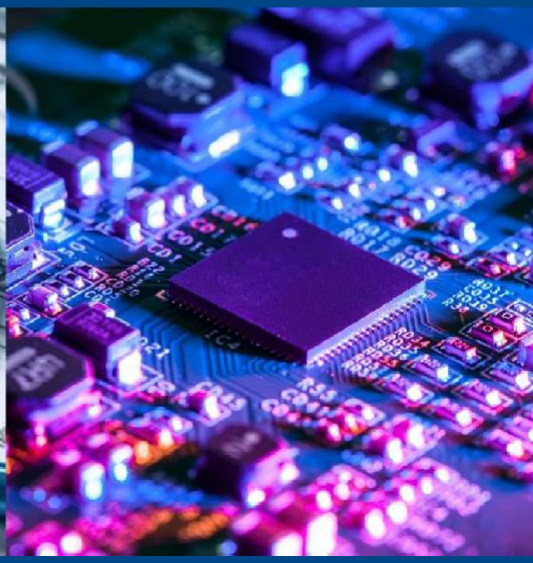
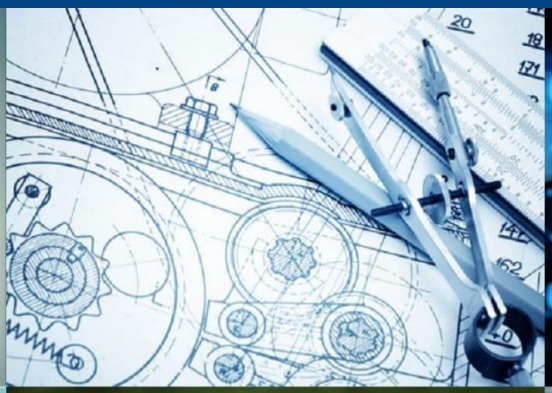
ISSN: 2582-7219

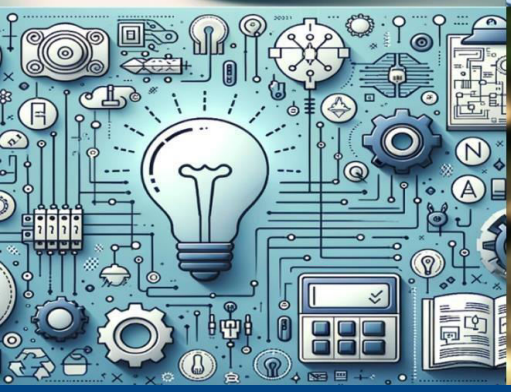




International Journal of Multidisciplinary Research in Science, Engineering and Technology

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



Impact Factor: 8.206 **Volume 8, Issue 7, July 2025**

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807046

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Blockchain and Deep Learning for Ensuring Integrity and Chain of Custody of Digital Evidence

MR. J. Eswarapandian [1], Ms. M. Vijayalakshmi [2]

PG Scholar, Department of Master of Computer Applications, RVS College of Engineering, Dindigul, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Applications, RVS College of Engineering, Dindigul, Tamil Nadu, India[2]

ABSTRACT: The secure storage model for digital forensics addresses the primary issues with preserving and safeguarding digital data, marking a significant advancement in the field. This approach uses the best key generation techniques and the most contemporary encryption algorithms to guarantee the confidentiality and integrity of the data during the course of the inquiry. An intelligent advancement of digital forensics to protect against online hacking is cloud forensics. However, the credibility of digital evidence is diminished by centralized evidence collection and maintenance. An Infrastructure as a Service (IaaS) cloud platform's digital forensics architecture is an essential component meant to make the gathering and safeguarding of evidence while maintaining the authenticity and provenance of digital items using cloud-based techniques. In the context of forensic investigations, this architecture combines a variety of modules and techniques to handle the unique challenges modeled by cloud computing (CC) environments. This study uses the Authentication with Optimal Key Generation Encryption (DFA-AOKGE) technique to create a novel digital forensic architecture. The DFA-AOKGE method's primary goal is to spread data among multiple peers for data gathering and secure storage using a BC-distributed design. Furthermore, the Secure Block Verification Mechanism (SBVM) is used by the DFA-AOKGE model for the authentication process. The hidden keys can also be generated by applying the model known as the Enhanced Equilibrium Optimizer (EEO). Additionally, the data is encrypted using a multikey homomorphic encryption (MHE) technique before being stored on the cloud server. The DFA-AOKGE methodology's simulation value occurs in terms of several factors. According to the simulation results, the DFA-AOKGE system performs noticeably better than other current methods across a range of metrics.

KEYWORDS: Digital Evidence, Blockchain, Chain of Custody (CoC), Deep Learning, Tamper Detection, Digital Forensics.

I. INTRODUCTION

Leading digital analyses are now necessary due to the rise in cyberattacks and data exploitation. Reliability and standardization for improved performance have become essential for minimizing human errors brought on by unrelated evidence [1]. The majority of forensic artifacts are Shuangqing Wei was the assistant editor who oversaw the manuscript's evaluation and gave the go-ahead for publication. important since they provide proof of an event when they are analyzed and processed. Even though there are forensic artifacts in a court of law, they can be examined and require verification and cross-examination.Maintaining the Confidentiality, Integrity, and Availability (CIA) triad—accessibility, integrity, and confidentiality—requires digital proof[2].Because digital evidence may contain sensitive information like credit card numbers and other unique identifiers, its confidentiality should be protected. Strict access control is necessary to protect the evidence, or an encryption method can be used to ensure that only investigators or authorized parties can access the material proof [3]. Verifying the digital evidence's integrity is an important step in some digital analysis since the investigator must show that the evidence hasn't been altered or falsified in any way.

A forensic copy of the original evidence, a chain of custody, and software logs are kept in order to do this. As stated in the documentation, the advancement enabled the inspector to acquire the proof that was also sought [4]. During the time of collection and storage, the forensic hash of the evidence must be taken into consideration multiple times to ensure that the investigator's approach is broad and cannot modify the evidence in any way, and the original evidence could not be changed [5]. Therefore, it may be advantageous to use a protective storage approach to improve the research process and safeguard any sensitive data collected. Both small and large enterprises, as well as individual individuals, are impacted by a similar problem with digital forensic ready models. These techniques efficiently collect

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

evidence, thus procedures for storing and safeguarding it might be crucial to ensuring its validity and authenticity [6]. A cloud forensics model based on blockchain (BC) offers an effective way to predict privacy breaches in cloud services. This approach incorporates immutability the openness of BC technology with cloud forensics expertise to enhance privacy and security [7]. Although information and services may be provided, cloud environments rely on a cloud platform. It is a private cloud, public cloud, or hybrid cloud infrastructure. Various information sources inside the cloud platform have been collected and tracked for research purposes in relation to data gathering [8]. It includes network traffic, user activity, logs, system activity, and other pertinent data. One of the most effective cloud forensics techniques for preserving higher-level security is user authentication. Protecting evidence from unauthorized users is now a crucial objective [9]. For effective authentication, one-time passwords (OTPs) and email verification could be used. Possibly BC-assisted cloud forensic model has robust authentication, which is necessary for evidence sources, and it is protected [10]. The Authentication with Optimal Key Generation Encryption (DFA-AOKGE) technique is used in this paper to provide a revolutionary digital forensic architecture. The DFA-AOKGE The approach is innovative in that it incorporates a multi-key homomorphic encryption technology and a BC-distributed strategy for decentralized data allocation, ensuring secure and transparent digital forensic processes. The DFA-AOKGE technique uses a BC-distributed architecture to disperse data among multiple peers for safe storage and evidence gathering. Furthermore, the Secure Block Verification Mechanism (SBVM) is used by the DFA AOKGE approach for authentication. Moreover, the Enhanced Equilibrium Optimizer (EEO) method can be used to create the secret keys. Additionally, the data is encrypted using a multikey homomorphic encryption (MHE) technique and stored in the server in the cloud. The suggested method strengthens the security of digital forensic data by combining encryption and authentication in a synergistic way. By ensuring that only authorized workers with legitimate credentials can enter, authentication devices prevent unauthorized access. At the same time, encryption protects the integrity and confidentiality of the stored data, making it resistant to unauthorized access or alteration. In addition to providing a robust defense against potential security breaches, the seamless integration of encryption and authentication validates a comprehensive model for secure digital forensic evidence, enhancing the overall integrity and privacy of crucial data during the investigation process. A variety of measures are used to experimentally validate the DFA-AOKGE approach. The following is a summary of the study's main contributions:

• Introduces DFA-AOKGE, a novel digital forensic design. This affects Optimal Key Generation Encryption authentication. This architecture represents an innovative method to raise the security and effectiveness of digital forensic processes.
• Incorporates a BC-distributed strategy for sharing data among numerous peers. This addition gives digital forensic data more flexibility and integrity by certifying decentralized data collection and secure storage.
• As part of the authentication procedure, the SBVM is executed. By providing a reliable way to verify the accuracy of data and guaranteeing the integrity of digital forensic evidence, this gadget enhances the method's safety.
explains how to generate secret keys using the EEO approach. This addition strengthens the system's cryptographic capabilities, offering a secure and effective model for generating secret keys that are essential for data security and encryption.
• Employs a multi-key homomorphic encryption approach to encrypt data that has been stored on a cloud server. This novel encryption approach significantly contributes to the confidentiality and defense of forensic evidence by protecting and maintaining the privacy of calculations.

II. EXISTING SYSTEM

Nowadays, forensic software is used as better evidence for the process of the description and identification of the electronic user, digital signature and automatic audit trail, etc. Still, there is a great distance from the usual chain of custody software to the effective questions of the court and users. Nowadays, this process is executed by the process of CoC. The CoC is a set of consecutive documentation that records the order of custody, its control, transfer, analysis, and physical or electronic evidence. CoC contains unsafe steps during the process of investigation and at the time of submitting the evidence in court.The current traditional digital forensic process lacks standardized procedures and mechanisms making it inherently vulnerable to various tampering and forgery occurrences against the recent cybercrime incidents.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

III. PROPOSED SYSTEM

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.

- **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.

- **Deep Learning Models for Tamper Detection**

Different deep learning models are proposed for tamper detection in various types of files, including Image with CNN, Word Document Embeddings using BERT, Video Frame-level Analysis with TCN, Audio Spectrogram Analysis with HMM, and PDF Document Structure Analysis.

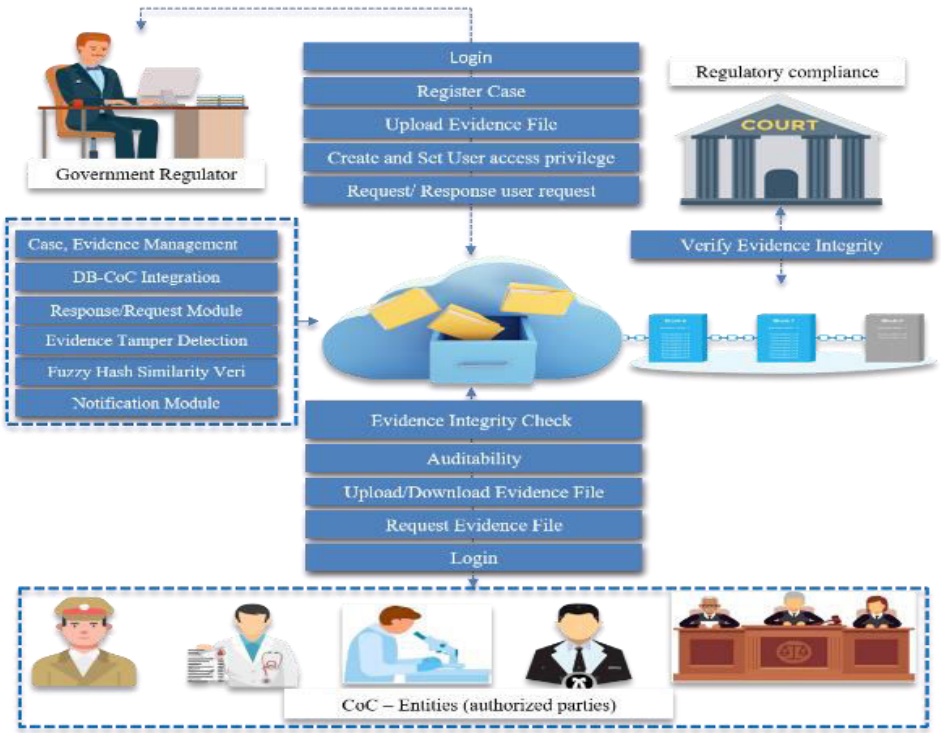
- **Fuzzy Hash Functions**

The utilization of fuzzy hash functions is highlighted, enabling forensic investigators to handle permissible alterations of digital evidence. This involves standardizing forensic processes to ensure consistency and reliability.

- **Data Provenance and Traceability**

The DB-CoC architecture promises complete data provenance and traceability, ensuring trust between chain of custody events during the collection, storage, analysis, and interpretation of digital evidence.

IV. SYSTEM ARCHITECTURE



© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807046

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

The architecture diagram illustrates a secure Digital Evidence Management System designed to ensure the integrity, confidentiality, and auditability of digital evidence throughout its lifecycle. At the top, the Government Regulator plays a supervisory role, responsible for registering cases, uploading evidence, setting user access privileges, and handling request/response interactions. The core of the system relies on cloud storage, which securely hosts all evidence files and integrates with multiple modules such as case and evidence management, chain of custody (CoC) database integration, tamper detection, fuzzy hash similarity verification, and a notification system.

V. RESULTS

This figure illustrates the structured process of documenting the sequence of custody, control, transfer, analysis, and disposition of digital evidence. It highlights how each authorized entity interacts with the evidence, ensuring a tamper-proof and traceable record of every action.

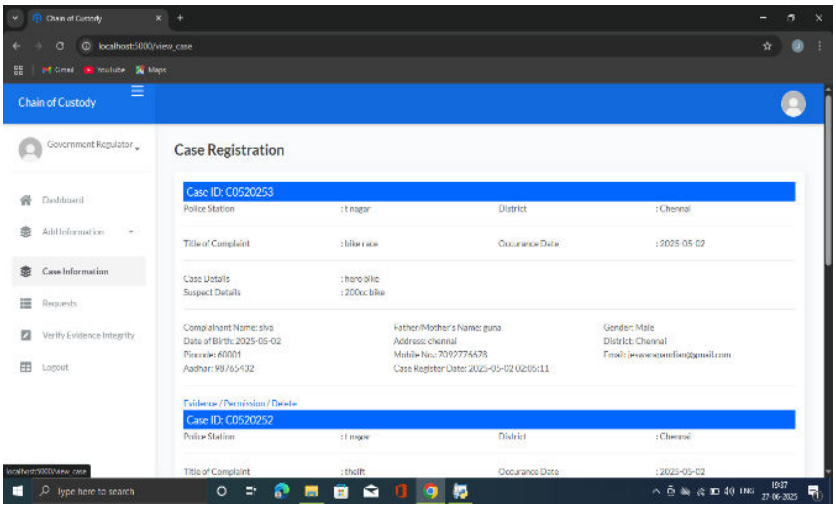


Fig 5.1 Chain of custody (COC)

This figure represents the role of the government authority in managing the digital evidence system. The regulator is responsible for case registration, assigning user privileges, uploading evidence, and maintaining overall governance and compliance with legal standards.

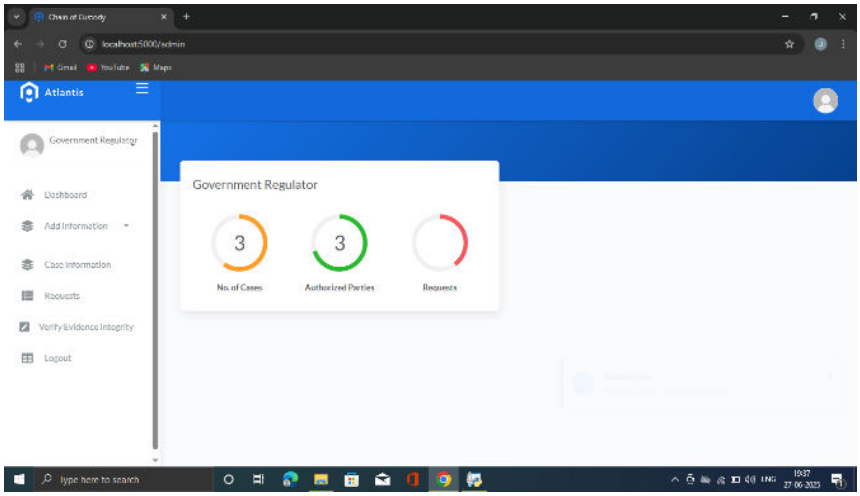


Fig 5.2 Government Regulator

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807046

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Depicted here is the secure access interface used by all system participants. It ensures that only authenticated and authorized users can interact with the system, supporting role-based access control and protecting sensitive evidence data.

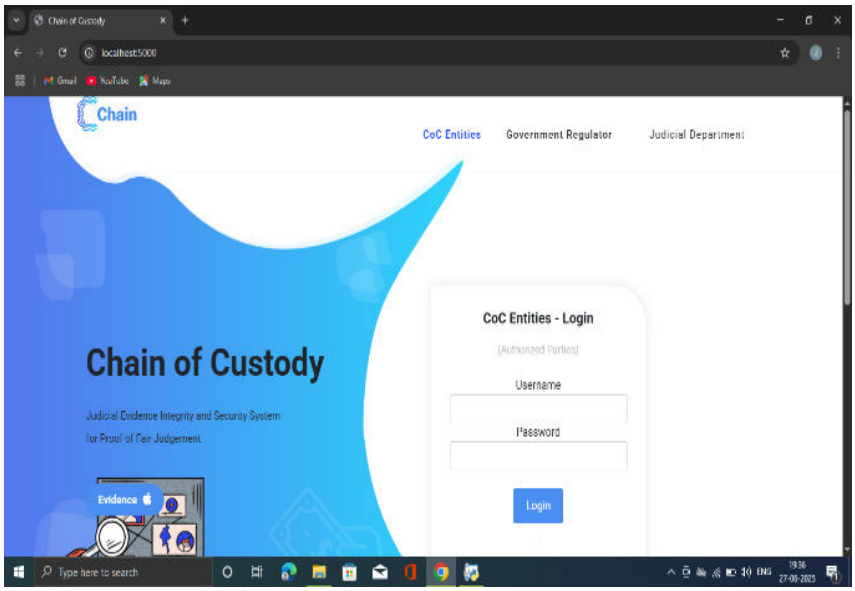


Fig 5.3 Login Page

This figure showcases the involvement of the judiciary in the digital evidence process. The department verifies the integrity and authenticity of the evidence and ensures its compliance with court requirements, making it admissible for legal proceedings.

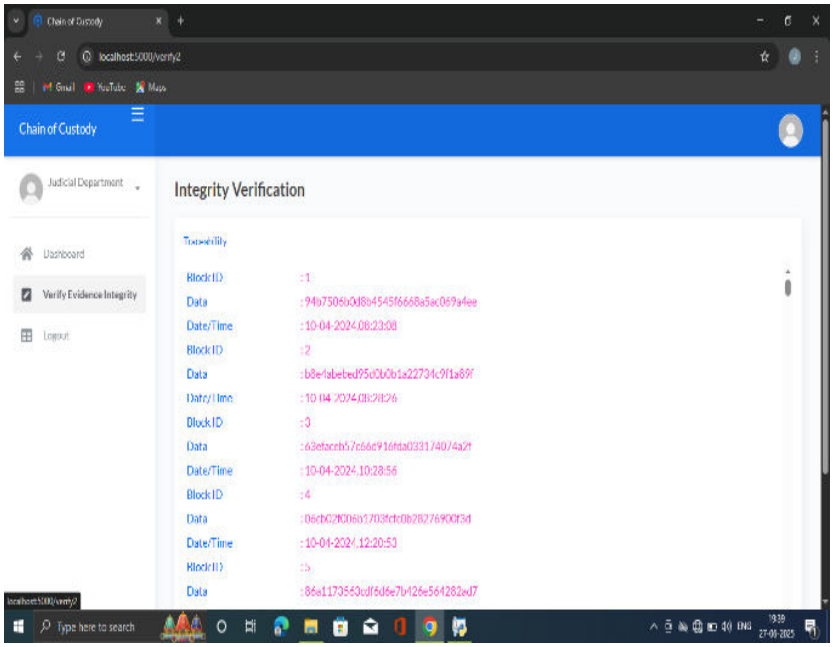


Fig 5.4 Judicial Department

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

VI. CONCLUSION

The integration of Blockchain and Deep Learning technologies provides a robust framework for ensuring the integrity and chain of custody (CoC) of digital evidence. Blockchain offers a decentralized, tamper-proof ledger that records every action taken on the evidence, ensuring transparency, auditability, and non-repudiation. This immutable record strengthens the legal admissibility of evidence by maintaining a verifiable trail of its handling.

VII. FUTURE ENHANCEMENTS

A Hybrid Blockchain-Deep Learning Model for Robust Digital Evidence Integrity and Chain of Custody Management In the digital age, the integrity and traceability of digital evidence are critical to ensuring justice and maintaining trust in forensic investigations. Traditional methods of managing digital evidence often lack transparency, are prone to tampering, and fail to provide a verifiable chain of custody. This paper presents a hybrid model that integrates blockchain technology with deep learning to address these challenges. Blockchain ensures immutability, decentralized access, and traceable transactions, making it ideal for securing digital evidence records and maintaining an auditable chain of custody. Concurrently, deep learning algorithms are employed to detect anomalies, authenticate evidence, and assist in forensic analysis by automatically identifying patterns and irregularities. The proposed model enhances security, reliability, and efficiency in evidence management, while enabling real-time verification and automated decision support. Experimental results demonstrate the robustness of the system against data tampering, unauthorized access, and manipulation, indicating its potential as a transformative solution in digital forensics and legal proceedings.

REFERENCES

1. P. M. Bachiphale and N. S. Zulpe, "Optimal multisecret image sharing using lightweight visual sign-cryptography scheme with optimal key generation for gray/color images," *Int. J. Image Graph.*, Jul. 2023, Art. no. 2550017. [Online]. Available: https://doi.org/10.1142/S0219467825500172
2. G. Kumar, R. Saha, C. Lal, and M. Conti, "Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications," *Future Gener. Comput. Syst.*, vol. 120, pp. 13–25, Jul. 2021.
3. L. Raji and S. T. Ramya, "Secure forensic data transmission system in cloud database using fuzzy based butterfly optimization and modified ECC," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 9, p. e4558, Sep. 2022.
4. E. A. Abdel-Ghaffar and M. Daoudi, "Personal authentication and cryptographic key generation based on electroencephalographic signals," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 5, May 2023, Art. no. 101541.
5. P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan, "Enhancing blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," *Mater. Today, Proc.*, vol. 37, pp. 2653–2659, 2021.
6. V. O. Nyangaresi, M. Ahmad, A. Alkhayyat, and W. Feng, "Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things," *Expert Syst.*, vol. 39, no. 10, p. e13126, Dec. 2022.
7. S. Nasreen and A. H. Mir, "Enhancing cloud forensic investigation system in distributed cloud computing using DK-CP-ECC algorithm and EKANFIS," *J. Mobile Multimedia*, vol. 19, no. 3, pp. 679–706, Feb. 2023.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com