International Journal of Science, Strategic Management and Technology
Volume **02** Issue **04** April-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Secure Data Storage using Block Chain

Saran S
Department of Computer Science and Information Technology
VELS Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, India
Clifford J
Department of Computer Science and Information Technology VELS Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, India
Supervisor : **Dr.SK. Piramu Preethika**
MCA,B.Ed.,M.Phil,Ph (Assistant Professor) Dept of CS & IT, VISTAS, Chenna

https://doi.org/10.55041/ijsmt.v2i4.655

Cite this Article: S, S. & J, C. (2026). Secure Data Storage using Block Chain. International Journal of Science, Strategic Management and Technology, *02*(04). https://doi.org/10.55041/ijsmt.v2i4.655

Abstract— Centralized data storage systems face significant challenges regarding unauthorized tampering and a lack of verifiable audit trails. This paper presents BlockSecure, a web-based secure storage system that integrates AES-256 encryption with a custom C#-based blockchain engine. Built on ASP.NET Core MVC and MongoDB, the framework ensures data confidentiality through unique per-file encryption keys and provides immutability via a Proof-of-Work (PoW) consensus mechanism. SHA-256 hashes of encrypted files are anchored into a permanent ledger, enabling real-time detection of data tampering. Experimental results confirm that the proposed system delivers superior security and accountability compared to conventional cloud-based storage solutions.

Keywords— Blockchain, AES-256, Data Integrity, Proof-of-Work, ASP.NET Core, MongoDB, Cybersecurity.

I. INTRODUCTION

In the current digital era, the secure management of sensitive information has become a critical challenge for both individuals and organizations [cite: 635]. Traditional cloud to each password, protecting against dictionary and rainbow table attacks [cite: 792].

B. Encryption and Storage Engine

Files are processed through an AES-256 CBC encryption pipeline [cite: 690]. Each file receives a unique ***K*** (encryption key) and ***IV*** (initialization vector) [cite: 641, 848]. Binary data is stored using MongoDB GridFS, which splits files into 255KB chunks for optimized handling of large assets [cite: 687, 759].

TABLE I: MINIMAL HARDWARE SPECIFICATIONS

Component	**Requirement**
Processor	Intel Core i3 (64-bit)
RAM	4 GB (Min)
Storage	10 GB Free Space
OS	Windows 11

C. Blockchain Implementation

The heart of the system is a custom-built blockchain engine implemented in C# [cite: 642, 841]. It follows astorage platforms like Google Drive and Dropbox rely on centralized architectures that often lack robust, independent sequential chain where each block is of linked to the ***H***

integrity verification mechanisms [cite: 636]. This makes them vulnerable to unauthorized access and silent data modification [cite: 637, 656].

BlockSecure is proposed as a solution to bridge these security gaps by combining blockchain technology with military-grade encryption [cite: 638, 678]. Unlike existing systems that may use a common key for multiple files, our architecture generates unique encryption parameters for every upload, ensuring maximum isolation of sensitive data [cite: 641, 848].

II. SYSTEM DESIGN AND MODULES

The BlockSecure framework is composed of six primary functional modules designed to operate in a unified web environment [cite: 640, 688].

A. User Authentication

Security begins at the entry point. The system utilizes BCrypt password hashing to store credentials securely in MongoDB [cite: 688, 791]. This approach adds a unique salt

the preceding block [cite: 660]. The SHA-256 hash of the encrypted file is permanently recorded in this ledger [cite: 642].

III. METHODOLOGY

The system employs a Proof-of-Work (PoW) mining algorithm to ensure the chain's immutability [cite: 642, 1080].

A. Mining Process

For each block, a nonce value is incremented until a hash satisfying the difficulty requirement (two leading zeros) is found [cite: 1081]. This computational commitment prevents easy alteration of the historical records, as any change would require re-mining all subsequent blocks [cite: 660, 683].

B. Access Control Workflow

A "Request-Approve-Deny" logic is implemented to give file owners full authority [cite: 692, 854]. Users requesting a file must wait for the owner's explicit approval [cite: 669]. Unauthorized access attempts are not only blocked but also

logged in the blockchain and reported via real-time Gmail SMTP alerts [cite: 645, 1112].

IV. RESULTS AND ANALYSIS

Functional testing was conducted across all modules, including authentication, encryption, and blockchain verification [cite: 1116]. The system successfully maintained a tamper-proof audit trail for diverse file formats, including PDF, DOCX, and ZIP archives [cite: 689, 709].

Performance metrics showed that the use of MongoDB GridFS allowed the system to handle files up to 100MB efficiently without degrading user experience [cite: 689, 936]. The dark-themed responsive interface ensured accessibility across mobile and desktop devices [cite: 647, 671].

V. CONCLUSION

BlockSecure represents a successful integration of blockchain principles into a practical data storage application [cite: 648, 1184]. By combining per-file AES-256 encryption with a decentralized integrity ledger, the system provides a robust defense against the data tampering risks inherent in conventional storage models [cite: 673, 873].

REFERENCES

[1] Microsoft Corp, "ASP.NET Core MVC Documentation," Microsoft Developer Network, 2024. [cite: 1187]

[2] Microsoft Corp, ".NET 8 SDK Documentation," Microsoft Developer Network, 2024. [cite: 1187]

[3] Microsoft Corp, "AES-256 Encryption — System.Security.Cryptography," MSDN, 2024. [cite: 1187]

[4] MongoDB Inc, "MongoDB Manual — Official Documentation," 2024. [cite: 1188]

[5] MongoDB Inc, "GridFS — Storing Large Files," Official Documentation, 2024. [cite: 1188]

[6] BCrypt.Net, "Password Hashing Library Version 4.1.0," NuGet Gallery, 2024. [cite: 1188]

[7] Tagore College of Arts and Science, "BlockSecure Project Thesis," Dept. of Computer Science, 2026. [cite: 701]