International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 04 | April – 2025 DOI: 10.55041/ISJEM02958
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

SERVER-CLIENT SECURED STORAGE WITH IP AUTHENTICATION AND TRACKING

Lalitha Kameswari N V[1], NithyaShree G[2], Vimal S[3] , Mrs. Durga Devi[4] , Mrs. K Saranya[5] 1,2,3.B.sc ISCF students, Dr.M.G.R Educational and Research Institute Deemed to be University, Chennai.
Corresponding Email ID: viswaboy0904@gmail.com
4. Assistant Professor, Dr.M.G.R Educational and Research Institute, Deemed to be University , Chennai.
5. Assistant Professor, Dr.M.G.R Educational and Research Institute, Deemed to be University, Chennai.

ABSTRACT

In the digital era, where data privacy and security have become a top priority, traditional storage systems often fail to provide robust protection against unauthorized access and cyber threats. This journal presents a secured server-client storage system equipped with IP authentication and tracking features to ensure data confidentiality, integrity, and accountability. The system validates each user's identity through secure credentials and cross- verifies their IP address, enabling reliable user verification and access logging. Designed with encryption mechanisms, role-based access controls, and an intuitive web interface, the system ensures that only authorized clients can interact with the stored data. IP tracking provides a layer of transparency, enabling effective monitoring and auditing of system usage. The proposed solution is scalable and suitable for both enterprise and individual-level data security needs.

1. INTRODUCTION

Protecting digital data from unwanted access has grown more difficult as it continues to expand at an exponential rate. Despite the fact that many systems have authentication methods, they frequently lack useful client tracking tools. Unauthorized access, data leaks, and spoofing cyberattacks have highlighted how crucial it is to track users' network origins in addition to user verification.

Accountability and threat detection can be significantly enhanced by combining IP-based tracking with conventional authentication. In order to improve overall data security, this journal investigates the architecture and deployment of a server-client secured storage system that integrates IP authentication and tracking.

© 2025, ISJEM (All Rights Reserved)

2. REQUIREMENT ANALYSIS

2.1 OBJECTIVE OF THE PROJECT

- **Establish a Secure Storage Environment:** Provide a safe platform that allows for the safe storage and retrieval of data between client and server systems while upholding strict access control.

- **Put IP-Based Authentication into Practice:** By incorporating IP-based authentication, you can strengthen user verification and make sure that only known and trusted devices have access to sensitive data.

- **Track and Record User Activities:** To improve accountability, keep a thorough record of user activities, including access times, file operations, and originating IP addresses.

- **Access Controls:** Turn on role-based access control to reduce the possibility of unwanted data manipulation by allocating access rights according to user roles (admin, user, guest, etc.).

- **Secure Data Transmission:** To guard against interception and tampering, use encryption and SSL protocols while data is in transit.

- **Improve System Monitoring:** Give administrators access to a centralized dashboard so they can keep an eye on system performance.

2.2 EXISTING SYSTEM

The majority of data storage systems in use today are based on conventional client-server architectures that use simple authentication methods like username and password. Even though these techniques offer a basic degree of access control, they are frequently insufficient in the dangerous digital environments of today. Granular tracking features are lacking in the majority of current systems, particularly with regard to identifying and recording the IP addresses that users use to access the system. Vulnerability detection and accountability are seriously compromised by this omission.

Furthermore, a lot of current platforms lack strong encryption features and role-based access controls, which could allow unauthorized users to access private information. Logging mechanisms are either non-existent or restricted to access timestamps, failing to record the full context of the interaction, including device fingerprint, IP address, and geographic location.

The lack of alert systems or real-time monitoring features, which are crucial for identifying and reacting to suspicious activity as it occurs, is another limitation. IT staff may find it challenging to properly audit usage or enforce data governance policies in these systems due to their potentially confusing administrative interfaces.

In conclusion, complete data protection, traceability, and adaptability are not adequately provided by the current systems.

Disadvantages

- No client verification or IP tracking.
- Insufficient or non - existent user activity audit trails.
- Susceptible to phishing and brute force attacks.
- Inadequate role-based access management.
- No monitoring system or real-time alert.

2.3 PROPOSED SYSTEM

By including a number of cutting-edge features like IP-based user authentication, real-time activity logging, encryption, and improved user tracking, the suggested system is intended to overcome the drawbacks of current storage options. With an emphasis on security, scalability, and user accountability, this architecture aims to offer a more reliable solution for managing data storage.

- **IP Verification and User Authentication:**

The suggested system does not rely only on username and password combinations for user authentication. Rather, IP address verification is included with every login attempt to make sure users are logging in from authorized and registered locations. The system adds an extra degree of security to guard against unwanted access by comparing the client's IP address to a predetermined list of trusted IPs or IP ranges supplying an extra degree of confirmation to guard against unwanted access. The system either blocks access or requests more verification (such as multi-factor authentication) if the IP address doesn't match the expected pattern or geographic location.

- **Role-Based Access Control (RBAC):**

The suggested system incorporates Role-Based Access Control (RBAC) to guarantee that users can only access the data they are permitted to interact with. The system specifies a number of roles, each with distinct permissions, including Admin, User, and Guest. While users can upload, download, and edit files within the parameters of their permissions, administrators can control user access and settings. Depending on the security needs of the organization, guests might only have read-only access or limited functionality. This reduces the possibility of unauthorized users making malicious or unintentional changes.

Advantages

- Security and traceability are enhanced by IP-based user authentication.
- Complete the audit trails for every instance of data access.
- Secure data transfer and encrypted data storage.
- The management of user permissions is improved by role-based access control.
- Alerts for questionable activity and real-time monitoring.
- Scalable and intuitive administration web interface.

3. REQUIREMENT SPECIFICATIONS

3.1 HARDWARE REQUIREMENTS

- Processor : Intel core I3 3.80 GHz 64 bit.
- RAM : 2GB
- Hard disk : 160 GB
- Compact Disk : 650 Mb
- Keyboard : Standard keyboard

3.2 SOFTWARE REQUIREMENTS

- Operating system : Windows 10
- Platform : Anaconda3
- Development Framework: Flask
- Frontend : python
- Backend :Mysql

4. MODULES

1. User Authentication
2. IP Verification
3. File Management
4. Encryption
5. Admin Dashboard
6. Logging and Monitoring

1. User Authentication

Only authorized users can access the system thanks to the User Authentication Module. This module manages the safe login procedure by confirming users using both IP address validation and credentials (password and username).

- **Login Process:** To authenticate themselves, users input their login information (password and username).
- **Multi-Factor Authentication (MFA):** People may be asked to use another authentication method (such as one-time passwords sent by email or SMS) if IP verification is unsuccessful or if there are higher security requirements.
- **Password Hashing**: To ensure that user passwords are not kept in plaintext, they are hashed using algorithms like SHA-256 or Bcrypt.

2. **IP Verification**

By verifying that the user's request originates from a trusted network or a registered IP address, the IP Verification Module provides an additional degree of protection.

- **IP Address Verification:** A whitelist or collection of approved IP addresses kept in the database is compared to the user's IP address.
- **Geolocation**: To increase security, the system makes use of geolocation services to confirm that the IP address corresponds to the user's anticipated location.
- **IP blocking:** When an unauthorized IP address is identified, access is blocked, and the system records the unsuccessful attempt for administrators to review.

3. **File Management**

Users can interact with the system's storage through the File Management Module. Users can safely upload, download, and manage their files.

Uploading and downloading files to and from the server is safe for users. Every file operation is recorded along with the IP address, timestamp, and user ID.

File metadata management allows users to see and control information about a file, including its name, type, size, and modification date.

4. Encryption

Data confidentiality is guaranteed by the encryption module while it is being transmitted and while it is being stored on the server.

- **AES Encryption:** Before files are saved on the server, the system encrypts them using the Advanced Encryption Standard (AES) and a strong key length (such as AES-256).
- **Secure Data Transmission:** To guard against data manipulation and eavesdropping, SSL/TLS protocols encrypt data being sent between the client and server.

5. Admin Dashboard

An interface for managing system users, keeping an eye on activity, and guaranteeing system security is offered to administrators by the Admin Dashboard Module.

- **User management:** Administrators have the ability to assign roles (Admin, User, Guest, etc.) and add, edit, or remove users.
- **System Monitoring:** Offers real-time tracking of active sessions, storage utilization, and system health.
- **Activity Log Review:** Administrators have access to comprehensive logs of every action taken by users.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 04 | April – 2025 DOI: 10.55041/ISJEM02958
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

6. **Monitoring and Logging**

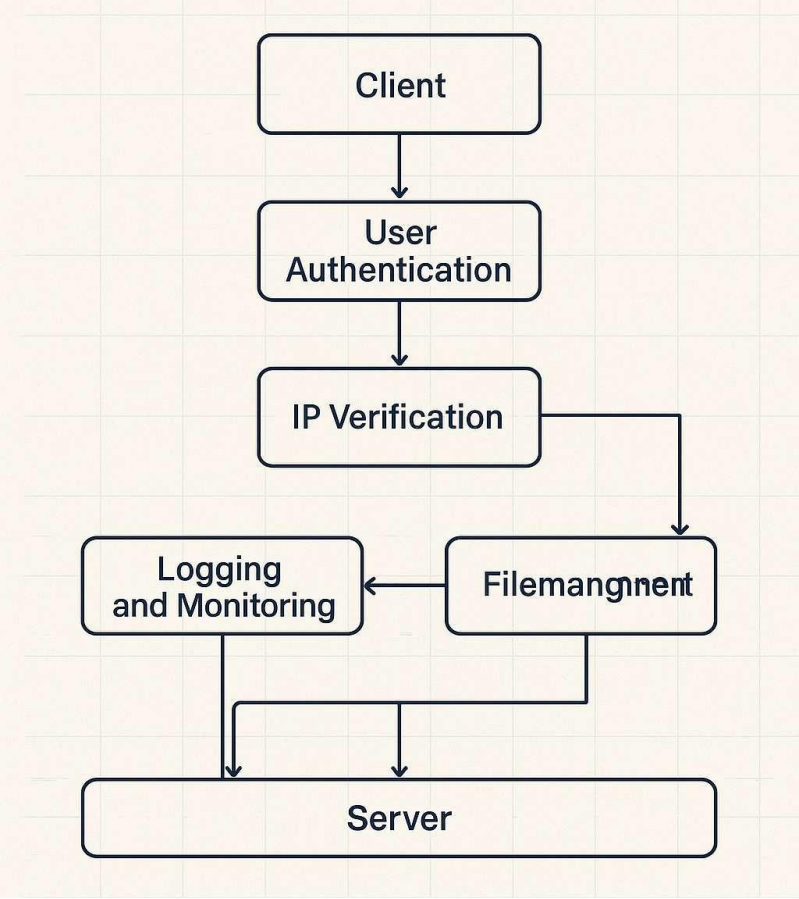
All system activity is tracked and recorded by the Logging and Monitoring Module. This module is essential for auditing as well as for quickly identifying and addressing possible security breaches.

- **Comprehensive Activity Logs:** All system interactions, including file operations, IP verifications, and login attempts, are recorded with pertinent information.

5. ARCHITECTURE DIAGRAM

It can provide client devices connecting to a central server via a secure protocol. Each request is passed through an authentication layer, followed by IP verification. File storage and database management are handled at the backend.

Fig no.1 ARHITECTURAL DIAGRAM



6. IMPLEMENTATION

There are several crucial steps involved in putting the server-client secured storage system with IP authentication and tracking into practice. The user first creates an account, and hash functions like Bcrypt are used to safely store credentials. When the user logs in, the system logs the client's IP address and compares it to trusted or predefined IP entries in the database.

Access is allowed if the IP verification is successful; if not, the user is either refused entry or asked to verify again.
Once inside the system, the user interface allows file uploads, downloads, deletions, and management through a browser-based dashboard. Each action is logged with metadata including user ID, timestamp, file ID, and originating IP address.

Encryption using AES-256 ensures that data stored on the server is protected at rest, while SSL encryption secures data in transit. The backend is developed using Python and Flask for REST API handling, PostgreSQL for relational data storage, and Nginx as a secure reverse proxy.

Administrative functionalities include a real-time activity monitoring dashboard, user role assignments, and automatic alert systems for suspicious login attempts or access from unrecognized IP addresses. Log files and audit reports can be generated on demand for compliance and forensic analysis. This implementation ensures a robust, scalable, and secure solution for data storage with transparency and traceability as core features.

7. CONCLUSION

The creation and deployment of a server-client secured storage system with IP authentication and tracking features raises the bar for digital data security considerably. This solution offers a multi-layered defense model that cross-verifies user identity using both login credentials and the originating IP address, in contrast to traditional systems that only use basic credentials. This guarantees that IP-level controls can still prevent unwanted access even in the event that login credentials are compromised. Additionally, data confidentiality is guaranteed while in transit and at rest thanks to the combination of SSL and AES encryption protocols. Role-based access control, thorough user activity logging, and real-time monitoring all help create an environment that is transparent and auditable.

8. REFERENCES

[1] W. Stallings, *Cryptography and Network Security*, 7th ed., Pearson Education, 2017.

[2] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed., Prentice Hall, 2011.

[3] R. Housley, S. Polk, W. Ford, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," *RFC 5280*, May 2008.

[4] OWASP Foundation, *Security Guidelines for Web Applications*, 2023. [Online]. Available: https://owasp.org

[5] National Institute of Standards and Technology (NIST), *Cybersecurity Framework*, 2020. [Online]. Available: https://www.nist.gov/cyberframework

[6] International Organization for Standardization, *ISO/IEC 27001:2013 – Information Security Management*, 2013.

[7] Microsoft Azure Docs, *Implementing IP-based Security*, Microsoft, 2024. [Online]. Available: https://docs.microsoft.com

[8] Python Software Foundation, *Python Cryptography Toolkit*, [Online]. Available: https://pypi.org/project/cryptography/

[9] S. K. Bansal and S. D. Singh, "A review on cryptographic algorithms for data security in cloud computing," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 6, pp. 48-56, Jun. 2015.

[10] M. Kumar, A. Mehta, and R. K. Gupta, "A novel approach for securing cloud storage using blockchain and encryption," International Journal of Computer Applications, vol. 162, no. 6, pp. 33-39, Mar. 2017.

[11] A. Gupta and H. Arora, "Securing cloud storage using hybrid encryption technique," International Journal of Computer Science and Technology, vol. 6, no. 2, pp. 47-50, Jun. 2015.