International Research Journal of Education and Technology

Peer Reviewed Journal, **ISSN: 2581-7795**



# BLOCKCHAIN-BASED SECURE E-SIGNATURE AND DIGITAL EVIDENCE TAMPER DETECTION FRAMEWORK FOR TRUSTED DOCUMENT VERIFICATION.

Mr. Manoj Kumar. S, Mr. S. Sano

III B.Sc. Digital and Cyber Forensic Science

Dr. Ramaprabha, Associate Professor

Department of Digital and Cyber Forensic Science

Nehru Arts and Science College

Coimbatore

## I. Abstract

The rapid growth of digital documentation and online transactions has increased the need for secure and trustworthy systems for document authentication and verification. Traditional digital signature systems provide authentication and integrity but often rely on centralized infrastructures that are vulnerable to tampering, unauthorized access, and single points of failure. This research proposes a blockchain-based secure e-signature and digital evidence tamper detection framework integrated with Public Key Infrastructure (PKI) to ensure reliable document verification and integrity preservation.

**Keywords:** Blockchain, Public Key Infrastructure (PKI), E-Signature, Digital Evidence, Tamper Detection, Document Verification, Cryptographic Hashing, Data Integrity, Secure Document Management.

## II. Introduction

The increasing adoption of digital technologies has transformed the way documents are created, stored, and shared across various sectors such as government, legal systems, healthcare, finance, and education. Digital documents and electronic signatures (e-signatures) have become essential for enabling fast, paperless, and efficient transactions. However, with the rise of digital communication and online document exchange, ensuring the security, authenticity, and integrity of digital documents has become a critical challenge. Unauthorized modifications, document forgery, and tampering with digital evidence can lead to serious legal, financial, and security consequences.



## III. Literature Survey

Recent work on blockchain-based document verification systems highlights the limitations of traditional centralized verification methods. A study proposing a blockchain document verification system called *Blockcert* explains that traditional systems are vulnerable to forgery, high operational costs, and inefficiencies.

## IV. Methodology

The proposed system presents a Blockchain-Based Secure E-Signature and Digital Evidence Tamper Detection Framework for trusted document verification. The methodology integrates Public Key Infrastructure (PKI), cryptographic hashing, blockchain technology, and tamper detection mechanisms to ensure document authenticity, integrity, and non-repudiation.

**1. System Initialization**

In the initial stage, users are registered in the system through a secure registration process. Each user is provided with a public key and private key pair using the Public Key Infrastructure (PKI).

**2. Document Upload and Hash Generation**

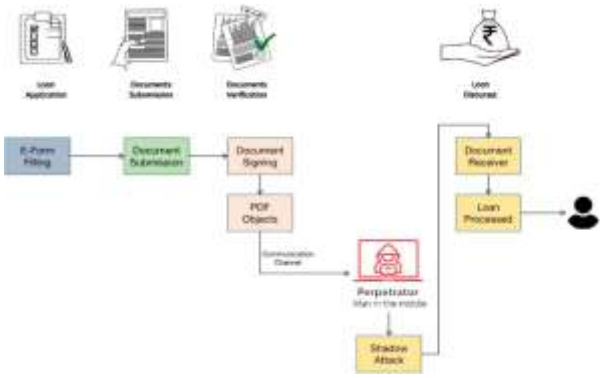
When a user uploads a document for signing, the system generates a cryptographic hash value of the document using a secure hash algorithm such as SHA-256.

**3. Secure E-Signature Generation**

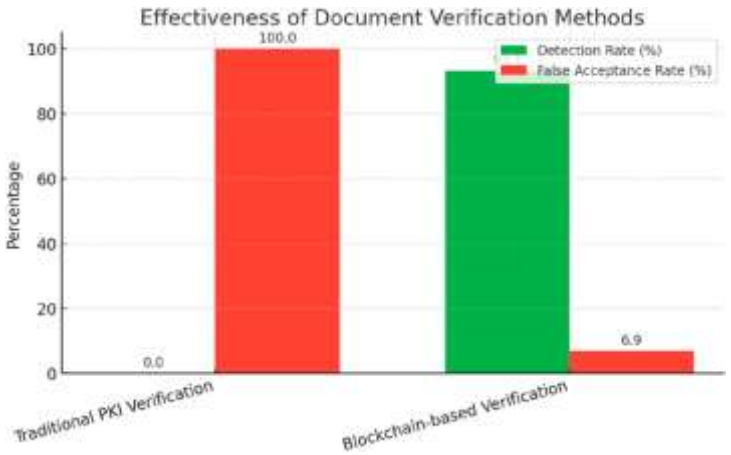
After the hash is generated, the user signs the document using their private key. The digital signature ensures the authenticity of the document and confirms the identity of the signer.

## V. Architecture

The architecture of the Blockchain-Based Secure E-Signature and Digital Evidence Tamper Detection Framework consists of multiple interconnected components that work together to ensure secure document signing, verification, and tamper detection. The system follows a layered architecture that integrates users, PKI-based authentication, blockchain storage, and verification modules.




**Overall Workflow:**
User Registration → Document Upload → Hash Value Generation → Digital Signature Creation → Blockchain Recording → Document Retrieval for Verification → Verification Result




# VII. Analysis of Problem

The shift toward digital document management and online transactions has created significant challenges in ensuring the security, authenticity, and integrity of digital records. While digital signatures and Public Key Infrastructure (PKI) provide authentication and non-repudiation, several key problems persist:

### Limitations of Existing System

Existing digital signature and document verification systems, while widely used, have several critical limitations that reduce their effectiveness in ensuring security, authenticity, and tamper detection:

**1. Centralized Authority Dependency**



Most traditional e-signature systems rely on centralized servers or certificate authorities (CAs) to manage user authentication and digital certificates.

**2. Weak Tamper Detection**

Conventional PKI-based systems often only verify the signature's validity rather than the

**3. Poor Compliance Enforcement**

Current file transfer systems do not automatically validate compliance with security standards or regulatory frameworks.

# VIII. Applications and Future Scope

The Blockchain-Based Secure E-Signature and Digital Evidence Tamper Detection Framework has wide-ranging applications across industries where document authenticity, integrity, and tamper-proof verification are critical. In addition, the framework offers avenues for future enhancements and research**.**

## Future Scope

 **Integration with Smart Contracts**

- Automated execution of contracts when predefined conditions are met.
- Enhances trust and reduces human intervention in document workflows.

 **AI-based Tamper Detection**

- Use of machine learning and AI to detect subtle modifications in documents, images, or PDFs beyond simple hash comparisons.
- Enhanced detection of semantic tampering, such as changed text meaning.

 **Scalability for Large-Scale Systems**

- Implementing permissioned blockchains for enterprise or government-scale deployment.
- Efficient handling of millions of documents with optimized storage and retrieval.

 **Cross-Platform Interoperability**

- Integration with cloud services, IoT devices, and decentralized storage networks like IPFS.
- Secure document verification across multiple organizations or jurisdictions.

 **Mobile and Web-Based Verification Tools**

- Real-time verification of e-signatures and document integrity via mobile apps or web interfaces.



## VIII. Challenges

Implementing a Blockchain-Based Secure E-Signature and Digital Evidence Tamper Detection Framework involves several technical, operational, and practical challenges. Understanding these challenges is essential for designing an effective and scalable system.

## X. Conclusion

The proposed framework not only addresses current limitations of digital signature and verification systems but also lays the foundation for secure, decentralized, and tamper-proof digital document ecosystems. Its applications span legal, governmental, financial, healthcare, and educational domains, with future enhancements enabling automation, AI-driven security, and scalable adoption.

## XI. Reference

1. AlZain, M. A., Pardede, E., Soh, B., & Thom, J. A. (2012). *Cloud computing security: From single to multi-clouds*. **2012 IEEE World Congress on Services**, 201–208. https://doi.org/10.1109/SERVICES.2012.29
2. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf
3. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). *An overview of blockchain technology: Architecture, consensus, and future trends*. **2017 IEEE International Congress on Big Data (BigData Congress)**, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85
4. Christidis, K., & Devetsikiotis, M. (2016). *Blockchains and smart contracts for the Internet of Things*. **IEEE Access**, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
5. Sharma, P., & Singh, K. (2020). *Blockchain-based digital signature system for secure document management*. **International Journal of Advanced Research in Computer Science**, 11(5), 22–28.
6. Kshetri, N. (2017). *Blockchain's roles in strengthening cybersecurity and protecting privacy*. **Telecommunications Policy**, 41(10), 1027–1038.



Manoj Kumar S (USN: 23UGDF024) is an aspiring professional with a strong interest in Digital and Cyber Forensic Science. He is passionate about exploring advanced techniques in cybercrime investigation, digital evidence analysis, and emerging security technologies with a keen focus on cybersecurity, forensic methodologies, and ethical digital practices, his aims to contribute to building a secure and trustworthy digital environment. He can be reached manojkumar963333@gmail.com or via mobile at 9633332534 for academic and research collaboration.



Sano S (USN: 23UGDF037) is an aspiring professional specializing in Digital and Cyber Forensic Science. He is deeply passionate about exploring cybercrime investigation, digital evidence analysis, and emerging security technologies, with a strong focus on cybersecurity, forensic methodologies, and ethical digital practices. Sano aims to contribute to creating a secure and trustworthy digital ecosystem by leveraging advanced forensic techniques and research-driven approaches. He is actively seeking opportunities for academic and research collaboration, and can be reached at: Email: s.sano2277@gmail.com Mobile: 9626808501