ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

LANDCRYPT: A LIGHTWEIGHT ENCRYPTION FRAMEWORK FOR TRUSTED LAND INFORMATION MANAGEMENT

BOYINA GOPI RAJU[1], AVULA SPANDANA[2].

[1] HOD &Associate Professor, Department of CSE, Chirala Engineering College, Chirala, Andhra Pradesh, India-523157.

Email: rajuboyina001@gmail.com

[2] PGS Student, Department of CSE, Chirala Engineering College, Chirala, Andhra Pradesh, India-523157

Email: spandana.baby22@gmail.com

ABSTRACT

Land record management has evolved from handwritten registers to partially computerized systems; however, many administrative processes, including ownership verification, record maintenance, and land transaction validation, still depend on manual procedures. This reliance on physical documents and human intervention often results in duplicate records, ownership disputes, unauthorized modifications, document tampering, and difficulties in retrieving historical land information. Existing systems also lack secure data-sharing mechanisms, reliable backup facilities, comprehensive audit trails, and adequate protection of sensitive information during storage and transmission, leading to reduced efficiency and transparency. To address these challenges, this paper presents a Digital Land Record Storage and Ownership Verification (DLRSOV) System, a secure web-based platform for efficient digital management of land records. The proposed system enables administrators, Mandal Revenue Officers (MROs), and landowners to perform record management, ownership verification, and ownership transfer through a role-based workflow. It is developed using the Flask framework for interactive web access and TinyDB for lightweight and organized data storage. To ensure confidentiality and data integrity, the system employs Salsa20 cryptographic encryption for secure backup generation, encrypted record downloads, and protected information sharing. Role-based authentication further restricts unauthorized access and enhances operational security. By integrating automated verification, encrypted storage, searchable digital repositories, and secure transaction processing, the proposed system minimizes manual effort, strengthens transparency and accountability, improves data protection, and provides a reliable, efficient, and trustworthy solution for modern digital land record management.

Keywords: Land Records Management, Role-Based Access Control (RBAC), Salsa20 Encryption, Cryptographic Security, Flask Web Application.

1. INTRODUCTION

A recent survey highlighted that 37% of employees in US firms reset their passwords more than 50 times each year and have been losing around 426 USD annually due to password glitches, in addition to the fact that this is affecting their efficacy at work. Additionally, a world bank survey revealed that around 14% of the global population lacks proof of identity in any form. Providing individuals with an identity and maintaining secure and reliable identity storage are major challenges. Compared with providing

individuals with an identity, managing a secured and reliable identity is a far more significant challenge. In a recent incident, Cambridge Analytica leaked 87 million Facebook users' PII details due to a security breach in the system of a third-party service provider. There are many examples of data breaches due to the centralized nature of data recordings and the use of third-party service providers. Digital identities and their security are becoming more critical with the advancement and adaptation of online services. The main problem with the current system is inadequately coordinated information across different government departments that are not coordinated adequately, making it easy for unscrupulous officials to modify official land records. Many fraud cases related to land titling are only detected locally, which means that a centralized system is insufficient in this case. As a result, land records may be tampered with, and forged. Verifying the identity of all participants in a transaction is essential to avoid fraud. Current land registry systems have several shortcomings which can be avoided by using Decentralized System.

2. LITERATURE SURVEY

Johannes Pandeni Paavo et, al. [1] presented a Blockchain Land Registration system designed as a tool for enhancing land administration in South Saharan Africa (SSA). Drawing inspiration from Namibia, we have developed a user interface comprising a homepage/landing page, a users' registration form, a login form that incorporates MetaMask authentication prompts, and an authenticated dashboard for landowners and purchasers.

Mitrea et, al. [2] proposed a decentralized, blockchain-based property platform designed to streamline these processes using Non-Fungible Tokens (NFTs) and artificial intelligence (AI) agents to modernize public-sector asset management. The work addressed the persistent inefficiencies of paper-based property registration and ownership transfer by embedding legal and administrative logic within smart contracts and automating compliance through an intelligent conversational interface.

Muhammad Masood Tariq et, al. [3] presented government-controlled systems demonstrate inadequate proficiency along with safety protocols to execute fair inheritance distribution, mainly impacting marginalized populations. This research introduced a blockchain system known as the Land Registration and Inheritance Automation System (LRIAS) which prioritizes the female protection of inheritance privileges.

Reyan M. Zein et, al. [4] facilitated secure and transparent land transactions from planning to certificate issuance, but also integrates the management of land sales, significantly reducing the need for intermediaries. By providing a detailed exploration of the system's goals, technical hurdles, and practical deployment insights, this research contributes valuable knowledge to the implementation of blockchain technology in LR, with findings that are applicable to similar contexts globally.

Yang Yang et, al. [5] examined the impact path of land property rights on forest resources. The estimation results show that both the forestland use right and disposal right are able to significantly improve the forest output by encouraging households to invest and optimizing the allocation of forestry labor. Particularly, the results revealed that the use right has a positive impact on forest output through forestland investment.

Kusmiarto Kusmiarto et, al. [6] evaluated the readiness of a land office to achieve digital transformation visions. Here, we apply the Digital Governance Assessment Framework (DGRA), adapted to the land service sector, as the basis for conducting this evaluation. The nine core indicators of the DGRA toolkit are used as a basis for assessment. Desk studies were conducted to identify formal legislation and to find the technical specifications.

Shewakena Aytenfisu Abab et, al. [7] explored the factors that influence the acceptance and actual use of national rural land administration information system (NRLAIS) to gauge its operational success in Ethiopia. Data were

collected both from primary and secondary sources using surveys, key informant interviews, and a literature review. Survey data were collected from 201 staff of 50 woreda land administration offices in three regional states (Amhara, Oromia, and SNNP) and analyzed using a structural equation model.

Pierre-François Blin et, al. [8] introduced a series of principles for cyber risk management applied to Land Administration Systems. The aim is to maintain the integrity of cadastral data and land transactions while maintaining vulnerability awareness and risk treatment. The methodology combined Business Process Modeling Notation (BPMN) 2.0, EBIOS Risk Manager and Obérisk in compliance with ISO standards.

Aldi Azmi Arfian et, al. [9] demonstrated the viability of our proposed methodology for encrypting color images using the Salsa20 algorithm, renowned for its stream cipher characteristics, which inherently afford it a swift processing speed. The encryption method they used is to take each pixel from the original image and convert it into bytes based on the RGB value in it, then encrypt it using a keyword that has been converted using a hash function.

Musaab I. Hameed et, al. [10] presented a method that provides security and privacy for data stored on the cloud, and this method consists of a combination of two lightweight algorithms (mCrypton and salsa20) to form a new lightweight hybrid algorithm based on the mCrypton algorithm, where stages were added to it and other modifications. Additionally, chaos has been added to generate encryption keys.

Rebwar Khalid et, al. [11] delved into the prevalent cryptographic methods and algorithms utilized for prevention and stream encryption, examining their encoding techniques such as advanced encryption standard (AES), Blowfish, Twofish, Salsa20, and ChaCha20. The primary objective of this research is to identify the optimal times and throughputs (speeds) for data encryption and decryption processes.

Yunliang Li et, al. [12] defined the model, divides roles into abstract roles and specific roles, and designs the operating process of the access control model. The model has four characteristics: support role name repetition, platform–domain isolation management, inter-domain isolation management, and fine-grained cross-domain sharing.

3. PROPOSED SYSTEM

The proposed methodology as shown in Fig. 1 follows a structured and secure approach for managing digital land records with a strong focus on ownership verification, controlled access, and tamper detection. It adopts a layered architecture that integrates user interaction, backend processing, secure storage, and encryption mechanisms to protect sensitive land data. All system operations begin with authenticated user access and proceed through role-based validation to ensure authorized actions. A centralized web-based framework enables seamless interaction between landowners and administrative authorities while maintaining operational consistency. Data is persistently stored using a lightweight database that supports ownership history, transfer records, and audit logs. Encryption mechanisms safeguard data during storage, transmission, and backup processes.



Fig. 1: System architecture of digital land record storage system

User Interaction and Role-Based Access: Users such as administrators, MROs, and landowners interact with the system through a web-based interface. Each user logs in with

assigned credentials, and access is strictly controlled based on roles. This ensures that users can perform only authorized actions such as viewing, verification, or approval.

Request Handling through Web Application: All user actions are forwarded to the Flask-based web application, which acts as the central controller. The backend validates sessions, enforces permissions, and routes requests to appropriate functional modules. This layer ensures secure and coordinated system operation.

Land Record Storage and Management: Land records are stored in a structured TinyDB database that maintains ownership details, verification status, and historical updates. The system supports record entry, search, and retrieval operations while ensuring data consistency. All database interactions are mediated through the backend.

Ownership Verification and Audit Logging: Verification activities are performed by authorized officials to confirm land ownership authenticity. Every verification and update is logged with timestamps and user identity, creating a reliable audit trail. This enhances accountability and supports dispute resolution.

Secure Transfer Processing: Ownership transfer requests initiated by landowners are reviewed and approved or rejected by verification authorities. The system updates ownership records only after successful validation. This controlled workflow prevents unauthorized ownership changes.

Security, Backup, and Data Sharing: Sensitive data is encrypted using secure encryption mechanisms before storage, download, or backup. The system supports encrypted backups, secure record downloads, and protected messaging between roles. These measures ensure confidentiality, tamper resistance, and long-term data protection.

Salsa20 Encryption

Salsa20 is a high-speed symmetric stream cipher designed to provide strong data confidentiality with low computational overhead. It uses a fixed-length secret key along with a unique nonce to generate a secure keystream for encryption. The encryption process operates on data streams, making it well suited for real-time applications and secure file handling. Each encryption operation produces a different ciphertext even for identical inputs due to nonce variation. This property helps prevent replay and pattern-based attacks. Salsa20 is known for its simplicity, efficiency, and resistance to cryptanalytic attacks. Its lightweight design makes it suitable for systems requiring fast and secure data protection.

Key and Nonce Initialization: The Fig. 2 encryption starts by loading a fixed-length secret key and generating a unique nonce for the encryption session. The nonce ensures that the same key does not produce identical keystreams. This step forms the initial secure state for encryption.

State Matrix Formation: The key, nonce, and constant values are arranged into an internal state matrix. This matrix acts as the foundation for keystream generation. Proper initialization ensures randomness and resistance to predictable patterns.

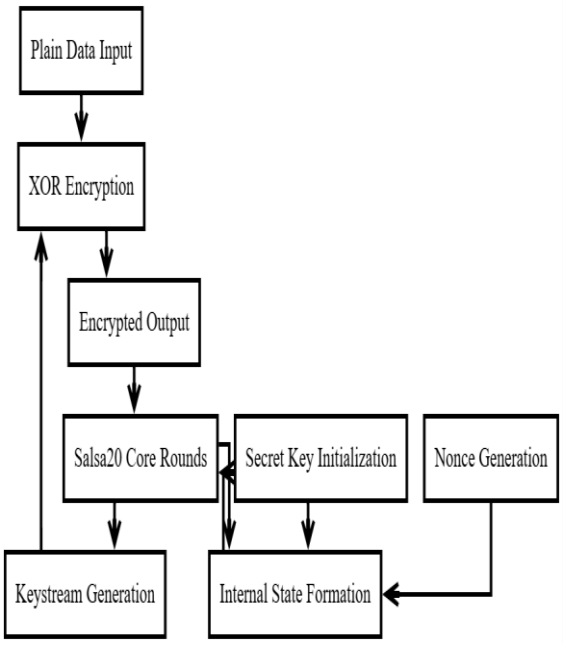


Fig. 2: Internal workflow of Salsa20 encryption.

Round-Based Mixing Process: The cipher performs multiple rounds of arithmetic and bitwise operations on the state matrix. These operations thoroughly mix the internal state to

create strong diffusion. This step is critical for cryptographic strength.

Keystream Generation: After completing the mixing rounds, the cipher produces a keystream block. The keystream appears random and is independent of the plaintext. This keystream is used directly for encryption.

Ciphertext Formation: The plaintext is encrypted by XORing it with the generated keystream. The resulting ciphertext is combined with the nonce and prepared for secure storage or transmission. This completes the encryption process.

Encryption and Output Formation: The plaintext is encrypted by XORing it with the generated keystream. The resulting ciphertext is combined with the nonce and prepared for secure storage or transmission. This ensures safe data handling.

Salsa20 Decryption

Salsa20 decryption is a symmetric stream-based process that reconstructs the original data using the same secret key and nonce employed during encryption. The encrypted input contains both the nonce and the ciphertext, allowing the cipher to regenerate the identical keystream used earlier. Decryption relies on deterministic keystream generation rather than reversing encryption rounds. By XORing the ciphertext with the regenerated keystream, the original plaintext is recovered. This approach ensures fast and reliable data recovery with minimal computational overhead. The design maintains strong security while supporting real-time and large-scale data processing.

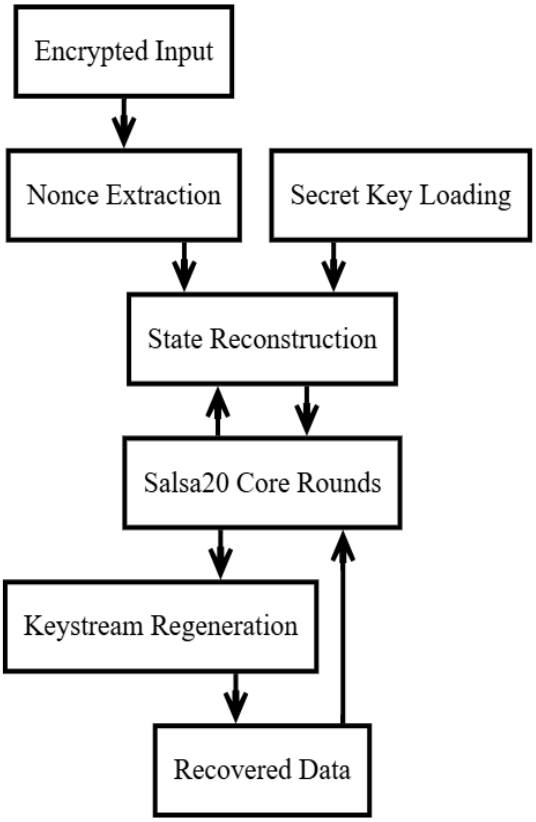


Fig. 3: Internal workflow of Salsa20 decryption.

Encrypted Input Handling: The Fig 3 flow starts when encrypted data is received along with the embedded nonce. The nonce is separated from the ciphertext to prepare the cipher state. This step ensures correct session alignment for decryption.

Key and Nonce Loading: The secret key and extracted nonce are loaded into the decryption engine. These inputs recreate the original cipher configuration. Proper loading is critical for accurate keystream regeneration.

State Reconstruction: The cipher rebuilds its internal state using constants, key, and nonce. This state mirrors the one used during encryption. It forms the basis for deterministic keystream production.

Round-Based Transformation: Multiple rounds of arithmetic and bitwise operations are applied to the state. These rounds regenerate the same pseudo-random sequence. The process ensures cryptographic consistency.

Keystream Regeneration: A keystream identical to the encryption phase is produced. This stream is independent of the ciphertext

content. It enables direct recovery of original data.

Plaintext Recovery: The ciphertext is XORed with the regenerated keystream. This operation reveals the original plaintext. The recovered data is then made available to authorized components.

4. Results Description

Fig. 4 illustrates the Digital Land Record Storage Home Page Screen, which serves as the primary access point for users interacting with the digital land record system. It introduces the platform's purpose of managing land ownership data in a centralized and secure manner. The screen enables users to proceed toward authenticated access based on their designated roles. It provides a structured entry to various land-related services offered by the system. This page establishes the foundation for secure, role-based interaction with digital land records.

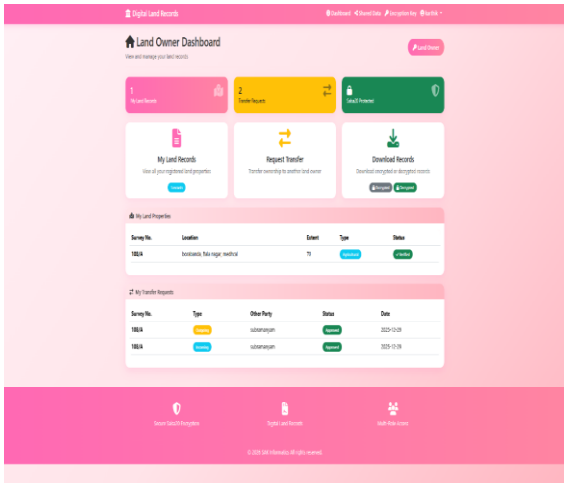


Fig 4: Digital Land Record Storage Home Page Screen

Fig. 5 illustrates the Admin Dashboard Screen, which allows administrators to monitor and manage the overall functioning of the land record system. It provides access to user management, system reports, and record oversight functions. The dashboard enables administrators to review system statistics and operational status. It supports decision-making by offering consolidated control over platform activities. This screen ensures efficient governance and centralized administrative control.

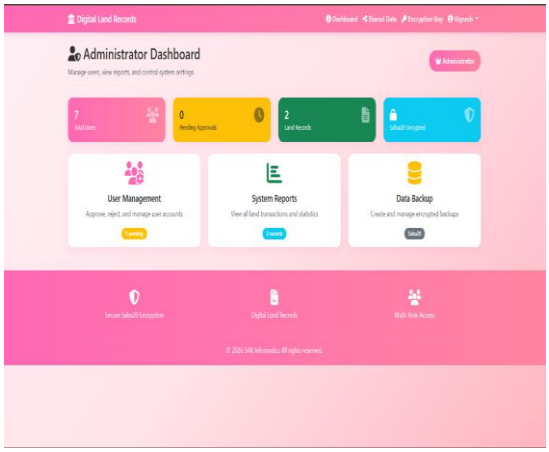


Fig. 5: Admin Dashboard Screen

Fig. 6 depicts the Data Backup Management Screen, which facilitates the creation and management of secure backups of system data. It ensures that land records and user information are protected against data loss. The screen supports encrypted backup generation for system recovery purposes. It contributes to data reliability and long-term storage assurance. This feature is essential for maintaining system resilience and data safety.

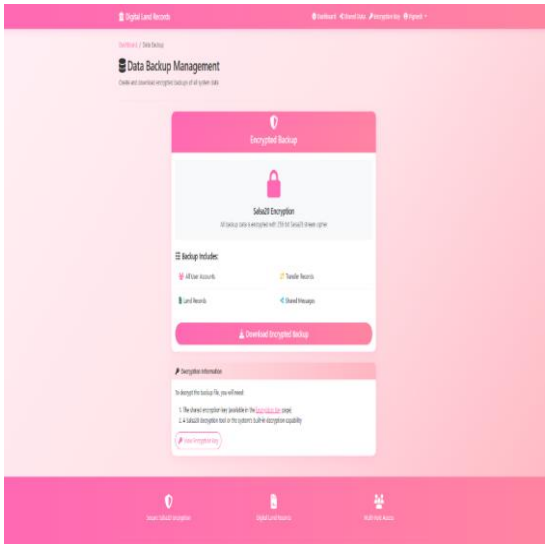


Fig. 6: Data Backup Management Screen

Fig. 7 depicts the Land Record Entry Screen, which is used for creating and registering new land records in the system. It captures essential land, boundary, and ownership details required for record generation. The screen ensures standardized data entry for land registration. It supports official documentation and verification processes. This interface is critical for maintaining accurate and structured digital land records.

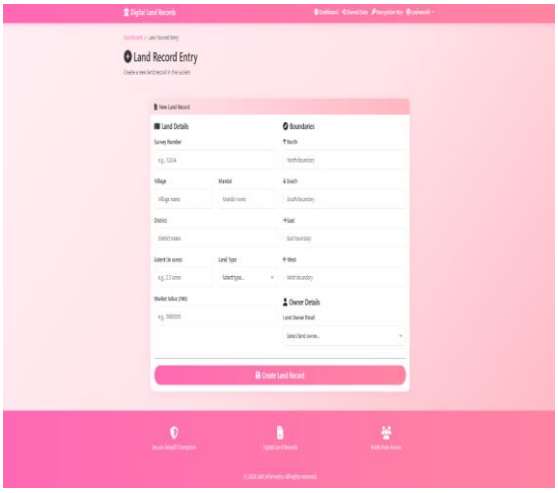


Fig. 7: Land Record Entry Screen

Fig. 8 illustrates the Record Verification Screen, which is used to authenticate and validate land ownership records within the system. It enables authorized officials to review land details, ownership information, and boundary data before confirmation. The screen supports verification of records submitted into the digital repository. It plays a critical role in preventing fraudulent or incorrect land entries. This process ensures that only verified land records are marked as authentic in the system.

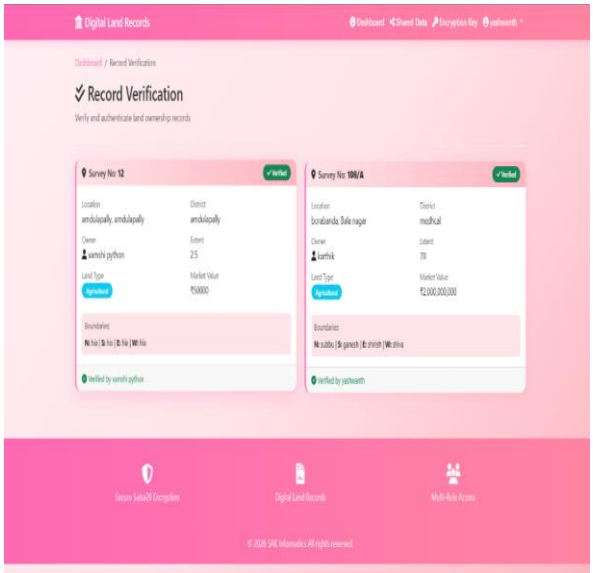


Fig. 8: Record verification Screen

Fig. 9 depicts the Transfer Management Screen, which facilitates the processing of land ownership transfer requests. It allows officials to review transfer details between current and proposed owners. The screen supports approval and tracking of ownership changes initiated by users. It ensures that all transfers follow official verification and authorization procedures. This functionality helps maintain accuracy and legal validity of ownership records.

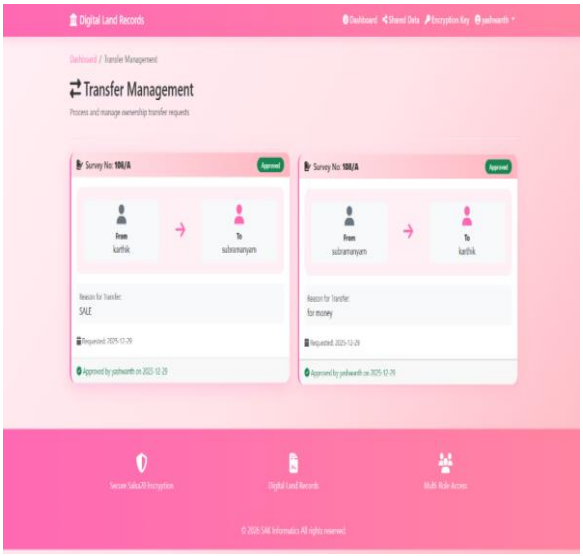


Fig. 9: Transfer Management Screen

Fig. 10 depicts the Request Ownership Transfer Screen, which is used by landowners to initiate the transfer of property ownership. It allows users to select registered land and specify the new owner details. The screen captures the reason for transfer and submits the request for official review. It integrates the ownership transfer workflow with administrative verification. This ensures that ownership changes follow a structured and regulated process.

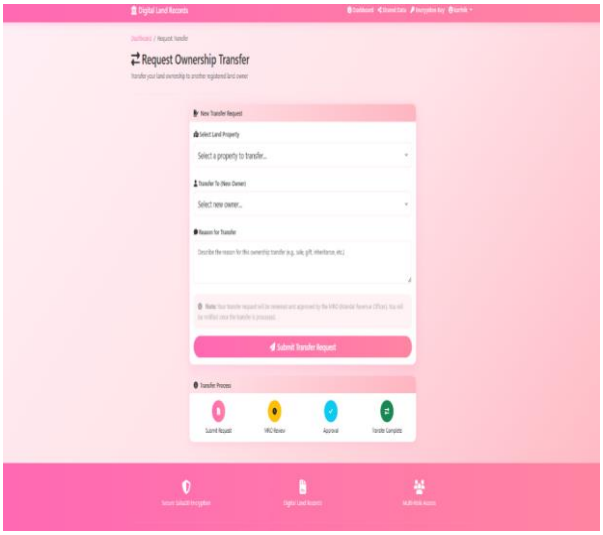


Fig. 10: Request Ownership Transfer Screen

5. Conclusion

This research successfully demonstrates the implementation of a secure and efficient DLRSOV system using a web-based

architecture. By integrating role-based access control, encrypted data storage, and structured verification workflows, the system significantly improves transparency and trust in land record management. The use of Salsa20 encryption ensures fast and reliable data protection with minimal computational overhead, resulting in improved system performance during record storage, retrieval, and backup operations. Lightweight data management using TinyDB reduces latency and enables quick read/write operations compared to traditional database-heavy solutions. Automated verification and controlled ownership transfer workflows minimize manual intervention, thereby reducing processing time and human error. Audit logging enhances traceability and accountability, supporting dispute resolution and legal validation. The modular Flask-based backend improves scalability and maintainability, allowing efficient handling of concurrent user requests. Overall, the system delivers better performance, stronger security, and higher reliability than conventional manual or semi-digital land record systems.

REFERENCES

[1] Paavo, J.P.; Rodríguez-Puentes, R.; Chigbu, U.E. Practicality of Blockchain Technology for Land Registration: A Namibian Case Study. Land 2025, 14, 1626. https://doi.org/10.3390/land14081626

[2] Mitrea, D.A.; Marian, C.V.; Manolescu, R.A. Digital Transformation: Design and Implementation of a Blockchain Platform for Decentralized and Transparent Property Asset Transfer Using NFTs. World 2025, 6, 166. https://doi.org/10.3390/world6040166

[3] Tariq, M.M.; Ihsan, U.; Alamsyah, Z. Land Registration and Inheritance Automation System Using Blockchain. Eng. Proc. 2025, 107, 97. https://doi.org/10.3390/engproc2025107097

[4] M. Zein, R.; Twinomurinzi, H. Information Sharing in Land Registration Using Hyperledger Fabric Blockchain. Blockchains 2024, 2, 107-133. https://doi.org/10.3390/blockchains2020006

[5] Yang, Y.; Li, H.; Cheng, L.; Ning, Y. Effect of Land Property Rights on Forest Resources in Southern China. Land 2021, 10, 392. https://doi.org/10.3390/land10040392

[6] Kusmiarto, K.; Aditya, T.; Djurdjani, D.; Subaryono, S. Digital Transformation of Land Services in Indonesia: A Readiness Assessment. Land 2021, 10, 120. https://doi.org/10.3390/land10020120

[7] Abab, S.A.; Wakjira, F.S.; Negash, T.T. Determinants of the Land Registration Information System Operational Success: Empirical Evidence from Ethiopia. Land 2021, 10, 1394. https://doi.org/10.3390/land10121394

[8] Blin, Pierre-François & Aditya, Trias & Claramunt, Christophe & Kermarrec, Y. & Santosa, Purnama. (2022). Cybersecurity risk-management to maintain integrity land data transactions: application to indonesian and french land administration systems. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. XLVIII-4/W3-2022. 29-31. 10.5194/isprs-archives-XLVIII-4-W3-2022-29-2022.

[9] Arfian, Aldi & Sari, Atika & Rachmawanto, Eko & Isinkaye, Folasade. (2024). Imperceptible and Robust Encryption: Salsa20 Stream Cipher for Colour Image Data. Sinkron. 9. 221-229. 10.33395/sinkron.v9i1.13049.

[10] Hameed, Musaab & Hoomod, Haider. (2023). New hybrid encryption algorithm for cloud computing security using chaotic system and mCrypton-salsa20 algorithms. AIP Conference Proceedings. 2591. 030046. 10.1063/5.0119644.

[11] Khalid, Rebwar & Aziz, Ribwar & Hassan, Alla & Aladdin, Aso & Sayda, Shaida & Rashid, Tarik & Hassan, Bryar. (2024). Comparative Analysis of AES, Blowfish, Twofish, Salsa20, and ChaCha20 for Image Encryption.

10.36227/techrxiv.172971943.34625654/v2.

[12] Li, Y.; Du, Z.; Fu, Y.; Liu, L. Role-Based Access Control Model for Inter-System Cross-Domain in Multi-Domain Environment. Appl. Sci. 2022, 12, 13036. https://doi.org/10.3390/app122413036