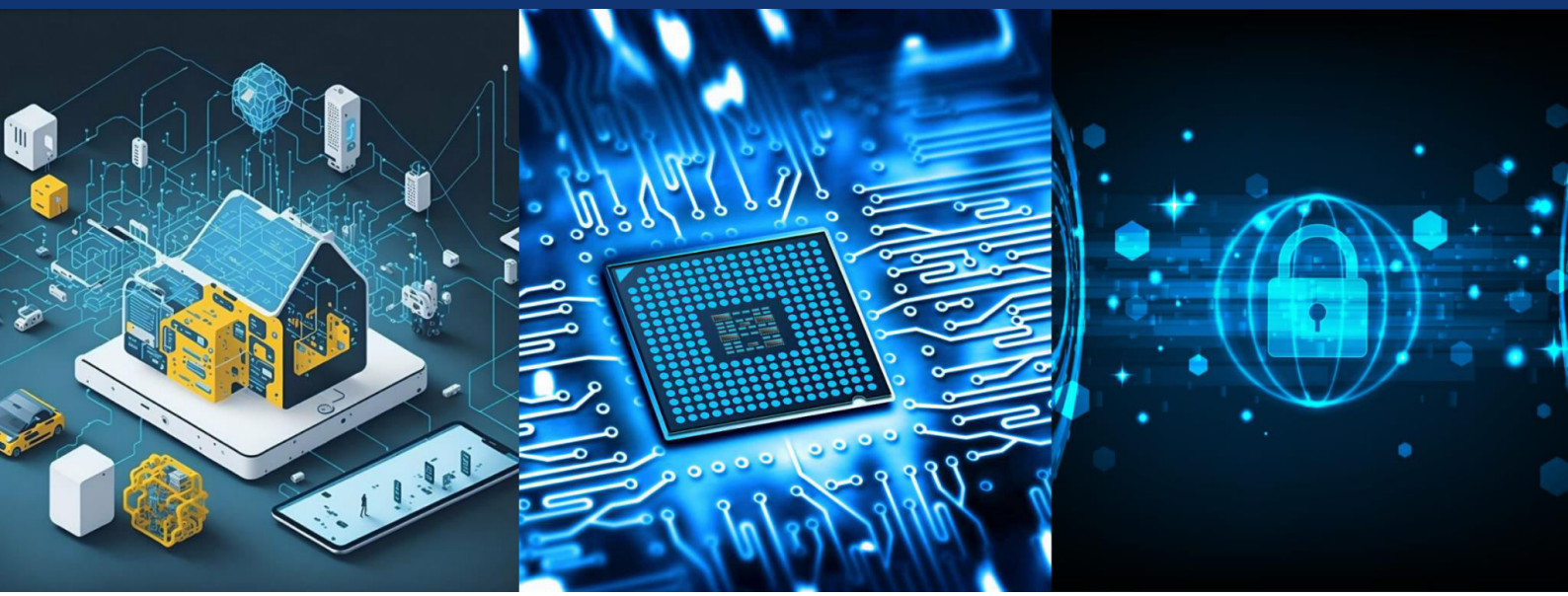
IJIRCCE

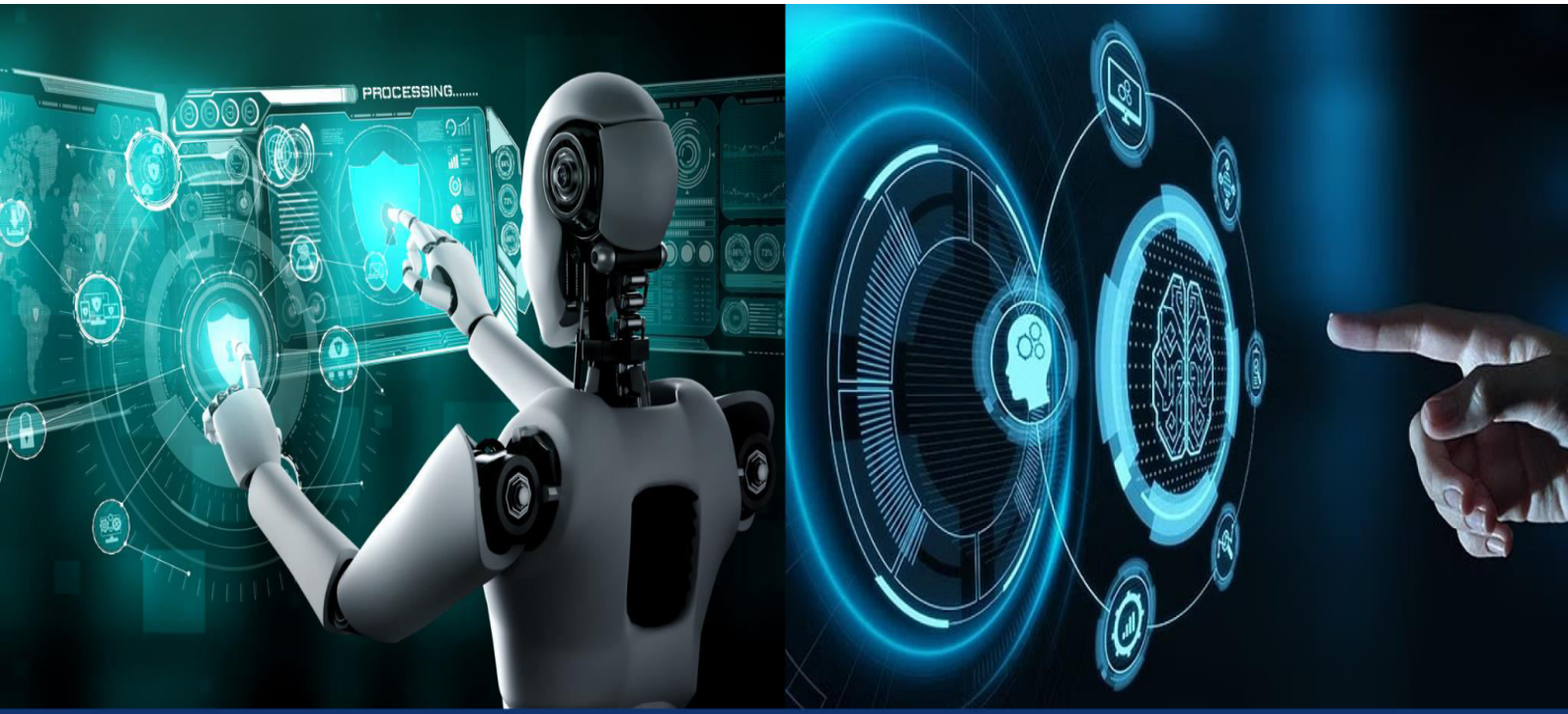
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 4, April 2025

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304059

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Judicial Evidence Integrity and Security System using Blockchain and Deep Learning

Mr. G. Vishvantha Sundharam M.E, Balaezhilan B, Jayaprakash M, Muthuganesh M

Assistant Professor, Dept. of Cyber Security, Muthayammal Engineering College, Namakkal, Tamil Nadu, India

UG Students, Dept. of Cyber Security, Muthayammal Engineering College, Namakkal, Tamil Nadu, India

ABSTRACT: The integrity and security of judicial evidence are paramount to ensuring fair and transparent legal proceedings. Traditional evidence management systems are vulnerable to tampering, loss, and unauthorized access, which can compromise justice delivery. This paper proposes an innovative system leveraging blockchain technology and deep learning to enhance the reliability, security, and efficiency of judicial evidence handling. Blockchain's decentralized and immutable nature provides a secure framework for storing and tracking evidence, ensuring its authenticity and preventing unauthorized alterations. Each piece of evidence is hashed and timestamped before being stored on the blockchain, creating an auditable chain of custody. Deep learning models are integrated into the system to automate evidence classification, authentication, and anomaly detection. For instance, deep neural networks can verify the integrity of digital evidence, such as images orvideos, by identifying manipulations or inconsistencies. This dual-layer approach combines the trustworthiness of blockchain with the analytical power of deep learning, offering a robust solution for modern judicial systems. The proposed system not only bolsters evidence security but also streamlines judicial workflows by reducing manual intervention. By addressing critical challenges in evidence management, this work aims to build trust in judicial processes and ensure justice is served with greater efficiency and accuracy.

KEYWORDS: Judicial evidence management, Evidence integrity verification, Blockchain-based security, Digital chain of custody, Tamper-proof evidence storage, Secure data ledger, Deep learning for evidence classification, AI-powered forensic analysis, Smart contracts in legal systems, Decentralized evidence tracking, Legal data authentication, Cryptographic hashing of evidence, Immutable data records, Blockchain in law enforcement, Automated evidence validation.

I. INTRODUCTION

The increasing reliance on digital evidence in judicial proceedings necessitates robust mechanisms to ensure its integrity, security, and authenticity. Traditional methods of evidence handling are vulnerable to tampering, unauthorized access, and data loss, which can compromise the fairness and accuracy of legal outcomes. To address these challenges, this project proposes a **Judicial Evidence Integrity and Security System** that leverages the combined power of **Blockchain technology** and **Deep Learning**. Blockchain offers a decentralized and immutable ledger that ensures the secure storage and traceability of digital evidence, preventing unauthorized alterations and establishing a verifiable chain of custody. Each piece of evidence is hashed and recorded on the blockchain, guaranteeing its authenticity over time. Complementing this, Deep Learning algorithms are utilized for intelligent analysis and classification of evidence, enabling efficient identification of tampered data, as well as automating tasks such as facial recognition, object detection, and content verification. By integrating these cutting-edge technologies, the system aims to enhance the transparency, reliability, and efficiency of judicial processes. This solution not only secures digital evidence from manipulation but also supports legal professionals in evidence management and decision-making, paving the way for a more trustworthy and technologically advanced judicial system.

II. SCOPE OF THE PROJECT

The proposed project, titled **"Judicial Evidence Integrity and Security System Using Blockchain and Deep Learning,"** aims to revolutionize the way digital evidence is stored, secured, and analyzed in the judicial domain. The scope of this project encompasses the design, development, and implementation of a comprehensive framework that ensures the integrity, authenticity, and accessibility of digital evidence through the integration of blockchain technology

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304059

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

and deep learning techniques. The system will provide a **tamper-proof environment** for storing digital evidence such as documents, images, videos, and audio recordings. Using blockchain, every piece of evidence will be hashed and time-stamped to create an immutable record, ensuring that any alterations or unauthorized access attempts can be easily detected and traced. This guarantees a verifiable chain of custody, which is crucial in legal proceedings. On the other hand, **deep learning** models will be employed for intelligent evidence analysis. These models can perform tasks such as **object detection, facial recognition, content classification, and anomaly detection**, which assist legal authorities in understanding and validating the authenticity of the evidence more efficiently. Additionally, automated analysis can significantly reduce the time and effort required for manual review of large volumes of digital content. The scope also includes the development of a **user-friendly interface** for legal professionals to upload, access, and verify evidence securely. Role-based access control will ensure that only authorized personnel can interact with specific evidence files. This project is not limited to criminal cases; it can be extended to civil, corporate, and administrative law proceedings where digital evidence plays a role. Furthermore, the system can be integrated with existing legal infrastructure to enhance transparency, reduce delays, and foster trust in the judicial process. Overall, the project aims to provide a scalable and secure solution for the digital transformation of the justice system.

III. PROPOSED WORK

The core of the proposal is an efficient forensics architecture that leverages blockchain technology for establishing the Chain of Custody (CoC) and deep learning models for tamper detection. This combination aims to address security and forensic aspects throughout the investigation lifecycle.

- **System Architecture and Flowchart:**

The system architecture integrates three core components: **Evidence Acquisition Module**, **Blockchain Network**, and **Deep Learning Engine**. Digital evidence (images, videos, documents) is first acquired and pre-processed. A unique cryptographic hash of the evidence is generated and stored on the **Blockchain**, ensuring immutability and a tamper-proof chain of custody.

Simultaneously, the evidence is analyzed by the **Deep Learning module** for classification, anomaly detection, or verification. Results are stored and linked to the blockchain record. Users, including law enforcement and legal personnel, access evidence through a secure interface, ensuring traceability, authenticity, and real-time verification throughout the judicial process.

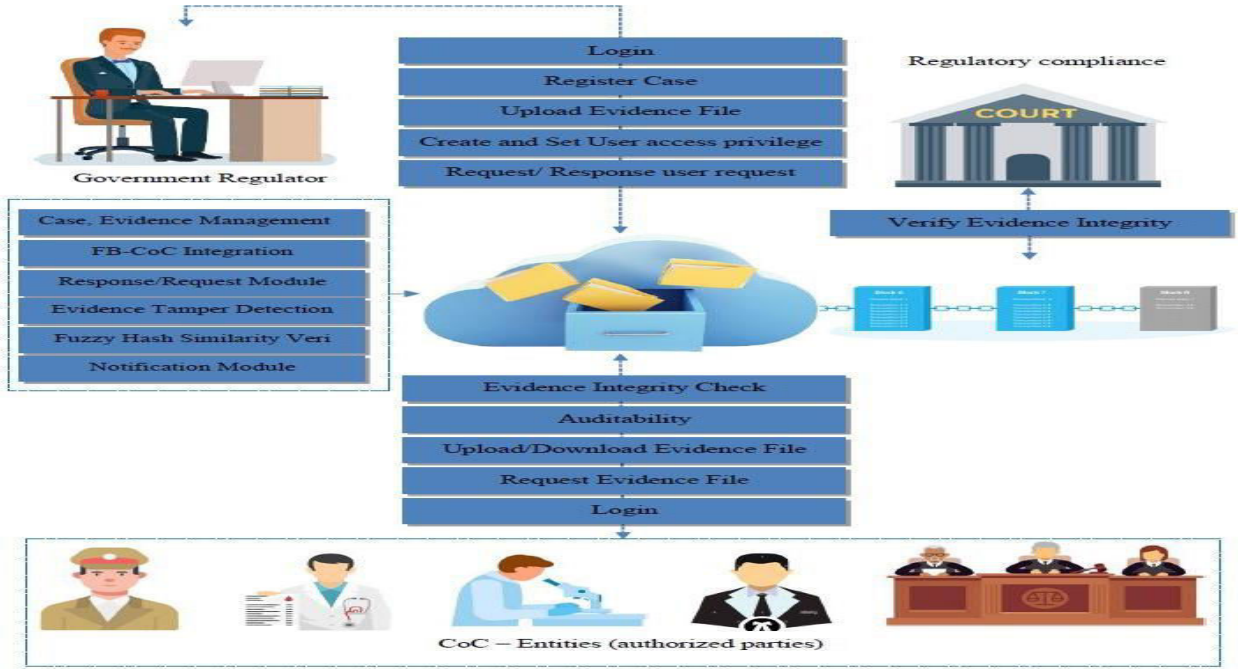


Fig 1. System Architecture and Flowchart

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304059

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- **DB-CoC Architecture:**

The proposed architectural solution, referred to as DB-CoC, is designed to provide robust information integrity, prevention, and preservation mechanisms. It involves the permanent and immutable storage of evidence (chain of custody) in a private, permissioned, and encrypted blockchain ledger.

- **Blockchain for Chain of Custody:**

Blockchain technology is suggested to establish a secure and tamper-evident Chain of Custody. Participants in the investigation process create a private network to agree on and record various activities on the blockchain ledger.

- **Three Types of blockchain:**

1. Public Blockchain:- A public, or permission-less, blockchain network is one where anyone can participate without restrictions. Most types of cryptocurrencies run on a public blockchain that is governed by rules or consensus algorithms.
2. Permissioned or Private Blockchain:- A private, or permissioned, blockchain allows organizations to set controls on who can access blockchain data. Only users who are granted permissions can access specific sets of data. Oracle Blockchain Platform is a permissioned blockchain.
3. Federated or Consortium Blockchain:- A blockchain network where the consensus process (mining process) is closely controlled by a preselected set of nodes or by a preselected number of stakeholders.

- **Deep Learning:**

Deep Learning is a part of machine learning, which is a subset of Artificial Intelligence. It enables us to extract information from the layers present in its architecture. It is used in Image Recognition, Fraud Detection, News Analysis, Stock Analysis, Self-driving cars, and Healthcare like cancer image analysis, etc. By inputting more data into the network, the layers get trained very well. They can be classified into Supervised, Semi-Supervised, and Unsupervised categories. Each layer is known for extracting information specifically. For example, in Image recognition, the first layer will find the edge, lines, etc, second layer like the eye, ear, nose, etc.

- **Attacker Modules**

In this module the attacker performs the following types of attack to change the evidence file. The name itself is an acronym for the following threat types:

1. Spoofing:- The attacker impersonates another person or uses their password to act as that person. Spoofing is a threat to authenticity.
2. Tampering:- It is the act of purposefully modifying data and violates the integrity of data.
3. Repudiation:-Untraceable illegal actions fall into repudiation threats. A user can dispute his crime since no proof can be given otherwise.
4. Information disclosure:- Nowadays known as privacy breach, is the threat where sensitive information is visible to people that are not supposed to see it. Confidentiality is desired to counter information disclosure.
5. Denial of service (DoS):- A threat where the system becomes temporarily unavailable. These kind of attacks lower the reliability of the system.
6. Elevation of privilege (EoP):- A person gives himself unlawful privilege to restricted actions which can compromise the whole system. Authorization is the desired property to suppress such threats.

IV. TOOLS AND LIBRARIES

CoC FORENSIC TOOL: This module is intended to serve as an interface for authorization, access permissions, and media. It allows for the downloading of digital evidence and certificates of authenticity in line with access permissions and levels. The blockchain interface enables participants to see, invoke, and query blocks, transactions, and chain codes. The front end produces a hash of the digital evidence and a nonce that uniquely identifies it (Evidence ID). As the hash generates the ID and the value nonce is randomly selected to guarantee the uniqueness of the evidence's identification, it aids in preserving the integrity of digital evidence throughout its lifetime. This component is responsible for enabling communications between all the users. It incorporates access control and evidence management; creating a new record, evidence state verification, and disposal of evidence.

DB-BLOCKCHAIN INTEGRATION: Fuzzy Blockchain (FB): This component describes the private blockchain implementation using, for instance, private Blockchain called FuzzyBlockchain, as the main underlying system for cybercrime application. Participating roles and responsibilities will act as active nodes of the FB blockchain network. The FB contains an essential element to its structure, i.e., shared ledger or DLT, which will be able to log all collective and transferred evidence and immutability shared among all the different and authorized entities. The DLT is governed

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

by lawmakers and law enforcement institutes. The FB has three sub-functions, which together form the operation of FB. These are:

Secure Transaction—This carries the evidence track records, e.g., submission, archiving, transfer, fetching, etc. Each transaction entails necessary information and a unique identifier. Information details are set as per forensic investigation standards to include data type, timestamp, submitter and receiver IDs, geographical locations, etc. The transaction is then hashed, and once verified by the consensus algorithm, will be stored in the CB DLT and distributed among all active network nodes;

Smart Contract—Each transaction can be automated using a smart contract. A smart contract is a set of predetermined executable instructions based on the nature of a certain transaction or input. An output can also trigger another smart contract. For example, a case is created, the smart contract logs the submitter ID and associated evidence provided by the analysis phase. Based on the analysis output, the smart contract initiates another instance to request more evidence from the submitter or witnesses. If the submitted evidence is sufficient for the case, then the smart contract proceeds to the analysis and investigation procedures. Additional steps in the investigation process, e.g., evidence transfer and archival, are not presented in this paper;

Consensus Node—This is a function with a set of rules that is responsible for maintaining, verifying and approving BF records/transactions and updating the ledger. It also ensures trustworthiness when reliability, availability, accuracy, and authenticity are built in by design. The on-chain governance of the CB blockchain is achieved by consensus nodes in not only restricting access to the CB ledger, but also who can perform different actions, e.g., validation of transactions. There are different implementations of consensus algorithms, such as proof of work (PoW), proof of stake (PoS), delegated proof of stake (DPoS), practical byzantine fault tolerance (pBFT), proof of authority (PoA), etc. A private (permissioned) implementation of the CB model is suggested with the use of practical byzantine fault tolerance (pBFT) as a consensus algorithm. The pBFT is considered for the CB model with the assumption that some of the consensus nodes may act faultily or maliciously in the network, hence our taking proactive measures to ensure consistent and valid voting/validation. The pBFT does not scale to accommodate other blockchains or larger volume, but to maintain evidence handling, the author believes it should suffice.

FUZZY HASH: To account for the uncertainty associated with evidence item changes, we utilized Fuzzy Hashing (FH) rather than conventional hashes such as SHA 256 in this project. FH, also known as Context- Triggered Piecewise Hashing (CTPH), is a mix of Piecewise and Rolling Hashing (RH). Unlike traditional hashes, where their hashes (checksums) can be interpreted as correct or incorrect, and as black or white, CTPH is more akin to the “grey hash type” as it can identify two files that are likely near duplicates of one another but would not be detected using traditional hashing methods. RH generates ‘segments’ of conventional hash strings by generating a pseudo-random value depending on the context of the input. In comparison, PH (Piecewise Hashes), such as conventional hashes, produce a final checksum for the whole picture. They circumvent the latter’s restrictions by segmenting the whole image into defined segments and then generating hash values for each of these parts. Finally, the produced values comprise the final hash sequence. FH employs the concept of PH to preserve data similarity in this study. Additionally, PH was designed to minimize possible mistakes during forensic imaging, ensuring that the data’s integrity is absolute and complete since only one hash segment is void.

ALGORITHMS:

1. Convolutional Neural Network(CNN):- In CNN, the processing of data involves breaking the images into many numbers of overlappingtiles instead of feeding entire images into our network. And then, we use a technique called a sliding window over the whole original image and save the results as a separate tiny picture tile. The Sliding window is a kind of brute force solution where we scan all around for a given imageto detect the object for all possible sections, each section at a time until we get the expected object.
2. Temporal Convolutional Network(TCN):- The Temporal Convolutional Network (TCN) is a type of neural network architecture designed primarily for sequential data processing tasks, such as time series forecasting, natural language processing, and speech recognition. TCNs leverage the power of convolutional layers to capturedependencies across time efficiently.
3. Bidirectional Encoder Representations from Transformers(BERT):- BERT is a state-of-the-art natural language processing (NLP) model developed by Google. It is a deep learning model developed by Google for natural language processing tasks. It uses a transformer architecture to process text in both directions (left-to-right and right-to-left),

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304059

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

enabling better context understanding. BERT excels in tasks like sentiment analysis, question answering, and text classification.

4. Hidden Markov Model(HMM):- The Hidden Markov Model (HMM) is a statistical model used to model sequential data, where the underlying system is assumed to be a Markov process with unobservable states. An HMM consists of a finite set of hidden states S={S 1,S 2 ,...,S N}, where each state represents a particular situation or configuration of the system being modeled. These states are not directly observable but are associated with the emissions observed at each time step. Each hidden state is associated with a probability distribution over possible observations. These observations are the visible outputs or emissions of the system. Each state emits observations according to a probability distribution , often represented as an emission probability matrix. (o) denotes the probability of observing symbol o when the system is in state. The model also includes an initial state distribution π, which represents the probability distribution over the hidden states at the initial time step (time step 0).

V. PROGRAM

```
import mysql.connector

mydb = mysql.connector.connect(
  host="localhost",
  user="root",
  passwd="",
  charset="utf8",
  database="coc_new"
)


app = Flask(__name__)
##session key
app.secret_key = 'abcdef'
UPLOAD_FOLDER = 'static/upload'
app.config['UPLOAD_FOLDER'] = UPLOAD_FOLDER
#####

@app.route('/',methods=['POST','GET'])
def index():
    cnt=0
    act=""
    msg=""
    if request.method == 'POST':
        username1 = request.form['uname']
        password1 = request.form['pass']
        mycursor = mydb.cursor()
        mycursor.execute("SELECT count(*) FROM coc_register where uname=%s && pass=%s",(username1,password1))
        myresult = mycursor.fetchone()[0]
        if myresult>0:
            session['username'] = username1
            result=" Your Logged in sucessfully**"
            return redirect(url_for('home'))
        else:
            msg="Invalid Username or Password!"
```

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304059

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. RESULT AND DISCUSSION

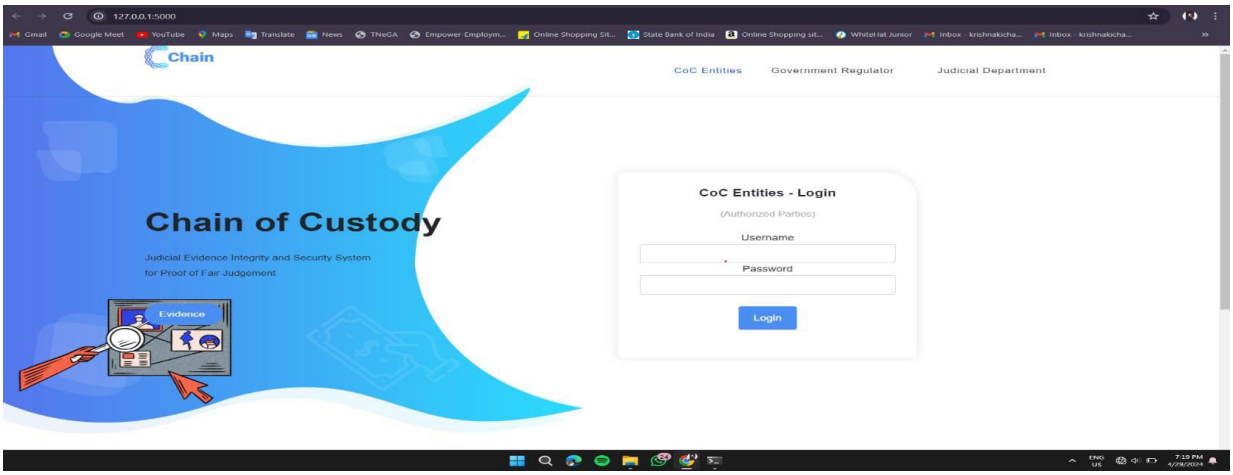


Fig. 1

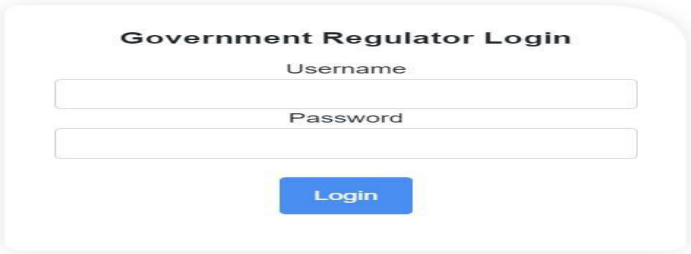


Fig. 2

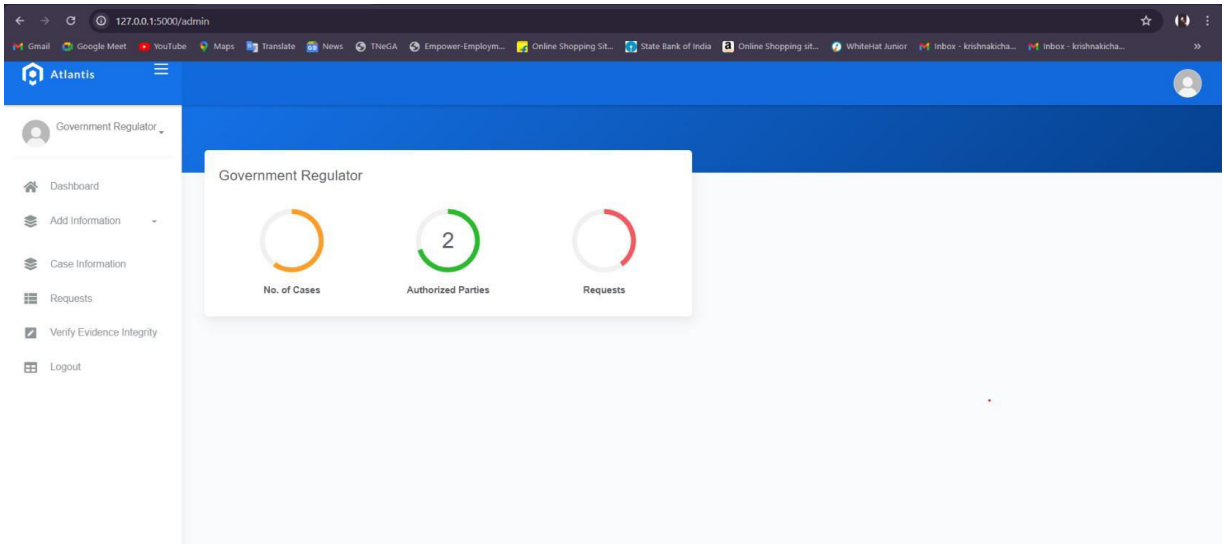


Fig. 3

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304059

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

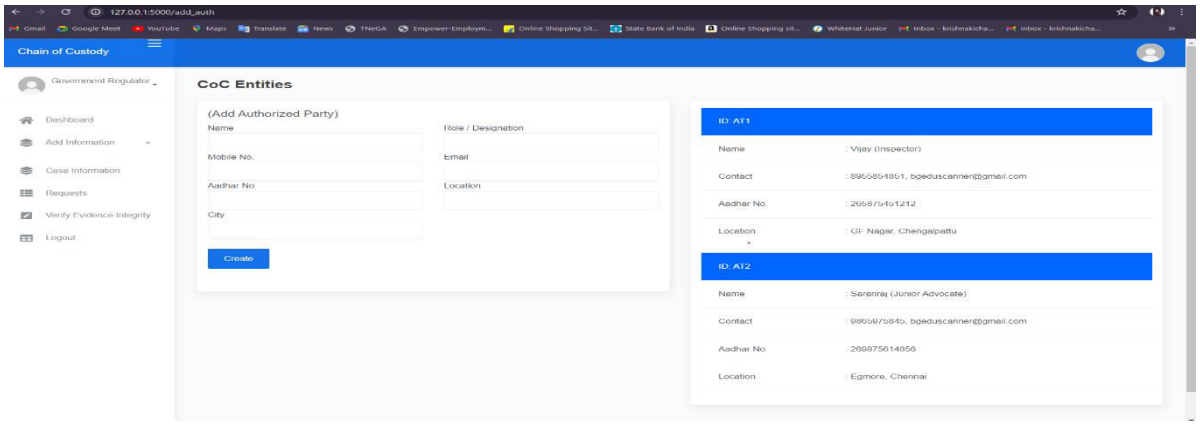


Fig. 4

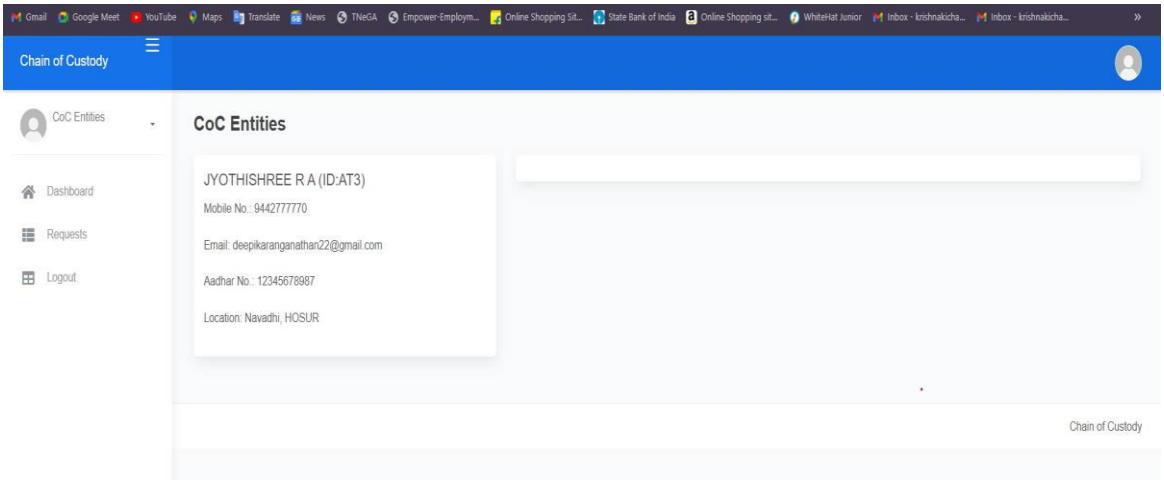


Fig. 5

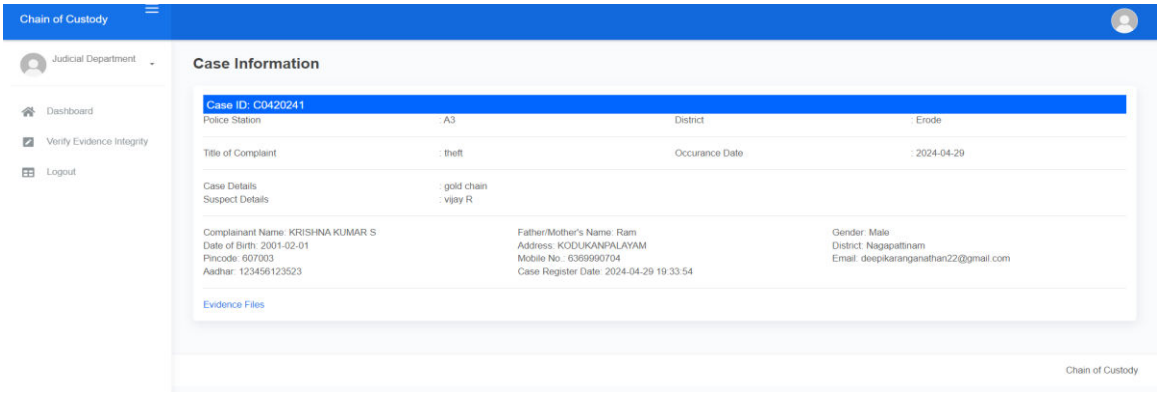


Fig. 6

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304059

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

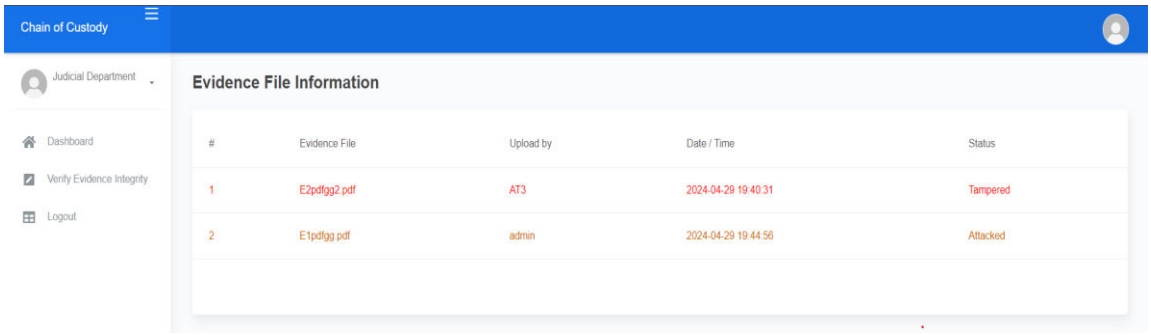


Fig. 7

VII.CONCLUSION

In today's ever-growing digital world, we are facing huge challenges in securing our digital infrastructures against different types of cybersecurity incidents. The goal of digital forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a digital infrastructure network or computing devices involved and who was responsible for it to mitigate and halt such cyber incidents. In conclusion, this project developed a FB – CoC model and a platform to secure Multimedia Forensic Digital Evidence (MFDE) and to ensure the forensic soundness of the stored evidence.

The purpose of this FB- CoC is to determine the efficacy of fuzzy hashing algorithms inside blockchain technology, as opposed to conventional cryptographic hash algorithms, in preserving the integrity of digital evidence in image forensics.

According to the performance evaluation, fuzzy hash-based blockchains proved to be an effective support for the chain of custody process due to their ability to sustain a realistic workload with a manageable overhead in terms of memory used to store the chain and their ability to handle the chain of custody-related uncertainty. With FB - CoC an investigator does not need to be concerned about verification and authenticity of evidence when performing a digital investigation.

REFERENCES

1. Hany M. Elgohary, Saad M. Darwish, Saleh Mesbah Elkaffas “Chain of Custody in Digital Forensic Investigations: Issues and Challenges” IEEE Access Volume 10,2022 ,10.1109/ACCESS.2022.3147809.
2. Arif Rahman Hakim, Kalamullah Ramli, Teddy Surya Gunawan “A Novel Digital Forensic Framework for Data Breach Investigation” Volume 4,2022 IEEE Access DOI 10.1109/ACCESS.2022.DO.
3. Qian Ren, Yue Li, Yingjun Wu, Yuchen Wu, Hong Lei, Lei Wang and Bangdao Chen “DECLOAK: Enable Secure and Cheap Multi- Party Transactions on Legacy Blockchains by a Minimally Trusted TEE Network” IEEE Transaction on Information and Security, volume 18, No.06, July 2023.
4. Lusetti .M, L. Salsi, and A. Dallatana, ``A blockchain based solution for the custody of digitalfiles in forensic medicine," Forensic Sci. Int., Digit. Invest., vol. 35, Dec. 2020, Art. no. 301017.
5. Uddin .M, ``Blockchain medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry," Int. J. Pharmaceutics, vol. 597, Mar. 2021, Art.no. 120235.
6. Battiato .S, O. Giudice, and A. Paratore, ``Multimedia forensics: Discovering the history of multimedia contents," in Proc. 17th Int. Conf. Comput. Syst. Technol., Jun. 2016, pp. 5-16.
7. Bayar .B and M. C. Stamm, ``Design principles of convolutional neural networks for multimedia forensics," Electron. Imag., vol. 2017, no. 7, pp. 77-86, Jan. 2017.
8. Hasan .H .R, K. Salah, R. Jayaraman, M. Omar, I. Yaqoob, S. Pesic, T. Taylor, and D. Boscovic, ``A blockchain-based approach for the creation of digital twins," IEEE Access, vol. 8, pp. 34113-34126, 2020.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

9. Jeong .J, D. Kim, B. Lee, and Y. Son, ``Design and implementation of a digital evidence management model based on Hyperledger fabric," J. Inf. Process. Syst., vol. 16, no. 4, pp. 760- 773, 2020.
10. Khan .A .A , M. Uddin, A. A. Shaikh, A. A. Laghari, and A. E. Rajput, ``MF-ledger: Blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture," IEEE Access, vol. 9, pp. 103637-103650, 2021.
11. Kumar .M .R and N. Bhalaji, ``Blockchain based chameleon hashing technique for privacy preservation in E-governance system,"Wireless Pers. Commun., vol. 117, no. 2, pp. 1-20, 2020.
12. Lal .C, M. Conti, and D. Hu, ``LEChain: A blockchain-based lawful evidence management scheme for digital forensics," Future Gener. Comput. Syst., vol. 115, pp. 406-420, Feb. 2021.
13. Li .D, W. Liu, L. Deng, and B. Qin, ``Design of multimedia blockchain privacy protection system based on distributed trusted communication," Trans. Emerg. Telecommun. Technol., vol. 32, no. 2, p. e3938, Feb. 2021.
14. Lone .A.H and R. N. Mir, ``Forensic-chain: Blockchain based digitalnforensics chain of custody with PoC in hyperledger composer," Digit. Invest., vol. 28, pp. 44-55, Jan. 2019.
15. Lusetti .M, L. Salsi, and A. Dallatana, ``A blockchain based solution for the custody of digital files in forensic medicine," Forensic Sci. Int., Digit. Invest., vol. 35, Dec. 2020, Art. no. 301017.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details