International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

Online Block Chain Based System for Notarial Office

Mr. Aditya Y. Vyas[1], Mr. Vidul A. Dabir[2], Mr. Ritwik M. Dhande[3], Mr. Pranav P. Madeshwar[4]

Prof. Rais Abdul Hamid Khan[5]

[1-4]Student of Computer Science & Engineering Department, GHRU Amravati, Maharashtra, India
[5]Professor, Computer Science & Engineering Department, GHRU Amravati, Maharashtra, India

---

Abstract - *The Notary office, 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 a slew of problems. Non-local paper materials are rejected by the Notarial Office due to their reduced credibility in the local area, and as a result, cross-border services are unavailable. Because copies of paper items have been stored, it is also easy to leak sensitive information. Because of its benefits, a blockchain-based solution is ideal to address the issues in this scenario (e.g, decentralized, immutability, transparency, auditability).*

This system was built on top of the Hyperledger Fabric. Furthermore, we use smart contracts to substitute manual activities, create multiple ledgers to offload different types of transactions, and encrypt private data as necessary. At the end of the day.

Key Words: **Blockchain, Notary Office, E-government, certificate, Security, Encryption, AES, SHA.**

1.INTRODUCTION

Residents in numerous nations rely on government certifications on a daily basis. On the other side, citizens' faith in government is eroded due to a lack of transparency, excessive bureaucracy, and even instances of corruption. The Notary Office has most official certifications to establish estate ownership, familial links, death, and so on. The purpose of creating a Notary Office is to standardize the certification process, minimize the number of certificate papers, and improve certification validity and acceptance. To produce a specific certificate, the Notary Office requires documents signed by other government offices. The current notary process is under the manual handling and we are trying to bring that manual handling process on to the digital platform where people can apply for different certificates from their home and no need to visit physically in any Notary office.

Blockchains are distributed record that allows participants to interact with one another in a safe, irreversible manner without the use of middlemen and blockchain-based system has a high level of availability and transparency. In addition, to secure personal sensitive information, a symmetric encryption function has been included to encrypt user personal data and prevent from data misuse, On the other hand, we feel that the design provided can be used to a wide range of government sectors.

2. Literature Review

The blockchain was created in order to build a decentralized and trustworthy cryptocurrency that may help people avoid financial risk. Blockchain technology is now a prominent and promising technology that is being used in areas other than bitcoin, such as Internet of Things (IoT) Electronic health, financial applications, crowdsourcing, and e-government. Blockchain can be utilized to improve government service in efficiency and effectiveness (e.g., transparency, lower costs, accurate record-keeping) [5] It has a promising future in optimizing the business processes through secure sharing of data [06] Using blockchain technology to offer a public notary service can also enables some activities with the public and private sectors such as residency approaches in Estonian [08]. Their technique, which is based on a three-level electronic certificate architecture, constructs and simulates this system, and the findings demonstrate that it can greatly reduce the size of electronic certificate data flow.[09] In [10] build an electronic certificates catalog sharing system(ECCS) based on the Hyper Fabric(v1.1) for all circumstances involving the exchange of electronic certificates Reference [17] displays a Blockchain system that uses proof-of-concept (POC) consensus to ease the visibility of shared data among many stakeholders, as well as smart contracts to automate decision-making in cell tower and building modifications. Chenfu Xu et al.. According to Pengbin Han et al. Authors in [18] design a digital education certificate prototype utilizing the permissioned framework Hyperledger Fabric (V1.4).

Blockchain technology is useful for electronic government services in general. Researchers, on the other hand, generally concentrate on developing their solution using the blockchain infrastructure. When discussing the practicality, they seldom take other governments into account. People do, after all, want more throughput and lower latency, and the performance of a blockchain system is inextricably influenced by the distances between governments and the varied levels of development of cities. As a result, we offer a strategy that takes this issue into account and achieves superior performance in particular

3. Blockchain Technology

Blockchain technology was firstly introduced in 2008 for cryptocurrency transactions because it is a technology that keeps the track of every record and store data in such a way that altering, hacking is difficult or impossible. Each block on the chain comprises a number of transactions, and whenever a new transaction takes place on the blockchain, a record of it is added to each participant's ledge.

It means that if one block in a chain is changed, it will be obvious that the entire chain has been tampered with. If hackers wanted to take down a blockchain system, they'd have to change every block in the chain across all distributed versions. Now days blockchain technology is getting used on different platforms like marketing, healthcare etc. because of it's security and efficiency.

4. Related work

The existing notary system management system has issues such as:

Data insecurity, absence of a notary officer in your region, if the officer is inaccessible, your job will be delayed. The data acquired by the officer to generate the certificate is maintained in his office, which takes up a lot of space and demands the officer manages all of the files, which often leads to erroneous data.

In proposed system, blockchain technology is used with IPFS server because blockchain technology is not suitable for storing large amounts of data. Each file uploaded to the network is given a unique cryptographic hash value on the ipfs server, which allows the ipfs network to detect duplication and monitor version history for each file.

We are using the Advanced Encryption Standard and Secure Hashing Algorithm to encrypt the data. The Advance Encryption Standard is a symmetric block cypher that can encrypt and decrypt data. Encryption changes data to a unintelligible form called ciphertext, while decryption converts it back to its original form called plaintext. Every file that the user submits will be assigned a unique hash value that cannot be duplicated by any other piece of data.

The notary system is processed using a variety of technologies; the first tool used to build the notary system was Eclipse IDE. It provides a graphical user interface (GUI) that allows us to access the code editor, compiler, interpreter, and debugger from a single location. The backend of the system is written on 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 notary system. 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 extensively used. Before publishing it to the main server, we utilize the xampp apache server to test the website and client on computers. Java servlets are used to enhance the capabilities of a server that hosts a request-response application. Notary system also utilizing JSP/Java Beans for server-side programming. A bean wraps numerous objects into a single object that may be accessed from multiple locations. The MVC approach is proposed because is follows the model-view-controller. The database in use is the mySql database, which is open source software and the quickest database. All of the data received is saved in a structured way using the mySql database.

4.1 System Design

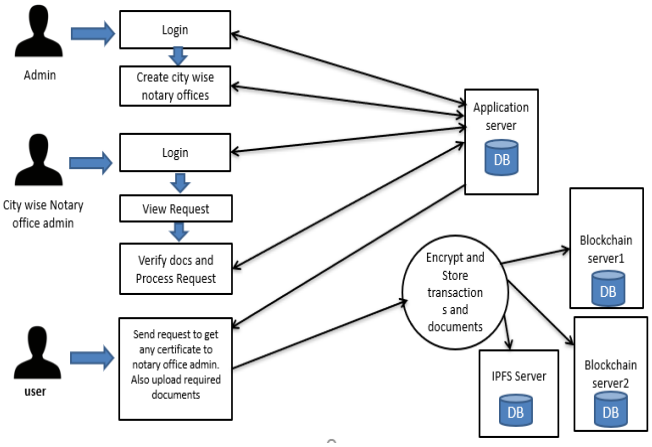

Fig-1: System design

We developed four databases based on the notary system concept. The first is the application server, which is Apache Tomcat, which allows clients and servers to connect over networks via the TCP/IP protocol. The other two servers in the system are used to store data in a structured way in a MySQL database. Because of blockchain technology is insufficient for storing vast amounts of data; the final server will be an IPFS server that will store the encrypted file.

4.2 Working of System.

The admin is the organization's leader he has full access to the system and can view all of the system's features that are hidden from the city's wise officers and users. The senior admin's job is to create notary officers for each city and ensure that everything in the system is running properly. The administrator has the ability to remove and create the profiles of city wise officials and users who are attempting to undermine the system by submitting fraudulent documents. Coming to user side working the user must register with the notary system by providing all of the relevant information, such as an email address, a cell phone number, and an address. After registering on the system, the user must log in to the system with his log in credentials. After logging in, the application server will verify for the user's credentials. If the specified credentials are found on the server and match with the users, then user will be granted access to the system.

User management options involve registration, log in, upload documents, send a certificate request to a notary

officer if necessary, see the progress of your application, password recovery, and downloading the issued certificate. All of these functions are available to the user through his panel. The notary officer's panel contains view requests, verify the documents provided by the user, assign the certificate, and upload forms. The notary officer must provide a list of certificates that he may issue, such as birth certificates and marriage certificates, as well as the form that the user must fill out. After the list has been uploaded by the officer, the user may view it and apply for the various certificates that are required. However, before applying for the certificate, the user must upload all of his required documents as instructed by the notary. After submitting an application for a certificate, the user can check the progress of his application. The officer can see how many individuals have applied for the certificate and then verify all of the user's documents. If there are no concerns with the verification, the officer will generate the certificate and transmit it to the user's account. After that, the user must authenticate his identity via One Time Password before he can download the certificate. All document exchanges are done in encrypted manner additionally; data is saved in the form of encrypted files on the server.

5. Encryption

Because of its extensive use and great efficiency, we chose the AES method to encrypt transactions to avoid the leakage of sensitive information. Although the difference parameter affects the efficiency of many algorithms, the AES method achieves the best results in a variety of use situations, including time consumption, response time, request execution per second, and battery power consumption.

The AES algorithm is well-suited to handling a high volume of transactions while also encrypting certificates. Furthermore, no extra components are required to implement this technique, resulting in a reduction in the complexity of our framework. Instead of storing encryption information on a device, users simply need to recall a set of words or numbers. After a user uploads a document, AES generates a 32-bit key to encrypt it and store it on an IPFS server as well as distributed blockchain servers.

5.1 Algorithm's.

Algorithm 1 material 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

An electronic certificate sharing system based on consortium blockchain is being developed in this notary project to meet the issues of government services, particularly in terms of auditability, efficiency, and privacy. A prototype implementation is used to assess performance. In this paper, we examine the needs of the Notarial Office, which issues certificates to residents, and find that a blockchain-based solution can handle the majority of issues that arise in these offices. In addition, we have improved the performance of the blockchain network by changing the commonly utilized structure. All transactions are now classified as local transactions, which are then off-loaded to separate ledgers. The experiments show that this strategy performs well. We may also assume that the real performance will be higher since the distance metric and the degree of development of cities must be considered. Finally, we offer security assessments on a variety of topics.

It can assist in improving transaction efficiency and reducing transaction storage space, for example, entries on the local ledger do not need to be maintained and can be used to create certificates as materials in our case. In our circumstance, we needed to produce the certifications as materials.

However, we must examine the consistency of information across multiple blockchains, but for government actions, each entity has a high level of confidence. In some cases, this implies we may utilize entries from a local ledger belonging to a single city as extra 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.

BIOGRAPHIES

Mr. Aditya Yashvant Vyas.
Pursuing Bachelor of Technology.
(Computer Science & Engineering).

Mr. Vidul Abhiram Dabir.
Pursuing Bachelor of Technology.
(Computer Science & Engineering).

Mr. Ritwik Milind Dhande.
Pursuing Bachelor of Technology.
(Computer Science & Engineering).

Mr. Pranav Purshottam Madeshwar.
Pursuing Bachelor of Technology.
(Computer Science & Engineering).

Prof. Rais Abdul Hamid Khan.
Computer Science & Engineering Department,
G.H. Raisoni University, Amravati, Maharashtra, India