Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

Hybrid Security Framework based on Biometrics Features

Emtinan H. Rabee
Computer science
Iraqi Commission for Computer & Informatics (IIPS-ICCI)
Baghdad, Iraq

Dr. Muhammed N. Abdullah
Computer Engineering Dept.
University of Technology
Baghdad, Iraq

***Abstract*— In most information systems, security is one of the important aspects that consider when design the system. In transferring data, ensuring that the data is delivered to the recipient with confidentiality, by applying security methods. More than one algorithm is used to encrypt information in order to increase protection and reduce vulnerabilities. In this paper we present a design and implementation of system that use biometric technique in addition to hybrid encryption algorithms which are (AES, TDES). By using finger vein authentication and variant key selection to enhance the security and increased the complexity.**

Keywords—Hybrid security; AES (Advance encryption seurity); TDES (Triple Data Encryption Standard ; Finger Vein; LDA (Linear Discriminant Analysis)

I. INTRODUCTION

With the rapid development of digital data with its adoption and consideration as a basis in transactions, it became necessary to secure the types of data for transmission over the network. Hybrid Security can apply to get better secure data, by aggregation of two or more security methods such as symmetric and asymmetric cryptographic algorithms, wire and wireless techniques, protocols or biometric authentication to enhance the security, and others. Biometric technologies are applied for human features analyzing used in security purpose. Biometric authentication present high security and more appropriateness and easy to use than the traditional ways like passwords [1]. Encryption methodology addresses the necessity of data confidentially, and ensures the integrity of data. There are many encryption algorithms used in data security that can be classified into two categories: symmetric and asymmetric. In symmetric encryption one key is used at the two ends for encryption and decryption that is known before transmission. The key size is considered as significant factor in strength the encryption operation [2]. Advanced encryption standard (AES), triple data Encryption standard (TDES) are cryptographic standards intended for encrypting and decrypting a block of data. combination of algorithm with authentication feature take advantage of the all standard used and make it complex for intruder to get specified data. In the present system which aim to design and implement a framework using biometric finger veins with two encryption algorithms, finger veins biometric dataset is work as confirmation an assertion, applying preprocess operation to get feature vectors value to use it as a key encrypted by AES algorithm, while TDES used getting key for data encryption.

II. RELATED WORK

Many researchers are presenting hybrid security in different aspect as following:

Ranjith Jayapal suggested a system that used biometric merits to construct the high security biometric encryption system. fingerprints dataset is used to produce cryptography key to rise the security level. some steps of image processing to get minutiae points that lead to generate cryptographic keys to use it in different application [3].

F. Abundiz-Pérez, C. Cruz-Hernández, M. A. Murillo-Escobar,R. M. López-Gutiérrez, and A. Arellano-Delgado presented a structure of fingerprint ciphering using hyperchaotic Rössler map to support high security and privacy of user biometric merit, desist from identity theft problem, and raise the powerful of biometrics system. Security capabilities of presented structure are verified by security analysis to use in an application and apply security of biometric systems [4]

Susan Mohammed, Hussein Lafta and Saif Alalak proposed to build hybrid security protocol using two encryptions symmetric and asymmetric which are (AES) and Elliptic Curve Cryptography (ECC). Various keys are produced from the proposed integration of ECC algorithms and hash function, the keys obtained are used to encrypt the data by applying AES algorithm. Diehard test is used to check the high randomness of proposed system [5].

Wencheng Yang et al. suggested a cancelable finger-vein based bio-cryptosystem, that provide more security by authentication in addtion to encrypting the healthcare data using biometric cryptographic technique and fuzzy commitment scheme (FCS). The suggested system applied on smart card that provide further security with investment cancelable biometrics technique [6].

Rami k. Ahmed and Imad J. Mohammed proposed hybrid security by merge symmetric stream cipher RC4 algorithm and DNA-indexing algorithm to get hiding data safety and increased the complexity of framework. The result of proposed system provides high security performance and deformed in hybrid encryption algorithm [7].

III. PROPOSED SYSTEM

The proposed system idea is to use the finger vein authentication as a security factor to generate a security key and merge it with two encryption algorithms AES and TDES.

A. System phases

Four main phases are the system involved as follows:

1. **Finger veins data set:** Finger veins dataset images are used from open source dataset presented by the Chinese university Shandong, the acquired dataset via Group of Machine Learning and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

Applications "MLA" by Shandong University-Homologous Multimodal Traits "SDUMLA-HMT" include106 individual pattern, with 18 images for each sides of index, middle, ring fingers both hands.

2. **Preprocessing images:** The data set images may have some noise or infiltration, so that some operation in this phase included as follows:
   - RGB to grayscale level: To convert 3 channels of color (24-bit) to one channel (8-bit), by using Luminosity approach.
   - Histogram equalization: to redistributed the image pixels' densities.
   - Resizing: To be convenient for processing using bilinear interpolation method.
3. **Feature extraction:** In feature extraction phase utilize the LDA algorithm, with resulted feature vectors, a series of numbers are got that can be used as a key for TDES encryption algorithm. The characteristic of this step that the key is different with each finger vein patterns entered.
4. **Applying encryption algorithms:** The key obtained from previous phase encrypted using Advance Encryption Standard (AES) algorithm with standard key, and the entered data encrypted using Triple Data Encryption Standard TDES algorithm with the key obtained. "Fig. 1" show the system flowchart.

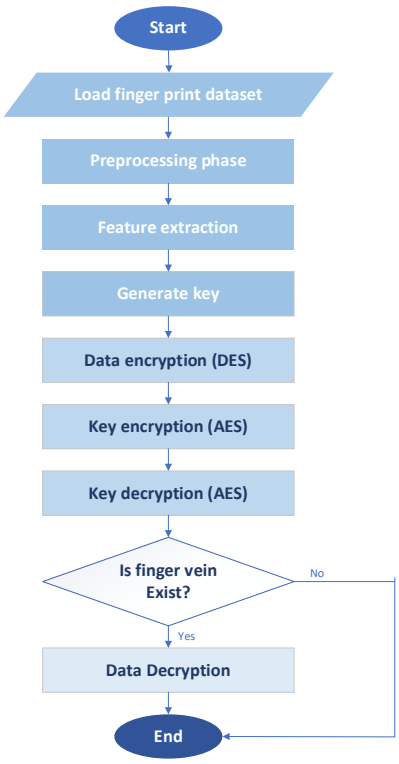


Fig.1. System Flowchart

B. System Design

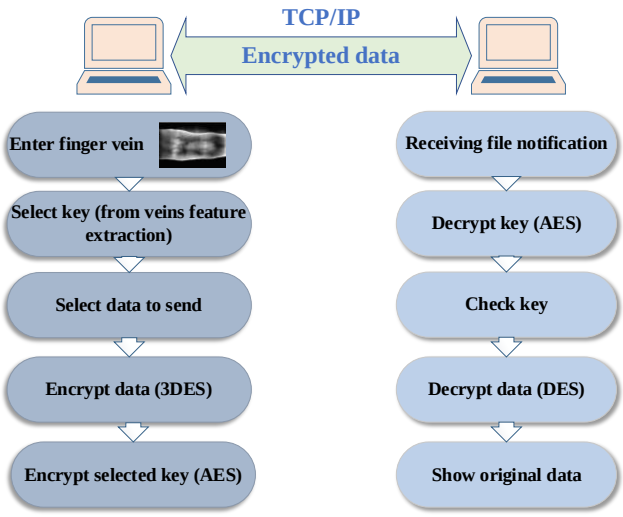


Fig. 2. System Design Overview

The hybrid security framework is based on client-server architecture. At the client side the user entered his finger vein to generate security key by using feature that extracted by LDA, this security key will be used for TDES encryption algorithm for selected data, the security key is also encrypted using AES encryption algorithm. Then the encrypted data and key are sent over TCP/IP protocol. At the server side, the security key is decrypted, then the system check if the individual is authorized to decrypt and show the message. "Fig. 2" above show system design overview.

C. System Implementation

The framework is established using java programming language under NetBeans 8.0.2 IDE, and C++ programming language under Visual studio 2013 for image processing operations, computer with the following properties: Windows-10 operating system. Processor: Intel Core i3 CPU (1.70) GHz. Memory: (4GB) RAM. At the sender side, the user has to add his finger vein to the system, so that he can send and received specified data. Finger vein is considered as a security key that user can use it to encrypt data using TDES algorithm, and then encrypt the key using AES algorithm to send the data. The key size used in AES algorithm to encrypt the key (from feature extraction) is 128-bit. At the recipient side notification message is appearing to tell about data received. the key is decrypted first, then the system check if the individual is authorized and return the identity of user to decrypt and show the message. If not, the system deactivates the decrypt data bottom. The proposed system deals with text data. "Fig. 3.a", "Fig. 3.b," show system interfaces.

Three classes of users who at the receiver side:

- ✓ User not exist in finger veins database so he can't decrypt and see data.
- ✓ User exist in the database but unauthorized to see data.
- ✓ Authorized user who can decrypt and see data.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

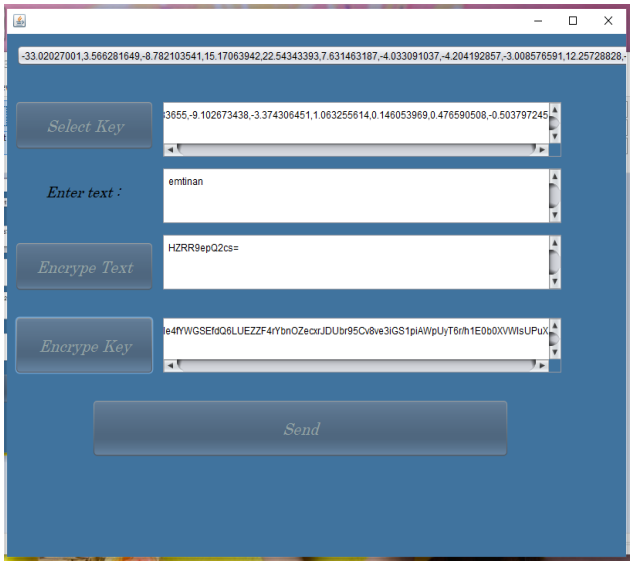


Fig 3.a. client interface

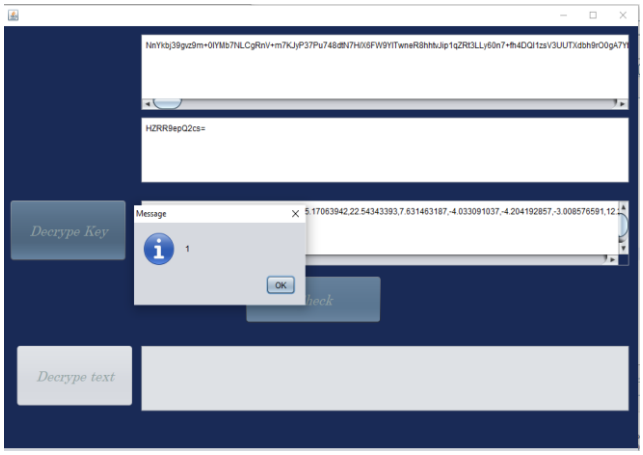


Fig 3.b. server interfaces

An example authorization of access an office with central site that can access all departments “Fig. 4” illustrate the example, and each head of department can get access of his employees only. Colored ellipse is representing the privacy of each department.

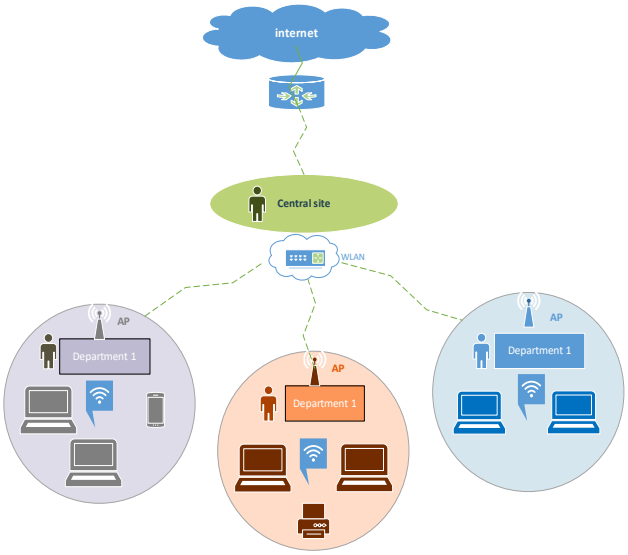
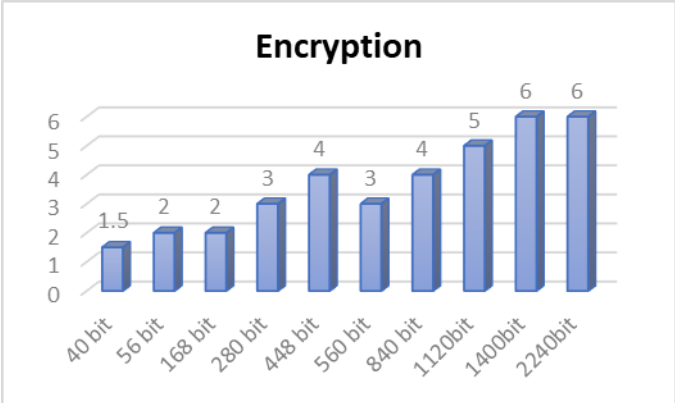
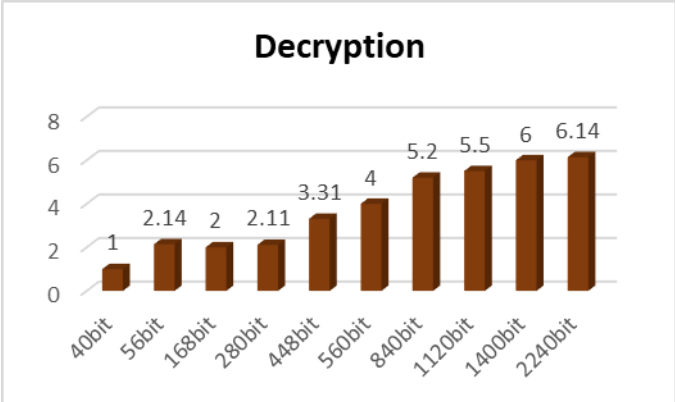


Fig. 4. access authorization example

IV. Result And Discusion



Graph 1



Graph 2

Graph "1" and graph "2" show the encryption time and decryption time (in Millisecond) during testing system for several entered data with different keys. System execution with different data is fast, and consider light, it consumes less power and CPU space according to the properties of the computer used.

V. Conclusion

In this paper we shown that hybrid security can take various form, using finger vein authentication with two symmetric encryption algorithms are used in the system, which are used one secret key at the two sides when encrypt and decrypt data, in proposed system data encrypted by TDES algorithm, and the decryption operation is not fixed with one key for all data. Thus, it acts like digital signature but in a symmetric mechanism this enhance the system security. Ciphering the key in addition to ciphering data with variation of TDES key increased the complexity of system so make it harder to vulnerability.

REFERENCES

[1] Kišasondi, T., Bača, M., & Lovrenčić, A. “Biometric cryptography and network authentication”. Journal of Information and Organizational Sciences, in 2007.

[2] Elminaam, D. S. A., & City, R. “Performance Evaluation of Symmetric Encryption Algorithms”. In 2009.

[3] Jayapal, R., & Govindan, P. “Biometric encryption system for increased security”. IMCIC 2018 - 9th International Multi-Conference on Complexity, Informatics and Cybernetics, Proceedings, in 2018.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

[4] F. Abundiz-Pérez, C. Cruz-Hernández, M. A. Murillo-Escobar, R. M. López-Gutiérrez, & A. Arellano-Delgado, A Fingerprint Image Encryption Scheme Based on Hyperchaotic Rössler Map. Hindawi Publishing Corporation, Volume 2016, Article ID 2670494, in 2016.

[5] Susan Mohammed, Hussein Lafta and Saif Alalak, "Hybrid Security Technique for Wireless Sensor Network" A Thesis Submitted to the Council of the Collage of Science for Women at the University of Babylon in April 2019.

[8] Yang, W., Wang, S., Hu, J., Zheng, G., Chaudhry, J., Adi, E., & Valli, C. Securing mobile healthcare data: A smart card based cancelable Finger-Vein Bio-Cryptosystem. IEEE Access, in 2018.

[9] Ahmed, R. K., & Mohammed, I. J. (). "Developing a New Hybrid Cipher Algorithm using DNA and RC4". International Journal of Advanced Computer Science and Applications, in 2017.