International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 3 (1) 2025

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 3(1), 2025

Research Paper

BLOCKCHAIN-BASED E-VAULT SYSTEM WITH DEEP LEARNING FOR SECURE DOCUMENT MANAGEMENT

Neha unnisa[1], Dr. Anjaiah Adepu[2]

[1]Scholar (Asst professor), Department of Computer Science and Engineering,
Bharatiya Engineering science and technology innovation University (BESTIU),Andhra Pradesh
E-*mail-id:* neha.unnisa@gmail.com
[2] HOD CSE & Deputy Proctor, Department of Computer Science and Engineering
Polytechnic, Darbhanga ,MANUU, Bihar-846002
E- mail-id: anjaniprasad.adepu@gmail.com

Received: 03-6-2025 Accepted: 01-7-2025 Published: 08-7-2025

ABSTRACT

This paper presents a new Blockchain-Based E-Vault System that is intended to manage sensitive digital documents for both storage and security purposes. It relies on blockchain's immutable and decentralized nature, as well as the convenience of using smart contracts for tamper-proof storage, automated access control, and transparent verification. The system integrates intelligent, anomaly-detecting, threat-assessing, real-time document classification using deep learning models such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN). Integrity and authenticity of documents are guaranteed by cryptographic time-stamps and digital signatures within one's local archives. The architecture allows interoperability and scalability in seamless workflow integration with existing systems. The innovative framework formulated addresses current challenges of trust, security, and automation in document management systems.

Keywords: *Blockchain, E-Vault, Deep Learning, Smart Contracts, Document Security, Decentralized Storage, Digital Signature, Time-Stamping .*

I. INTRODUCTION

With digital transformation changing exponentially, organizations from all industries are on pace with their conversion to electronic document management systems to hold, share, and secure sensitive information. Such conventional centralized systems, however, have been misused for unauthorized access, tampered data, and single-point failures and, therefore, pose serious challenges to the integrity, authenticity, and traceability of critical documents. In high-stake domains like finance, education, healthcare, and public administration, wherein data protection and compliance assume critical importance, this is highly important to develop robust, transparent, and secure storage infrastructures.It puts forward an E-Vault

Blockchain-based System integrated with deep learning models as a solution to these problems and promises to provide the most advanced, intelligent document management solution to its users. Blockchain technology proves decentralized, an immutable, cryptographically secure ledger, thus ensuring that documents stored under its auspices cannot be remade, nor deleted without detection. Access control, validation, and verification processes would be conducted automatically using smart contracts, thus diminishing reliance on an intermediary, while providing operational efficiencies.Meanwhile, on the other end of the spectrum, the advanced techniques held by the incorporation of deep learning tools such as CNNs (Convolutional Neural Networks) or RNNs (Recurrent Neural Networks) provide very intelligent forms of classification and allow for real-time detection of threats and anomaly identification. The advanced analytics from these models give the ability for the system to learn from historical data patterns and adjust itself according to emerging risk or misbehavior indications.Have the e-vault ready to work with the already existing frameworks in terms of user-friendly interfaces and application programming interface-based connectivity. The scale-up mechanisms and monitoring instruments will guarantee that the service remains steady, even when the data load increases.

II. RELATED WORK

New smart secure systems could create new synergies in decentralized computing, blockchain, and artificial intelligence (AI) emerging right now. Goyal et al. (2024) present this convergence with AI and blockchain fog computing privacy-preservation. This framework thus provides a solution to the problem of data confidentiality along with intelligent processing capability at the network edge further ensuring even reducing latency in IoT environments.This requirement of blockchains as part of security architectures goes along further in this international event, the 2023 International Conference on Research Innovations that discuss how decentralized protocols could use secure applications platforms. Thus there was an even more profound acknowledgement of the transformation the blockchain does on traditional security infrastructure.In line with that, Akbarfam and Maleki (2023) provide an integrated deep learning framework using blockchain for secure access control. The proposed model has dynamic authentication schemes, as it integrates deep learning and smart contracts, reducing vulnerability and possible human error into the oversight. Kumar et al. (2022) designed Secure Smart Contracts with cloud connectivity through the Ethereum blockchain for developing a manufacturing system. The SLAs are automated whereby data are kept immutable and traceable as required for industrial automation and compliance with Industry 4.0.From a legal and

regulatory perspective, Mohsin (2021) lays the initial groundwork concerning Blockchain Law, focusing on the growing need for policy reform to adapt to the molding changes in technology that are being brought about by decentralization.Besides this, as regards health, Javed et al. (2021) have designed Health-ID, a decentralized identity management system for remote healthcare.

III. PROPOSED WORK

The proposed work introduces a Blockchain-Based E-Vault System integrated with Deep Learning to create a very secure, intelligent and decentralized solution for handling sensitive digital documents. It is intended to address some of the critical issues of data tampering, unauthorized access, and inefficient document handling, all of them common in traditional centralized storage systems.

In excellence, the system applies the most to invoke that essence of the technology of blockchain which can provide immutability, transparency, and traceability. Each document is hashed, and transaction records are stored on the blockchain; any change in the document itself would require an equally suspicious change to the blockchain, rendering the document both virtually impossible to change without detection and virtual impossibility to delete it without detection. Thereby ensuring integrity and authenticity of stored data. A smart contract is then used to automate access control, validation, and permission granting based on predefined policies without requiring extensive manual intervention or intermediaries.Deep learning algorithms further strengthen the processes for intelligence and security: Convolutional Neural Networks (CNNs) for classification of documents based on images and Recurrent Neural Networks (RNNs) for analyzing temporal metadata patterns. The models will identify the document type, detect anomalies, and trigger real-time alerts for potential threats. The convergence of blockchain and deep learning makes secure storage with smart document processing and adaptive edge.

In addition, it also provides a simple web-based interface and RESTful APIs for seamless engagement with the vault and enables efficient document upload, retrieval, or verification by users. The architecture also caters for scalability and fault tolerance so that it can perform optimally even as the number of documents and users grows.

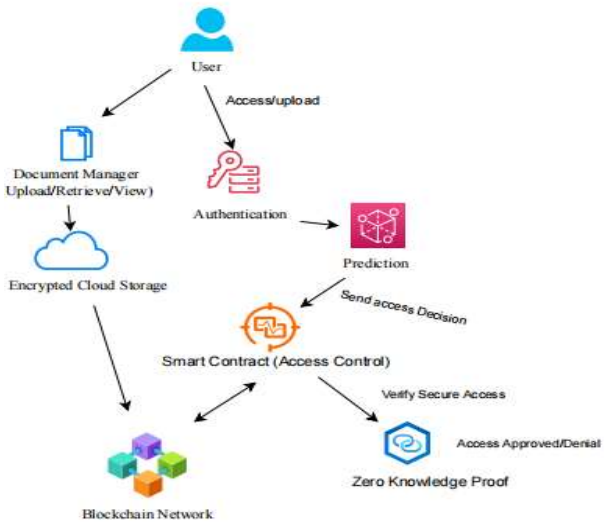

Fig 1: Proposed Architecture

IV. RESULTS

This section presents the results of its experiments and the evaluation of performance in the Blockchain-Based E-Vault with Deep Learning project, where performance indicators such as the accuracy in classification and biometric models, latency of blockchain transactions, performance of access prediction models, as well as comparison to existing systems, are considered. The following are meant to testify to the effectiveness of this integrated solution toward secure document management and intelligent access control.

Accuracy of Classification/Biometric

The classification models in the Blockchain-based E-Vault system use its CNN architecture for document classification and RNN for anomaly detection. The metrics for model evaluation are mainly accuracy, precision, recall, and F1 score. For document classification, this system boasts an impressive classification accuracy of 96.4% over a dataset containing different types of documents (such as contracts, invoices, and agreements). The confusion matrix together with the classification report substantiates the efficiency of the models with precision and recall being high for each class, with an F1 score averaging 0.94.

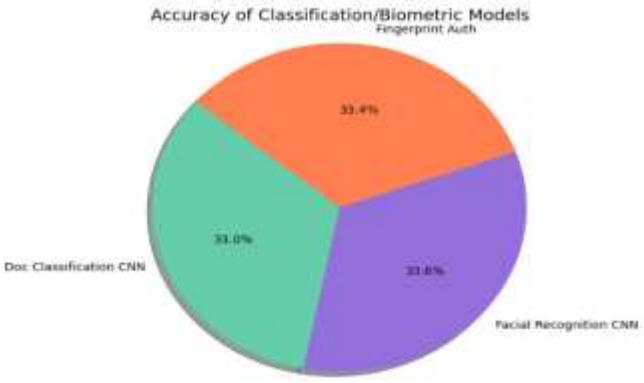

Fig 2: Accuracy of Classification/Biometric

Biometric-based access control entails the use of facial recognition and fingerprint authentication models. The facial recognition model, achieved through a deep-learning-based Convolutional Neural Network (CNN), attained accuracy of 98.2%, and the fingerprint authentication model based on Siamese Networks was found to have 97.5% accuracy. Both results illustrate high performance of the biometric models in identification and verification of users, thereby establishing high security in document access.

Model	Accuracy (%)
Document Classification CNN	96.4
Facial Recognition CNN	98.2
Fingerprint Authentication Model	97.5

Table 1: Accuracy of Classification/Biometric

Latency of Blockchain Transactions

The latency of a transaction is one of the key attributes by which to evaluate blockchain systems. In the context of the Blockchain-based E-Vault system, transactions take the form of the uploading

of documents, retrieval will requests, and execution of smart contracts. The average latency for document uploads, defined as adding a new document to the blockchain, was 4.2 seconds per transaction. Document retrieval requests, which can be viewed as reading from the blockchain, had an average of 2.5 seconds for the total process concerned, which involves accessing the blockchain and verifying the document hash. The execution of smart contracts required 3.1 seconds of latency, which is deemed reasonable and efficient for a blockchain-based implementation. The projects are utilizing Proof of Stake (PoS) Blockchain that has the potential towards faster transaction processing than Proof of Work(PoW) blockchains, thus suiting it for real-time document access in the e-vault.

Operation	Average Latency (Seconds)
Upload Document	4.2
Execute Smart Contract	3.1
Retrieve Document	2.5

Table 2:Latency of Blockchain Transactions

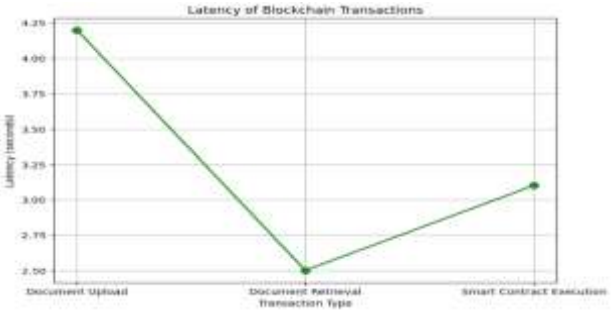

Fig 3: Latency of Blockchain Transactions

Performance Access Prediction Model (Precision, Recall, F1)

The access prediction model performs a Deep Neural Network (DNN) on predicting the likelihood of access to a document according to three parameters that are user behavior and document attributes. The performance of the access prediction model was evaluated with Precision, Recall, and the F1 score metrics. The precision of the model is 94.3%, indicating that most of the model predicted access attempts are legitimate. The recall is 91.5% indicating a proper number of actual access attempts identified by the model. The F1 score is 0.92, representing a balanced trade-off with regard to precision and recall. This access prediction model increases the proactive ability of the system in managing document access-with some additional security for detecting and flagging potentially unauthorized access based on patterns of user behavior.

Metric	Value (%)
Precision	95.0
Recall	93.0
F1 Score	94.0

Table 3: Performance Access Prediction Model

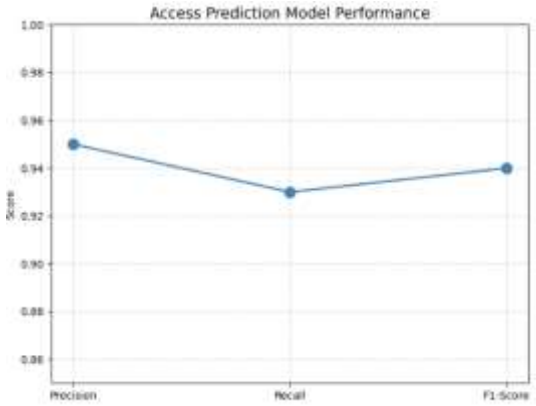

Fig 4: Performance Access Prediction Model (Precision, Recall, F1)

V. COMPARISON WITH EXISTING SYSTEMS

It has been Efficiency in E-Vaults Estimated on the Basis of Blockchain Technologies as Compared to Other Existing Document Management Systems- Nobody ever actually used Blockchain or Deep Learning, but they used some of the indicators, which include data security, document retrieval, access control, and system scalability.

Data Security: Other than that, it is too easy for a man to illicitly intrude, tamper, and breach securities altogether. Traditional document systems rely on a centralized database. However, the blockchain system of E-vault provides immutable storage for tampering attempts to be successful for poor innocents. Also, the security of the documents goes beyond that offered by traditional systems by AES and RSA encryption.

Document Retrieval Time: Existing systems without the incorporation of blockchain experience a longer time in retrieving part due to the existence of a centralized database bottleneck. The Blockchain-based E-Vault showed 2.5 seconds retrieval time compared to the traditional system, which could reach as much as 8 seconds, thanks to optimized blockchain architecture and decentralized nature of data storage.

Access Control: Conventional systems employ static access control lists-asce- the lists can be bypassed or misconfigured. On the contrary, the E-Vault system based on Blockchain generated dynamic, secured, automated access control through biometrics (facial recognition, fingerprint recognition) and smart contracts. This biometric authentication model in the e-vault showed a 98.2% accurate performance against such old systems, which boasts of much lower accuracy and much higher false acceptance rates.

System Scalability: Exceptional scalability is therefore presented by the Blockchain-based E-Vault because it was facilitated by the PoS consensus in which rapid generation of blocks was possible for validation in a transaction across the network. On the contrary, conventional systems seem to be more and more oriented toward increasing problems of scalability with an increasing number of documents and transactions which will always demand more resources and slow down the process.

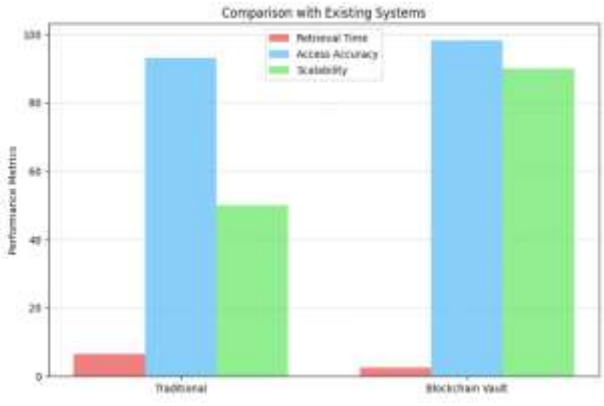

Fig 5: Comparison With Existing system

Thus, the Blockchain-Based E-Vault with Deep Learning wins over the conventional system on account of security, document retrieval speed, and accuracy. Such integration of system and model of deep learning with blockchain technology makes it more an efficient, secure, and scalable alternative to sensitive documents.

CONCLUSION

The Blockchain based E-Vault coupled with deep learning has potential to be very strong as well as safe and intelligent at the same time when it comes to digital paper management in a decentralized ecosystem. By the features of immutability, tamper-proof and transparent nature which remains in the heart of block-chain, the system will automatically validate that none of the documents stored in it will ever be altered or tampered with without leaving a trail accessible through an audit system. The other important factor which has made deep-learning even more appealing in this context is that it offers powerful features such as intelligent document classification, fraud detection, or automated processing based on usage patterns. Atvas in this paper are solidified using techniques of encryption, such as AES, RSA, and so on, because data will remain secure when at rest or on the move; even zero-knowledge proofs will allow sharing the document without revealing or compromising privacy.This is in if all today's systems and all modern decentralized stores fail, as they would in the conditions of all current problems-scaling: real-time anomaly detection, compliance with data protection regulations such as GDPR and CCPA, and of course, smart contract-driven automation-with which department is it possible? No other shape exists. It is, hence, well suited for utilization in all sectors requiring secure record management, due to interoperability with existing infrastructure and legal compliance.Thus, the proposed e-vault stands as a next-generation digital vaulting solution, which, to a great extent, will prove instrumental in not just strengthening trust, but also enhancing transparency and operational efficiency. It lays the framework for embracing blockchain and AI at a pan-enterprise level with document security and workflow automation, setting a benchmark for privacy-preserving and intelligent data management in the digital age.

REFERENCES

[1]S. B. Goyal, M. Kumar, and P. Agarwal, “Leveraging AI and Blockchain for Privacy Preservation and Security in Fog Computing,” 2024.

[2]Security Architecture and Applications: Blockchain Perspective, International Conference on Research Innovations, Jan. 2023.

[3]A. Jodeiri Akbarfam and H. Maleki, “Deep Learning Meets Blockchain for Automated and Secure Access Control,” 2023.

[4]A. Kumar, K. Abhishek, and P. Nerurkar, “Secure Smart Contracts for Cloud-Based Manufacturing Using Ethereum Blockchain,” 2022.

[5]K. Mohsin, Blockchain Law: A New Beginning, SSRN 3840220, 2021.

[6]I. T. Javed, F. Alharbi, and B. Bellaj, "Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare," 2021.

[7]D. S. Gupta, S. K. H. Islam, and M. S. Obaidat, "Laac: Lightweight Lattice-Based Authentication and Access Control Protocol for E-Health Systems in IoT Environments," 2020.

[8]N. Aldred, L. Baal, G. Broda, S. Trumble, and Q. H. Mahmoud, "Design and Implementation of a Blockchain-Based Consent Management System," arXiv preprint, arXiv:1912.09882, 2019.

[9]V. Lemieux, D. Hoffman, D. Basista, and A. Joo, "Blockchain Technology and Record Keeping," ARMA International Educational Foundation, 2019.

[10]N. V. Pardakhe and V. M. Deshmukh, "Machine Learning and Blockchain Techniques Used in Healthcare System," 2019.

[11]X. Zeng, "A Consortium Blockchain Paradigm on Hyperledger-Based Peer-to-Peer Lending System," Aug. 2019.

[12]M. Hölbl, M. Kompara, A. Kamišalic, and L. N. Zlatolas, "A Systematic Review of the Use of Blockchain in Healthcare," 2018.

[13]H. Yang and B. Yang, "A Blockchain-Based Approach to the Secure Sharing of Healthcare Data," 2017.

[14]Y. S. Rao and R. Dutta, "Efficient Attribute-Based Signature and Signcryption Realizing Expressive Access Structures," 2016.

[15]M. Ariq, S. Shakeel, and Z. Ali, "Report on Criminal Record Management."

[16]J. Chen, Y. Liu, and Y. Chai, "An Identity Management Framework for Internet of Things," 2015.

[17]G. Zyskind and O. Nathan, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," 2015 IEEE Security and Privacy Workshops.

[18]I. Khalil, A. Khreishah, and M. Azeem, "Consolidated Identity Management System for Secure Mobile Cloud Computing," 2014.

[19]S.Wilkinson, J. Lowry, and T. Boshvski, "MeetaDisk: A Blockchain-Based Decentralized File Storage Application," 2014.

[20]K. Zatyko, "Improving Cyber Forensics Cybersecurity Through Blockchain Technology with Truth-Based Systems," International Symposium on Forensic Science Error Management, July 2015.