Double Encryption Based Secure Biometric Authentication System

S.Kavin hari hara sudhan[(1)], Prof.S.Ramamoorthy[(2)]

[(1)]M.Tech student in Computer Science and Engineering

[(2)]Professor in Computer Science and Engineering

Dr.MGR Educational and Research Institute, Chennai, Tamilnadu , INDIA

***ABSTRACT*: Nowadays bio-metric authentication systems are widely used in order to provide authentication without possessing any physical materials. Bio-metric authentication systems are mainly concentrating on security, revocability, privacy, and accuracy. In this paper, we propose a provably two way secured biometric authentication system, which addresses the concerns of user's privacy, template protection, trust issues, network security, and accuracy. The system is two way secured in the sense, biometric details are going to be encrypted twice, the system won't reveal any additional information about the user or biometric, to the authenticating server's database or to the insecure network. In this system two different encryption algorithms have been used both in the client and server side. One is public key cryptography another one is private key cryptography. User's privacy as concern it is revealing only the identity of the user. In template protection this protocol will store the template as encrypted form. Protocol will provide trust between remote user and server, while a remote user cannot be reliably identified without biometric information. Since network security as concern protocol is not revealing the plain biometric details while it is passed through the network. The proposed approach has no restrictions on the biometric data used and it is applicable for multiple biometrics (face, iris, hand geometry, and finger print). Authentication by using two way encryption will give additional layer of security when comparing with existing systems.**

***KEY TERMS*: accuracy, authentication, biometrics, crypto systems, privacy, protocol, public key cryptography, revocability, security.**

I. INTRODUCTION

British biometric passports have hacked by Lucas Grunwald, a consultant with a German Security Company, and discovered a method for cloning the information stored in new passports[11]. *FastCompany.com* is reporting that the biometric data of almost every Israeli citizen has been compromised and is now available on the Internet. Clearly, as more governments, such as India and Germany, collect more biometric data on their citizens, the security of such information will continue to be an issue[12].We are concentrating our proposed work towards this issue.

Biometric authentication systems are gaining wide-spread popularity in recent years due to the advances in sensor technologies as well as improvements in the matching algorithms [1] that make the systems both secure and cost-effective. They are ideally suited for both high security and remote authentication applications due to the non-repudiate in nature and user convenience. Most biometric systems are assumed to be secure but there are chances of getting hacked. There are two places to be attacked: (i) one is on communication link and another (ii) on server's database. In order to protect from this type of attacks we propose this system. However a variety of applications of authentication need to work over a partially secured or in-secured networks such as ATM networks or the Internet. Authentication over insecure public networks or with un-trusted servers raises more concern in privacy and security. The primary concern is related to the security of the plain biometric templates, which cannot be replaced, once they are compromised. The privacy concerns arise from the fact that the biometric samples reveal more information about its owner (medical, account, etc.) in addition to the identity. Widespread use of biometric authentication also raises concern of tracking a person, as every activity that requires authentication can be uniquely assigned to an individual.

A. FEATURES FOR GOOD BIOMETRIC AUTHENTICATION SYSTEM

1) Template protection- It is the process of storing biometric information securely, it should be protected from various types of attacks. Critical information could be revealed if the server's biometric template database is compromised.

2) User's privacy- Each and every individual has unique biometrics, so the privacy of the user can be easily maintained.

3) Trust between client and server- Sometimes client and server have disbelief on each other. Denial of service should be overcome by using public key cryptography.

4) Accuracy- False acceptance rate(FAR) and False rejection rate(FRR) should be minimized.

To clarify our problem, let us consider the following usage scenario:

"Person A" wants to create an account in "Peron B's mail", that requires biometrics based authentication. However, "A" neither trusts "B" to handle his biometric data securely, nor trusts the network to send his plain biometric. The primary problem here is that, for "A", "B" could either be incompetent to secure his biometric or even curious to try and gain access to his biometric data, while the authentication is going on. So "A" does not want to give his biometric data in plain to "B". On the other hand, "B" does not trust the client as he could be an impostor. He could also repudiate his access to the service at a later time. For both parties, the network is insecure. A biometric system that can work securely and reliably under such circumstances can have a multitude of applications varying from accessing remote servers to e-shopping over the Internet.

For social applications , when the user is able to authenticate himself using a strongly encrypted version of his biometric (say using RSA [3]), then many of the concerns on privacy and security can be addressed. However, this would require the server to carry out all the computations in the encrypted domain itself. Unfortunately, encryption algorithms are designed to remove any similarity that exists within the data to defeat attacks, while matching algorithms require the similarity of data to be preserved to achieve high accuracy. In other words, security/privacy and accuracy seem to be opposing factors. Different secure authentication solutions try to make reasonable trade-offs between the opposing goals of security and accuracy, in addition to make specific assumptions about the representation or biometric being used.

We overcome this unavoidable problem by designing the system in such way that the matching should be done in the plain feature space, which allows us to maintain the performance of the biometric. We show that it is possible to achieve a practical solution using distribution of work between client system and the server, using our proposed scheme. In client we are using strong public key encryption known as RSA algorithm and in server we are using private key cryptography known as triple DES.

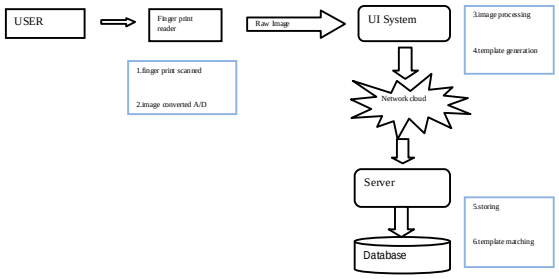

Fig. 1. Biometric Authentication System

A. Characteristics of biometrics

1) *Universality*: every individual has their own biometric details.
2) *Distinctiveness*: no two persons are having the same biometric details.
3) *Permanence*: biometric details won't change from time to time.
4) *Collectability*: biometric details can be easily measured.
5) *Performance*: biometric details will give better performance in terms of accuracy and speed.
6) *Acceptability*: which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives.

Table 1: COMPARISON BETWEEN VARIOUS BIOMETRICS

Biometric characteristic	Universality	Persistence	Collectability	Performance	Acceptability	Circumvention
Face	High	Medium	High	Low	High	Low
Fingerprint	Medium	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	High	Medium	Medium	Medium
Iris	High	High	Medium	High	Low	High
Retinal Scan	High	Medium	Low	High	Low	High
Signature	Low	Low	High	Low	High	Low
Voice	Medium	Low	Medium	Low	High	Low
Thermogram	High	Low	High	Medium	High	High

Source: Book Understanding biometrics from http://www.griaulebiometrics.com

II.RELATED WORK

All reliable personal recognition schemes are used to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes are to ensure that the legitimate user is using the system or not. Examples of

such applications include secure access to buildings, computer systems, laptops, cellular phones and ATMs. Without this personal biometric authentication system all the above said applications are vulnerable to many types of attacks. Biometric recognition, or simply biometrics, refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. By using biometrics it is possible to confirm or establish an individual's identity based on "who he is", rather than by "what he possesses" (e.g., an ID card) or "what he remembers" (e.g., a password). Even though there are chances of hacking plain biometric details from the database or from the network. To overcome this drawback we are proposing encrypted version of the finger print to be used.

The second existing work in the area of encryption-based security of biometric templates used to model the problem as that of differentiating the genuine and impostor samples in the encrypted domain. However, a strong encryption may destroy any pattern in the data, which adversely affects the accuracy of verification. Hence, any such matching mechanism necessarily makes a compromise between template security (strong encryption) and accuracy (retaining patterns in the data). The primary difference in that approach is that they are able to design the matching in the plain feature space, which allows us to maintain the performance of the biometric itself, while carrying out the authentication on data with strong encryption, which provides high security/privacy .

Over the years a number of attempts have been made to address the problem of template protection and privacy concerns. In this section, we will look at the existing work in light of this security-accuracy dilemma, and understand how this can be overcome by communication between the authenticating server and the client. To provide better communication between client and server they introduced trusted third party(TTD)

To provide trust between client and the server ,in the existing paper they used Trusted Third Party(TTP). It requires more computation and there is a chance of TTP can be hacked. This scenario can be overcome by public key cryptography which is used in the proposed system.

Our proposed work addresses all the features for good biometric authentication system mentioned above .

1) The ability to use two different strong encryptions in client and server side addresses template protection issues as well as privacy concerns.
2) Non-repudiate authentication can be carried out even between non trusting client and server using a public key cryptography solution.
3) Two way encryption enhances the security. It provides provable protection against replay and client side attacks even if the keys of the user are compromised.
4) As the enrolled templates are encrypted using a key, one can replace any compromised template, providing revocability, while allaying concerns of being tracked.
5) Accuracy of the system can be maintained as the authentication takes place in the decrypted domain.

III.PROPOSED WORK

The proposed system works with the following scenario. The client and server are communicating with each other, while doing the enrollment and authentication. Each and every individual has been assigned with unique user name, password. Individual's finger print has been appended with unique user name and password during enrollment. The finger print has been safe guarded by using two different encryption algorithms in both client and server side in order to secure the finger print both in network and database.

In client side we are using RSA algorithm and in server side we are using 3DES algorithm.RSA algorithm will reduce the denial of service problem since it is a public key cryptography.

During authentication, One who wants to authenticate himself has to give his username, password and his finger print to the authenticating server. Matching has been done with plain biometric details so it will maintain accuracy. After matching took place in the server and on success, authentication is confirmed. This is implemented through the following algorithms.

A. THE ALGORITHM

Algorithm 0

Step 1:start
Step 2:call algorithm 1(enrollment).
- Step 2.1:call algorithm 5(minutiae extraction)in client side.
- Step 2.2:call algorithm 3(RSA algorithm) in client side.
- Step 2.3:call algorithm 3(RSA algorithm)in server side.
- Step 2.4:call algorithm 4(3DES algorithm)in server side.
- Step 2.5:store encrypted data in database.

Step 3:call algorithm 2 (authentication).
- Step 3.1:call algorithm 5(minutiae extraction)in client side.
- Step 3.2:call algorithm 3(RSA algorithm) in client side.
- Step 3.3: forward the RSA encrypted finger print to the server side.
- Step 3.4: call algorithm 3 for decrypting RSA encrypted finger print.
- Step 3.5: get 3DES encrypted equal data from database.

Step 3.6: call algorithm 4(3DES algorithm) in server side for decryption.
Step 3.5: call algorithm 6 for matching.
Step 4: reply authentication confirmation.

Algorithm 1:Enrollment

Step 1: client collects multiple samples of biometric from User
Step 2: Feature vector Xi are computed for each sample.
Step 3: client request for a key from server.
Step 4: encryption of Xi,E1(Xi) using RSA algorithm
Step 5: forwarding E1(Xi) to server.
Step6: decryption D1(Xi) by using RSA in the server side.
Step7: again encryption E2(Xi) in the server side by using Triple DES.
Step8: storing it in the database.
Step9: client is then notified about the success.

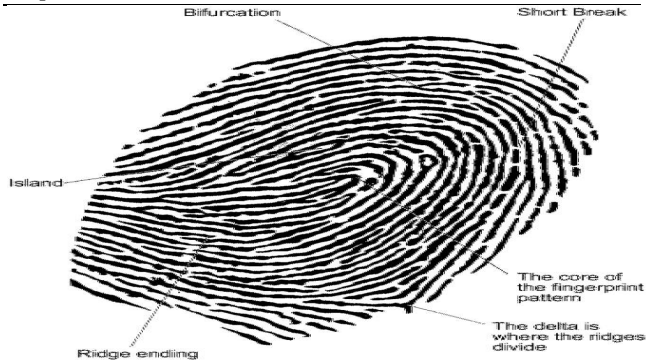

Fig. 2.finger print and its features

At the time of enrollment the user has to give his finger print samples to the client machine. The client machine will extract the features like ridge ending, bifurcation etc, then It will request for the key from the server in order to do the public key encryption. Here we used RSA algorithm to encrypt the minutiae details by using the key of the server. The encrypted minutiae has been forwarded to the server. In the server side that encrypted minutiae has been decrypted by using RSA algorithm and then it is going to be encrypted by using triple DES. Then that resultant encrypted finger print has been stored in the database. Then that client has been notified with the success of enrollment.

Algorithm 2:Authentication

Step 1: client computes feature vector x1…n from input Finger print.
Step 2: requesting for key from the server.
Step 3: each feature Xi is encrypted E1(Xi) and sent to server.
Step 4: server computes D1(Xi) and get Xi.
Step 5: server gets equivalent E2(Xi) from database.
Step 6: again computes D2(Xi) and get Xi by using triple DES.
Step 7: matching has been done. Store the result in S
Step 8: if $S > \alpha$ then
Step 9: return Accepted to the client
Step 10: else
Step 11: return rejected to the client
Step 12: end if.

Where α is minimum threshold.

While doing authentication plain biometric details have been given along with the username and password. It has to be encrypted using RSA algorithm with the key from server. Then encrypted minutiae has been forwarded to the authenticating server. In the server side RSA decryption has been carried out , then that result has been compared with already stored minutiae details of intended user. here minimum threshold(α) has been used. If result is greater than minimum threshold then the user has been notified with "accepted" comment else "rejected" comment will be forwarded to the client.

Algorithm 3:RSA algorithm

Key Generation:
Step 1 : Select two prime no's p & q
Step 2 : Calculate n as product of p & q, i.e. n=pq
Step 3 : Calculate m as product of (p-1) & (q-1) i.e. m = (p-1)(q-1)
Step 4 : Select any integer e<m such that it is co-prime to m, i.e gcd(e,m) =1
Step 5 : Calculate d such that de mod m = 1 , i.e. $d = e^{-1} \bmod m$
Step 6: The public key is {e,n)
The private key is {d,n}

Encryption:
Plaintext=P&P<n
Ciphertext = C

$C = P^e \bmod n$

Decryption:
Ciphertext = C
Plaintext = P and $P = C^d \bmod n$

Algorithm 4:Triple DES

- Key size: 64 bits - 56 key bits and 8 parity bits.
- Effective key size: 56 bits.
- Block size: 64 bits.
- Rounds in the algorithm: 16.
- Type of cipher: Permutation and Substitution.

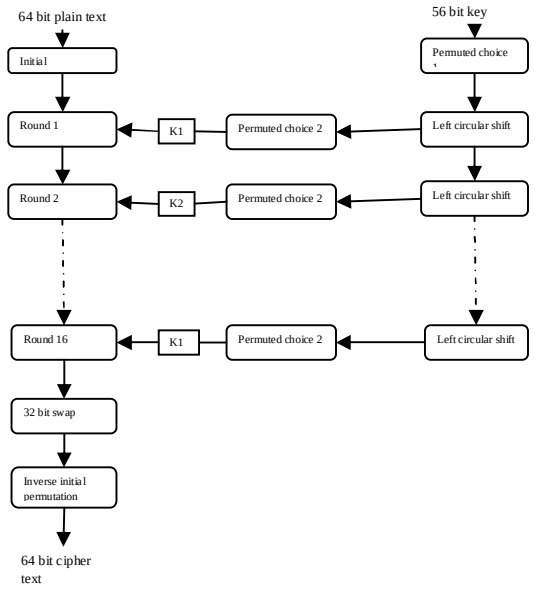

Fig. 3.DES algorithm

Use of multiple length keys leads us to the Triple-DES algorithm, in which DES is applied three times. If we consider a triple length key to consist of three 56-bit keys K1, K2, K3 then encryption is as follows:

• Encrypt with K1
• Decrypt with K2
• Encrypt with K3

Decryption is the reverse process:

• Decrypt with K3
• Encrypt with K2
• Decrypt with K1

Algorithm 5:Minutiae extraction from finger print

Step 1:plain finger print image has been taken.

Step 2:It has to be subjected to preprocessing unit

2.1.Image size has been altered to323x352 pixels.

2.2.Clarity of image has been maintained.

2.3.Image has been converted to bit map format.

Step 3:core of the finger print has been identified.

3.1.cut of 50,50,50,50,pixels in the four sides.

3.2.find center point which is having 270 degree or more curvature angle

3.3.Note the X&Y co-ordinate values.

Step 4: Chain link algorithm is used to give continuity if image contains some impurities.

Step 5: Hit and miss algorithm is used to give width stroke in one pixel.

Step 4:calculate ridge ending, bifurcation, island distances from core and store X&Y co-ordinate values of each.

Algorithm 6:Matching algorithm

Step 1:Image can be in any angle it will do the matching.
Step 2:Matching has been done with the core of the image first.
Step 3:Distance can be calculated by using
$(X1-X2)^2 + (Y1-Y2)^2$.(Distance from core to the features)
Step 4:Cos and sin values of the angle has been taken for matching in the curvature.
Step 5:Store compared results in the match count.
Step 6:Then compare the match count with minimum threshold.

B. Design

The proposed work has been designed in two architecture diagrams, one for enrollment and another one for authentication by using a software tool called Edrawmax Version 5.0.

Architecture Diagram

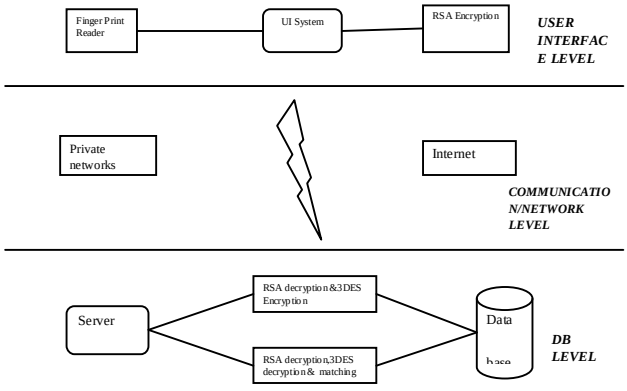

Fig. 4.System Architecture

C. IMPLEMENTATION

The implementation has been done with the help of above two architecture diagrams .All experiments are done on an Intel Pentium Dual Core processor, with 2GB RAM and 160GB hard disk. In the software requirements wise windows XP operating system has been used. For front end designing purpose Visual studio 2008, and for back end data storage purpose SQL server 2005 has been used. The development language C# has been used. For RSA algorithm and 3DES, We used open source software codes from internet. For test data we used *Biometrics ideal test* website with the URL of http://biometrics.idealtest.org. In this implementation we have succeeded with the all five parameters like template protection, user privacy, security, accuracy, trust between client and server.

EXAMPLE TEST DATA

Fig 5.Example test data

D. RESULT ANALYSIS

We measured the system performance by implementing our technique and is visualized. The system performance can be measured by means of False acceptance rate(FAR), and False rejection rate(FRR).

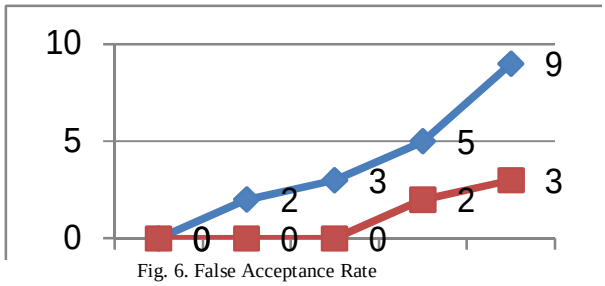

Fig. 6. False Acceptance Rate

The graphs (Fig 6) are been drawn with X-axis as number of persons using the system and Y-axis as number of persons who are falsely accepted. The result shows that the FAR of the existing system is 0.09 and of the proposed system is 0.03.

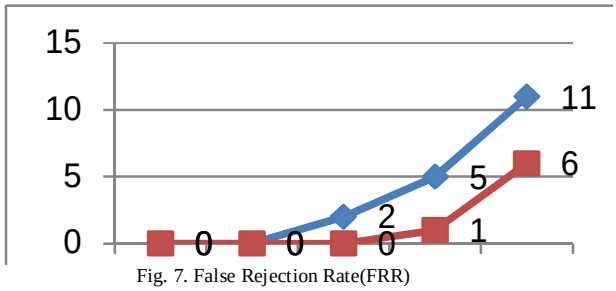

Fig. 7. False Rejection Rate(FRR)

The graph (Fig 7) has been drawn with X-axis as number of persons using the system and Y-axis as number of persons who are falsely rejected(FRR).From this result we can conclude that the FRR of existing system is 0.11 and of proposed system is 0.06.

The above two graphs depict the false acceptance rate and false rejection rate of existing and proposed system. It is concluded that the FAR and FRR of proposed system is less than existing system and hence the proposed (our) systems outperforms the existing system.

As security has concern our proposed system is more secure than the existing system with double encryption , the proposed work won't reveal any plain biometric details in the network as well as in the server's database. One more encryption will give additional layer of security.

IV.CONCLUSION AND FUTURE WORK

The main advantage of the proposed system involves two level security and accuracy. Very strong encryption schemes have been used in order to provide more security. The accuracy can be achieved by means of matching algorithms. In our system we used dynamic warping based matching and variable length features of finger print.

The proposed work is extremely secure under a variety of attacks and it can be used in various biometric traits. In future it can be applied to other biometrics like iris, palm print, face recognition systems. It can also be implemented with any other strong cryptographic algorithms.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1,pp. 4–20, Jan. 2004.
[2] Book Understanding biometrics from http://www.griaulebiometrics.com.
[3] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol.40, no. 3, pp. 614–634, Mar. 2001.
[4] in *Proc. Worshop on Biometrics (CVPR)*, Anchorage, AK, 2006, 07.

[5] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no.2, pp. 120–126, 1978.
[6] C. Fontaine and F. Galand, "A survey of homomorphic encryption for nonspecialists," *EURASIP*, vol. 1, pp. 1–15, 2007.
[7] C. Gentry, "Fully homomorphic encryption using ideal lattices," *STOC*, pp. 169–178, 2009.
[8] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security,"*EURASIP*, vol. 8, no. 2, pp. 1–17, 2008.
[9] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar," Efficient biometric verification in the encrypted domain," in *3rd Int.Conf. Biometrics*, Jun. 2009, pp. 906–915.
[10] test data used from *Biometrics ideal test* website with the URL of http://biometrics.idealtest.org.
[11] http://www.natlawreview.com/article/israeli-biometric-data-hacked.
[12]http://www.theinquirer.net/inquirer/news/1009515/british-biometric-passport-hacked

AUTHORS PROFILE

(1)Author S. Kavin Hari Hara Sudhan is an M.Tech student in computer science & engineering, Dr.MGR University, Chennai, Tamil Nadu, India. He has published 1 paper in international conference and 2 papers in national conferences. He shall be contacted through mailmekavin.s@gmail.com

(2)Author, S. Ramamoorthy, is a Professor in Computer Science & Engineering Department, Dr. MGR University, Chennai, Tamil Nadu, India. He has published more than 10 papers in National Conference , 3 papers in International Conference and 5 papers in International Journals. He shall be contacted through srm24071959@yahoo.com