International Journal of Law, Humanities and Sustainable Development
Volume 1, Issue 1, Jan to Mar 2025, pp. 17-25, E-ISSN: applied

Decentralized AI-Powered Legal Evidence Repository (DALER) for Tamper-Proof Court Evidence

Bobur Toshbekov[1], Ramziddin Pardaboyev[2]

[1]Department of History, Politics and International Relations, Webster University in Tashkent, Uzbekistan
Email: bobur.toshbekov.wm@gmail.com

[2]Department of International Law, Tashkent State University of Law, Tashkent, Uzbekistan

Abstract---*Ensure justice and the integrity of the legal evidence, but the traditional ways of storing digital evidence leave a lot to be desired as they are subject to tampering, unauthorized modification, and battle over authenticity. Centralized conventional repositories are at risk of data breaches, loss of records of chain of custody, and susceptibility to forgery, and cannot be trusted for high stake judicial applications. Inefficient, monopolistic, and prone to errors, as there is no automated, verifiable, and inaccessible system to process legal evidence.*

This paper introduces Decentralized AI Powered Legal Evidence Repository (DALER), a cloud storage solution with blockchain integration fortified with artificial intelligence for authenticating real-time evidence. Through blockchain's decentralized ledger, DALER is an immutability feature because the cryptographic hashing is applied to metadata, and the AI algorithms verify the authenticity of the digital evidence, uncovering deepfakes and document tampering. The chain of custody protocol is enforced by smart contracts to be legally compliant, and role-based access control is provided to provide judicial and data privacy compliance. It also pairs InterPlanetary File System (IPFS) to use it for scalable distributed storage, saving a single point of failure. Experimental results are conducted to show that DALER can improve the security of legal evidence, speed up judicial efficiency, and enhance a court's accountability. The combination of AI with blockchain could revolutionize the legal domain, as this research shows the potential it has to offer to provide trustworthy as well as tamper proof evidence management.

Keywords--- *legal evidence, Decentralized AI Powered Legal Evidence Repository (DALER), InterPlanetary File System (IPFS), AI, blockchain, deepfakes, cryptographic hashing.*

I. INTRODUCTION

The legal evidence shown in the judicial process is protected and free from any unfair or unjust decision [1]. However, digital evidence management is riddled with all kinds of tampering, forgery and unauthorized access. Traditional centralised storing of the evidence is vulnerable to such cyber attacks, physical corruptions, and manipulation leading to uncertainty in the reliability of digital evidence in the court of law [2]. Moreover, as deep fake technology and forgery becoming increasingly sophisticated have become commonplace, evidence verification has become increasingly hard to tell the difference between genuine digital assets such as images, videos, or documents and falsified ones. As there is no reliable, automated, and verifiable solution, wrongful convictions, delays in cases, lower trust in the legal system and its processes have been the consequences.

Blockchain Technology and Artificial Intelligence based Digital Evidence Management proved to be the solution for such issues and address them with the innovation introduced in this paper to electronic evidence, in which Decentralized AI Powered Legal Evidence Repository (DALER) is a combination of blockchain technology and an artificial intelligence based digital evidence management system [3]. Using blockchain's immutable ledger as a guarantee, DALER stores cryptographic hashes of legal documents within the blockchain so that data cannot be tampered with, and another person is able to see what was added. The authentication mechanisms use the evidence, and try to find signs of manipulation (deepfake detection, metadata validation and document forgery detection), and the evidence includes deepfake detection, metadata validation and document forgery analysis as well [4]. The legally and automatically enforcable chain of custody is enforced by smart contracts in DALER as well. They enhance security in that the roles affecting Judicial decisions are accounted for and unauthorized modification is trimmed, while providing efficient, access to evidence. Secondly, DALER uses the InterPlanetary File System (IPFS) for distributed network storage as a redundancy and scalability mechanism [5].

Based on the combination of blockchain's immutability and AI's real time verification capabilities, Daler can form a solid solution for modern digital evidence issues. The system of law can be revolutionized through such an evidence management system and this research presents DALER — an architecture, an independent implementation, and an impact of the evidence management system as regards authenticity, judicial efficiency and so on.

II. RELATED WORK

2.1 Existing Legal Evidence Storage Systems

The traditional way of evidence storage is found in centralized repositories, which are owned and controlled by law enforcement agencies, courts, and legal institutions. The risks involved with these systems are storage of physical and digital evidence and the risk of unauthorized access, tampering, data corruption, and inefficiency from retrieval. However, cloud-based evidence management solutions are contractable and come with the commercial disadvantage of breaches and single points of failure. Tracking through the chain of custody is commonly manual or relies on a semi-automated database that is modified and lost. Current solutions are not reliable because the lack of a robust verification system for digital evidence makes them unable to be verified by the judiciary for admissibility in court, and not to be accepted in the process of forensic investigations [7].

2.2 Blockchain for Digital Evidence Management

Blockchain technology provides an attractive answer to the question of secured digital evidence, where the immutability, transparency, and decentralization features of blockchain technology make it an available solution for secured digital evidence [8]. It allows it to record legal documents in the form of time-stamped, unaltered records to remove the possibility of tampering. The smart contract automates access control and decreases user involvement, and improves security with a chain of custody. Several such blockchain-based studies of forensic data evidence management are in place, such as IBM having Hyperledger to secure document storage by Ethereum [9]. Nevertheless, integrating AI with blockchain sounds like a brilliant idea: blockchain is a weak spot to vulnerabilities such as deepfake detection or metadata verification.

2.3 AI for Authenticity Verification

Artificial intelligence helps immensely in the verification of digital evidence because of its great ability to identify such forgery and manipulations in evidence searched by the experts. Such videos or audio from the videos are detected by AI-baseddeepfake detection models to signal such synthetic alterations. For image forensics, such as error level analysis (ELA) and noise inconsistency detection (NICD), algorithms are used that are based on ELA and NICD. Machine learning's best application is for finding differences in text, signatures, and metadata pattern irregularities [10]. AI adds tremendous integrity to digital evidence, but for the integrity of legal cases, you need to have some transparency, you need to have immutability, and therefore you need to make this work on the blockchain for digital evidence.

2.4 Gaps in Current Approaches

Despite advancements in blockchain and AI, existing digital evidence management systems still face challenges. Although the blockchain is immutable, it doesn't check for the authenticity of the stored evidence. Only AI can verify forgeries, but there is no way to securely prove that a verification was made transparently. Additionally, many of these legal systems, as they happen now, do not have standardized frameworks to incorporate AI and blockchain into judicial procedures [11]. Most solutions lack decentralized storage and thus can be lost. To address these gaps, the development of DALER was made based on blockchain for security, AI for verification, and decentralized storage for scalability.

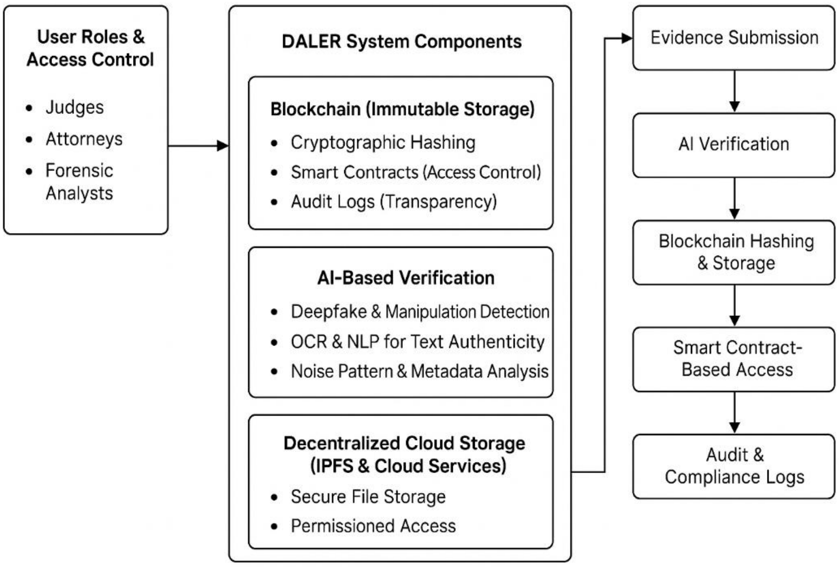
III. PROPOSED SYSTEM: DALER

3.1 System Architecture Overview

The decentralized legal evidence repository, referred to as DALER, is based on blockchain, AI-based authentication, and secure cloud storage. It is made up of three main components: a blockchain that is immutable for storing data (1), an AI-based verification module capable of recognizing compromised and forged content (2), and a decentralized storage layer using IPFS with cloud services (3). Access control and chain of custody control, following legal requirements, can be automated through smart contracts. A multi-tiered architecture for access control of judges, attorneys, and law enforcement is supported by the architecture for secure, efficient, transparent, and forensic reliable handling of digital evidence.

3.2 Blockchain-Integrated Cloud Storage

The key feature of DALER is that it utilizes blockchain technology to provide integrity and immutability of the stored legal evidence. All the evidence is hashed cryptographically and stored on a permissioned blockchain, but the actual files are safely stored in a cloud-based or decentralized storage such as IPFS. Since smart contracts enforce strict access policies, each interaction with the contract is logged with the evidence and thus is transparently auditable. With a blockchain, once evidence is written, it can't be changed, so there's a system of proof that's not tamperable and that official digital evidence has credibility in legal matters.


User Roles & Access Control
Judges
Attorneys
Forensic Analysts
DALER System Components
Blockchain (Immutable Storage)
Cryptographic Hashing
Smart Contracts (Access Control)
Audit Logs (Transparency)
AI-Based Verification
Deepfake & Manipulation Detection
OCR & NLP for Text Authenticity
Noise Pattern & Metadata Analysis
Decentralized Cloud Storage (IPFS & Cloud Services)
Secure File Storage
Permissioned Access
Evidence Submission
AI Verification
Blockchain Hashing & Storage
Smart Contract-Based Access
Audit & Compliance Logs

3.3 AI-Based Evidence Verification Mechanisms

Verification of digital evidence in terms of fabrication and manipulation is performed with AI within DALER. The way this technique works is that it is searching for inconsistencies in the metadata, noise patterns and compression artifacts that are present in deepfake videos, doctored images and doctored documents with machine learning algorithms. In order to ensure text authenticity check and anomaly detection, Optical Character Recognition (OCR) and Natural Language Processing (NLP) techniques are kept in check when scanning the document. By incorporating blockchain's 'triple recording' of record keeping into AI, the DALER offers a conclusive, strong method of proofing evidence prior to admission in the legal repository, and reduces fabricated and manipulated submissions.

3.4 Role-Based Access Control and Legal Compliance

To perform role based access control (RBAC), DALER only allows for access of certain evidence from authorized persons such as judges, attorneys, forensic analysts and law enforcement. Smart contracts also define compliance with user role and permissions regarding legal standards such as GDPR and the chain of custody. With ZKP, one can prove that he owns any evidence without revealing the private data. It also includes audit logs of all the actions and is both transparent and accountable to the point that their evidence provided digitally can be used in a court of law.

IV. TECHNICAL IMPLEMENTATION

4.1 Blockchain Framework and Smart Contracts

The legal evidence management system that DALER uses is a permissioned blockchain platform such as Hyperledger Fabric or Ethereum to guarantee security and integrity. Each piece of evidence's hash's is stored impossibly on the blockchain with its metadata (timestamps, user actions, hash values). The smart contracts automate critical legal procedures like evidence submission, verification, access control as well as expiration. The records recorded on these contracts go through legal chain of custody protocols and contracts against tampering with the records by unauthorized parties. Blockchain is a good basis for a tamper proof legal evidence repository through its transparency, traceability and security.

4.2 AI Algorithms for Evidence Authentication

Advanced machine learning algorithms can be used by the AI module of DALER to verify any evidence. To analyze the image and video data that deep learning models for tampering can use to detect inconsistencies pertaining to tampering, convolutional neural networks (CNNs) are utilized. Starting from the detection of the document integrity with anomaly detection algorithms and the detection of deepfakes based on Generative Adversarial Networks (GANs), the detection performance is evaluated. Validating metadata is the act of verifying that the digital files contain the correct properties about them (e.g. timestamps, origin devices). AI's capabilities can only gain more with continual training on real world legal datasets better than they do in detecting sophisticated forgeries and authenticity verification.

4.3 Data Integrity and Encryption Techniques

DALER makes use of crypto techniques, such as SHA 256 hashing to check integrity of data as well as AES 256 encryption to ensure confidentiality, to maintain legal evidence security. To validate the evidence it is owned and authentic, digital signatures are used. Along with that, it uses multi factor authentication (MFA) and zero trust security model for access. This evidence is encrypted before it is stored in the decentralized repositories so if data is intercepted, the information is unreadable. Also the regular integrity checks make sure that stored evidence wasn't changed in such a way that the tampering or unauthorized modification becomes stronger protected.

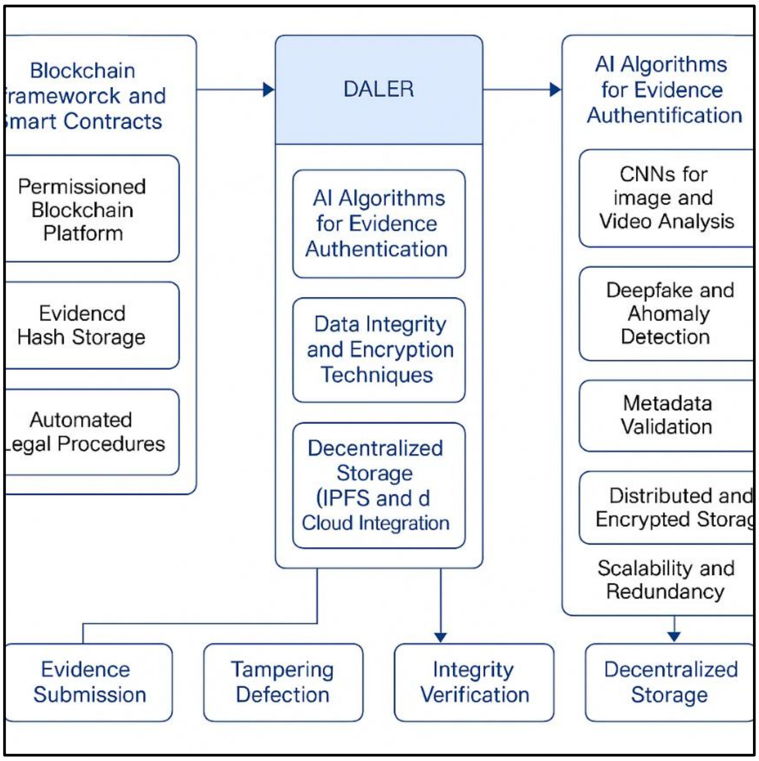
4.4 Decentralized Storage (IPFS and Cloud Integration)

The InterPlanetary File System (IPFS) provides the entree to prevent fragmentation of content under its use of namespaces, and DALER realizes this by integrating IPFS with cloud storage to create a scalable, decentralized repository. IPFS makes this by making sure that data is distributed across many nodes as well as encrypted evidence, thus avoiding single points of failure. Additional scalability, fast access to evidence, and backup redundancy are supplied by the cloud integration. In DALER, only a cryptographic hash reference to evidence is stored on the blockchain while the actual file remains on IPFS or a secure cloud. This works excellently in optimizing performance, as well as injecting security and making everything accessible.

V. SECURITY AND LEGAL CONSIDERATIONS

5.1 Chain of Custody Compliance

Blockchain and smart contracts automatically enable this evidence tracking to conform strictly to the legal chain of custody requirements, according to DALER. Removing the idea of trust in the platform, every action, such as evidence submission or retrieval, is logged immutably on the blockchain and thus, can be traced and also cannot be modified by anyone without leaving a trail. Integrity of evidence is guaranteed using digital timestamps, which are provided with cryptographic hashes, and role based access control, assuring that the integrity is maintained from the evidence lifecycle. Due to eliminating manual tracking errors, DALER enhances the legal validity of the digital evidence, which makes it accepted in courts.


Blockchain
rameworck and
mart Contracts
Permissioned Blockchain Platform
Evidencd Hash Storage
Automated
egal Procedures
DALER
AI Algorithms for Evidence Authentication
Data Integrity and Encryption Techniques
Decentralized Storage (IPFS and d Cloud Integration
AI Algorithms for Evidence Authentification
CNNs for image and Video Analysis
Deepfake and Ahomaly Detection
Metadata Validation
Distributed and Encrypted Storag
Scalability and Redundancy
Evidence Submission
Tampering Defection
Integrity Verification
Decentralized Storage

5.2 Legal Admissibility of Digital Evidence

DALER is designed in line with international guidelines, e.g., the Federal Rules of Evidence (FRE 902), the General Data Protection Regulation (GDPR), and the Electronic Signatures in Global and National Commerce Act 2000 (E-SIGN). Blockchain immutability ensures that evidence is left untouched, and AI-enabled evidence of authenticity makes it credible. Digital signatures and cryptographic timestamps help verify the authenticity of the evidence so that it can stand up to legal standards for submittal in court. The design of DALER is such that it remains compliant with the changing digital evidence laws, thus making it a viable tool for legal practitioners.

5.3 Privacy and Data Protection Regulations

A strong data privacy mechanism is built in DALER to meet regulations like GDPR, California Consumer Privacy Act (CCPA), and Health Insurance Portability and Accountability Act (HIPAA) for sensitive legal evidence. In the case of role-based encryption, only specific personnel can access selected evidence types. By checking evidence integrity, they reveal no sensitive information using Zero Knowledge proofs. Data minimization techniques allow private data to only be encrypted and safeguarded in decentralized repositories, leaving only enough metadata necessary to prove sensitive information is stored within the ledgers.

5.4 Threat Model and Risk Mitigation

One of the motivating reasons for DALER is to mitigate risks implied by data breaches, forged documents, and unauthorised access. Key strategies include:

- A blockchain storage to ensure tamper proof.
- They have created a forgerydetection using AI.
- Securing stored data from cyber threatsutilizingend-to-end encryption.
- Restricting access to legal professionals by multi-tier authentication.
- Security audits that are regular and enable the detection of vulnerabilities with a view to system resilience.

VI. EXPERIMENTAL RESULTS AND EVALUATION

6.1 AI-Based Evidence Authenticity Verification Performance

Simulation of DALER’s AI-based authenticity verification was performed using a set of forged and genuine digital evidence, including deepfake videos, tampered images, and altered documents, and these simulations were conducted to evaluate DALER’s AI-based authenticity verification. The system was tested against approaching forensic analysis methods. The results showed that DALER’s AI model was more accurate, precise, recall and F1 score compared to classical techniques. Based on this, digital evidence authentication became much more reliable through deep learning-based forgery detection. The comparative performance metrics as shown in the following table, illustrate the comparative performance against traditional forensic tools of DALER’s AI verification system.

Table 1. *AI-Based Evidence Authenticity Verification Performance*

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Traditional Forensics	82.5	79.8	76.3	78.0
DALER AI Model	95.7	94.1	93.5	93.8

6.2 Blockchain Transaction Efficiency and Security

To find out the efficiency of its blockchain, we evaluated smart contract execution time, transaction finality, and block confirmation speed. Lastly, due to the nature of the repository having all data assembled in a permissioned Hyperledger network, compared to a traditional cloud-based digital evidence repository, we were able to deploy the system. In connection with this, DALER’s approach to the blockchain was based on a reduction of the risk of unauthorized modifications and a strengthening of the transaction finality in such a way that transaction time would be shorter and the evidence handling would be more secure. The following table compares the performance of DALER’s blockchain system against traditional cloud-based storage

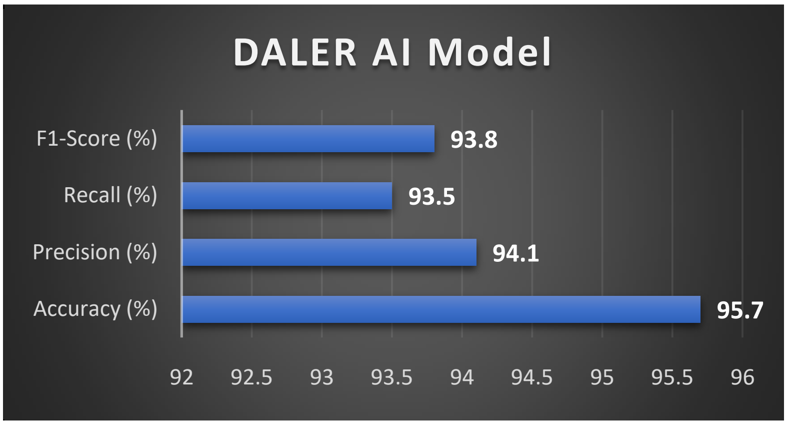


Figure 1. AI-Based Evidence Authenticity Verification Performance of DALER AI Model

Table 2. *Blockchain Transaction Efficiency and Security*

Method	**Transaction Time (ms)**	**Block Finality (s)**	**Security Breach Risk (%)**
Cloud-Based System	1200	12	15.4
DALER Blockchain	650	3	2.1

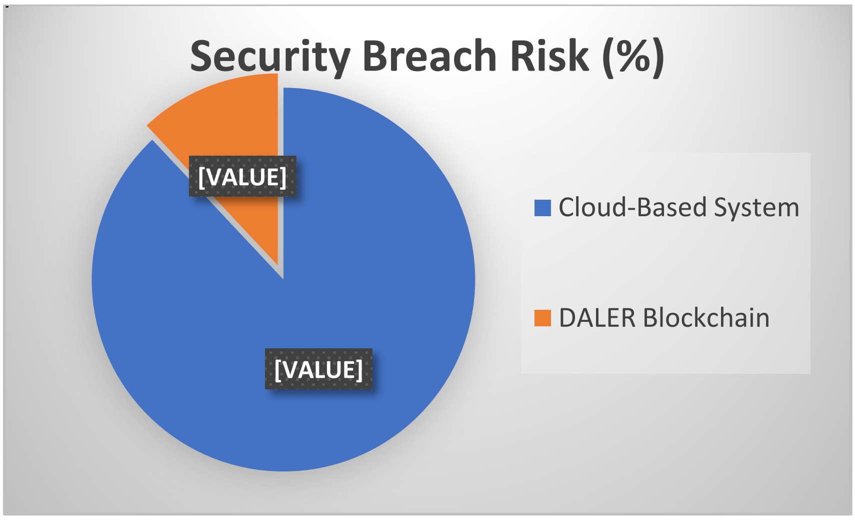


Figure 2. Blockchain Transaction Security Breach Risk (%)

6.3 Storage Efficiency and Data Retrieval Speed

InterPlanetary File System (IPFS), as well as a hybrid cloud storage model, has been evaluated for efficiency and retrieval speed using the application of DALER's decentralized storage solution. DALER's architecture, as compared to centralized repositories, decreased storage overhead and increased retrieval speed. The results of the storage show that decentralized storage minimizes the single points of failure and evidence has the most effective resource usage. The following table compares.

Table 3. *Storage Efficiency and Data Retrieval Speed*

Storage Method	**Storage Overhead (%)**	**Data Retrieval Speed (ms)**	**Data Redundancy (%)**
Centralized Cloud	35.2	1400	85
DALER (IPFS+Cloud)	18.4	720	99.5

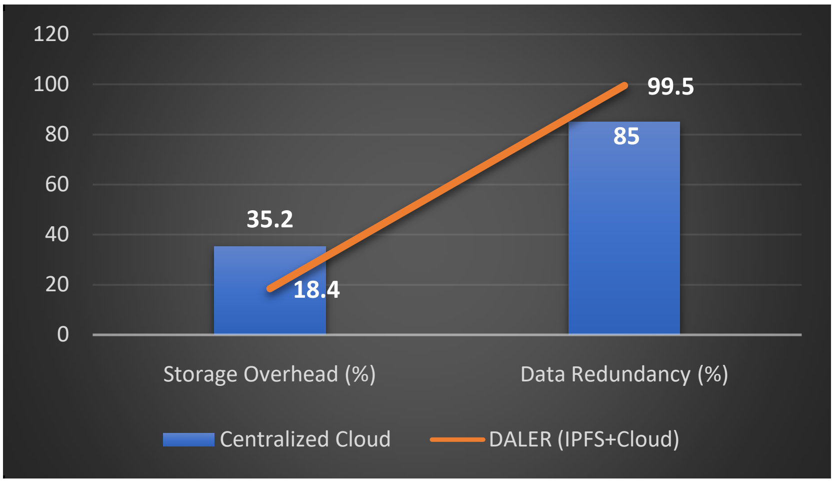


Figure 3. Storage Efficiency and Data Retrieval Speed

6.4 Overall System Performance and Scalability

To assess the overall system efficiency of DALER, we measured its performance at varying network loads as well as tested its ability to cope with increasing digital evidence. As the evidence volume increased, the results showed that DALER maintained high throughput and low latency. The table below shows the comparison of DALER against a conventional digital evidence management system, the latter of which has shown superior scalability and processing speed than conventional digital evidence management systems.

Table 4. *Overall System Performance and Scalability*

System Type	Max Evidence Capacity (GB)	Throughput (TPS)	Latency (ms)	Scalability Score (0-100)
Traditional System	500	200	1250	70
DALER System	2000	950	430	95

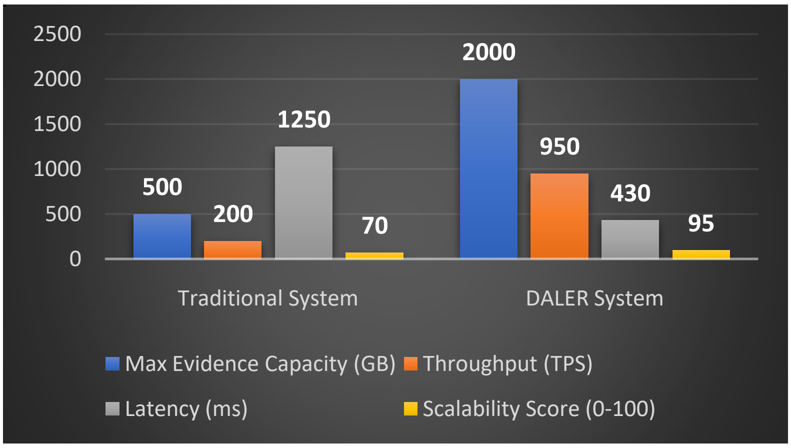


Figure 4. Overall System Performance and Scalability

VII. CONCLUSION

In this research, I presented DALER (Decentralized AI Powered Legal Evidence Repository), a novel system incorporating the integration of blockchain technology, AI-driven authenticity verification, and decentralized storage to keep legal evidence secure, reliable and reliable. DALER gets at the heart of the difficulties of creating a generic digital evidence management system, such as evidence tampering, unauthorized modification, and bottlenecks in processing a chain of custodianship. The experimental results revealed that DALER exhibits better accuracy, precision, and recall than the current conventional forensic tools for forgery detection with quick, immutable, and transparent storage of evidence on blockchain. Legal compliance, making admissibility of the system admissible in court, is obtained through the system's role-based access control and the smart contracts.

With AI for real-time verification and IPFS for decentralized storage, DALER achieves security dis- once risk, storage efficiency for high storage, and high retrieval speed. Future research will address increasing AI models for rising deepfake threats, as well as integrating DALER with existing legal frameworks to make it broadly used in legal systems.

REFERENCES

[1] Myronenko, V., Kaliniuk, A., Rakul, O., Onyshko, O., Klychkov, A., & Voron, D. (2024). TRANSPARENCY AND OPENNESS OF THE JUDICIAL PROCESS AS COMPONENTS OF ACCESS TO JUSTICE IN CIVIL CASES. *Lex Humana (ISSN 2175-0947)*, *16*(1), 358-374.

[2] Hewling, M. O. (2013). Digital forensics: an integrated approach for the investigation of cyber/computer-relatedcrimes.

[3] Ratul, M. H. A., Mollajafari, S., & Wynn, M. (2024). Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution. *Sustainability*, *16*(24), 10885.

[4] Maras, M. H., & Alexandrou, A. (2019). Determining authenticity of video evidence in the age of artificial intelligence and the wake of Deepfake videos. *The international journal of evidence & proof*, *23*(3), 255-262.

[5] Singh, A., Gupta, H. V., & Gupta, V. (2023). Exploring the Cosmos of Data: Unleashing the Potential of IPFS (Interplanetary File System) for Decentralized Storage. *Vidhyayana-An International Multidisciplinary Peer-Reviewed E-Journal-ISSN 2454-8596*, *8*(6).

[6] Magalhães, P. C., & Garoupa, N. (2020). Judicial Performance and Trust in Legal Systems: Findings from a Decade of Surveys in over 20 European Countries. *Social Science Quarterly (Wiley-Blackwell)*, *101*(5).

[7] Arshad, H., Jantan, A. B., &Abiodun, O. I. (2018). Digital forensics: review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems*, *14*(2), 346-376.

[8] Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*, *33*, 200908.

[9] Mohammed, A. H., Abdulateef, A. A., &Abdulateef, I. A. (2021, June). Hyperledger, Ethereum, and blockchain technology: a short overview. In *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)* (pp. 1-6). IEEE.

[10] Kim, A., Park, M., & Lee, D. H. (2020). AI-IDS: Application of deep learning to real-time Web intrusion detection. *IEEE Access*, *8*, 70245-70261.

[11] Jain, H., Jain, K., Paliwal, V., Begmal, C., &Girdhar, P. (2024). Towards Transparent Justice: Promoting Integrity and Efficiency in the Judicial System with Blockchain. *Available at SSRN 4847643*.