Journal of Theoretical and Applied Information Technology
30th April 2014. Vol. 62 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SECURE BIOMETRIC BASED APPROACH FOR PROVIDING SECURITY SERVICES IN RESOURCE-AWARE DISTRIBUTED COMPUTING ENVIRONMENT

[1]T. HEMALATHA, [2]G. ATHISHA

[1]Associate Professor, Department of Computer Science & Engg, P.S.N.A. College of Engineering and Technology, Dindigul

[2]Professor, Department of ECE, P.S.N.A. College of Engineering and Technology, Dindigul

E-mail: [1]hemashek@yahoo.com, [2]gathisha@yahoo.com

ABSTRACT

In recent years there is a need for a security infrastructure for our ubiquitous digital life without using Public key infrastructure and shared session key cryptography algorithms. Since the system scales up, the peer to peer approach is attractive to Distributed Computing Environment due to increase in large amount of resources. The resources in such environment possess different characteristics. The need for security services for such resource restricted environment is a challenging issue. Hence, in this paper a novel algorithm is proposed that uses the macro feature of the fingerprint biometric of the sender and the receiver to generate key(s). The proposed technique provides different security services like Authentication, Non repudiation and Confidentiality. In this work a novel key generation algorithm is proposed to generate unique set of keys by using both sender and receiver's fingerprint biometrics. These keys are shared between the sender and the receiver by using the underlying concrete S-MIME protocol. Several samples are collected and the macro features are extracted using Finger print feature extraction algorithm. Out of 'n' ridges, a ridge is selected and plotted on the x-y axis. Plotting is done as per the sender's choice. A set of points are selected and the key is generated. The proposed algorithm is implemented in C# DotNet and MATLAB and the results are tested and verified by taking a set of samples. The results of the proposed algorithm are compared with the existing PKI based algorithm with respect to the encryption time, decryption time and memory required.

Keywords: *Biometric, Finger Print, Key Generation, Security, Ubiquitous*

1. INTRODUCTION

Everywhere in internet we are in need of authenticity. It is a process in which one entity called the claimant proves its identity to another entity called the prover. Entity authentication technique tends to prevent impersonation of an entity by an intruder. Systems and Applications should be accessed only by legitimate users. The objective of any authentication technique is to acquire reasonable assertion that the identity declared at the identification stage belong to the party in communication. The user authentication depends on various methods available of which there are three main methods viz. by using a password or pass phrase, by using a token or by using a measurable trait. The simplest mechanism by which one can authenticate is by the use of passwords. Passwords have several problems viz. they can be stolen or it may be written in some easily accessible locations or it may be shared or guessed. Passwords should satisfy the strong password policy and it should not hold true for any of the characteristics of weak password policy. This scheme is fixed and time-invariant. It is known as weak authentication scheme. Besides it is unique and the user is required to possess an authenticating token. A token is generally issued to a user is registered when it is presented initially for authentication. The token is verified for its legitimacy. The identifying label of the token is used to verify its registration. These tokens fall into two categories. a. Storage token b. Dynamic Token. Storage tokens are generally made up of smart cards and USB (Universal Serial Bus) tokens. But the problem with the storage token is that anyone in possession of it can use it or if the token is lost or stolen still entry can be gained. But still passwords can be employed with tokens to prevent from such happening. This multifactor authentication method has the weakness of both token and associated password can be loaned or stolen. Dynamic tokens

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

are used to generate a one-time authentication code. This code can act as a challenge. The dynamic token is not sufficient for authentication. Hence, it must be used in conjunction with a password which is inconvenient for the user to adapt this approach. But, we are in need of strong authentication schemes in certain applications. Strong authentication is the use of two or more different authentication methods such as smart card and a pin or a password and a form of biometrics such as fingerprint or a retina scan [21]. Some applications use Public key techniques in the form of Challenge-response authentication. Storage tokens are often used in conjunction with digital certificates. The certificates are stored within the token and further it is used for authentication. It is called certificate based login which is used in windows 2000 and XP or in a Kerberos environment for granting an access ticket.

Computing devices are becoming ubiquitous in our daily lives. The rapid decrease in the size and cost coupled with increase in capability has enabled a rapid proliferation of small and very capable devices into our daily lives. As these devices become better connected, we have the basic building blocks of smart environments available [4]. Such ubiquitous computing environment raises more constraints and challenges since they are populated with heterogeneous devices and providers. Achieving high security between two principals poses greater challenges in heterogeneity and variable connectivity [6]. Every application accessed in such environment needs to be authenticated and the messages that we communicate between two entities needs to be secured. The rapid deployment of the internet application has led to cropping up of various challenges to meet the current growing demands and as a result we are in need of newer protocols, algorithms and methods to enhance the Quality of Service in various environments. PKI (Public Key Infrastructure) is suitable only for a well structured and trusted environment like specific community. But it is inefficient and ineffective to support secure transactions in an open, dynamic and ad-hoc environment [8]. In ubiquitous environments, there is a need to access the internet for performing various operations in a secured manner. Since ubiquitous environments are populated with heterogeneous devices and providers, the possibility of achieving high security between two principals poses high challenges because of variable connectivity and heterogeneity [2]. There is a challenge in handling the keys in such situations and to depend on huge computational power and memory which is not available everywhere in such environments. PKI technology is too hard for end-users in such environment.

The proliferation of camera-equipped mobile phones presents a powerful platform that can be leveraged to conveniently provide strong authentication between devices that share no prior context, without the assistance of a trusted authority. Adrian Perrig and Mike Reiter explored applications for Seeing-is-Believing (SiB), a system that utilizes machine vision on camera-phones to achieve security properties formerly unattainable in a non-intrusive way. Secure Key Setup between Ubiquitous Devices is done. This research leverages the human-verifiable visible channel to transfer legitimate keys to remote devices [3]. The past five years have seen a significant growth in biometric research resulting in the development of innovative sensors, robust and efficient algorithm and novel applications [13]. In addition biometric cryptosystems provide mechanisms for generating biometric dependent key [9].

Our objective is to propose a novel algorithm for Key generation using finger print of the principals involved in peer to peer communication. In addition we have proposed novel algorithm for providing security services like Secrecy/Confidentiality and integrity without relying upon existing Cryptography Protocols and Public Key Infrastructure.

The rest of the paper is organized as follows. Section 2 describes the analysis of existing cryptographic mechanisms and section 3 describes the classification of biometrics and Macro features of fingerprint. Section 4 and 5 presents the proposed algorithm for key generation, Encryption and decryption and performance analysis of the proposed algorithm.

2. COMMON CRYPTOGRAPHIC TECHNIQUES

There are several common Symmetric and asymmetric cryptographic techniques, which are used in internet applications for authentication and secured transmission of messages. The most popular among them are Advanced Encryption Standard (AES), Digital Signature Algorithm (DSA), Rivest Shamir Adleman (RSA), Elliptic Curve and Diffie Hellman (DH) algorithms. The third party authentication service use Secure Socket Layer (SSL) certificates for authentication and such

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

certificates rely on encryption is using Public and private keys based on the RSA algorithm.

2.1. Analysis of Public Key Cryptography

Many of the Public key cryptosystem algorithms are complicated that they are based on the apparent difficulty of solving certain computational problems that require large number of computational cycles to convert the plain text to cipher text [1]. The Public key protocols have a serious drawback in the sense they are slower than the secret key counterpart. If a huge amount of data is to be encrypted or decrypted, it significantly becomes slower compared to the symmetric key cryptosystem. In certain situations and in specific devices one cannot always use these computationally intensive algorithms to provide the following security services like Authentication and Confidentiality, since there are still several open issues about interoperability between PKI's operated by different organization and predominant use of Certificate Revocation List (CRL). The CRL makes the system not scalable because of inherent drawbacks. They are

- Since CRL is a large document, the latency incurred in delivering the recent CRL is considerable.
- The revocation is not notified reliably to systems until all issued CRLs are updated completely.
- Does not provide any real time information about the validity of Certificates
- Distribution and checking is time and resource consuming.
- Extremely vulnerable to Denial of Service attacks.
- Maintaining fresh CRLs increases very high load for servers which distribute them to the clients

3. FINGER PRINT BIOMETRIC

3.1. Biometrics

Biometric technology drives the future direction of strong authentication. Like any technology it needs time to mature and find its place in the computing infrastructure of enterprises. Biometrics is being put to work from replacing the need for Password authentication to strongly binding the physical and digital identities. Biometrics is ready for use and can make the internet computing environment more secure [7].

Biometrics can be seen as a Privacy-enabling technology. The third method of authentication is by using Measurable Trait. Biometric is a physical trait which can be reliably measured. Every user always possesses the physical trait which cannot be stolen, loaned or guessed and it is hard to subject it to brute force attack. Hence biometrics can be used for authentication. The three modalities in the biometrics field are Finger print, face and iris [18]. In most of the real time applications the Biometric systems are used in one of two modes verification or identification. Verification is used to verify a person's identity and identification is used to determine who a person is. Biometric decision making is generally very fast since the process is well automated and in most of the cases it takes only few seconds in real time [22].

In this work in addition to these two modes we have proposed a novel key generation algorithm that generate key based on either the sender or receiver or both fingerprint biometric macro feature. The generated key is used to provide Authentication and Confidentiality. The binary strings can be extracted from biometrics and this opens up several applications where a strong binding is required between a person and cryptographic operations [16].

Biometrics can be defined by the level of involvement the user needs to provide which can be geometrically measured. The biometric system falls into two categories. Based on the user involvement, they are Active biometrics and Passive biometrics. An active biometric requires the user to actively submit to measurement. This type of system is known as Overt. Active biometrics is used in the applications that authenticate User's identity. Examples are Fingerprint, Hand Geometry, Iris scanning and Retinal Scanning. They are not much environmentally dependent and high level of certainty can be attained to the User's identity.

Passive Biometrics does not require the user to actively submit to measurement. These types of systems are generally called Covert. Examples of such are Face, voice and Gait which are generally used in the surveillance applications. Since these are influenced by the environment, they are more suitable for identification system and not for authentication systems. A good biometric is defined in terms of User acceptance, Ease of use, Technology costs, Deploy ability, Invasiveness of technology, Maturity of technology and Time it takes for the user to get habituated. Out of all the above quantifiable measurements, the user acceptance requires the most analysis. Based on the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

characteristics of good biometric, Fingerprint is chosen in this paper for further work.

In our work, we have selected the Active Biometric Fingerprint as a source for achieving security services like Authentication, Confidentiality and non repudiation. In this paper we have proposed an algorithm for Key generation, Encryption and Decryption by using Sender's fingerprint biometric and Receiver's fingerprint biometric. We can use this proposed algorithm both for One-way authentication and Mutual authentication between two principals. The macro feature Ridge Patterns are used for generating keys at both sides. Then the generated keys are shared mutually between the sender and receiver through S-MIME. These keys are used for generating Session keys. The session key is used for securing messages which is sent across the public channel.

3.2. General Description of Fingerprints

Fingerprints are identified by both macro and micro features. The macro features are ridge patterns, ridge pattern area, core point, delta point, type lines and ridge count. The micro features are made up of Minutia Points. The minutia points are classified by Type, Orientation, Spatial frequency, Curvature and Position. In this proposed work we have used the Macro feature Ridge Pattern. They are large in size which can be seen by unaided human eye. The most visible feature is ridge pattern. Ridge patterns are further classified into Arch, Loop and Whorl. Arches are open curves which account for approximately five percent of the ridge pattern. Arches are further classified into tented arch in which the arch angle is much more obtuse than in a normal arch. Approximately loops are 60% of the ridge patterns. Loops may slant left or right or be presented as a double loop. A double loop has both a left and a right loop conforming to each outer outline. Whorls account for thirty five percent of the ridge patterns. They are defined by at least one ridge making a complete circle. Ridge pattern area is the area in the print where all the macro features are found. It is the diverging ridge flows that form a delta. Core points are found at the centre of the finger print image. It may or may not correspond to the centre of ridge pattern area. It is used as a reference point for measuring other minutia and also during classification. Delta point is a definite fixed point used to facilitate ridge counting and tracing. The type lines are the two parallel innermost ridges that define the ridge pattern area. Ridge count is the number of ridges that intersect a line drawn from delta to core. The features which cannot be seen by unaided human eye are called micro features.

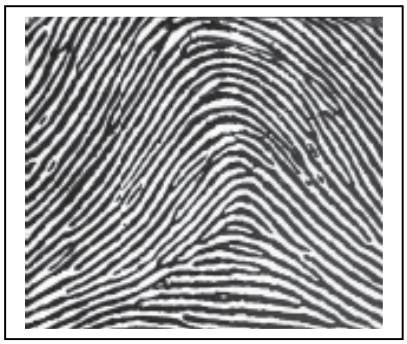

Figure 1: Sample Fingerprint Image with Macro Feature

3.3. General Description of Fingerprints

In the secret key cryptosystem if the keys are lost or stolen then it cannot provide non-repudiation. It consumes lot of memory and CPU time to provide Confidentiality, integrity and non-repudiation to the end user. C. Rathgeb and A. Uhl described a comprehensive survey of biometric cryptosystems and cancellable biometrics and presented an outlook to the future prospects [9].

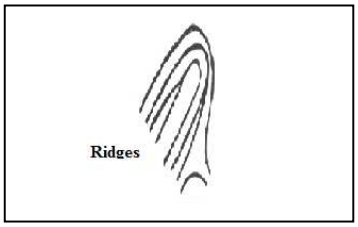

Figure 2: Ridges in the Fingerprint

Cavoukian and Alex explained about the method of Biometric encryption. It is a process that securely binds a digital key to a biometric. Biometric encryption is related to cancelable biometrics which is a privacy enhancing technology [11].

Biometric Cryptosystems (BCSs) are designed to securely bind a digital key to a biometric or generate a digital key from a biometric. In such systems the biometrics are stored in a database [21]. Cancelable Biometrics is a way to incorporate protection and the replacement features into biometrics. It performs distortion of the biometric image or features and the variability in the distortion parameters provides the cancellable nature of the scheme [22]. The BCSs require helper data to retrieve or generate keys. Helper data is biometric dependent public information which is stored in a separate central database. The helper data is derived separately by using Fuzzy Extractors [12]. This mechanism is more vulnerable to conduct attacks since the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

biometric templates and keys are stored separately in plain form. In this proposed work the sender's and receiver's biometric are not stored in the database. It is acquired only at the initiation phase of key generation.

4. PROPOSED SYSTEM

We have developed a novel algorithm for providing security services like authentication and confidentiality using Finger Print of either the Sender or Receiver or both called Finger Print based Security Algorithm (FPSA). In this work we have collected the data set of around 135 individuals and used it for analysis of the Ridges and Ridge count. The proposed algorithm consists of two phases. They are Key generation phase and Encryption / Decryption phase. The notations used in this paper are summarized in table 2 which is given at the end of the references.

4.1. FPSA Key Generation

The macro feature of a fingerprint minutia is used for generating keys on-demand by the sender process. Data acquisition of the sender's fingerprint is performed. Then enhance the image and minutiae are detected on the enhanced image using MINDTCT algorithm. It is a minutia detector algorithm which automatically locates and records ridge bifurcations and ending in a fingerprint image.

In this work out of 'n' samples two principals left thumb fingerprint are selected as a source for key generation. We can use any one of the fingerprint out of 10 fingers. Ridges are used for generating keys in this stage. In order to handle the noise that is captured during data acquisition phase pre processing is done on the captured image. The phases involved in this stage are a. Noise Removal and Feature extraction (Image processing) b. Selection of a ridge pattern from the processed image c. plotting the selection (made in step 2) in X-Y axis which is shown in Fig. 3 and Fig. 4.

Steps:

1. Capture the Finger print image using Finger print Acquisition device.

2. Process the Finger Print image using MINDTCT algorithm.

3. Select any one ridge from the processed image.

4. Plot the ridge in X-Y axis.

5. Select a point or set of points randomly on the ridge and extract the corresponding (x, y) coordinates from the corresponding location or locations.

6. Let the coordinates be named GP(x, y). It is a global public element which is to be shared between the sender and the intended receiver in one-to-one secure communication.

7. Save global public element GP(x, y) in the most secured location at the sender side.

8. Share the global public element GP(x, y) using S-MIME (Secured - Multipurpose Internet Mail Extension).

9. If the principals are willing to communicate through Mutual authentication repeat the steps 1 – 8 for Receiver's finger print ridge feature.

4.1.1. FPSA Key Generation – version 1

Input: A Processed Finger Print Image of the Sender / Receiver

Output: GP(x, y) → Global Public Element which is shared only by the Sender and the Receiver.

Steps: @ Sender Side and Receiver Side

1. Select a Ridge from the Input Finger Print Image

2. Plot the ridge in X-Y Axis

3. Pick a random point on the selected ridge (X, Y). Let it be Global Public Element - GP(x, y)

4. Return the Pair of Co-ordinates as the Secret Key. The macro feature of a fingerprint minutia is used for generating

4.1.2. FPSA Key Generation – version 2

Input: A Processed Finger Print Image of the Sender / Receiver

Output: An array of size 'n' rows and 2 columns. Set of points are selected randomly and the corresponding X-Y coordinates are stored.

Steps: @ Sender Side and Receiver Side

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1. Select a Ridge from the Input Finger Print Image

2. Plot the ridge in X-Y Axis

3. Pick a set of 'm' random points (X, Y) on the selected Ridge and store the coordinates in a two Dimensional array. Let it be Global Public Element of sender and receiver – GPa[x][y] and GPb[x][y].

4. Return the Set of Pair of Co-ordinates as the Secret Key.

Assume Alice and Bob are the Principals involved in secured Communication. Let the Secret key of Sender and Receiver be GPa(x,y) and GPb(x,y). Sharing of the secret keys between Alice and Bob GPa(x,y) and GPb(x,y) is performed by using S-MIME.

4.2. FPSA Session Key Generation

Session key is generated both at the sender side as well as at the receiver side. This is implemented in two ways. In the first only a pair of coordinate is selected as a secret key by both the sender and the receiver. In second a set of 'n' points are randomly selected from the selected principal's ridge feature where n = 2,…,m and these coordinates are used as a sub keys for encrypting long messages.

Steps:
1. Read Pa(x) & Pb(x)
2. Read Pa(y) & Pb(y)
3. Compute x = Pa(x) + Pb(x)
4. Compute y = Pa(y) + Pb(y)
5. Return Ks(x, y)

Input: GPa(x,y)and GPb(x,y) (Sub Keys Generation)
Steps:
1. for i=1,…,m
2. { Read Pa(x) & Pb(x)
4. Read Pa(y) & Pb(y)
5. Compute x = Pa(x) + Pb(x)
6. Compute y = Pa(y) + Pb(y)}
7. Return Ks[x][y]

4.3. FPSA Encryption

The proposed algorithm is a block cipher which processes the message in the form of blocks. In this work we have used the IEEE set of standards for converting data between various logical formats. A message which has to be protected from malicious users has to be encrypted. Such messages consist of either Human-readable text or numbers or keys of Secret key cryptographic protocols or combination of any of the above. Hence it is mandatory to convert such messages to bit strings before the cryptographic algorithm is applied. We have used the following IEEE standards in order to operate on data of various types and to enhance interoperability there by it facilitates simplicity in handling data. It also removes ambiguity and improves applicability and acceptability of the proposed algorithm. IEEE draft P1363 and P1363.1 are specific algorithms for converting data among the various format of which we have used BS2OS (Bit String to Octet String), OS2BS (Octet String to Bit String), I2BS and BS2I.

Algorithm: BS2OS
1. A bit string is broken up in to 8 Bits
2. If (Length [input_bit_string] mod 8 == 0)
3. Pack it into Octets
4. Else
5. Do Padding (n)

Algorithm: Padding(n)

1. Compute l = length[input_bit_string]
2. Compute r = l MOD 8
3. Zero bits should be added to the left of the input_bit_string.

Algorithm: OS2BS
1. if(Length[input_Octet _string] ! = multiples of 8)
2. ERROR; BREAK;
3. else
4. Check the left most 'r' bits
5. if(r bits != 0) then
6. REPORT ERROR;
7. else
8. remove the left most 'r' bits

return [BS]

4.3.1. FPSA Encryption using Single Key

Input: Session Key Ks(x, y), Plain Text Message {m = m1, m2… mr / where each mi is bit strength of length 8}
Output: The Cipher text message {c = c1, c2… cr where each ci is bit strength of length 8}
Steps:
Call BS2OS(Message)
for i = 1,…,r
{
$c_i = m_i \oplus x$ }

4.3.2. FPSA Encryption using set of Sub Keys

Input: Session Key Ks[x][y], Plain Text Message {m = m1, m2… mr where each mi is a bit strength of length 8}

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Output: The Cipher text message {c = c1, c2… cr where each ci is a bit strength of length 8}
Steps:
Call BS2OS(Message)
// let us assume that there are 'l' equal sized blocks of Plain Text and 'n' sub keys in the Key array Ks[x][y].
for n = 1,…,l
for i = 0,…,n-1
for j = 0,…,1
{ $C_n = m_n \oplus Ks[i][j]$ }

4.4. FPSA Decryption

4.4.1. FPSA Decryption using Single Key

Input: Session Key Ks(x, y), Cipher Text Message {m = m1, m2,…,mr where each mi is a bit strength of length 8}
Output: The Plain text message {c = c1, c2,…,cr where each ci is a bit strength of length 8}
Steps:
Call OS2BS(Message)
for i = 1,…,r
{
$m_i = c_i \oplus x$ }

4.4.2. FPSA Decryption using Set of Sub Keys

Input: Session Key Ks[x][y], Cipher Text Message {c = c1, c2,…,cr }where each ci is a bit strength of length 8
Output: The Plain text message {m = m1,m2,…,mr} where each mi is a bit strength of length 8
Steps:
Call OS2BS(Message)
// let us assume that there are 'l' equal sized blocks of Cipher Text and 'n' sub keys in the Key array Ks[x][y].
for n = 1,…,l
for i = 0,…, n-1
for j = 0,…,1
{
$m_n = c_n \oplus Ks[i][j]$
}

5. ANALYSIS OF FPSA ALGORITHM

The proposed algorithm FPSA is implemented using C-Sharp in dot net environment. The finger print image obtained is processed by using MATLAB V7.5 and the results are stored in a file in the most secured location at the sender machine. Since finger print is used, it significantly contributes to the strength of authentication. The images acquisitioned at the time of authenticating to any application is processed using web services which was developed, tested and deployed in our experimental setup [20]. The finger print processing is performed and tested using Dynamic Web service based Image Processing System [20]. The performance and functionality of the proposed encryption scheme is compared with PKI Scheme. The existing algorithms that are designed to provide minimal security services consume more time and memory. In each step the number of operations involved is more and it requires lot of memory at runtime. Since the resources in any ubiquitous or DCE do not have sufficient memory and computational resources an alternate robust and simple mechanism for such resource constraint environment is needed. Since RSA is used in SSL encryption scheme, it is compared with FPSA encryption scheme. The parameters considered for analyzing the performance of the proposed algorithm with the existing algorithm are the time taken for key generation, Encryption and Decryption processes. These parameters are estimated and tabulated in table 1.

In any distributed computing environment where there is limited resource constraints and fewer infrastructures, this proposed algorithm is best suited. Hence Computational power, network latency and amount of memory needed are considered as major significant factors that decide the applicability of the proposed security services in which the computing environment has fewer infrastructures.

Table 1: Comparison between PKI scheme and Proposed Algorithm.

Metrics	PKI Model In ms	Proposed Algorithm in ms
Time Taken for Key Generation	NA	256ms
Time taken for Certificate validation with Certificate Authority (Certificate Acquisition is not considered)	532 ms	NA
Encryption Time	343 ms Using RSA (1024 bits)	143 ms
Decryption Time	493 ms Using RSA (1024 bits)	157 ms
Memory required	High	Low

NA – Not Applicable

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The complexity theory suggests that the provably difficult intractable problem cannot be used for building cryptographic protocols. There is a list of formal complexity classes where Class P forms the languages accepted by deterministic polynomial time Turing Machines and Class NP constitute languages accepted by non- deterministic polynomial time Turing Machines. It is always recommended to use only NP-Complete problems for building secure cryptosystem [1].

In this proposed algorithm every individual has 'n' no of ridges on an average as a macro feature which is unique among individuals. Probability of selecting a particular ridge Ri out of 'n' ridges increases the strength of this algorithm. Then plotting increases additional complexity and selecting a specific point Pi on the ridge Ri is infeasible thereby it increases the strength of the key. Since Key size is smaller it takes only less time to convert the Plain text and Cipher Text and vice versa. The proposed algorithm result is found to be capable enough to provide a cryptosystem with minimal set of security features authentication and confidentiality in a highly dynamic environment.

6. CONCLUSION

In this paper we proposed a Finger Print based Security Algorithm FPSA in which the principal's finger print biometric is used for key generation. Authentication, Confidentiality and non-repudiation can be achieved with the smaller key size without any overhead. This algorithm can be used in smaller and resource limited devices. It serves as a model of trust by using biometric based identity of the users. The proposed algorithm can be further modified to provide integrity security service for such highly dynamic environment where there is less memory. But for large enterprise applications which covers a wide area this mechanism is not suffice. It can be combined with the existing TLS/SSL mechanism in order to add one more level of security. The proposed algorithm can be extended by including multimodal biometrics where authentication is more important than the time involved and additional complexity in key generation algorithm. The algorithm can be further enhanced to generate one time password. The proposed algorithm is best suited for resource constrained DCE.

REFRENCES:

[1] Abhijit Das and C.E. Veni Madhavan, Public-Key Cryptography Theory and Practice, South Asia: Pearson Education, 2009.

[2] Middleware Technologies for Ubiquitous Computing Noha Ibrahim, Frédéric Le Mouël and Stéphane Frénot University of Lyon, INRIA INSA-Lyon, CITI, France DOI: 10.4018/978-1-60566-250-3.ch012

[3] David Garlan, David O'Hallaron, et. al., "Mobile and Pervasive Computing Research", Department of Computer Science, CMU, http://www.csd.cs.cmu.edu/research/areas/mopercomp/

[4] Narendar Shankar, William A. Arbaugh, "On Trust for Ubiquitous Computing" work sponsored by a Critical Infrastructure Protection Grant from the National Institute of Standards and by Fujitsu Labs America, DOI: 10.1.1.20.1375

[5] Kagal, L. Finin, T. Joshi, A., "Trust-based security in pervasive computing environments" Maryland Univ., Baltimore, MD, in IEEE Computers, : Dec 2001, Volume: 34, Issue: 12 On page(s): 154-157, DOI:10.1109/2.970591.

[6]. J. Roshan K. Thomas Ravi Sandhu McAfee Research, Network Associates, Inc. George Mason University and NSD Secuity "Models, Protocols, and Architectures for Secure Pervasive Computing: Challenges and Research Directions (Position Paper) Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW'04) 0-7695-2106-1/04, 2004U.

[7] Guide to Biometrics, Bolle et al., Springer Verlag, 2003

[8] Peter Guttmxan "PKI It's not Dead just Resting", IEEE Computer August 2002 Vol.35, issue 8 DOI: 10.1109/MC.2002.1023787, Pages 41-49.

[9] Christian Rathgeb and Andreas Uhl "A Survey on biometric cryptosystems and cancelable biometrics" EURASIP Journal on Information Security 2011, 2011:3 A Springer Open Journal doi:10.1186/1687-417X-2011-3 Issue 1.

[10] Uludag U, Pankanti S, Prabhakar S, Jain AK: "Biometric cryptosystems: issues and challenges". Proc IEEE June 2004, 92(6): 948-960.

[11] Cavoukian A, Stoianov A: "Biometric encryption. Encyclopedia of Biometrics"Springer; 2009

[12] Dodis Y, Ostrovsky R, Reyzin L, Smith A: "Fuzzy Extractors: How to Generate Strong

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Keys from Biometrics and Other Noisy Data" Proc Eurocrypt 2004, 2004:523-540, (LNCS: 3027)

[13] Jain AK, Flynn PJ, Ross AA: "Handbook of Biometrics". Springer US; Boston, MA. 2008

[14] Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BV: "Biometric Encryption", ICSA Guide to Cryptography. 1999

[15] Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BV: "Method for Secure Key Management using a Biometrics". US Patent 2001, 6219794.

[16] Hao F, Anderson R, Daugman J: "Combining cryptography with biometrics effectively". IEEE Trans Computing 2006, 55(9):1081-1088

[17] Nandakumar K: "A fingerprint cryptosystem based on minutiae phase spectrum". Proc of IEEE Workshop on Information Forensics and Security (WIFS) 2010

[18] Jain, Anil K., Ross, Arun A., Nandakumar, Karthik "Introduction to Biometrics" 2011, XVI, 311p, ISBN 978-0-387-77326-1.

[19] Jain AK, Ross A, Prabhakar S: "An introduction to biometric recognition". IEEE Trans Circ Syst Video Technol 2004, 14:4-20

[20] Hemalatha, T., Athisha, G., Jeyanthi, S. "Dynamic Web Service Based Image Processing System" 16th IEEE International Conference on Advanced Computing and Communications, 2008. ADCOM 2008. Digital Object Identifier: 10.1109/ADCOM.2008.4760468 Page(s):323-328.

[21] [Online] cryptome.org/2013/09/infosecurity-cert.pdf[22] [Online] www.gao.gov/new.items/d031137t.pdf

Journal of Theoretical and Applied Information Technology
30th April 2014. Vol. 62 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

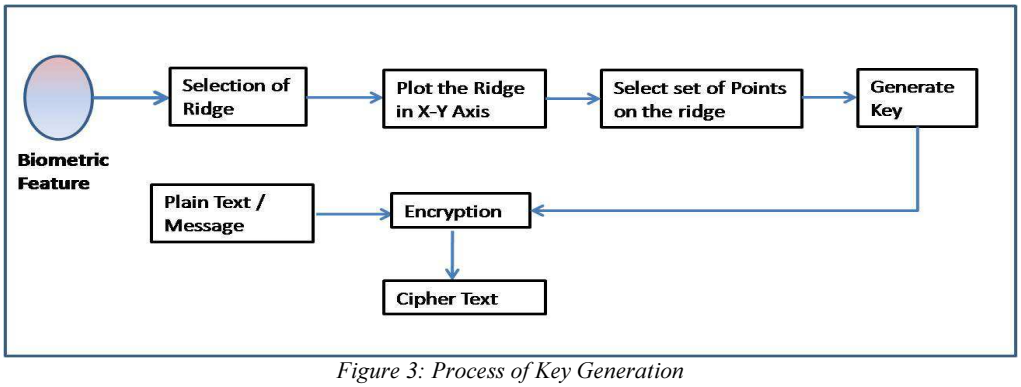

Figure 3: Process of Key Generation

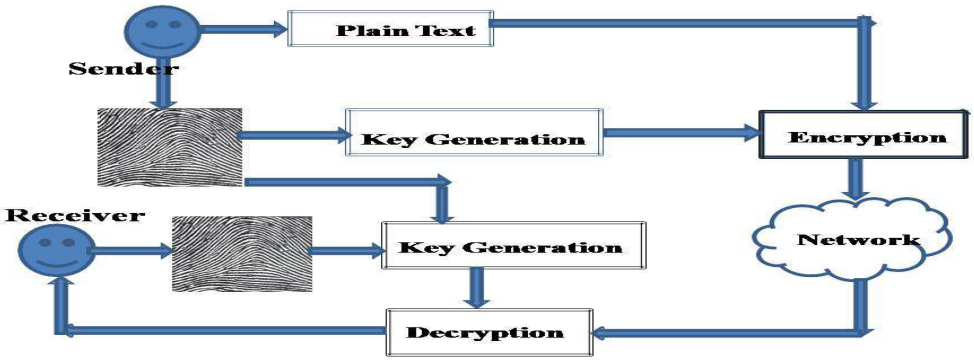

Figure 4: Message Composition and Key Generation & Exchange Scenario

Table 2: Nomenclatures used in this Paper.

Nomenclatures	
GP(x, y)	Global Public Element
P(x,y)	A Point 'P' on the plotted ridge is represented by two elements the 'x' coordinate of 'P' and the 'y' coordinate of 'P'
$GP_a[x][y]$	Global Public Element of Entity 'a'
$GP_b[x][y]$	Global Public Element of Entity 'b'
$P_a[x]$, $P_b[x]$	'x' Component of the Public Element of the Sender 'a' and Receiver 'b'
$P_a[y]$, $P_b[y]$	'y' Component of the Public Element of the Sender 'a' and Receiver 'b'
$K_s(x,y)$	Secret Key Computed by the sender and Receiver
BS2OS	Converts a bit string as an octet string. Do padding enough zeroes 'n' the left to make the number of bits a multiple of 8, and then breaks it up into octets. A bit string $b_{l-1}\ b_{l-2} \ldots b_0$ of length l shall be converted to an octet string $M_{d-1}\ M_{d-2} \ldots M_0$ of length d = ceil(l/8)
OS2BS	The primitive that converts octet strings to bit strings takes an octet string of length d and the desired length l of the bit string as input. It shall output the bit string if d = ceil (l/8) and if the leftmost 8d – l bits of the leftmost octet are zero; it shall output "error" otherwise.
I2BS	Primitive that converts integers to bit strings. It takes an integer x and the desired length l as input and outputs the bit string if $2^l > x$. It shall output "error" otherwise.
BS2I	The primitive that converts bit strings to integers. It takes a bit string as input and outputs the corresponding integer.