

Criminal Record Manager

Paidi Praneeth Kumar Computer Science and Engineering BML Munjal University Gurgaon, Haryana paidi.praneethkumar.18cse@bmu.edu.in	Venkata Abhiram Edapalapati Computer Science and Engineering BML Munjal University Gurgaon, Haryana edapalapati.venkataabhiram.18cs@bmu.edu.in	Kireet Gannavarapu Computer Science BML Munjal University Gurgaon, Haryana g.kirannagakiireetachary.18cse@bmu.edu.in	Chakka Sai Teja Computer Science BML Munjal University Gurgaon, Haryana chakka.saiteja.18cse@bmu.edu.in
---	--	---	--

Abstract

At present, the police stations are maintaining the criminal records with less security and which can be modified easily. The databases that are now maintained by the police stations for the criminal records are very much vulnerable to threats in the form of hacking, data tampering by un-authorized peoples and other officers. The database containing the criminal records of a person is a very important asset of the country and its security should be monitored strictly. To overcome this problem we can use Blockchain in maintaining the criminal records. When it comes to today, India is increasingly making its way into the modern age. After the announcement of the "Digital India" initiative, the Indian Police Department has replaced the manual system with a streamlined online process for filing complaints. In this paper we are going to introduce the use of Blockchain technology that is used for maintaining the criminal records. Blockchain is a method of storing data that makes it difficult or impossible to alter, hack, or defraud a country's judiciary. A blockchain is a decentralized database of transactions that is duplicated and replicated through the blockchain's entire network of computing systems. In order to make the criminal records tamper-proof we use the concept of hashing. The only people that are able to add or modify the data are the police officials. The Web3 Remote Procedure Call (RPC) protocol is used to link the local database to the Ethereum blockchain. In this we are also going to introduce the advanced technology blockchain, cloud computing and biometric recognition available to the police department which will come in hand to reduce the time duration for finding the culprit. A number of simulations have been run to assess the proposed framework's performance. The completed web application was able to successfully store the criminal records of various test cases with high security provided by the Blockchain.

1. Introduction

In recent years, we have seen incidents in police departments where the police have forged the details in the FIR's and complaints after filing it. There is also the problem that it's very difficult to search for a particular data in that huge no of records across all the states in police stations. The total amount of data stored in the world in the form of digital media is increasing rapidly each year. As everything these days are being stored on the internet, it becomes important to ensure the security of the data. India has moved to digital form and data is being stored online, many records can be tampered and it also becomes difficult to search through the data as it takes so long to find the record. So in order to overcome this we planned to work on this project. By using Blockchain we planned to make a medium to securely store the information of criminals in an online database which is not only secure but also fast.

a. Real World implications

There are no universally agreed protocols or operating networks. As a result, evaluating the consistency of available options and deciding how to better incorporate them into their current IT landscapes is difficult for them and the blockchain vendors are almost all start-ups, procurement departments can find it difficult to find long-term collaborators.

b. Futuristic Implications

Jurisdictional Problems: Since the nodes of a distributed ledger can exist around the whole world across multiple countries, it is difficult to understand which country's jurisdiction's laws and regulations are to be applied to a particular blockchain software. This also involves the problem of taxation since taxes are different in different countries.

Risk of Cyber-attack: The distinctive challenge to unorganized systems, significantly public blockchains, is that information input may be from any range of nodes, which means there's a risk of change of state at every node. The advantage of employing a ‘tamper proof’ technology is negated if the data held on the ledger is compromised to start with.

The Accountability: A crucial challenge for authorities in regards to decentralized structures is who should be kept responsible for violations of law and legislation. This is analogous to the issue of assessing transparency before the advent of blockchain on the Internet.

As citizens of our country, we wanted to make a project which can be useful to society. We find this as an opportunity to pay back to the society as its citizens. Police sector is one of the fields in which we can contribute to something useful. This was the reason why we chose to work on this project to provide the police sector with a software to manage their criminal records in a secure way.

There are two application domains covered in this project. One of them is a Judiciary domain and another one is Bioinformatics. Judiciary domain involves law enforcement and making sure that the country is running lawfully. Since our project involves the concept of recording the criminal records on a blockchain, it comes under the Judiciary domain. Bioinformatics is a field which involves methods and tools to understand biological data. Fingerprint identification, classification of biological information like face patterns, retina information come under this domain. Our project has a feature to detect faces of the criminals hence putting it under this domain.

Information stored on a blockchain is secure and safe from tampering due to how a blockchain is structured. We wanted to make a software that can store criminal data safely. This led us to the concept of blockchain which was a really good solution to the problem. As our main target is to prevent the tampering of data, we thought this could be achieved through blockchain technology where one can add the data but cannot delete it. So, the people who were filed in a particular case will get registered in the database.

2. Related Work

In [1] the authors have explored the ways of improving data management in the public sector using blockchain and they have used a method called Keyless Signature Infrastructure (KSI) to safeguard the all public sector data. This KSI creates a hash value which represents the large amount of data as a small numerical value. This hash value helps us to identify the records but not to reconstruct or manipulate the data present in it.

A method to use blockchain to improve the security of an FIR system was explored in [2]. For the reusability of data they have used multi-signature. They considered the ledger for the transactions in a distributed network fabric and the nodes act autonomously on the transactions and then these transactions are communicated to all the nodes using a multi-hop broadcast. A valid transaction makes the block and this is made into the block chain only after it meets the adequate consensus.

In [3] the authors have discussed an evolving technology in blockchain i.e. biometric blockchain. They explored the usage of facial recognition in blockchain using convolutional neural networks. A traditional biometrics can be hacked easily and cause conflicts. The approach used in [3] is illustrated in the fig 1 as given below:

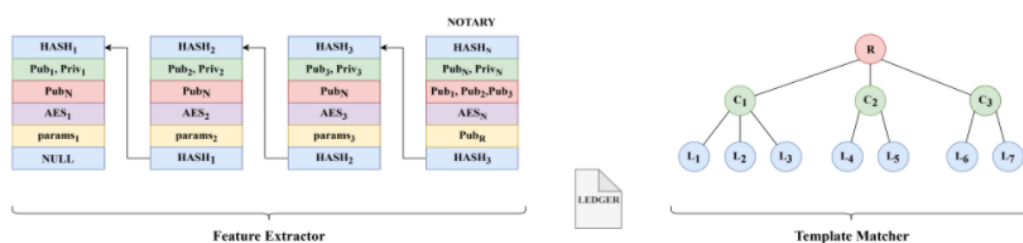


Fig 1. Biometric Blockchain Feature Extraction

In [4] authors provided a detailed overview about the legal issues associated with blockchain for emerging markets. They explained from an economical perspective and how blockchain will change the market. They also explain the legal issues of using a blockchain and the challenges faced like crypto assets, data protection, some are due to the law, privacy of the data and cyber-attacks like distributed DoS (denial of service) and double spending.

The authors of [5] proposed a framework focused on a clever agreement that was used to investigate the Ethereum blockchain's ability to provide integrity to e-FIR data stored in the police station's database, whereas the Local database could be interfaced with Ethereum blockchain using the Web3 RPC (Remote Procedure Call) protocol. A few simulations were run to evaluate the overall performance of a proposed system. The authors' findings show a trade-off between the number of transactions saved in a single block on the blockchain ledger and the exclusive hashing protection tiers for the offences facts.

The authors of [6] examined the implementation of Blockchain generation, which eliminates the need for a centralised authority by allowing an untrusted node network to continuously exchange transactional records. The authors proposed a machine that stores citizen criminal information in a decentralised manner using a permissioned blockchain. This machine has a competitive advantage over modern machines because it cryptographically ensures that information, once stored, can only be modified by a competent authority. It also increases the report's transportation to its destination, which can be extended for the length of the geographical territory.

In [7] authors have talked about that India has been growing thoroughly in generation wise however the system lacks in security angle. The authors' aim is to present a method for securing the FIR system using blockchain technology. This enables us to bring a critical theory of the blockchain age into the Indian police force, which will protect the FIR from malpractices. The authors used the multi-signature method for reusability statistics. They use an RSA set of rules to encrypt and signal the transmitted data, making it easier for receivers to confirm information.

3. Proposed System

a. Components

i. Solidity

Solidity is a statically-typed curly-braces item orientated programming language designed for growing smart contracts that run on Ethereum. Smart contracts are applications which govern the behaviour of bills in the Ethereum country. The benefits of using solidity are inheritance support and Application Binary Interface (ABI). ABI is an interface which enables interactions among two binary programs or applications. The dangers of the usage of solidity are transactional operations, restrained expressiveness and it's miles a new language which makes it more complicated to recognize and additionally has very less libraries to use for the builders. In this mission the solidity is utilized in growing clever contracts like including records to the blockchain and retrieving from the blockchain.

ii. Truffle

Truffle is an improvement of surroundings, checking out framework and asset pipeline for Ethereum, aiming to make existence as an Ethereum developer less difficult. The professionals of truffle in block chain are Development environment and checking out framework for Ethereum contracts, uses Mocha and Chai libraries, It lets in you to assemble, install and check the Smart Contracts, and further, configure the deployment scripts. Provides an Interactive console. Comes with Ganache software that can create and control a private and personal Blockchain. It additionally offers a CLI software to create a check Blockchain named "testrpcsc". In the task truffle is useful in trying out the clever contracts for ethereum.

iii. Flask

Flask, a python based micro net framework. It is considered as a microframework since flask does not need any precise equipment or libraries. It has no shape validation and database abstraction layer or any other additives wherein pre-present 3rd-celebration libraries provide not unusual functions. Flask is constructed on the Werkzeug WSGI toolkit and the Jinja template engine. It is less difficult than Django however has a smaller network and less libraries than Django. This mission makes use of flask to acquire api calls and send the requests to the web framework.

iv. PyMongo

PyMongo, A Python distribution which contains the equipment needed to work with MongoDB, and is the reliable way to work with MongoDB from Python.

v. MongoDB

MongoDB is a cross-platform source-available file-orientated database application. It is a NoSQL database software, MongoDB makes use of JSON-like files with elective schemas. There are numerous advantages using MongoDB inclusive of No complex joins are needed and There isn't any courting among statistics in MongoDB. It is likewise very clean to set up and set up. It uses record question language which is straightforward compared to the SQL queries. MongoDB uses internal memory for the storage to get entry which makes it quicker to access the data. This mission makes use of MongoDB to keep the photos of the wrongdoer.

vi. Google Cloud Platform

Google Cloud Platform, provided by Google, is a collection of cloud computing services that operate on the same infrastructure that Google uses internally for its non-consumer products, such as Google Search, Gmail, document storage, and YouTube. This project uses GCP to share the records to the authorised persons over the internet.

vii. OpenCV

OpenCV is a programming functions library mainly focused on the actual-time pc imaginative and prescient. Originally evolved through Intel later became by using Willow Garage then Itseez. The library is move-platform and loose for use under the open-supply Apache 2 License. OpenCV is quite speedy and makes use of Low RAM. It may be run on any tool that may run C. This mission makes use of the OpenCV to recognise the faces of the culprit inside the actual-international with CCTV cameras.

viii. Metamask

MetaMask is a cryptocurrency wallet which helps to interact with the Ethereum blockchain. Users can use metamask as a plugin extension or a smartphone app to access their Ethereum wallet, which can then be used to communicate with decentralised apps. This project uses Metamak for interacting with Blockchain which contains data about culprits

ix. Web3JS

WebJs is a collection of javascript libraries that allows us to interact with a neighborhood or remote ethereum node using HTTP, IPC or WebSocket. It takes care of encoding payloads and generating the RPC calls. The maximum used library for interacting with Ethereum is JavaScript and Node.js. Web3 isn't always an Ethereum node however as a substitute, it's used to speak to Ethereum nodes. There are different technologies just like Web3 JS like Go-lang(cross-ethereum) , Node js. The modern-day undertaking makes use of the Web3 js for RPC calls and encoding.

4. Methodology

The project has three different functionalities which flowed in a way of adding the record, finding the crimes of the culprit using the unique id, and finding the culprit in the real-world. The project is developed in different phases similar to the flow-chart below.

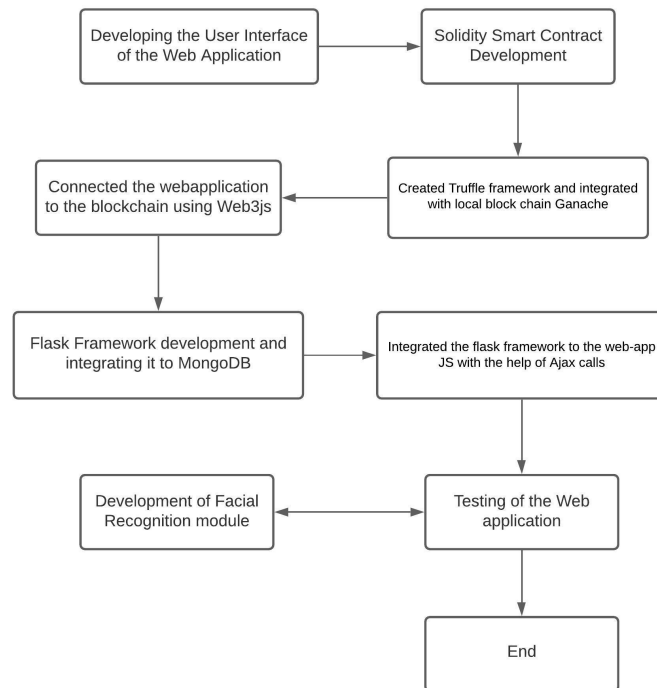


Fig 2. Flow-chart

a. System:

The final system is a web Application which includes all the functionalities at the same place which can be used by a local police station.

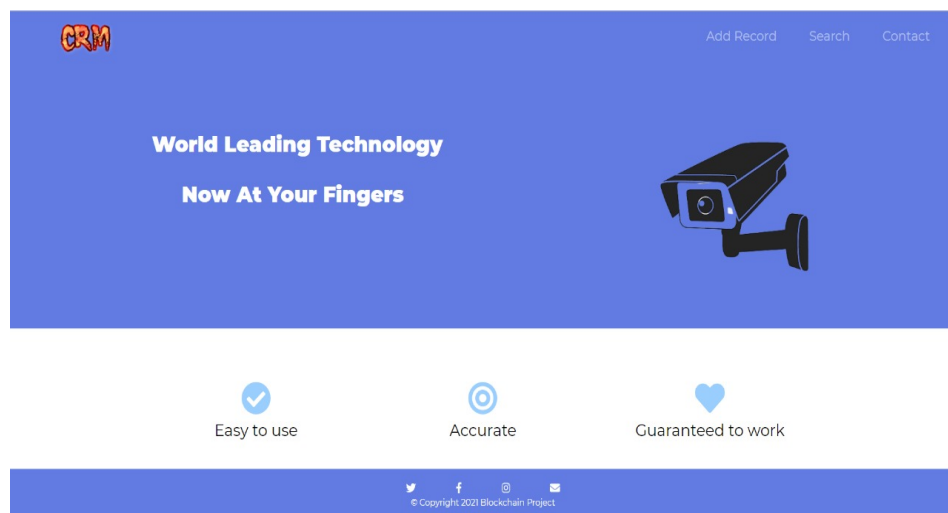


Fig 3. UI of Application

b. Adding record to blockchain:

Blockchain systems use public-private key cryptography, which encrypts data and allows only those with the private key to access it. Anyone with access to the data will see it,

but they have no means of unlocking it. This information is stored in blocks, which are linked to each new block added to the chain after a certain amount of time has passed. These blocks are exchanged by all on the network, and another cryptographic feature ensures that each block on each device is similar. In brief, we now have a way to demonstrate that a piece of data on the blockchain is original, unchangeable, and accessible only to the intended receiver.

Fig 4. Adding Record to blockchain using Web Application

Data is stored in a Block chain by means of contracts, in Solidity, a contract is a set of code with its functions and data i.e. the state that exists at a particular Ethereum blockchain address.

Fig 5. Creating a Record with MetaMask transactions

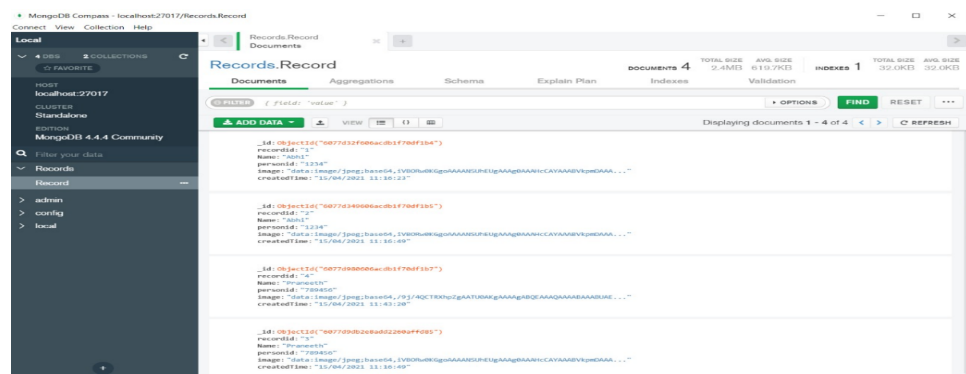
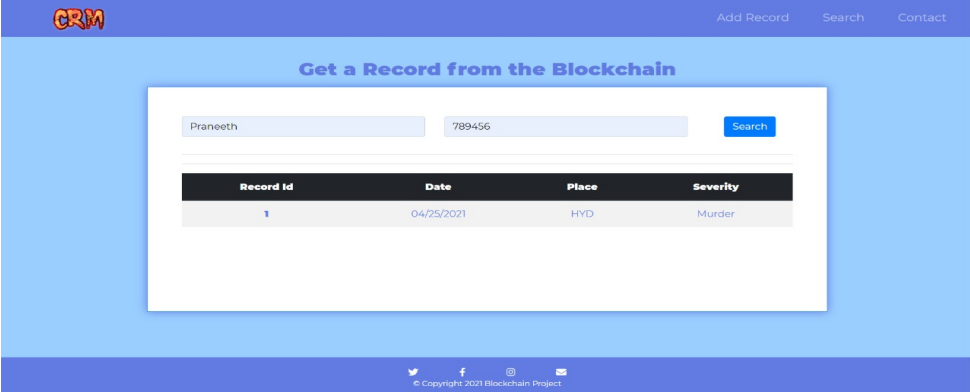


Fig 6. Storing a few amount of data into database

c. Finding the crimes of culprit :

Whenever the record is added using the above process of blockchain it creates an unique id for each block. The record then can be read or fetched using the id of the block. But it will be very much difficult to traverse the whole blockchain and find the id we use the name of the culprit and his unique id (Aadhar, voter id etc.,) to fetch the crimes of the culprit that has been committed by him.



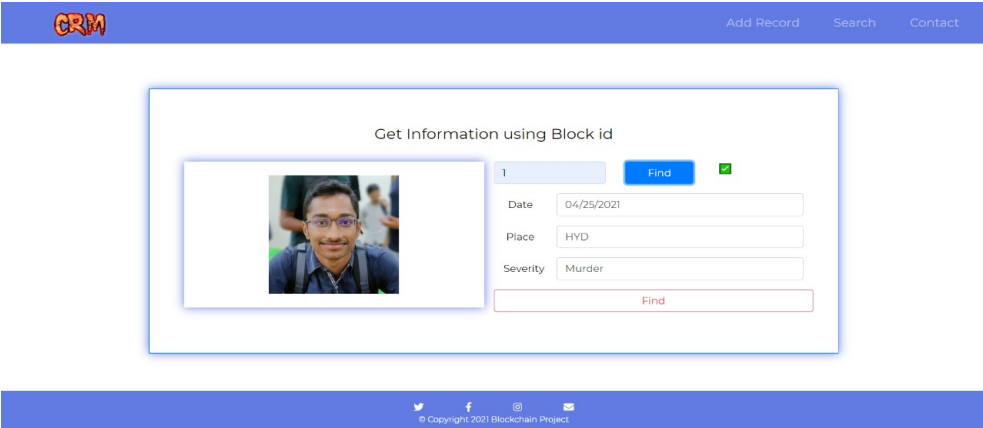
The screenshot shows the CRM application interface. At the top, there is a navigation bar with the CRM logo and links for 'Add Record', 'Search', and 'Contact'. The main heading is 'Get a Record from the Blockchain'. Below this, there is a search form with two input fields: one for the name 'Praneeth' and another for the unique ID '789456'. A 'Search' button is to the right of the ID field. Below the search form, a table displays the search results. The table has four columns: 'Record Id', 'Date', 'Place', and 'Severity'. The first row shows '1' for Record Id, '04/25/2021' for Date, 'HYD' for Place, and 'Murder' for Severity. At the bottom of the page, there are social media icons and a copyright notice: '© Copyright 2021 Blockchain Project'.

Record Id	Date	Place	Severity
1	04/25/2021	HYD	Murder

Fig 7. Finding Person crimes Id with the help of Unique ID

d. Finding the culprit :

The Crimes recorded in the blockchain have unique ids. These block ids are used to find the culprit in the real-world. The database is stored with the names of the culprits. While sending the details we use the id of the block to send the details or names of the culprit to the backend services. The services run all the time in the backend with the cameras being connected. The connected cameras are always activated and search for the culprit.



The screenshot shows the CRM application interface for retrieving a record. At the top, there is a navigation bar with the CRM logo and links for 'Add Record', 'Search', and 'Contact'. The main heading is 'Get Information using Block id'. Below this, there is a form with a 'Find' button and a green checkmark. To the left of the form, there is a placeholder image of a person. Below the 'Find' button, there are input fields for 'Date' (04/25/2021), 'Place' (HYD), and 'Severity' (Murder). At the bottom of the form, there is a 'Find' button. At the bottom of the page, there are social media icons and a copyright notice: '© Copyright 2021 Blockchain Project'.

Fig 8. Retrieving the record from the Block chain

Whenever the data of the culprit that has to be found is sent to the google drive where it is shared to the remote locations then using the camera we can scan the suspect and when it finds the culprit it recognizes the face and shows his name on the screen.

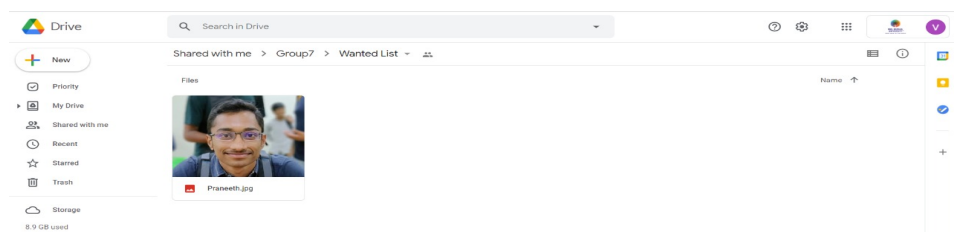


Fig 9. Uploading the persons Data into Cloud

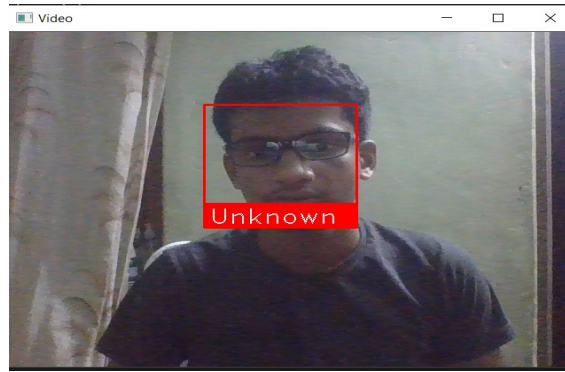


Fig 10. Scanning the people faces for the required person

e. Algorithm

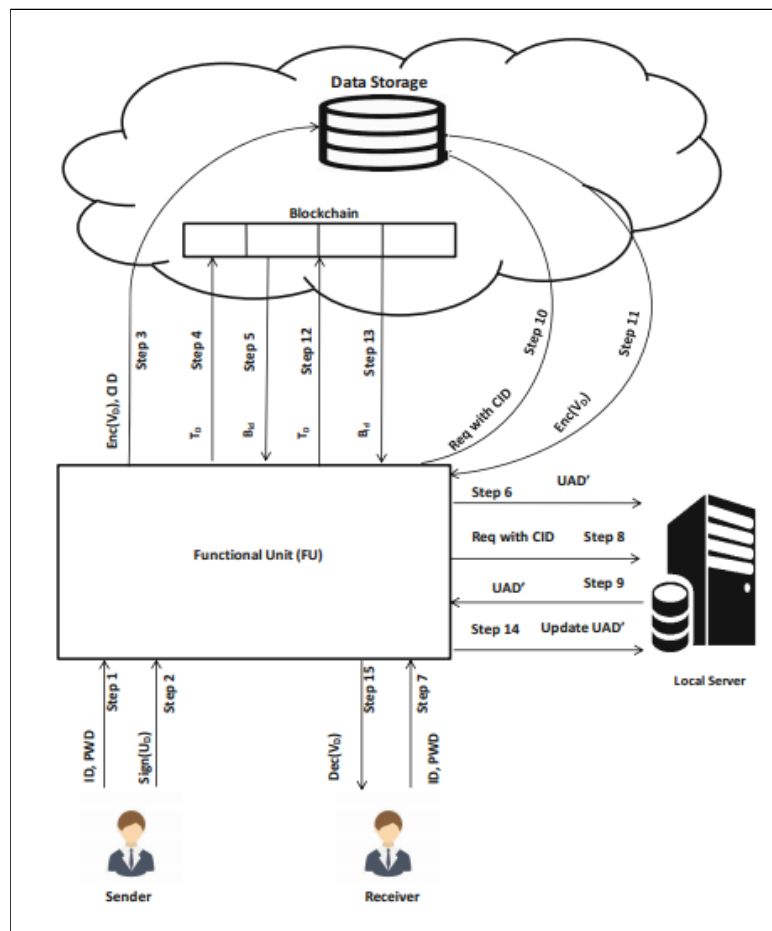


Fig 11. Algorithm

5. Conclusion and Future Work

Project explores the field of criminal record management in the police department for the prevention of unwanted leakage of data and data tampering using the concept of blockchain. In the project we have proposed a framework where we made a web application using Html and CSS for the front end of the website, using flask and web3 JS to connect the website to the blockchain and used OpenCV to do the facial recognition of the test criminals on the blockchain. Since we used blockchain to store our records, data

tampering is not possible because of the blockchain and the hashing algorithms we have used. Solving the problem of removal of information about a criminal from the blockchain. The web application was tested on multiple browsers using multiple test cases and simulations to test whether the application was working as intended.

The proposed system will be further investigated in the future by testing various other hashing methods to be used on the records in the blockchain and larger scale working of the software and better face recognition in the real time world.

References:

- [1] Steve Cheng, Matthias Daub, Axel Domeyer, and Martin Lundqvist, Using blockchain to improve data management in the public sector. (2017a, March 24). McKinsey & Company. <https://www.mckinsey.it/idee/using-blockchain-to-improve-data-management-in-the-public-sector>
- [2] “Bhushan Dube ,Mahesh Gangarde, Ankit Singh, Jitendra Pawar, Sagar Dhanake, Blockchain Based Digital Crime Record Management System, JAC : A JOURNAL OF COMPOSITION THEORY, <http://www.jctjournal.com/gallery/11-july-2020.pdf>”
- [3] “Goel, Akhil & Agarwal, Akshay & Vatsa, Mayank & Singh, Richa & Ratha, Nalini. (2019). Securing CNN Model and Biometric Template using Blockchain. 10.1109/BTAS46853.2019.9185999.”
- [4] “Salmon, John; Myers, Gordon. 2019. Blockchain and Associated Legal Issues for Emerging Markets. EMCompass;Note 63. International Finance Corporation, Washington, DC. © International Finance Corporation. <https://openknowledge.worldbank.org/handle/10986/31202> License: CC BY-NC-ND 3.0 IGO.”
- [5] “N. D. Khan, C. Chrysostomou and B. Nazir, "Smart FIR: Securing e-FIR Data through Blockchain within Smart Cities," 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), 2020, pp. 1-5, doi: 10.1109/VTC2020-Spring48590.2020.9129428.”
- [6] “A. T. Dini, E. Gabriel Abete, M. Colombo, J. Guevara, B. S. Menchón Hoffmann and M. Claudia Abeledo, "Analysis of implementing blockchain technology to the argentinian criminal records information system," 2018 Congreso Argentino de Ciencias de la Informática y Desarrollos de Investigación (CACIDI), 2018, pp. 1-3, doi: 10.1109/CACIDI.2018.8584365.”
- [7] “Mr.Bhushan Dube, Mr.Mahesh Gangarde, Mr.Ankit Singh, Mr.Jitendra Pawar, Prof. Mr.Sagar Dhanake, Blockchain Base Crime Record Management System,<http://www.jctjournal.com/gallery/11-july-2020.pdf>”
- [8] “Tasnim, Maisha & Omar, Abdullah & Rahman, Shahriar & Bhuiyan, Md. (2018). CRAB: Blockchain Based Criminal Record Management System. 294-303. 10.1007/978-3-030-05345-1_25.”
- [9] “Rahul Tyagi , Prashant Shukla , Anish Tyagi, 2020, Implementation of Blockchain on Criminality Record Checker, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 09, Issue 04 (April 2020)”
- [10] “Kim D, Ihm S-Y, Son Y. Two-Level Blockchain System for Digital Crime Evidence Management. *Sensors*. 2021; 21(9):3051. <https://doi.org/10.3390/s21093051>”
- [11] “Khan PW, Byun Y-C, Park N. A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities. *Electronics*. 2020; 9(3):484. <https://doi.org/10.3390/electronics9030484>”