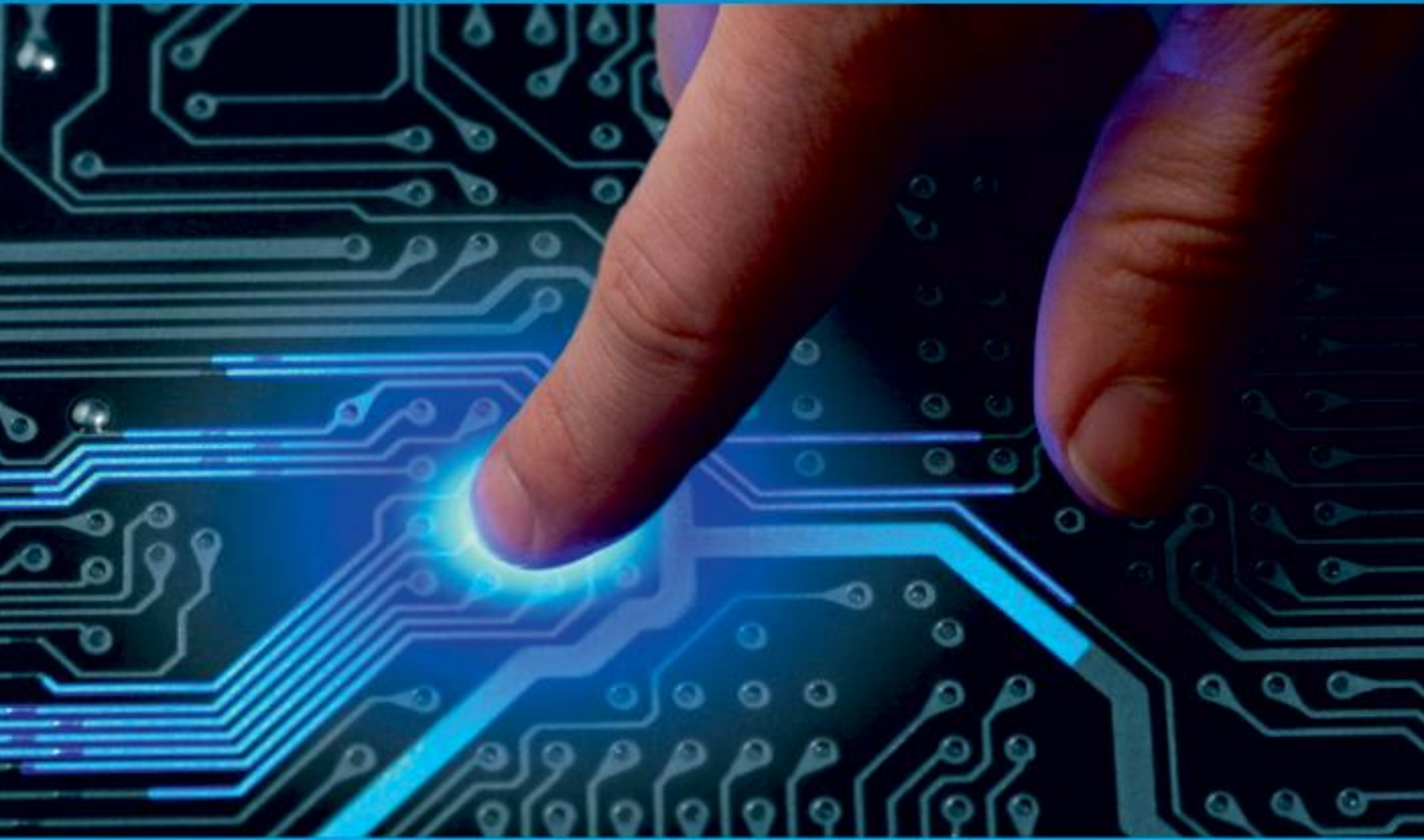
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205203 |

Folder Lock Security Using Fingerprint Authentication

Neha Kharkhande[1], Shrutika Sonawane[2], Sakshi Rane [3], Pradnya Wathore[4], Deepali Dhadwad[5]

Students, Department of Computer Engineering, Indira College of Engineering and Management, Pune, India[1,2,3,4]

Professor, Department of Computer Engineering, Indira College of Engineering and Management, Pune, India[5]

ABSTRACT: Our project is a Java implementation of AES algorithm for fingerprint encryption.
Biometric traits are unique to each person and wherever he goes, it goes with him. Lock folder is one of method that used to ensure nobody intentionally gets access to your private and confidential information.
Fingerprint authentication is an efficient system, as opposed to password-based authentication, where the password can be lost or forgotten or hack.
It has been proved and has been tested that using fingerprint as an authentication method is more secure and reliable.

KEY WORDS: AES, Biometric , fingerprint ,password

I. INTRODUCTION

A locked folder is a method used to ensure that no one intends to access your private and confidential information. Current password-based applications have many problems associated with problems such as requiring the user to remember passwords, passwords that can be guessed or broken violently and have non-rejection problems. In addition, the password verification method breaks as the keyword is allowed to access others. Therefore, it can be exposed and hacked using any means such as dictionary attacks, or social engineering. Due to regression, this method has no features in other features and the performance of the system is high limit and unacceptable error rate for one modular system verification. Multimodal biometric can be a combination of two types of any physical or behavioral biometric as used in the advanced system. Therefore, the system is proposed to overcome the above problems by adding multimodal biometric authentication that will provide an additional layer of security. Those issues are overcome and proven by adding another layer of security because authentication is much safer. It has been proven and tested to use a combination of two biometric methods, fingerprints and signatures, as the authentication method is the safest and most reliable.

II. LITERATURE SURVEY

Multimodal biometric can be at least combination of two types of any physical or behaviour biometric as it applies in the system that has been developed. Therefore, a system is proposed to overcome the aforementioned problems by adding multimodal biometric authentication will provide another layer of security. Those problems encountered have being overcome and it is proven that by adding another layer of security as the authentication is more secure. It has been proved and has been tested that using combination of two biometric methods, fingerprint and signature as an authentication method is more secure and reliable.[1]

One of the most challenging problems in fingerprint recognition continues to be establishing the identity of a suspect associated with partial and smudgy fingerprints left at a crime scene (i.e., latent prints or finger marks). Despite the success of fixed-length embeddings for rolled and slap fingerprint recognition, the features learned for latent fingerprint matching have mostly been limited to local minutiae-based embeddings and have not directly leveraged global representations for matching. In this paper, we combine global embeddings with local embeddings for state-of-the-art latent to rolled matching accuracy with high throughput. This leads to a multi-stage matching paradigm in which subsets of the retrieved candidate lists for each probe image are passed to subsequent stages for further processing, resulting in a considerable reduction in latency (requiring just 0.068 ms per latent to rolled comparison on an AMD EPYC 7543 32-Core Processor, roughly 15K comparisons per second).

Finally, we show the generalizability of the fused representations for improving authentication accuracy across several rolled, plain, and contactless fingerprint datasets.[2]

Security has always been a major concern for the households and the office environment, and for this concern various approaches are in place to address the problem. In the proposed system, fingerprints of the authorized users are enrolled and verified to provide access to a facility that is used by multiple users. A user can also be removed and a new user can be enrolled in the system. We have implemented a centralized control system from where we can control who can enter in which rooms and who cannot. This is an Arduino UNO device based flexible working device that provides physical security using the fingerprint sensor technology.[3]

Automatic fingerprint classification provides an important indexing scheme to facilitate efficient matching in largescale fingerprint databases for any Automatic Fingerprint Identification System (AFIS). A novel method of fingerprint classification, which is based on embedded Hidden Markov Models (HMM) and the fingerprint's orientation field, is described in this paper. The accurate and robust fingerprint classification can be achieved with extracting features from a fingerprint, forming the samples of observation vectors, and training the embedded HMM. Results are presented on two fingerprint databases, Finger db. and Finger/spl I.bar/DUT, respectively.[4]

Most biometric systems deployed in real-world applications are unimodal, such as they use a single source of information for authentication (e.g., single fingerprint, face, voice...). Some of the limitations +p by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity. In this paper, it is shown that fingerprint and face recognition can form a good combination for a multimodal biometric system and they are used in our work; where the system design in its hardware and software parts is done. The hardware part involves the capture devices, fingerprint signal processing unit, & PC. The software part includes the system software, databases, and face recognition module. The implementation of the system prototype as "Access Control System" with the suitable features was done.[5]

An urgent need to develop accurate biometric recognition system is expressed by governmental agencies at the local, state, and federal levels, as well as by private commercial companies. Fingerprinting is the most practical and widely used biometric technique. The pattern of ridges and valleys of each fingerprint is unique. The minutiae-based algorithm is widely used for fingerprint authentication. One of the significant parts of this algorithm is the classification of fingerprints which allows minimizing significantly the number of fingerprints referenced for each identification procedure. However, the minutiae algorithm has some serious drawbacks. If the core of a fingerprint is not visible, then identification cannot proceed. Yet in some cases, partial fingerprints need to be identified. We recently developed a novel contactless line scanner for recognition of fingerprint pattern that converts a three dimensional object like a finger into a two-dimensional image with minimal distortion. This novel imaging technique based on a line by line scanned image required the development of a new recognition algorithm. In this study, we propose two new algorithms. The first algorithm, called the spaced frequency transformation algorithm (SFTA), is based on taking the fast Fourier transform of the images. The second algorithm, called the line scan algorithm (LSA), was developed to compare partial fingerprints and reduce the time taken to compare full fingerprints. A combination of SFTA and LSA provides a very efficient recognition technique.[6]

III. PROPOSED SYSTEM

In our project, the step is to take the fingers using a fingerprint scanner. After fingerprinting we will use a fingerprint template and generate unique IDs for each user, after extracting the ID we will provide a place to lock and unlock user information such as files and use a folder byte rotation algorithm.

User data can be large in size, so our project provides a flexible way to process user data into smaller categories. The multiplayer simulation process is used to ensure multiple user finger verification. To achieve the fastest and most reliable security system, we use bio-metric fingerprint technology

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205203 |

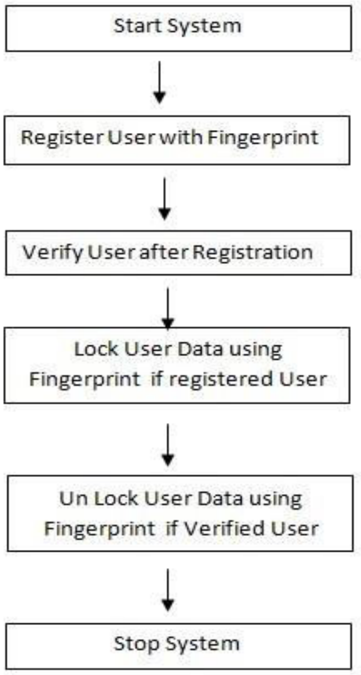

Start System
Register User with Fingerprint
Verify User after Registration
Lock User Data using Fingerprint if registered User
Un Lock User Data using Fingerprint if Verified User
Stop System

Chart -1: Flowchart

IV. ALGORITHM AND IMPLEMENTATION

Folder Lock is a software application used for securing and encrypting files and folders on a computer. While it does use AES (Advanced Encryption Standard) as one of its encryption algorithms, it typically doesn't directly involve fingerprint authentication

1. User Authentication:
 - Prompt the user to enter a password. - Verify the password against a stored password or hash.

2. Select Folder:
- Allow the user to select a folder to lock.
- Validate the folder's existence and permissions.

3. Encrypt Folder Contents:
- Encrypt all files and subfolders within the selected folder using a secure encryption algorithm (e.g., AES). 4. Lock the Folder:
- Hide or change the folder's attributes to make it inaccessible or less visible to users.

5. Access Control:
- Implement mechanisms to prevent unauthorized access to the locked folder, such as restricting access based on the entered password.

6. Unlock the Folder:
- Prompt the user to enter the correct password to unlock the folder.
- Decrypt the contents of the folder using the entered password.

7. Restore Original State:
- Restore the folder to its original state after unlocking, including file attributes and visibility.

8. Error Handling:
- Handle errors gracefully, such as incorrect passwords, file access issues, or unexpected program behavior.

9. User Interface:
- Develop a user-friendly interface for interacting with the application, including prompts, feedback messages, and options for managing locked folders.

10. Testing and Debugging:
- Test the application thoroughly to ensure it works as intended under various scenarios.

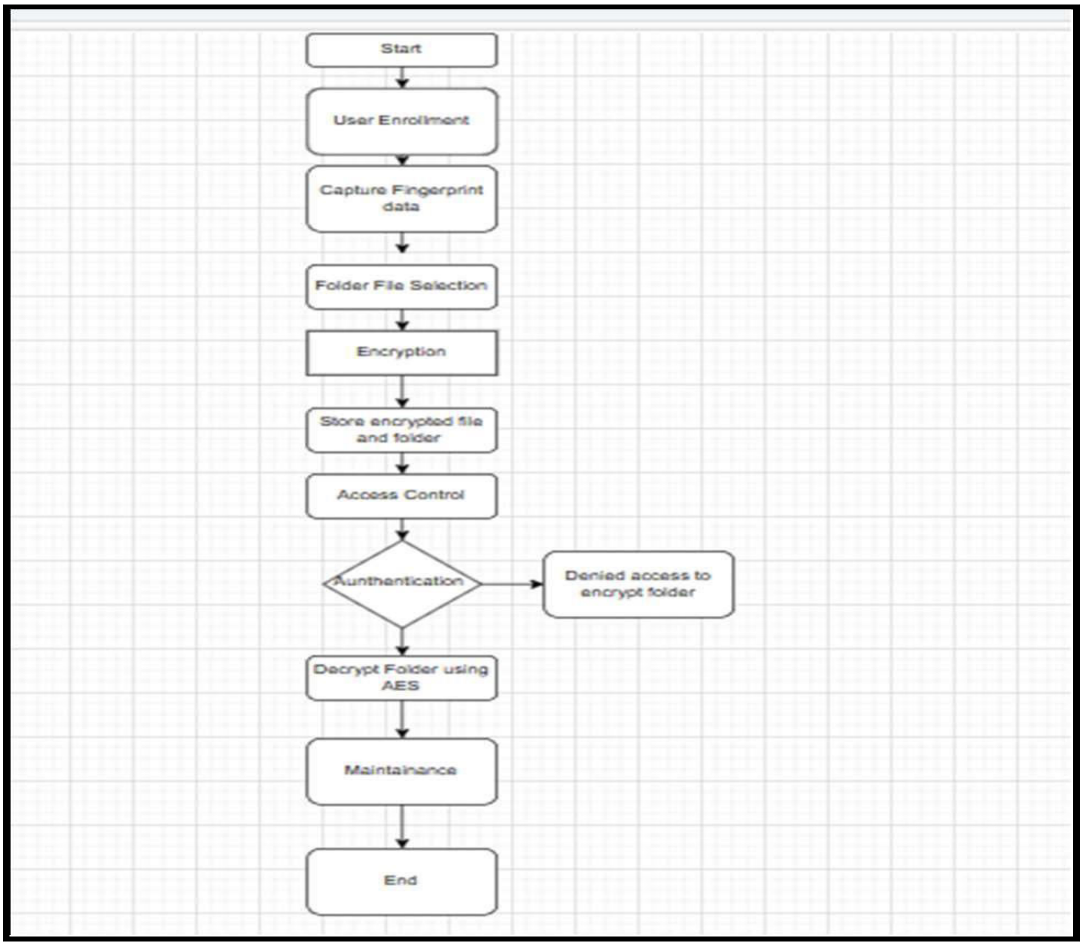
- Debug any issues that arise during testing.

11. Documentation:

- Document the project, including its purpose, features, implementation details, and usage instructions for users and developers.

12. Security Considerations:

- Ensure the application follows security best practices, such as securely storing passwords, using strong encryption algorithms, and protecting against common attacks like brute force or file system vulnerabilities



.

V. CONCLUSIONS

The fingerprint device-based system for securing the transactions of the user and providing the security for the User and even more for the Account verification using a finger print scanner has been followed.

This system is designed to overcome the limitations of traditional Password Authentication system by replacing password with Fingerprint Authentication System, making the system more secure and reliable. This Unimodal Biometric- Fingerprint Folder Lock system is useful not only at organizational level for protecting sensitive data but also at the individual level for protecting personal data. The system is designed with enhanced GUI making it more user friendly. The fingerprint device-based system for securing the transactions of the user and providing the security for the User and even more for the Account verification using a finger print scanner has been followed.

In the future we will try to increase Performance of the system in large amount of dataset and also implement speaking voice alarm can be used to indicate unauthorized person accessing the Account. We would like to express our sincere gratitude to Prof. Deepali Dhadwad, whose role as project guide was invaluable for the project. We are extremely

thankful for the keen interest she took in advising us, for the reference materials provided, and for the moral support extended to us. We express our deep sense of gratitude and humble thanks, for his valuable guidance throughout the project work. Furthermore, we are indebted to Prof. Sunil Rathod Project Co-ordinator, Dr. Soumitra Das HOD

VI. EXPERIMENTAL RESULT

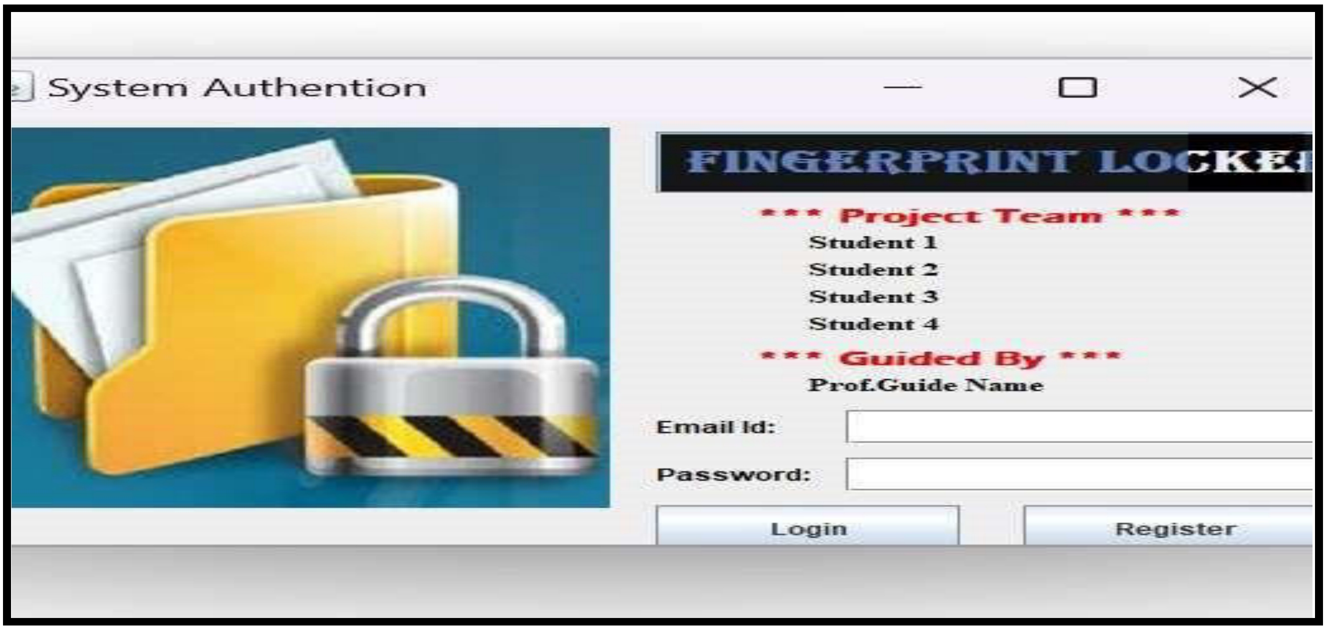
Folder lock security system using fingerprint authentication offers several advantages over other existing biometric systems:

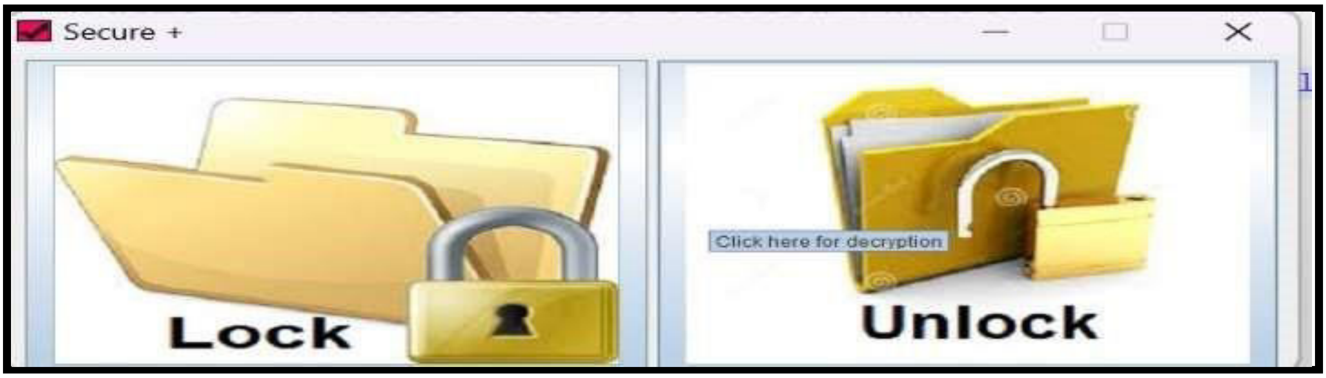
1. Unique Identity: Fingerprint authentication provides a unique and highly secure way to identify individuals. Each person's fingerprint is distinct, making it difficult for unauthorized users to gain access.
2. Convenience: Fingerprint authentication is convenient for users since they don't have to remember passwords
3. or carry around access cards. They simply need their fingerprint, which is always with them.
4. Accuracy: Fingerprint recognition technology has become very accurate over the years, with low false acceptance and false rejection rates. This ensures that only authorized users can access the system.
5. Non-transferable: Unlike access cards or passwords, fingerprints cannot be easily transferred or stolen. This adds an extra layer of security to the system.
6. Speed: Fingerprint authentication is fast and efficient, allowing for quick access without any delays.
7. Cost-effective: Implementing fingerprint authentication can be cost-effective in the long run since it eliminates the need for physical access cards and reduces the risk of password-related security breaches.
8. Unique Identity: Fingerprint authentication provides a unique and highly secure way to identify individuals. Each person's fingerprint is distinct, making it difficult for unauthorized users to gain access.
9. Convenience: Fingerprint authentication is convenient for users since they don't have to remember passwords
10. or carry around access cards. They simply need their fingerprint, which is always with them.
11. Accuracy: Fingerprint recognition technology has become very accurate over the years, with low false acceptance and false rejection rates. This ensures that only authorized users can access the system.
12. Non-transferable: Unlike access cards or passwords, fingerprints cannot be easily transferred or stolen. This adds an extra layer of security to the system.
13. Speed: Fingerprint authentication is fast and efficient, allowing for quick access without any delays.
14. Cost-effective: Implementing fingerprint authentication can be cost-effective in the long run since it eliminates the need for physical access cards and reduces the risk of password-related security breaches.

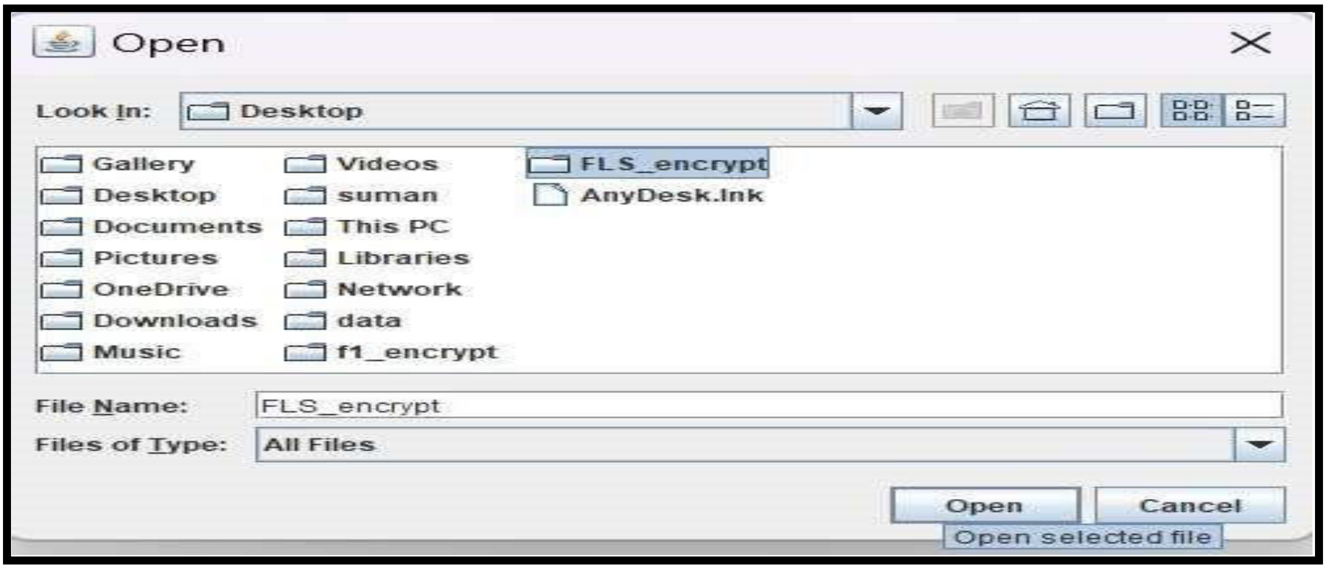
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205203 |



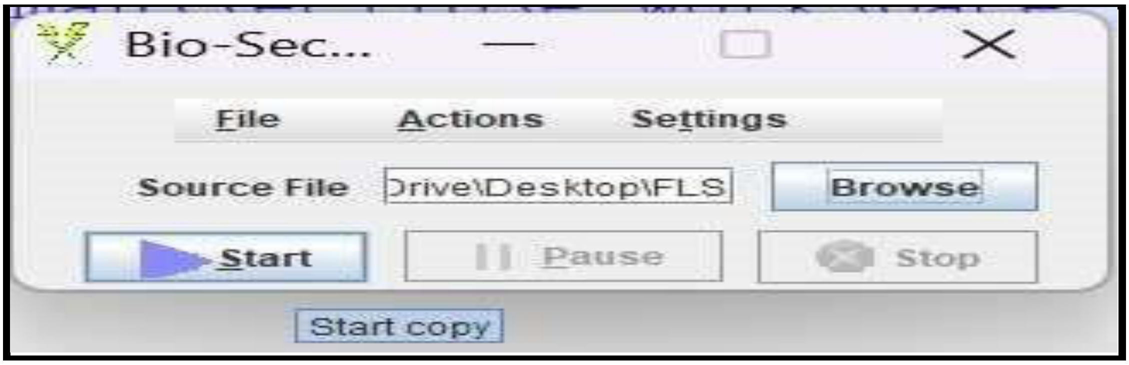




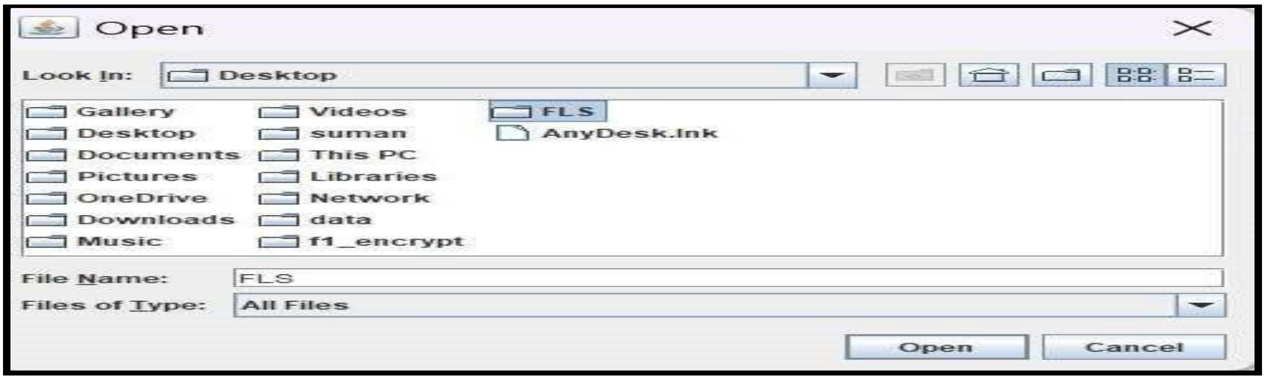
Look In: Desktop

File Name: FLS_encrypt

Files of Type: All Files



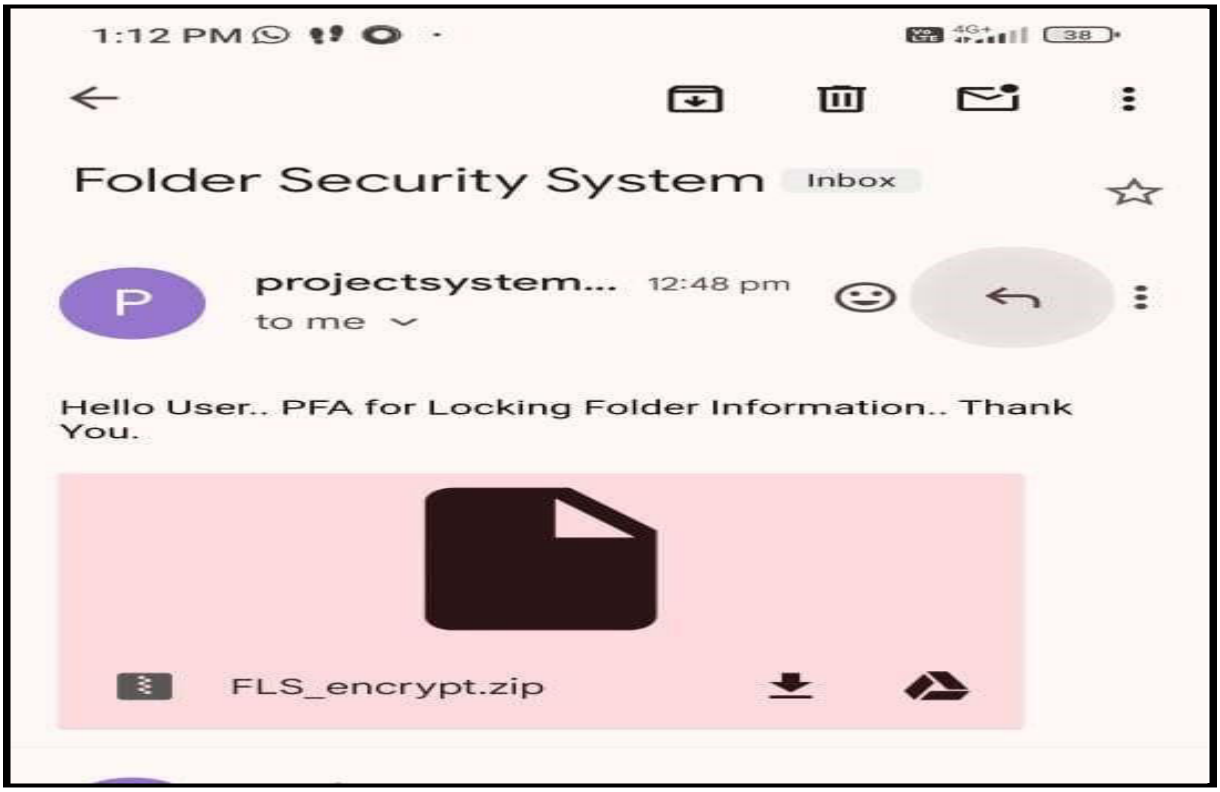
Source File)rive\Desktop\FLS



Look In: Desktop

File Name: FLS

Files of Type: All Files



Folder Security System

projectsystem... 12:48 pm

to me

Hello User.. PFA for Locking Folder Information.. Thank You.

FLS_encrypt.zip

REFERENCES

1. D. Florencio & c. Hurley, " Folder Lock by using Multimodal Biometric: Fingerprint and Signature Authentication "in WWW '07: Proceedings of the 16th International Conference On the World Wide Web. Banff, Alberta, Canada: ACM, 2021, pp. 657–666.
2. Norhaiza Bt Ya Abdullah, Herny Ramadhani Bt Mohd Husny Hamid "Automated Latent Fingerprint Recognition" A Global Perspectives, Vol. 17, no. 1, pp. 45–54, 2020.
3. S. M. Rahal, H. A. Aboalsalamah, K. N. Muteb
4. "Multimodal biometric authentication system"
5. Proceedings of the annual meeting of the Human Factors and Ergonomics Society, Vol. 53, pp. 459–463 (5), September 2020.
6. H. Guo, Z. Ying Ou, Y. He "Automatic fingerprint classification based on embedded hidden Markov models." 29th Proceedings Conference on Information
7. Communication. Piscataway, NJ, USA: IEEE Press, 2019, pp. 983–991.
8. J. S. Mil'shtein, A. Pillai, A. "Fingerprint recognition algorithms for partial and full fingerprints" Security and Privacy, IEEE, Vol. 2, No. 5, pp. 25–31, 2019. [6] S. Madabusi, V. Srinivas, S. Bhaskaran and M. Balasubramanian, "On-line and off-line signature verification using relative slope algorithm," Proceedings of the 2005 IEEE International Workshop on Measurement Systems for Homeland Security, Contraband Detection and Personal Safety Workshop, 2005. (IMS 2005), Orlando, FL, USA, 2005, pp. 11-15, Doi: 10.1109/MSHS.2005.1502546. [7] S. Mil'shtein, A. Pillai, A. Shendye, C. Liessner and M. Baier, "Fingerprint Recognition Algorithms for Partial and Full Fingerprints," 2008 IEEE Conference on Technologies for Homeland Security, Waltham, MA, USA, 2008, pp. 449-452, doi: 10.1109/THS.2008.4534494.
9. S. Madabusi, V. Srinivas, S. Bhaskaran and M. Balasubramanian, "On-line and off-line signature verification using relative slope algorithm," Proceedings of the 2005 IEEE International Workshop on Measurement Systems for Homeland Security, Contraband Detection and Personal Safety Workshop, 2005. (IMS 2005), Orlando, FL, USA, 2005, pp. 11-15, Doi: 10.1109/MSHS.2005.1502546.
10. S. Mil'shtein, A. Pillai, A. Shendye, C. Liessner and M. Baier, "Fingerprint Recognition Algorithms for Partial and Full Fingerprints," 2008 IEEE Conference on Technologies for Homeland Security, Waltham, MA, USA, 2008, pp. 449-452, doi: 10.1109/THS.2008.4534494.
11. R. Moganeshwaran, M. Khalil Hani and M. Annuar Suhaini, "Fingerprint-fingervein multimodal biometric authentication system in field programmable gate array," 2012 IEEE International Conference on Circuits and Systems (ICCAS), Kuala Lumpur, Malaysia, 2012, pp. 237242, doi: 10.1109/ICCircuitsAndSystems.2012.6408317. [9] A. M. Bazen, "Fingerprint identification - feature extraction matching and database search", 2002. [10] J. G. A. Dolfing, E. H. L. Aarts and J. J. G. M. Van Oosterhout, "On-line signature verification with hidden markov models", vol. 2, pp. 1309-1312, 1998.
12. J. G. A. Dolfing, E. H. L. Aarts and J. J. G. M. Van Oosterhout, "On-line signature verification with hidden markov models", vol. 2, pp. 1309-1312, 1998.
13. A. M. Bazen, "Fingerprint identification - feature extraction matching and database search", 2002.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 © 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details