IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 3, Ser. I (May - June 2019), PP 06-12
www.iosrjournals.org

Encryption and Decryption of Biometric Traits

Brinzel Rodrigues [1], Rushikesh Pawar[2], Pranay Patil[3], Ankit Gour[4]

[1]*(St. John College of Engineering & Management, India)*

[2]*(St. John College of Engineering & Management, India)*

[3]*(St. John College of Engineering & Management, India)*

[4]*(St. John College of Engineering & Management, India)*
Corresponding Author: Brinzel Rodrigues

Abstract: *Biometric authentication has been incredibly useful in services such as access control to authenticate individuals based on their biometric traits. Unlike password or identity documents, biometric traits, such as fingerprint, iris and behavioral characteristic are physically linked to an individual that cannot be easily manipulated.*
The traditional biometric authentication model uses a server-centric model, where a service provider maintains the biometric database and is totally responsible for the security of templates. The end-users have to fully trust the provider in storing, processing and managing their private templates. As a result the end-user templates could be compromised by outside attackers or even the service provider itself. As a result we propose a user-centric biometric authentication scheme that enables end users to encrypt their own templates with our proposed lightweight encryption scheme at the time of authentication.

Keywords: *User centric model, Biometric Authentication, Encryption, Decryption, AES Algorithm*

Date of Submission: 18-04-2019 Date of acceptance: 04-05-2019

I. Introduction

In Recent times Biometric Authentication has been reached to a whole new different level in services such as authentication of individual based on their traits. Previously the authentication system was based on password or identity documents which were difficult to remember as the user has multiple accounts on different sites. As a result we use Biometric traits for authentication which are physically linked to an individual that cannot be manipulated easily [1]-[2].

The biometric system that are currently running generally employee a two phase mechanism [3]. In the first phase the end user submits his/her biometric template to the service provider who will store the template along with the end users id in the database. In a query phase the end user requesting for certain services will submit a fresh template to the service provider for authentication based on the end users id the service provider will retrieve the enrolled template for comparison. Only if the two templates are close enough the end user will be successfully authenticated.

The above mentioned model is regarded as server centric. That is, end user is fully responsible for the security of end user templates. To address the above issue, we propose a user centric model for biometric authentication. In terms of security the user centric model has many benefits over the traditional server centric model. Firstly, the biometric template of the user will be encrypted at the user side and then it will be transmitted to the server side. The Service provider only be able to see the encrypted version of registered template and query template. Secondly, the secret keys and the templates are generated and processed locally, thus never leaving the local environment. Third, computations that are involved in authentication process are all carried out on cipher text, meaning that no templates are exposed in plain text during the authentication. To meet the demands of the proposed user centric model, the underlying encryption scheme should be efficient and expose as little information as possible. Since the main part i.e key management and authentication are carried out on user side, the encryption scheme should be computationally efficient.

A few existing encryption scheme such as predicate encryption [5], inner product encryption and homomorphic encryption [4] which rely on important cryptographic operations may not be realistic in such a scenario.In this paper we propose a primitive named Advanced Encryption Scheme (AES). The popular and widely used symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found faster than many other symmetric encryption algorithms. In present day cryptography, AES is widely used and supported in both hardware and software. Till date, no practical cryptography attacks against AES have been discovered. Moreover, AES has built-in flexibility of key length, which allows a amount of 'future-proofing' against progress in the capability to perform thorough key searches.

II. Literature Review

In this section , we will look at several similar systems that are been researched and implemented by other researchers for further understanding on their methods and techniques , refer to the reference page at the end of this report to search or text or even websites published.

RSA based biometric encryption system using FPGA for increased security, the paper was published in IEEE International Carnahan Conference on Security Technology (ICCST) in the year 2016.

The intention of this research is to propose an RSA based biometric encryption system which can be realized on field programmable gate arrays (FPGAs) using hardware-software co-design methods. Due to the high number of hackers that stand to profit from sub-par security methods, the proposed design will serve as a high level of security. This implementation can be applied in many areas of life including but not limited to password replacement, building and equipment access, and payroll and reliability procedures.[7]

Biometrics-as-a-service: A framework to promote innovative biometric recognition in the cloud, this paper was published in IEEE 2018.

It present a framework for Biometrics-as-a-Service (BaaS) which perform biometric matching operations in the cloud, while relying on simple and ever-present end user devices such as smart phones or personal devices. Further, the framework promote innovation by providing interfaces for a plurality of software developers to upload their identical algorithms to the cloud. When a biometric authentication request is submitted, the system uses criteria to automatically select an appropriate matching algorithm. Every time a particular algorithm is selected, the equivalent developer is rendered a micropayment. This creates an inventive and ready for action ecosystem that benefits both software developers and the consumers.[8]

Design of Biometric Authentication System using Three Basic Human Trait, the paper published in IJSR in the year 2016.

It discusses about biometric system use in various system for the recognition or authentication approval. Biometric authentication system utilize various biometric behaviour for the matching between various biometric traits. Various approaches have been used for the removal of features from various types of biometric traits. In the proposed work system the biometric traits utilize are face, fingerprint and iris. Single Biometric trait system is fail to provide accuracy for the validation of different identities because due to single biometric trait the chances of mismatching increases. So to overcome these disadvantages of single trait biometric system, multimodal biometric system come into reality. Multimodal biometric system use face, finger and iris images for the expansion of planned system. Feature from each biometric credential has been extracted and fused on the basis of score level fusion to reduce feature dimension. Computation speed increases due to reduction in feature measurement of fused features. This proposed system provides accuracy of 100%. This provides better security than other biometric system because illegal accessibility of all the traits of single person is not available to match and perform any illegal operation.[9]

Development of a new Methodology for iris algorithm in Biometric authentication using hamming distance concepts, the paper published in IEEE in the year 2017.

Since biometrics is extremely difficult to forge and cannot be elapsed or stolen, Biometric authentication offers a convenient, accurate, irreplaceable and high secure alternative for an individual, which makes it has advantages over traditional cryptography-based authentication schemes.In the recent years, this biometrics has become most identifiable method of recognizing the person in all round fields & is gaining prominence in the defence, banking, retail, consumer product, examinations, etc. In this context, a sincere effort is being made to develop some novel method of identifying a person in form of developing a unique biometric identification system that has got some good advantages over the existing methodologies in the current scenario. Fast processing algorithms are being developed by keeping into mind the speed of computation (3-4 secs). The huge database is being considered to start with, followed by the pre-processing, segmentation, normalization, feature extraction & the matching scenario with the final matched results.[10]

Can homomorphic encryption be practical? The paper published in proceedings of the 3rd ACM workshop on Cloud Computing Security Workshop, in the year 2011.

It discusses about the vision of outsourcing an growing amount of data storage and management to cloud services which raises many new privacy concerns for individuals and businesses alike. The privacy con0cerns can be adequately addressed if users encrypt the data they send to the cloud. If the encryption scheme is homomorphic, the cloud can still carry out meaningful computations on the data, even though it is encrypted. In answer to the question of whether homomorphic encryption can be practical, we give several concrete applications to useful cloud computing scenarios.[4]

III. Research Methodology

Following is the architecture for the project. The Biometric Authentication is done with the help of Fingerprint Scanner. Biometric traits are being encrypted at the time of Registration. While that template is being stored at the database. At the time of Login that template is being fetched with the help of unique id assigned to it and that template is Decrypted at the user side. After the minute extraction is being verified and it is matching template then only the user can access the portal or else access is denied.

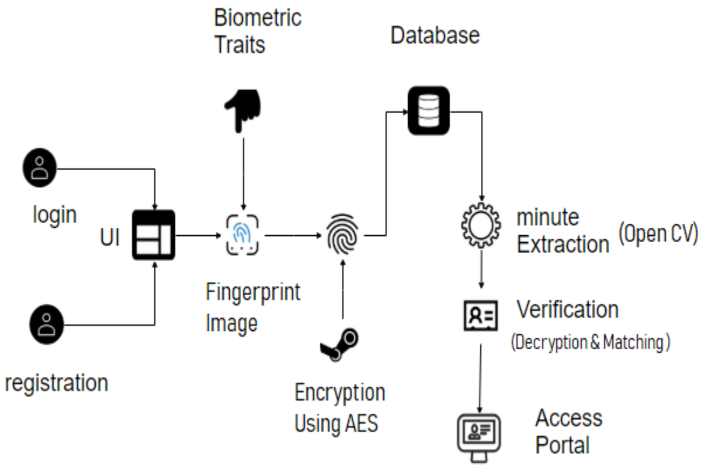


Fig.1. System Architecture The proposed system is divided into following steps:

1. The first step is to take the Biometric Template from user through finger print scanner, with which a unique ID is assigned to the user.
2. In second step this Biometric Template will be encrypted using Advanced Encryption Standard (AES) algorithm.
3. The third step consists of saving this encrypted Biometric Template on the cloud/database.
4. When the user tries to access (login) the system using its unique ID and by scanning finger print then again the biometric template of the user will be encrypted and the server based on unique id of the user will fetch the registered encrypted biometric template from the cloud/database.
5. The first step is to take the Biometric Template from user through finger print scanner, with which a unique ID is assigned to the user.
6. In second step this Biometric Template will be encrypted using Advanced Encryption Standard (AES) algorithm.
7. The third step consists of saving this encrypted Biometric Template on the cloud/database.
8. When the user tries to access (login) the system using its unique ID and by scanning finger print then again the biometric template of the user will be encrypted and the server based on unique id of the user will fetch the registered encrypted biometric template from the cloud/database.
9. Now the server will compare these encrypted template, the one which was stored in the database at the time of registration and the one whenever the user tries to login.
10. If both the template are within a specific threshold value than at the user side the encrypted template will be decrypted and the access will be given to the user.

IV. Algorithm Implementation

Some of the features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details

- Software implementable in C and Java

Operation of AES:

Advanced Encryption Standard (AES) algorithm is mostly used algorithm and it is based on the principle of ‘substitution–permutation network’. It is based on ‘substitution–permutation network’. It comprises of a number of operations that are linked with each other, out of the many operation some include substitution i.e. replacing the input by specific output and the other operation is known as permutation i.e. it involve shuffling of bits around .

Unlike some other algorithm which performs its computation on bits Advanced Encryption Standard (AES) perform all of its computation on bytes. AES computes on bytes and therefore it treats all the bits as bytes for example 128bits is treated as 16 bytes Advanced Encryption Standard (AES) algorithm basically functions on 4 x 4 matrix. Therefore the bytes are arranged in four rows and four columns matrix for processing.

AES is quite different than DES and hence the number of rounds in AES is variable. The round in AES completely depends upon the length of the key. Advanced Encryption Standard (AES) uses 10 rounds, 12 rounds and 14 rounds for 128 bit keys, 192 bit keys and 256 bit keys respectively. Every round in the AES algorithm uses diverse 128 bit round key and this is calculated from none other than the original AES key itself.

Encryption Process:

Here, we limit to depiction of a typical round of AES encryption. Each round consists of four sub-processes. The first round process is depicted below –

1) Byte Substitution

The 16 input bytes are substituted by looking up a permanent table (S-box) given in design. The outcome is in a matrix of four rows and four columns.

2) Shiftrows

All of the four rows of the matrix is shifted to the left. Any entry that ‘fall off’ are re-inserted on the right side of row. Shift is carried out as follows –

- First row of the matrix is not shifted.
- Second row is shifted by one (byte) place to the left.
- Third row of the matrix is shifted two positions to the left.
- Fourth row of the matrix is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with value to each other.

3) MixColumns

Each column of four bytes is now altered using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is a different new matrix consisting of 16 new bytes. It should be noted that this measure is not performed in the last round.

4) Addroundkey

The 16 bytes of the matrix or the environment are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output of this is cipher text. Otherwise, the resultant 128 bits are interpreted as 16 bytes and we begin another similar round.

5) Decryption Process

The process of decryption of an AES cipher text is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the overturn order

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round or in each process are in reverse style, dissimilar for a Feistel Cipher, the encryption and decryption algorithms needs to be individually implemented, although they are very closely related.

V. Result and Analysis

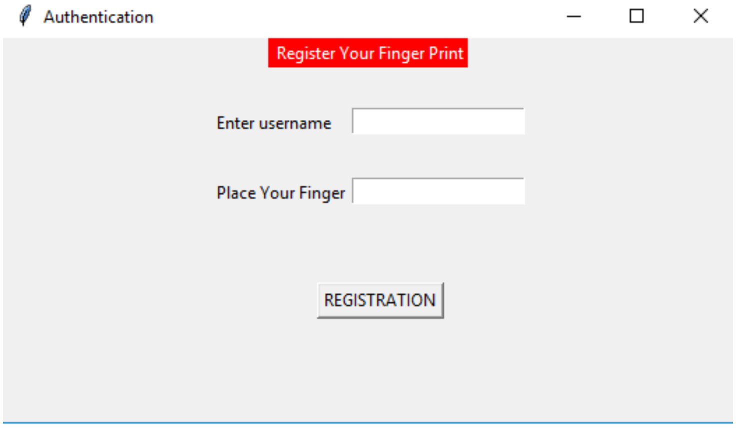
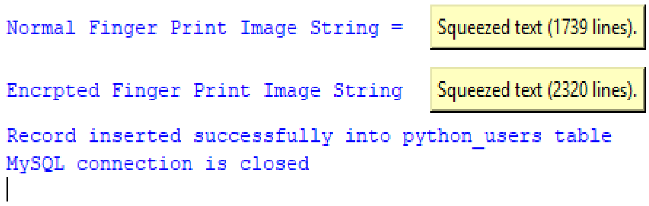


Fig.2. (a) Snapshot of Registration Page

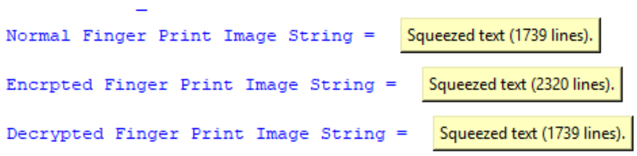


```
Normal Finger Print Image String =  Squeezed text (1739 lines).

Encrpted Finger Print Image String  Squeezed text (2320 lines).

Record inserted successfully into python_users table
MySQL connection is closed
```

Fig.2. (b) Snapshot of Fingerprint image String lines (Normal & Encrypted)



```
Normal Finger Print Image String =  Squeezed text (1739 lines).

Encrpted Finger Print Image String =  Squeezed text (2320 lines).

Decrypted Finger Print Image String =  Squeezed text (1739 lines).
```

Fig.2. (c) Snapshot of Fingerprint image String lines (Encrypted & Decrypted)

At the time of Registration the user is supposed to provide a unique ID which is his/her username and with this username Biometric traits are considered as password for the sytem. Here Fingerprint scanning is being considered as Biometric trait. At the time of Registration, meanwhile the Biometric trait i.e Fingerprint traits are being Encrypted at user side which is then after stored in database in encrypted format. The Normal Fingerprint Image is of String Format, which is being encrypted and stored in the Database. The Encrypted Fingerprint Image String is of more number of lines compared to Normal Fingerprint Image String. Thereafter when user tries to login into system, he/she provides username and fingerprint as password then with the help of username, the encrypted image fingerprint String is being fetched from database and it gets decrypted at the user side and squeezed text of particular no. of lines(similar number as of Normal Fingerprint Image String) is obtained which gets compared and if similarities are identified then user gets authenticated and gets access to the system.

Following is the analysis of some minutiae patterns:

- Ridge ending is a point where the ridge ends.
- Ridge bifurcation means where the single ridge branches out into two or more ridges.
- Ridge dots are nothing but the small ridges.
- Ridge islands are little longer than dots and occupy the central space between two ridges.
- Ponds or Lakes are nothing but the empty space between ridges.
- Bridges as the name suggest it join two longer adjacent ridges.
- Crossovers are created when two ridges crosses each other.

The most commonly used minutia types are ridge endings and ridge bifurcations as all the other minutiae are based on the combination of the above two ridges. Following figure shows some of the common minutiae patterns.

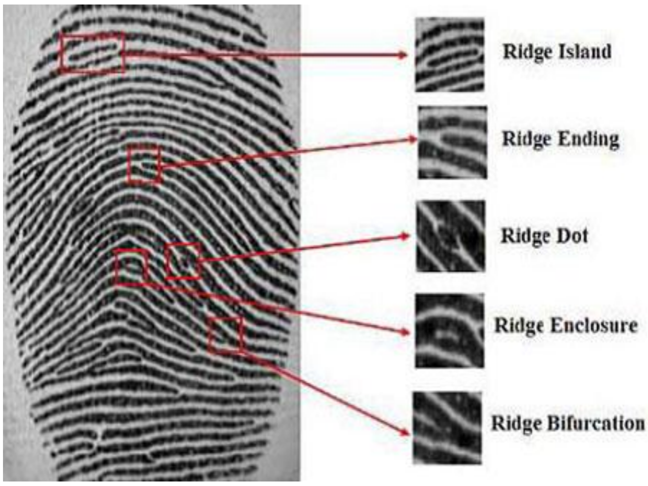


Fig.2. (d) Some minutiae patterns

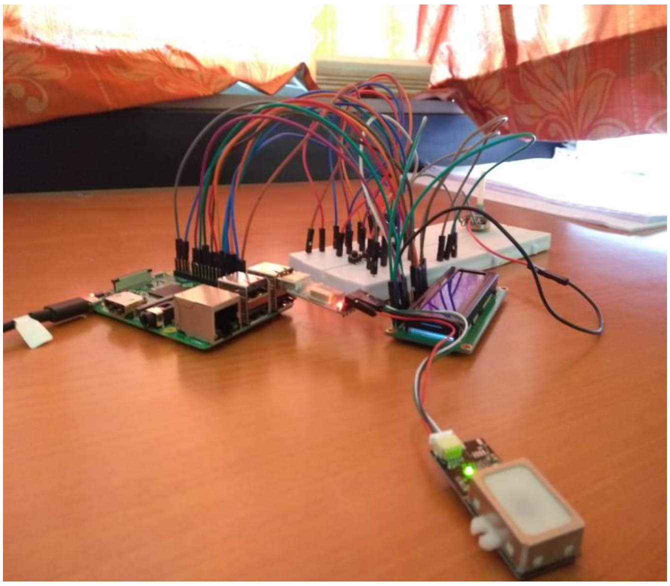


Fig.2. (e) Setup to take fingerprint from user using raspberry pi

VI. Conclusion and Future Scope

This proposed system gives better results when compared to the earlier existing systems. With rising computing power, existing algorithms were considered weak against extensive key search attack. In this project we proposed an Advanced Encryption Standard (AES) scheme. Based on AES we proposed User Centric Biometric Authentication. One key feature is that in this the end-user himself can encrypt their own biometric template and register it to the service provider. Such a computational model can be widely used in much application requiring computation on encrypted data while preserving the data security and privacy.

References

[1]. Author A.k. Jain Nandakumar and A. Ross “50 years of biometric research : Accomplishments,challeges,and opportunities.” Pattern Recognition Letters Vol.79 pp. 80-105.Elsevier 2016.

[2]. A.K. Jain and K .Nandakumar, “Biometric Authentication : System Security User Privacy.” IEEE Computer . Vol 45 no .11. pp 87-91. IEEE 2012.

[3]. S.Rane, Y.Wang S.C. Draper , and P.Ishwar , “Secure biometric : concepts ,authentication architecture , and challenges,” IEEE signal processing Magazine vol. 30. No. 51-64 , IEEE 2013.

[4]. M. Naehrig, K. Lauter, and V. Vaikuntnathan, “Can homomorphic encryption be practical?.” in proceedings of the 3rd ACM workshop on Cloud Computing Security Workshop, pp 113-124, ACM, 2011.

[5]. J. Katz, A. Sahai, and B. Waters, “Predicate encryption supporting disjunction, polynomial equations, and inner products.” In Advances in Cryptology-EUROCRYPT 2008, pp. 457-473, Springer, 2009.

[6]. N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “Generating cancelable fingerprint templates,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 561–572, 2007.

[7]. Michael Bourg, Pramod Govindan “RSA based biometric encryption system using FPGA for increased security” , International Carnanan Conference on Security Technology (ICCST), Orlando, FL, USA, 2016.

[8]. Terry Ferrett, Veeru Talreja, Arun Ross, “Biometrics-as-a-service: A framework to promote innovative biometric recognition in the

cloud", IEEE, 2017.

[9]. Palvi Sharma , Manit Kapoor , Dr. Naveen Dhillon, "Design of Biometric Authentication System using Three Basic Human Traits", International Journal of Science and Research (IJSR), 2016.

[10]. N. Jagadeesh , Chandrashekhar M. Patil, "Development of a New Methodology for iris algorithm in Biometric authentication using Hamming Distance concepts", International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Brinzel Rodrigues. "Encryption and Decryption of Biometric Traits." IOSR Journal of Computer Engineering (IOSR-JCE) 21.2 (2019): 06-12.