A Blockchain Based Authentication System for Digital Documents

Hari prasad[1], Manivannan[2], Ramesh[3], Prabhu[4]

Hari prasad,BTECH (INFORMATION TECHNOLOGY), Sri Muthukumaran Institute Of Technology, Tamilnadu, India[1]
Manivannan,BTECH (INFORMATION TECHNOLOGY), Sri Muthukumaran Institute Of Technology, Tamilnadu, India[2]
Ramesh,BTECH (INFORMATION TECHNOLOGY), Sri Muthukumaran Institute Of Technology, Tamilnadu, India[3]
Prabhu,BTECH (INFORMATION TECHNOLOGY), Sri Muthukumaran Institute Of Technology, Tamilnadu, India[4]

Abstract

The rapid growth 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 is also increasing. However, various challenging and tedious processes have made document verification very complex and time-consuming which motivated us to conduct this research. In this paper, we present a decentralized web application for digital document verification using Ethereum blockchain-based technology in P2P cloud storage to enhance the verification process by making it more open, transparent, and auditable. The proposed model includes several methods such as public/private key cryptography, online storage security, digital signatures, hash, peer-to-peer networks and proof of work which has made the verification of any uploaded documents for any organization or authority faster and convenient with just a click. Furthermore, respective hash values are also assigned to each individual document. Our proposed model successfully meets up all the criteria for a digital document verification system by alleviating the gaps and difficulties in the traditional methods in document verification.

Keywords: *Hashing, Ethereum, Document Verification, Digital Signature, Cryptography*

I. INTRODUCTION

The main aim of this project is to solve the problem of counterfeiting certificates we are proposing an digital certificate system based on blockchain technology and to verify the traveler’s identity using live camera, which allows faster convergence and more generalizable representations.

Synopsis: Numerous activities in our daily life require us 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, labor 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. In this paper, we propose DocFace+ to meet this objective. We first show that gradient-based optimization methods converge slowly (due to the underfitting of classifier weights) when many classes have very few samples, a characteristic of existing ID-selfie datasets. To overcome this shortcoming, to update the classifier weights, which allows faster convergence and more generalizable representations. Next, a pair of sibling networks with partially shared parameters are trained to learn a unified face representation with domain-specific parameters. Cross-validation on an ID selfie dataset shows that while a publicly available general face matcher.

II. SYSTEM ANALYSIS

2.1 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, labor 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 traveler's identity by face comparison, the gate is automatically opened for the traveler to enter. For IDselfie matching, they are comparing a scanned or digital document photo.

2.2PROPOSED SYSTEM

We are proposing a certificate system based on blockchain 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 blockchain. This technology was selected because it is incorruptible, encrypted, and trackable and permits data synchronization. By integrating the features of blockchain, 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.

III. REQUIREMENT SPECIFICATIONS

3.1 INTRODUCTION

The rapid advancement of information sharing and exchanging is driving more and more companies and individual users towards the use of digitized documents. Moreover, the cumbersome and time-consuming use and validation process of traditional physical documents contribute to motivating people to use modern ways of issuing and validating important documents. Though digital documents are undoubtedly convenient to use, proving the authenticity of these documents is often a matter of concern. Due to the technological revolution and ease of access to cheap and advanced equipment, the forgery of important documents has become quite easy and made document authentication quite a tedious task. The implication arising from the problem of fake documentation is causing serious and alarming impacts and needs to be urgently taken into consideration. Therefore, a system to validate the authenticity of important documents would be greatly beneficial to users for maintaining their digital documents. There is an open-source, immutable, and consensus model available called blockchain to solve this problem [3].

Blockchain technology is a recent invention to enhance the document verification process and entangle the task of reducing document fraud and misuse [4]. Blockchain simply refers to a distributed database that chronologically stores multiple blocks chained together with each data pack or block storing documents in a way that makes it impossible to manipulate these documents [8]. Blockchain is an advanced technology that can play many significant roles in the industry to overcome any failure. Blockchain ensures trust, integrity, consensus, autonomy, and safety [13]. Owing to the purely reliable, transparent, and incorruptible method of storing and validating the transactions, we have also been motivated by this blockchain technology to use it in our work to authenticate important digital documents.

3.2 HARDWARE AND SOFTWARE SPECIFICATION

3.2.1 HARDWARE REQUIREMENTS

➢ Hard Disk	:	80GB and Above

RAM	:	4GB and Above
Processor	:	P IV and Above

3.2.2 SOFTWARE REQUIREMENTS

- Windows 10
- JDK 1.7
- J2EE
- Tomcat 7.0
- MySQL

IV. CONCLUSION

We need not carry the documents for verification insteadofwe can make the documents in digital format for verification. KNN algorithm is one of the simplest classification algorithms. Even with such simplicity, it can give highly competitive results. KNN algorithm can also be used for regression problems. Which allows faster convergence and more generalizable representations. Next, a pair of sibling networks with partially shared parameters are trained to learn a unified face representation with domain-specific parameters. Cross-validation on an ID selfie dataset shows that while a publicly available general face matcher.

V. REFERENCES

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

[2] A. Prashanth Joshi, M. Han, and Y. Wang, “A Survey on Securityand Privacy Issues of Blockchain Technology,” (2018), MathematicalFoundations of Computing, Volume 1, Issue 2, pp. 121-147, doi:10.3934/mfc.2018007.

[3] W. Chen, Z. Xu, S. Shi, Y. Zhao, and J. Zhao, “A Survey ofBlockchain Applications in Different Domains,” (2018), pp. 17-21, doi:https://doi.org/10.1145/3301403.3301407.

[4] K. Gilani, E. Bertin, J. Hatin and N. Crespi, ”A Survey on BlockchainbasedIdentity Management and Decentralized Privacy for PersonalData,” 2020 2nd Conference on Blockchain Research and Applicationsfor Innovative Networks and Services (BRAINS), Paris, France, 2020,pp. 97-101, doi: 10.1109/BRAINS49436.2020.9223312.

[5] J. Wang, S. Wang, G. Junqi, Y. Du, S. Cheng, and X. Li, “A Summaryof Research on Blockchain in the Field of Intellectual Property,”(2019), Procedia Computer Science, Volume 147, pp. 191-197, doi: https://doi.org/10.1016/j.procs.2019.01.220