EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

CNN and Blockchain Integrated E-Governance Framework System for Tamper-Proof Documents

C. Rupa[1], K. Venkata Subba Reddy[2], Jagirdar Srinivas[3], Pulluri Srinivas Rao[4], N. Md. Jubair Basha[1], Md. Sirajuddin[1,*]

[1]School of Computer Science and Engineering (SCOPE), VIT-AP University, Amaravati, India
[2]Department of CSE(AI&ML), Vidya Jyothi Institute of Technology, Telangana, India
[3]Department of I.T, Matrusri Engineering College, Hyderabad, India
[4]Department of CSE, Jayamukhi Institute of Technological Sciences, Warangal, India

Abstract

Land registration and record management systems worldwide continue to face significant challenges, including document fraud, long processing times, and inefficient maintenance procedures. Traditional methods involve several technical limitations that reduce reliability and transparency. To address these issues, the proposed system leverages blockchain technology to improve process efficiency, data integrity, and security in land registration workflows. In the proposed framework, users upload property details and supporting land documents while initiating a sale. However, fraudulent document uploads remain a common issue, enabling sellers to receive payments using forged records without the buyer's knowledge. To mitigate such risks, a Convolutional Neural Network (CNN) is integrated to authenticate and validate uploaded land documents before further processing. Only documents verified as authentic are stored on the blockchain. The government authority converts these validated documents into Non-Fungible Tokens (NFTs) and mints them on the Ethereum blockchain. A unique hash is generated for each document, enabling secure verification and traceability through platforms such as Etherscan. Once the documents are confirmed to be valid, the property is approved for sale, and the ownership transfer between the seller and buyer is securely executed through the blockchain enabled system. We evaluated the performance of proposed framework by considering both blockchain performance metrics and CNN evaluation metrics.

Keywords: Blockchain, Land Registration, CNN, Non-Fungible Token, Verification System.

Received on 23 December 2025, accepted on 12 April 2026, published on 03 June 2026

doi: 10.4108/eetiot.11425

1. Introduction

Blockchain plays a vital role in Industry 4.0 globally. It is a decentralized digital ledger technology that allows data to be stored securely and transparently. It is important because it provides a secure and tamper-proof way to store and transfer data and assets without the need for intermediaries like banks or other financial institutions [1-3]. This makes it ideal for a wide range of applications, including financial transactions, supply chain management, identity verification, and more.

One of the key benefits of blockchain is its ability to create trust in a trustless environment, as all transactions are recorded and verified by a network of participants rather than a single entity. By eliminating the need for intermediaries processes, blockchain can help businesses save time and money while also improving security and reducing the risk of fraud.

The traditional land registration process is plagued by fraud, inefficiencies, high costs, and delays due to its reliance

*Corresponding author. Email: siraj538@gmail.com

on centralized authorities and intermediaries. Middlemen often charge excessive fees, and land disputes arise from forged documents, ownership conflicts, and slow verification procedures. Additionally, maintaining accurate land records is challenging due to manual errors, forgery, and lack of a unified digital system. These challenges highlight the urgent need for a secure, transparent, and efficient registration system.

Recent advancements in blockchain technology have led to innovative approaches in land registration systems. Existing studies proposed a novel tokenization method for global digital registers that enhances transparency and reduces transaction costs. Despite these advancements, existing solutions face significant challenges in document authentication, with most frameworks relying on centralized verification authorities or simplistic hash-based validation that cannot detect sophisticated document forgeries. Additionally, current implementations struggle with scalability issues, high transaction costs, and limited interoperability between different blockchain networks. Our research addresses these limitations by integrating Convolutional Neural Networks (CNN) for document verification with NFT-based storage on Ethereum blockchain, providing a comprehensive solution that ensures both the authenticity of land documents and the security of their digital representation.

However, they remain vulnerable to data manipulation, unauthorized access, and corruption. The involvement of multiple intermediaries leads to further complexities, increasing processing time and costs. To address these challenges, this research proposes a blockchain-based decentralized application (dApp) for land registration that integrates deep learning techniques such as Convolutional Neural Networks (CNN) for document authentication. The major contributions of the proposed work are:

(i) Identify the fake documents involved in the land registration process using deep learning techniques.
(ii) The land documents are verified by the government authority who has been assigned by the contract owner.
(iii) NFT (Non-Fungible Tokens) provides the unique hash for each transaction to redeem the information.
(iv) Ensuring the preservation of land documents using Ethereum blockchain.

The remaining part discusses in the following way, Related Work in section 2, proposed methodology in section 3, Security Analysis in section 4, Results and analysis in section 5, Conclusion in section 6.

2. Related Work

Zhou [4], et.al focused on the security and privacy aspects of NFTs (Non-Fungible Tokens) in blockchain storage. The existing approaches for privacy-preserving NFT storage in the blockchain. It provides an overview of the privacy-preserving techniques used to protect the privacy of NFTs in the blockchain such as differential privacy, homomorphic encryption, and zero-knowledge proof, providing a useful resource for researchers and practitioners in the field The disadvantages include Scalability and Energy consumption issues.

Sherwood [5], et.al provided an in-depth analysis of the current infrastructure of the Ethereum blockchain and its suitability for NFT storage. The work discusses the scalability challenges faced by the Ethereum blockchain, including slow transaction times and high transaction fees, and the impact of these challenges on NFT storage. It also provides an overview of the security features of the Ethereum blockchain, including its consensus mechanism and smart contract architecture, and their relevance to NFT storage. The disadvantages of this work include no suitability of other blockchain platforms for NFT storage.

Fan,J [6], presented a CNN-based model for fake document detection and apply transfer learning to the model to enhance its performance. A pre-trained model is used as a starting point for training a new model on a different problem using the machine learning technique. In this work, the authors use a pre-trained model for image classification. Dataset limited size affects in performance of the model with low accuracy are the limitations of this work. Imam et.al [7] has been described the faking of an important documents like land and government documents, educational certificates et cetera in current days. They have proposed an Ethereum blockchain-based technology in P2P cloud storage, also provide a modular application to revolutionize the process of verification. This suggested model incorporates a number of techniques, including cryptographic protocols, online cloud security, user authentication, encoding, P2P networks. However, their system can be consumer Fractionated and does not support of multiple file upload.

Mingdong Tang et.al [8] they discussed about many logistics networking sensing devices are a major aspect of smart logistics. However, they feel that there are many logistics records including responsive information are typically kept in centralised cloud facility because of the absence of local computing and storage capabilities in Iot nodes, which may also easily result in data breaches. The disadvantage include that it does not allow easy modification of data once recorded. Fatemeh Rezaeibagha et.al [9] authors described PHRs (Personal Health Records) having lately been dogged by security vulnerabilities also including private medical information breach, unauthorised access to patient data, and data tampering. Hence, they have proposed a decentralised PHR-sharing algorithm which is based on blockchain and message digest protocol CP-ABE (Ciphertext Policy-Attribute Based Encryption). This work ensures inefficient and complicated since each encryption text must be deciphered with parameters.

3. Proposed Methodology

People have encountered a number of issues with the traditional land registration process, such as time delays and an increase in the number of fraud cases. The proposed

system enhances the process acceleration, transparency and security of current land registration process due to the involvement of blockchain [10-14]. This framework implementation supports public blockchain i.e., Ethereum which uses smart contracts to implement the land registration process. Convolution Neural Networks (CNN) are used to authenticate land documents; only legal documents are accepted and stored in the blockchain.

Table 1. Summary of the Related Work

Authors	BCT	Authority	Implementation/ Design	Tool	Data Privacy	Access Control	Verification
Zhou et al.[4]	Public	No	Only Designed	Not Specified	Yes	Yes	Yes
Sherwood et al.[5]	Public	No	Only Designed	Ethereum	Yes	Yes	No
Fan,J et al.[6]	Private	No	Both	Not specified	Yes	Yes	Yes
Imam et al. [7]	Public	Yes	Not Implemented	Ethereum	Yes	Yes	No
Mingdong et al. [8]	Public	No	Both	Not Specified	Yes	No	No
Fatemeh et al.[9]	Private	No	Not Implemented	Not Specified	Yes	Yes	No
Proposed System	Public	Yes	Both	Ethereum	Yes	Yes	Yes

The blockchain-based Non-Fundable Tokens (NFT) are used to store the documents. The NFT generates a unique hash to the document while storing it in a blockchain as a block transaction. Thus, generated hash value can be used in ether's canto fetch the integrity check of existed transactions. Figure 1 shows the proposed system process architecture. The proposed system consists of three modules such as

a) Land document validation using CNN
b) Valid Document Storage in blockchain
c) Minting of NFT on Ethereum blockchain.

3.1. Land Document Verification Using CNN

The user should connect to the system using the MetaMask or the private key provided in the Ganache. After successfully registering, the user enter the land's information and upload the document. The data is encrypted and stored in blocks, which makes it secure and tamper-proof. The system should be able to classify the documents as valid or not using CNN [15]. The CNN network processes an input document through multiple layers of convolution, activation, pooling, and fully connected layers to predict whether the document is real or fake as shown in Algorithm 1. The trained CNN model can then be used to analyse new documents and determine whether or not they have been manipulated. The process to detect invalid land documents through CNN can be outlined as follows:

3.1.1 Pre-processing

(i) Load and pre-process the dataset of real and fake land images.
(ii) In this module, performs certain operations like resize the images dimension into 224 x 224 x 3, pixel value normalisation, and noise removal

3.1.2 Feature Extraction Using CNN

(i) Train a CNN model on the training set to extract features from images such as edge and font features from the convolution layers, stamp, seal and layout features from the deep layers.
(ii) Use the trained CNN model to extract features from images in the validation and test sets.
(iii) Flatten the extracted feature maps into a feature vector for each image.
(iv) Then dense layers those are in fully connected learn high level decision pattern with the activation of ReLU to detect real or forged document. This total process has shown in Figure 1. But the main objective this paper work is preserving the authorized document into a public blockchain.

3.2 Valid Document Storage in Blockchain

The government authority has the right to verify the user in this module based on the MetaMask account address. The users who have been approved by the government can list their land for sale. Algorithm 2 depicts the storage of land documents in blockchain [16-18] which are considered as valid. The government authority stores the documents in Non-Fungible Tokens (NFT) and mints them on the Ethereum Blockchain in accordance with the ERC-721 standard. This process generates a unique hash value for each document in the Ether scan. Figure 2 shows the proposed system architecture. NFT as an on – chain storage stored the hash value of land document, Token ID of NFT, Wallet Address of the owner, Time stamp, and Transaction hash with Metadata via Ethereum. Full land document was not stored due to gas cost constraints. Hence, generally, the

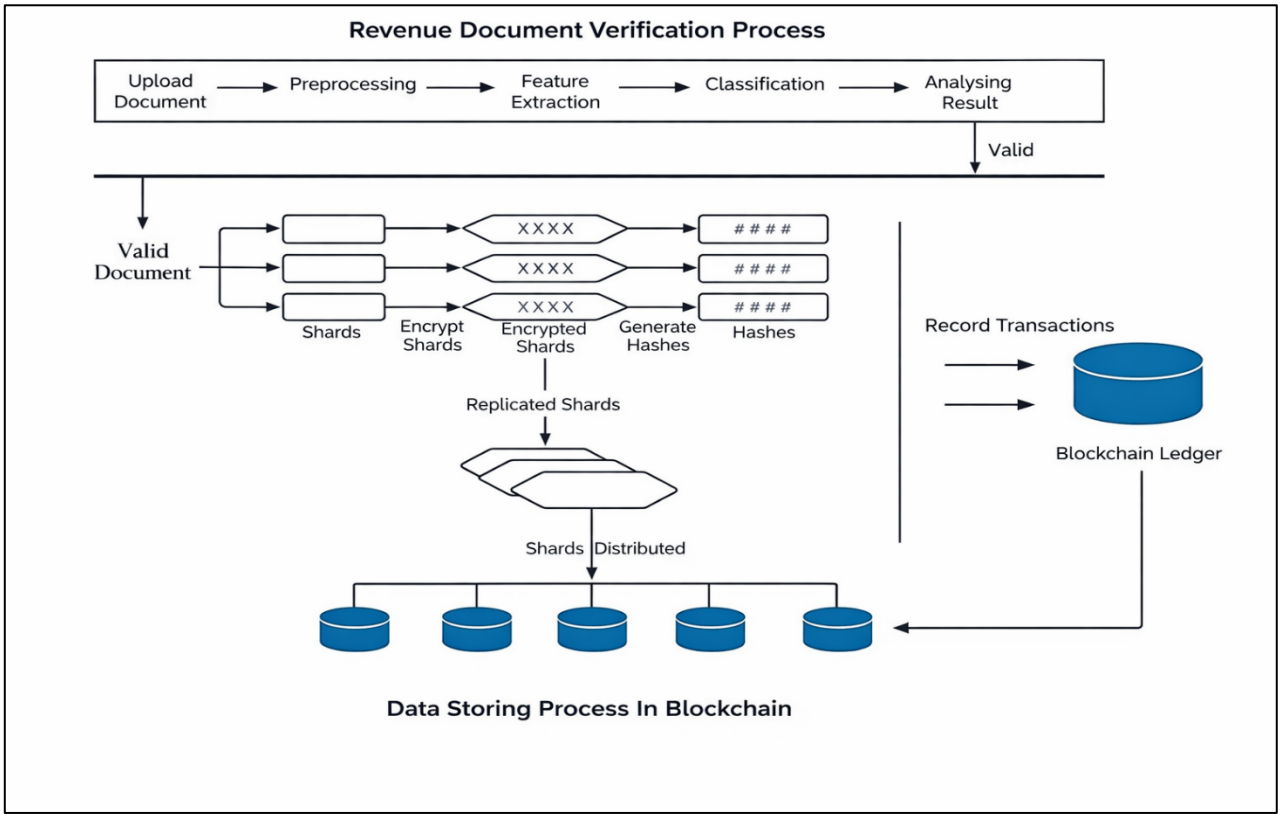

Figure 2. Proposed System Architecture

full land document with the CNN verification logs is stored in IPFS (Inter Planetary File System) as an off -chain storage. NFT data is immutable so if any document alteration changes the hash value of the corresponding land document. Then fails the validation verification phase due to mismatch of hash values which leads to integrity guarantee.

Algorithm 1: Land document validation using CNN

Input: Land document Image 'L' for validation

Output: Determination of authenticity of the document- valid or invalid document

Step 1: Upload dataset and Pre process

Let us consider the dataset has both fake and real documents. $L = \{L_1, L_2, \ldots L_n\}$ and labelled dataset $M = \{ M_1, M_2, \ldots M_n\}$, $M_i \in \{0, 1\}$ to represent (0 = real, 1 = fake)

Step 2: Pre-process the dataset

a. Normalization: The values are scaled to [0, 1]

$$L_i^{Norm} \leftarrow L_i / 255$$

b. Resizing: Each image to be resized to a fixed spatial dimension 224 X 224 X 3

$$L_i^{Resize} \in \mathbb{R}^{224 \times 224 \times 3}$$

c. Data Augmentation: Apply a transformation function T(.) on the resized images

$$L_i^{A} \leftarrow T(L_i^{Resize})$$

d. Dataset Splitting into (L_{train}, M_{train}), (L_{test}, M_{test}), (L_{val}, M_{val})

Step 3: Training for feature extraction using CNN

Apply forward pass using Eq (1) to extract the feature maps then compute the final out probability using Eq (2). Then update the parameters using gradient descent optimization on the result of loss function by binary cross entropy using Eq (3) and Eq (4)

$$f_i \leftarrow FP(L_{train}, \theta) \quad (1)$$

Where θ is trainable parameters like watermarks, seal, signature, etc

$$P_i \leftarrow \sigma (W f_i + b) \quad (2)$$

Where $\sigma (.)$ is the sigmoid function i.e.

$\sigma(z) = 1/(1 + e^{-z})$, w = Weight vector and b =bias

$$£ \leftarrow - \Sigma [(M_{train,\, i} \log (P_i) + (1 - M_{train,\, i}) \log(1 - P_i)] \quad (3)$$

$$\theta \leftarrow \theta - \eta \nabla_\theta £ \quad (4)$$

Step 4: Validation and testing by using Eq (1) and Eq (2)

Features are passed through the fully connected dense layers to get the predicted probabilities.

$f_{val} \leftarrow FP(L_{val}, \theta)$ $\quad$ $f_{test} \leftarrow FP(L_{test}, \theta)$

$P_{val} \leftarrow \sigma (W f_{val} + b)$ $\quad$ $P_{test} \leftarrow \sigma (W f_{test} + b)$

Step 5: Apply decision rule

$$\text{Label} = \begin{cases} 1 \text{ if } p \geq 0.5 \text{ Fake} \\ 0 \text{ if } p < 0.5 \text{ Real} \end{cases}$$

Algorithm 1 shows the step-by-step process of the validation of the document using CNN by addressing the internal logical layers functionalities. As a result of this module, real document will become an input to the next module such as maintain the document in a blockchain which is shown in Algorithm 2.

Algorithm 2: Storage of land documents in blockchain

Input: Land document
Output: Document stored in blockchain
Step 1: Define a hash function H(x) that takes an input x and produces a fixed-length output hash value.
$H(x) = y$, where H is the hash function, x is the input data, and y is the output hash value.
Step 2: Divide the land documents into fixed-size blocks of B bytes. Land document = $B_1, .., B_n$, where B is the block size, and $B_1, .., B_n$ are the individual blocks.
Step 3: Compute 1st block hash value using the hash function H(x). i.e. $H_1 = H(B_1)$
Step 4: Create a block containing the hash value H1 and the first block of land documents, and add it to the blockchain. $Block_1 = (H_1, B_1)$
Step 5: For each subsequent block of land documents, compute the hash value of the block using the hash function H(x), and call it Hn. $Block_n = (H_n, B_n)$
Step 6: Create a new block Bn contains the hash value Hn, and add it to the blockchain. $Block_n = (H_n, B_n)$
Step 7: Each block contains a reference to the previous block in the blockchain. $Block_n = (H_n, B_n, H_{n-1})$,
Step 8: To retrieve Block n: Follow the reference to $Block_{n-1}$, and continue until you reach $Block_1$.

Algorithm 3: Minting of NFT on Ethereum blockchain

Input: Land document
Output: Land Document stored in NFT and minted upon blockchain
Step 1: Let D be the digital representation of the land document, and let FD be the file hash of D:
$$FD = hash(L)$$
Step 2: Let ID be the unique identifier for the NFT:
$$ID = hash(FD)$$
Step 3: To mint the NFT, a smart contract is deployed on the Ethereum blockchain that conforms to the ERC-721 standard:
$$contract = deploy\_contract()$$
Step 4: The minting transaction M that creates the NFT with ID is sent to the Ethereum network:
$$M = contract.mint(ID)$$
Step 5: The minting fee F_{mint} and gas fee F_{gas} are paid in Ether:
$$F_{total} = F_{mint} + F_{gas}\,, \qquad pay(F_{total})$$
Step 6: Monitor the transaction status of M and wait for it to be confirmed: $confirm(M)$
Step 7: View transaction details on Ethers can using the transaction hash of M:
$$details = etherscan.get\_trannsaction\_details(M)$$

The generated hash value can be used in the ether scan to obtain transaction details such as the owner's name, account address, and the file stored in the NFT. Minting of NFT on Ethereum Blockchain is as follows, when the buyer sends the landowner a purchase request, the seller approves the request after the landowner confirms that the requester's address is correct. Once the request is approved, the buyer will be able to acquire the property. If the property is authorised, the funds are transferred from the buyer's to the landowner's account. The Nomics API is used to convert INR (Indian Rupee) into ETH (Ethereum) in real time [19,20], and the resulting amount of ETH is deducted from the buyer's MetaMask account. Algorithm 3 shows the minting of NFT on Ethereum blockchain.

3.3 Dataset Description

The dataset consists of 2819 synthetic land image documents were generated using controlled document simulation for experimental validation. Among them, 1409 images are generated for authentic classified as Class '0' and 1410 images are forgery samples those are generated inspiring by CASIA image tampering detection dataset, classified as class '1'. According to the Pareto rule, 70:30 ratio was considered for splitting the dataset into training and testing.

4. Security Analysis

The proposed blockchain based dApp was examined using five threat scenarios those are as follows.
Theorem 1: Consider a scenario where someone wishes to manipulate the land document which was securely stored in the blockchain.
Proof: The proposed application employs blockchain technology to keep vestige of the property that changes identity and assigns a unique property ID to each of the land document. Each block's hash value will be distinct since it is connected to the previous block's hash. Hence, it will be a challenge for an attacker who would try to access the land documents.

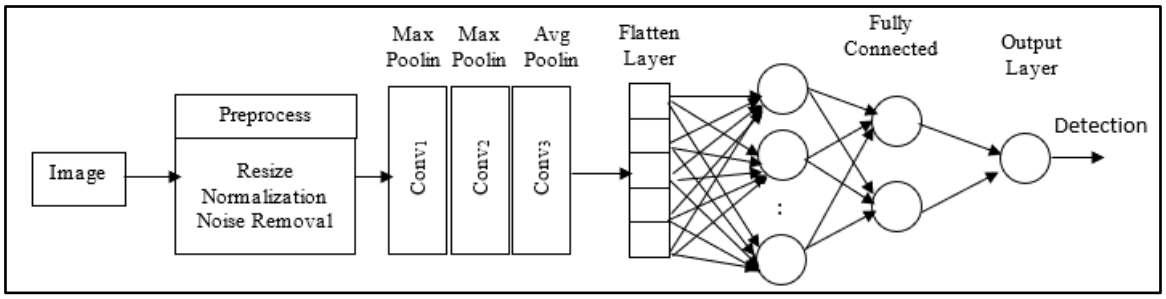

Figure 1. Process of Document Verification

Theorem 2: Consider a scenario where someone tries to impersonate as the owner of the land by uploading fake land documents.
Proof: The proposed system also verifies the uploaded land documents. The dApp has a login created for the government authority who is provided with a username and password used to validate whether the uploaded land documents are legally appropriate or not. The government authority has the right to ratify or prohibit the application of a seller primarily based on the land document and details uploaded. Therefore, it will be difficult for a person to provide fraud or incorrect information regarding the land.

Theorem 3: Consider a scenario where a person tries to attack the seller by providing misleading information such as incorrect account address.
transaction. The network rejects the vendor transaction because it only accepts valid blocks. When transferring land, the vendor should possess at least six corroborate.

4.1. Security Threats and Attacks Analysis

There are several attacks possibilities on blockchain technology, while secure in many ways, is not impervious to security threats and attacks. These attacks can undermine the trust and credibility of the blockchain, which is critical for its adoption and success. Therefore, it's important to implement security measures to prevent these attacks and regularly monitor the network for potential threats. Here are some common security threats and attacks that can occur in a blockchain network [21,22].

4.1.1. DDoS Attack

A DDoS attack aims to overload the enumerate and storage resources of nodes in a blockchain network by overwhelming them with requests, thus causing them to be unable to perform their normal functions and hindering the synchronization of blocks. Our approach to mitigating DDoS attacks is to improve the resistance of the system by expanding the number of nodes, using rate limiting and cloud firewall in the blockchain network.

4.1.2. The Sybil Attack

In P2P networks, the Sybil attack is a common method used to attack data redundancy. This occurs when a malicious node creates multiple virtual nodes using virtualization technology. This can weaken the decentralization of the blockchain and even allow the malicious node to control transaction data and become the central node of the entire network. To address this, our system requires that a node attempting to unite the blockchain provide a outlandish certificate for official authorization. Only one certificate can be held by a single node, ensuring that there is a 1 to 1 relationship between nodes and certificates.

4.1.3. Double Spend Attack

This attack involves rolling back confirmed transactions to reuse tokens, leading to multiple spendings of the same

Proof: The proposed application assigns a unique account address for each user and the seller has an option to verify the request of the buyer. The landowner considers the buyer's wishes and, after conversing with them, decides whether to allow them to purchase the land. They can either accept or deny the request.Hence, it will be a challenge for a person to buy the land with misleading information.
Theorem 4: Consider a double-spending attack that builds a chain to support fraudulent transactions.
Proof: The fault creator generates two transactions with the same amount. A valid block is included in the first transaction. Meanwhile, the attacker conducts a second transaction for the same amount with the vendor. If the vendor agrees to transfer the land and allows the attacker transaction without network confirmation, the attacker instantly sends the mined block that includes the first
digital currency. This would ruin the crypto currency dealing and weaken the immutability of the blockchain. In token-less blockchains, double-spend attacks involve revoking previously confirmed records. Based on the longest chain principle, the revocation can occur if the alternate chain becomes the long-drawn out one. This attack is the foundation of the 51% attack.

Here assumed that blockchain consensus is secure with government authority controls the contract deployment. Users interact the proposed dAPP system through authenticated wallet system. Furthermore, an authority model is assumed that has three main nodes: Registrar Authority (RA), Verified Citizen (VC), and Blockchain Nodes (BN). The Admin Role is played by RA, the User role is played by VC, and Consensus role is played by BN. Table 2 shows the threats analysis with mitigation.

Table 2. Threat Analysis and mitigation

Threat	Risk	Mitigation
DDoS	Services Disruption	Increase number of nodes with rate limiting, Cloud Firewall
Sybil	Fake IDs	KYC (Know your client or customer) based wallet linking system
Double Spend	Ownership Manipulation	Strengthen Blockchain consensus
Insider Attack	Unauthorized minting	Strengthen Role based Access control
Single point of trust	Administer compromise	Multi signature Authentication system (wallet)

5. Results and Analysis

The proposed blockchain-based dApp enhances security, transparency, immutability, and authentication in the land registration system. By integrating Solidity for smart contracts, CNN for document verification, and NFTs for secure storage, automates critical processes, minimize fraud risks and ensures data integrity. Table 3 summarizes the gas

consumption and transaction sizes for each smart contract, offering insights into the computational cost of executing these operations. The results indicate that the system significantly reduces manual record maintenance effort by 99%, streamlining property verification and transfer processes.

Table 3. Gas Cost for Operations Performed in System

Caller	Function Name	Gas cost	TxN size (In bytes)
Administrator	isUserRegistered()	0.00089481	36 bytes
Administrator	verifyUser()	0.00087382	36 bytes
Administrator	isUserVerified()	0.0007493	6 bytes
Administrator	addLand()	0.00057118	34 bytes
Administrator	transferOwnership()	1.05184002	132 bytes

Figure 3 illustrates the MetaMask-based ETH balance, which plays a crucial role in executing the operations of the proposed blockchain-based system. MetaMask serves as a digital wallet that facilitates secure transactions and interactions with the Ethereum blockchain. This balance represents the amount of ETH available to users, which is required to cover transaction fees, smart contract executions, and operations.

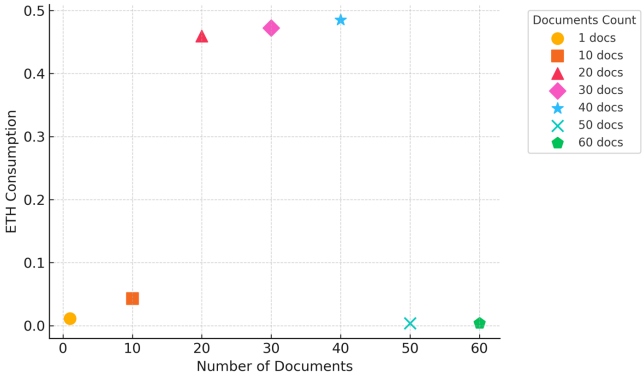

Figure 3. Eth consumption for number of documents

Table 4 presents the ETH consumption for varying numbers of documents, ranging from 1 to 10. It details the Gas Limit, ETH Cost, Price, Total ETH Consumption, and Document Size, providing a comprehensive overview of blockchain resource utilization. Figure 4 illustrates the block information in Ganache, displaying the total number of blocks and transactions per block, which offers insights into the system's performance and scalability. The findings suggest that implementing Layer-2 scaling solutions could further optimize transaction costs.

Table 4. Gas Cost for Operations Performed in System

No. of Documents	Gas Limit (in Units)	EthCost (Total)	Price (in CGWEI)	ETH Total	Document Size (KB/MB)
1	28499	0.01138	20	0.01138	139 KB
10	73805	0.04287	20	0.2279	52 KB
20	59728	0.45953	20	0.02574	51 KB

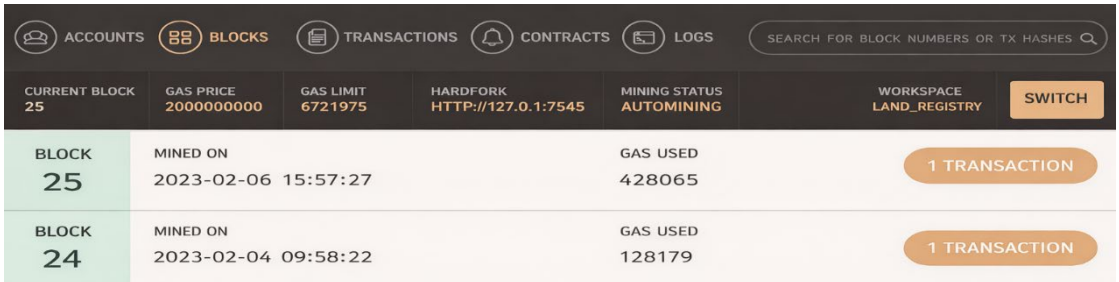

Figure 4. Block Information in Ganache

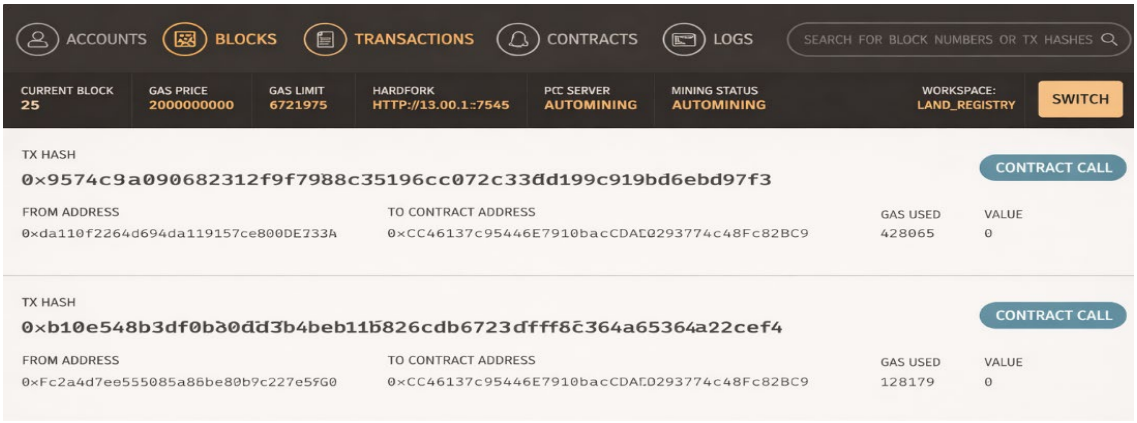

Figure 5. Transaction details in Ganache

Table 5 outlines the operational costs associated with smart contract function related to land document management within the blockchain environment, highlighting the efficiency of transaction execution.

Table 5. Cost Operations Performed on a System

From Address: 0x36a27d9fAC8C7FA89e93072092Fe50dE2F712220							
To Address: 0xdda010F26d46E09b14F91576ceBD80EEd52A193E							
Function	Amount Gasused	Fee (TxN)	Hash (TxN)	Block Details (Mine)	Block size (Bytes)	Nonce (TxN)	Index (TxN)
isRegistered User( )	1138	0.00113 8 Eth	0x1649261e01550957dd8b aa8527790ca1f7526fda956 d93ce6f229f90bcf1b993	57	132	40	57
verifyUser( )	861	0.00086 1 Eth	0x615ec41c5b56707566933 a741346a5f1e4941045ed36 e009fefec2c86817c3a3	168	4	150	168
isUserVerifi ed( )	1619	0.01619 Eth	0xb71c0b33b37b034e4c879 d21648952d0f04a012d05e3 f83b19e6c8334cc25d54	170	36	162	172
addLand( )	15879	0.15879 Eth	0x34c895c20880c429595ef 922b23bd5194a43aec3181a 046414b07237d3b460a8	187	8	175	178
transferOwn ership( )	1138	0.1138 Eth	0x4316Fb7f44E2715c614C 15B9aB62b6a3184aa84c00 7763213d394d66	194	8	179	182

Table 6 compares our proposed system with existing studies, emphasizing key differences in authorization mechanisms, cryptocurrency integration, and document verification techniques.

Table 6. Cost Operations Performed on a System

Authors	Authorization	dAPP	Crypto-currency	Doc. Integrity Technique
Zhou [4], et.al	NE	No	Not Specified	External Checker
Sherwood [5], et.al	NE	No	ETH	NE
Fan,J [6]	NE	Yes	Not specified	CNN
Imam et.al [7]	Admin Authority	No	ETH	NE
Mingdong Tang et.al [8]	NE	Yes	Not Specified	NE
Fatemeh et.al [9]	NE	No	Not Specified	NE
Madhu et.al[11]	Trusted Domain Authority	No	Not specified	Reward based DQlearning

Liu et.al[17]	SupplyChain – Kernal PCA	No	Not specified	DeepESN
Proposed System	Admin Authority	Yes	ETH	CNN

NE* - Not Existed

Figure 5 illustrates the transaction details in Ganache, depicting the hash values for transactions between seller and buyer addresses. These transaction details are critical for ensuring security, traceability, and fraud prevention within the system.

The significance of these findings extends beyond technical improvements to practical applications in governance and property management. By reducing manual record maintenance effort by 99% and streamlining verification processes, our system addresses critical inefficiencies in traditional land registration that particularly affect developing economies. The integration of CNN for document authentication represents a paradigm shift in how blockchain technology can be applied to real-world document verification challenges, creating opportunities for similar applications in other domains requiring secure document management, such as healthcare records, educational certificates, and legal contracts.

5.1 Evaluation Details

The performance was evaluated using certain quantitative metrics [19] such as confusion matrix, accuracy, precision, recall and F1-Score. Figure 6 shows the confusion matrix based analysis report. According the values from Figure 6 evaluated the other metrics performance where as 92.4% of accuracy, 92.7% of Precision forgery Class -1, 92.1% of Recall forgery class -1 and 92.4% for F1-score. These are evaluated using the following formulas

Accuracy = [TP + TN] / [TP + TN + FP +FN]
Precision = [TP] / [TP + FP]
Recall = TP / [TP + FN]
F1 Score = [2 x (precision x Recall)] / [Precision Recall]

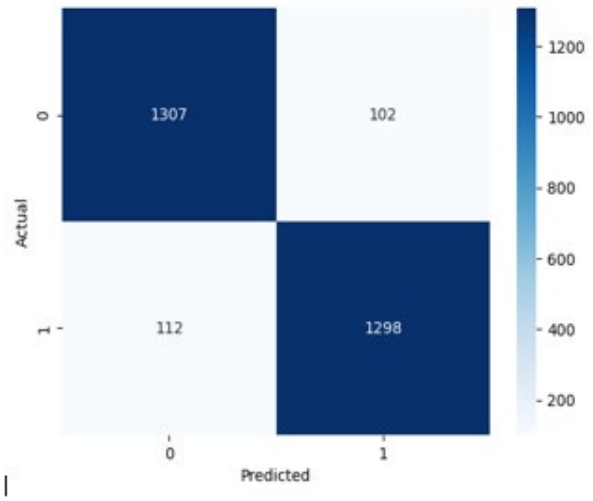

Figure 6. Evaluation Matrix

6. Conclusion

In this work, we have proposed and implemented a blockchain-based land registry document verification system, addressing key challenges in traditional land registration processes. By leveraging blockchain technology, smart contracts, and NFT-based verification, our approach ensures transparency, security, and immutability in land transactions. The integration of Convolutional Neural Networks (CNN) for document authentication further enhances fraud detection, reducing the risks associated with fake land documents. Beyond providing a secure and efficient solution, our research contributes to the broader adoption of decentralized applications in real-world scenarios. The findings demonstrate that blockchain can significantly streamline administrative processes, reducing the reliance on intermediaries and manual record-keeping. However, challenges such as scalability, transaction fees, and regulatory compliance still need to be addressed for widespread adoption. Future research could explore integrating artificial intelligence (AI) and machine learning techniques to improve document verification accuracy and fraud detection.

References

[1] Ramakurthi, V.B. et al. 2026. A Block chain and Neural Network Approach to Enhancing Reverse Logistics of Electronic Gadget Life Cycle Tracking. *EAI Endorsed Transactions on Digital Transformation of Industrial Processes*. 1, 4 (Jan. 2026). DOI:https://doi.org/10.4108/dtip.9841.

[2] K, L. et al. 2024. Blockchain Technology for Manufacturing Sector. *EAI Endorsed Transactions on Internet of Things*. 10, (Aug. 2024). DOI:https://doi.org/10.4108/eetiot.7034.

[3] Ch. Rupa, Divya Midhunchakkaravarthy, Mohammad Kamrul Hasan, Hesham Alhumyani, Rashid A. Saeed. Industry 5.0: Ethereum blockchain technology based DApp smart contract[J]. Mathematical Biosciences and Engineering, 2021, 18(5): 7010-7027. doi: 10.3934/mbe.2021349.

[4] Zhou, J., Song, M., & Wang, W. (2022). Secure and Privacy-Preserving NFTs in Blockchain Storage. Journal of Information Security and Applications, 56, 102198.

[5] Sherwood, M. C. (2021). NFT Storage on the Ethereum Blockchain: An Analysis of Scalability, Security, and Sustainability. Journal of Information Technology and Politics, 18(1), 1-15.

[6] Fan, J., Zhang, Y., Chen, Y., & Zhang, J. (2020). Fake Document Detection Using Convolutional Neural Network with Transfer Learning. Applied Sciences, 10(17), 6098

[7] T. Imam, Y. Arafat, K. S. Alam and S. A. Shahriyar, "DOC-BLOCK: A Blockchain Based Authentication System for Digital Documents," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 1262-1267, doi: 10.1109/ICICV50876.2021.9388428.

[8] H. Li, D. Han and M. Tang, "A Privacy-Preserving Storage Scheme for Logistics Data With Assistance of Blockchain," in IEEE Internet of Things Journal, vol. 9, no. 6, pp. 4704-4720, 15 March15, 2022, doi: 10.1109/JIOT.2021.3107846.

[9] L. Zhang, T. Zhang, Q. Wu, Y. Mu and F. Rezaeibagha, "Secure Decentralized Attribute-Based Sharing of Personal Health Records With Blockchain," in IEEE Internet of Things Journal, vol. 9, no. 14, pp. 12482-12496, 15 July15, 2022, doi: 10.1109/JIOT.2021.3137240.

[10] O. Mayer and M. C. Stamm, "Exposing Fake Images With Forensic Similarity Graphs," in IEEE Journal of Selected Topics in Signal Processing, vol. 14, no. 5, pp. 1049-1064, Aug. 2020, doi: 10.1109/JSTSP.2020.3001516.

[11] Madhu, G. and Peroumal, V. 2025. Blockchain-Assisted Authentication and Energy-Efficient Clustering Framework for Secure IoT Communication. *EAI Endorsed Transactions on Internet of Things*. 11, (Dec. 2025). DOI:https://doi.org/10.4108/eetiot.9520.

[12] Rupa, C., Srivastava, G., Gadekallu, T.R., Maddikunta, P.K.R., Bhattacharya, S. (2021). A Blockchain Based Cloud Integrated IoT Architecture Using a Hybrid Design. In: Gao, H., Wang, X., Iqbal, M., Yin, Y., Yin, J., Gu, N. (eds) Collaborative Computing: Networking, Applications and Worksharing. CollaborateCom 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 350. Springer, Cham. https://doi.org/10.1007/978-3-030-67540-0_36.

[13] C. Rupa and D. Midhunchakkaravarthy, "Preserve Security to Medical Evidences using Blockchain Technology," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2020, pp. 438-443, doi: 10.1109/ICICCS48265.2020.9120948.

[14] Leo Raju, S Surabhi, K M Vimalan, "Blockchain based energy transaction in microgrid", 2022 IEEE 19th India Council International Conference (INDICON), pp.1-6, 2022.

[15] Zaher Haddad, Mostafa M. Fouda, Mohamed Mahmoud, Mohamed Abdallah, "Blockchain-based Authentication for 5G Networks", 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), pp.189-194, 2020.

[16] S. Sivanantham, M Sakthivel, V. Krishnamoorthy, N. Balakrishna, V. Akshaya, "Reliable Data Storage and Sharing using Block chain Technology and Two Fish Encryption", 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), pp.561-565, 2022.

[17] Liu, Y. 2024. Research on Credit Risk Prediction Method of Blockchain Applied to Supply Chain Finance. *EAI Endorsed Transactions on Scalable Information Systems*. 11, 6 (Mar. 2024). DOI:https://doi.org/10.4108/eetsis.5300.

[18] Sultana, S.A.; Rupa, C.; Malleswari, R.P.; Gadekallu, T.R. IPFS-Blockchain Smart Contracts Based Conceptual Framework to Reduce Certificate Frauds in the Academic Field. Information 2023, 14, 446.

[19] G. Kusuma, C. Rupa, S. Reshma and G. Rochana, "Secure Storage of Land Records and Implementation of Land Registration using Ethereum Blockchain," 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2023, pp. 404-409, doi: 10.1109/ICAIS56108.2023.10073887.

[20] Rupa, C.; Midhun Chakkarvarthy, D.; Patan, R.; Prakash, A.B.; Pradeep, G.G. Knowledge engineering–based DApp using blockchain technology for protract medical certificates privacy. IET Commun. 2022, 16, 1853–1864.

[21] Muath A. Obaidat, Joseph Brown, "Perspectives of Blockchain in Cybersecurity", Industry Use Cases on Blockchain Technology Applications in IoT and the Financial Sector, pp.109, 2021.

[22] C. Rupa, G. S. Varshitha, D. Divya, T. R. Gadekallu and M. J. Piran, "Blockchain-based DApp for Drug Supply Chain with AI-driven Drug Recommender System," in IEEE Consumer Electronics Magazine, 2025 doi: 10.1109/MCE.2025.3536326.

[23] Kuznetsov, Oleksandr, Emanuele Frontoni, Kateryna Kuznetsova, Ruslan Shevchuk, and Mikolaj Karpinski. "NFT Technology for Enhanced Global Digital Registers: A Novel Approach to Tokenization." Future Internet 16, no. 7 (2024): 252.

[24] Mendelson-Shwartz, Eynat, Ofir Shwartz, and Nir Mualam. "Protecting street art rights using an NFT-based system." Journal of Urban Technology 30.3 (2023): 81-100.

[25] Vivekrabinson, K., Bharath Singh, Rajesh Kumar, M. Vijay, and D. Vijayakumar. "Blockchain Enabled Real Estate Property Transactions using NFT: An Approach." In 2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), pp. 1-6. IEEE, 2023.