IJIRMET ISSN (Online): 2456-0448

International Journal Of Innovative Research In Management, Engineering And Technology

Vol. 9, Issue 3, April 2024

# Judicial Evidence Integrity and Security System Using Blockchain and Deep Learning

[1] Dr. P. Sumathi, [2] Deepika R, [3] Janani M, [4] Jyothishree R A

[1] Adhiyamaan College of Engineering, Hosur, India sumithirulogu@gmail.com

[2] B.Tech. Student Department of Information Technology, Adhiyamaan College of Engineering, Hosur, India
deepikaranganathan22@gmail.com

[3] B.Tech. Student Department of Information Technology, Adhiyamaan College of Engineering, Hosur, India
jananimogan998@gmail.com

[4] B.Tech. Student Department of Information Technology, Adhiyamaan College of Engineering, Hosur, India
jyothishreeramesh2501@gmail.com

Abstract: ***Digital evidence is defined as information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. In criminal investigations, civil lawsuits, and regulatory compliance, digital evidence such as electronic documents, recordings, and transaction records forms the basis for decision-making. However, factors like data alteration, unauthorised access, or flaws in centralised storage can threaten the security and integrity of digital evidence. Therefore, a secure storage model is needed to improve the investigation process and safeguard any sensitive information collected. To address the lack of an automated mechanism for preserving evidence and maintaining integrity, a model was developed targeting the various security and forensic aspects during the investigation lifecycle. An efficient forensics architecture is proposed that establishes the Chain of Custody (CoC) in blockchain technology and tamper detection using Deep Learning Models, where participating stakeholders create a private network to exchange and agree on different investigation activities before being stored on the blockchain ledger. Detecting tampering in various types of files using deep learning algorithms are Image with CNN, Word Document Embedding's using BERT, Video Frame-level Analysis with TCN, Audio Spectrogram Analysis with HMM, PDF Document Structure Analysis. Utilizing fuzzy hash functions enables forensic investigators to successfully deal with permissible alteration of digital evidence by standardizing the forensics processes, DB-CoC architecture enforcing a standard approach and improves the quality of the finished result. The proposed architectural solution delivers robust information integrity, prevention, and preservation mechanism to permanently and immutably store the evidence (chain of custody) in a private permissioned encrypted blockchain ledger. The proposed DB-CoC architecture provides complete data provenance, traceability, and assurance for performing different operations as well as trust between the chain of custody events while collecting, storing, analysing, and interpreting the digital evidence.***

***Key Terms: CNN, HMM, BERT, TCN, Fuzzy Hash***

## I. INTRODUCTION

The importance of judicial evidence in legal proceedings across various domains has surged in the contemporary digital landscape. Whether in criminal inquires, civil litigations, or regulatory adherence , the utilization of digital evidence such as electronic documents, transaction records, and recordings. Nevertheless, the preservation and security of digital evidence face numerous challenges, including but not limited to data tampering, unauthorized entry, and vulnerabilities within centralized storage infrastructures. In response, we unveil a scholarly article unveiling a decentralized paradigm leveraging smart contracts on the blockchain, aimed at mitigating these concerns. Our proposed solution, tailored to uphold the authenticity, permanence, and availability of digital evidence, harnesses blockchain technology, with a focus on the blockchain. The exceptional ability of the Polygon blockchain to effortlessly accommodate growth and maintain minimal transaction expenses renders it the ideal ecosystem for launching decentralized applications. This framework guarantees reliability, transparency, and responsibility at every stage of digital evidence existence, leveraging the functionalities embedded within smart contracts. In this article, we discuss how our decentralized system works and what it's made of. We focus on the Polygon blockchain and how it suits our research goals. We also talk about smart contracts, which help set rules and enforce them automatically, making it easier to keep digital evidence safe. By combining smart contracts with the Polygon blockchain, our method makes managing digital evidence more secure and reliable. We explore the benefits of our decentralized approach compared to traditional centralized methods. By moving away from relying on a single central authority, our model reduces the risks of unauthorized access and data tampering. The transparency and immutability of the blockchain ensure the integrity of digital evidence, making it resistant to tampering and easily verifiable. Furthermore, our decentralized storage setup enhances accessibility and minimizes the chances of data loss. We highlight the advantages of our decentralized model while also recognizing its limitations.

## II. RELATED WORK

[19] DECLOAK, a novel approach designed to facilitate secure and cost-effective multi-party transactions on existing blockchains using a minimally trusted Trusted Execution Environment (TEE) network. The concept involves leveraging TEE technology to establish a network of trusted execution environments that provide a secure and isolated environment for executing multi-party transactions. By minimizing the trust requirements and utilizing existing blockchain infrastructure, DECLOAK aims to address the limitations of legacy blockchains in handling complex multi-party transactions efficiently and securely.

[2] This article proposes a novel approach to address the challenges of conducting digital forensic investigations within the interconnected environments of the Internet of Things (IoT) and social systems. By leveraging blockchain technology, the paper aims to enhance the integrity and reliability of digital evidence by providing a secure and transparent framework for data preservation and analysis. The conceptual framework will outline the integration of blockchain into the investigation process, emphasizing its potential to ensure the immutability and authenticity of forensic data while addressing the decentralized nature of IOT devices and the dynamic interactions within social systems.

[12] This research paper proposes novel methods and techniques to enhance the reliability and reduce uncertainty in the chain of custody for image forensic investigation applications. The chain of custody refers to the chronological documentation of the handling, transfer, and storage of digital evidence, crucial for establishing its authenticity and admissibility in legal proceedings. Recognizing the inherent challenges and uncertainties associated with digital image evidence, such as metadata manipulation and data tampering, this paper aims to address these issues through innovative approaches.

[4] This article proposes the utilization of smart ledger technologies to regulate electronic data sharing and processing in supply chains, with a focus on enhancing security. Supply chains are complex networks involving multiple stakeholders and processes, making them vulnerable to various

security threats such as data breaches, counterfeiting, and supply chain disruptions. By leveraging smart ledger technologies, which combine the benefits of blockchain and smart contracts, this paper aims to establish a transparent, immutable, and automated framework for regulating data sharing and processing activities within supply chains.

[15] This research paper introduces Eunomia, a novel approach designed to enable anonymous and secure digital forensics in vehicular environments, leveraging blockchain technology. Vehicular digital forensics involves the collection, analysis, and preservation of digital evidence from vehicles, which is crucial for investigating accidents, cyber- attacks, and other incidents. However, existing methods often lack anonymity and may be susceptible to tampering or data breaches. Eunomia addresses these challenges by integrating blockchain technology to provide a decentralized and immutable ledger for storing forensic data while ensuring the anonymity of vehicle owners and users.

[16] This research paper proposes the concept of adaptive observability tailored for microservice architectures to ensure forensic readiness. Microservice systems, with their distributed nature and dynamic behaviour, pose challenges for traditional forensic investigations due to the complexity of tracing and monitoring individual service interactions. The concept of adaptive observability involves the dynamic instrumentation and monitoring of microservices to capture relevant data for forensic analysis while minimizing overhead and ensuring scalability. This paper will delve into the design and implementation of adaptive observability mechanisms, including techniques for fine-grained logging, distributed tracing, and anomaly detection, optimized for microservice environments.

[13] This research paper proposes a novel log management scheme leveraging hybrid blockchain technology to enhance the security and non- repudiation capabilities of smart grid systems. Smart grids, characterized by their decentralized nature and reliance on digital communication, generate vast amounts of data crucial for monitoring and managing energy distribution. However, ensuring the integrity and authenticity of this data is challenging due to potential tampering and disputes. The proposed scheme combines the benefits of both public and private blockchains to establish a secure and scalable log management infrastructure for smart grids.

[17] This research paper presents a comprehensive evidence management system powered by blockchain technology. Traditional evidence

management systems often face challenges related to data integrity, security, and transparency. Leveraging blockchain's decentralized and immutable nature, the proposed system aims to address these challenges by providing a secure and transparent platform for managing various types of evidence, such as legal documents, digital artifacts, and physical objects. The system utilizes blockchain to create an indelible record of evidence custody, ensuring its integrity and authenticity throughout its lifecycle. Smart contracts are employed to automate and enforce the rules governing evidence handling, including chain of custody, access control, and audit trails.

[7] The paper aims to provide a comprehensive survey of the utilization of blockchain technology for enhancing security and forensic management in edge computing environments within the realm of information technology (IT). Edge computing, characterized by decentralized processing and data storage at the network edge, presents unique challenges for security and forensic investigations due to its distributed and heterogeneous nature. Blockchain technology offers promising solutions by providing decentralized consensus, tamper-proof data storage, and transparent audit trails.

[5] Digital forensics plays a critical role in investigating cybercrimes and ensuring the integrity of digital evidence for legal proceedings. However, maintaining the chain of custody, which documents the handling and transfer of evidence, poses significant challenges in traditional systems. Blockchain technology offers a promising solution by providing a decentralized and tamper-proof ledger to record every transaction or interaction with digital evidence.

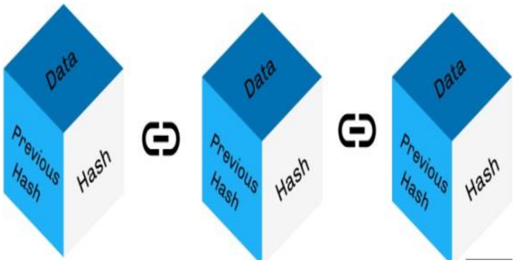
## III. ISSUES WITH THE CONVENTIONAL JUDICIAL APPROCH

The traditional approach involves recording all actions connected to collecting and submitting evidence, from its creation to its submission in court, using manual documents. Details like the time and location of the evidence's origin, physical descriptions, information on who handled it and for how long, the unique identifiers of the investigators, and the procedure for transferring evidence between people are all included in the recorded data.
But there are a few things that can prevent important evidence from being admitted into court, rendering it legally inadmissible. Due to their lack of knowledge, plaintiffs frequently rely on advocates to help them through the complicated legal processes, which results in expensive fees. This dependency

could result in unfavourable outcomes like lying, overspending, etc.
Accountability is a problem because, rather than taking accountability, court officials may blame delays on work-related stress, which will ultimately affect the common person. Since the current system cannot review and examine evidence, evidence provenance is likewise vulnerable to manipulation. Lack of openness compromises transparency and makes it possible for court officials to misuse information without other stakeholders knowing about it.
Records are tough to combine in the existing system because data integration is hard, especially when a case crosses several zones. Scalability becomes problematic when legal processes span multiple states or countries. In order to tackle these obstacles and streamline the process of managing and submitting evidence, a blockchain- based solution is suggested. Blockchain technology offers the potential to improve data integration, accountability, and transparency while reducing the risk of evidence manipulation and scalability problems in the legal system.

## IV. FUNCTIONS OF BLOCKCHAIN

As illustrated in the diagram, a blockchain functions as a chain of interconnected blocks, linked together through a hashing algorithm.



The distributed ledger, supported by blockchain technology, is renowned for its unalterable nature, robust security features, and decentralized structure. The authors conducted a research study focusing on prevalent practices for sharing medical records. They identified various challenges associated with traditional methods, including privacy issues, centralized data storage, and trust-related concerns. Consequently, their attention shifted towards exploring blockchain-supported methods for exchanging medical data, encompassing both public and private blockchain alternatives.

The framework underlying any application supported by blockchain relies on fundamental principles such as transactions, peer-to-peer

networks, consensus algorithms, decentralized ledgers, and smart contracts. Transactions involve any form of communication or interaction between nodes in a peer-to-peer network, ranging from cryptocurrency transfers to file ownership, data storage, and data access. In a peer-to-peer network, all nodes share similar capabilities or resources, eliminating the conventional client-server distinction. The consensus algorithm serves as the mechanism by which network nodes collectively decide whether to approve or reject a given transaction. The decentralized ledger, accessible to all nodes, records transactions through a consensus mechanism.

A smart contract is software specifically designed to facilitate agreements between parties capable of communication, triggered by specific system events. Blockchain technology finds diverse applications in industries like insurance and digital asset management. Notably, in the legal system, it securely digitizes document storage through distributed ledger technology. Peer-to-peer networks ensure secure data sharing among all relevant parties. The ledger, featuring encrypted information, ensures complete transparency by documenting every instance of data access. Any attempt to compromise data integrity can be traced and verified. The proposed model suggests combining back-end data storage with blockchain technology, storing digital evidence in data storage while recording all evidence access transactions in theblockchain. Fuzzy hashing is a technique used in cybersecurity and digital forensics to compare files or data sets for similarity based on their content rather than relying on traditional cryptographic hashes. Fuzzy hashing algorithms compute a hash value that represents the content of a file or data set in such a way that similar content produces similar hash values, even if the files are not identical.

## V. FUNCTIONS OF DEEP LEARNING ALGORITHM

Deep learning algorithms perform a multitude of functions across various domains, showcasing their versatility and power in handling complex tasks. One primary function is feature learning, where these algorithms autonomously identify and extract relevant features from raw data, enabling them to recognize patterns and representations. Another crucial role is classification, as deep learning models excel in categorizing and assigning labels to input data based on learned features. These algorithms are also adept at regression tasks, predicting continuous values with high accuracy. In the realm of image and speech recognition, deep learning algorithms demonstrate remarkable capabilities by interpreting and understanding complex visual and auditory information. Moreover, they play a pivotal role in natural language processing tasks, comprehending and generating human-like language. The ability to optimize and adapt their parameters through training allows these algorithms to continually improve their performance over time.

### A. DEEP LEARNING LIFE CYCLE

The life cycle of deep learning involves several stages from problem definition to model deployment. Here's a detailed note on each stage along with a simplified diagram:

Problem Definition: Identify the problem that can benefit from deep learning solutions. Define the objectives and constraints of the problem. Determine the availability and quality of data for training.

Data Collection: Gather relevant data for the problem at hand. Ensure data quality, cleanliness, and representativeness. Split the data into training, validation, and test sets.

Data Preprocessing: Clean and preprocess the data to handle missing values and outliers. Normalize or standardize the data to ensure consistent scales. Augment data if necessary to increase diversity for better generalization.

Model Design: Choose the appropriate type of deep learning architecture (e.g., neural network, convolutional neural network, recurrent neural network). Define the number of layers, neurons, and activation functions. Configure parameters like learning rate, batch size, and optimization algorithms.

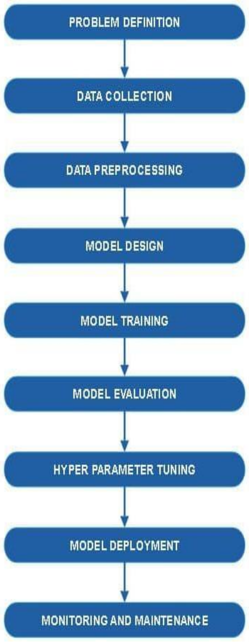
Model Training: Feed the training data into the model. Use a loss function to measure the difference between predicted and actual values. Optimize the model by adjusting weights through backpropagation. Monitor performance on the validation set to prevent overfitting.

Model Evaluation: Assess the model's performance on the test set. Analyse metrics like accuracy, precision, recall, and F1 score. Identify areas for improvement and potential adjustments.

Hyperparameter Tuning: Fine-tune hyperparameters based on performance evaluation. Experiment with different configurations to optimize the model's performance.

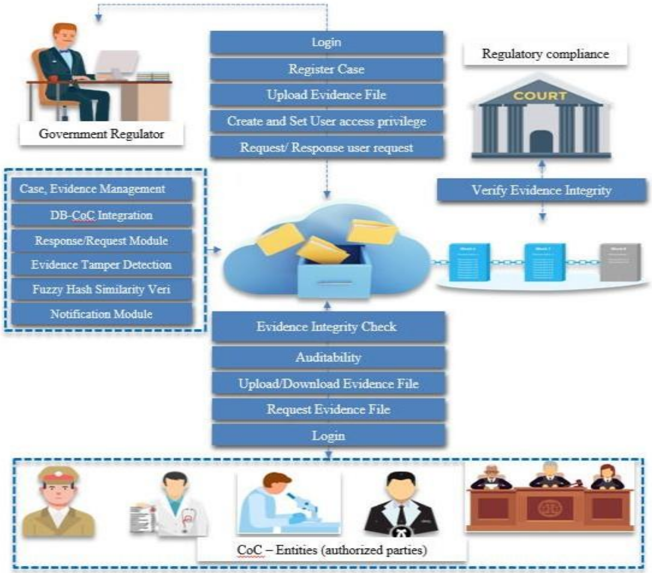
Model Deployment: Integrate the trained model into the production environment. Develop APIs or interfaces for model interaction. Implement monitoring mechanisms for ongoing performance evaluation.

Monitoring and Maintenance: Continuously monitor the model's performance in the real-world environment. Update the model as needed with new data or improved algorithms. Address issues related to concept drift or changing data patterns.



## VI. PROPOSED MODEL

### A. SYSTEM MODEL


Login
Register Case
Upload Evidence File
Create and Set User access privilege
Request/ Response user request
Government Regulator
Regulatory compliance
COURT
Verify Evidence Integrity
Case, Evidence Management
DB-CoC Integration
Response/Request Module
Evidence Tamper Detection
Fuzzy Hash Similarity Veri
Notification Module
Evidence Integrity Check
Auditability
Upload/Download Evidence File
Request Evidence File
Login
CoC – Entities (authorized parties)

In order to solve the weaknesses in managing digital evidence in legal proceedings, compliance processes, and investigations, a comprehensive solution is presented by the proposed model. It recognizes that in order to improve the integrity of digital evidence, a secure storage model is required due to the dangers connected with data tampering, unlawful access, and storage system defects. The creation of a novel architecture that combines deep learning algorithms with blockchain technology to create a strong Chain of Custody (CoC) and successfully identify tampering is essential to this strategy. The design uses blockchain technology to establish a private network amongst the investigation's stakeholders.
This software uses advanced deep learning methods customized for various kinds of digital evidence to identify alterations. For example, bidirectional encoder representations from Transformers (BERT) are used for Word Document Embedding, and Convolutional Neural Networks ( are used for image analysis. Video frames are examined using Temporal Convolutional Networks (TCNs), and audio spectrogram analysis is performed with Hidden Markov Models (HMMs). Fuzzy hash functions are another feature of the approach that helps forensic investigators manage legal modifications of digital evidence while standardizing forensic procedures.

## B. WORK FLOW

1. Smart contracts is deployed by the government regulatory or admin
2. Government regulator will login into the system and Register the new case as a block
3. After registering the new case as a new block the government regulator will upload the case evidence one by one
4. Government regulator set the user privileges for the evidence to be accessed by the authorized parties and the government regulator can request /respond to the user requests
5. The authorized parties can login into the system using specific pass and they can upload/download any evidence for the specific case, Request some evidence file, audit the file and they can also check the evidence integrity
6. Once the case block is added into the COC block chain network it can’t be modified and its integrity and confidentiality is maintained by some DL algorithms such as CNN, TCN, BERT and HMM 7.These algorithms are responsible for tamper detection of evidence

**FUZZY HASHING:**

Fuzzy hashing is not inherently specific to blockchain or deep learning. It's a method used primarily in the field of digital forensics and cybersecurity to identify similarities between files, detect variations of known malware, or identify duplicate files. However, it's possible to integrate fuzzy hashing techniques into blockchain analysis or deep learning systems as part of a broader approach to cybersecurity or forensic investigations. For example, fuzzy hashing could be used within blockchain analysis tools to identify similar or

potentially malicious transactions. Similarly, fuzzy hashing algorithms could be integrated into deep learning models to enhance their capabilities in detecting and analysing pattern in large datasets, including blockchain data.

Algorithm: Forensic Investigation with Fuzzy Hash

```
Load Fuzzy Hash Function
Input the digital files or data
define the path of the file
Read the file
file_content = file.read()
Generate fuzzy hashes for each digital file
hash_value = ssdeep.hash(file_content)
compare the hash value
similarity_score = ssdeep.compare(hash_1, hash_2)
if (similarity_score > 90)
Files are potentially similar
Else(Files are not similar)
```

HMM:

Audio Spectrogram Analysis with Hidden Markov Models (HMM) represents a sophisticated approach to understanding and interpreting sequential acoustic data. Spectrograms provide a time- frequency representation of audio signals, revealing intricate patterns and characteristics. In this context, Hidden Markov Models are employed to model the temporal dynamics inherent in audio sequences. HMMs excel at capturing complex relationships between acoustic features over time, making them well-suited for tasks such as speech recognition, speaker identification, and audio event detection.

The algorithm involves breaking down the audio signal into smaller time frames and extracting relevant features to construct a spectrogram. Hidden Markov Models are then trained on these spectrogram representations to learn the underlying patterns and transitions. The trained models can subsequently be used to analyse and recognize patterns in new audio data, offering a powerful tool for applications in fields such as audio forensics, surveillance, and voice-controlled systems.

Algorithm: Audio Spectrogram Analysis with HMM

```
1.    Load audio
2.    Initialize Gaussian HMM model
3.    Analyse Audio and Extract features
4.    positive_features = ExtractFeatures("positive_audio.wav")
5.    negative_features = ExtractFeatures("negative_audio.wav")
6.    log_likelihood_positive = AnalyzeAudio("unknown_audio.wav", positive_model)
7.    log_likelihood_negative = AnalyzeAudio("unknown_audio.wav", negative_model)

8.    if (log_likelihood_positive > log_likelihood_negative)
9.    Then
10.   The unknown audio is considered positive evidence
11.   else
12.   The unknown audio is considered negative or unrelated
13.   end if
```

TCN:

Temporal Convolutional Networks (TCN) are powerful architectures for sequence modeling and have been applied successfully in various domains, including video analysis. When used for Video Frame-level Analysis, TCN allows for efficient and effective processing of sequential data at the frame level.

Algorithm: video Analysis with TCN

```
1.    video_frames = extract_frames(video_path)
2.    frame_features = []
3.    for frame in video_frames:
4.    feature_vector = apply_tcn(frame)
5.    frame_features.append(feature_vector)
6.    tcn_model = train_tcn_model(frame_features)
7.    new_video_frames = extract_frames(new_video_path)
8.    new_frame_features = []
9.    for frame in new_video_frames:
10.   feature_vector = apply_tcn(frame)
11.   new_frame_features.append(feature_vectr
      )
12.   predicted_labels = tcn_model.predict(new_frame_features)
13.   decision =
post_process_predictions(predicted_labels
      )
14.   print("Video Analysis Decision:", decision)
```

BERT:

Word document embeddings using BERT entail leveraging BERT, a powerful pre-trained language model, to generate contextualized embeddings for words and documents. BERT, or Bidirectional Encoder Representations from Transformers, is known for its ability to

capture rich contextual information from text data. In this process, a word document is first tokenized into individual words or sub words, and then fed into the BERT model. BERT generates embeddings for each token, representing its context within the document. These embeddings capture semantic relationships and syntactic structures, enabling a deeper understanding of the document's content. To obtain a document-level embedding, the individual word embeddings are aggregated, typically by averaging or summing them. The resulting document embedding encapsulates the semantic meaning and context of the entire document in a high-dimensional vector space. This approach has various applications, including document classification, information retrieval, and semantic similarity analysis.

Algorithm: Word Document Embedding's using BERT
1.Load BERT model and tokenizer
2.bert_model = BertModel.from_pretrained('bert- base-uncased')
3.tokenizer = BertTokenizer.from_pretrained('bert- base-uncased')
4.Define the Function to embed word document 5.def embed_word_document(word_document): 6.Tokenization
7.Obtaining embeddings
8.embeddings = outputs.last_hidden_state 9.Aggregating document embedding (e.g., using mean)

CNN:
Image Analysis with Convolutional Neural Networks (CNNs) involves employing deep learning techniques to extract meaningful features and make predictions from images. CNNs have revolutionized image analysis tasks due to their ability to automatically learn hierarchical representations directly from pixel values, alleviating the need for handcrafted feature engineering. The process begins with loading and preprocessing the image dataset, which may include tasks such as resizing, normalization, and data augmentation to improve model generalization. Next, a CNN architecture is defined, typically comprising convolutional layers followed by activation functions like ReLU, pooling layers, and fully connected layers.

Algorithm: Image Analysis with Convolutional Neural Networks (CNN)
1. Load image dataset containing labeled images.
2. Preprocess images (resize, normalize, augment).
3. Define CNN architecture (e.g., VGG, ResNet).
4. Compile CNN model with appropriate loss and optimizer.
5. Train CNN model on the training dataset. 6.model.fit(train_images, train_labels, epochs=10, validation_data=(test_images, test_labels))
7. Evaluate model performance on the test dataset. 8.test_loss, test_acc = model.evaluate(test_images, test_labels)

9. Fine-tune model if necessary.
10. Make predictions on new images using the trained model.
11.predictions = model.predict(new_images)

## VII. BENEFITS AND LIMITATIONS

Improved Security: By leveraging blockchain technology, the proposed model establishes a secure chain of custody (CoC) for digital evidence. This ensures that the integrity and authenticity of evidence are maintained throughout the investigation process, reducing the risk of tampering or unauthorized access.

Tamper Detection: Deep learning models such as Convolutional Neural Networks (CNN), Hidden Markov Models (HMM), and Transformer Convolutional Networks (TCN) are employed for detecting tampering in various types of digital files including images, audio, video, and documents. This enhances the reliability of the evidence by identifying any alterations or modifications made to the data. Standardisation of Forensics Processes: The utilization of fuzzy hash functions standardizes forensic processes, enabling investigators to effectively deal with permissible alterations of digital evidence. This consistency in approach enhances the quality and reliability of the investigation outcomes. Data Provenance and Traceability: The proposed architecture ensures complete data provenance and traceability, providing a clear record of the chain of custody events. This enhances transparency and accountability throughout the investigation lifecycle, making it easier to track the handling of digital evidence and maintain its integrity.

Robust Information Integrity: By permanently and immutably storing the evidence on a private permissioned encrypted blockchain ledger, the model ensures robust information integrity. This prevents unauthorized modifications or deletions of evidence, thereby preserving its integrity and reliability.

Complexity: Implementing the proposed DB-CoC architecture may be complex and require significant expertise in blockchain technology, deep learning, and forensic analysis. This could pose challenges for organizations with limited resources or technical capabilities.

Resource Intensive: Deep learning algorithms such as CNN, HMM, BERT, and TCN may require substantial computational resources and data for training and inference. This could lead to increased costs and infrastructure requirements, especially for large-scale investigations or organizations with limited IT resources.
Privacy Concerns: While blockchain technology provides a secure and immutable ledger for storing digital evidence, it also raises privacy concerns. The use of private permissioned blockchains may

mitigate some of these concerns, but careful consideration must be given to data protection and compliance with regulations such as GDPR. Scalability: The scalability of the proposed model may be a concern, especially in cases where a large volume of digital evidence needs to be processed and analysed. Ensuring efficient handling of increasing data volumes and maintaining performance could be challenging over time.
Integration Challenges: Integrating the proposed architecture into existing forensic workflows and IT infrastructure may pose challenges. Compatibility issues, data migration, and training requirements for personnel could impact the adoption and effectiveness of the model.

## VIII. CONCLUSION AND FUTURE WORK

The proposed DB-CoC architecture presents a comprehensive solution to the challenges associated with securing and maintaining the integrity of digital evidence in investigations. By leveraging blockchain technology for establishing the Chain of Custody (CoC) and employing deep learning models for tamper detection across various file types, the architecture offers a robust mechanism to preserve evidence and ensure its authenticity throughout the investigation lifecycle. Additionally, the utilization of fuzzy hash functions enhances the forensic process by standardizing procedures and addressing permissible alterations in digital evidence.The DB-CoC architecture not only provides a secure storage model but also offers complete data provenance, traceability, and assurance in handling digital evidence.
By enforcing a standard approach and enhancing the quality of the investigation process, it fosters trust among stakeholders involved in collecting, storing, analyzing, and interpreting digital evidence. There are several avenues for further research and development. Firstly, refining and optimizing the deep learning models for tamper detection across different file types could enhance the accuracy and efficiency of the architecture. Additionally, exploring advancements in blockchain technology, such as integrating smart contracts for automated verification of chain of custody events, could streamline the investigation process further. Moreover, conducting real-world testing and validation of the DB-CoC architecture in various investigative scenarios would provide valuable insights into its practical applicability and effectiveness. Lastly, continuous monitoring of emerging threats and evolving forensic techniques will be essential to adapt and enhance the architecture to meet the evolving needs of digital investigations.

## IX. REFERENCES

[1] Nieto, R. Roman, and J. Lopez, ‘‘Digital witness: Safeguarding digital evidence by using secure architectures in personal devices,’’ IEEE Netw., vol. 30, no. 6, pp. 34– 41, Nov. 2016.
[2] Shancang Li, Tao Qin, Geyong Min, “Blockchain- Based Digital Forensics Investigation Framework in the Internet of Things and Social System”, IEEE Transactions on Computational Social Systems, vol. 6, Issue. 6, July 2019
[3] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, ‘‘Block-DEF: A secure digital evidence framework using blockchain,’’ Inf. Sci., vol. 491, pp. 151–165, Jul. 2019.
[4] Gregory Epiphaniou, Prashant Pillai, Mirko Bottarelli, Haider Al-Khateeb, Mohammad Hammoudesh, Carsten Maple, “Electronic Regulation of Data Sharing and Processing Using Smart Ledger Technologies for Supply-Chain Security”, IEEE Transactions on Engineering Management vol. 67, Jan 2020.
[5] Mrunali Chopade, Sana Khan, Uzma Shaikh, Renuka Pawar, “Digital Forensics: Maintaining Chain of Custody Using Blockchain”, 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),
March 2020
[6] S. Ghimire, J. Y. Choi, and B. Lee, ‘‘Using blockchain for improved video integrity verification,’’ IEEE Trans. Multimedia, vol. 22, no. 1, pp. 108–121, Jan. 2020.
[7] Zhuofan Liao, Xiang Pang, Jingyu Zhang, Bing Xiong, Jin Wang, “Blockchain on Security and Forensics Management in Edge Computing for IoT: A Comprehensive Survey”, oct 2021
[8] M. Li, C. Lal, 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.
[9] Amerini, A. Anagnostopoulos, L. Maiano and L. Celsi, "Deep learning for multimedia forensics. Foundations and Trends", Comput. Graph. Vis., vol. 12, no. 4, pp. 309-457, 2021.

[10] A. Shafarenko, ‘‘A PLS blockchain for IoT applications: Protocols and architecture,’’ Cybersecurity, vol. 4, no. 1, pp. 1–17, Feb. 2021.

[11] G. Horsman, "Defining principles for preserving privacy in digital forensic examinations", Forensic Sci. Int. Digit. Invest., vol. 40, Mar. 2022.

[12] Hang M. Elgohary, Saad M. Darwish, Saleh Mesbah Elkaffas, “Improving Uncertainity in Chain of Custody for Image Forensics Investigation Applications”, IEEE Access, vol. 10, Jan 2022

[13] Tuan-Vinh Le, Chien-Lung Hsu, Wei-Xin Chen,” A Hybrid Blockchain-Based Log Management Scheme With Nonrepudiation for Smart Grids”IEEE Transactions on Industrial Informatics, vol. 18, Sep 2022

[14] Hany M. Elgohary, Saad M. Darwish, Saleh Mesbah Elkaffas, “Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications”IEEE Access, Jan 2022

[15] Meng Li, Yifei Chen, Chhagan Lal, Mauro Conti, Mamoun Alazab, Donghui Hu, “ Eunomia: Anonymous and Secure Vehicular Digital Forensics Based on Blockchain”, IEEE Transactions on Dependable and Secure Computing, vol. 20, Feb 2023

[16] Davi Monteiro, Yijun Yu, Andrea Zisman, Bashar Nuseibeh,” Adaptive Observability for Forensic-Ready Microservice Systems”, IEEE Transactions on Services Computing, vol.16, Oct 2023.

[17] Shyam Mehta, K. Shantha Kumari, Paras Jain, Harshal Raikwar, Shubham Gore,” Blockchain driven Evidence Management System”,2023 3rd International conference on Artificial Intelligence and Signal Processing (AISP), IEEE, June 2023

[18] R. Stoykova, ‘‘The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations,’’ Comput. Law Secur. Rev., vol. 49, Jul. 2023.

[19] Qian Ren, Yue Li, Yingjun Wu, Yuchen Wu, Hong Lei, Lei Wang, Bangdao Chen, “DECLOAK: Enable Secure and Cheep Multi-Party Transanctions on Legacy Blockchain by a Minimally Trusted TEE Network”, vol.18, no.6, July 2023.