iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** II **Month of publication:** February 2023

DOI: https://doi.org/10.22214/ijraset.2023.49222

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue II Feb 2023- Available at www.ijraset.com

Digital Identity

Anindita Karmakar[1], Komal[2], Kshitij Johri[3], Ms. Rupam[4], Ms. Gurminder Kaur[5]
[1, 2, 3]*CSE Scholar, BMIET Sonepat*
[4]*A.P.CSE,* [5]*ASSOC. P. CSE, BMIET Sonepat*

Abstract: Our digital and physical lives are increasingly linked to the apps, services, and devices we use to access a rich set of experiences. This digital transformation allows us to interact with hundreds of companies and thousands of other users in ways that were previously unimaginable. The whole concept here is to make a decentralized network of blockchain to provide each person in the world a unique identity based on their biometrics with great privacy and no intervention of a single authority. We have used a distributed blockchain system for this purpose, SHA-256 for hashing, digital certificated for identity verification. This project will give a unique identity and can be trusted by every organisation. It can be integrated with storing digital documents and verification of the credential for any organisational use, of course only with the permission of a individual.

I. INTRODUCTION

In India, the basic structure of a student's studies goes like taking admission in kindergarten, after that changing of school for primary, secondary, and high school studies. Now, after completing high school students, need to get admission into junior college. For graduation, there's also once again changing of college. This is the basic cycle for student's study years. After this, some students continue to pursue higher studies. Due to this, an unwanted scenario rises i.e. tampering and production of fake or duplicate certificates. There are a lot of hidden agencies in our country who are running this scam behind everyone's back. Technology has moved quite forward until now. Distinguishing between a fake and an original certificate will require a lot of concentration and result in wastage of precious time. For removing this disadvantage, a technology named Blockchain comes into our life as a savior.

II. MOTIVATION

We covered a case study in to gain our motivation for the scenario:- The Mohali police have busted a gang that was active throughout the country and provided fake degrees and certificates of various courses at school, college and university level. In the preliminary investigation, it has come to light that the gang has issued around 1,000 fake degrees of at least 16 government and private universities and school boards. They were duping students on the pretext of providing them degree certificates of various renowned Indian universities, said the SP. In return, they were collecting a big amount of money as well as ID proofs from the students. The students who wished to study abroad or who wanted to fill the gap years were their main targets. At least, 1,000 such students were been identified yet.

A. Problem

Our digital and physical lives are increasingly linked to the apps, services, and devices we use to access a rich set of experiences. This digital transformation allows us to interact with hundreds of companies and thousands of other users in ways that were previously unimaginable. So, the goal here is to make a decentralized network of blockchain to provide each person in the world an unique identity based on their biometrics with great privacy and no intervention of a single authority.

B. Solution

For the loopholes in our current methodologies, we have proposed our system which will automatically generate certificates as well as validates them. The data will be authenticated, reliable and unchangeable.

C. Objective

The main objectives of this application are:-

1) To have a unique ID for each user on the network.
2) To provide a system which can't be penetrated by anyone and protect personal data.
3) To give user full right to control their data.
4) To provide third party organizations to have a trustworthy identity verification service.

III. METHODOLOGY

A. SHA-256

SHA 256 is a part of the SHA 2 family of algorithms, where SHA stands for Secure Hash Algorithm. Published in 2001, it was a joint effort between the NSA and NIST to introduce a successor to the SHA 1 family, which was slowly losing strength against brute force attacks. The significance of the 256 in the name stands for the final hash digest value, i.e. irrespective of the size of plaintext/cleartext, the hash value will always be 256 bits. The other algorithms in the SHA family are more or less similar to SHA 256.

B. Database Structure

This is our database structure. Our database structure is named as identity db. It contains three collections (a) Document Details (b) Share Details (c) User Details

C. API

API capture the requests, executes them as python functions written in backend and sends back responds back in the form of json documents to the frontend code.

D. Database Connection

This database connection code connects python to the backend cloud deployed MongoDB database server. It establishes connection, fetches, add, modify document in the respective database. databaseConnection.py

E. Blockchain Connection

This blockchain connection port implements the function required to connect deployed blockchain. Frontend Frontend code represents all the frontend webpages for users, Issuer, Verifier In Reactjs. http://api.py

IV. SCOPE OF THE PROJECT

1) The project is helpful for maintaining the security of the documents provided by government as well as checking the validity of documents.
2) This project can be helpful in organization where documents are sensitive and verification is required.
3) Can be adopted by Government as a central platform with all the participating authorities as various organizations where they are the majority body to access and approve the changes made.

Technology Used Software Requirement Specification

a) *Operating System:* The project is independent on the Operating System platform. But we are using Linux (Ubuntu) as the Operating System platform.
b) *Visual Studio Code:* Visual Studio Code for the Web provides a free, zero-install Microsoft Visual Studio Code experience running entirely in your browser, allowing you to quickly and safely browse source code repositories and make lightweight code changes
c) *MongoDB:* MongoDB, the most popular NoSQL database, is an open-source document-oriented database. The term NoSQL' means 'non-relational". It means that MongoDB isn't based on the table- like relational database structure but provides an altogether different mechanism for storage and retrieval of data. This format of storage is called BSON (similar to JSON format).
d) *Web Browser:* A web browser takes you anywhere on the internet. It retrieves information from other parts of the web and displays it on your desktop or mobile device. The information is transferred using the Hypertext Transfer Protocol, which defines how text, images and video are transmitted on the web.
e) *Python PyMongo:* The PyMongo distribution contains tools for interacting with MongoDB database from Python. The bson package is an implementation of the BSON format for Python. 194 ofCarnufor E. 19 amiis1a97 Colloaa off Emai19001 WEB3:- Web3 enhances the internet as we know it today with a few other added characteristics. web3 is

- Verifiable
- Trustless
- Self-governing
- Permissionless

f) Ethereum Blockchain; The Ethereum blockchain has spearheaded the modernization of a true decentralized marketplace. That's about as technical as we're going to get. One of the things that keep certain folks who could make good money on the Ethereum blockchain from doing so is a lack of understanding of how things work.

V. HARDWARE REQUIREMENT SPECIFICATION

The algorithms used in the project are computationally intensive and thus require high computing capabilities in terms of hardware. For the testing and demo purpse we used basic hardware usually found in desktop type of computers. But to reduce the computation time of the project.

We recommend to use high performance system or cloud based computing facilities

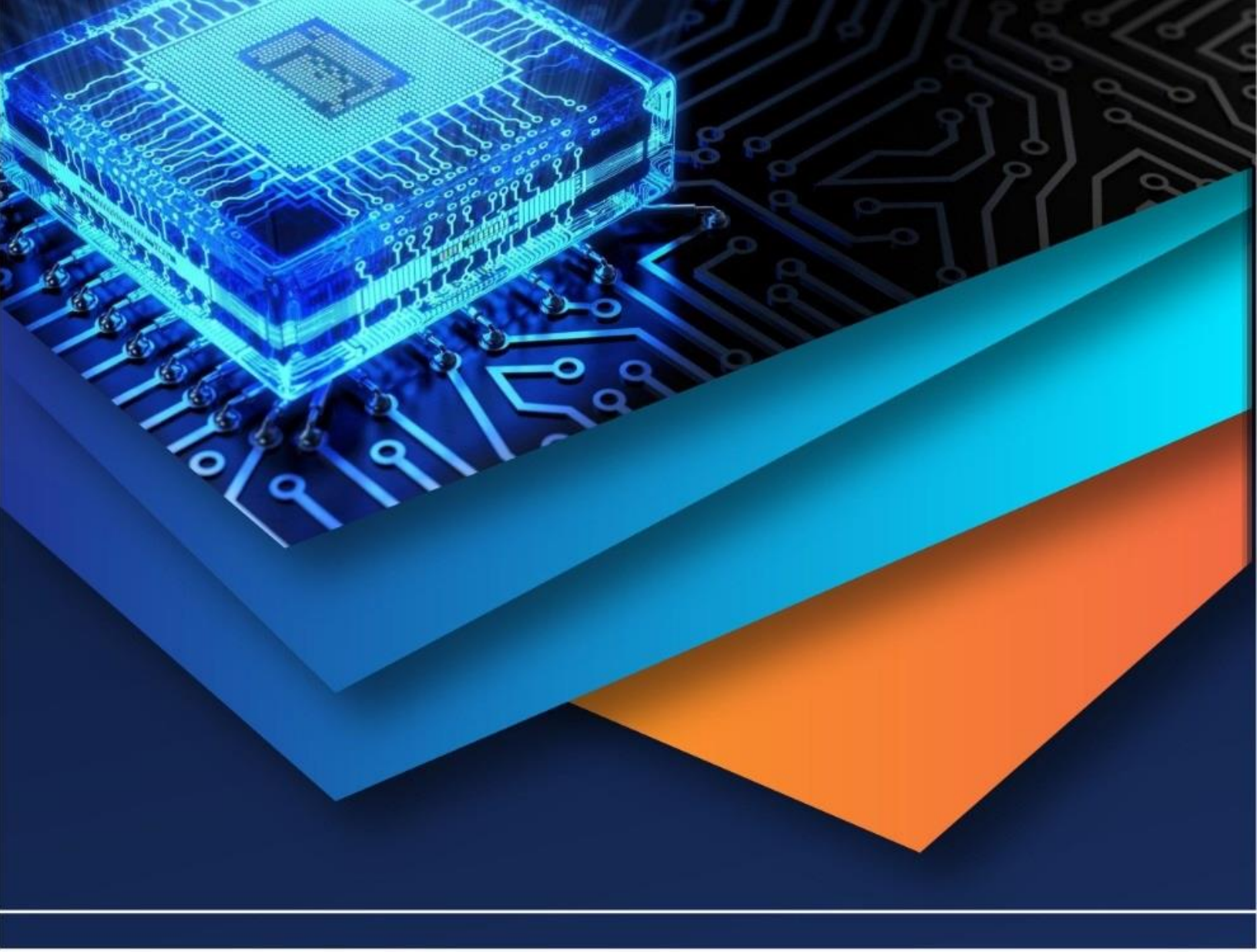
1) Machine with Windows or Linux Platform
2) Processor i3 or above
3) Ram 4GB or above
4) Hard Disk manage data well.

VI. CONCLUSION

The document is easily stored and accessed through a working frontend, and stored at backend with use of blockchain technology where, changes are accepted only when the users with hash key permits it to. If any unauthorized persons/hacker gets the access of a block the next blocks will be inaccessible and couldnt get all the data.

REFERENCES

[1] Zibin Zheng , Shaoan Xie, Hong-Ning Dai, Xiangping Chen , An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, IEEE 6th International Congress on Big Data, 2017.
[2] Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, Blockchain and Smart Contractfor Digital Certificate, Proceedings of IEEE International Conference on Applied System Innovation 2018.
[3] Maharshi Shah, Priyanka Kumar, Tamper Proof Birth Certificate Using Blockchain Technology, International Journal of Recent Technology and Engineering (IJRTE),Volume7, Issue-5S3, February 2019.
[4] Emmanuel Nyaletey, Reza M. Parizi, Qi Zhang, Kim-Kwang Raymond Choo, BlockIPFS – Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability, IEEE International Conference on Blockchain, 2019.
[5] Gunit Malik, Kshitij Parasrampuria, Sai Prasanth Reddy, Dr. Seema Shah, Blockchain Based Identity Verification Model, International Conference on VisionTowards Emerging Trends in Communication and Networks



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY