A

Major Project

On

AN IMPLEMENTATION OF BLOCK CHAIN TECHNOLOGY IN

FORENSIC EVIDENCE MANAGEMENT

(Submitted in partial fulfillment of the requirements for the award of Degree)

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

By

E.SHIVANI (197R1A05K7)

G.VIDYADHARI (197R1A05L2)

D.SUMANTH (197R1A05K6)

Under the Guidance of

RAHEEM UNNISA

(Assistant Professor)



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CMR TECHNICAL CAMPUS

UGC AUTONOMOUS

(Accredited by NAAC, NBA, Permanently Affiliated to JNTUH, Approved by AICTE, New Delhi) Recognized Under Section 2(f) & 12(B) of the UGCAct.1956, Kandlakoya (V), Medchal Road, Hyderabad-501401.

**2019-2023**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**



**CERTIFICATE**

This is to certify that the project entitled **“AN IMPLEMENTATION OF BLOCKCHAIN**

### TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT” being submitted

by D.SUMANTH (197R1A05K6),G.VIDYADHARI (197R1A05L2) and E.SHIVANI

(197R1A05K7**)** in partial fulfilment of the requirements for the award of the degree of B.Tech in Computer Science and Engineering to the Jawaharlal Nehru Technological University Hyderabad, is a record of bonafide work carried out by them under our guidance and supervision during the year 2022-23.

The results embodied in this thesis have not been submitted to any other University or Institute for the award of any degree or diploma.

|  |  |
| --- | --- |
| **Raheem unnisa**  (Assistant Professor)  INTERNAL GUIDE          **Dr. K. Srujan Raju**  HOD | **Dr. A. Raji Reddy**  DIRECTOR  **EXTERNAL EXAMINER** |
| **Submitted for viva voice Examination held on** |  |

### ACKNOWLEDGEMENT

Apart from the efforts of us, the success of any project depends largely on the encouragement and guidelines of many others. We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project.

We take this opportunity to express my profound gratitude and deep regard to my guide **Raheem unnisa,** Assistant Professor for her exemplary guidance, monitoring and constant encouragement throughout the project work. The blessing, help and guidance given by her shall carry us a long way in the journey of life on which we are about to embark.

We also take this opportunity to express a deep sense of gratitude to the Project Review Committee (PRC) **Dr. Punyaban Patel, Ms. Shilpa, Dr. M . Subha Mastan Rao & J. Narasimharao** for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **Dr. K. Srujan Raju,** Head of the Department of Computer Science and Engineering**,Dr.Ashuthosh Saxena,Dean R&D**, and **Dr.D T V Dharmajee Rao,**Dean

Academics for providing encouragement and support for completing this project successfully.

We are obliged to **Dr. A. Raji Reddy,** Director for being cooperative throughout the course of this project. We also express our sincere gratitude to Sri. **Ch. Gopal Reddy,** Chairman for providing excellent infrastructure and a nice atmosphere throughout the course of this project.

The guidance and support received from all the members of **CMR Technical Campus** who contributed to the completion of the project. We are grateful for their constant support and help.

Finally, we would like to take this opportunity to thank our family for their constant encouragement, without which this assignment would not be completed. We sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project.

|  |  |
| --- | --- |
| **D.SUMANTH** | **(197R1A05K6)** |
| **G.VIDYADHARI** | **(197R1A05L2)** |
| **E.SHIVANI** | **(197R1A05K7)** |

### ABSTRACT

Evidence management is crucial in the field of forensic science. Evidences obtained from a crime scene are important in solving the case and delivering justice to the parties involved. Hence, protecting these evidences from any form of alteration is of utmost important. Chain of Custody is the process which maintains the integrity of evidence. Inability to maintain the chain of custody will make the evidence inadmissible in court, eventually leading to the case dismissal. Digitalization of forensic evidence management system is a need of time as it is an environment friendly model. Blockchains are digitally distributed ledgers of transactions signed cryptographically in chronological order that are sorted into blocks and is completely open to anyone in the blockchain network. Hyperledger Fabric is a consortium blockchain framework created by the Linux foundation and is mainly used for enterprise use. Based on the concept of Hyperledger Fabric, present study aimed to create a framework and further propose an algorithm to implement Blockchain Technology to digitalize forensic evidence management system and maintain Chain of Custody.

i

## LIST OF FIGURES

#### FIGURE NO FIGURE NAME PAGE NO

**Figure 4.1** Project architecture for Implementation of Blockchain  **10**

Technology in Forensic Evidence Management.

**Figure 4.2** Use case diagram for Implementation of Blockchain  **12**

Technology in Forensic Evidence Management.

**Figure 4.3** Class diagram for Implementation of blockchain  **13**

technology in forensic Evidence Management.

**Figure 4.4** Sequence diagram for Implementation of Blockchain  **14**

Technology in Forensic Evidence Management.

**Figure 4.5** Activity diagram for Implementation of Blockchain  **15**

Technology in Forensic Evidence Management.

ii

[LIST OF RESULTS](#_Toc47350)

[Screenshot 6.2 Login page 21](#_Toc47351)

[Screenshot 6.3 Home page 22](#_Toc47352)

[Screenshot 6.4 Adding the evidence 23](#_Toc47353)

[Screenshot 6.5 Saving the evidence 24](#_Toc47354)

[Screenshot 6.6 Fetching the evidence 25](#_Toc47355)

**SCREENSHOT NO SCREENSHOT NAME PAGE NO**

**Screenshot 6.1 Dash board 20**

iii

### TABLE OF CONTENTS

**ABSTRACT** i

**LIST OF FIGURES** ii

**LIST OF RESULTS** iii

**1.INTRODUCTION** 1

1.1 PROJRCT SCOPE1

1.2 PROJECT PURPOSE1

1.3 PROJECT FEATURES2

**2.LITERATURE SURVEY**

2.1 BCOC:A BLOCKCHAIN-BASED CHAIN OF CUSTODY FOR 2

EVIDENCE MANAGEMENT IN DIGITAL FORENSICS.

2.2 DIGITAL FORENSICS USING BLOCKCHAIN.2

2.3 AUTHENTICATION & ENCRYPTION BASED SECURITY 3

SERVICES IN BLOCKCHAIN TECHNOLOGY.

2.4 A DECENTRALIZED DIGITAL IDENTITY ARCHITECTURE.3

2.5 FORENSIC-CHAIN: ETHEREUM BLOCKCHAIN BASED 4

DIGITAL FORENSICS CHAIN OF CUSTODY.

**3.SYSTEM ANALYSIS** 5

3.1 PROBLEM DEFINITION5

3.2 EXISTING SYSTEM5

3.2.1 DISADVANTAGES OF THE EXISTING SYSTEM5

3.3 PROPOSED SYSTEM6

3.3.1 ADVANTAGES OF PROPOSED SYSTEM6

3.4 FEASIBILITY STUDY6

3.4.1 ECONOMIC FEASIBILITY7

3.4.2 TECHNICAL FEASIBILITY7

3.4.3 BEHAVIRAL FEASIBILITY7

iv

3.5 HARDWARE & SOFTWARE REQUIREMENTS 8

3.5.1 HARDWARE REQUIREMENTS 8

3.5.2 SOFTWARE REQUIREMENTS 8

3.6 FUNCTIONAL REQUIREMENTS 8

3.7 NON FUNCTIONAL REQUIREMENTS 9

1. **ARCHITECTURE** 10
   1. PROJECT ARCHITECTURE 10
   2. DESCRIPTION 10
   3. MODULES 11
   4. USE CASE DIAGRAM 12
   5. CLASS DIAGRAM 13
   6. SEQUENCE DIAGRAM 14
   7. ACTIVITY DIAGRAM 15
2. **IMPLEMENTATION** 16
   1. SAMPLE CODE 16
3. **RESULTS** 20
4. **TESTING** 26
   1. INTRODUCTION TO TESTING 26
   2. TYPES OF TESTING 26
      1. UNIT TESTING 26
      2. INTEGRATION TESTING 26
      3. FUNCTIONAL TESTING 27
   3. TEST CASES 28
      1. CLASSIFICATION 28

**8.CONCLUSION AND FUTURE SCOPE** 29

* 1. PROJECT CONCLUSION 29
  2. FUTURE SCOPE 29

v

#### 9. BIBLIOGRAPHY 30

##### 9.1 REFERENCES 30

###### 9.2 GIT HUB LINK 31

**10.PAPER PUBLICATION 11.CERTIFICATION**

vi

**1.INTRODUCTION**

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

**1.INTRODUCTION**

### 1.1 PROJECT SCOPE

In propose paper to store crime forensic data author is suggesting to use Blockchain technology due to its inbuilt support for tamper proof. Crime forensic evidences plays a vital role to identify correct culprit and this evidences data must be tamper proof. Existing technique were maintaining evidences data either manually or recording in centralized server.

#### 1.2 PROJECT PURPOSE

Now a days all organizations are shifting their business data to Blockchain as its support Tamper proof and decentralized (data saved at multiple nodes or servers) data storage which means no body can alter data saved on Blockchain due to its data encryption and hash code technique. Blockchain store each data as block of transaction and associate each transaction with hash code and before storing any new block hash code of previous blocks will be verified and if no data alter then hash code verification will be successful and new block will be added and if verification failed then node will be consider as attacked.

#### 1.3 PROJECT FEATURES

The main features of the project is manual recording is a tedious task and can be alter and recording in centralized can also be hack by attacker and can alter data.To overcome from above problems author of this paper is using Blockchain to record forensic evidences. Blockchain provides following facilities.

1. Records cannot be tamper.
2. Each record will get verified and new records will be stored linking with its hashcode as PROOF of WORK.
3. Each block will be stored in encrypted format.
4. Inbuilt support for public and private key generation.

Two types of Blockchain are available as permission less (public Blockchain) and permissioned (private Blockchain). In this project we are using permissioned less Blockchain tool called Ethereum.

CMRTC 1

**2.LITERATURE SURVEY**

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### 2.LITERATURE SURVEY

**2.1 BCoC: A Blockchain-based chain of custody For Evidence Management in Digital Forensics.**

**AUTHORS:**  Silvia Bonomi, Marco Casini, Claudio Ciccotelli

**ABSTRACT:** One of the main issues in digital forensics is the management of evidences. From the time of evidence collection until the time of their exploitation in a legal court, evidences may be accessed by multiple parties involved in the investigation that take temporary their ownership. This process, called Chain of Custody (CoC), must ensure that evidences are not altered during the investigation, despite multiple entities owned them, in order to be admissible in a legal court. Currently digital evidences CoC is managed entirely manually with entities involved in the chain required to fill in documents accompanying the evidence. In this paper, we propose a Blockchainbased Chain of Custody (B-CoC) to dematerialize the CoC process guaranteeing auditable integrity of the collected evidences and traceability of owners. We developed a prototype of B-CoC based on Ethereum and we evaluated its performance.

**2.2 Digital Forensics using Blockchain.**

**AUTHORS:**  Dr.S. Harihara Gopalan, S. Akila Suba, C. Ashmithashree,A. Gayathri, V. Jebin Andrews.

**ABSTRACT:** On considering the integrity of electronic evidence, in particular,we can see that such evidence needs to be protected from a number of undesirable outcomes namely, alteration or destruction. We need to guard against these events and others when trying to maintain system integrity and preserve the purity of evidence so that it could be acceptable in the court. Chain of Custody is nothing but the consecutive documentation of records. The Chain of Custody has all the necessary steps that a crime investigator must follow to make sure whether the information is honest. The Chain of Custody is significant because it cannot be proven that evidence was not altered during the time between collection and its usage in court. Then the collected evidence is not credible. Blockchain technology,a decentralized network currently used by Bitcoins and other Cryptocurrency networks, helps provide a secure.

CMRTC 2

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

database with the help of hashing the data and storing it in blocks.We propose to implement blockchain technology for the process of Chain of Custody, which helps in tracking the people who access the data and assist in assuring the credibility of the data provided during the time of submission in court.

**2.3 Authentication & Encryption Based Security Services in Blockchain Technology.**

**AUTHORS:**  Varshney, T., Sharma, N., Kaushik, I., Bhushan, B.

**ABSTRACT:** Without any involvement of third party, block chain has shown tremendous potential in establishing secure links with IoT.This technology can be widely used without using any centralized authority. By combining both the technologies throughput of the system can be enhanced. Due to its various applications it is being widely used in almost every field which makes it vulnerable to various attacks. In this paper, blockchain architecture along with its key properties has been discussed. Later part of paper comprises of various security principles such as confidentiality, integrity and availability, various attacks on network along with its countermeasures.

**2.4 A Decentralized Digital Identity Architecture.**

**AUTHORS:**  Goodell, G., & Aste, T.

**ABSTRACT:** Current architectures to validate, certify, and manage identity are based on centralized ,top-down approaches that rely on trusted authorities and third-party operators. We approach the problem of digital identity starting from a human rights perspective, with a primary focus on identity systems in the developed world. We assert that individual persons must be allowed to manage their personal information in a multitude of different ways in different contexts and that to do so, each individual must be able to create multiple unrelated identities. Therefore, we first define a set of fundamental constraints that digital identity systems must satisfy to preserve and promote privacy as required for individual autonomy. With these constraints in mind, we then propose a decentralized,standards-based approach, using a combination of distributed ledger technology and thoughtful regulation, to facilitate many-to-many relationships among providers of key services. Our proposal for digital identity

CMRTC 3

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

differs from others in its approach to trust in that we do not seek to bind credentials to each other or to a mutually trusted authority to achieve strong non-transferability. Because the system does not implicitly encourage its users to maintain a single aggregated identity that can potentially be constrained or reconstructed against their interests, individuals and organizations are free to embrace the system and share in its benefits.

**2.5**  **Forensic-chain: Ethereum blockchain based digital forensics chain of custody.**

**AUTHORS:**  Lone, A. H., & Mir, R. N.

**ABSTRACT:** Digital evidence plays an important role in cyber crime investigation, as it is used to link persons with criminal activities. Thus it is ofextreme importance to guarantee integrity, authenticity, and auditability of digital evidence as it moves along different levels of hierarchy in chain of custody during cyber crime investigation. Blockchain technology’s capability of enabling comprehensive view of transactions (events/actions) back to origination provides enormous promise for the forensic community. In this research we proposed to use a blockchain that can be leveraged for forensic applications in particular bringing integrity and tamper resistance to digital forensics chain of custody.

CMRTC 4

**3.SYSTEM ANALYSIS**

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

**3.SYSTEM ANALYSIS**

### SYSTEM ANALYSIS

System Analysis is the important phase in the system development process. The System is studied to the minute details and analyzed. The system analyst plays an important role of an interrogator and dwells deep into the working of the present system. In analysis, a detailed study of these operations performed by the system and their relationships within and outside the system is done. A key question considered here is, “what must be done to solve the problem?” The system is viewed as a whole and the inputs to the system are identified. Once analysis is completed the analyst has a firm understanding of what is to be done.

### 3.1 PROBLEM DEFINITION

Now a days all organizations are shifting their business data to Blockchain as its support Tamper proof and decentralized (data saved at multiple nodes or servers) data storage which means no body can alter data saved on Blockchain due to its data encryption and hash code technique. Blockchain store each data as block of transaction and associate each transaction with hash code and before storing any new block hash code of previous blocks will be verified and if no data alter then hash code verification will be successful and new block will be added and if verification failed then node will be consider as attacked.

### 3.2 EXISTING SYSTEM

Evidence management is critical in the field of forensic science. Main concerns in forensic investigation are the management of evidences and their documentation. Starting from the point of collection till the final judgment from the court of law, maintaining the integrity of the evidence is of utmost importance.Evidences obtained from a crime scene are important in solving the case and delivering justice to the parties involved.

#### 3.2.1 DISADVANTAGES OF EXISTING SYSTEM

• Problem in solving the case and delivering justice to the parties involved.

CMRTC 5

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### 3.3 PROPOSED SYSTEM

Chain of Custody is the process which maintains the integrity of evidence. Inability to maintain the chain of custody will make the evidence inadmissible in court, eventually leading to the case dismissal. Digitalization of forensic evidence management system is a need of time as it is an environment friendly model. Blockchains are digitally distributed ledgers of transactions signed cryptographically in chronological order that are sorted into blocks and is completely open to anyone in the blockchain network. Hyperledger Fabric is a consortium blockchain framework created by the Linux foundation and is mainly used for enterprise use. Based on the concept of Hyperledger Fabric, present study aimed to create a framework and further propose an algorithm to implement.

#### 3.3.1 ADVANTAGES OF PROPOSED SYSTEM

* Blockchain technology to digitalize forensic evidence management system and maintain chain of custody.
* Hence,protecting these evidences from any form of alteration of utmost important.

### 3.4 FEASIBILITY STUDY

The feasibility of the project is analysed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

* Economical Feasibility
* Technical Feasibility
* Social Feasibility

CMRTC 6

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

#### 3.4.1 ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

The following are some of the important financial questions asked during preliminary investigation:

* The costs conduct a full system investigation.
* The cost of the hardware and software.
* The benefits in the form of reduced costs or fewer costly errors.

Since the system is developed as part of project work, there is no manual cost to spend for the proposed system. Also all the resources are already available, it give an indication that the system is economically possible for development.

#### 3.4.2 TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

#### 3.4.3 BEHAVIORAL FEASIBILITY

This includes the following questions:

* Is there sufficient support for the users?
* Will the proposed system cause harm?

CMRTC 7

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### 3.5 HARDWARE & SOFTWARE REQUIREMENTS

#### 3.5.1 HARDWARE REQUIREMENTS

Minimum hardware requirements are very dependent on the particular software being developed by a given Enthought Python / Canopy / VS Code user. Applications that need to store large arrays/objects in memory will require more RAM, whereas applications that need to perform numerous calculations or tasks more quickly will require a faster processor.

• Operating system : windows, linux

|  |  |  |  |
| --- | --- | --- | --- |
| • | Processor |  | : minimum intel i3 |
| • | Ram |  | : minimum 4 gb |
| • | Hard disk |  | : minimum 250gb |

#### 3.5.2 SOFTWARE REQUIREMENTS

The functional requirements or the overall description documents include the product perspective and features, operating system and operating environment, graphics requirements, design constraints and user documentation.

The appropriation of requirements and implementation constraints gives the general overview of the project in regards to what the areas of strength and deficit are and how to tackle them.

* Python idel 3.7 version (or)
* Anaconda 3.7 ( or)
* Jupiter (or)
* Google colab

### 3.6 FUNCITONAL REQUIREMENTS

1. Add Evidences to Blockchain.
2. Fetch Evidences from Blockchain.

CMRTC 8

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

#### 3.7 NON-FUNCTIONAL REQUIREMENT (NFR)

specifies the quality attribute of a software system. They judge the software system based on Responsiveness, Usability, Security, Portability and other non-functional standards that are critical to the success of the software system. Example of nonfunctional requirement, *“*how fast does the website load*?”* Failing to meet non-functional requirements can result in systems that fail to satisfy user needs. Non- functional Requirements allows you to impose constraints or restrictions on the design of the system across the various agile backlogs. Example, the site should load in 3 seconds when the number of simultaneous users are > 10000. Description of nonfunctional requirements is just as critical as a functional requirement.

* Usability requirement
* Serviceability requirement
* Manageability requirement
* Recoverability requirement
* Security requirement
* Data Integrity requirement
* Capacity requirement
* Availability requirement
* Scalability requirement
* Interoperability requirement
* Reliability requirement
* Maintainability requirement
* Regulatory requirement
* Environmental requirement

CMRTC 9

**4.ARCHITECTURE**

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

**4.ARCHITECTURE**

### 4.1 PROJECT ARCHITECTURE

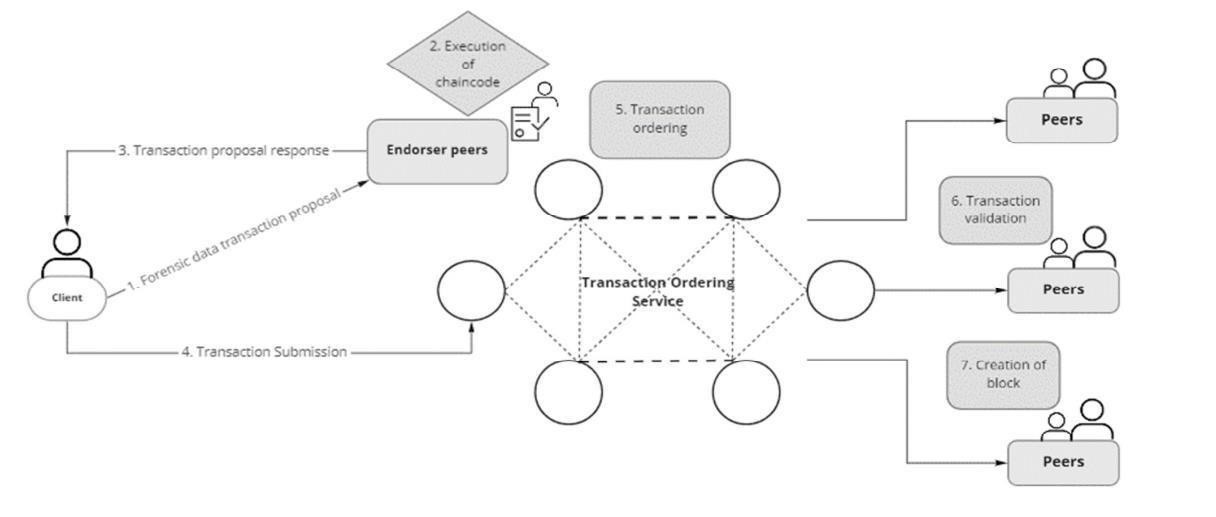


Figure 4.1: Project architecture for Implementation of Blockchain Technology in Forensic Evidence Management.

### 4.2 DESCRIPTION

Evidence management is critical in the field of forensic science. Main concerns in forensic investigation are the management of evidences and their documentation. Starting from the point of collection till the final judgment from the court of law, maintaining the integrity of the evidence is of utmost importance. Chain of Custody (CoC) is the documentation of the evidences handled throughout the investigation in chronological order. It is essential to maintain the CoC for the evidence to be accepted in court.

* The evidence should be able to relate to the crime and act as a proof.
* Each and every entity that has come in contact with the evidence must be able to verify the process.
* No unauthorized person is allowed to deal with the evidence, to avoid any sort of alteration or manipulation of the evidence.

CMRTC 10

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### 4.3 MODULES

* To implement this project we have designed following modules
* Admin Login: using this module police peoples can login to application by using username as ‘admin’ and password as ‘admin’.
* Add Evidences to Blockchain: using this module police peoples can add evidences to Blockchain Ethereum tool
* Fetch Evidences from Blockchain: using this module police peoples can extract all evidences stored in Blockchain and valid police peoples only can extract evidences from Blockchain**.**

CMRTC 11

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### 4.4 USE CASE DIAGRAM

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

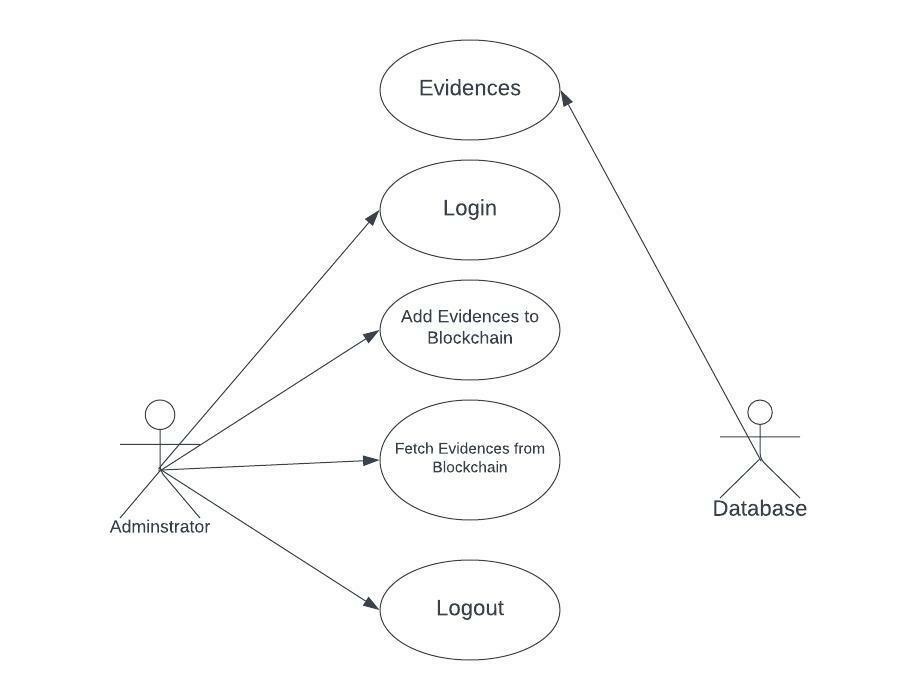


Figure 4.2: use case diagram for Implementation of Blockchain Technology in Forensic Evidence Management.

CMRTC

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### 4.5 CLASS DIAGRAM

The class diagram is used to refine the use case diagram and define a detailed design of the system. The class diagram classifies the actors defined in the use case diagram into a set of interrelated classes. The relationship or association between the classes can be either an "is-a" or "has-a" relationship. Each class in the class diagram may be capable of providing certain functionalities. These functionalities provided by the class are termed "methods" of the class.

Apart from this, each class may have certain "attributes" that uniquely identify the class.

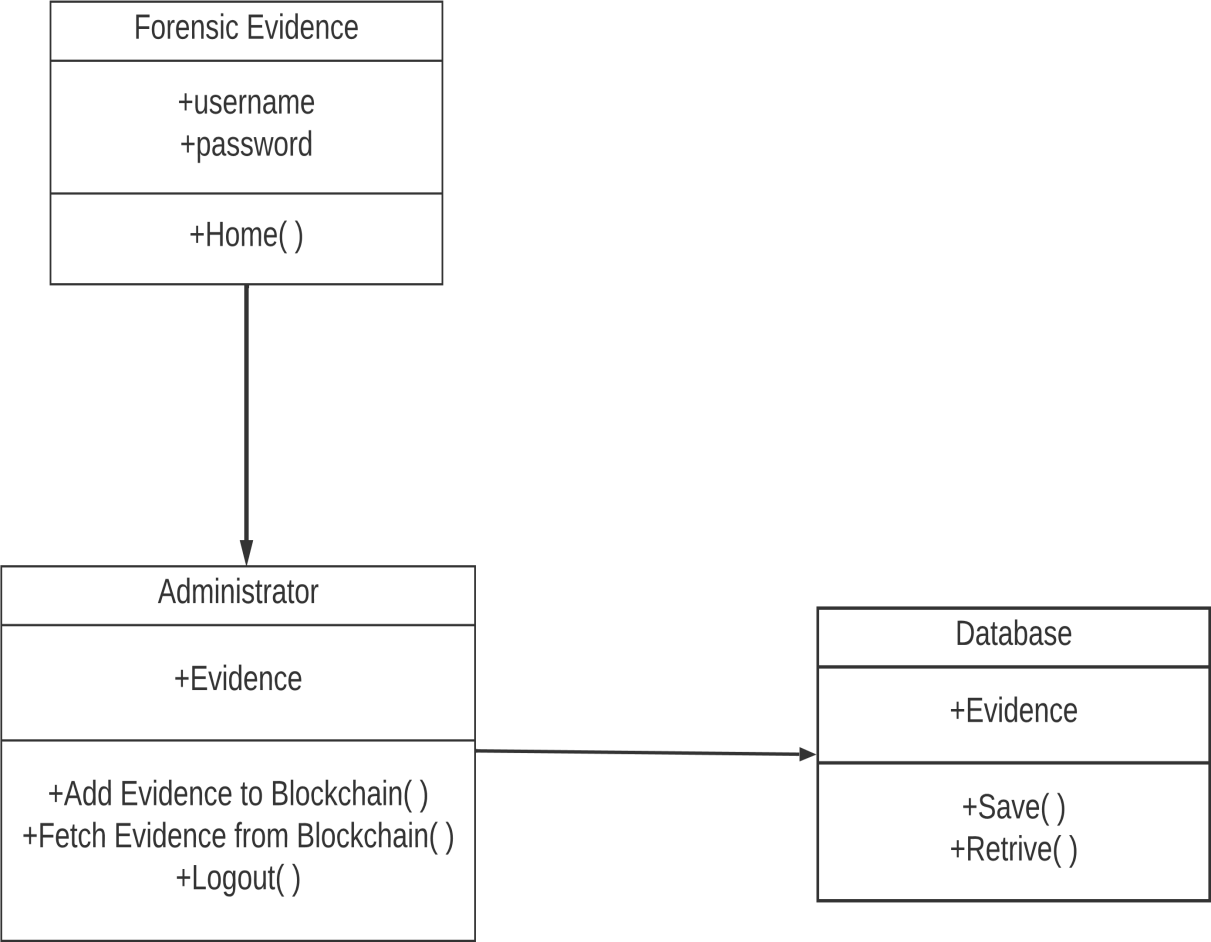


Figure 4.3: class diagram for implementation of blockchain technology in forensic Evidence Management.

CMRTC

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### 4.6 SEQUENCE DIAGRAM

A sequence diagram represents the interaction between different objects in the system. The important aspect of a sequence diagram is that it is time-ordered. This means that the exact sequence of the interactions between the objects is represented step by step. Different objects in the sequence diagram interact with each other by passing "messages".

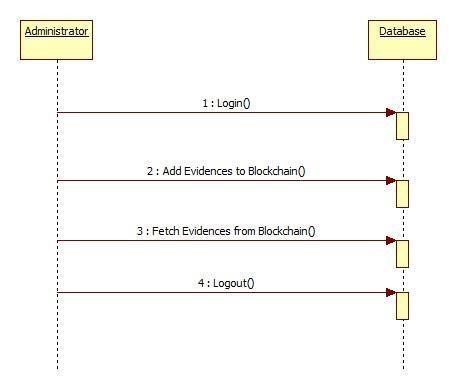
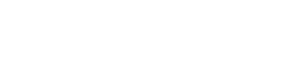


Figure 4.4: sequence diagram for Implementation of Blockchain Technology in Forensic Evidence Management

CMRTC

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT **4.7 ACTIVITY DIAGRAM**

The process flows in the system are captured in the activity diagram. Similar to a state diagram, an activity diagram also consists of activities, actions, transitions, initial and final states, and guard conditions.

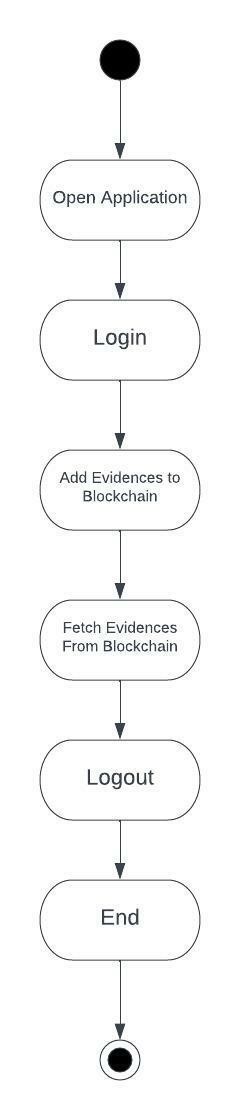


Figure 4.5: Activity diagram for Implementation of Blockchain Technology in Forensic Evidence Management.

CMRTC

**5.IMPLEMENTATION**

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

**5.IMPLEMENTATION**

### 5.1 SAMPLE CODE

from django.shortcuts import render from django.template import RequestContext from django.contrib import messages from django.http import HttpResponse from django.conf import settings from datetime import date import json

from web3 import Web3, HTTPProvider

global details

def readDetails(): global details

blockchain\_address = 'http://127.0.0.1:9545' #Blokchain connection IP web3 = Web3(HTTPProvider(blockchain\_address)) web3.eth.defaultAccount = web3.eth.accounts[0]

compiled\_contract\_path = 'ForensicEvidenceContract.json' #forensic contract code

deployed\_contract\_address = '0xdbdeB1d0fe02FBE6a05f5C2194e187D3A92F2229' #hash address to access forensiccontract with open(compiled\_contract\_path) as file:

contract\_json = json.load(file) # load contract info as JSON

contract\_abi = contract\_json['abi'] # fetch contract's abi - necessary to call its functions file.close()

contract = web3.eth.contract(address=deployed\_contract\_address, abi=contract\_abi) #now calling contract to access data

details = contract.functions.getData().call() if len(details) > 0: if 'empty' in details:

CMRTC 16

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

details = details[5:len(details)] def saveDataBlockChain(currentData): global details global contract

blockchain\_address = 'http://127.0.0.1:9545' web3 = Web3(HTTPProvider(blockchain\_address)) web3.eth.defaultAccount = web3.eth.accounts[0] compiled\_contract\_path = 'ForensicEvidenceContract.json'

deployed\_contract\_address = '0xdbdeB1d0fe02FBE6a05f5C2194e187D3A92F2229' with open(compiled\_contract\_path) as file:

contract\_json = json.load(file) # load contract info as JSON

contract\_abi = contract\_json['abi'] # fetch contract's abi - necessary to call its functions file.close()

contract = web3.eth.contract(address=deployed\_contract\_address, abi=contract\_abi) readDetails() details+=currentData

msg = contract.functions.setEvidenceDetails(details).transact() tx\_receipt = web3.eth.waitForTransactionReceipt(msg)

def index(request):

if request.method == 'GET':

return render(request, 'index.html', {})

def Admin(request):

if request.method == 'GET':

return render(request, 'Admin.html', {})

def AddEvidence(request): if request.method == 'GET':

return render(request, 'AddEvidence.html', {})

CMRTC 17

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

def AdminLogin(request):

if request.method == 'POST':

username = request.POST.get('t1', False) password = request.POST.get('t2', False) if username == 'admin' and password == 'admin': context= {'data':'welcome '+username} return render(request, 'AdminScreen.html', context) else:

context= {'data':'login failed'}

return render(request, 'Admin.html', context)

def ViewEvidence(request): if request.method == 'GET':

global details readDetails() print("p det "+details) arr = details.split("\n") output = ''

font = "<font size=3 color=black>" for i in range(len(arr)-1): array = arr[i].split("$");

output+="<tr><td>"+font+array[0]+"</td>" output+="<td>"+font+array[1]+"</td>" output+="<td>"+font+array[2]+"</td>" output+="<td>"+font+array[3]+"</td>" output+="<td>"+font+array[4]+"</td>" output+="<td>"+font+array[5]+"</td>" output+="<td>"+font+array[6]+"</td>" context= {'data':output}

CMRTC 18

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

return render(request, 'ViewEvidence.html', context)

def AddEvidenceAction(request): if request.method == 'POST':

rid = request.POST.get('t1', False) crime\_type = request.POST.get('t2', False) desc = request.POST.get('t3', False) evidence = request.POST.get('t4', False) area = request.POST.get('t5', False) witness = request.POST.get('t6', False) today = date.today()

data = rid+"$"+crime\_type+"$"+desc+"$"+evidence+"$"+area+"$"+witness+"$"+str(today)+"\n" saveDataBlockChain(data)

context= {'data':'Evidence details saved in Blockchain'} return render(request, 'AddEvidence.html', context)

CMRTC 19

**6.RESULTS**

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### Dash board

In screen click on ‘Administrator’ link to get below login screen.



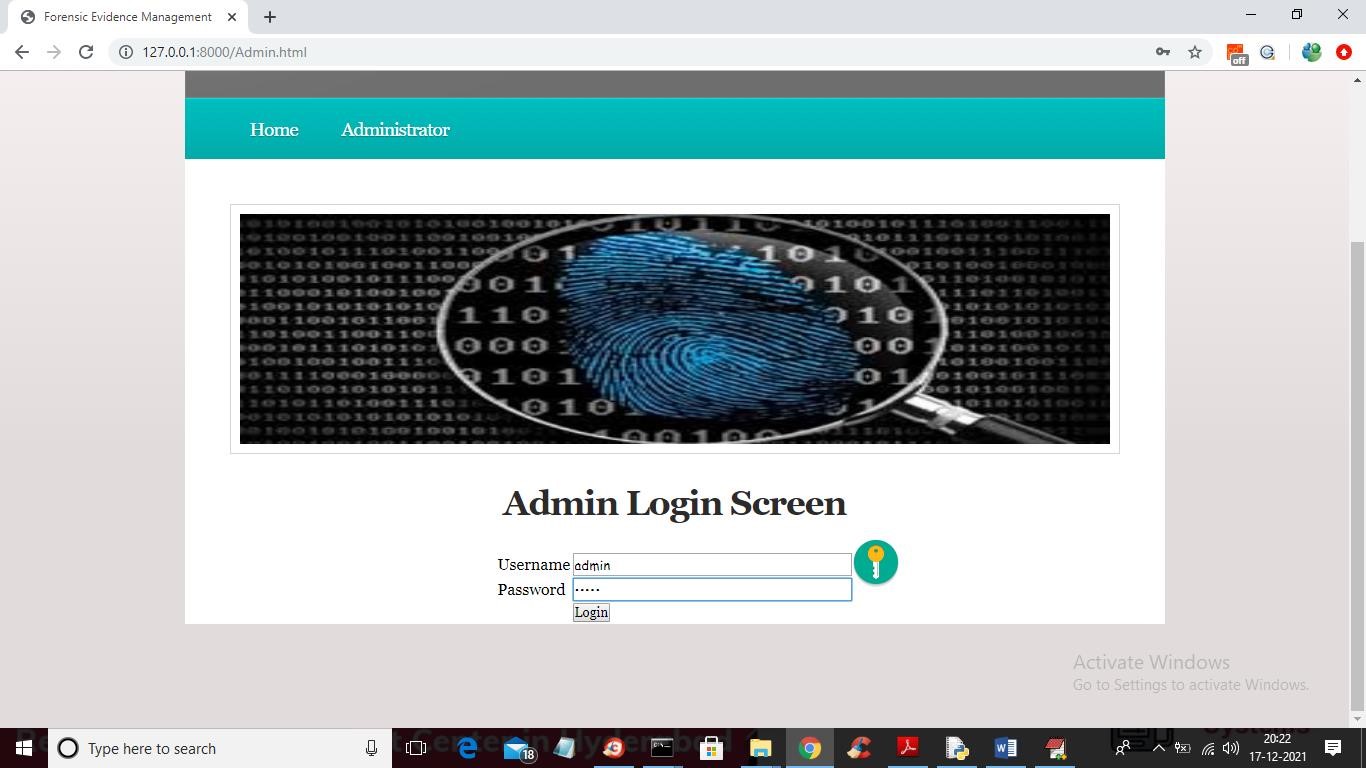
Screenshot 6.1: Dash board

CMRTC 20

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### Login page

In above screen enter username as ‘admin’ and password as ‘admin’ and then press ‘Login’ button to get below screen.

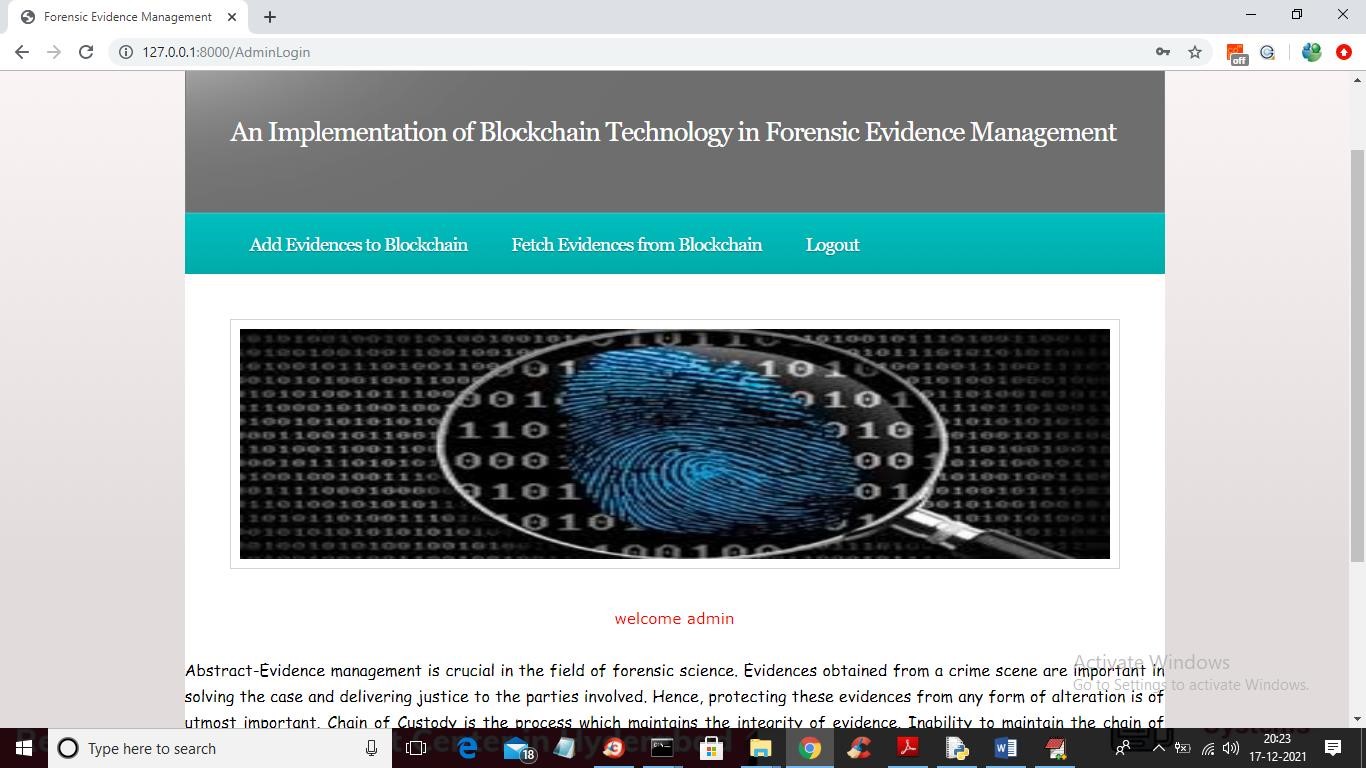


# Screenshot 6.2: Login page

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### Home page

In above screen now admin can click on ‘Add Evidences to Blockchain’ link to get below screen and to record evidences.



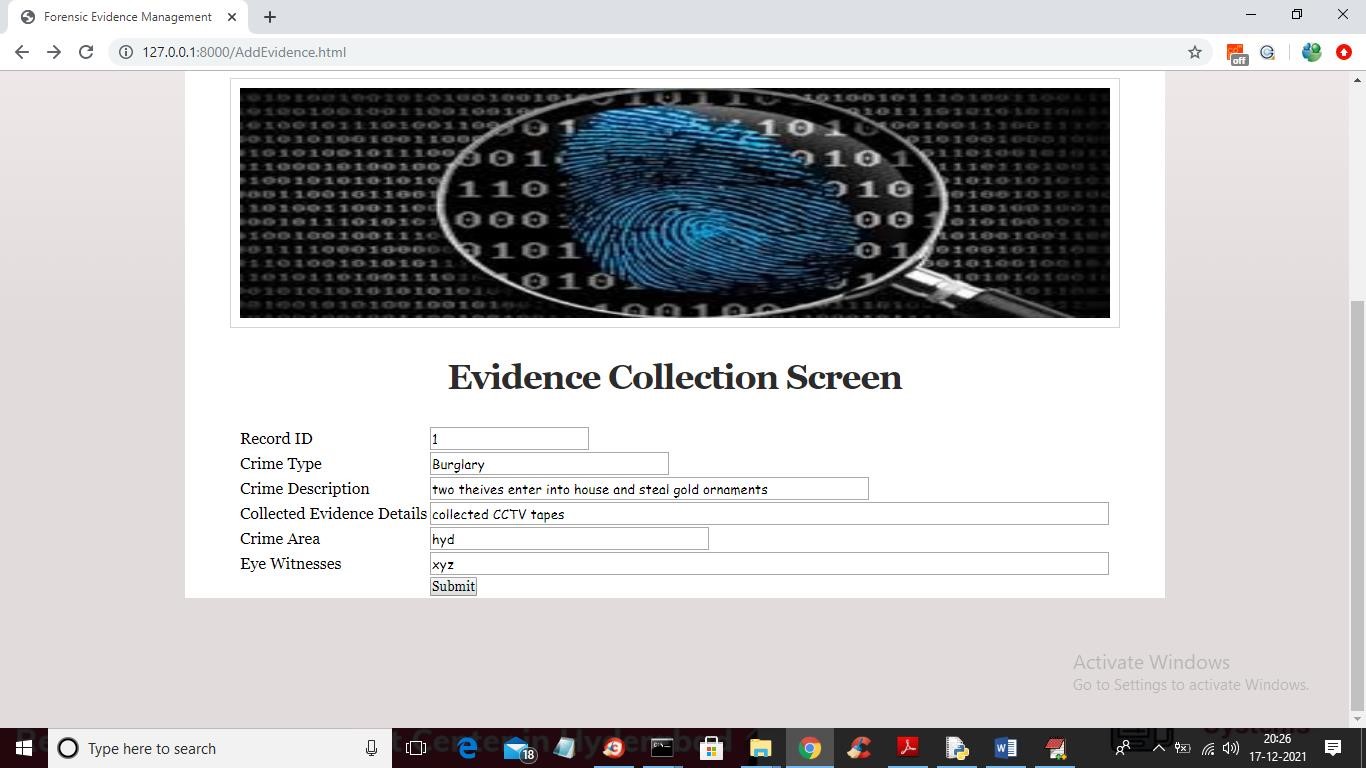
# Screenshot 6.3: Home page

CMRTC 22

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### Adding evidence

In above screen police personnel or admin may record all crime and evidences details and then click on ‘Submit’ button to get below screen.

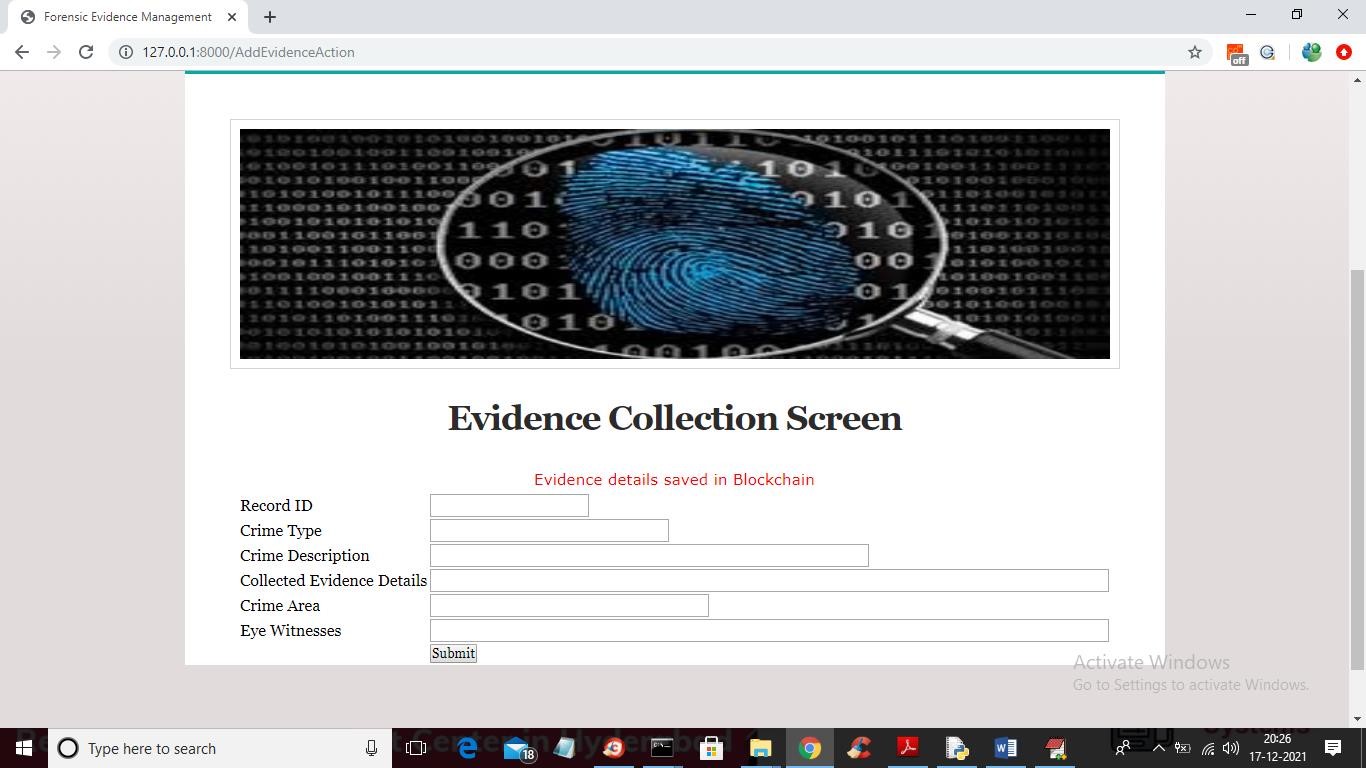


# Screenshot 6.4: Adding evidence

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### Saving the evidence

In above screen in red colour text we can see data saved in Blockchain and now click on ‘Fetch Evidences from Blockchain’ link to get all details.



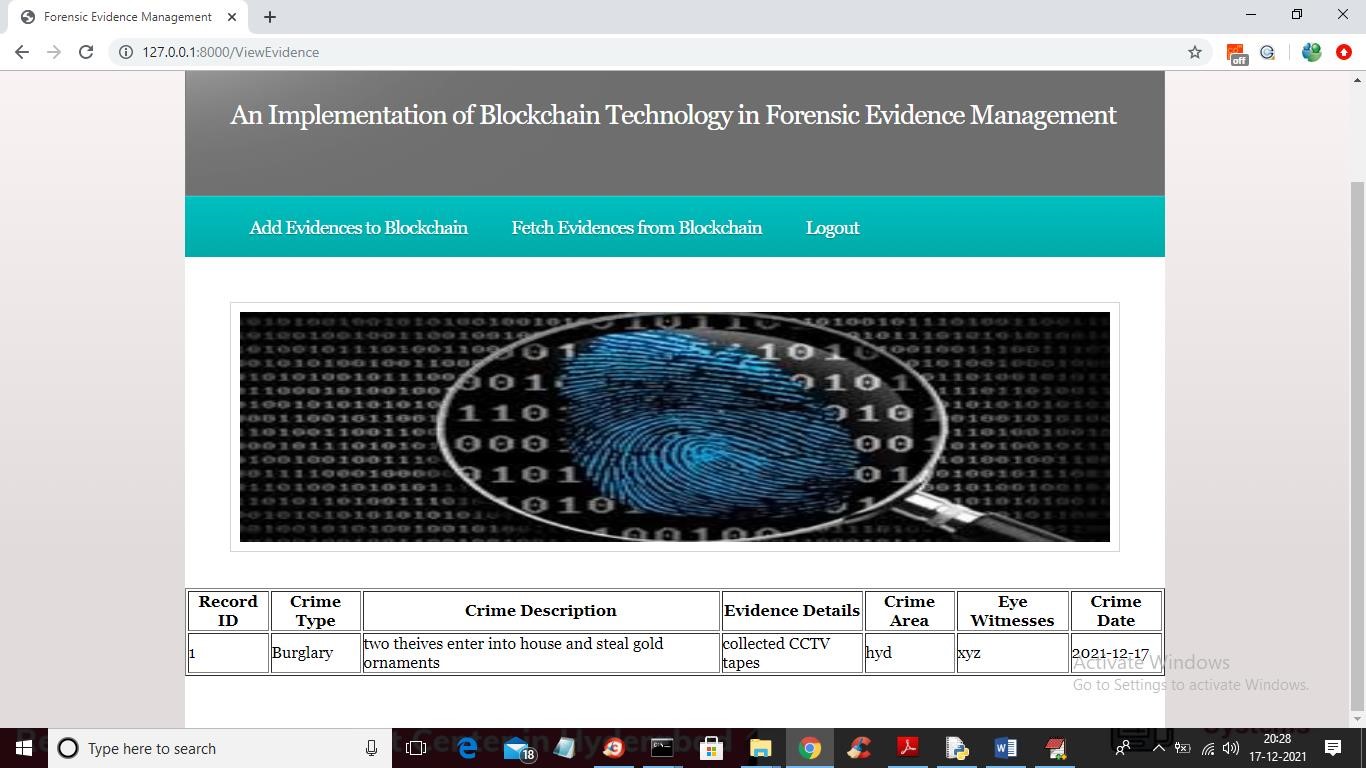
# Screenshot 6.5: Saving the evidence

CMRTC 24

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### Fetching the evidence

In above screen admin can fetch all evidences details from Blockchain and can be used in court for correct judgement. Similarly admin can add N crime details in the application and record in Blockchain.



# Screenshot 6.6: Fetching the evidence

**7.TESTING**

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

**7.TESTING**

### 7.1 INTRODUCTION TO TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

### 7.2 TYPES OF TESTING

#### 7.2.1 UNIT TESTING

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

#### 7.2.2 INTEGRATION TESTING

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

CMRTC 26

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

#### 7.2.3 FUNCTIONAL TEST

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised.

Systems/Procedures: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

CMRTC 27

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### 7.3 TEST CASES

#### 7.3.1 CLASSIFICATION

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test case ID** | **Test case name** | **Purpose** | **Input** | **Output** |
| **1.** | **Sign up** | To enter the evidence portal. | Enter the user name and password | User name and password is invalid |
| **2.** | **Sign up** | To enter the evidence portal. | Enter the user name and password. | Loged in to the home page. |
| **3.** | **Login** | Adding the evidences | Give the evidences | Evidences has added to blockchain |
| **4.** | **Login** | Fetching the evidences | Enter  the ID  of record | Evidences has displayed on screen |
| **5.** | **Login** | Fetching the evidence | Enter the user name and password | User name and password are  invalid |

CMRTC 28

**8.CONCLUSION**

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### 8.CONCLUSION AND FUTURE SCOPE 8.1 PROJECT CONCLUSION

From the time evidence is collected from the crime scene until court of law make the judgment, maintaining the integrity of the evidence is of most importance. Maintaining the chain of custody is important as it can prove if the evidence is tampered or not during the collection and analysis process. Implementation of Blockchain technology to digitalize chain of custody will ensure security, authenticity and integrity of the forensic data transactions. Application of blockchain will not only make it environment friendly but also increase security with the help of encryption which can be accessed remotely by authorized personnel. We intend to work on an algorithm that executes the chain of custody process utilizing blockchain technology, specifically Hyperledger Fabric.

### 8.2FUTURE SCOPE

Furthermore, we can couple blockchain technology with artificial intelligence/ machine learning which will help in forensic investigation.

CMRTC 29

**9.BIBLIOGRAPHY**

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

### 9.BIBLIOGRAPHY 9.1 REFERENCES

1. Bonomi, S., Casini, M., & Ciccotelli, C. (2018). BCoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics. arXivpreprint arXiv:1807.10359.
2. Gopalan, S.H., Suba, S.A., Ashmithashree, C., Gayathri, A., Andrews, V.J. (2019). Digital

Forensics using Blockchain. International Journal of Recent Technology and

Engineering, 8(2S11), 182–184. <https://doi.org/10.35940/ijrte.b1030.0982s1119>

1. Bou Abdo, J., El Sibai, R., & Demerjian, J. (2020). Permissionless proofofreputation‐X: A hybrid reputation‐based consensus algorithm for permissionless blockchains. Transactions on Emerging Telecommunications Technologies, 32(1), 1. <https://doi.org/10.1002/ett.4148>
2. Varshney, T., Sharma, N., Kaushik, I., Bhushan, B. (2019). Authentication &

Encryption Based Security Services in Blockchain Technology. International

Conference on Computing, Communication, and Intelligent Systems (ICCCIS), India,

63-68. doi: 10.1109/ICCCIS48478.2019.8974500

1. Kahate, A. (2003). Cryptography and Network Security. McGraw-Hill Education.
2. Dominique Guegan. Public Blockchain versus Private blockchain. 2017. ⟨halshs-

01524440⟩

1. BlockchainTechnologyOverview.(2018,October).
2. Castor, A. (2017). A short guide to blockchain consensus protocols. Coindesk.

<https://www.coindesk.com/short-guide-blockchainconsensus-protocols>

1. Cong T. Nguyen, Dinh T. Hoang, Diep N. Nguyen, Dusit Niyato, Huynh Tuong

Nhuyen & Eryk Dutkiewicz. (2019).

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnum ber=8746079

[10]Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., et al. (2018). Hyperledger fabric.

Proceedings of the Thirteenth EuroSys Conference, 1–15. <https://doi.org/10.1145/3190508.3190538>

CMRTC 30

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC EVIDENCE MANAGEMENT

[11]Goodell, G., & Aste, T. (2019). A Decentralized Digital Identity Architecture. Frontiers in Blockchain, 2, 1. <https://doi.org/10.3389/fbloc.2019.00017>

### 9.2 GIT HUB LINK

https://github.com/197R1A05K7/Evidence-management-

CMRTC 31

**10. PAPER PUBLICATION**



**AN IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN**

**FORENSIC EVIDENCE MANAGEMENT**

**Edakula Shivani1, Gone Vidyadhari2, DondetiSumanth Reddy3, Raheem Unnisa4**

1B. Tech Student, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India, shivanireddyedakula@gmail.com

2B. Tech Student, Department of Computer Science and Engineering, CMR Technical Campus,

Hyderabad, Telangana, India, vidyadharigone@gmail.com

3B. Tech Student, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India, sumanthreddydondeti@gmail.com

4Assistant Professor, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India, raheemaswcet.17@gmail.com

**Abstract :** Evidence management is pivotal in the field of measurable science. To settle a case and deal with those capable, proof accumulated from the location of a crime is fundamental. Subsequently, shielding these confirmations from altering of any kind is fundamental. Chain of guardianship is the strategy for protecting the respectability of proof. The proof will be unacceptable in court in the event that the chain of authority isn't saved, and the case will be excused. Because of its harmless to the ecosystem nature, digitalizing measurable proof administration frameworks is a dire necessity. Blockchains are painstakingly circled records of cryptographically checked trades in consecutive solicitation that are arranged into blocks and are totally available to anybody in the blockchain network. The Hyperledger Texture consortium blockchain innovation was created by the Linux Establishment and is fundamentally used for business purposes. Measurable proof administration frameworks can be digitalized and Chain of Care safeguarded utilizing Blockchain Innovation, as per the ongoing review's system and calculation.

***Index Terms :*** *Blockchain, Hyper ledger, Forensic evidence*

*.*

**1. INTRODUCTION**

Evidence management is significant in the field of scientific science. In legal examination, the essential contemplations are proof dealing with and recording. From the time the proof is accumulated to the court's official choice, protecting its integrity is fundamental. The Chain of Custody (CoC) is the sequential documentation of the confirmations took care of during the examination. For the proof to be acknowledged by the court, keeping the CoC is fundamental. During the CoC cycle, various necessities should be met, including the accompanying:

Corruption and tampering with evidence must be avoided.

From the time it is accumulated until it is introduced in court, the development of the evidence during the examination should be perceptible.

The evidence should give confirmation and be relevant to the crime. The technique should be affirmed by each substance that has come into contact with the evidence.

No unauthorised person is permitted to handle the evidence in order to prevent any tampering or manipulation.

Digitalization of forensic evidence administration frameworks decreases costs, saves space, and is better for the climate. Evidence that can be used in court is acceptable due to the CoC's authenticity and legality. Blockchain technology can be used to keep them current. We can store multiple system data in a single network using blockchain technology, making them safe and accessible to customers. Utilizing technology can cut down on the amount of time required for paper examinations.

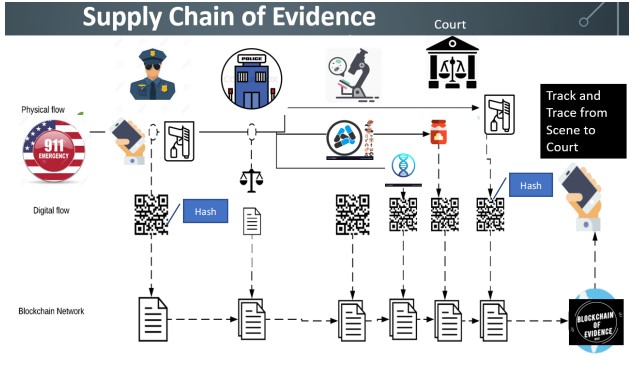


Fig 1 Example Figure

Since Blockchain supports tamper-proof and decentralized (data stored at multiple nodes or servers) data storage, which means that no one can modify data saved on Blockchain due to its data encryption and hash code approach, all businesses are now migrating their corporate data to Blockchain. Blockchain stores every exchange as a block of information and connects every exchange with a hashcode; prior to putting away any new block, the hashcode of past blocks is checked; The hashcode verification is successful if no data are altered, and the new block is added; The node is considered to be under attack if the verification fails.

The creator of a proposed study to store criminal legal information recommends utilizing Blockchain innovation attributable to its underlying capacity for sealed. The data of crime forensic evidence must be tamper-resistant because it is essential for determining the correct perpetrator. Previously, evidentiary data was either recorded on a centralized server or manually preserved.

Centralized recording can be hacked and data altered by an attacker, while manual recording is a timeconsuming task that can be altered.

The author of this study is recording forensic evidence using Blockchain to address the aforementioned issues. Blockchain provides the following services: 1. There is no way to change records.

1. Each record will be checked as PROOF OF WORK, and new records will be kept with their hashcode.
2. Each block will be saved and encrypted. 4. Both public and private key generation are supported.

Blockchain can be thought of in two ways: private Blockchain, which is permissioned, and public Blockchain, which is permissionless. We are utilizing Ethereum, a permissionless Blockchain technology, in this project.

**2. LITERATURE SURVEY**

**BCoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics.** The administration of proof is quite possibly of the main test in advanced legal sciences. From the time they are gathered until they are utilized in an official courtroom, different members in the examination can see the proof, and they take brief responsibility for. Despite the fact that various organizations control the proof, this strategy, known as Chain of Custody (CoC), should guarantee that it doesn't change during the examination for it to be acknowledged in a court. Computerized confirmations of CoC are presently totally constrained the hard way, and associations in the chain are expected to finish up going with documentation. To guarantee auditable proof honesty and proprietor recognizability while dematerializing the CoC cycle, we propose a Blockchain-based Chain of Custody (B-CoC) technique in this work. We tried the exhibition of an Ethereum-based B-CoC model.

**Digital Forensics using Blockchain.**

At the point when we center around the honesty of electronic proof specifically, we can see that it should be shielded from different unwanted results, such as altering or annihilation. We should be keeping watch for these and different situations while endeavoring to safeguard the immaculateness of proof and the trustworthiness of the framework for it to be acknowledged in court. The sequential recording of records is all that makes up the chain of custody. The Chain of Care contains each of the cycles that a criminal examiner should take to guarantee that the data is precise. Since it is difficult to demonstrate that proof was not changed during its assortment and use in court, the Chain of Custody (COC) is critical. Thus, the gathered proof isn't solid. By hashing and putting away information in blocks, blockchain innovation, a decentralized organization utilized by Bitcoin and other digital currency organizations, makes a protected data set. For the COC methodology, we suggest utilizing blockchain innovation since it assists keep with following of who approaches the information and guarantees that the data submitted to the court is exact.

**Authentication & Encryption Based Security Services in Blockchain Technology**

Block chain is a technique that is comprehensively material without the requirement for incorporated power and has shown huge commitment for making secure associations with IoT without the mediation of an outsider. By joining the two innovations, the framework's throughput could be gotten to the next level. It is widely used in almost every industry because of its many uses, making it vulnerable to a variety of threats. This study has looked at the important characteristics of the blockchain architecture. The remainder of the article discusses numerous network threats and responses as well as security concepts like confidentiality, integrity, and availability.

**A Decentralized Digital Identity Architecture.** Present day distinguishing proof frameworks depend on brought together, hierarchical frameworks that depend on respectable specialists and administrators from outsiders. According to the point of view of common liberties, we examine computerized ID, with an emphasis on personality frameworks in created countries. We contend that people should have the option to deal with their own data in different settings and that this expects them to have the option to make various irrelevant personalities. As an outcome of this, we start by characterizing a bunch of essential limitations that computerized personality frameworks should stick to shield and advance security, which is vital to the freedom of people. Considering these constraints, we propose a disseminated record innovation and shrewd administration way to deal with working with many-to-numerous associations between significant specialist organizations. Our way to deal with trust varies from others in that we don't endeavor to lay areas of strength for out adaptability by connecting qualifications to one another or to a commonly confided in power. Since the framework doesn't verifiably urge clients to hold a solitary collected character may conceivably be restricted or remade against their inclinations, people and associations are allowed to embrace the framework and receive its rewards.

**Forensic-chain: ethereum blockchain based digital forensics chain of custody**

In cybercrime examinations, advanced proof is pivotal in light of the fact that associating individuals to criminal behavior is utilized. As an outcome of this, it is extremely vital to ensure the auditability, legitimacy, and respectability of computerized proof as it travels through various degrees of ordered progression in the chain of guardianship during an examination concerning cybercrime. For the legal sciences local area, the capability of blockchain innovation to give a total image of exchanges (occasions/activities) back to their starting points is huge. In this review, we recommended utilizing a blockchain for legal purposes, explicitly to safeguard the computerized criminology chain of guardianship from altering and uprightness.

**3. METHODOLOGY**

Evidence management is significant in the field of scientific science. In legal examination, the essential contemplations are proof dealing with and recording. From the time the evidence is gathered to the court's final decision, it is essential to preserve its integrity. In order to solve a case and bring those responsible to justice, evidence gathered from the scene of a crime is essential.

difficulties in settling the dispute and ensuring that the parties involved receive justice.

Chain of custody is the methodology for safeguarding the respectability of proof. The evidence will be unacceptable in court in the event that the chain of guardianship isn't safeguarded, and the case will be excused. Because of its harmless to the ecosystem nature, digitalizing legal proof administration frameworks is a critical prerequisite. Blockchains are painstakingly coursed records of cryptographically stamped trades in successive solicitation that are arranged into blocks and are totally open to anybody in the blockchain network. The Hyperledger Texture consortium blockchain innovation was created by the Linux Establishment and is principally used for business purposes. In view of the Hyperledger

Texture idea, the ongoing review endeavored to plan a structure and afterward propose an execution calculation.

Benefits

1. The forensic evidence administration framework will be digitalized and the Chain of Custody will be safeguarded utilizing blockchain innovation.
2. Consequently, it is essential to safeguard these evidences against any kind of tampering.

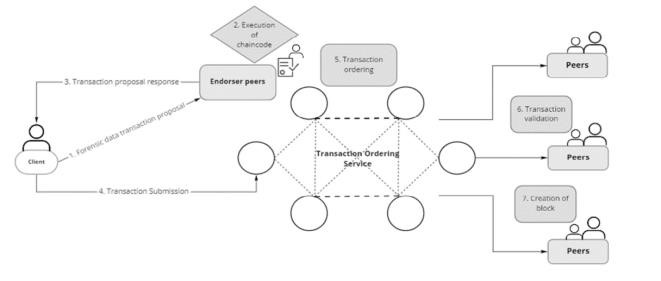


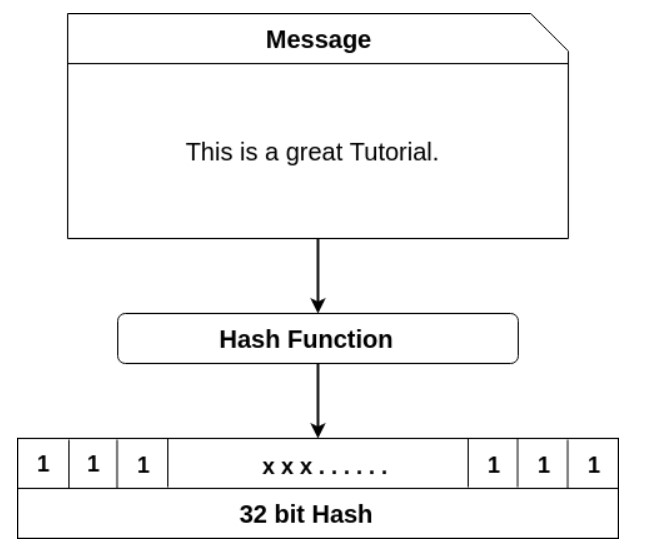
Fig 2 Proposed Architecture **Modules:**

The following modules were developed to assist us in completing this task.

1. Login as Admin: Using the username and password "admin," police officers can use this module to access the program.
2. Contribute Blockchain-Based Evidence: Police officers can upload evidence to the Ethereum Blockchain tool using this module.
3. Retrieve Blockchain-based Evidence: With this module, police officers can access all Blockchainstored evidence; only authorized officers can access Blockchain-stored evidence.
4. **IMPLEMENTATION**

**Blockchain Hash Function**

An information string (numbers, letter sets, or media documents) of any length is changed into a line of a foreordained length utilizing a hash capability. Contingent upon the hash calculation utilized, the proper piece length might shift (for instance, 32 pieces, 64 pieces, 128 pieces, or 256 pieces). A hash is the result with a proper length. A hash estimation's cryptographic outcome is moreover this hash. The representation beneath assists us with understanding.



The qualities of the hash calculation are as per the following: It delivers a special result, otherwise called a hash. There is just a single way it very well may be utilized. The blockchain's agreement cycle utilizes the qualities of this cryptographic hash capability with regards to digital forms of money like Bitcoin. A condensation, or computerized finger impression, of a bunch of information is a cryptographic hash. Cryptographic hash capabilities accept exchanges as info and cycle them through a hashing interaction to create a fixed-size yield. The subsequent hash can't be utilized to recover the whole text in light of the fact that the Hash capability is one-way. This is not the same as standard cryptographic tasks like encryption, where you utilize the way to encode something and afterward use unscrambling to decipher the message back to its unique structure.

**Block chain**

Blockchain is a dispersed, unchanging record that simplifies it to monitor resources and record exchanges in a business organization. Elusive resources incorporate protected innovation, licenses, copyrights, and land, among other actual resources. Nearly anything of significant worth can be checked and sold on a blockchain network, bringing down hazard and expenses for all gatherings included. Data is an organization's soul. The sooner it is gotten and the more exact it is, the better. Since it conveys prompt, shareable, and straightforward information put away on a permanent record that must be seen by network clients with authorization, blockchain is great for giving such data. Orders, installments, records, and creation can be generally followed by a blockchain network. You can likewise see all parts of an exchange from start to finish since individuals have a bound together viewpoint of reality. This gives you more certainty and opens up new open doors and efficiencies.

1. **EXPERIMENTAL RESULTS**



Fig 3 Home Page

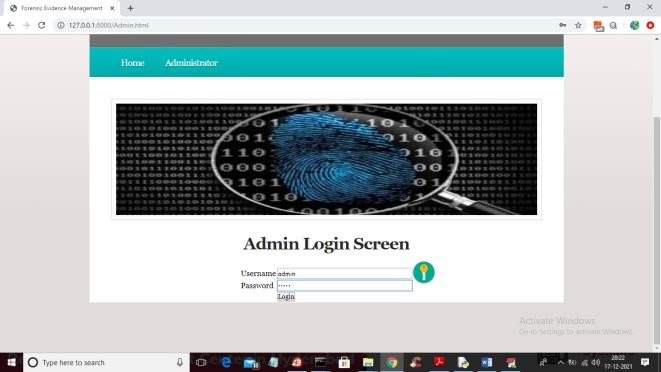


Fig 4 Login Page



Fig 5 Add evidences block page



Fig 6 Upload values



Fig 7 Prediction Result

1. **CONCLUSION**

From the moment evidence is obtained from the scene of the crime until a decision is made by a court, it is essential to preserve its integrity. It is essential to preserve the chain of custody because it may demonstrate whether the evidence was tampered with during the process of collecting and processing it. The digitalization of the chain of custody through the application of Blockchain technology guarantees the security, validity, and integrity of forensic data exchanges. Not only will the use of blockchain make it better for the environment, but it will also improve security thanks to encryption, which can only be viewed remotely by authorized individuals. The chain of custody procedure will be carried out by an algorithm that will make use of blockchain technology, specifically Hyperledger Fabric.

1. **ACKNOWLEDGEMENT**

We thank CMR Technical Campus for supporting this paper titled“AN IMPLENENTATION OF BLOCKCHAIN TECHNOLOGY IN FORENSIC

EVIDENCE MANAGEMENT”,which provided good facilities and support to accomplish our work. Sincerely thank our Chairman, Director, Deans, Head Of the Department, Department Of Computer Science and Engineering, Guide and Teaching and Non-Teaching faculty members for giving valuable suggestionsand guidance in every aspect of our work

1. **FUTURE SCOPE** Also, forensic examinations can profit from the incorporation of blockchain innovation with artificial intelligence and machine learning.

**REFERENCES**

1. Bonomi, S., Casini, M., &Ciccotelli, C. (2018). BCoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics. arXiv preprint arXiv:1807.10359.
2. Gopalan, S.H., Suba, S.A., Ashmithashree, C., Gayathri, A., Andrews, V.J. (2019). Digital Forensics using Blockchain. International Journal of Recent Technology and Engineering, 8(2S11), 182–184. <https://doi.org/10.35940/ijrte.b1030.0982s1119>[3] Bou Abdo, J., El Sibai, R., &Demerjian, J. (2020). Permissionless proof‐ of‐ reputation‐ X: A hybrid reputation‐ based consensus algorithm for permissionless blockchains. Transactions on Emerging Telecommunications Technologies, 32(1), 1. <https://doi.org/10.1002/ett.4148>
3. Varshney, T., Sharma, N., Kaushik, I., Bhushan, B. (2019). Authentication & Encryption Based Security Services in Blockchain Technology. International Conference on Computing, Communication, and Intelligent Systems (ICCCIS),

India, 63-68. doi:

10.1109/ICCCIS48478.2019.8974500

1. Kahate, A. (2003). Cryptography and Network Security. McGraw-Hill Education.
2. Dominique Guegan. Public Blockchain versus Private blockchain. 2017. ⟨halshs-01524440⟩
3. Blockchain Technology Overview. (2018, October). <https://doi.org/10.6028/NIST.IR.8202>
4. Castor, A. (2017). A short guide to blockchain consensus protocols. Coindesk. [https://www.coindesk.com/short-guideblockchainconsensus-protocols](https://www.coindesk.com/short-guide-blockchainconsensus-protocols)
5. Cong T. Nguyen, Dinh T. Hoang, Diep N. Nguyen, Dusit Niyato, Huynh TuongNhuyen& Eryk

Dutkiewicz. (2019). https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnu m ber=8746079

[10]Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., et al. (2018). Hyperledger fabric. Proceedings of the Thirteenth EuroSys Conference, 1–15. <https://doi.org/10.1145/3190508.3190538>

[11]Goodell, G., &Aste, T. (2019). A Decentralized Digital Identity Architecture. Frontiers in Blockchain, 2, 1. <https://doi.org/10.3389/fbloc.2019.00017>

[12]Krstić, M., &Krstić, L. (2020). Hyperledger frameworks with a special focus on Hyperledger Fabric. VojnotehnickiGlasnik, 68(3), 639–663.

<https://doi.org/10.5937/vojtehg68-26206>

**11.CERTIFICATION**







