Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

A Centralized Cloud Security Storage System using Blockchain Technique

Mahijit M
Department of Information Science and Engineering,
Don Bosco Institute of Technology,
Bengaluru, India

Bhuvan M
Department of Information Science and Engineering,
Don Bosco Institute of Technology,
Bengaluru, India

Harshith M
Department of Information Science and Engineering,
Don Bosco Institute of Technology,
Bengaluru, India

Tejas N
Department of Information Science and Engineering,
Don Bosco Institute of Technology,
Bengaluru, India

Swathi B Patil
Assistant Professor,
Department of Information Science and Engineering,
Don Bosco Institute of Technology,
Bengaluru, India

Abstract **- Cloud storage systems are widely used for managing and accessing digital data, but they often face major security challenges such as unauthorized access, data leakage, and tampering of sensitive information. To overcome these issues, this project proposes a centralized cloud security storage system integrated with blockchain technology and facial recognition mechanisms for enhanced data protection and user authentication. The system begins with the collection of user details and facial image data during the secure registration process. User identity verification is performed using the K-Nearest Neighbours (KNN) face recognition algorithm, ensuring that only authenticated users can access the system. Before storing files in the cloud environment, sensitive information is encrypted to maintain confidentiality and prevent unauthorized disclosure.**

Keywords **- Blockchain, Zero Trust, Cloud Security, Face Recognition, Smart Contracts, AES Encryption, Biometric Authentication, Access Control, Cybersecurity, Secure Cloud Storage**

I. INTRODUCTION

Cloud computing has transformed the way organizations and individuals store, manage, and access data by providing scalable, flexible, and cost-effective storage solutions. With the increasing dependence on cloud platforms, the volume of sensitive digital information stored online has grown rapidly. However, traditional centralized cloud storage systems are highly vulnerable to security threats such as unauthorized access, data breaches, identity theft, and data tampering. These challenges highlight the need for advanced security mechanisms that can ensure confidentiality, integrity, and reliable user authentication in cloud environments. To enhance security in cloud storage systems, biometric authentication techniques have gained significant importance in recent years. Among these techniques, face recognition has emerged as an effective and user-friendly method for verifying user identity. In the proposed system, facial image data and user details are collected during the registration process, and the K-Nearest Neighbors (KNN) algorithm is used for face recognition and identity verification. This approach provides secure and accurate authentication, reducing the risks associated with password-based systems such as password theft, duplication, and unauthorized access.

In addition to biometric authentication, encryption techniques play a major role in protecting sensitive information stored in cloud systems. Before uploading data to the cloud environment, the proposed system encrypts all confidential information to prevent attackers from accessing original data even if the storage system is compromised. Furthermore, blockchain technology is integrated into the system to provide decentralized identity management and tamper proof logging of user activities. Blockchain maintains immutable records of user access requests, file transactions, and authentication events, thereby improving transparency, accountability, and trust within the cloud storage environment.

The proposed centralized cloud security storage system combines cloud computing, blockchain technology, encryption, and face recognition to provide a secure and efficient data management framework. Continuous monitoring and verification of user activities ensure that only authorized users can retrieve stored information based on predefined access control rules. After successful verification, encrypted data is securely decrypted and presented to legitimate users. This integrated approach not only enhances data security and privacy but also improves reliability and resistance against cyber-attacks, making the system suitable for applications in healthcare, banking, education, government organizations, and enterprise data management systems.

II. LITERATURE SURVEY

Efficient Key-Aggregate Cryptosystem With User Revocation for Selective Group Data Sharing in Cloud Storage The authors address secure group data sharing in cloud storage

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

where data is encrypted before being uploaded to the cloud. A major problem considered is **user revocation**, because users may leave a group after receiving access to encrypted data. The paper proposes a Key-Aggregate Cryptosystem with User Revocation (KAC-UR), allowing data owners to delegate decryption rights using a constant-size aggregate key.

GrAC: Graph-Based Anonymous Credentials From Identity Graphs on Blockchain GrAC proposes a blockchain-based identity-management system using an identity graph. The objective is to overcome the single point of failure and limited transparency associated with centralized identity registries. The system stores and manages identity information on blockchain without requiring an intermediate credential issuer.

Stateless Blockchain-Based Lightweight Identity Management Architecture for Industrial IoT Applications This work proposes a lightweight blockchain-based identity-management architecture for Industrial IoT. The researchers identify the storage growth and privacy problems associated with storing identity information on blockchain. To address these issues, the proposed system uses a stateless blockchain and cryptographic accumulator. The system supports identity registration, modification, revocation, and verification while reducing blockchain storage requirements.

Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication The paper focuses on the problem of identity security in Zero Trust environments. Traditional authentication mechanisms can create centralized points of failure, while public blockchain environments may expose personal information. The authors therefore propose a privacy-preserving Multi-Factor Authentication framework based on blockchain. The system uses a **Distributed Authentication Mechanism (DAM)**, blockchain-based Zero-Knowledge Proofs for OTP verification, and non-transferable authentication tokens. The objective is to provide continuous and reliable identity verification without exposing sensitive authentication information.

HA-CAAP: Hardware-Assisted Continuous Authentication and Attestation Protocol for IoT Based on Blockchain HA-CAAP addresses continuous authentication in dynamic, multi-authority IoT environments. The authors identify problems such as device spoofing, cloning, and Sybil attacks when devices frequently change their network connections. The proposed protocol combines hardware-assisted authentication with blockchain. PUF-based authentication is used for IoT devices, while a private blockchain enables gateways to exchange connectivity information and maintain a dynamic device inventory. A TEE-based continuous gateway-attestation mechanism is also included to verify gateway integrity.

Secure and Fair Data Trading Based on Blockchain With Enhanced Access Control The paper proposes a blockchain-based Fair Data Trading scheme called **FairDT**. It addresses the dependence on trusted third parties in data exchange and adds fine-grained access control to blockchain-based transactions. Smart contracts are used to provide decentralized and automated data trading. The scheme combines commitment mechanisms, Merkle trees, encryption, smart contracts, and multi-authority attribute-based encryption. Experiments on an Ethereum test net demonstrate that the on-chain overhead remains constant with changes in data size.

Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments The paper proposes a Unified Quantum-Resilient Blockchain-Zero-Knowledge Proof Privacy Authentication Framework (QBC-ZKPAF). It combines blockchain with Zero Trust Architecture, Zero-Knowledge Proofs, and post-quantum cryptography for privacy-preserving authentication and access control.

Blockchain maintains immutable identity and access-management records, while ZKP enables authentication without revealing sensitive information. The framework also incorporates multi-factor authentication and dynamic key selection.

DedupChain: A Secure Blockchain-Enabled Storage System With Deduplication for Zero-Trust Network DedupChain addresses the storage and privacy problems caused by the full-backup nature of permissioned blockchain when blockchain is used as a Zero Trust storage foundation. The authors propose secure data deduplication to remove duplicate data while preserving confidentiality. The system combines an SGX trusted execution environment with ORAM to implement **oblivious data deduplication**, protecting against offline brute-force and frequency-analysis attacks. The authors implemented a prototype and reported upload throughput exceeding **400 TPS**.

Blockchain-Based Solutions for Enhancing Data Security in Cloud Computing Environments This paper examines the use of blockchain to improve cloud data security. It focuses on important security requirements including data protection, access control, privacy, decentralized identification, and smart-contract-based automation. The study identifies blockchain's immutability and decentralization as mechanisms for reducing single points of failure and improving trust. It also highlights practical challenges including **scalability, delay, and interoperability** when blockchain is integrated with cloud computing.

Securing Biometric Authentication System Using Blockchain Technology This paper investigates the combination of biometric authentication, deep learning, and blockchain. It proposes a fingerprint authentication system in which a CNN extracts discriminative biometric features. The extracted information is hashed using SHA-256 and the resulting information is managed through blockchain and smart contracts. The approach aims to overcome weaknesses in conventional biometric systems, including spoofing, forgery, centralized storage, and privacy risks. Blockchain provides immutable and traceable storage while the original biometric

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

material is protected.

Blockchain-Enhanced Data Integrity and Authentication in WSN-IoT Systems A blockchain-based approach for improving data integrity and authentication in WSN-IoT systems. The study analyzes blockchain's impact on security, latency, scalability, and resource usage. The approach improves data verification and reduces security risks, but blockchain overhead and resource limitations of IoT devices remain challenges. The work is relevant to the proposed system because it demonstrates the use of blockchain for secure authentication and tamper-resistant data management.

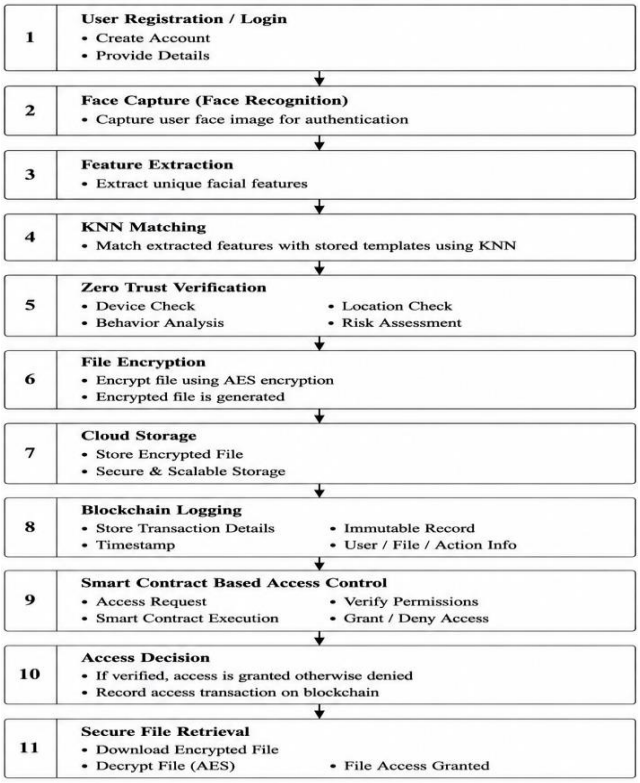
Blockchain-Enabled Trust Models in Next-Generation Information Networks This paper proposes a blockchain-enabled trust framework for next-generation information networks covering 5G/6G, edge-cloud environments, IoT, cyber-physical systems, and data spaces. It introduces a **Trust-by-Design** stack incorporating identity, provenance, attestation, privacy, and cross-domain compliance. The methodology uses design-science principles, threat modelling, mathematical models for consensus and permissioned operation, Zero-Knowledge-based verifiable computing, and smart-contract policy automation. The paper evaluates Fabric, Quorum, and Tender mint networks with different node configurations and WAN conditions.

III. PROPOSED SYSTEM

The proposed system presents a blockchain-enabled secure cloud storage framework integrated with Zero Trust Architecture for improving data confidentiality and access control. The system verifies users continuously using biometric authentication and stores encrypted data in the cloud environment. Blockchain technology is used to maintain immutable transaction records and prevent unauthorized modifications. The framework improves transparency, reliability, and overall cloud security compared to traditional centralized systems.

The proposed model also incorporates face recognition-based authentication using machine learning algorithms such as KNN to provide secure user verification. User facial data is captured during registration and later used for identity validation during login and access requests. AES encryption is applied before storing data in the cloud to ensure confidentiality and data integrity. The integration of biometric authentication with encryption techniques strengthens system security and reduces dependency on passwords.

In addition, smart contracts are implemented for automated access control and permission management. The system continuously monitors user activities under the Zero Trust approach and grants access only to authorized users. Blockchain-based logging ensures tamper-proof storage of access records and improves accountability within the system. The proposed framework eliminates single points of failure, enhances trust, and provides a scalable and decentralized solution for secure cloud data management.



A. Equations

KNN (Face Recognition)

$$d=\sqrt{\sum_{i=1} ^{n}(x_i - y_i)^2}$$

Where:

- (d) = Euclidean distance
- (x_i, y_i) = feature vectors

AES Encryption

$$C=E (K, P)$$

Where:

- (C) = Ciphertext
- (K) = Secret Key
- (P) = Plaintext

AES Decryption

$$P = D (K, C)$$

Where:

- (D) = Decryption function

Blockchain Hashing

$$H = Hash (Data + Previous Hash)$$

Where:

- (H) = Hash value
- (Data) = Transaction data

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

B. Algorithm

Algorithm 1: Algorithm for Secure Access System

```
SECURE_ACCESS_SYSTEM(U)
U ← RECEIVE (User Request)
F ← CAPTURE_FACE(U)
VF ← VERIFY_FACE (F, KNN)
if VF = Authorized User then
   A ← ZERO_TRUST_AUTH(U)
   E ← ENCRYPT (Data, AES)
   B ← STORE_BLOCKCHAIN_LOG(U)
   S ← STORE_CLOUD(E)
   DISPLAY (Access Granted)
else
   DISPLAY (Access Denied)
end if
return S
```

Algorithm 2: Algorithm for Blockchain-Based Authentication

```
BLOCKCHAIN_AUTHENTICATION(U)
U ← RECEIVE (User Details)
F ← CAPTURE_FACE(U)
K ← EXTRACT_FEATURES(F)
M ← MATCH_FACE (KNN_Dataset)
if M = Valid User then
   T ← VERIFY_ZERO_TRUST(U)
   H ← GENERATE_HASH (U_Data)
   B ← STORE_IN_BLOCKCHAIN(H)
   DISPLAY (Authentication Successful)
else
   DISPLAY (Authentication Failed)
end if
return B
```

REFERENCES

[1] J. Liu, J. Qin, X. Zhang, and H. Wang, "Efficient Key-Aggregate Cryptosystem With User Revocation for Selective Group Data Sharing in Cloud Storage," *IEEE Transactions on Knowledge and Data Engineering*, 2024, doi: **10.1109/TKDE.2024.3397721**.

[2] W. Tang, S. S. Mukherjee, S. Park, C. Chenli, H. Oh, J. Kim, and T. Jung, "GrAC: Graph-Based Anonymous Credentials From Identity Graphs on Blockchain," in *Proc. 2024 IEEE International Conference on Blockchain*, 2024, doi: **10.1109/Blockchain62396.2024.00024**.

[3] K. Zhang, C. K. M. Lee, and Y. P. Tsang, "Stateless Blockchain-Based Lightweight Identity Management Architecture for Industrial IoT Applications," *IEEE Transactions on Industrial Informatics*, 2024, doi: **10.1109/TII.2024.3367364**.

[4] J. J. Diaz Rivera, A. Muhammad, and W.-C. Song, "Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication," *IEEE Open Journal of the Communications Society*, 2024, doi: **10.1109/OJCOMS.2024.3391728**.

[5] V. Malamas, P. Kotzanikolaou, K. Nomikos, C. Zonios, V. Tenentes, and M. Psarakis, "HA-CAAP: Hardware-Assisted Continuous Authentication and Attestation Protocol for IoT Based on Blockchain," *IEEE Internet of Things Journal*, 2025, doi: **10.1109/JIOT.2025.3530775**.

[6] Z. Feng, Q. Wu, Y. Liu, B. Qin, M. Zhai, and W. Susilo, "Secure and Fair Data Trading Based on Blockchain With Enhanced Access Control," *IEEE Internet of Things Journal*, 2025, doi: **10.1109/JIOT.2024.3497953**.

[7] M. A. Aleisa, "Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments," *IEEE Access*, 2025, doi: **10.1109/ACCESS.2025.3529309**.

[8] S. Qi, Q. Wang, W. Wei, X. Yang, H. Zhao, Y. Liu, X. Yang, and Y. Qi, "DedupChain: A Secure Blockchain-Enabled Storage System With Deduplication for Zero-Trust Network," *IEEE Journal on Selected Areas in Communications*, 2025, doi: **10.1109/JSAC.2025.3560043**.

[9] P. Khobragade, M. Dhone, P. K. Dhankar, S. A. Thakur, P. K. Adakane, and P. Saraf, "Blockchain-Based Solutions for Enhancing Data Security in Cloud Computing Environments," in *Proc. 2025 1st International Conference on Data Science and Intelligent Network Computing (ICDSINC)*, 2025, doi: **10.1109/ICDSINC66221.2025.11448121**.

[10] V. Kumari and N. Poonguzhali, "Securing Biometric Authentication System Using Blockchain Technology," in *Proc. 2025 4th International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN)*, 2025, doi: **10.1109/ICSTSN67075.2025.11397935**.

[11] G. Tuteja, S. Rani, and A. Sharma, "Blockchain-Enhanced Data Integrity and Authentication in WSN-IoT Systems," in *Proc. 2024 Global Conference on Communications and Information Technologies (GCCIT)*, 2024, doi: **10.1109/GCCIT63234.2024.10862083**.

[12] W. Y. Leong, "Blockchain-Enabled Trust Models in Next-Generation Information Networks," in *Proc. 2025 Asian Conference on Communication and Networks (ASIANComNet)*, 2025, doi: **10.1109/ASIANComNet68615.2025.11579721**.