Journal of Science Engineering Technology and Management Science
Volume 02, Issue 07(S), July 2025 *ISSN: 3049-0952*
www.jsetms.com *DOI: 10.64771/jsetms.2025.v02.i07(S).802-812*

OPTIMAL KEY GENERATION AND AUTHENTICATION FOR A SECURE STORAGE MODEL TO ENHANCE DIGITAL FORENSIC SECURITY

SHYAMALA NAGAJYOTHI
Assistant Professor
Matrusri Engineering College

To Cite this Article
Shyamala Nagajyothi, "Optimal Key Generation And Authentication For A Secure Storage Model To Enhance Digital Forensic Security", Journal of Science Engineering Technology and Management Science, Vol. 02, Issue 07(S), July 2025,pp: 802-812, DOI: http://doi.org/10.64771/jsetms.2025.v02.i07(S).pp802-812
Submitted: 13-06-2025 *Accepted: 21-07-2025* *Published: 28-07-2025*

OBJECTIVE

An increase in cyberattacks and data exploitation has developed the requirement for leading digital analyses. Standardization and reliability for better performances have become crucial for providing the minimum number of human errors due to irrelevant evidence

ABSTRACT

Secure storage model for digital forensics represents essential progress in the domain, addressing the major problems associated with protecting and maintaining digital evidence. This method employs recent encryption systems and optimal key generation methods to ensure the confidentiality and integrity of data throughout the investigative process. Cloud forensics is an intelligent development of digital forensics to be preserved against online hacking. But, centralized evidence gathered and preservation reduces the reliability of digital evidence. The architecture for digital forensics in an Infrastructure as a Service (IaaS) cloud platform is a crucial structure intended to simplify the collection and protection of evidence while preserving the integrity and origin of digital objects within cloud-based methods. This architecture integrates numerous modules and methods to address the exclusive tasks modeled by cloud computing (CC) environments in the framework of forensic investigations. This paper develops a new digital forensic architecture utilizing the Authentication with Optimal Key Generation Encryption (DFA-AOKGE) technique. The main intention of the DFA-AOKGE method is to use a BC-distributed design to allocate data between numerous peers for data collection and safe storage. Additionally, the DFA-AOKGE model uses the Secure Block Verification Mechanism (SBVM) for the authentication procedure. Also, the secret keys can be produced by the usage of the Enhanced Equilibrium Optimizer (EEO) model. Furthermore, the encryption of the data takes place using a multikey homomorphic encryption (MHE) approach and is then saved in the cloud server. The simulation value of the DFA-AOKGE methodology takes place in terms of different aspects. The simulation results exhibited that the DFA-AOKGE system shows prominent performance over other recent approaches in terms of different measures.

I. INTRODUCTION

BACKGROUND AND CONTEXT

The advancement of digital technologies has led to a rapid transformation in the way data is created, shared, and stored. While this evolution has brought convenience and efficiency to many sectors, it has also opened new doors for cybercrimes and digital fraud. From data breaches and financial fraud to identity theft and illegal data manipulation, digital crimes are not only increasing in frequency but also in sophistication. This has made **digital forensics** the science of identifying, preserving, analyzing, and presenting digital evidence—a critical component in modern-day criminal investigations and legal proceedings. Traditionally, digital forensic investigations have relied heavily on centralized data storage and manual verification techniques. While functional, these systems are prone to various vulnerabilities, including unauthorized access, data tampering, loss of audit trail, and difficulties in maintaining the integrity of digital evidence. Additionally, the absence of real-time evidence validation mechanisms increases the risk of presenting compromised data in judicial settings. As a result, the forensic community and cybersecurity professionals have emphasized the need for a more **secure, decentralized, and transparent framework** for evidence collection, storage, and validation. Blockchain technology, known for its immutable, distributed ledger system, has emerged as a promising solution to address many of these challenges. It offers a way to **record transactions and data in a verifiable and tamper-proof manner**, ensuring that once digital evidence is stored, it cannot be altered or erased without detection.

PROBLEM STATEMENT

Despite the critical role of digital evidence in criminal justice and corporate investigations, current forensic storage systems often suffer from significant drawbacks:

- **Centralized Storage Models**: Most existing systems store digital evidence in centralized databases, which creates a single point of failure. These systems are highly vulnerable to cyberattacks, unauthorized modifications, and data breaches.
- **Lack of Transparency and Traceability**: Without a verifiable trail of actions performed on the evidence, it is difficult to establish the chain of custody—a key requirement in legal proceedings.
- **Integrity Challenges**: Ensuring the evidence has not been tampered with is difficult without cryptographic proof or immutable storage.
- **Limited Real-Time Verification**: Existing systems lack mechanisms to quickly validate the authenticity of stored evidence using publicly verifiable systems.
- **Administrative Inflexibility**: Most systems lack role-based access control, making it challenging to separate responsibilities between evidence contributors and investigators or administrators.

These limitations can lead to compromised investigations, legal disputes, and even wrongful convictions or acquittals. Therefore, there is a pressing need for a solution that is **secure, transparent, traceable, and auditable**, providing all stakeholders with confidence in the forensic process.

OBJECTIVES OF THE PROJECT

The main objective of this project is to design and implement a **secure, blockchain-based digital forensic storage system** that leverages the power of decentralized technologies to ensure the integrity and authenticity of digital evidence. The system is developed using **Django** (a Python-based web framework) for the backend and **Ganache** (a local Ethereum blockchain simulator) for blockchain operations.

The key goals of the system are:

- To allow authenticated users to **upload digital evidence**, which is then hashed and securely stored both in the database and on the blockchain.

- To ensure **evidence immutability** through blockchain integration, using transaction hashes and timestamps as proof of authenticity.
- To maintain a reliable and transparent **chain of custody** for each piece of evidence.
- To empower administrators to **view, verify, approve, or reject** evidence while maintaining a full audit trail.
- To provide a **transaction verification tool**, allowing admins to verify the legitimacy of any transaction hash recorded on the local blockchain.
- To use a **role-based access control model**, separating user and admin functionalities while maintaining secure session tracking.

SYSTEM OVERVIEW

The proposed system is composed of two main roles: **Users** and **Administrators**.

- **Users** (e.g., forensic agents, security personnel, witnesses) can:
  - Log into the system using secure authentication.
  - Upload digital evidence such as documents, images, or log files.
  - View their submission history and track the status of each submission.
  - Review blockchain transaction details linked to their submissions.
- **Administrators** (e.g., forensic analysts, legal investigators) can:
  - Monitor all evidence submissions.
  - Approve or reject submitted evidence after manual review or integrity checks.
  - Verify transaction hashes through the local blockchain to validate data integrity.
  - Maintain oversight of the system to ensure procedural compliance.

The blockchain layer ensures that every transaction (i.e., evidence upload) is **cryptographically recorded and time-stamped** in an immutable format, using smart contracts deployed via Ganache. Each file's SHA-256 hash is stored on-chain, serving as a permanent proof of content integrity.

Significance and Impact

The implementation of a blockchain-enabled forensic system addresses several long-standing issues in digital investigations:

Enhanced Security

By decentralizing the evidence recording process, the risk of unauthorized tampering or deletion is virtually eliminated. Each transaction on the blockchain is validated and confirmed, providing a robust defense against manipulation.

Auditability and Transparency

Blockchain inherently maintains a complete, chronological record of all actions. This makes it easy for investigators and legal personnel to trace the lifecycle of each evidence item—when it was submitted, by whom, and with what outcome.

Increased Trust in Forensic Data

Judicial processes depend heavily on the credibility of the evidence. With this system, courts and stakeholders can trust that the evidence presented has not been altered and that it has an indisputable digital fingerprint tied to a blockchain transaction.

Scalability and Real-Time Access

Since the application is built using Django, it can scale easily across organizations and agencies. Features such as role-based dashboards and transaction search allow users and admins to interact with the system in real time.

Improved Chain of Custody

The use of session IDs, user tracking, and blockchain transaction IDs creates an integrated and verifiable chain of custody, which is critical in upholding the validity of digital evidence in legal environments.

Technology Stack

The core technologies used in this project include:

- **Django**: A high-level Python web framework that handles user authentication, evidence management, and admin interfaces.
- **Web3.py**: A Python library used to interact with the Ethereum blockchain and smart contracts.
- **Ganache**: A local blockchain emulator used to deploy smart contracts and simulate real Ethereum transactions.
- **Solidity**: The smart contract programming language used to write the logic for evidence storage and retrieval on the blockchain.
- **HTML/CSS & Bootstrap**: For building responsive and clean user interfaces.
- **SQLite/PostgreSQL**: For persistent storage of user data and metadata related to evidence.

CHALLENGES AND SOLUTIONS

During the development process, several technical and conceptual challenges were encountered:

- **Smart Contract ABI Mismatches**: Mismatched or outdated ABI files often caused errors when calling blockchain functions. This was resolved by enforcing a strict compilation and deployment workflow.
- **Transaction Delay Handling**: Waiting for transaction receipts was necessary to ensure that data was confirmed on-chain before being shown to users. Web3's wait_for_transaction_receipt() solved this.
- **File Integrity Verification**: SHA-256 hashing was implemented to provide a consistent and secure way to generate fingerprints for files, ensuring their identity remains intact during storage.
- **User-Wallet Mapping**: In a future phase, mapping Django users to individual Ethereum wallet addresses will further enhance the accountability and traceability of transactions.

II. LITERATURE SURVEY

In the realm of cybercrime investigation and data integrity assurance, digital forensics has emerged as a critical discipline. As digital devices increasingly serve as both tools and targets of crime, the ability to collect, preserve, and analyze digital evidence has become indispensable. However, traditional forensic methods face significant challenges such as centralization, lack of transparency, limited tamper-proof mechanisms, and manual validation inefficiencies. Recent studies suggest that integrating emerging technologies—particularly **blockchain**, **encryption algorithms**, and **intelligent key generation techniques**—can greatly enhance the effectiveness and trustworthiness of forensic systems.

This section reviews key literature that forms the foundation for the proposed system, which aims to secure digital forensic evidence using blockchain and cryptographic techniques, implemented through Django and Ganache.

Digital Forensics and Its Challenges

Digital forensics traditionally involves the identification, acquisition, analysis, and presentation of digital evidence. As per Casey (2011), the integrity of evidence is paramount, and every step in the forensic process must be reproducible and tamper-proof to maintain judicial admissibility.

However, several challenges persist in modern forensic environments:

- **Lack of secure storage** methods for digital artifacts.
- **Difficulty in preserving chain of custody** in decentralized or cloud-based infrastructures.
- **High vulnerability** to internal data manipulation and external cyberattacks.

According to Agarwal et al. (2019), most legacy forensic systems depend heavily on centralized data stores, making them vulnerable to tampering, unauthorized access, and data loss. These limitations have prompted the search for a more robust, transparent, and verifiable solution.

Blockchain in Digital Forensics

Blockchain technology offers immutable and decentralized ledger functionality, which can serve as a secure backbone for digital forensic processes. Nakamoto (2008) originally introduced blockchain to support Bitcoin, but it has since found applications far beyond cryptocurrencies.

G. Kumar et al. (2021) proposed an **Internet-of-Forensics (IoF)** model that utilizes blockchain to enhance forensic analysis in IoT environments. Their model recorded digital activities immutably, improving evidence traceability.

In a similar vein, Rajashree et al. (2022) developed a blockchain-based data validation system using Secure Hash Algorithm (SHA) and AES encryption. This system demonstrated how tamper-resistant blockchain ledgers could complement secure cryptographic operations to protect evidence integrity in legal contexts.

Apirajitha and Devi (2023) introduced a **BC-based multi-objective optimization algorithm** for cloud forensics, achieving notable success in maintaining privacy and preventing evidence loss or manipulation.

These studies underline the **natural alignment between forensic integrity requirements and blockchain properties**, especially for maintaining **tamper-proof audit trails**, **data provenance**, and **decentralized control**.

Cryptographic Techniques for Data Security

Encryption plays a foundational role in safeguarding digital information, especially in transit and at rest. Recent innovations have focused on **lightweight and homomorphic encryption** systems to allow encrypted data processing without needing decryption.

Sheeja (2022) proposed a **multifactor scalable lightweight cryptographic approach** suitable for IoT-cloud environments, utilizing digital signature algorithms and attribute-based encryption. This framework emphasized multi-layered access control and data protection for forensic applications.

Chen et al. (2019) further advanced the field with **multi-key homomorphic encryption (MKHE)**, enabling computations on encrypted data from multiple sources. This feature is particularly relevant for forensic systems dealing with sensitive data from varied origins.

Such encryption schemes, when combined with blockchain, create a **dual security layer**—encryption for confidentiality, and blockchain for integrity and traceability.

Optimal Key Generation Algorithms

Key management is another core element of secure digital systems. Static keys are vulnerable to brute-force attacks and unauthorized access if not properly randomized and updated. To address this, researchers have focused on **metaheuristic-based key generation algorithms** that provide dynamic and context-aware key evolution.

Houssein et al. (2023) proposed the **Enhanced Equilibrium Optimizer (EEO)**, a physics-inspired algorithm that mimics mass balance principles to find optimal solutions. EEO demonstrated significant improvements in generating unpredictable and high-entropy cryptographic keys.

In the context of digital forensics, employing such algorithms during evidence encryption can help **dynamically secure files** before storage or transmission, ensuring they cannot be easily decrypted or tampered with by unauthorized entities.

Smart Contract-Based Authentication and Verification

Smart contracts have emerged as powerful tools for automating forensic processes. They provide deterministic, tamper-proof execution environments where verification logic can be embedded securely.

Shankar et al. (2023) implemented a smart contract-based multi-signature authentication system using the Ed25519 digital signature algorithm. Their system allowed only authorized forensic agents to commit evidence to the chain, improving access control and auditability.

Deebak and Fadi (2021) introduced a lightweight smartcard-based authentication model that leveraged smart contracts for session management and multi-user data sharing within a secure forensic cloud platform.

These systems collectively highlight the potential of **smart contracts to automate integrity checks**, **trigger validation workflows**, and **enforce access rules** without relying on human intermediaries.

Web Frameworks and Blockchain Integration

The use of web technologies like **Django** in conjunction with blockchain platforms like **Ganache** or **Ethereum testnets** has become more prevalent in both academic and industrial prototypes. Django provides a powerful MVC (Model-View-Controller) architecture that is ideal for building structured web applications with user roles and permission systems.

Integrating Web3.py with Django allows developers to:

- Access blockchain contracts directly from the backend.
- Sign and send transactions programmatically.
- Maintain consistency between local databases and decentralized ledgers.

Khan and Verma (2021) proposed a **Software Defined Networking (SDN) and blockchain hybrid architecture** for forensic data collection in cloud environments. Their Django-based prototype validated forensic evidence across distributed nodes using real-time hash matching.

These works underscore the **viability of integrating traditional web technologies with blockchain infrastructure**, offering both scalability and security in real-world forensic systems.

Gap Analysis and Novelty of the Current Project

While each of the aforementioned studies offers valuable contributions to forensic science, most are either:

- Focused on theory or simulation without practical implementation.
- Overly dependent on public blockchains, which may introduce latency and scalability issues.
- Lacking in full-stack integration between user interfaces, smart contract layers, and backend management.

The current project addresses these gaps by:

- Using **Ganache** as a **private blockchain**, ensuring low-latency, cost-free, and controlled transaction environments.
- Integrating a **full-stack web application** (built with Django) that supports real-world evidence workflows, including file uploads, admin review, and blockchain verification.
- Employing **optimal key generation** and **cryptographic hashing** to protect digital evidence at every stage.
- Supporting **role-based access controls** to differentiate between user submissions and administrative actions.

This combination of technologies ensures a secure, scalable, and auditable system that can be adapted to real investigative environments with minimal overhead.

III. EXISTING SYSTEM

The traditional digital forensic systems in use today often follow a **centralized, manual, and siloed approach** for the collection, storage, and analysis of digital evidence. While functional to some extent, these systems are increasingly insufficient in addressing the challenges posed by modern cybercrime, especially in terms of **data integrity, transparency, and trust**.

Key Characteristics of Existing Systems:

1. **Centralized Storage**
    - Evidence is stored in central databases or physical servers, making them susceptible to tampering, unauthorized access, and single points of failure.

2. **Manual Chain of Custody**
    - The tracking of who accessed or modified the evidence is often logged manually or via logs that themselves can be manipulated.
3. **Lack of Real-Time Verification**
    - There is no mechanism to verify whether the submitted digital evidence remains unchanged or authentic over time.
4. **Poor Transparency**
    - Investigators, judges, and external parties have limited visibility into the timeline and actions performed on a piece of evidence.
5. **Minimal Use of Cryptographic Techniques**
    - Evidence may not be hashed, encrypted, or signed cryptographically, making it vulnerable to undetected tampering.
6. **No Integration with Blockchain**
    - Most systems lack decentralized and tamper-proof ledger functionality, which is essential for traceability and long-term trust.
7. **No Role-Based Web Interface**
    - Users and admins often interact with the same portal or via static file systems, increasing the risk of accidental or unauthorized access.

Limitations of Existing Systems:

- Vulnerable to data loss, corruption, and insider threats.
- No cryptographic assurance of data integrity.
- Lack of automated, trustworthy verification mechanisms.
- Inadequate for compliance with modern digital investigation standards.
- Inflexible architecture not suited for cloud or decentralized environments.

PROPOSED SYSTEM

To overcome the limitations of existing systems, the proposed solution is a **blockchain integrated forensic evidence management system** built using **Django** (as the web application framework) and **Ganache** (as a local Ethereum blockchain network). This system introduces a **transparent, secure, and decentralized approach** to evidence submission, verification, and administrative approval.

Key Features of the Proposed System:

1. Blockchain-Backed Evidence Storage

- Every piece of submitted evidence is hashed using **SHA-256** and immutably recorded on a local **blockchain ledger** via a **smart contract**.
- This ensures that the integrity and timestamp of the evidence are **verifiable and tamper-proof**.

2. Decentralized Verification

- Administrators can verify the validity of evidence using **transaction hashes**.
- The system fetches transaction details like block number, sender, timestamp, and gas used directly from the blockchain.

3. Role-Based Interface

- Two main roles:
    - **Users**: Can upload evidence and track their submission history.
    - **Admins**: Can view all submissions, verify blockchain integrity, and approve or reject evidence.

4. Secure Evidence Upload & Metadata Tracking

- Files are securely uploaded and hashed upon submission.
- The database stores file metadata, transaction hash, user session ID, and status (Submitted, Approved, or Rejected).

5. Smart Contract-Based Integrity Logs

- A custom smart contract (TaskContract) manages evidence records on-chain.
- Each file hash is tied to a blockchain transaction for long-term auditability.

6. Efficient Transaction Management

- The system connects to Ganache using Web3.py for all blockchain interactions, ensuring:
  - Low latency
  - No real Ether costs
  - Complete local control

7. Evidence Verification Tool (Admin Utility)

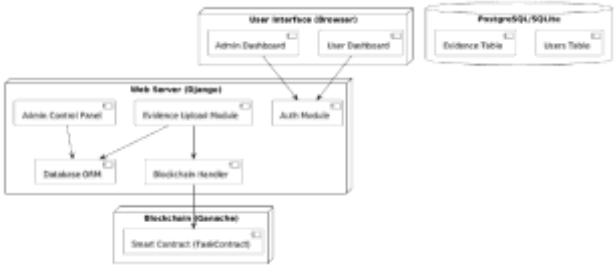
- Admins can enter a transaction hash and view its validity and metadata via the blockchain.
- This tool supports real-time proof-of-integrity checks.

8. User Dashboard with Pagination

- Logged-in users can view their past submissions in a paginated table.
- Each record shows file name, hash, blockchain status, and submission date.

IV. IMPLEMENTATION

SYSTEM ARCHITECTURE



V. MODULES

- **ADMIN**
- **USER**

MODULE DESCRIPTION

USER

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like upload, my_evidences, userhome

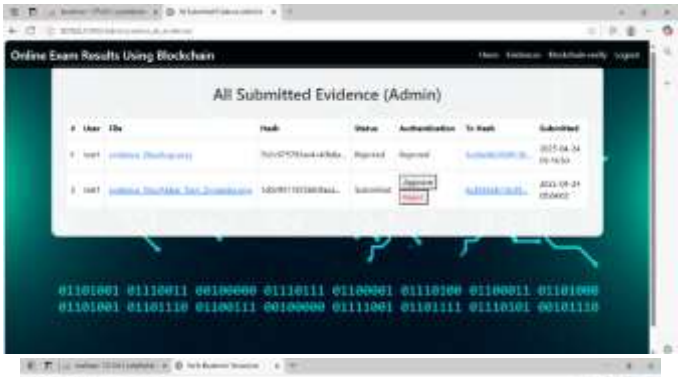
ADMIN

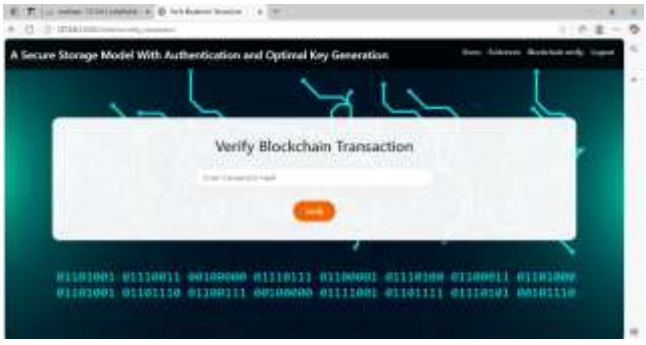
In this module, the ADMIN has to login by using valid user name and password. After login successful he can do some operations such as adminhome,verify_transaction, admin_all_evidence

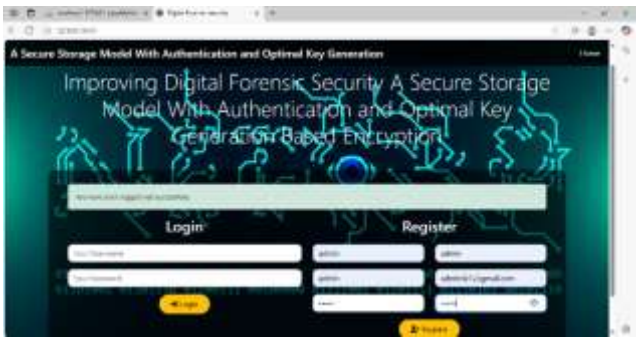
VI. RESULTS


A Secure Storage Model With Authentication and Optimal Key Generation
Improving Digital Forensic Security A Secure Storage Model With Authentication and Optimal Key Generation Based Encryption
Login
Register


A Secure Storage Model With Authentication and Optimal Key Generation
Manage Users


Online Exam Results Using Blockchain
All Submitted Evidence (Admin)


A Secure Storage Model With Authentication and Optimal Key Generation
Verify Blockchain Transaction


A Secure Storage Model With Authentication and Optimal Key Generation
Improving Digital Forensic Security A Secure Storage Model With Authentication and Optimal Key Generation Based Encryption
Login
Register

VII. CONCLUSION

In this article, we have developed a novel DFA-AOKGE technique to accomplish security of the digital images. The DFA-AOKGE technique makes use of a decentralized BC technology to share data among different peers for evidence collection and secure storage. By including a strong authentication device utilizing SBVM and producing optimum cryptographic keys utilizing the EEO model, this technique confirms a difficult defense besides illegal access and potential threats to image privacy. The authentication layer offers a safe gateway, permitting only official users to entree and adapt images, so justifying the danger of unofficial modifications or data breaches. The finest key generation utilizing the EEO model further supports the encryption procedure, guaranteeing that cryptographic keys are dynamic and well-produced dependent upon the single features of the images. An extensive range of experimental studies specified the supremacy of the developed model over other current techniques. The possible impact on forensic studies is important, offering enhanced data reliability, boosted privacy, and efficient access control. The model's flexibility creates it a real-world choice for boosting the safety of digital forensic data, thereby definitely influencing the efficiency of forensic investigations in real uses. Future work must concentrate on the improvements in

authentication protocols, including multi-factor authentication or biometric-based confirmation, which can additionally strengthen access control devices. Furthermore, exploring innovative encryption models and algorithms, such as homomorphic encryption or post-quantum cryptography, may donate to improving the complete flexibility of image safety. Future works must concentrate on refining authentication devices, discovering innovative encryption methods, and incorporating emerging tools to safeguard a strong, adaptive, and future-proof solution for the ever-growing loads of secure image storage and transmission.

REFERENCES

1. Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press, 2011.
2. Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. https://bitcoin.org/bitcoin.pdf
3. Agarwal, A., Gupta, P., & Rao, B. (2019). *Digital forensics: Challenges and future research directions*. In 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1–5). IEEE.
4. G. Kumar, P. Shukla, & A. S. Kumar. (2021). *Blockchain-based Internet of Forensics (IoF): Architecture, Challenges, and Solutions*. *Computer Communications*, Elsevier.
5. Apirajitha, A., & Devi, V. S. (2023). *Secure blockchain-based optimization model for cloud forensic investigation*. *Journal of Cloud Computing*, Springer.
6. Rajashree, R., Ramya, R., & Karthikeyan, M. (2022). *Blockchain-Based Secure Data Validation Using SHA and AES Algorithms*. *International Journal of Computer Applications*, 975–8887.
7. Sheeja, K. R. (2022). *Secure and Efficient Cryptographic Approach for Scalable IoT Cloud Forensics Using Digital Signatures*. *Computer Science Review*, Elsevier.
8. Chen, H., Laine, K., & Player, R. (2019). *Simple Encrypted Arithmetic Library – SEAL (v3.4)*. Microsoft Research.
9. Houssein, E. H., Hassanien, A. E., & Das, S. (2023). *Enhanced Equilibrium Optimizer (EEO): A Novel Optimization Algorithm Based on Mass Balance Dynamics*. *Expert Systems with Applications*, Elsevier.
10. Shankar, K., et al. (2023). *Smart Contract-Based Multi-Signature Authentication in Digital Forensics using Ed25519 and Blockchain*. *Journal of Information Security and Applications*, Elsevier.
11. Deebak, B. D., & Fadi, A. M. (2021). *Lightweight Smartcard Authentication Protocol for Secure Multi-User Forensics in Cloud Environments*. *Journal of Network and Computer Applications*, Elsevier.
12. Khan, R. A., & Verma, P. (2021). *SDN and Blockchain-Based Secure Framework for Digital Forensic Evidence Management*. *International Journal of Network Security*, 23(2), 202–210.
13. Django Software Foundation. (n.d.). *Django Documentation*. https://docs.djangoproject.com
14. Truffle Suite. *Ganache – Personal Ethereum Blockchain*. https://trufflesuite.com/ganache
15. Web3.py. *A Python Library for Ethereum*. https://web3py.readthedocs.io