]. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557-564, 2017.
[13]. J. Singh and J. D. Michels, “Blockchain as a Service (BaaS): Providers and Trust,” 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 67-74, London, UK, Apr. 2018.
[14]. Cui, Pinchen & Guin, Ujjwal & Skjellum, Anthony & Umphress, David., “Blockchain in IoT: Current Trends, Challenges, and Future Roadmap”, Journal of Hardware and Systems Security, Vol. 3., pp. 338-364, 2019.
[15]. Conoscenti, Marco & Vetro, Antonio & De Martin, Juan Carlos, “Blockchain for the Internet of Things: a Systematic Literature Review”, DoI 10.1109/AICCSA.2016.7945805, 2016.
[16]. Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. A secure sharding protocol for open blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, pages 17-30,
New York, NY, USA, 2016. ACM
[17]. Shafagh H., Burkhalter L., Hithnawi A., Duquennoy S., “Towards blockchain- based auditable storage and sharing of iot data”, Proceedingsof the 2017 on Cloud Computing Security Workshop, 2019.
[18]. Zhang Y., Wen J., “The IoT electric business model: using blockchain technology for the internet of things”, Peer-to-Peer Netw Appl, vol.
10, no. 4, pp. 983–994, 2017.
[19]. Xu Y., Zhao S., Kong L., Zheng Y., Zhang S., Li Q. (2017) ECBC: A High Performance Educational Certificate

Blockchain with Efficient Query. In: Hung D., Kapur D. (eds) Theoretical Aspects of Computing – ICTAC 2017. ICTAC 2017. Lecture Notes in Computer Science, vol. 10580. Springer, Cham.
[20]. M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform", IEEE Access, vol. 6, pp. 5112-5127, 2018.
[21]. Meng Han, Zhigang Li, Jing (Selena) He, Dalei Wu, Ying Xie, and Asif Baba, "A Novel Blockchain-based Education Records Verification Solution", Association for Computing Machinery, New York, NY, USA, 178–183, 2018.
[22]. Zavolokina, Liudmila & Ziolkowski, Rafael & Bauer, Ingrid & Schwabe, Gerhard, "Management, Governance and Value Creation in a Blockchain Consortium", MIS Quarterly Executive, 2020.
[23]. Chenxing Li, Peilun Li, and Dong Zhou, Zhe Yang, Ming Wu, and Guang Yang, "A Decentralized Blockchain with High Throughput and Fast Confirmation", Conflux Foundation, 2020.
[24]. Vivek Bagaria, Sreeram Kannan, David Tse, Giulia Fanti, and Pramod Viswanath. Prism: Deconstructing the blockchain to approach physical limits. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS '19, page 585-602,New York, NY, USA, 2019. Association for Computing Machinery.
[25]. Aggelos Kiayias and Giorgos Panagiotakos. Speed-security tradeoffs in blockchain protocols. IACR Cryptology ePrint Archive, 2015:1019,2015.