A Blockchain based Authentication System For Digital Documents With Face Recognition

Swamynathan.M[1], Sundhar.U[2], Ambiga.R[3]
[1, 2] Dept of Computer Science and Eng.,
[2, 3]Assistant Professor, Dept. of Computer Science and Eng
[1, 2, 3] Thiruvalluvar College of Eng. & Tech., Vandavasi

Abstract- *The rapid development in the sector of information technology and easy access to cheap and advanced office instruments in the market, the faking of important documents has become a matter of concern nowadays. Therefore, the need for verification and authentication practices of various important documents in the form of banking documents, government documents, transaction documents, educational certificates etc., however, various challenging and tedious processes have made document verification very complex. We present a decentralized web application for digital document verification using Ethereum block chain-based technology in P2P cloud storage to enhance the verification process by making it more open, transparent, and auditable.*

Keywords- Block Chain, Face Recognition, ID Matching

I. INTRODUCTION

Identity verification plays an important role in our everyday lives. For example, access control, physical security and international border crossing needs us to verify our access (security) level and our identities. A common approach to this problem involves comparing an individual's live face to the face image found in his/her Identification document. For example, immigration and customs officials look at the passport photo to authorize a traveler's identity. Clerks at supermarkets in the United States look at the customer's face and driver license to check his/her age when the customer is purchasing alcohol. Instances of ID document photo matching can be found in numerous circumstances. On the other hand, it is primarily conducted by humans by hand, which is time consuming, costly, and prone to operator errors. A study in Sydney, Australia, shows that even the trained officers perform below par in matching unexperienced faces to passport photos, with a 14% false acceptance rate.

Therefore, an accurate and automated system for efficient matching of ID document photos to selfies is required. In addition, automated ID-selfie matching systems also enable remote authentication applications that are otherwise not feasible, such as onboarding new customers in a mobile app (by verifying their identities for account creation), or account recovery in the case of forgotten passwords. One application scenario of our ID-selfie matching system is illustrated.

II. HISTORY

A number of automated ID-selfie matching systems have been deployed at international border crossings. Deployed in 2007, SmartGate in Australia is the earliest of its kind. Due to an increasing number of travellers to Australia, the Australian government introduced SmartGate at most of its international airports as an electronic passport check for ePassport holders. To use the SmartGate, travelers only need to let a machine read their ePassport chips containing their digital photos and then capture their face images using a camera mounted at the SmartGate. After verifying a traveller's identity by face comparison, the gate is automatically opened for the traveller to enter Australia. Similar machines have also been installed in the U.K. (ePassport gates), USA (U.S. Automated Passport Control) and other countries.

In China, such verification systems have been deployed at various locations, including train stations, for matching Chinese ID cards with live faces. In addition to international border control, some businesses are utilizing face recognition solutions to ID document verification for online services. The problem of ID-selfie matching poses numerous challenges that are different from general face recognition. For typical unconstrained face recognition tasks, the main challenges are due to pose, illumination and expression (PIE) variations.

On the other hand, in ID-selfie matching, we are comparing a scanned or digital document photo to a digital camera photo of a live face. Assuming that the user is cooperative, both of the images are captured under constrained conditions and large PIE variations would not be present. However, the low quality of document photos due to image compression and the large time gap between the document issue date and the verification date remain as the primary difficulties. In addition, since state-of-the-art face recognition systems are based on deep networks, another issue faced in our problem is the lack of a large training dataset (pairs of ID photos and selfies).

III. EXISTING SYSTEM

In the existing system, Identity verification plays an important role in our daily lives. For example, access control, physical security and international border crossing require us to verify our access (security) level and our identities. To verify who we are by showing our ID documents containing face images, such as passports and driver licenses, to human operators. However, this process is slow, labour intensive and unreliable.

As such, an automated system for matching ID document photos to live face images (selfies) in real time and with high accuracy is required. After verifying a traveller's identity by face comparison, the gate is automatically opened for the traveller to enter. For ID-selfie matching, they are comparing a scanned or digital document photo.

IV. PROPOSED SYSTEM

We are proposing a certificate system based on block chain to overcome the problem. Data are stored in different nodes, and anyone who wishes to modify a particular internal datum must request that other nodes modify it simultaneously. Thus, the system is highly reliable. We developed a decentralized application and designed a certificate system based on Ethereum block chain. This technology was selected because it is incorruptible, encrypted, and track able and permits data synchronization. By integrating the features of block chain, the system improves the efficiency operations at each stage. The system saves on paper, cuts management costs, prevents document forgery, and provides accurate and reliable information on digital certificates and compare user live face with verified document face.

Advantages

- System Reliability is very high
- Decentralized Block chain Technology is Used
- Incorruptible, Encrypted and trackable Data.
- System Efficiency is improved
- Prevent Document Forgery and Reduce Management Cost.

V. TECHNOLOGY USED

5.1 KNN Algorithm

KNN can be used for both classification and regression predictive problems. However, it is more widely used in classification problems in the industry. To evaluate any technique we generally look at 3 important aspects:

1. Ease to interpret output
2. Calculation time
3. Predictive Power

The KNN Algorithm Work

Let's take a simple case to understand this algorithm. Following is a spread of red circles (RC) and green squares (GS):

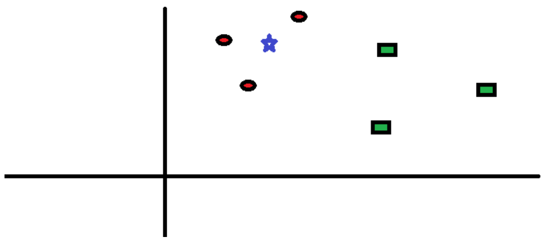


Fig 5.1

You intend to find out the class of the blue star (BS). BS can either be RC or GS and nothing else. The "K" is KNN algorithm is the nearest neighbors we wish to take vote from. Let's say K = 3. Hence, we will now make a circle with BS as center just as big as to enclose only three data points on the plane.

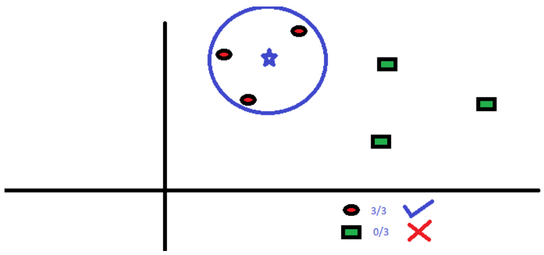


Fig 5.2

The three closest points to BS is all RC. Hence, with good confidence level we can say that the BS should belong to the class RC. The choice of the parameter K is very crucial in this algorithm.

5.2 Machine Learning

Machine learning (ML) is the scientific study of algorithms and statistical models that computer systems use to perform a specific task without using explicit instructions, relying on patterns and inference instead. It is seen as a subset of artificial intelligence. Machine learning algorithms build a mathematical model based on sample data, known as "training data", in order to make predictions or decisions without being explicitly programmed to perform the task. Machine learning algorithms are used in a wide variety of applications, such as email filtering and computer vision, where it is difficult or infeasible to develop a conventional algorithm for effectively performing the task.

The study of mathematical optimization delivers methods, theory and application domains to the field of machine learning. Data mining is a field of study within machine learning, and focuses on exploratory data analysis through learning.

VI. SYSTEM ARCHITECTURE

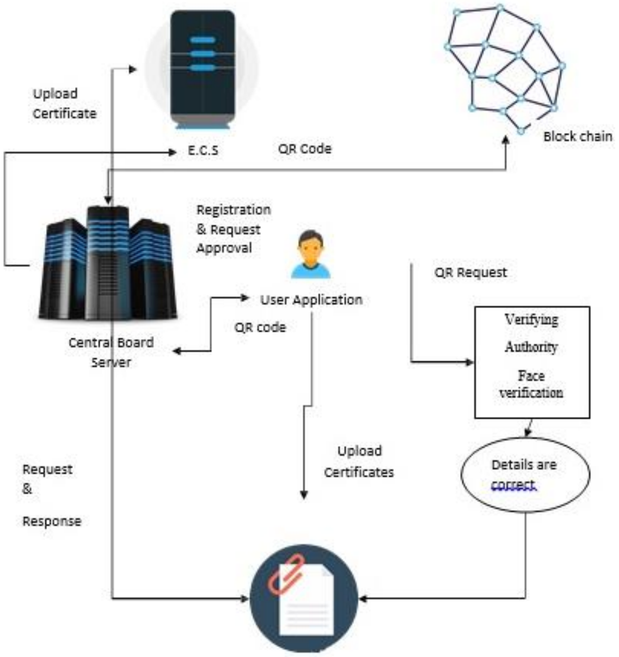


Fig 6.1 Architecture

Description

User needs to registers into his application and a request will be sent to central board server for authentication. Unless the central board server approves the request user cannot login into his account. When central board server approves the request a key will be generated and user can login into his account.

After user login into his account he needs to upload certificates namely pan card, aadhar card, voter id, ssc certificates to central board server. Central board server will review the certificates and accepts or decline the certificates. If central board server accepts the certificate those details will be stored in E.C.S and Block chain. If central board server declines the certificate it won't be stored in E.C.S. or Block Chain. If user needs a certificate he will send request to central board server.

If central board server found the user details to be genuine he accepts the request and forward a request to E.C.S where all the certificates will be there. E.C.S. responds for the request and certificates will be provided to the user. If user wants to apply for any certificates he will send request to central board server and central board server will check the details and forward the request to E.C.S. E.C.S will generate the QR Code and forwarded to user via central board server.

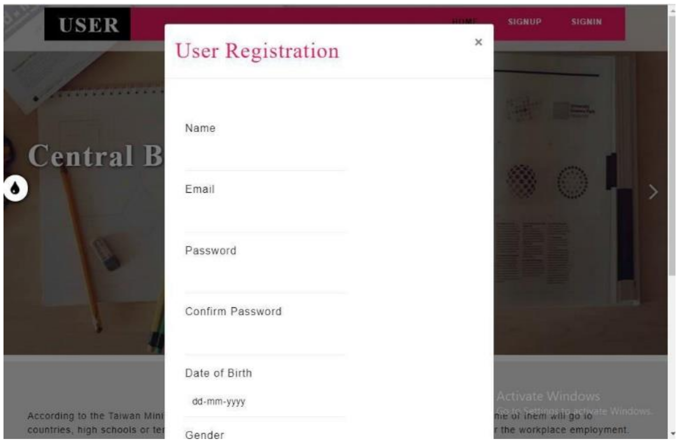
User forwards the QR code to the verifying authority and if all details are correct and face matches with live face Verifying authority will issue the document.

VII. MODULES

A module is a software component or part of a program that contains one or more routines. One or more independently developed modules make up a program. An enterprise-level software application may contain several different modules, and each module serves unique and separate business operations. Modules make a programmer's job easy by allowing the programmer to focus on only one area of the functionality of the software application.

7.1 User Registration and Authentication

In this module user needs to registers into his application and a request will be sent to central board server for authentication. Unless the central board server approves the request user cannot login into his account. When central board server approves the request a key will be generated and user can login into his account.



User Registration

Name

Email

Password

Confirm Password

Date of Birth

dd-mm-yyyy

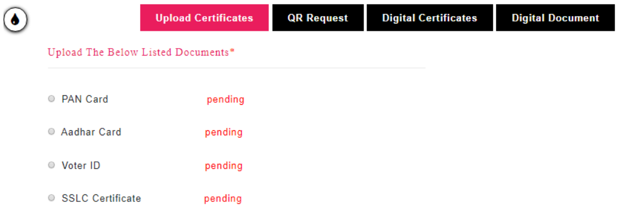
Gender

Fig 7.1

7.2 User Upload Certificate

After user login into his account he needs to upload certificates namely pan card, aadhar card, voter id, ssc certificates to central board server. Central board server will review the certificates and accepts or decline the certificates. If central board server accepts the certificate those details will be stored in E.C.S and Block chain. If central board server declines the certificate it won't be stored in E.C.S. or Block Chain.

After ECS User register their Details, this Details are sent to Central Board Authority for their Approval. Now the Central Board Authority Can Verify the User and has to Approve or Decline the User.



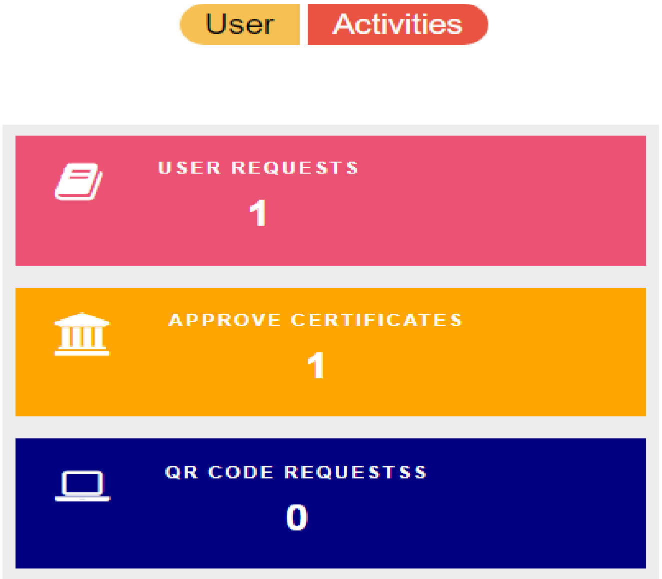
Upload The Below Listed Documents*

PAN Card	pending
Aadhar Card	pending
Voter ID	pending
SSLC Certificate	pending

Fig 7.2

7.3 Get Certificate

If user needs a certificate he will send request to central board server. If central board server found the user details to be genuine he accepts the request and forward a request to E.C.S where all the certificates will be there. E.C.S. responds for the request and certificates will be provided to the user.



User Activities

USER REQUESTS
1

APPROVE CERTIFICATES
1

QR CODE REQUESTSS
0

Fig 7.3

7.4 QR Request and Face Verification

If user wants to apply for any certificates he will send request to central board server and central board server will check the details and forward the request to E.C.S. E.C.S will generate the QR Code and forwarded to user via central board server. User forwards the QR code to the verifying authority and if all details are correct and face matches with live face Verifying authority will issue the document.

VIII. CONCLUSION

To avoid document forgery and misuse a better solution was needed for a long time. The main purpose of our developed system is to create a platform to store and verify any important documents like certificates, land/property/asset records, medical records, etc.

We implemented the whole system using Ethereum block chain network. The collaboration of some features like cryptographic hash, decentralization, and digital signature makes block chain technology immutable. As a result, there remains no central server to own the data rather all the information regarding any transactions is distributed to the whole network. After comparing our system with the general cloud-based data storage system and verification process we found significant progress in both security enhancement and time optimization. And using our proposed model data corruption and misuse will highly be reduced. In conclusion, our proposed model ensures integrity and security for every use case.

IX. FUTURE WORK

However, as a new and developing technology block chain has some minor complexities to use in every platform. But still, block chain technology outperforms any current system application available in the industry by a big margin in security and reliability. Despite all of that our future plan with this model is to create a terminal-based document authentication with the support of multiple file upload and other accessibility features to increase usability for better performance.

REFERENCES

[1] L. M. Arjomandi, G. Khadka, Z. Xiong and N. C. Karmakar,"Document Verification: A Cloud-Based Computing Pattern Recognition Approach to Chipless RFID," in IEEE Access, vol. 6, pp. 78007-78015, 2018.

[2] T. Bourlai, A. Ross, and A. Jain, "On matching digital face images against scanned passport photos," in Proc.

IEEE Int. Conf. Biometrics Identity Security (BIDS), 2009, pp. 1–10.

[3] W. Chen, Z. Xu, S. Shi, Y. Zhao, and J. Zhao, "A Survey of Blockchain Applications in Different Domains," (2018), pp. 17-21.

[4] S. Leible, S. Schlager, M. Schubotz, and B Gipp, "A Review on Blockchain Technology and Blockchain Projects Fostering Open Science," (2019), Front. Blockchain 2:16. doi: 10.3389/fbloc.2019.00016.

[5] D. White, R. I. Kemp, R. Jenkins, M. Matheson, and A. M. Burton, "Passport officers' errors in face matching," PLoS ONE, vol. 9, no. 8, 2014

[6] Xinjiang Heng an Perimeter Security Equipment Company. (2018). What Is ID- Person Matching? [Online]. Available: http://www.xjhazj.com/xjhazj/vip_doc/8380983.html