RESEARCH ARTICLE OPEN ACCESS

Documents Verification System and Blockchain Based Solutions

Mr. Aditya Shrikant Ingole[1], Mr. Vinayak R. Arjun[2], Mr. Nitin S. Patil[3],

Mr. Sumeet S. Shinde[4], Prof. Manjiri Pathak[5]

[1-4]Students of Computer Engineering Department, VPPCOE Mumbai, Maharashtra, India
[5] Professor of Computer Engineering Department, VPPCOE Mumbai, Maharashtra, India

---

Abstract - The verification center, which is responsible for issuing a variety of important certificates, still uses manual processes and relies on paper documents from other government agencies. This causes many problems. The verification center rejects paper materials that are not local. due to its reduced credibility in the local area and as a result, cross-border services are unavailable. Since copies of paper items have been stored, it is also easy to leak confidential information. Because of its Pros, a blockchain-based solution is ideal to address the issues in this scenario (e.g. decentralization, immutability, transparency, auditability). This system was built on Hyperledger Fabric. In addition, we use smart contracts to replace manual activities, create multiple ledgers to offload different types of transactions, and encrypt private data as needed.

***Key Words*: Blockchain, Verification Centre, E-government, certificate, Security, Encryption, AES, SHA.**

1.INTRODUCTION

Residents of many nations rely on official certifications on a daily basis. On the other hand, lack of transparency, excessive bureaucracy and even instances of corruption are eroding citizens' trust in government. The verification center holds most of the certifications for establishing property, family ties, death, etc. The purpose of establishing a verification center is to standardize the certification process, minimize the number of certificate papers, and improve the validity and acceptability of the certification.

In order to create a specific certificate, the verification center needs documents signed by other government agencies. The current verification process is managed manually and we are trying to bring this manual management process to the digital platform where users can request different certificates from home without having to physically go to a verification center.

Blockchains are distributed ledgers that allow participants to interact with each other securely and irreversibly without the use of intermediaries, and the blockchain-based system has a high level of availability and transparency. Also, to protect sensitive personal information, a symmetric encryption function has been integrated to encrypt the user's personal information and prevent data misuse. On the other hand, we believe that the design provided can be used in a variety of government sectors.

2. Literature Review

Blockchain was created to create a trustworthy, decentralized cryptocurrency that could help people avoid financial risks. Blockchain technology is now a prominent and promising technology that is being used in areas other than Bitcoin, such as the Internet of Things (IoT).) E-Health, financial applications, crowdsourcing and eGovernment. Blockchain can be used to improve government services in efficiency and effectiveness (e.g. transparency, lower costs, accurate records) [5] It has a promising future in optimizing business processes through secure data exchange [06] Leveraging blockchain -Technology to provide a public verification service can also enable some activities with the public and private sectors, such as Residency approaches in Estonian [08]. Their technique, based on a three-tier electronic certificate architecture, builds and simulates this system, and the results show that it can significantly reduce the size of the electronic certificate data stream.[09] In [10] Structure of an electronic certificate catalog exchange system (ECCS) based on Hyper Fabric (v1.1) for all circumstances concerning the exchange of electronic certificates. Reference [17] shows a blockchain system that uses proof-of-concept (POC) consensus to facilitate visibility of data shared between many stakeholders, such as smart contracts to automate decision-making in cell towers and building modifications. Chenfu Xu et al. according to Pengbin Han et al. The authors in [18] design a prototype of a digital certificate of education using the authoritative framework Hyperledger Fabric (V1.4).

Blockchain technology is useful for e-government services in general. Researchers, on the other hand, usually focus on developing their solution using the blockchain infrastructure. When it comes to practicality, they rarely consider other governments. They want more throughput and lower latency, and the performance of a blockchain system is inextricably affected by the distances between governments and the different stages of development of cities. As a result, we offer a strategy that takes this issue into account and, in particular, achieves superior performance results.

3. Blockchain Technology

Blockchain technology was first introduced in 2008 for cryptocurrency transactions as it is a technology that tracks every record and stores data in a way that is difficult or impossible to alter or hack. Each block in the chain comprises a series of transactions, and each time a new transaction occurs on the blockchain, a record of it is added to each participant's shelf.

This means if one block in a chain is changed, it's obvious that the entire chain has been changed. If hackers wanted to take down a blockchain system, they would have to change every block on the chain across all distributed versions. Today, blockchain technology is used in various platforms such as marketing, healthcare, etc. for your safety and efficiency.

4. Related work

The management of the existing verification system has problems such as: data insecurity, lack of a verification center in your region, when the officer is unavailable, his work is delayed. The data collected by the officer to create the certificate is stored in their hub, which takes up a lot of space and requires the officer to manage all the files, often resulting in erroneous data. The proposed system uses blockchain technology with the IPFS server because blockchain technology is not suitable for storing large amounts of data. Each file uploaded to the network is assigned a unique cryptographic hash value on the ipfs server, allowing the ipfs network to detect duplicates and control the version history of each file.

We use Advanced Encryption Standard and Secure Hash Algorithm to encrypt data. The Advanced Encryption Standard is a symmetric block cipher that can encrypt and decrypt data. Encryption changes data into an incomprehensible form called ciphertext, while decryption converts it back to its original form called plaintext. Each file that the user submits is assigned a unique hash value that cannot be duplicated by other data. The verification system is processed using a variety of technologies; The first tool used to create the verification system was Eclipse IDE.

It offers a graphical user interface (GUI) that allows us to access the code editor, compiler, interpreter and debugger from a single place. The backend of the system is written in Java Enterprise Edition and Java 16. Database connectivity and peer-to-peer web access are among the systems and services supported by Java. Python 3.9 is used to write the

Document encryption techniques. Apache Tomcat serves as the server for the verification system. By using the TCP/IP protocol, the Apache server allows clients and servers to communicate over networks. The open source Java application server Tomcat is the most widely used. Before we publish it on the main server, we use Apache xampp server to test the website and client on machines.

Java servlets are used to enhance the capabilities of a server hosting a request and response application. The verification system also uses JSP/Java Beans forserver-side programming. A bean wraps numerous objects into a single object that can be accessed from multiple locations. The MVC approach is suggested because it follows the Model-View-Controller.

The database used is the mySql database, which is open source software and the fastest database. All received data is stored in a structured manner in the mySql database.

4.1 System Design

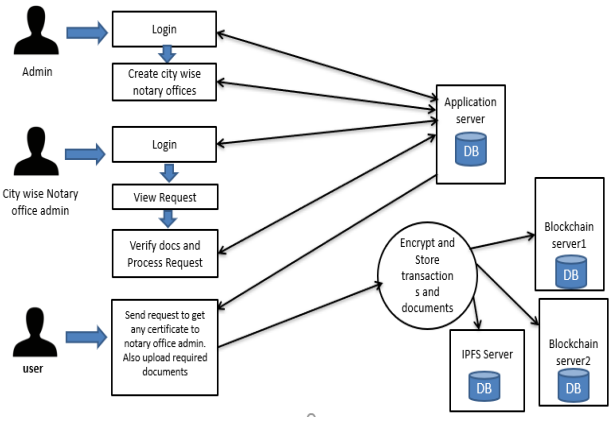


Fig-1: System design

We have developed four databases based on the concept of verification system. The first is the Apache Tomcat application server, which allows clients and servers to connect over networks using the TCP/IP protocol. The other two servers in the system are used for the structured storage of data in a MySQL database. Since blockchain technology is not enough to store large amounts of data, the last server will be an IPFS server that will store the encrypted file.

4.2 Working of System

The admin is the head of the organization, he has full access to the system and can see all the features of the system hidden from the wise city officials and users. The lead admin's job is to create verification centers for each city and make sure everything in the system is working properly. The admin has the ability to remove and create the profiles of the wise city officials and users who try to subvert the system by submitting fraudulent documents. Upon reaching, the user must register in the verification system. by providing all relevant information such as email address, mobile phone number and address.

After registering in the system, the user must log in to the system with their access data. After login, the application server validates the user's credentials. If the provided credentials are found on the server and match the user, access to the system is granted. User management options include registration, login, uploading documents, submitting a certificate request to a verification center if required, viewing the progress of your request, password recovery, and downloading the issued certificate. All these functions are available to the user through his panel.

The Verification Center panel includes viewing applications, verifying user-provided documents, assigning the certificate, and uploading forms. The verification center must provide a list of the certificates it can issue, such as B. Birth certificates and marriage certificates, as well as the form that the user must fill out. After the officer uploads the list, the user can view it and request the various certificates required. However, before the certificate is requested, the user must upload all required documents according to the verification instructions.

After submitting a certificate request, the user can check the progress of their request. The clerk can see how many people have applied for the certificate and then review all of the user's documents. If there are no issues with verification, the clerk creates the certificate and delivers it to the user's account. After that, the user has to authenticate himself via a one-time password before he can download the certificate the form of encrypted files on the server.

5. Encryption

Because of its widespread use and high efficiency, we chose the AES method to encrypt transactions to prevent leakage of confidential information. Although the difference parameter affects the efficiency of many algorithms, the AES method achieves the best results in a variety of usage scenarios, including time consumption, response time, request execution per second, and power consumption. The AES algorithm is suitable for processing a high volume of transactions and encrypting certificates. In addition, no additional components are required to implement this technique, which leads to a reduction in the complexity of our framework. Instead of storing encryption information on a device, users only have to remember a series of words or numbers.

After a user uploads a document, AES generates a 32-bit key to encrypt and store it on an IPFS server and distributed blockchain servers.

5.1 Algorithm's.

Algorithm 1 Documents/ Content Encryption

```
import os
from Crypto.Cipher import AES
from Crypto.Hash import SHA256
from Crypto import Random

def encrypt(key, filename):
    chunksize = 64 * 1024
    UPLOAD_DIR=os.getcwd()+"\\Documents\\"

    outputFile = "enc_" + filename
    filename=UPLOAD_DIR+filename
    outputFile=UPLOAD_DIR+outputFile
    filesize = str(os.path.getsize(filename)).zfill(16)
    IV = Random.new().read(16)

    encryptor = AES.new(key, AES.MODE_CBC, IV)

    with open(filename, 'rb') as infile:
        with open(outputFile, 'wb') as outfile:
            outfile.write(filesize.encode('utf-8'))
            outfile.write(IV)

            while True:
                chunk = infile.read(chunksize)

                if len(chunk) == 0:
                    break
                elif len(chunk) % 16 != 0:
                    chunk += b' ' * (16 - (len(chunk) % 16))
                outfile.write(encryptor.encrypt(chunk))

def decrypt(key, filename,dpath1):
    chunksize = 64 * 1024
    outputFile = filename[11:]
    outputFile=dpath1
    with open(filename, 'rb') as infile:
        filesize = int(infile.read(16))
        IV = infile.read(16)

        decryptor = AES.new(key, AES.MODE_CBC, IV)
            with open(outputFile, 'wb') as outfile:
            while True:
                chunk = infile.read(chunksize)
            if len(chunk) == 0:
                    break
    outfile.write(decryptor.decrypt(chunk))
            outfile.truncate(filesize)
def getKey(password):
    hasher = SHA256.new(password.encode('utf-8'))
    return hasher.digest()
```

Algorithm 2 Hashing algorithm

```
def getKey(inputText):
    hasher = SHA256.new(password.encode('utf-8'))
return hasher.digest()
```

For SHA(Secure hashing Algorithm) we have imported following package from Crypto.Hash import SHA256.

6. CONCLUSIONS

In this verification project, an e-certificate exchange system based on the consortium blockchain will be developed to solve the problems of government services, especially in terms of verifiability, efficiency and privacy. A prototype implementation is used to evaluate performance. In this paper, we examine the requirements of the Verification Center that issues certificates to residents and find that a blockchain-based solution can handle most of the problems encountered in these offices. In addition, we have improved the network performance of blockchain. Changing the structure commonly used.

All transactions are now classified as local transactions, which are then offloaded to separate ledgers. Experiments show that this strategy works well. It can also be assumed that the actual performance will be higher due to the distance and the degree of expansion of the cities to be taken into account. Finally, we offer security assessments on a variety of topics. It can help improve transaction efficiency and reduce transaction storage space, for example, entries in the local ledger do not need to be maintained and can be used in our case to create certificates as materials.

In our case, we had to create the certifications as materials. However, we need to examine the consistency of information across different blockchains, but for government action, each entity has a high level of trust. In some cases, this means you can use local ledger entries for a single city as additional information for the global ledger.

7. REFERENCES

[1] T.-T. Kuo, H. Zavaleta Rojas, and L. Ohno-Machado, ''Comparison of blockchain platforms: A systematic review and healthcare examples,'' J. Amer. Med. Inform. Assoc., vol. 26, no. 5, pp. 462–478, May 2019, doi: 10.1093/jamia/ocy185.

[2] Y. K. Tomov, ''Bitcoin: Evolution of blockchain technology,'' in Proc. IEEE XXVIII Int. Sci. Conf. Electron. (ET), Sep. 2019, pp. 1–4.

[3] A. Shahnaz, U. Qamar, and A. Khalid, ''Using blockchain for electronic health records,'' IEEE Access, vol. 7, pp. 147782–147795, 2019

[4] S. Ølnes and A. Jansen, ''Blockchain technology as s support infrastructure in e-government,'' in Electronic Government, M. Janssen, K. Axelsson, O. Glassey, B. Klievink, R. Krimmer, I. Lindgren, P. Parycek, H. J. Scholl, and D. Trutnev, Eds. Cham, Switzerland: Springer, 2017, pp. 215–227.

[5] D. Yermack, ''Corporate governance and blockchains,'' Rev. Finance, vol. 21, no. 1, pp. 7–31, Mar. 2017.

[6] A. Kaur, A. Nayyar, and P. Singh, ''Blockchain: A path to the future,'' Cryptocurrencies Blockchain Technol. Appl., pp. 25–42, May 2020, doi: 10.1002/9781119621201.ch2.

[7] N. Diallo, W. Shi, L. Xu, Z. Gao, L. Chen, Y. Lu, N. Shah, L. Carranco, T.-C. Le, A. B. Surez, and G. Turner, ''EGov-DAO: A better government using blockchain based decentralized autonomous organization,'' in Proc. Int. Conf. eDemocracy eGovernment (ICEDEG), Apr. 2018, pp. 166–171

[8] C. Sullivan and E. Burger, ''E-residency and blockchain,'' Comput. Law Secur. Rev., vol. 33, no. 4, pp. 470–481, Aug. 2017.

[9] P. Han, A. Sui, T. Jiang, and C. Gu, ''Copyright certificate storage and trading system based on blockchain,'' in Proc. IEEE Int. Conf. Adv. Electr. Eng. Comput. Appl. (AEECA), Aug. 2020, pp. 611–615

[10] C. Xu, H. Yang, Q. Yu, and Z. Li, ''Trusted and flexible electronic certificate catalog sharing system based on consortium blockchain,'' in Proc. IEEE 5th Int. Conf. Comput. Commun. (ICCC), Dec. 2019, pp. 1237–1242.

[11] H. Cheng, J. Lu, Z. Xiang, and B. Song, ''A permissioned blockchainbased platform for education certificate verification,'' in Blockchain and Trustworthy Systems, Z. Zheng, H.-N. Dai, X. Fu, and B. Chen, Eds. Singapore: Springer, 2020, pp. 456–471

[12] V. Buterin. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. [online] Available: https:// cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf

[13] A Blockchain Platform for the Enterprise. Accessed: Dec. 1, 2020. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release2.1/

[14] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, ''Comprehensive study of symmetric key and asymmetric key encryption algorithms,'' in Proc. Int. Conf. Eng. Technol. (ICET), Aug. 2017, pp. 1–7.

[15] S. Ølnes, J. Ubacht, and M. Janssen, ''Blockchain in government: Benefits and implications of distributed ledger technology for information sharing,'' Government Inf. Quart., vol. 34, no. 3, pp. 355–364, 2017.

[16] F. Casino, T. K. Dasaklis, and C. Patsakis, ''A systematic literature review of blockchain-based applications: Current status, classification and open issues,'' Telematics Informat., vol. 36, pp. 55–81, Mar. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0736585318306324

[17] H. Treiblmaier and C. Sillaber, A Case Study of Blockchain-Induced Digital Transformation in the Public Sector. Cham, Switzerland: Springer, 2020, pp. 227–244, doi: 10.1007/978-3-030-44337-5_11.

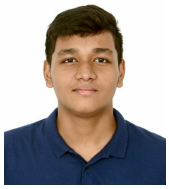
[18] H. Cheng, J. Lu, Z. Xiang, and B. Song, ''A permissioned blockchainbased platform for education certificate verification,'' in Blockchain and Trustworthy Systems, Z. Zheng, H.-N. Dai, X. Fu, and B. Chen, Eds. Singapore: Springer, 2020, pp. 456–471.

8. BIOGRAPHIES

Mr. Aditya Shrikant Ingole.
Pursuing Bachelor of Engineering.
(Computer Science).

Mr. Vinayak Rajaram Arjun.
Pursuing Bachelor of Engineering.
(Computer Science).

Mr. Nitin Shivaji Patil.
Pursuing Bachelor of Engineering.
(Computer Science).



Mr. Sumeet Suhas Shinde.
Pursuing Bachelor of Engineering.
(Computer Science).

Prof. Manjiri Pathak
Computer Engineering Department,
Vasantdada Patil Pratishthan's
College of Engineering & Visual
Arts, Mumbai, Maharashtra, India

