



# Multi Layer Security Model for Document Exchange and Communication

<sup>1</sup>Manish Kumar Sharma, <sup>2</sup>Irfan Khan

<sup>1</sup>M.Tech Scholar, <sup>2</sup>Assistant Professor

<sup>1</sup>Department Of Computer Science And Engineering,

<sup>1</sup>Shekhawati Institute Of Engineering & Technology, Sikar

**Abstract :** In today's era of digital data exchange, ensuring the security and privacy of shared documents is crucial. This research introduces an all-encompassing strategy to bolster document security by integrating biometric authentication and Aadhar-based encryption. The system proposed ensures that only authorized users can access and decrypt documents, employing a multi-layered security model. The user validation process includes utilizing biometric data, specifically fingerprint photos. During login, Blake2B hashes of these fingerprints are generated and validated. Additionally, unique transformations are applied to user Aadhar numbers, enhancing security without compromising user privacy. This multi-factor approach enhances the robustness of the authentication process. While encryption stands as the foundation of document security, the study recommends transitioning from the outdated DES (Data Encryption Standard) algorithm to more contemporary and robust encryption methods like AES (Advanced Encryption Standard) for safeguarding document content. The encryption key used is derived from Aadhar extracts of communicating users, boosting security without sacrificing user-friendly access. The research also underscores the importance of key management, secure communication protocols, and considerations for user privacy. It places significant emphasis on complying with data protection regulations and advocates for rigorous testing and regular updates to address emerging security challenges. The proposed approach aims to strike a balance between security and usability, enhancing the document sharing experience while ensuring that data remains confidential and accessible only to those with proper authorization. As technology advances and data breaches become more prevalent, this research offers a timely and comprehensive solution for secure document sharing in the digital age.

**Index Terms – Blake2B, Document Sharing , Hash Functions.**

## I. INTRODUCTION

User authentication is a critical process that verifies the identity of individuals seeking access to a system, application, or network. It utilizes credentials like usernames and passwords to establish identity and determine authorization. This process is fundamental for protecting sensitive information and preventing unauthorized access, reducing the risk of data breaches and potential harm to the system or users [1].

The significance of user authentication can be summarized in several key aspects:

- **Security:** Authentication plays a vital role in securing systems, applications, and networks by verifying user identities and preventing unauthorized access to sensitive information.
- **Data Protection:** User authentication safeguards sensitive data from unauthorized disclosure, modification, or deletion, ensuring that only authorized users can access and manipulate data [1].
- **User Privacy:** Authentication mechanisms protect user privacy by allowing only intended users to access their personal information, preventing unauthorized access and fraudulent activities.
- **Regulatory Compliance:** Many industries and jurisdictions mandate user authentication to meet specific regulations, ensuring legal compliance and avoiding potential consequences [2].
- **Accountability and Auditing:** User authentication enables accountability by associating user activities with specific identities, facilitating auditing and tracking of suspicious or unauthorized activities.
- **Prevention of Unauthorized Access:** Authentication serves as the first line of defense against unauthorized access attempts, reducing the risk of brute-force attacks and unauthorized entry [3].
- **Trust and User Confidence:** Robust authentication measures build trust and confidence in users, assuring them that their accounts and information are secure.

In summary, user authentication is essential for maintaining the security, integrity, and privacy of systems, applications, and networks.

### Authentication Techniques:

Authentication techniques are methods used to verify the identity of individuals accessing systems, applications, or networks. Key techniques include [3]:

- **Password-based Authentication:** Users provide a unique password, with the system verifying it against a stored password hash. Complexity requirements and anti-brute-force measures strengthen this method.
- **Multi-factor Authentication (MFA):** Combining two or more authentication factors, such as knowledge (password), possession (token or device), and inherence (biometric data), for enhanced security.
- **Biometric Authentication:** Verifying identity through unique physical or behavioral characteristics like fingerprints, facial features, iris patterns, or voice recognition [4].
- **Token-based Authentication:** Using physical or virtual tokens to generate one-time passwords or cryptographic codes, adding an extra layer of security.
- **Certificate-based Authentication:** Relying on digital certificates issued by trusted authorities to verify identity during authentication.
- **Social Authentication:** Leveraging identity verification from social media platforms to authenticate users without separate credentials [4].
- **Risk-based Authentication:** Assessing authentication risk based on factors like user behavior and location, dynamically adjusting measures accordingly.

These techniques can be combined or used individually based on specific security requirements, considering factors like data sensitivity, user convenience, and the overall threat landscape.

## II. PROBLEM STATEMENT

The current document sharing methods within the banking sector are susceptible to security breaches, exposing vulnerabilities to fraud, unauthorized access, and data manipulation. Malicious actors often target centralized systems, jeopardizing the confidentiality, integrity, and authenticity of shared documents. Additionally, traditional authentication methods may not offer adequate assurance of user identity. Consequently, there is a pressing need to develop a secure document sharing system for the banking sector that leverages blockchain technology and integrates multi-level security checks for both user authentication and document integrity. This proposed system aims to ensure the immutability, transparency, and decentralized consensus inherent in blockchain, while incorporating robust authentication measures like Aadhar verification, fingerprint authentication, and image rotation patterns. The objective is to establish a system that not only enhances document sharing security but also addresses the risks associated with conventional methods, fostering trust among stakeholders in the banking ecosystem.

## III. LITERATURE SURVEY

Cui, Z. et al. (2020): This study suggests a hierarchical blockchain-based authentication system for the Internet of Things (IoT) using a hybrid blockchain model. By incorporating both local and public chains, the proposed scheme ensures robust security and improved performance across various scenarios.

Madhu, A. et al. (2020): The authors have developed the Crop Monitor, a mobile app fostering direct interaction between farmers, logistics organizations, and customers through the Smart Agritech app. This promotes transparency, enables e-commerce without intermediaries, and offers real-time tracking, supply chain traceability, and recognition for farmers.

Giraldo, F. D. et al. (2020): The paper argues that blockchain can enhance trust in digital transactions, exploring its potential for commercial, industrial, and service systems. Emphasizing the use of Ethereum smart contracts and public/private key cryptography, the study presents a proof of concept for a blockchain-based voting system tailored for elections to improve stakeholder trust.

Teja, J. R. (2020): The author highlights the resource-intensive nature of maintaining accurate documents through intermediaries and suggests blockchain as a solution. This involves creating immutable ledger entries for document alterations, ensuring traceability through the use of Merkle tree algorithms for effective data storage.

Shree, J. et al. (2020): The paper introduces a smart and secure purchasing system integrating ERP, featuring a self-billing application for customers to eliminate waiting times. Using blockchain for product traceability throughout the supply chain, an RFID item tracker is included to detect unauthorized removal of goods and mitigate theft risks.

## IV. PROPOSED WORK

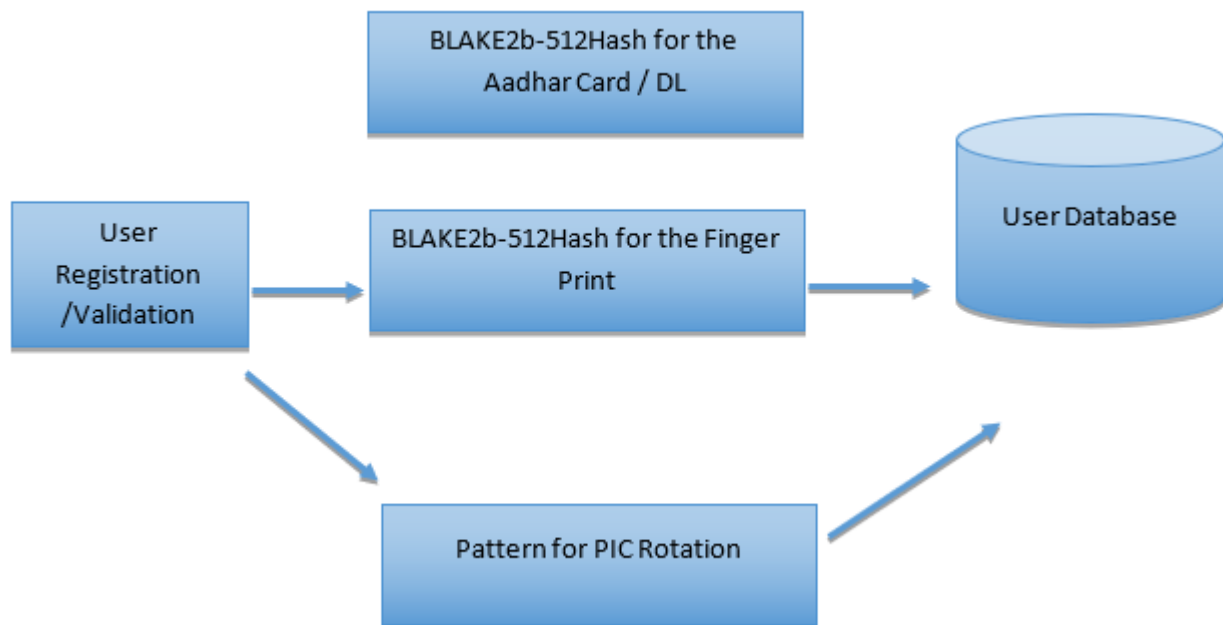


Fig 1. User Authentication

In the context of voter identity validation, the process involves collecting and verifying three distinct inputs from the user. Each input contributes to a multi-factor authentication approach, enhancing the overall security and reliability of the validation process. Let's delve into the details of each required input:

❖ **Digital Identity (Aadhar Card / Driving License):**

- **Definition:** Digital identity refers to a unique representation of an individual in electronic form. In this case, users are required to present a digital version of their government-issued identity documents, such as Aadhar Card or Driving License.
- **Explanation:** The digital identity serves as a primary document to establish the legal identity of the voter. It contains essential details like name, photograph, and a unique identification number. By requiring users to present a digital copy of these documents, the system aims to verify the authenticity of the voter's identity against recognized government records.

❖ **Fingerprint:**

- **Definition:** A fingerprint is a biometric identifier unique to each individual, formed by the ridges and valleys on the surface of the fingertip.
- **Explanation:** Fingerprint authentication is a biometric method used to confirm the identity of an individual by comparing their presented fingerprint with the stored fingerprint data. In the context of voter identity validation, users would be required to provide their fingerprint, which would be scanned and compared to the previously recorded fingerprints to ensure a match. This biometric factor adds an additional layer of security by using a distinctive and difficult-to-replicate characteristic.

❖ **Picture Rotation Pattern:**

- **Definition:** A picture rotation pattern involves the user interacting with an image, typically by rotating or manipulating specific elements to create a unique pattern.
- **Explanation:** Picture rotation pattern authentication is a form of visual recognition where users are prompted to interact with an image in a specific way, such as rotating a certain part of the image. This dynamic interaction ensures the user's active participation in the authentication process and adds an extra layer of security by requiring a specific, user-defined action. The unique pattern created through the picture rotation serves as an additional factor to validate the user's identity.

In summary, the voter identity validation process involves a comprehensive approach, combining traditional digital identity documents with advanced biometric (fingerprint) and interactive (picture rotation pattern) elements. This multi-factor authentication aims to enhance the accuracy and security of verifying a voter's identity, reducing the likelihood of fraudulent activities in the voting process.

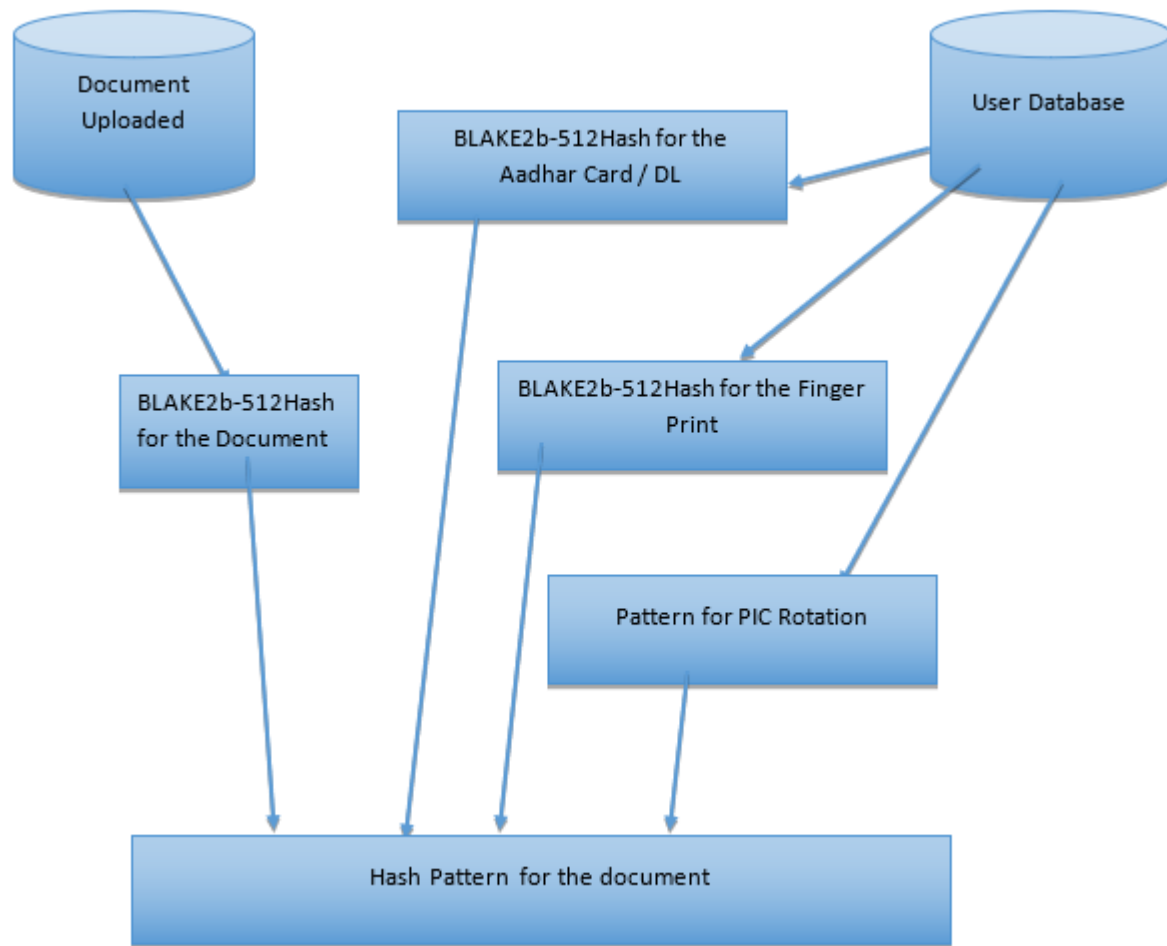


Fig 2. Document Sharing

### Process of Document Sharing:

#### ❖ Initiation:

- The document sharing process begins with a user or entity initiating the sharing request. This could involve selecting specific documents for sharing and identifying recipients or collaborators.

#### ❖ Authorization:

- Before proceeding with document sharing, the sender may authenticate and authorize the intended recipients. This step ensures that only authorized individuals have access to the shared documents.

#### ❖ Document Selection:

- The sender selects the documents to be shared, including digital copies of relevant identification documents like Aadhar Card or Driving License, as well as additional authentication factors like fingerprints and picture rotation patterns.

#### ❖ Document Uploaded:

- The selected documents are uploaded to the chosen platform or attached to an email, depending on the method of sharing. This step involves transferring the digital files to a location accessible by both the sender and recipients.

#### ❖ Hashing for Individual Documents:

- Unique BLAKE2b-512 hash values are generated for each uploaded document. This process involves applying a cryptographic hash function to create a fixed-size hash code that uniquely represents the content of each document.

#### ❖ Combination of Hashes:

- The BLAKE2b-512 hashes for the Document, Aadhar Card or Driving License, Fingerprints, and Picture Rotation Pattern are combined to create a composite hash pattern. This combined hash pattern uniquely represents the entire set of documents shared.

#### ❖ Hash Pattern for the Document:

- The final step involves creating a hash pattern for the document by incorporating the combined hash values. This hash pattern acts as a unique identifier for the shared document set, providing a secure and verifiable way to confirm the integrity and authenticity of the shared information.

In summary, the document sharing process involves initiating the sharing request, authorizing recipients, selecting and uploading relevant documents, generating individual hashes for each document, combining these hashes into a composite pattern, and creating a final hash pattern for the entire set of shared documents. This comprehensive approach ensures security, integrity, and authenticity throughout the document sharing process.

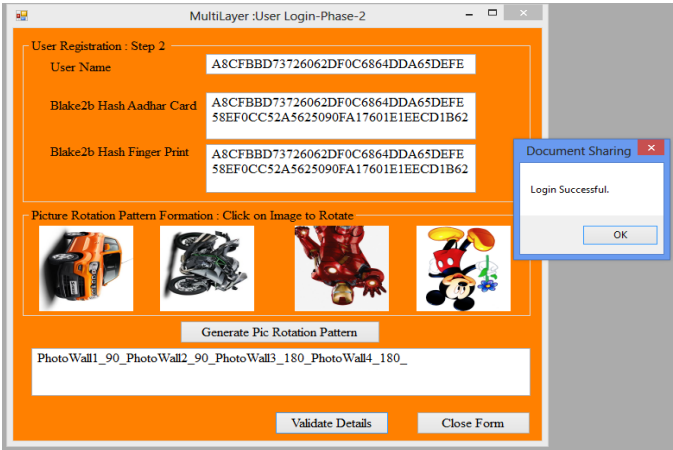


Fig 3. Implementation Details

IV. RESULTS AND DISCUSSION

One of the base papers for comparison, F. Z. Glory et al., 2019, formed the pattern on the basis of the concept then proposed on their paper, the sample pattern according to their concept is taken as, “Base Paper Password Pattern

{urAn29iRfan-

Proposed Password Pattern”

A8CFBBD73726062DF0C6864DD\_A8CFBBD73726062DF0C6864DD\_A8CFBBD73726062DF0C6864DD\_PhotoWall1

Table 1. Result Analysis

Website/Tool	Base Result	Proposed Result
Password Monster Tool	0.000005 trillion years	57 billion trillion trillion trillion trillion trillion trillion trillion years
Delinea.com Password Checker Tool	186 million years	32,514,707,246,498,062,000,000,000 quadragintillion years
How Secure is My Password Checker Tool	46 million years	8 septillion quadragintillion years

V. CONCLUSION

To safeguard data across diverse platforms and applications, organizations employ a combination of data encryption, hashing, tokenization, and key management practices. Document sharing is a crucial operation in every organization, and ensuring its security is paramount. The proposed system addresses this need by utilizing the Blake2B algorithm, offering a secure, trustworthy, and efficient approach to document sharing.

The system operates in two distinct segments:

- User Authentication Phase: During this phase, user validation occurs based on multiple factors, including Aadhar verification, fingerprint authentication, and a unique pattern generated through image rotation. These multi-level security checks enhance the authentication process and contribute to the overall security of document sharing.

- Document Sharing Approach: After successful user authentication, the document sharing phase commences. The system generates a File Sharing Key, comprising the Blake2B hash values of Aadhar, fingerprint, the shared document, and the picture rotation pattern. This approach ensures that the shared documents are protected with a robust layer of security.

The multi-level security checks implemented in the system have been substantiated through a thorough examination of various research papers and the use of tools to assess the strength of the generated patterns in terms of years and bits. This validation ensures that the system provides a high level of security, justified by its entropy and resistance to potential threats in the document sharing process..

## REFERENCES

1. Balamurali, A. , Harsha,M V R . , Hitesh, V S., Chaitanya, A S. (2019) , “Graphical password by image segmentation”,*International Journal of Innovative Technology and Exploring Engineering*, 8(6S4), pp. 462–464.
2. Chattopadhyay, A. *et al.* (2018) “A middle-school case study: Piloting A novel visual privacy themed module for teaching societal and human security topics using social media apps,” in *2018 IEEE Frontiers in Education Conference (FIE)*. IEEE, pp. 1–8.
3. Chung, W., Mustaine, E. and Zeng, D. (2017) “Criminal intelligence surveillance and monitoring on social media: Cases of cyber-trafficking,” in *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, pp. 191–193.
4. Colbaugh, R. and Glass, K. (2013) “Analyzing social media content for security informatics,” in *2013 European Intelligence and Security Informatics Conference*. IEEE, pp. 45–51.
5. Cui, Z. *et al.* (2020) “A hybrid BlockChain-based identity authentication scheme for multi-WSN,” *IEEE transactions on services computing*, 13(2), pp. 1–1.
6. Cui, X. (2019) “Social Media and Security,” in *2019 IEEE/ACIS 18th International Conference on Computer and Information Science (ICIS)*. IEEE, pp. 3–3.
7. Ekwunife, N. (2020) “National security intelligence through social network data mining,” in *2020 IEEE International Conference on Big Data (Big Data)*. IEEE, pp. 2270–2273.
8. Guidi, B. and Michienzi, A. (2020) “Users and Bots behaviour analysis in Blockchain Social Media,” in *2020 Seventh International Conference on Social Networks Analysis, Management and Security (SNAMS)*. IEEE, pp. 1–8.
9. Gupta, S. S., Thakral, A. and Choudhury, T. (2018) “Social media security analysis of threats and security measures,” in *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*. IEEE, pp. 115–120.
10. Giraldo, F. D., Milton C., B. and Gamboa, C. E. (2020) “Electronic voting using blockchain and smart contracts: Proof of concept,” *IEEE Latin America Transactions*, 18(10), pp. 1743–1751.
11. Heartfield, R. and Loukas, G. (2016) “Evaluating the reliability of users as human sensors of social media security threats,” in *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*. IEEE, pp. 1–7.
12. Herrick, D. (2016) “The social side of ‘cyber power’? Social media and cyber operations,” in *2016 8th International Conference on Cyber Conflict (CyCon)*. IEEE, pp. 99–111.
13. Huang, S.-Y. and Ban, T. (2020) “Monitoring social media for vulnerability-threat prediction and topic analysis,” in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, pp. 1771–1776.
14. Kunwar, R. S. and Sharma, P. (2016) “Social media: A new vector for cyber attack,” in *2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring)*. IEEE, pp. 1–5.