ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Multimodal biometric based authentication for ensuring data security in Cloud Computing

Teena Joseph[1*] and Latha Parthiban[2]
[1]Department of Computer Science & Engineering, St Peter's University, Tamilnadu, India. Email
[2]Department of Computer Science & Engineering, Pondicherry University Community College, Puducherry, India.
***Corresponding author: E-Mail: tinaajo85@gmail.com**

ABSTRACT

Biometrics is a technique of using the unique characteristics of individual for identification purpose. Multimodal biometrics has come to existence as single trait is not adequate and hybridization of cryptography and biometrics for generating cryptographic key has gained much reputation as it improves security. In this paper, a novel algorithm, which involves generation of secure biometric key with the help of multi modal biometric characteristics (Iris, Fingerprint and Palm print) as the key cannot be guessed by an at tracker is proposed. The approach introduced helps to provide better security and follows process of authentication in an effective e-manner.

KEY WORDS: Cloud storage, multimodal, biometrics, authentication.

I. INTRODUCTION

Cloud computing is the next generation architecture of IT enterprise with huge advantages like ubiquitous network access and usage based pricing. An important concern with remote data storage is data security of untrusted servers. With huge size of outsourced electronic data and client's constrained resource capability, the main problem is to find the best way to accomplish periodical data security without maintaining local copy of data files. In order to follow secure authentication and authorization of user, the field of biometrics was introduced. Biometrics is the field which involves usage of physiological/ behavioral and biological characteristics in order to identify an individual. The distinguishing character is tic information's like Iris, Ear, Fingerprint, and Palm print, Face, Gait, Pulse-rate, and Voice etc. are known as biometric traits. Biometric systems which uses single biometric trait at any given instance have limitations like uniqueness, high error rate, non-universality and noise. Later, these limitations were reduced by multimodal biometrics. With the advancement of technology transition from uni modal biometric (one single trait at a given instance) to multimodal biometric systems, (combinations of two or more traits) has been observed in order to enhance the security level.

2. MATERIALS AND METHODS

Proposed Architecture: The multi modal biometric system designed consists of five modules as in figure 1.

- Fingerprint analysis module.
- Iris analysis module.
- Palm print analysis module.
- Conversion and Fusion.
- Encryption/Decryption module.

Generation of secure biometric keys with the help of multi-modal biometrics such as iris, fingerprint and palm print is done as shown in figure 1.

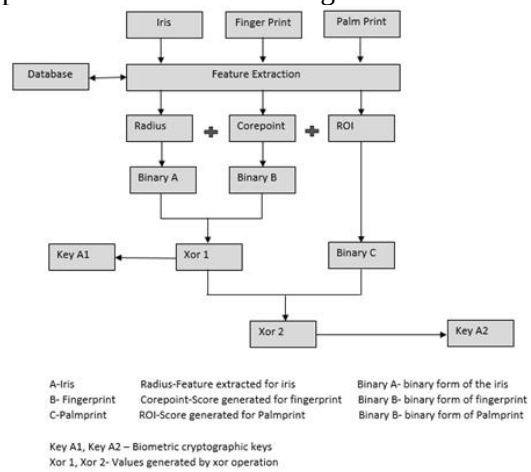


Figure.1. Generation of Secure biometric keys

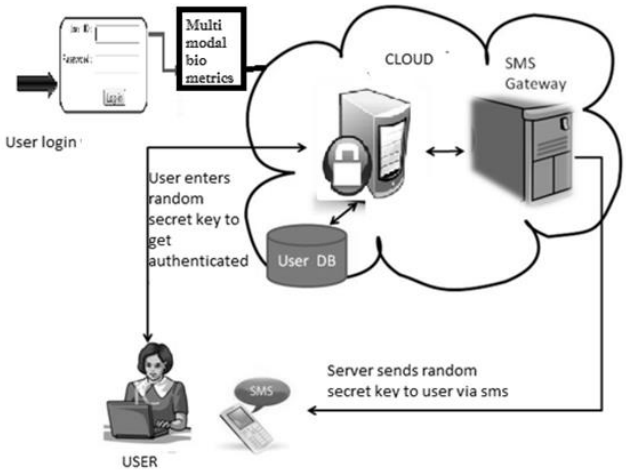


Figure.2. Multifactor Authentication in Cloud

Multi modal biometric authentication, in addition to username and password can be used to increase the security level, when the data accessed from cloud is sensitive. User ID and password shows what user know, fingerprint, Iris and Palm print biometric represents what the user are, and random secret keys are used for verifying user identity to server as shown in figure 2.

After the user is authenticated, he can upload the file which is encrypted with AES-256, which is converted to binary. This binary data with key is stored in cloud. The user can set time for self-destruction and share the data to friends. The user can access the encrypted data from cloud and decrypts with his private key as shown in figure 3.

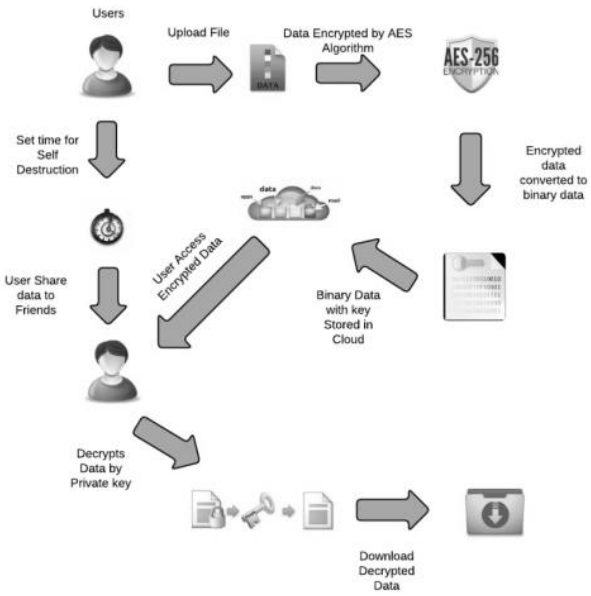


Figure.3.Secure file upload and download from cloud

Module Implementation: The minutiae points are extracted from fingerprint image, texture features from iris image and ROI score from palm print are generated. The features are now converted into respective decimals. The decimals are converted into binaries and all the three binary follows XOR operation to generate combined cryptographic key. The key is later compressed to Hexadecimal value which can act as encryption key. The encryption key is now used for AES encryption and decryption process. Again double encryption and decryption is followed based on the two ciphers generated

Module 1: Biometrics Sensing

This module helps to recognize the biometric information of the users via sensors.

- Images are generated which are further passed to module two for evaluation.
- The Module helps to collect the information of human biometrics
- The information to be collected are- Fingerprint, Palm print, Iris.

Module 2: Pre-processing -Feature Extraction Description

- It helps to extracts the features from human biometrics in order to generate biometric key
- The features are extracted in form of decimals which are then used to convert binary value
- Different techniques are followed for each biometric
- At first the image is enhanced, followed by thinning, segmentation.

Module 3: Normalization and Fusion Description

- This module helps to normalize the data or information gathered in form of features to the type which can be used to create or generate key.
- The features are then fused by following the x or operation of the biometric values obtained.

Module 4: Generation of Keys Description

- The above module and the current one are integrated to generate binary zed biometric ciphers
- The two binary keys generated are then considered as input to next module of encryption.

Module 5: Encryption and Decryption Description

- The module follows the process of encryption and decryption by incorporation AES encryption process.
- The binary keys generated from the above module are passed as inputs to generate encrypted ciphers.

3. RESULTS AND DISCUSSION

Analysis of about 7 different samples is followed and detailed evaluation can be seen from the table 1. Iris Shift Features are extracted and kept as constant throughout the analysis. All the features are extracted and normalized in form of binary values which later follows the proposed algorithm. All the values are made as input to the web application tool developed and respective results are observed. Few cases are rejected with 0.1% probability. □K1 represents the Biometric Cipher key 1 and □K2 represents the Biometric Cipher key 2.

The proposed technique provides better security due to 3 levels of multimodal biometrics. This paper combines the scores based on fusion of Iris, Fingerprint and Palm print data to generate biometric cryptographic keys. The analysis done provides information about the performance and estimate measures of the combined (proposed) biometric techniques. The Iris, Fingerprint and Palm print data are collected from about 70 individuals and used for evaluation. Scores for each biometric traits are generated respectively. The calculation of analysis parameters such as FAR, FRR are estimated.

The biometrics features for Iris, Fingerprint and Palm print are collected separately. Then, scores are obtained followed by the fusion technique discussed. FAR is False Acceptance Rate as presented in Table 2 and FRR is False Rejection Rate as presented in Table 3 . Figure 4 and 5 provides the comparative analysis of FAR and FRR.

Table.1. Multimodal biometric results of samples analyzed

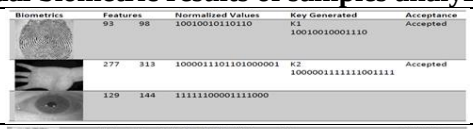
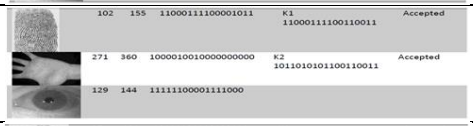
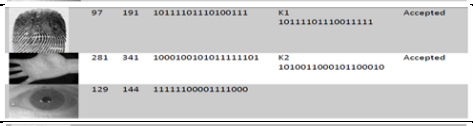
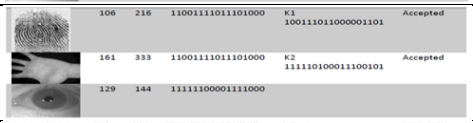
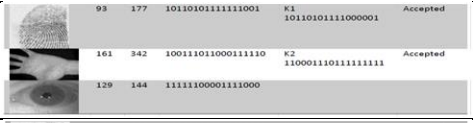
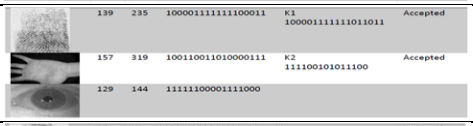
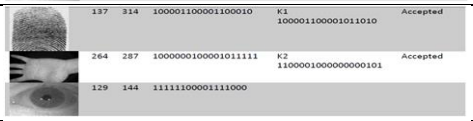
Sample 1		
Sample2		
Sample 3		
Sample 4		
Sample 5		
Sample 6		
Sample 7		

Table.2. False Acceptance Rate Analysis

User	Iris	Finger print	Palm print	Combination (All three)
1 – 10	0. 40	0. 44	0. 35	0. 12
11 – 20	0. 37	0. 43	0. 34	0. 13
21 – 30	0. 38	0. 42	0. 33	0. 09
31 – 40	0. 39	0. 47	0. 31	0. 10
41 – 50	0. 39	0. 48	0. 29	0. 08
51 – 60	0. 38	0. 41	0. 33	0. 03
61 – 70	0. 40	0. 45	0. 36	0. 11

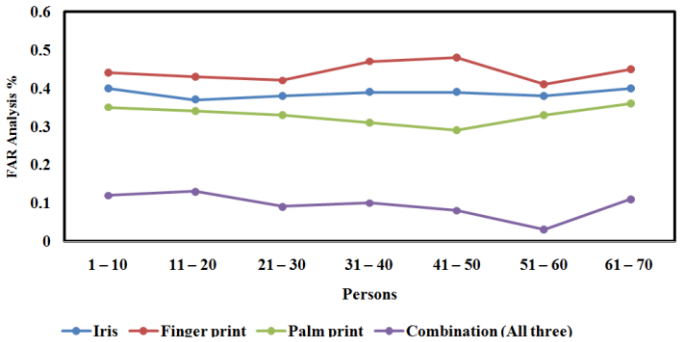


Figure.4. Comparative analysis of FAR (False Acceptance Rate) %

Table.3. False Rejection Rate Analysis

User	Iris	Finger print	Palm print	Combination (All three)
1 – 10	88. 3	91. 5	87. 8	85. 5
11 – 20	88. 5	91. 1	87. 3	84. 7
21 – 30	88. 7	92. 7	88. 1	86. 2
31 – 40	91. 4	93. 4	89. 6	84. 3
41 – 50	90. 6	91. 3	88. 8	83. 6
51 – 60	90. 3	91. 6	89. 2	84. 3
61 – 70	89. 2	92. 3	88. 5	85. 3

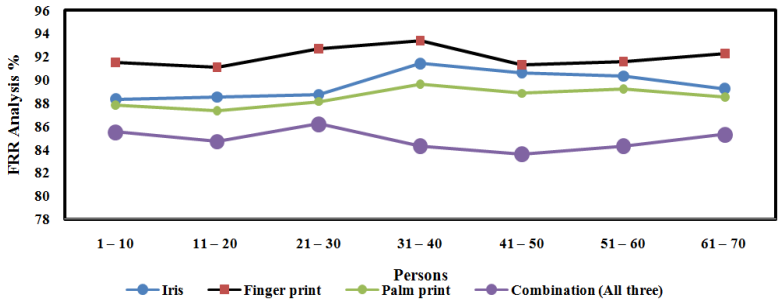


Figure. 5. Comparative analysis of FRR (False Rejection Rate) %

4. CONCLUSIONS

Security plays a vital role for various systems which are used by everyone on a daily basis. Biometrics recognizes the problems associated with security. It provides enhanced security by incorporation of various human behavioral features such as Iris, Fingerprint, Palm print, Voice, facial structure etc. Problems associated with bio metrics includes non-revocability and privacy compromise. Such problems are overcome by introduction to multi-modal biometrics which involves combination of two or more biometric features to strengthen the existing security. Combining complementary characteristics of biometrics and cryptographic systems provides much more secure systems as it addresses individual issues and helps to produce a more efficient system. This paper proposes an algorithm for generating biometric key using more than two biometrics. The biometric key is generated with the three level fusion which is not observed till now. Based on the analysis done, the experimental result shows that proposed technique is better and reliable as well as more secure due to involvement of three levels of biometrics.

REFERENCES

Arun A, Ross, Karthik Nanda Kumar and Anil K Jain, Handbook of Multi bio metrics, International Series on Biometrics, 2006.

Rinesh S & Mohanapriya M, Secure and Efficient Data Sharing in Cloud Using Hybrid Patient Controlled Biometric Encryption Scheme, IJCTA, 8(4), 2015, 1587-1596.

Shalaka K Saboo, Prof. Amit Zore, A Survey on Multimodal Security Mechanism Using Embedded System & Cloud Computing, International Journal of Innovative Research in Computer and Communication Engineering, 3(12), 2015, 12828-31.

Ziyad S and Rehman S, Critical Review of Authentication Mechanisms in Cloud Computing IJCSI International Journal of Computer Science Issues, 11(3), 2014, 145-149.