Ann. For. Res. 66(2): 291-300, 2023
ISSN: 18448135, 20652445

ANNALS OF FOREST RESEARCH
www.e-afr.org

FOLDER LOCK SYSTEM USING FINGERPRINT

Pooja Mishra[1], Mahesh Waghmare[2], Laxmikant Thombare[3], Vaishnavi Kute[4], Swapnil Awale[5]

[1,2,3,4,5]Dr. DY Patil Institute of Engineering Management & Research,
Akurdi-411035, Pune, Maharashtra, India

[1]pooja.mishra@dypiemr.ac.in, [2]mahesh.beed2018@gmail.com, [3]laxmikantthombare2001@gmail.com, [4]vaishnavikute2410@gmail.com, [5]swapnilawale1711@gmail.com

Abstract - Our research focuses on the implementation of the AES fingerprint algorithm exercise in Java, with a particular emphasis on securing specific folders, spaces, or disks rather than locking the entire system. This approach ensures that the entire system remains accessible to other users while providing targeted protection for restricted areas. In contrast to face ID and passwords, fingerprints offer a significantly higher level of security. Face ID systems can potentially be deceived using photographs or masks, compromising their reliability. Similarly, passwords are prone to being forgotten, shared, or easily guessed, making them vulnerable to unauthorized access. In comparison, biometric fingerprint recognition provides a more robust and reliable authentication method, enhancing overall system security. Biometric systems utilizing fingerprints not only provide a convenient and efficient means of verification but also offer a higher level of uniqueness and resistance to forgery. Each person possesses a unique fingerprint pattern, making it extremely difficult for impostors to replicate or tamper with. By incorporating biometric fingerprint techniques, our proposed study aims to reinforce the security and accuracy of the system. To achieve this, we will employ a biometric fingerprint sensor to scan documents, which will be integrated into a comprehensive authorization and access control system. The system will compile and manage user-accessible information, facilitating data retrieval and analysis for administrators. By implementing this arrangement, we ensure the system maintains accurate and up-to-date data, including any changes to the responsible personnel within the bureaucracy.

Keywords: AES, Biometric Fingerprint, Encryption Algorithms, Folder Lock,

1 . INTRODUCTION

You can be sure that nobody chooses to access your sensitive information by using an encrypted file. There are many problems with the current identification-located requests' guiding questions that call on the user to remember passwords, passwords that might be made up, or

questions that can be answered promptly and without rejection. Additionally, the password proof fails as the secret words for access are let to access the remaining portion of something. Due to its capacity to precisely identify people based on distinctive physiological or behavioural attributes, biometric authentication has attracted a lot of attention lately. The most popular and trustworthy biometric approach out of the several that are available is fingerprint recognition.

Both feature-based and correlation-based techniques can be used to recognise fingerprints. In order to verify the validity of a fingerprint, feature-based matching pulls specific information from input fingerprint photos and compares it with a reference database. This method ensures accurate recognition even in difficult situations and is especially resistant to deformations and fluctuations in fingertip circumstances.

As a result, it can be vulnerable to hacking using tools like vocabulary assaults or social science applications. Due to reversion, this technique has no characteristics in further consideration, and the system's behaviour is excessively limited and improperly incorrect for each modular structure's evidence. Multimodal biometrics, which are employed in the progressive plan, may be a combination of two different kinds of material or observable biometrics. Therefore, it is anticipated that bureaucracy will be able to resolve the aforementioned issues by enhancing multimodal biometric confirmation, which will offer an additional layer of security. Due to authentication's increased reliability, those problems are resolved and discovered by adding another layer of freedom. The most trustworthy and unambiguous confirmation method, which combines fingerprints and signs, has been devised and confirmed to work.

With increasing demands for automatic individual labelling during the past ten years, biometric authentication has received careful scrutiny. Biometrics search out identify things utilizing physiological or concerned with manner of behaving traits, in the way that ratina, fingerprint, iris, touch-print, and face. The most widely used biometric technique is fingerprint recognition, which is also the ultimate standard technique. Major approaches for fingerprint acknowledgment contemporary maybe broadly top-secret into feature-located approach and correlation-located approach. The majority of fingerprint recognition techniques use feature-located equal, which extracts trivia from the input mark figure and the recorded dab figure When deciding whether or not an image is a legitimate fingerprint, the number of trivia pairings that match between the two combined photographs is taken into consideration. Although weak-feature fingerprint representations can only be understood to a limited extent by featurebased matching, it is particularly robust against nonlinear fingerprint deformation accompanying low S/N percentage on account of surprising fingertip conditions (for example, dry fingertips, coarse fingertips, susceptible-skin fingertips) as well as feeble feeling of fingerprints. On the other hand, as one of the adept equivalence-located approaches, Biometric authentication (or completely biometrics) search out label a person established the corporeal or behavioral traits in the way that dab, face, iris, voice, signature, etc. So far, a assortment of biometric acknowledgment algorithms that combines calculating view, pattern recognition and countenance prepare methods have been projected. On the other hand, we have projected a united biometiric recognition treasure utilizing the signal processing located approach. Securing your private and something kept hidden is very main, because feasibility that few unlawful person can cause harm to it is extreme. Security issues stands when someone try to embezzle it or harm it founding a annoyance and loss. The process or operation of confirming an entity's validity, realness, or validity, as well as the method or operation of demonstrating the likeness of the user in order to permit access to only authorised customers. Replacing Password confirmation with Biometric Authentication has proofed expected more

favorable and appropriate. Private and confidential information must be protected because unauthorised access or interference can result in serious harm and financial loss. As a good and adequate substitute for password-based systems, biometric authentication establishes user identity using a user's distinctive biological traits.

The two categories of biometric authentication are physiological and behavioural. Physiological biometrics involve the recognition of physical characteristics like fingerprints, the retina, and faces, whereas behavioural biometrics involve the recognition of signatures, voices, and keystrokes. The system offers an additional layer of security to guarantee data confidentiality, integrity, and access control by utilising several modalities, such as fingerprint and signature.

The process of biometric authentication focuses on the distinctive organic characteristics of a person to confirm friendly similarity. Rules for biometric authentication match a biometric file capture to an authentic, often occurring file in a database. If two together samples of the biometric dossier match, confirmation is habitual. Biometric science is divided into two types that is to say, Physiological and Behavioral. Physiological Biometrics contains tangible features that is to say, Fingerprint flip through, Retina and Face recognition, when in fact Behavioral Biometrics contains Signature, Voice and Keystroke acknowledgment. Talking about Modality, has two types namely, Unimodal or Multimodal Biometrics. Unimodal Biometrics is the use of distinct organic feature while Multimodal Biometrics is the use of consolidation of more than individual physiognomy, thus adjoining another coating of protection.This system form use of Unimodal Biometric Authentication – Fingerprint Recognition for the purpose of locking and unlocking your pocket. The chapters of locked pocket will be stocked in encrypted format, so guaranteeing dossier confidentiality, dossier intergrity and chance. With the right encryption resolution, you can make sure that your dossier is cautious and that skilled is no rational way at which point hackers could conceivably catch their hands on the dossier. Although there are added method in which dossier manage conceivably be accessed, communicable the natural step toward encryption helps to form the job excessively troublesome for hackers that might usually act in accordance with mean your data.

2. LITERATURE SURVEY

The Blowfish algorithm is used by the File Encryption XP system to encrypt files. It guards against unauthorised people viewing or altering information. No encryption passwords are retained within the encrypted files because it employs a 384 bit key[1].

Data privacy is aided by SafeHouse Pro. Your sensitive data may be in danger at any time.

You must exercise greater caution as your data gets more portable. Thus, SafeHouse is employed for file encryption[1].

AES: There is no data transfer and an 8% energy usage increase when the key size in AES is increased by 64 bits. Larger key sizes affect how much battery and time are utilised with AES. [2].

Cloud storage was secured using hybrid cryptography [6]. A hybrid encryption and decryption algorithm was predicted using the RSA and AES algorithms. By claiming allure purity, the article was only drawing in bureaucratic unknowing uploading and downloading of dossiers.

Furthermore, the key disposal was extremely safe due to the delivery of three solutions for encryption and justification. To make the procedure more secure, only one key was generated.

When running file encryption/explanation and addressing the safety concerns needed to be resolved in cloud computing, Prakash et al. [7] suggested a key relation technique. They had also demonstrated through experiments that the CA inverter and shifter, when encryption and explanation are handled individually [8,] helps to reduce moment-of-fact complexity and handle different security assaults more expertly.

The public RSA cryptosystem and the backpack cryptosystem were combined to create a composite cryptographic technique [9]. Compared to using a single treasure, This suggested solution is more secure and less complicated. In order to proceed, you must first employ RSA encryption before attracting folks to the backpack approach. When executing the explanation at the recipient end, the reverse process must be anticipated.

[10] The face is found using an end-to-end facial recognition technology. With infrared lighting control, a frame differencing method is suggested. [11] Presented a facial recognition technology that could compare the image taken with database entries. [12] Viola-Jones used a classifier and applied it to a few panes inside the image to do confrontation identification.

uploaded a document using a variety of cryptographic techniques, including RSA, AES, and One Time Pad. This essay examined the variations among these three types of protection. It established that RSA and OTP were better suited for storing documents in the cloud after which a journalist was able to establish the critical moment, and the complexity of these innovations was less than that of other approaches. Jayapandian as well as others. For granting freedom in cloud data conversions, attracted on symmetrical key signalling code and irregular key signalling code methods. In symmetrical signalling code, the concept of a public and private key was employed to make the process more safe in cloud data conversion, as opposed to irregular key signalling code, where DES offers loans by using a single key.

3.PROBLEM STATEMENT :

To guarantee that only those who are authorised can access the secure data stored in cloud storage, we will be using an interface circuit in this project that opens and closes locks depending on fingerprints. The encryption technique used are for the best security and also the simplicity of the process to achieve that security.

Current System have many complex techniques and procedures as it increases the time of computing.

4.MOTIVATION :

The main slogan of system which controls organization search out better freedom for compartment plans at inferior costs that maybe inexpensive by all. security is a top priority for both businesses and individuals in the modern digital world. The suggested method tries to give more robust security safeguards while providing affordable options for managing sensitive data. Employing

this system enables organisations to compartmentalise their strategies effectively, enhancing control and access management.

Security is bigger concern immediately moment of truth. Bank document, government documents like pan card, itr, passwords etc all those are greatly private document so we needed to constitute spreadsheet that is extreme instability. Even Cloud are not secure as we should set our info on mediator attendant like google, amazon, azure, they might not always provide total security. A level of vulnerability is introduced when data is stored on third-party servers since the information is given to a mediator server. To protect the data from unauthorised access or potential breaches, it is crucial to adopt strong security measures, such as encryption and secure authentication processes.

An important strategy is developed to design the specified foundation using the fingerprint (bio-locker) system, When the SHA-256 technique is used for encryption and decryption, and fingerprint scanning is employed in documents to hide fingerprint information.

In this foundation the certified individual can store the main belongings like Passwords of main reports, Official and confidetial facts, concepts , videos and can catch approach of the room.

The main benefits concerning this foundation are:

- If some burglar tries to route the locker, therefore photographic equipment will inevitably captures the concept.
- Security thought-out as a conventional measure.

5. PROPOSED SYSTEM

In our project, the first step in the sequential process is taking people's fingerprints with a fingerprint scanner. The basis for developing a unique identify for every customer is this fingerprint data. We make sure that each fingerprint is properly recorded and processed by using a sophisticated fingerprint recognition algorithm.Once the fingerprint data has been collected, we move on to designate a specific location to safely store the person's information. The sensitive information will be kept in this place, which functions as a virtual vault. We use cutting-edge encryption techniques to turn the data into a digital gem while preserving its confidentiality and integrity.In order to manage user data effectively, our solution includes a flexible strategy, taking into account the future size and volume of user data. We assure effective data storage and retrieval by designing a system that divides data into more manageable categories.

Our solution uses a multi-layered imitation method to confirm the validity of user fingerprints in order to strengthen security measures. To accommodate for variances and guarantee precise identification, this method takes numerous samples of a person's fingerprint.The biometric measures used in our project's fingerprint science give the quickest and most reliable method of system security. We make sure that the fingerprint recognition process is quick, precise, and capable of providing strong protection by utilising cutting-edge technology and algorithms.Our project aims to provide the highest level of security and privacy for customer information by combining cutting-edge fingerprint scanning, encryption techniques, flexible data management, and multi-layered authentication. The objective is to develop a system that not only ensures the

protection of sensitive data but also offers users a seamless and convenient interaction with the system.

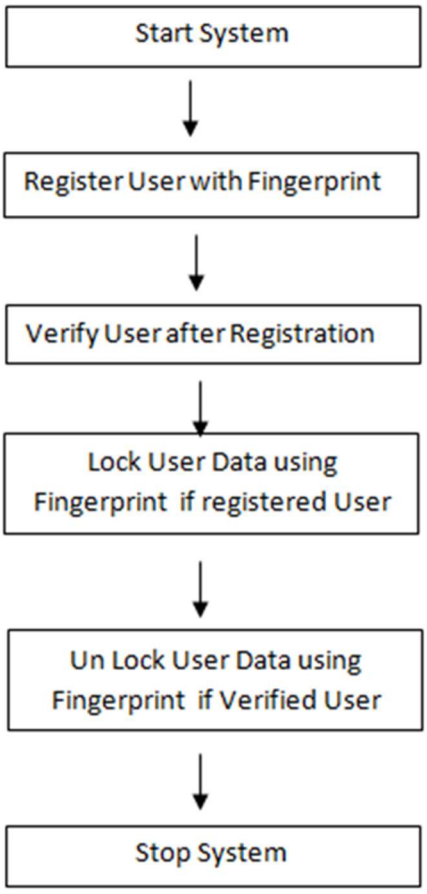

Fig 1.1 : Flow of Fingerprint Registration and verification

6. ADVANTAGES

1. The benefit of fingerprint authentication is that it removes the possibility of forgetting security codes or passwords.
2. A strong defence against unauthorised access or incursion attempts is offered by fingerprint authentication.
3. Due to the small number of distinctive fingerprint patterns, high security levels can be attained.
4. AES algorithm implementation guarantees robust security protections that are difficult to breach.
5. Since no other person may use a fingerprint that is an exact duplicate, fingerprint authentication provides exclusivity.
6. Fingerprint authentication is one type of biometric authentication that is thought to be secure and dependable.

7. By removing the requirement for password exchange, fingerprint authentication improves security in general.
8. Because fingerprint data is distinctive and challenging to duplicate, there is less chance of fraud or identity theft.
9. A further degree of security is provided by the inherent difficulty of forging or spoofing biometric features like fingerprints.
10. By giving a reliable and safe method of identification verification, fingerprint authentication brings piece of mind.

7. Architectural model:

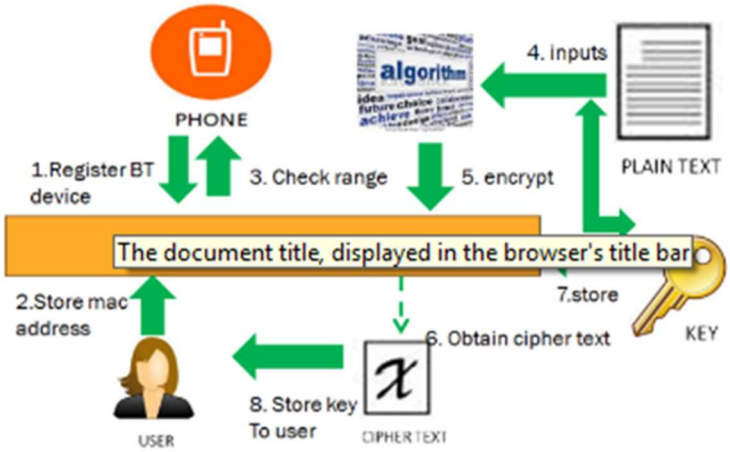

Fig 1.2 Architectural Model of Bio-Locker

8. LIMITATIONS

1. The calibre and condition of the person's fingerprints determine the precision and efficacy of the fingerprint scanner.
2. For real-time authentication and data transfer in the fingerprint authentication system, dependable internet connectivity is necessary.
3. The need for physical touch between the user and the fingerprint scanner raises questions about cleanliness and infection.
4. In fingerprint identification, false positives or false negatives can happen, which could result in access problems or security flaws.
5. The overall user experience and system performance may be impacted by the dependency on external elements, such as internet accessibility and fingerprint quality.
6. Continuous technological development and security measures are required to address and reduce worries about the chain of custody and potential breaches.
7. To ensure compatibility and smooth operation, integration with current infrastructure and systems may require extra hardware or software modifications.

9. CONCLUSION

This order is created to overcome the disadvantages of established Password Authentication whole by replacement identification accompanying Fingerprint Authentication System, making bureaucracy more secure and trustworthy. This Unimodal Biometric- Fingerprint Folder Lock order is beneficial not only at administrative level for keeping delicate data but more at the individual level for safeguarding private data. One of the notable advantages of this system is its ability to overcome the vulnerabilities associated with password-based authentication. With passwords, there is always a risk of unauthorized access due to weak or stolen passwords. However, with fingerprint authentication, each individual's unique biometric data acts as the key, significantly reducing the likelihood of unauthorized access.

Through this document, we may learn about the encryption techniques that were in use at the time as well as the advantages of the proposed strategy.

Additionally, this system's use of encryption techniques adds still another level of protection. The document provides information on the encryption methods that were widely used at the time, guaranteeing that confidential information is shielded from unauthorised access or alteration.The system streamlines access control procedures while simultaneously enhancing security by implementing fingerprint technology across the entire organisation. Each person's fingerprint is distinctive, ensuring that only authorised individuals may access critical information and lowering the possibility of breaches or data leaks.

The need of using fingerprint technology as a reliable and secure form of verification is emphasised throughout this document. With its cutting-edge fingerprint optical scanning for account confirmation, the system offers consumers the highest level of protection and reassurance, protecting them from potential dangers.

This document aids us in accepting the value of incorporating Fingerprint technology across our entire. Although skilled are miscellaneous different joining orders but in accordance with the study Fingerprint comes decided upon be highest in rank order. The feature offers more safety in our request because the MAC address is unique. This framework protects our freedom from point to point interference by undocumented women. A mark scheme structure to confirm consumer undertakings and supply User protection accompanying ultimate state-of-the-art Account confirmation utilizing a fingerprint optical scanning trailed.

10. FUTURE SCOPE

- The fingerprint authentication system offers a simple and safe approach to protect documents in government programmes like Digi-Locker while improving performance through aspects like memory and speed.
- A voice alert can quickly identify an unauthorised user accessing an account, offering an added degree of security.
- The programme may be made to work seamlessly with modems or cellphones, making it possible to access accounts from various devices with ease.

- The solution can accommodate increasing user counts and integrate with current security systems because to its scalability and versatility.
- The solution improves security and inhibits unauthorised access attempts by integrating two-factor authentication and sophisticated fraud detection.
- Secure account access on the go is made possible via mobile applications and remote access features.
- The fingerprint authentication system makes sure that privacy laws are followed and protects sensitive information.
- By removing password-related problems and expediting the authentication process, the system's implementation results in time and money savings.

11.REFERENCES

[1] D. Florencio etc. Hurley, "A Comprehensive Study of Web Passwords Practices, "in WWW '07: Proceedings of the 16th World Conference On the World Wide Web. Banff, Alberta, Canada: ACM, 2007, pages 657-666.

[2] J. E. Weber, D. Guster, p. Safonov, and M. B. Schmidt, "weak password Security: A Powerful Lesson. Data Security Journal: Global Ways, Vol. 17, no. 1, pages 45-54, 2008.

[3] P. Hunkecker, Ann. Borno and P P. Karayon, "Password Verification From a human point of view: research results among end users, " Procedures for the annual meeting of the Human Factors and the Ergonomics Society,
Vol. 53, pages 459-463 (5), September 2009.

[4] M. Dell'Amico, p. Mikiardi, and Y. Raudier, "Password strength: State Analysis, "In INFOCOM'10: 29 Processes
Information Communication Conference. Piscataway, NJ, USA:IEEE Press, 2010, pages 983–991.

[5] J. Yan, a. Blackwell, R. Anderson, and A. Grant, "Memorization and Password Security: Art Effects," Security and Privacy, IEEE, Vol. 2,No. 5, pages 25-31, 2004.

[6] V. S. Mahalle and A. K. Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa&Aes) encryption algorithm," 2014 International Conference on Power, Automation and Communication (INPAC), Amravati, 2014, pp. 146-149.doi: 10.1109/INPAC.2014.6981152.

[7] G.L.Prakash, M.Prateek and I.Singh, 'Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System', International Journal of Engineering and Computer Science, Vol. 3, Issue 4, April 2014, pp. 5215-5223.

[8] Akshita Bhandari, Ashutosh Gupta, Debasis Das. "A framework for data security and storage in Cloud Computing", 2016 International Conference Techniques in Information and Communication Technologies (ICCTICT), 2016.

[9] Fadhil Salman Abed, "A Proposed Method of Information hiding based on Hybrid Cryptography and Seganography", International Journal of Application or Innovation in Engineering & Management, Vol. 2, Issue 4, April 2013.

[10] Jinwoo Kang, David V. Anderson, and Monson H. Hayes, "Face recognition for vehicle personalization with near infrared frame differencing," IEEE, vol. 62, no. 3, Aug. 2016.

[11] S. Nishanthini, M. Abinaya, and Dr. S. Malathi "smart video surveillance system and alert with image capturing using android smart phones," in International Conference on Circuit, Power and Computing Technologies [ICCPCT], p. 201.

[12] Alpika Gupta and Dr. Rajdev Tiwari, "Face detection using modified viola jones algorithm," March, International Journal of Recent Research in Mathematics Computer Science and Information Technology, vol. 1, no. 2, pp. 59–66, Month: October 2014 – March, Available at: www. paperpublications.org Page | 59.2015.