K.Sekar *et al*, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 12, December- 2017, pg. 14-20 **ISSN: 2321-8363**
Impact Factor: 5.515

Identity and Authentication Using Fingerprint Biometrics MJ_2-RSA Cryptosystem in Health Care System

K.Sekar[1], M.Padmavathamma[2]
[1]Research Scholar, Dept. of CS, S.V.U. College of CMCS, S.V.Universtiy, Tirupati, A.P, INDIA
[2]Professor, Dept. of CS, S.V.U. College of CMCS, S.V.Universtiy, Tirupati, A.P, INDIA
[1] konetisekar1974@gmail.com, [2] prof.padma@yahoo.com

Abstract: ***The Identity and authentication use most import section in the Health care system. Biometric feature such as fingerprint can provide the uniqueness factor, whereas randomness can be induced using different combinations of fingerprints. We propose a technique to generate the asymmetric key pair (for MJ_2-RSA) by making use of combination of fingerprints. Identity will endorse the user's accessibility of the data.***

Keywords: Biometrics, Cryptography, Fingerprints, Key Generation, Identity, Authentication

1. Introduction

In recent years, the growth of the communication technologies has increased in exponential rate and these data is shared in the publicly shared media. The main problem is to protect our data in a unique way that could only be worked upon by the sender and the recipient. As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is mainly, to protect e-mail messages, credit card information, and corporate data. Traditional techniques that are probably in-use today, emphasizes on keys that are generated by generic function, algorithms or in random key generators. But the query is whether this key is unique and authentic in nature. More than how can these keys be unique to one and one person only? The answer to this would be Biometric Cryptosystems.

Biometric identifiers are categorized into two distinct types: physiological and behavioural characteristics. Biometrics technology is an approach to positively identify a person's identity using physiological characteristics including fingerprint, face recognition, palm vein, retina and iris recognition. Behavioural biometrics assesses uniquely identifying and measurable patterns of human traits, including characteristics like voice, gait and typing rhythms. Biometrics input or data is typically processed using an algorithm to identify data-specific points entered into a scanner where biometrics information is translated to match the data points, hence, giving authentication access for the user.

The newest members of the field of security is biometric cryptosystems. The important basis of this biometric cryptosystem depends on the fact that special features of human body are significantly unique to each and every human in the world, such as fingerprint, DNA sequence, Iris, etc. Based on those biometric we are able to generate an exclusive key that will be unique for each and every individual. Now using these generated keys we can encrypt our message without any afraid of attacks. Chance of there will be a matching keys also less because these keys are uniquely generated for individual persons. As we use MJ_2-RSA algorithm. Using this technique encrypted message to decrypting by eavesdropper or third unwanted parties have to acquire right set of keys which is more difficult case. This technique will give more secure feature for the data.

©2017, IJCSMA All Rights Reserved, www.ijcsma.com

In our research paper we categorized Enrolment, Identification, Authentication Control and Health solution using the bio-cryptography. In Enrolment phase user finger print will be collect, proceed and storied into the look-up table, passing these finger print data as parameter to the cryptosystem to generate the keys of the user's this is used as Identification phase in Authentication control phase will provide the access of system to the user's on the Authentication level.

In this paper we discussing a secure approach for the privacy protection of the biometric feature fingerprint in authentication system. Fingerprint recognition is an active research area. In many areas we are using fingerprint recognition to improve the security and privacy. In fingerprint recognition system the recognition can be done by fingerprint matching techniques. Fingerprint matching techniques are classified in two categories namely:- fingerprint verification and fingerprint identification. In this system we use fingerprint verification. Moreover fingerprint techniques have widespread applications in this era. In ancient days fingerprint matching was used extremely for forensic purposes and it performed manually by the human experts. Privacy Protection of fingerprint in authentication system is an important issue. Traditional encryption involves decryption and it required before the fingerprint matching so it is not sufficient for fingerprint privacy protection because which exposes the fingerprint to the attacker. Therefore, in recent years, significant efforts have been put into developing specific protection techniques for fingerprint. Most of the previous techniques make use of the key for the fingerprint privacy protection, which creates inconvenience. They may also be vulnerable when both the key and the protected fingerprint are stolen. In this system we use an idea of combining two fingerprints from two different fingers and generate a combination and stored in a database. This will be a virtual identity. Then apply conventional RSA method to the virtual identity to generate PKI keys. Using these keys store the information in a database. In authentication phase access is granted based on the matching

2. Literature Survey

In the recent decades biometric implementation is increased almost all the mobiles are using fingerprint and iris for authentication. Using fingerprint security will give more features to compare with other biometric like iris, voice etc., and also less expenses compare with others. Processing of fingerprint is easier to compare with other biometrics like iris, voice etc., so in our research work we are concentrating more on the fingerprint biometrics for securing the data.

Tab 1. Different methods of secure systems

Method	**Examples**	**Comments**
What you know	User ID, password, PIN	Can be forgotten Easily shared Many passwords are easy to guess
What you have	Cards, badges, keys	can be lost or stolen Easily shared Can be duplicated
What you know and what you have	ATM + PIN	PIN is a weak link Writing PIN on card Easily shared
What you are	Fingerprint, face, Voice …	Non-repudiable authentication

Using Bio-metric authentication will be more secure and also its non-reputable authentication compare to smart card, password and card and password system. In our research paper we are using fingerprint is using wide scope in our work.

Biometric will unique to a single identity. No two people can share the same biometrics data, Biometrics technology ensures authentication is performed on live identities cannot copied. It can't be shared

©2017, IJCSMA All Rights Reserved, www.ijcsma.com

Unique to the individual's physical characteristics and eliminates duplication. The main advantage of utilizing cryptography is its availability for high and adjustable security levels to access and manage data, resources and services. On the other hand biometrics brings in nonrepudiation and eradicates the necessity to memorize passwords or to carry tokens. Many researchers have worked and proposed new approaches to enhance performance of cryptographic key generated from biometrics in terms of security to abolish the requirement for key storage based on passwords.

The results of these researches and new approaches have endeavoured towards merging biometrics with cryptography, so as to increase overall systems security. Biometric Cryptosystems (BCS) indicates systems designed to securely bind a digital key to user biometric information or generate a digital key from a biometric trait.

3. Related Work

Recently, many researches and works have realized approaches on developing cryptographic key generation from biometric features and authenticating users by combining multiple biometric modalities.

Figure 1: finger print

In every human fingerprint there are certain patterns made due to ridges and valleys which are almost unique. The various patterns are ridge endings, ridge bifurcations, isolated points, deltas, pores, lakes, spurs and crossing points. In the proposed model we extract the features namely ridge bifurcation, ridge ending, crossing points and isolated points.

In our research work we categorized Enrolment, Identification, Access Control and Health solution using the bio-cryptography. In Enrolment phase user finger print will be collect, proceed and storied into the look-up table, passing these finger print data as parameter to the cryptosystem to generate the keys of the user's this is used as Identification phase in access control phase will provide the access of system to the user's on the access level.

Enrolment Phase: - In enrolment phase the user finger print will input for our cryptosystem Based on this extracted information and our proposed coding strategies, a combined minutiae template is generated and stored. In our model we will collect the 10 finger data and stored in the user's lookup table from f1, f2, f3, f4, f5,…f10 as bits, In those finger bits we are selecting randomly two finger bits are calculating new by prime number P and Q. Applying these P and Q in our MJ_2-RSA cryptosystem we are calculating the public and private keys to secure our data

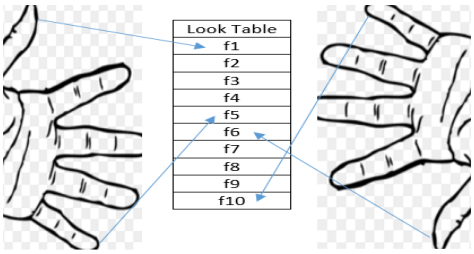

Figure 2: look table of finger print

©2017, IJCSMA All Rights Reserved, www.ijcsma.com

In our research work it is proposed to generate key, which uses a combination of fingerprints to generate the MJ2-RSA key. In our research work first phase will be the biometric data collection from the user's and those values are stored in the user's lookup (f1,…f10) table. In key generation phase user's finger's biometric are taken from the look table randomly and calculating the nearby prime numbers and providing these prime number to MJ2-RSA algorithm and calculating the public and private key. Using these key's we are securing the user's data from the intruder's to protecting the authorization and authentication.

3.1 Key Generation:

User's finger's lookup (f1,f2,…f10) table selecting randomly two finger's values from the lookup table i.e. f2 and f6 and calculating there nearby primes those are P and Q

Such that N = PQ.

Let K be an integer such that $1 \leq K \leq N$.

Compute $J_k(N) = N^k \prod_{P/N} (1-1/p^k)$ and consider

$\left(Z_{J_K}(N), +J_k(N), xJ_k(N)\right)$ a commutative ring with unity of order J_k (N) as a message space. Assign the numerical equivalents to the alphabets taken from $Z_{J_K}(N)$.

M is the message belongs to $Z_{J_K}(N)$.

Select a random integer e such that gcd (e, J_k (N)) = 1, where 1 < e <J_k (N)

E≡ M mod J_k (N) ∈ message space $Z_{J_K}(N)$

Select integer d such that ED ≡ 1 (mod J_k (N))

i.e., D = E^{-1}mod J_k (N) where $1 \leq D \leq J_k$ (N)

Public-Key PK = (E, J_k (N))
Private Key SK = (D, J_k (N))

Encryption: Given a public-key (J_k (N), E) and a message $M \in Z_{J_K}(N)$, compute the ciphertext

C = M^E mod J_k (N)

Decryption: Given a public-key (J_k (N), D) and ciphertext C, compute the message

M = C^D mod J_k (N)

©2017, IJCSMA All Rights Reserved, www.ijcsma.com

The correctness of J_k-RSA decryption is verified as follows

$C^D \bmod J_k(N) = (M^E)^D \bmod J_k(N) = (M^{ED} \bmod J_k(N)$

$= (ED).M \bmod J_k(N) = 1.M \bmod J_k(N)$

$= M$

4. Authentication

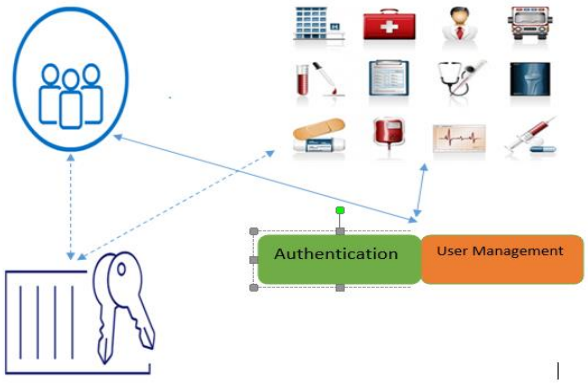

Figure 3: proposed model of Health Care system improvement

In our proposed model authentication phases verifies the user accessibility of the system and also the user management. Using authentication phase user can access the their respective Health Care data from the system which is shown in the fig.3 and also user's transaction, other actives such has finical transaction and communication authenticated with less efforts because biometric authentication cannot be copied. Along with User management user can manage their data accessibility with other parties such has internal/external hospitals. In our secure system will improve the user data access between the network hospitals and non-network hospitals

5. Conclusion

Generally multiple biometrics is used to generate the key. Using multiple biometric modalities needs multiple devices for feature acquisition. In our proposed system will provide the more secure and accessibility of the user data using finger print biometric along with MJ_2-RSA cryptosystem. The proposed model will provide the access management of the health care data and transaction

REFERENCES

[1] Abhishek Nagar and Santanu Chaudhary, Biometrics based Asymmetric Cryptosystem Design using Modified Fuzzy Vault Scheme, Proc. 18th International Conference on Pattern Recognition(ICPR-06), Hong Kong, Aug 20-24, 2006, 537-540,.

[2] R. K. Sharma, Generation of Biometric Key for Use in DES, IJCSI International Journal of Computer Science Issues, 9(6), 2012, 312-315.

[3] Umut Uludag, Sharath Pankanti, Salil Prabhakar and Anil K.Jain , Biometric Cryptosystems Issues and Challenges, Proceedings of the IEEE, 92(6), 2004, 948-960.

[4] P. Balakumar and R. Venkatesan, Secure Biometric Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris , IJCSI International Journal of Computer Science Issues, 8(5), 2011, 349-356.

[5] R.K. Nichols, Chapter 22, ICSA Guide to cryptography (McGraw Hill New York 1999), 649-675.

©2017, IJCSMA All Rights Reserved, www.ijcsma.com

[6] A. Jaya Lakshmi, I. Ramesh Babu, Design of security key Generation algorithm using Fingerprint based Biometric Modality, IOSR Journal of Engineering(IOSRJN), 2(2), 2012,325-330.
[7] Abhishek Nagar, Designing Biometrics-based Cryptosystem, Post-Graduate diss , Department of Mathematics, IIT Delhi- May 2006.
[8] R.Sesshadri and T.Raghu Trivedi, Efficient Cryptographic Key Generation using Biometrics, International journal of Computer Technology and Applications, 2(1), , 182-187,
[9] A Jagadeesan and Dr K.Duraiswamy , Secured Cryptographic key generation from multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris, International Journal of Computer Science and Information Security, 7(1), 2010, 296-305.
[10] Rivest, R.; Shamir, A.; Adleman, L., A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21 (2), 1978, 120-126.
[11] A, Juels and M. Sudan, A Fuzzy vault scheme, Proc. IEEE International Symposium for Information Theory. A Lapidoth and E. Teletar, Eds., 2002, 408.
[12] W. Stallings, Cryptography and Network Security: Principles and Practices(Edn. 4).
[13] Bashar Ne'ma and Hamza Ali, Multi-Purpose Code Generation Using Fingerprint Images, The International Arab Journal of Information Technology, 6(4), 2009, 418-423.
[14] Praveen Namburu, A Study on Fingerprint Image Enhancement And Minutiae Extraction Techniques, Post Graduate diss, Department of Computer Science and Engineering, National Institute of Technology, Rourkela, 2007.
[15] R.Sesshadri and T.Raghu Trivedi, Generate a key for MAC Algorithm using Biometric Fingerprint, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) ,1(4), 2010, 38-45.
[16] Roli Bansal, Priti Sehgal and Punam Bedi, Minutiae Extraction from Fingerprint Images - a Review, IJCSI International Journal of Computer Science Issues, 8(5), 2011, 74-85.
[17] Kamini H Solanki, Chandni Patel, "Biometric Key Generation In Digital Signature Of Asymmetric Key Cryptographic To Enhance Security Of Digital Data", International Journal of Engineering Research & Technology (IJERT), Vol. 2, Issue 2, pp. 1-8, Feb.2013.
[18] Dr. Manish Manoria, Ajit Kumar Shrivastava, Satyendra Singh Thakur, DebuSinha, "Exploring the Prospect of Secure BiometricCryptosystem using RSA for Blind Authentication", International Journal of Wisdom Based Computing, Vol. 1 (2), pp. 24-27, August 2011.
[19] Priyanka Patel, "Secure Fingerprint Identification System and Matching by UsingImage Registration and Key Matching Techniques", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 6, pp. 2012-2017, June 2013.
[20] A. Jaya Lakshmi, I. Ramesh Babu, "Design of Secured Key Generation Algorithm using Fingerprint Based Biometric Modality", IOSR Journal of Engineering (IOSRJEN), Vol. 2 Issue 2, pp. 325-330, Feb. 2012.

[1]**Mr.K.Sekar(Koneti Sekar)** obtained his Bachelor Degree in Computer Science from Sri Venkateswara University. The he obtained his Masters Degree from University of Madras and pursuing Ph.D in Sri Venkateswara University. Currently He is an Associate Professor working in the Department of Computer Science and Engineering, S.V.Engineering College for Women, Tirupati. His Specializations include Software Engineering, Computer Programming, Computer Security, Computer Organization and Object Oriented Programming.

©2017, IJCSMA All Rights Reserved, www.ijcsma.com

[2]**Prof.M.Padmavathamma(Mokkala Padmavathamma)** born in Chittoor District,A.P., India, in 1963. She received M.Sc , M.Phil,M.Ed,Ph.D from S.V.University, Tirupathi and M.S(Software Systems) from BITS PILANI. Currently she is working as Head, Department of computer science, S.V. University, Andhra Pradesh, India. Her research interests lie in the areas of Number theory, Cryptography, Network Security, Distributed Systems and Data Mining. She has published 35 research papers in national/International journals and conferences. She published TWO text books as one of the author. Also she is life member of cryptology Research Society of India (CRSI) and Andhra Pradesh Association Mathematical Teachers (APAMT).

©2017, IJCSMA All Rights Reserved, www.ijcsma.com