IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 5, Oct-Nov, 2013
ISSN: 2320 - 8791
www.ijreat.org

SIMHA : Secure Biometric Multi-Host Authentication

Ramya K P[1], Chithra Devi R[2] and Revathi M K[3]

[1] **Information Technology, Dr.Sivanthi Aditanar College of Engineering, Tiruchendur, Tamil Nadu 628215, India**

[2] **Information Technology, Dr.Sivanthi Aditanar College of Engineering, Tiruchendur, Tamil Nadu 628215, India**

[3] **Information Technology, Dr.Sivanthi Aditanar College of Engineering, Tiruchendur, Tamil Nadu 628215, India**

Abstract

Biometric is the most secure and convenient authentication tool. It can't be borrowed, stolen, or forgotten, and forging one is practically impossible. In that, Fingerprint evidence is the most positive investigative means of identifying people. Every fingerprint is unique. So fingerprint is used as both the user ID and the password. The existing password based systems were designed over a single or two server. In the proposed system, it distributes the password database as well as some functions to multiple servers. During registration the user must provide their fingerprint detail that is stored in the server. It uses the scanner for extraction of fingerprint string. The front-end server encrypts and splits the string to the back-end servers who are joined at runtime. This allows the server to determine runtime backend servers at the time of registration; also it uses random class for generating different order for password storage. During verification the encrypted passwords are gathered and at server side it gets decrypted. The decrypted passwords are concatenated to develop the original password. The experimental results will show the security and efficiency of the proposed system.

Keywords: *Multi-server, AES, Cryptography, Biometric, Network Security.*

1. Introduction

Biometric matching systems use some unique features, such as retina, face, fingerprint, hand and etc., to identify the personality. Different approaches in authentication system but the biometric system especially fingerprint system is a major role for the different basic processing system. There is an increasing amount of transactions using communications over network. Therefore secure communication will be provided by the cryptography techniques such as encryption and decryption. Another basic approach for security is multi-server authentication system. Past research provides a password based system mainly intended to completely protect user authentication. Here each user shares a password or password verification data with two server. These systems are essentially intended to defeat offline dictionary attacks by outside attackers and assume that the server is completely trusted in protecting the user password database. Once an authentication server is compromised, the attackers perform an offline dictionary attacks against the user passwords.The multi server architecture provides a high level of security for storing the passwords. Strong authentication is essential to verify the identities of stored locations as well as individual users. This ensures that only authorized users are given access to the network. It also controls the access of other outside users to the applications. Encryption algorithms are used to scramble the data so that only those have encryption key can read the information. Therefore secure communication will be essential for the exploitation of network to its full potential, such as for the transfer of sensitive data like passwords. Even though the password which is in an individual system is decrypted it won't give the whole data to access the system. It only provides the part of the password. The major observation is that the multiple levels of security upon several servers with unauthorized entities. Particularly this system is suitable for online secured web applications due to its high efficiency.

2. System Model and Background

2.1. Types of Biometric Authentication

2.1.1. Voice Recognition

Voice recognition systems look for voice pattern matches. Voice recognition systems have the advantage of being user friendly, but such things as background noise and changes to the voice due to colds, sinus congestion, anxiety, etc. can result in false negatives.

2.1.2. Eye Scans

Two types of eye scan are retinal and iris scans. Retinal scanning scans the patterns of the retina, in the interior of

the eye. It is a highly accurate and well-established security method. It requires that the user make physical contact with the scanner, which raises hygiene problems, and for an accurate reading, the user must hold a focus on a particular point. Iris scanning involves scanning the patterns of the iris, the colored part of the eye. The scan can be done at a distance and without removal of eyeglasses. The images used by iris scans are larger than retinal scan images and so require more storage space.

2.1.3. Facial Recognition

Facial recognition systems are the newest biometric authentication technology. They look for distinctive facial features such as the location and shape of the nose and eyes, the sides of the mouth, cheekbones, etc. The technology is still being developed, and as of now it works best when comparing two static images.

2.1.4. Fingerprints

Fingerprint verification is the most common type of biometric authentication currently in use. Fingerprint scanners have the advantage of being small, low-cost, easy to implement and highly accurate.

2.2. Multi-Host Model

The proposed multi-host model comprises more than one servers at the server side, one of which is a users server exposing it to users called front-end host and the other of which is a back-end host staying behind the scene, where the users contact only the front-end host. But the servers work together to authenticate users. In this architecture, a user ends up establishing a session key only with the front-end host, and the role of back-end control host is to assist the front-end server in order to authenticate the users. The overall system security is also improved in this model as service server is alone exposed to users and is prone to dictionary attacks.

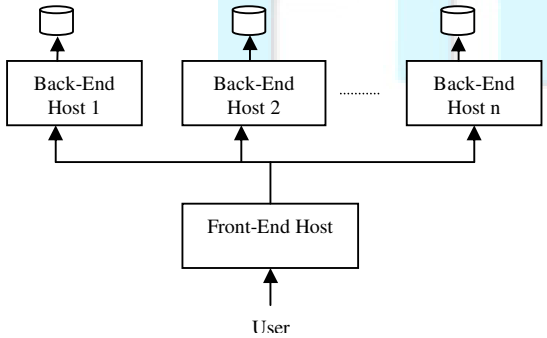

Fig. 2.1 Multi-Host Model

2.2. Cryptography and Security

Exchange and storage of information in an efficient, reliable and secure manner is of fundamental importance. There is an increasing amount of transactions using communications over network. Therefore secure communication will be essential for the exploitation of network to its full potential, such as for the transfer of sensitive data such as documents and texts. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (Internet). Cryptography is fundamental in order to protect information against unauthorized changes and other misuse of information. A cryptanalyst studies vulnerabilities of ciphers and other cryptographic techniques. The proposed paper used the Advanced Encryption Standard(AES)[11] for encryption and decryption.

AES is a block cipher. This means that the number of bytes that it encrypts is fixed. AES can currently encrypt blocks of 16 bytes at a time; no other block sizes are presently a part of the AES standard. If the bytes being encrypted are larger than the specified block then AES is executed concurrently. This also means that AES has to encrypt a minimum of 16 bytes. If the plain text is smaller than 16 bytes then it must be padded.

3. Related Works

The password based system is mainly intended to completely protect user authentication in the existing system. In this system each users shares a password or password verification data with two server[1]. These systems are essentially intended to defeat offline dictionary attacks by outside attackers and assume that the server is completely trusted in protecting the user password database Once an authentication server is compromised, the attackers perform offline dictionary attacks against the us er passwords. Later the two server architecture was implemented, it can also be easily compromised. In this two server architecture, the backend server is easily known by the hackers within several experiments.

4. Proposed Works

In proposed system the fingerprint string of the user is stored in the registration moment. The user has to register their fingerprints, and this will be compared with the already stored data in the database during login time. Thus it provides access to the user. This project consists of the following modules.

- Registration Module
- Verification Module

4.1. Registration Module

This makes the user to first register in the network to access some information. It contains the following steps.
Fingerprint Scanning

- Fingerprint Scanning
- Encryption
- Dynamic Connection
- Shuffling
- Splitting
- Broadcasting and Updating

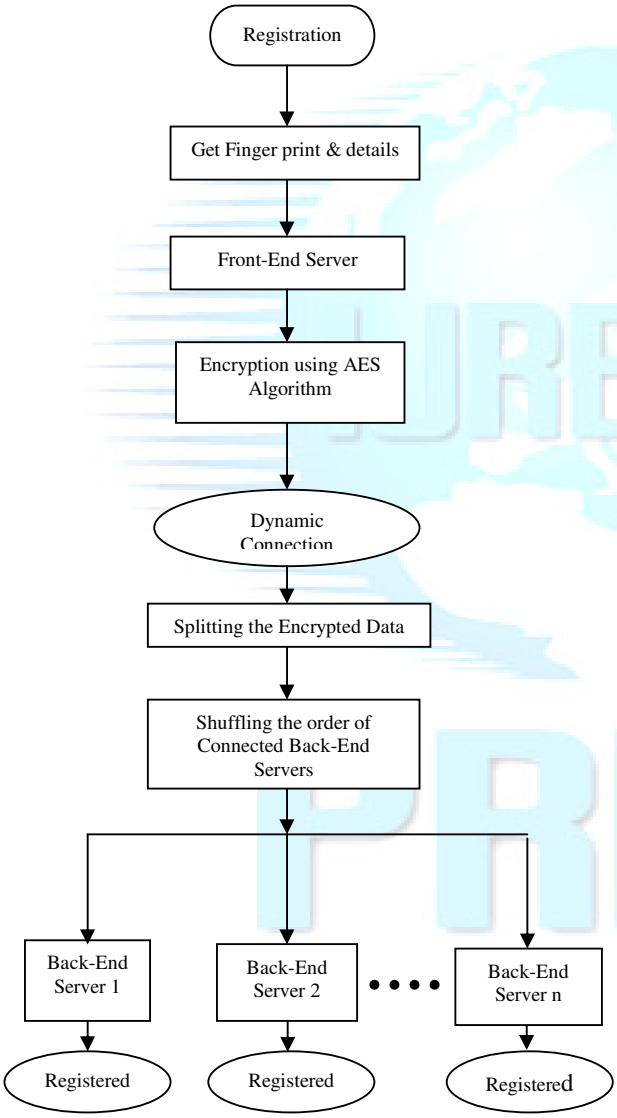

Fig. 4.1 Registration Phase Overview

4.1.1. Fingerprint Scanning

Fingerprint scanning is the acquisition and recognition of the person's fingerprint characteristics for identification purposes. This allows the recognition of a person through quantifiable physiological characteristics that verify the identity of an individual. There are basically two different types of fingerprint scanning technology that make this possible. One is an optical method, which starts with a visual image of a finger. The other uses a semiconductor generator electric field to image a finger. Here the fingerprint image is captured from the user and it is converted into string format. This will be enrolled as a password and at once the ID is generated for the user.

4.1.2. Encryption

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as key. The result of the process is encrypted information (referred to as cipher text). Here AES encryption algorithm is used. It encrypts the fingerprint string and makes it unreadable.

4.1.3. Dynamic Connection

When the front end is ON it listens for the connections from the back end servers. If the backend servers request for connection in the server's port . The front-end server automatically accepts the connection and allows that server to be joined in the network. In this dynamic connection the backend server is assumed that it is the only client which is connected with the server. It does not have the knowledge about the other backend servers.

4.1.4. Shuffling

Shuffling is the process of rearranging the order of backend servers. So it is impossible to hack the client details. Here pseudorandom generator is used to shuffle the order of clients that are connected. It has seed value which is responsible for the rearrangement. The front end server only maintains this data. Thus it provides more security.

4.1.5. Splitting

As per the number of client connections the splitting has to be done dynamically. After the connection is established front end server is responsible for determining the number of connections.

The splitting algorithm splits the encrypted string according with the number of connections made to the front end server.

4.1.6. Broadcasting and Updating

The splitted strings are broadcasted as per the shuffling order of clients gets connected. When the backend server is ready to accept, the data gets updated in their databases respectively along with the appropriate ID.

4.2. Verification Module

Verification takes place during the login time. It consists of the following process.

- Login
- Retrieving
- Reshuffling
- Concatenation
- Matching

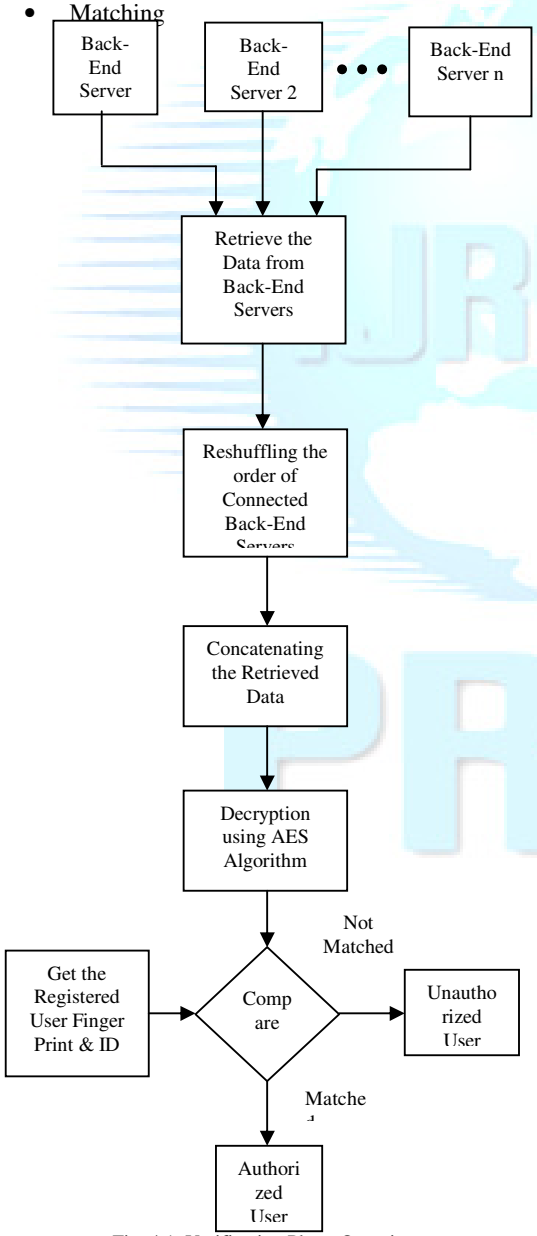

Fig. 4.1 Verification Phase Overview

4.2.1. Login

It is done after the registration process gets completed. It determines whether the user is authorized or not. Initially the user provide their id and fingerprint string as password, its gets submitted. At once it passes this information to all backend servers.

4.2.2. Reshuffling

It is the process of arranging the client in correct order. It uses seed value in the pseudo random generator for getting previously shuffled order of clients specifically for this user with his id. Thus it is necessary to find this rearranged order to retrieve the correct password parts that have been stored in these clients.

4.2.3. Retrieving

Initially the user login with their id and password. Then this id gets broadcasted to all the clients in the order of shuffling. Hence it retrieves the data from all the clients which have the corresponding id.

4.2.4. Concatenation

It is the process of combining all the parts of data into one string. Thus here when it receives all the parts for the corresponding id, it rearranges the shuffled order in correct order and combine these password parts into one string with correct order. It assures security, because that it concatenate only after it receives all the distributed data.

4.2.5. Matching

It is the major process of verification. When the original string is retrieved after concatenation it gets decrypted at the server side. The user access the information only when the current string matches with the string already stored in the database for this corresponding id (decrypted data). If it is not matched it shows that the user is not the authorized person. If it matches it allows the user to access the information.

5. Experiments and Results

The visual representation of our work example gives maximum accuracy and robust security in multi-tier technology. Some of the visual representation of the output will be presented below.

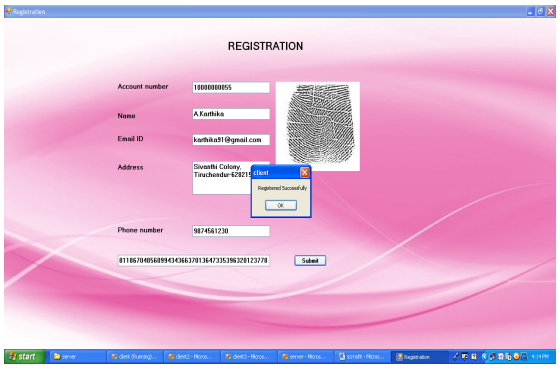

Fig 5.1 Registration

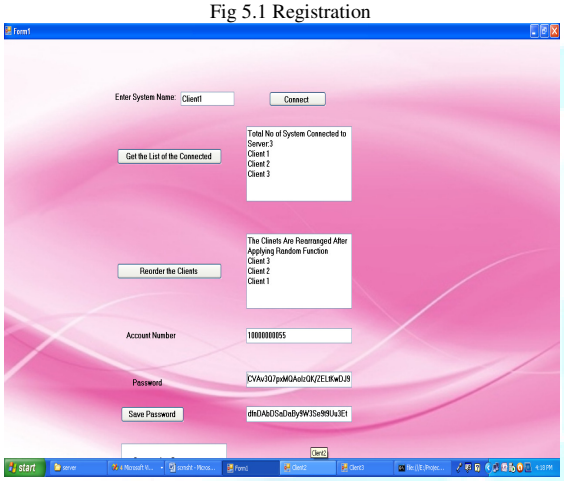

Fig 5.2 Connecting and Reordering the Backend Servers

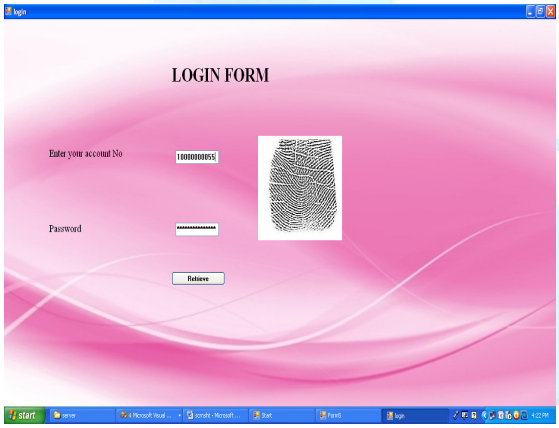

Fig 5.2 Login

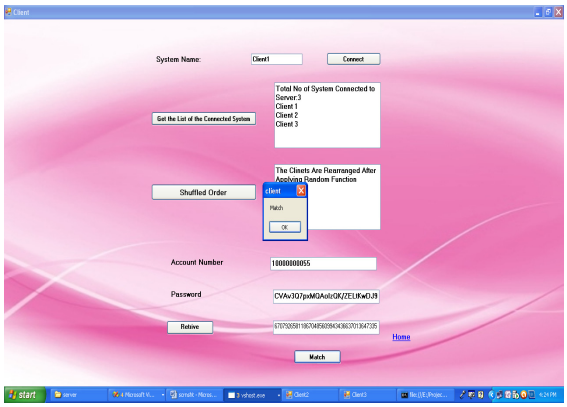

Fig 5.2 Retrieving Password and Verification

6. Conclusion and Future Enhancements

6.1. Conclusion

The Secure Biometric Multi-Host Authentication System is suitable for number of practical applications like Biometric ATMs. Compared with previous solutions, this system possesses many advantages, like highly efficient in terms of both computation and communications. It is also applied to existing standard single sever biometric based security applications. Also it can be used in online web application and in federated enterprise setting, where a single control server supports the multiple servers. Implementation of this process will envisage for modernize and purifying the authentication process in the most networking places. It is eminent that there is no hacking occurs in the authentication process. Also it is not transparent and more secured one compare to other processes possess for authentication security adopted before because it deeply notices on the encryption. This provides a new way for the identification of user joining a closed network based on cryptography. It will be exemplary and will be appreciated worldwide if brought in to adoption.

6.1. Future Enhancements

This paper can be extended to provide more security by using some additional techniques. Apart from that iris can be used as a password instead of fingerprint. It can be implemented to avoid specific attacks. Focus on steps to improve database security will be implemented further. Entire system will be implemented to online so that anyone can access from anywhere just by using fingerprint or iris. This idea is later imposed on practical application like biometric ATMs and online webpage accessing.

References

[1] Dr. S. Arumugaperumal and D. Bennet, “Fingerprint Based Multi-Server Authentication System”, IEEE, Vol 4, 2011, pp. 115-119

[2] L. Hong, Y. Wan, and A. Jain, “Fingerprint Image Enhancement: Algorithm and Performance Evaluation,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no.8, 1998, pp.777-789.

[3] D. Boneh, “The Decision Diffie-Hellman Problem”, Proc. Third Int'l Algorithmic Number Theory Symp., 1998. pp. 48-63.

[4] Anil k. Janin, “Pores and Ridges: High Resolution Fingerprint Using Level 3 Features”, IEEE vol.29 No.1 2007.

[5] Y. Chen, S.C. Dass, and A.K. Jain, “Fingerprint Quality Indices for Predicting Authentication Performance,” Proc. Audio- and Video- Based Biometric Person Authentication, pp. 160-170, 2005.

[6] Yanjiang Yang, Robert H. Deng, Feng Bao, "A Practical Password-Based Two-Server Authentication and Key Exchange System," IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 2,2006 pp. 105-114.

[7] D.C. Huang, "Enhancement and Feature Purification of Fingerprint Images," Pattern Recognition, vol. 26, no. 11, 1993, pp. 1,661-1,671.

[8] A. Jain, L. Hong and R. Bolle, "On-Line Fingerprint Verification," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 4, 1997, pp. 302-314.

[9] M. Kawagoe and A. Tojo, "Fingerprint Pattern Classification," Pattern Recognition, vol. 17, no. 3, 1984, pp. 295-303.

[10] N. Ratha , S. Chen and A. K. Jain "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Pattern Recognition, vol. 28, no. 11, 1995, pp.1657 -1672.

[11] H Nover, "Algebraic Cryptanalysis of AES: An Overview", University of Wisconsin, USA, 2005.