Research Journal of Applied Sciences, Engineering and Technology 11(1): 95-101, 2015
DOI: 10.19026/rjaset.11.1680
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: March 7, 2015 Accepted: April 13, 2015 Published: September 05, 2015

Research Article

Multi-model Bio-cryptographic Authentication in Cloud Storage Sharing for Higher Security

P. Selvarani and P. Visu
Department of CSE, Vel Tech University, Avadi, Chennai-62, Tamil Nadu, India

Abstract: To achieve data storage security in cloud, bio cryptography techniques can be used. This study presents Personal identification using fingerprint and Iris biometric technology. Usually unimodal biometric techniques are used. Cloud computing provides many resources, very convenient charged service and minimum cost computing. This leads the cloud computing to become the most dominant computing in the recent years. Even though the cloud provide secured service, it also undergoes with some security problem especially form hackers. The existing unimodal bio cryptography techniques often have limitations such as consciousness to noise, intra class consistency, data aspect and other factors. This research study presents personal identification using fingerprint, iris and cryptographic technologies. Combined biometric technology will secure the data from unauthorized users. The purpose of this study is to study the combination of fingerprint and iris and also to include the cryptographic methods to achieve the higher accuracy and more security. The result of this study can overcome some of the limitations of using single biometric technology. The combination of Finger print and Iris form the key for Blowfish algorithm to store the secured data from unauthorized users in cloud environment.

Keywords: Cloud security, fingerprint recognition, iris recognition, multimodal biometric

INTRODUCTION

C.L.O.U.D (Communities and Libraries Online Union Database): Cloud Computing is an internet based computing which relies on distributing computing resources instead of having local servers or personal devices to hold the applications. Cloud is used because of reduction of Cost, We Can use Anytime, Anywhere, Any Device Access, Ease of Collaboration, Elastic computing, Improve Efficiency, Pay as you use, Reliable, Scalable, Higher security, Better functionality, Higher flexibility, Less Complexity etc.

Cryptography: Cryptography is used to encrypt information from plain text to cipher text to ensure the data security. The original message is converted to ciphertext usina an encryption key and to retrieve back decryption key is used. The encryption process is explained in the Fig. 1.

It consists three types of algorithms: Symmetric key algorithm, Asymmetric key algorithm and Hashing Table 1.

Biometrics: The programmed use of psychological and Behavioral characteristics to determine an identity. There are 2 types of Biometric technology Single modal biometric and Multimodal biometric technology. In the Single modal Biometric System they use only one biometric sample to recognize a user (iris, fingerprint, retina scanner, face, palm) any one of them used. In the Multimodal Biometric System use 2 or more biometric sample from the same person in order to identify him/her.

Types of biometric technology: Figure 1 shows types of biometric technology. There are 2 types of Biometric Features. Behavioral features and psychological features. In behavioral features like fingerprint, Iris, Hand Geometry and facial recognition. In Psychological features like Voice and Hand written signatures.

Levels of fusion: Sakshi and Anil (2014) was presented in the information of the multimodal system can be fused at any of the four model.

Fusion at the sensor level: In this model different sensors are fused from the raw data.

Fusion at the feature extraction level: The data from the multiple sensors or sources are fused together. Feature vector is formed by extracting feature from each sensor. A single new vector is formed by concatenating feature vector. We can use same feature extraction algorithm or different feature extraction algorithm on different modalities whose feature has to be fused.

Corresponding Author: P. Selvarani, Department of CSE, Vel Tech University, Avadi, Chennai-62, Tamil Nadu, India

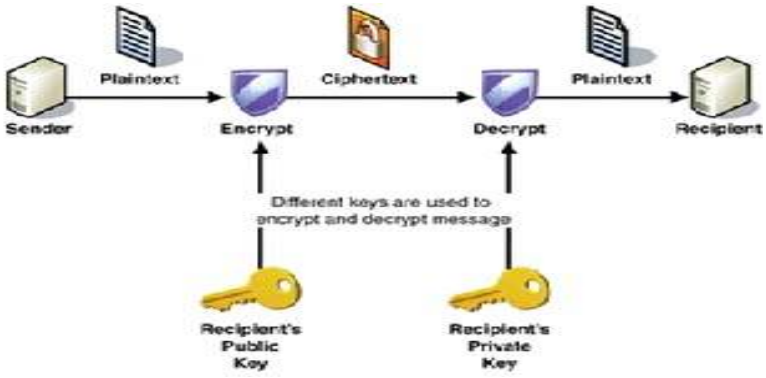

Fig. 1: Cryptography technique

Table 1: Symmetric key algorithm vs. asymmetric key algorithm

Symmetric-key algorithm	Asymmetric key algorithm
Same key is used for both encryption and decryption.	Different key is used for both encryption and decryption. The 2 keys are private key and public key
Symmetric key algorithm is divided into 2 types. Block cipher and Stream cipher.	Public key: used by the sender for encryption
Block cipher: The size of the block cipher consist of block of text and it is taken from standard input.	Private key: used by the receiver for decryption
Stream cipher: One bit at a time in stream cipher is encrypted.	
Symmetric key algorithm used in cloud computing are DES, triple DES, AES and blowfish algorithm	Asymmetric key algorithm used in cloud computing are: homomorphic encryption, RSA, IKE and Diffie-Helman key exchange

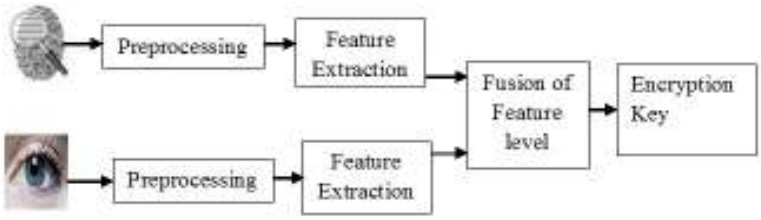

Fig. 2: Multibiometric system

Matcher score level: Each system provides a matching score indicating the proximity of the feature vector with the template vector. Normalization technique is followed to map the scores obtained from different matches on the same range.

Fusion at the decision level: The final output of the multiple classifiers are combined.

A majority vote scheme can be used to make final decision. Biometric system that integrate information at the early stages are more effective than those in which integration is done in later stage.

Multi biometric system: Figure 2 shows the multimodal biometric system. Initially we apply preprocessing for feature extraction from each biometric image. Then the fusion of feature level both fingerprint and iris are used for encryption (Sakshi and Anil, 2014).

Bio-cryptography: Biometric encryption is a process that securely bind a digital key to a biometric. Biometric authentication is used as cryptographic key instead of passcode. When a user is ready to access a secured key, they will be allow to capture the biometric sample. If the verification sample is matches with registration template then only the key is released and it is used for data encryption (or) decryption. The biometric authentication key can be used to protect the passcode. This provides users no longer have to remember a passcode and secure identity confirmation. Only the valid user can release the key with the increasing demand of information exchange across the internet and the storage of sensitive data on a open network cryptography is becoming important feature of computer security. Many number of cryptographic algorithms are available for information security. There are main bio-cryptography schemes namely key generation, Key binding and key release.

Cloud environment: In cloud environment many encryption algorithms are available to provide more secure data transmission process. Some of the algorithms are DES, AES, RC4, Blowfish and 3DES for symmetric category and RSA, DCH for asymmetric category. The study implements Blow fish algorithm to

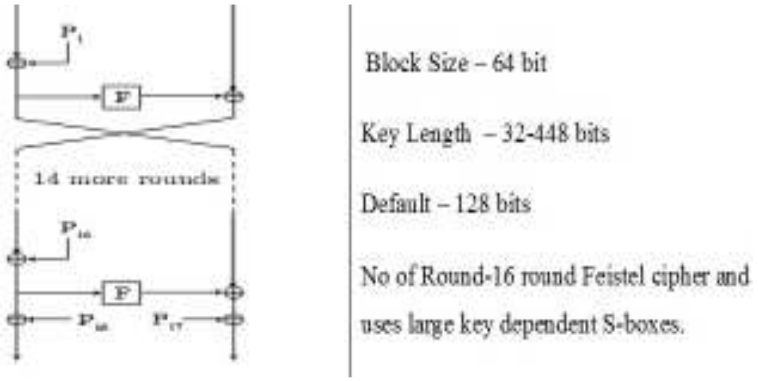

Fig. 3: Key expansion of blowfish algorithm

Table 2: Blowfish encryption algorithm

Designed in the year	1993
Author	Bruce schneir
Block size	64-bit block size
No. of rounds	16 rounds
Key length	1-448 bits
Encrypts	More than 232 data blocks
Usage	Unpatented, license free and available for all users
There are 2 parts in this algorithm	Expansion of key Encryption of the data

send a secured data in cloud environment. The Key is generated using Multi biometric system (Visu *et al*., 2012a).

Blowfish encryption algorithm: The Table 2 shows Blowfish Encryption Algorithm.

Expansion of key:

- Split the original key into a set of sub keys
- 4168 bytes is divided into 448-bit key. There is P-array and four 32 bit S-boxes
- P-array contains Eighteen 32 bit sub keys
- While Each S-Box contains 256 entries

Encryption of data:

- X denotes 64 bit input and Pi denotes P-array (i-iteration)

Key expansion of blowfish algorithm:

Step 1: Initialize the P-array and S-boxes
Step 2: XOR P-array with the key bits
Step 3: Use the above method to encrypt the all-zero string
Step 4: This new output is now P1 and P2
Step 5: Encrypt the new P1 and P2 with the modified sub keys
Step 6: This new output is now P3 and P4
Step 7: Repeat 521 times in order to calculate new sub keys for the P-array and the four S-boxes

Figure 3 Shows Key Expansion of Blowfish Algorithm.

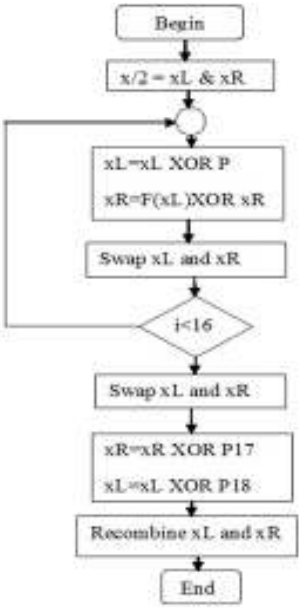

Fig. 4: Blowfish algorithm

Flow chart of blowfish algorithm: Figure 4 Shows Flowchart of Blow fish Algorithm.

Blowfish's F function: Figure 5 shows Blowfish's F function.

The function F: Initializing P-array and S-boxes with values derived from the hexadecimal digits of pi the secret key is then XORed with the P entries.
A 64-bit all-zero block is then encrypted with the algorithm.
P1 and P2 as a result instead of cipher text.
Cipher text is encrypted again with the new sub keys.

P3 and P4 are replaced by new cipher text (This continues).

Replacing the entire P-array and all the S-box entries.

Figure 6 shows The Function F of Blowfish Encryption Algorithm.

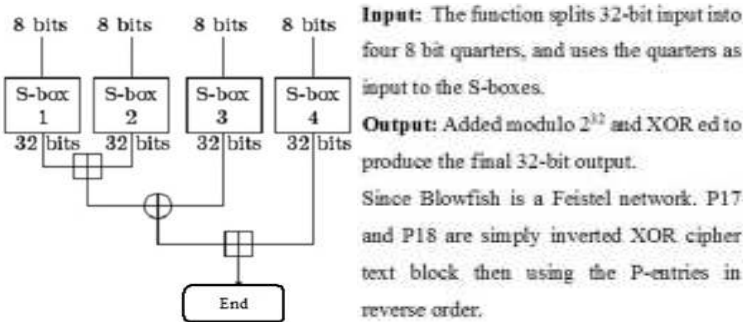

Fig. 5: Blowfish's F function

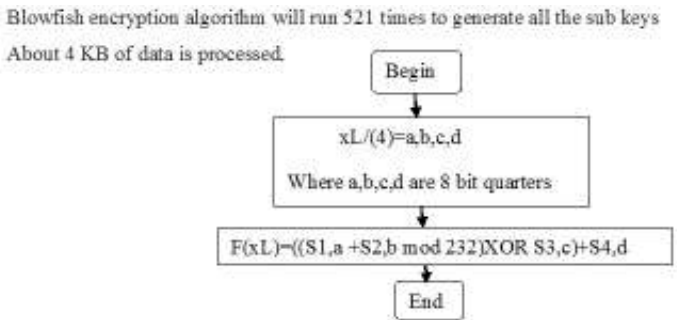

Fig. 6: The function F

LITERATURE REVIEW

Velciu *et al*. (2014) proposed a novel implementation for a bio-cryptographic infrastructure, as a safer authentication mechanism for Cloud storage sharing. This study implemented a Voice based fuzzy vault authentication mechanism, for secure access and encryption support within cloud platforms and cloud storage sharing.

Sanjekar and Patil (2013) has thrown some light on the shortcomings of unimodal biometrics such as noisy data, intra class variation and spoofing which result in the system that possess less accuracy and low security. To overcome these problems and to rise level of security multimodal biometrics came. Multimodal biometrics makes the use of multiple source of information for personal authentication.

Mane and Jadhav (2013) stated that the fusion of multiple biometrics helps to minimize the system error rates. Fusion options include processing biometric modalities sequentially until an acceptable match is obtained. Another one works in a way that combine scores from separate classifiers for every modality. He stressed on the fact that most of the biometric systems deployed in real world applications are unimodal that possess considerably high False Acceptance Rate (FAR) and False Rejection Rate (FRR). He also explained that today's unimodal system are having limited discrimination capability.

Bellare *et al*. (2013) talk about the possibility of storing the data on a remote cloud without having the problems of information leakage between users. They take a next step in this approach as they propose also a way of data de-duplication without decrypting any bit of information.

Patrascu and Patriciu (2013) presents a new and novel way of monitoring user activity in cloud environments using a secure cloud forensic architecture. This study talks about the architecture of such framework and emphasize the way in which this research applied on top of new or existing cloud infrastructures.

Zawoad *et al*. (2013) which presents an architecture for a secure cloud logging service that can be easily adapted to regular file storage.

Koteeswaran *et al*. (2012) the central idea in their paper is the interaction between multiple modules across the cloud infrastructure in order to create a secure environment for processing and storing data.

Shweta and Chander (2013) here author presents an approach to enhance the invisible watermarking technique with cryptography (Sumeet, 2013). The biometric trait is modified using invisible watermark information and is further secured using cryptography. The template is made more secure using encryption techniques like AES, MAES and finally stored in database.

Sheeba and Justin Bernard (2012) laid emphasis on that multimodal biometric systems have been widely adopted to overcome the shortcomings of unimodal biometric systems. Among various multimodality options, fingerprint and finger vein multimodality

ensures higher performance and spoofing resistance. This multimodal technology has reached an unparalleled level of security, accuracy and performance.

Radha *et al*. (2010) Propose a biometric verification system, investigating the combined usage of retina biometric features. Hardened by Fuzzy Vault scheme.

Sasidhar *et al*. (2010) converged on fact that multimodal biometric systems perform well than unimodal biometric systems and are popular even more complex also at the same time. His study also epitomes the notion of accuracy and performance of multimodal biometric authentication systems using state of the art Commercial Off-The-Shelf (COTS) products.

Nandakumar *et al*. (2007) presents also a fully automatic implementation of the Fuzzy Vault Scheme, based on fingerprint minutiae. They proposed the extraction of high curvature points derived from the fingerprint orientation and their use as helper data to align the template and query minutiae. Further, they applied a minutiae matcher for non-linear distortion and showed that performance improvement can be achieved by using multiple fingerprint impressions.

Visu *et al*. (2012b) propose the combination of biometrics cryptography with the purpose of developing a verification system.

Problem statement: One of the relative recent approaches for enhancing the modern cryptosystems security is to add the biometrics layer to the existing cryptographic frameworks. The Biometric Encryption process suggests combining the soft biometrics with existing cryptographic keys, overthrowing many of the biometric systems vulnerabilities. From the above literature reviews it is noted that by using biometrics and cryptography techniques in the security side for the cloud computing is sufficient. But most of the paper ensures implementation for a bio-cryptographic framework, as a safer authentication mechanism for Cloud storage sharing with maximum of two parameters. So there should be a technique which includes more than two parameters for bio cryptographic security.

METHODOLOGY

The main drawback of Cloud technology adoption was given by the lack of confidence it gained from potential beneficiaries, especially casual Internet users. The problems with password is that it is not secured. Passwords can be easily stolen and forgotten. Passwords are the main target for hackers through keystroke loggers and spyware. Passwords are rarely changed. Therefore by only using password is not sufficient. Thus biometric parameters are used here. A

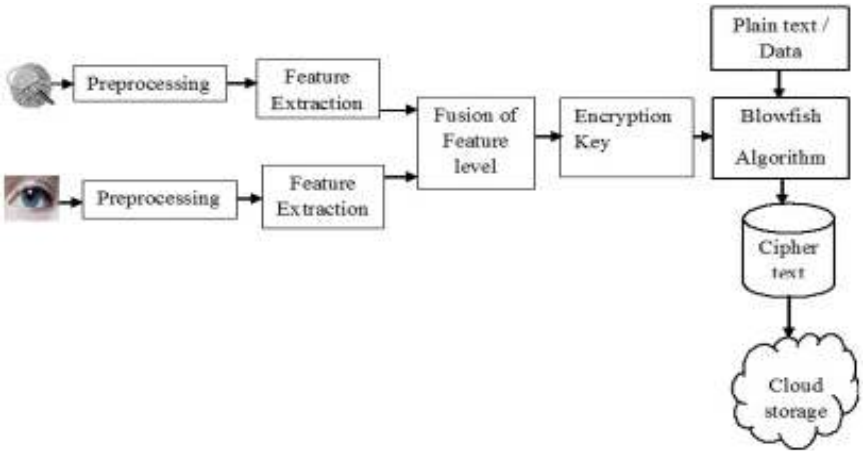

Fig. 7: Data encryption in cloud

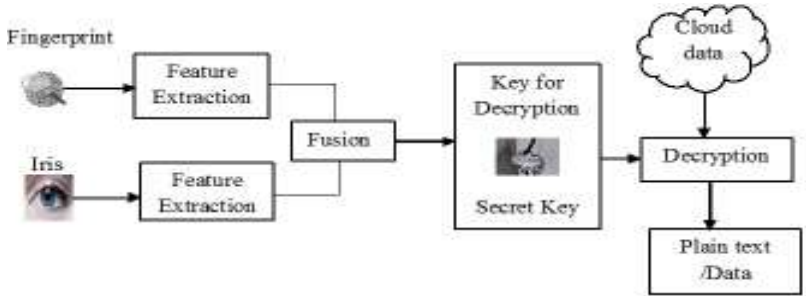

Fig. 8: Data decryption in cloud

successful and trustworthy multimodal biometric system wants a powerful fusion scheme to combine biometric characteristics.

Data encryption in cloud: Figure 7 shows the block diagram of Data Encryption in Cloud Computing.

Initially we apply preprocessing for feature extraction from each biometric image. Then the fusion of feature level both fingerprint and iris are used for encryption key for blow fish algorithm. The output of the blow fish algorithm is cipher text which is stored in the cloud environment. The intruders cannot able to read the cipher text in the cloud environment.
Figure 7 Shows Data Encryption in Cloud.

Data decryption in cloud: Figure 8 shows Data Decryption in cloud. The data from cloud is accessed by corresponding user by a secret key which is framed by the combined bio-metric of Finger print an Iris for decryption. The user will get the original message after decryption.
Figure 8 shows Data Decryption in Cloud.

RESULTS

Cryptographic technique is implemented using Blow-Fish algorithm. The fusion of both finger print and IRIS biometric is used as encryption/decryption key for the blow fish algorithm. The output of Blow-Fish algorithm is cipher text and it is stored in the cloud environment. The intruders cannot be able to read the cipher text in the cloud environment. The data from cloud is accessed by corresponding used by a secret key which is framed by the combined biometric of fingerprint and iris for decryption. The user will get the original message after decryption. Finally the user can achieve the data storage security in cloud environment from unauthorized users. The biometric cryptographic system is implemented using C++ language.

CONCLUSION

While consider the evolution of security threats in the past, the development of more authentication mechanisms has becomes demand, especially when dealing with Cloud technology. This study demonstrates that recent day's vastly used biometric techniques are capable of securing data. It explains that requires multiple layers of trust. Trustable same encryption to protect data and cloud security threats is enough to determine here are three choices on offer, encryption, finger print and iris parameters provide high accuracy is presented.

RECOMMENDATIONS

Future work will focus on enhancing the security of the proposed system, by using a random challenge based multimodal. Also, we take into consideration the use of another biometric characteristic, for improving system's performances, somehow, without lowering too much its acceptance and ease of use.

REFERENCES

Bellare, M., S. Keelveedhi and T. Ristenpart, 2013. Message-locked encryption and secure deduplication. Proceeding of the International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT.

Koteeswaran, S., J. Janet, E. Kannan and P. Visu, 2012. Terrorist intrusion monitoring system using outlier analysis based search knight algorithm. Eur. J. Sci. Res., 74(3): 440-449.

Mane, V.M. and D.V. Jadhav, 2013. Review of multimodal biometrics: Applications, challenges and research areas. Int. J. Biometrics Bioinformat. 3(5): 90-95.

Nandakumar, K., A.K. Jain and S. Pankanti, 2007. Fingerprint-based fuzzy vault: Implementation and performance. IEEE T. Inf. Foren. Sec., 2(4): 744-757.

Patrascu, A. and V. Patriciu, 2013. Beyond digital forensics: A cloud computing perspective over incident response and reporting. Proceeding of the IEEE International Symposium on Applied Computational Intelligence and Informatics.

Radha, N., S. Karthikeyan and P. Anupriya, 2010. Securing retina fuzzy vault system using soft biometrics. Global J. Comput. Sci. Technol., 10(7): 13-18.

Sakshi, K. and L. Anil, 2014. Improving performance by combining fingerprint and iris in multimodal biometric. Int. J. Comput. Sci. Inf. Technol., 5(3): 4522-4525.

Sanjekar, P.S. and J.B. Patil, 2013. An overview of multimodal biometrics. Signal Image Process. Int. J., 4(1): 57-64.

Sasidhar, K., V.L. Kakulapati, K. Ramakrishna and K. KailasaRao, 2010. Multimodal biometric systems-study to improve accuracy and performance. Int. J. Comput. Sci. Eng. Surv., 1(2): 54-61.

Sheeba, T. and M. Justin Bernard, 2012. Survey on multimodal biometric authentication combining fingerprint and finger vein. Int. J. Comput. Appl., 51(5): 55-60.

Shweta, M. and K. Chander, 2013. A novel approach for securing biometric template. Int. J. Adv. Res. Comput. Sci. Softw. Eng., 3(5): 397-403.

Sumeet, K., 2013. Enhancing template security by a biometric key generating cryptosysytem: A review. Int. J. Adv. Res. Comput. Sci. Softw. Eng., 3(8): 973-976.

Velciu, M.A., A. Patrascu and V.V. Patriciu, 2014. Bio-cryptographic authentication in cloud storage sharing. Proceeding of the 9th IEEE International Symposium on Applied Computational Intelligence and Informatics, pp: 165-170.

Visu, P., J. Janet, E. Kannan and S. Koteeswaran, 2012a. Optimal energy management in wireless adhoc network using Artificial Bee Colony based routing protocol. Eur. J. Sci. Res., 74(2): 301-307.

Visu, P., S. Koteeswaran and J. Janet, 2012b. Artificial bee colony based energy aware and energy efficient routing protocol. J. Comput. Sci., 8(2): 227-231.

Zawoad, S., A.K. Dutta and R. Hasan, 2013. SecLaaS: Secure logging-as a- service for cloud forensics. Proceeding of the ACM Symposium on Information, Computer and Communications Security.