ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(34), DOI: 10.17485/ijst/2016/v9i34/86374, September 2016* ISSN (Online) : 0974-5645

Data Security in Cloud using Multi Modal Biocryptographic Authentication

P. Selvarani* and N. Malarvizhi

Department of CSE, Vel Tech University, Avadi, Chennai – 600062, Tamilnadu, India;
selvarani.meena@gmail.com, drnmalarvizhi@gmail.com

Abstract

Objectives: Higher data security can be achieved by using Multimodal bio cryptographic technique for data encryption and decryption to avoid the intruders to access the data. **Methods:** Iris and fingerprint are used as a key for both data encryption and decryption in Multimodal biometric based blowfish algorithm. The data stored in cloud environment after encryption. **Findings:** The problem with storing the data in cloud environment using password system is, it is not secured, forgotten and easily stolen. Hackers can able to trace the password through keystroke loggers and spyware. In multi-model biometric system it is not possible to hack the data by the intruders. For both data decryption and encryption blowfish algorithm is used. Combined biometric of both fingerprint and iris uses as a secret key for a blowfish algorithm. **Applications:** To run the middleware for connecting the cloud system no need of advanced hardware system. High data security is enough.

Keywords: Cloud Data Security, Data Decryption, Data Encryption, Fingerprint Recognition, Iris Recognition, Multimodal Biometrics

1. Introduction

Storing information in cloud computing is cost effective. But security is the concern in storing the data in cloud. Authorized owners are losing billions of dollars due to illegal activities like sharing copying of digital data in cloud. So it is very essential to protect the data in cloud from unauthorized users[1]. To overcome these difficulties cryptography is used for encryption and decryption. The password based authentication system is unsecure because, if the password is chosen easily it is easy to guess and if the password is chosen very complex it is very hard to remember. To overcome these difficulties biometric system is used for encryption and decryption[2]. Biometric system cannot be forgotten or easily stolen. Biometric authentication is more powerful and it is alternative for traditional existing system. In the proposed system multimodal biometric is used for authentication in cloud storage[3].

1.1 Organization of the Paper

The remaining part of this paper is organized as follows: Section 2 describes the related work. Section 3 describes the problem statement. Section 4 describes the proposed work. Sections 5 discuss the results and analysis. Section 6 provides the conclusion analysis and the future scope of the work.

2. Related Work

P. Selvarani et.al.[4] proposed data security in cloud environment. To increase the data security in the cloud environment Multimodal biometric technique can be used. The plain text information is transferred to cipher text using encryption technique and original message can be retrieved from the cloud using decryption technique.

M. Rohit et.al.[5] proposed two techniques based on the watermarking which is mingled with the Cloud Security theory for authentication and the protection for the biometric system. They have suggested the techniques with watermarking which provides security at system database with biometric against stolen and spoofing attacks. Here the result shows that these technique performance authentications are not efficient. This paper

* *Author for correspondence*

merges the watermarking technique with the compressive sensing theory for the security of multi biometric data.

Saminathan K. et.al.[6] proposed work hold up for Iris Recognition based on Hamming Distance and Multi Block Local Binary Pattern. This paper considered experiments based on support vending machine and hamming distance with multiple block of binary pattern were applied and verified. The results were obtained with high performance of 0% of FAR and 97.5% of accuracy. This presented work is advisable for both authentication and identification.

Koteeswaran S. et.al.[7] proposed job sequence was enhanced by improving the scheme of schedule in the YARN. The data were handled more accurately by the active scheduling scheme.

M. A. Velciu et.al.[8] proposed a new implementation which includes the infrastructure of a bio-cryptographic for the safer authentication method in the cloud storage. This work implements a fuzzy vault authentication mechanism based on voice, for encryption support and safe access within cloud storage sharing and cloud platform.

Mahalakshmi U. et.al.[9] proposed the method of ECC. In ECC selected portion of multi biometric image is fused into single image. One time password is appended for high authentication to the system. This system implements the ECC and OTP methodologies to maintain a high level authentication. This system promotes the efficiency and accuracy rate in authentication.

Mohammad Abdolahi et.al.[10] the problem of single biometric spoof attack due to noise is unacceptable error rate can be solved by multimodal biometric system. In multimodal biometric system the recognition accuracy is more than unimodal. The decision was taken by the fusion of both fingerprint and Iris biometrics system.

Rupesh Wagh et.al.[11] proposed the characteristics of both fingerprint and Iris were used in multimodal biometric system. The features taken from biometric template were stored in fusion of feature level. After fusion then it is encrypted using different security technologies. Authors look biometric sample from virtual database and real database. In the experimental result it was proved the accuracy of multimodal biometric is higher than unimodal biometric system.

R. N. Kankrale et.al.[12] proposed the biometric features such as Iris and fingerprint were combined at decision level with fuzzy logic. To minimize the false acceptance rate as well as two or more physical traits were conducted using multimodal biometric system. Then the biometric result is weighted in final decision. Fuzzy logic is used for the biometric combination.

Radha N. et.al.[13] proposed the biometric multimodal system using fingerprint and iris. They use Fisher Linear Discriminant and Principal Component Analysis (PCA) methodology for biometric recognition. This paper presents the difference between the logistic regression methods and borda count method. From the comparison results that the logistic regression approach with the rank-level fusion and recognition rate were increased and error rate were decreased in Multibiometric system.

S. Sumathi et.al.[14] proposed the multi biometric authentication using Discrete Wavelet Transform (DWT). A new novel technique based on DWT for identification of user. It utilizes support vector machine for the absolute result, the efficiency of the design is analyzed in terms of Genuine Acceptance Rate and False Acceptance Rate.

Bhawna Chouhan[15] proposed the Image segmentation and feature extraction were focused in Iris recognition process. The performance depends on edge detection. Canny edge detector is used as a image processing tool.

Xi K. and Hu J.[16] introduction to Bio cryptography Book. Bio cryptography can implement the below listed modes: key generation, key binding and key release: 1. Key Generation: The key which was not being stored in database is derived from the biometric data, 2. Key binding: Here the template and the key are combined within a cryptographic framework, 3. Key Release: Biometric authentication is totally decoupled from the mechanism of key release. The key and the biometric features are stored separated, if the matching process result is successfully then only the key will be released.

Bo Fu et.al.[17] proposed a mechanism of multi biometric cryptosystem by binding the multiple features of biometrics to cryptography there are 2 levels of combining i.e. combining at the biometric level and cryptographic level.

Besbes F. et.al.[18] proposed Fingerprint and IRIS features were used in multimodal biometric system. This approach is based on Iris encoding and fingerprint minutia extraction through mathematical representation of extracted region of IRIS.

3. Problem Statement

The main obvious concern is for privacy considerations

another person can be able to access all your data within cloud data storage. In a cloud environment a person should not gain another person's data. Data should be invisible to all tenants except owner Authentication mechanism should be implemented to make sure no cloud tenant can assume the identity of another tenant. No user should be able to delete belonging to another person's data. One of the modern approaches for upgrading cryptographic security is to add biometric system to enhance the data security in cloud environment. The main disadvantageous of password are it can be easily stolen and forgotten. Intruder can able to trace the passwords by using spyware and keystroke logger. The passwords are rarely changed by some of the user. Due to the infrequent changes of password it is not only sufficient to secure the data. Therefore biometric parameters are used in combination with the password to secure the data in cloud environment.

4. Proposed Work

To overcome this difficulty in the proposed system to use multimodal biometric system like fingerprint, iris and secret key for generating key for blowfish algorithm. This paper proposes a implementation of multimodal biometric system in cloud. Here Finger and iris biometric technology is used. Biometric based Blowfish algorithm can be used for the decryption and the encryption can be executed to embellish security framework over the network.

4.1 Data Encryption in Cloud

Figures 1, 2 show the block diagram of Data Encryption and Decryption in Cloud Environment.

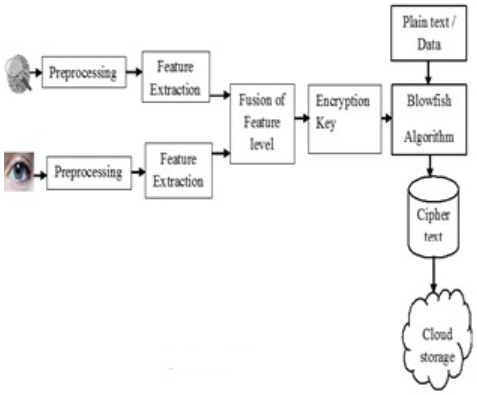

Figure 1. Data encryption in cloud.

In the First stage preprocessing and feature extraction is to be applied for the each image of biometric system. In the Second Stage fusion of feature level is used for both Iris and Fingerprint as a encryption key for biometric based blowfish algorithm. Finally after conversion of Plain text to Cipher text is stored in cloud environment. The Cipher text could not be able to read by the intruders.

4.2 Data Decryption in Cloud

The cloud data is accessed by the owner by using secret key which is a combination of Iris and Fingerprint. The original message can be retrieved by the user after decryption.

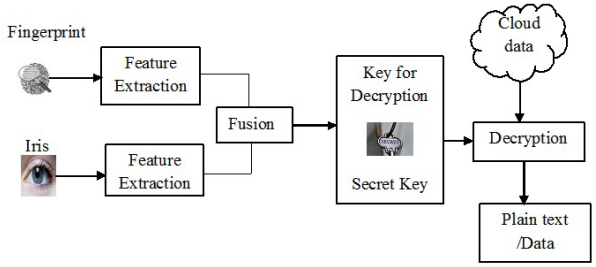

Figure 2. Data decryption in cloud.

- **Blow Fish Encryption Algorithm**

Blowfish was designed by Bruce Schenier and it is included in a huge number of cipher suites and encryption products. Same key is applied for both decryption and encryption. Figure 3 shows the Block diagram of Blowfish algorithm. The algorithm contains variable key length with 64 bit block cipher. This algorithm has been used because it requires less memory and it is easy to implement. There are 2 Parts of algorithm. They are expansion of key and encryption of data.

- **Blow fish Key Expansion**

Original key is divided into a set of sub keys. Each block consists of 448 bit key. It consist of 32 bit S-Boxes and P-Array. P-array is having 18 numbers of 32 bit sub keys; Each S-Box is having 256 entries.

- **Blowfish Encryption**

T[i] indicates 64 bit input and P[i] indicates P-array (i-iteration) it.

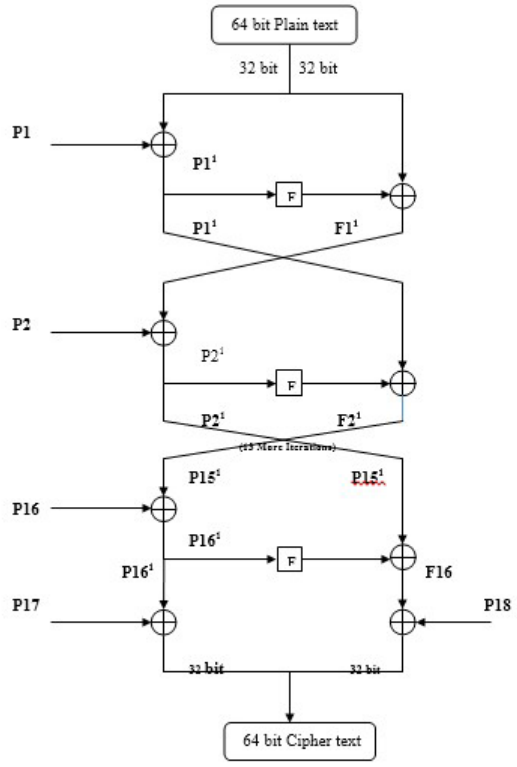

Figure 3. Blow fish algorithm.

4.4 Blowfish Algorithm

Encryption:

This algorithm has 16 Iterations.

The Input text is divided into block size of 64 bits.

Split the 64 bit block sizes into 32 bits. TIL (Text Input Left) and TIR. (Text Input Right)

Start: Initialize variable I=0.

TIL = TIL XOR with P [i]

TIR= Fun [TIL] XOR with TIR

Swap TIR and TIL

Repeat the Iteration and go to start location for until 16 Iterations are completed.

After 16th Iteration

Swap TIL and TIR.

Then Right Input [TIR] XOR with P [17]

And Left Input TIL XOR with P [18]

Then Recombined

Decryption:

Decryption is the reverse process of encryption. The only the difference is in P-array.

The P-array is in reverse order in decryption like P[18], P [17]… P [1].

4.5 Design Feature Of Blowfish Algorithm

Table 1 shows design feature of biometric based blowfish algorithm. Blowfish is a symmetric block cipher key. (Here a single key is used for both the data decryption and the data encryption).

Table 1. Design feature of blowfish algorithm

Platform	Cloud Computing	Scalability	Scalable
Designed	1993	Key used	Same key is used for both data encryption and data decryption.
Author	Bruce Schenier	Usage	Unpatented, License free and it's available for all users. Symmetric Block cipher is used for encryption.
Block Size	64 bit	Two Parts of the algorithm	Expansion of Key and Encryption of Data
Variable Key Length	32-448 bits	Execution time	Lesser time to execute and reduce the time for data encryption and decryption
No of rounds	16	Authentication type	Comparable to AES
Encryption	More than 2^{32} data blocks	Utilization	Replacement for IDEA/DES.
Memory usage	4 KB of data can be processed	Security	Secure for both cloud provider & user/Client side.
Initial vector size	64 bits	Encoding	CBC
Network	Feistel	Comparable to other algorithm	It is significantly faster than DES. Very fast, Highly secure.
Possible keys	2^{32}-2^{448}	Attack	No Attack
Speed	Very fast	Padding	PKC55
Modes	CBC,ECB	Performance	High

5. Results and Discussion

By using multimodal biometric, like fingerprint, iris and secret key used to protect the data from unauthorized

user. So the intruder cannot able to access the cloud storage data. Only authorized person is allowed to access the corresponding cloud data. Higher accuracy and more security have been provided by using fingerprint and iris. The total time taken for both decryption and encryption in the blowfish algorithm using multimodal biometric technique is very much reduced. Strong Authentication can be provided to restrict the unauthorized person to access the cloud storage data.

Table 2, 3 and 4 describes the encryption and decryption process of our results.

Table 2. Encryption and decryption process of our result (input1)

Plain text message string is	Biometric Based Blowfish algorithm
Key	Cloud Computing
Encrypted message String is	C33e0bc8601f2ec0d4cfe-1758ecd9a3b928a4e414b-cb131fb0906c68ecc73d-4144f9acb46c368
Decrypted message String is	Biometric Based Blowfish algorithm

Table 3. Encryption and decryption process of our result (input 2)

Plain text message string is	Biometric Based Blowfish Algorithm
Key	Data security
Encrypted message string is	165a2d-14ce31e2e8f7350e3144f507f-deabe649384ba63b-c0c33d3a29ce0c-cefd123571781f5649
Decrypted message string is	Biometric Based Blowfish Algorithm

Table 4. Encryption and decryption process of our result (input 3)

Plain text message string is	Fingerprint and iris based data encryption
Key	F986e745a4b31d2c
Encrypted message string is	de9f43fc5fd2140c7f9c-b6cfefea8598a29e6b-7909006c8cfeaf35193b57d-312362ba2cf970be-f7e0eb695469149d
Decrypted message string is	Fingerprint and iris based data encryption

6. Conclusion and Future Enhancement

Fingerprint and Iris are used as a secret key for biometric based blowfish algorithm for storing the data in cloud environment. Security algorithms considered for advanced decryption and encryption can be implemented in future to enhance security over the cloud computing. In the future, will prolong our research by providing algorithm implementations to legitimate our concepts of security for the cloud computing.

7. References

1. Jain A, Ross A, Pankanti S. Biometrics: A Tool for Information Security. IEEE Transactions on Information Forensics and Security. 2006 June; 1(2):125–43.
2. Stallings W. Cryptography and Network Security: Principles and Practices, 3rd ed. Upper Saddle River, NJ: Prentice-Hall, 2003, Guest Editorial, S. Pankanti, R. Bolle, A. K. Jain (Guest Editors) Special Issue of IEEE Computer on Biometrics, Feb. 2000.
3. Jain A, Ross A, Prabhakar S. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology. Special Issue on Image and Video Based Biometrics. 2004 Jan; 14(1):4–20.
4. Selvarani P, Visu P. Multi-model Bio-cryptographic Authentication in Cloud Storage Sharing for Higher Security. Maxwell Scientific Organization. 2015 Sep; 10(1):95-101.
5. Rohit M. Thanki, Komal R. Borisagar. Experimental Study of Sparse Watermarking Techniques for Multibiometric System. Indian Journal of Science and Technology, 2015 Jan; 8(1):42-48.
6. Saminathan K, Chakravarthy T, ChithraDevi M. Comparative Study on Biometric Iris Recognition based on Hamming Distance and Multi Block Local Binary Pattern. Indian Journal of Science and Technology. 2015 Jun; 8(11):1-8.
7. Koteeswaran S, Visu P, Kannan E. Enhancing JS– MR Based Data Visualisation using YARN. Indian Journal of Science and Technology. 2015; 8(11):1-11.
8. Velciu MA, Patrascu.A, Patriciu VV. Biocryptographic authentication in cloud storage sharing. Proceeding of the 9th IEEE International Symposium on Applied Computational Intelligence and Informatics, 2014, 165-70.
9. Mahalakshmi U, Shankar Sriram VS. An ECC Based Multibiometric System for Enhancing Security. Indian Journal of Science and Technology. 2013 Apr; 6(4):4299-305
10. Mohammad Abdolahi, Majid Mohamadi, Mehdi Jafari. Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic. International Journal of Soft Computing and Engineering (IJSCE). 2013 Jan; 2(6):504-10.

11. Rupesh Wagh, Arati P. Choudhary. Analysis of Multimodal Biometrics with Security Key. International Journal of Advanced Research in Computer Science and Software Engineering. 2013 Aug; 3(8):1363-1365.
12. Kankrale RN, Jawale MA. Fuzzy Logic Concatenation in Fingerprint and Iris Multimodal Biometric Identification System. International Journal of Advanced Research in Computer Science and Software Engineering. 2013 Oct; 3(10):120-126.
13. Radha.N, Kavitha A. Rank Level Fusion Using Fingerprint and Iris Biometrics. Indian Journal of Computer Science and Engineering (IJCSE). 2012; 2(6):917-23.
14. Sumathi S, Rani Hemamalini R. Multibiometric authentication, using DWT and score level fusion. European Journal of Scientific Research. 2012; 80(2):213-23.
15. Bhawna Chouhan, Shailja shukla. Iris Recognition System using canny edge detection for Biometric Identification. International Journal of engineering Sciences and Technology (IJEST). 2011 Jan; 3(1):155-167.
16. Xi K, Hu J. Introduction to Bio-Cryptography. In: Bio-Cryptography Handbook of Information and Communication Security. Springer 2010.
17. Bo Fu, Simon X. Yang, Senior Member, IEEE, Jianping Li, Dekun Hu. Multi biometric Cryptosystem: Model structure and performance analysis. IEEE Transactions on Information Forensics and Security. 2009 Dec; 4(4):867-82.
18. Besbes F, Trichili H, Solaiman B, Multimodal biometric system based on Fingerprint identification and Iris recognition, In: Proceeding 3rd International IEEE Conference on Information Communications Technologies: From Theory to Applications (ICTTA 2008), Damascus, 2008, 1–5.