



IJIRCCCE

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



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 4, April 2023

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

Secure Biometric Lock for Files and Application

Ms. M.kkute, Vedant Malpure , Chetan Patil, Aditya Pharatale , Sahil Taksal

Lecturer, Department Computer Engineering, Pimpri Chinchwad Polytechnic College, Nigdi, Pune, India

Student, Department Computer Engineering, Pimpri Chinchwad Polytechnic College, Nigdi, Pune, India

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. Fingerprint authentication is an efficient system, as opposed to password-based authentication, where the password can be lost or forgotten or hack

KEYWORDS: AES, Biometric

I. INTRODUCTION

A locked folder is a method used to ensure that no one intentionally has access to your private and confidential information. Currently used password based systems have many associated inconveniences and problems such as requiring the user to remember passwords, passwords can be guessed or broken through brute force and also have non-rejection problems is. In addition, the password authentication method is breakable as a keyword is allowed to access some. Therefore, it can be leaked and cracked using any method such as dictionary attack, or social engineering. Due to the drawback, this method lacks the universality of some features and the system's validation performance is the upper limit and the unacceptable error rate for a single modal authentication system. Multimodal biometric can be a combination of two types of any physical or behavioral biometric as it is applied in a system that has been developed. Therefore, a system is proposed to overcome the above problems by adding multimodal biometric authentication that will provide another layer of security. Those problems are being overcome and it has been proven that by adding another layer of security because authentication is more secure. It has been proven and tested that using a combination of two biometric methods, fingerprint and signature, as an authentication method is more secure and reliable.

1.2 Literature Survey

A locked folder is a method used to ensure that no one intentionally has access to your private and confidential information. Currently used password based systems have many associated inconveniences and problems such as requiring the user to remember passwords, passwords can be guessed or broken through brute force and also have non-rejection problems is. In addition, the password authentication method is breakable as a keyword is allowed to access some.

Therefore, it can be leaked and cracked using any method such as dictionary attack, or social engineering. Due to the drawback, this method lacks the universality of some features and the system's validation performance is the upper limit and the unacceptable error rate for a single modal authentication system. Multimodal biometric can be a combination of two types of any physical or behavioral biometric as it is applied in a system that has been developed. Therefore, a system is proposed to overcome the above problems by adding multimodal biometric authentication that will provide another layer of security. Those problems are being overcome and it has been proven that by adding another layer of security because authentication is more secure. It has been proven and tested that using a combination of two biometric methods, fingerprint and signature, as an authentication method is more secure and reliable. types may be used if needed for special purposes.

II. PROPOSED SYSTEM

In our project, the step is to capture the fingerprint using a fingerprint scanner. After finger capturing we will use the fingerprint template and generate unique IDs per user, after extracting the ID we will provide the facility to lock and unlock user information like files and using the folder byte rotation algorithm .

User data can be large in size, so our project provides a chunking mechanism to process user data in small segments. The multiplayer matching technique is used to verify the verification of multiple user fingerprints. To achieve high speed and reliable security system, we are using bio-metric fingerprint technology

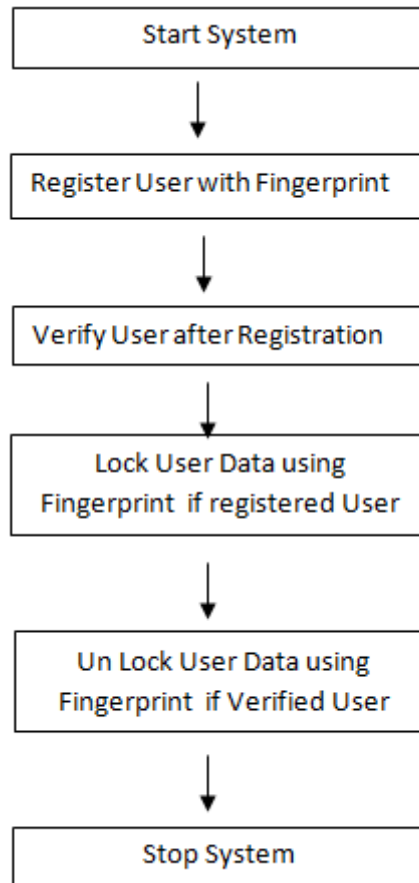


Chart -1: Flowchart

Advantage:

Biometrics has no risk of

1. Forgetting it
2. Getting in stolen
3. Getting it copied Being used by anyone else

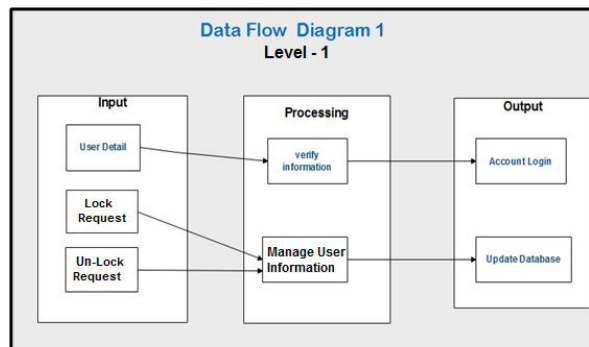


Fig -1: DFD 1

Future Scope : Performance can be increased in terms of speed and memory.

A speaking voice alarm can be used to indicate unauthorized person accessing the Account.

The system can be made to communicate with modems or mobile phones

1. Register a finger.
2. Keep your finger on the scanner and click capture.
3. The application will be closed after registration of the finger, now again open the application, enter the password and click on verify.
4. Match the fingerprint. You will get two options of lock and unlock if the print matches with the database.
5. click on lock. Browse the file you want to lock and click start.
6. The file gets locked and if you try to open the file ,error will occur.

III. 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.

ACKNOWLEDGEMENT (Optional)

The authors can acknowledge any person/authorities in this section. This is not mandatory.

REFERENCES

- [1] D. Florencio & c. Hurley, "A Large-Scale Study of Web Passwords Habits, "in WWW '07: Proceedings of the 16th International Conference On the World Wide Web. Banff, Alberta, Canada: ACM, 2019, pp. 657–666.
- [2] J. E. Weber, D. Guster, p. Safonov, and M. B. Schmidt, "weak password Security: An Empirical Study. Journal of Information Security: A Global Perspectives, Vol. 17, no. 1, pp. 45–54, 2018.
- [3] P. Hunkecker, Ann. Borno and P. Karayon, "Password Authentication From a human factors perspective: results of a survey among end users, "Proceedings of the annual meeting of the Human Factors and Ergonomics Society, Vol. 53, pp. 459–463 (5), September 2021.
- [4] M. Dell'Amico, p. Mikiardi, and Y. Raudier, "Password strength:An Empirical Analysis, "In INFOCOM'10: 29th Proceedings Conference on Information Communication. Piscataway, NJ, USA:IEEE Press, 2020, pp. 983–991.
- [5] J. Yan, a. Blackwell, R. Anderson, and A. Grant, "Password memorization and security: Empirical results," Security and Privacy, IEEE, Vol. 2,No. 5, pp. 25–31, 2021.



INNO  **SPACE**
SJIF Scientific Journal Impact Factor
Impact Factor: 8.379

doi[®]
CROSS **ref**

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



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