GENERATE A KEY FOR AES USING BIOMETRIC FOR VOIP NETWORK SECURITY

P.Arul[1], **Dr.A.Shanmugam**[2]

[1] Senior Lecturer in Computer Science, CMS College of Science and CommerceCoimbatore – 641 006.
[2] Principal BIT, Sathyamangalam-638 401.
[1]Mobile : 99655 37890, [2]Mobile : 98422 17170
Email : [1]phdarul2008@yahoo.co.in, [2]principal@bitsathy.ac.in

ABSTRACT

VoIP technology in general refers to the set of software, hardware and industry standards that enable "voice" to be transported using the Internet Protocol (IP). The technology is compelling to a wide audience for several reasons:

- VoIP phone bills are typically cheaper than traditional phone bills to the consumer.
- VoIP networks offers providers easier IT management and reduction in operating cost for a combined network for voice and data.
- VoIP technology is feature rich to support next generation multimedia applications

With private phone conversations being conducted on insecure public networks, security of VoIP communications is increasingly important. VoIP has a very different architecture than traditional circuit based telephony, and these differences result in significant security issues. Encryption is one of the essential security technologies for computer data, and it will go a long way toward securing VOIP[1,2,3]. In our discussion we proposed a Biometric-Crypto system which generates a cryptographic key from the fingerprints for Encrypting and Decrypting the voice data packets for VoIP Security. if your VoIP packets traverse the Internet to reach a destination, a number of attackers have a shot at your voice data. The calls are also vulnerable to hijacking or a man in the middle attack . In such a scenario, an attacker would intercept a connection and modify call parameters. This is an especially scary attack, since the participants likely wouldn't notice a change. The ramifications include spoofing or identity theft and call redirection, making data integrity a major risk. One way to help protect your privacy is to encrypt these conversations so that they aren't simply floating around out there for potential hackers to latch onto. In our approach we have proposed a system which will encrypt the VoIP data packets using Advanced Encryption Standard (AES)[7] with the novel method of Biometrics based Key Generation technique.

Keywords : *VoIP, AES, Fingerprint, Encryption, Decryption, Minutiae point, Bio-metric cryptosystem, ROI.*

1 INTRODUCTION

Voice over Internet Protocol (VoIP) [1] is a protocol optimized for the transmission of voice through the Internet or other packet switched networks. VoIP is often used abstractly to refer to the actual transmission of voice . VoIP is also known as IP Telephony[2,4], Internet telephony, Broadband telephony, Broadband Phone and Voice over Broadband. "VoIP" is pronounced voyp.

VoIP calls can take place between LAN or on WANs, as is the case with internal calls on a corporate network. If a VoIP user wishes to call a destination on POTS, a special gateway is used. These devices act as connectors between the data network and the SS7 network used by POTS. They translate the incoming data into a format the recipient, be it IP or SS7, can understand. In the process of saving money and increasing efficiency, two crucial portions of any infrastructure, voice and data, were combined. As if these data security concerns weren't enough, VoIP servers acting as gateways, special routers, phones, new protocols and operating systems are now thrown into the mix. The burden of voice and telecommunications security has been shifted from the carrier to the IT team. It has moved from an obscure PSTN, to an IP network every cracker is familiar with. Let's examine the risks and how you can mitigate them.

Companies providing VoIP service are commonly referred to as providers, and protocols which are used to carry voice signals over the IP network are commonly referred to as Voice over IP or VoIP protocols. They may be viewed as commercial realizations of the experimental Network Voice Protocol (1973) invented for the ARPANET providers. Some cost savings are due to utilizing a single network to carry voice and data, especially where users have existing underutilized network capacity that can carry VoIP at no additional cost. VoIP to VoIP phone calls are sometimes free, while VoIP to public switched telephone networks, PSTN, may have a cost that is borne by the VoIP user.Voice over IP protocols carry telephony signals as digital audio, typically reduced in data rate using speech data compression techniques, encapsulated in a data packet stream over IP.

The security factors of a voice over IP network, let's examine the rationale behind it[2]. The traditional telephone network, known as POTS (plain old telephone service) or the PSTN (public switched telephone network), served us well for many years. Unfortunately, it was costly, managed by only a few companies and inefficient. Each voice call over POTS uses a unique connection, allotted 64K of bandwidth. Moreover, a silent moment, or lapses in speech still consume the 64K. VoIP deployments capitalize on the inefficiency of this design. The analog voice signal is digitized, compressed, chunked into packets and sent over a data network. Advanced compression algorithms reduce the bandwidth necessary for a quality voice call to a fraction of the 64K required by POTS. The silence and background noise transmission of POTS can be eliminated as well . As if the bandwidth savings weren't enough, VoIP deployments also reduce cost and enhance scalability by employing standard data networking components (routers, network switches), instead of expensive, complicated telephone switches. Now the same team handling the data network can manage a voice network - great news for all of you overworked IT staffers.

One way to help protect your privacy is to encrypt these conversations so that they aren't simply floating around out there for potential hackers to latch onto. In our approach we have proposed a system which will encrypt the VoIP[3] data packets using Advanced Encryption Standard (AES) [7], with the novel method of Biometrics [7] based Key Generation technique.
Biometric cryptosystems can operate in one of the following three modes, (i) key release, (ii) key binding and (iii) key generation. In the *key release mode*, biometric authentication is completely decoupled from the key release mechanism. The biometric template and the key are stored as separate entities and the key is released only if the biometric matching is successful. In the *key binding mode*, the key and the template are monolithically bound within a cryptographic frame work . It is computationally infeasible to decode the key or the template without any knowledge of the user's biometric data. A crypto- biometric matching algorithm is used to perform authentication and key release in a single step. In the *key generation mode*, the key is derived directly from the biometric data and is not stored in the database. Though it is easy to implement a biometric cryptosystem in the key release mode, such a system is not appropriate for high security applications because it has two major vulnerabilities. Firstly, the biometric template is not secure. Template security is a critical issue in biometric systems because stolen templates cannot be revoked. Secondly, since authentication and key release are decoupled, it is possible to override the biometric matcher using a Trojan horse program . Biometric cryptosystems that work in the key binding/generation modes are more secure but difficult to implement due to large intra-class variations in biometric data, i.e., samples of the same biometric trait of a user obtained over a period of time can differ substantially.

2 ADVANCED ENCRYPTION STANDARD

Encryption is one of the essential security technologies for computer data, and it will go a long way toward securing VOIP. Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. An encryption algorithm along with a key is used in the encryption and decryption of data. Advanced Encryption Standard (AES) , is one of the most popular algorithms used in symmetric key cryptography. AES [7,8] is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information . It has been analyzed extensively and is now used widely world wide enough to protect classified information up to the TOP SECRET level, which is the highest security level and defined as information which would cause "exceptionally grave damage" to national security if disclosed to the public. AES supports key sizes of 128 bits, 192 bits and 256 bits and will serve as a replacement for the Data Encryption Standard which has a key size of 56 bits. In addition to the increased security that comes with larger key sizes, AES can encrypt data much faster than Triple-DES, a DES enhancement that which essentially encrypts a message or document three times. According to NIST's "The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information".

It is clear that we need an algorithm to generate keys(Gen), an encryption (Enc) algorithm and a decryption (Dec) algorithm.

A triplet (Gen, Enc, Dec) of algorithms, a message space M and a key space K, is called a symmetric key encryption scheme if :

a. The key-generation algorithm : Gen is an algorithm that returns a key K using the finger print, dentoted by k ← Gen, such that k €K.

b. The encryption algorithm : Enc is an algorithm that takes a key k and a voice-data m €M, and outputs a cipher data c ← Enck (m).

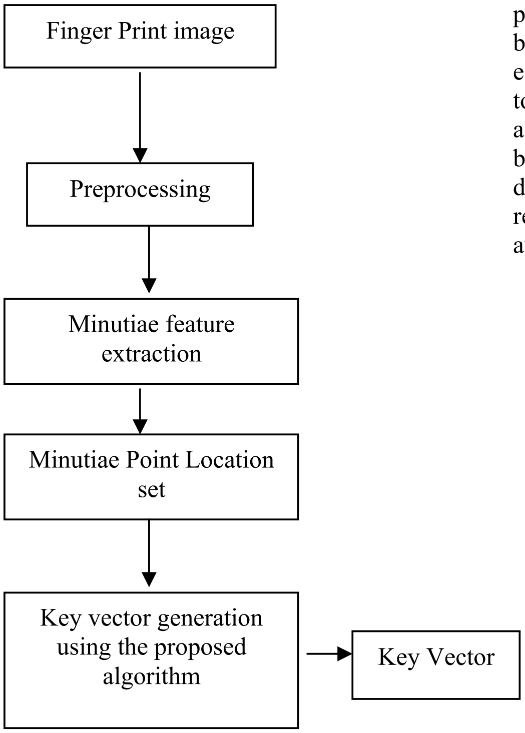
c. The decryption algorithm : Dec is an algorithm that takes a key k and cipher data c and outputs a voice-data m.

d. The scheme should satisfy the following property : For all m € M and k €K,

[Deck(Enck (m)) = m] = 1.

In this paper we are discussing about the key generation method using biometric Crypto systems(ie finger print).

Figure - 1: Generate key vector from finger print


Finger Print image
Preprocessing
Minutiae feature extraction
Minutiae Point Location set
Key vector generation using the proposed algorithm
Key Vector

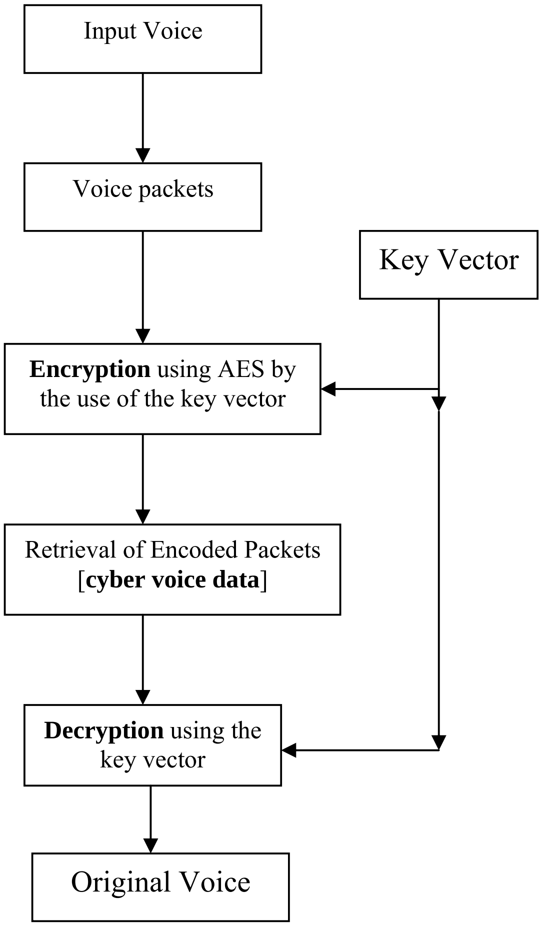
From the figure - 1 we can get idea how to generate key vector for encrypt and decrypt the input voice The key vector is formed based on minutiae points[ridge ending and ridge bifurcation] are encountered in the given finger print image.

Similarly the figure - 2 will help to encrypt and decrypt data using key vector. The input voice is digitized and encrypted based on AES using key vector which is generated from the finger print. The same encrypted data also decrypted from the receiving end based on AES using key vector .

3. BIOMETRIC CRYPTO SYSTEMS

Cryptography provides the secure manner of information transmission over the insecure channel. It authenticates messages based on the key but not on the user. It requires a lengthy key to encrypt and decrypt the sending and receiving the messages, respectively . But these keys can be guessed or cracked. Moreover, Maintaining and sharing lengthy, random keys in enciphering and deciphering process is the critical problem in the cryptography system. The above mentioned problem is solved by a Biometric cryptosystems. Biometric cryptosystems [11] combine cryptography and biometrics to benefit from the strengths of both fields. In such systems, while cryptography provides high and adjustable security levels, biometrics brings in non-repudiation and eliminates the need to remember passwords or to carry tokens etc. In biometric cryptosystems, a cryptographic key is generated from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication.

Figure - 2 : Encrypt and Decrypt using Key


Input Voice
Voice packets
Key Vector
Encryption using AES by the use of the key vector
Retrieval of Encoded Packets [cyber voice data]
Decryption using the key vector
Original Voice

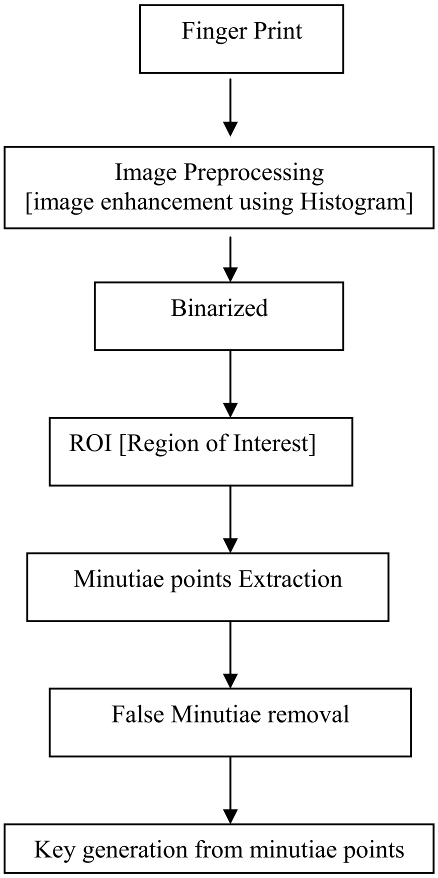
4. CRYPTOGRAPHIC KEY GENERATION FROM BIOMETRICS

Numerous biometrics have been proposed for user authentication and conceivably many are candidates for generating cryptographic keys using recently proposed techniques. In our approach we have selected fingerprint as the biometrics feature for generating cryptographic key. We have extracted minutiae points from the fingerprint and used that point set for generating cryptographic key.

4. 1. Extracting Minutiae Points From Fingerprint

For extracting minutiae points from fingerprint [13],(see figure-3) a three-stage approach is widely used by researchers. They are preprocessing, minutia extraction and post processing stage. For the fingerprint image preprocessing, Histogram Equalization and Gabor Filters are used to do image enhancement [14]. And then the fingerprint image is binarized using the locally adaptive threshold method. Then the Region of Interest [ROI] is extracted by Morphological operations. For minutia extraction stage, three thinning algorithms are tested and the Morphological thinning operation is finally bid out with high efficiency and pretty good thinning quality.

Figure - 3 : Key generation from minutiae points


Finger Print
Image Preprocessing [image enhancement using Histogram]
Binarized
ROI [Region of Interest]
Minutiae points Extraction
False Minutiae removal
Key generation from minutiae points

4. 2. Histogram Equalization

Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information. The original histogram of a fingerprint image has the bimodal type, the histogram after the histogram equalization occupies all the range from 0 to 255 and the visualization effect is enhanced.

4.3. Binarization

Fingerprint Image Binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black color while furrows are white. A locally adaptive binarization method is performed to binarize the fingerprint image.

Such a named method comes from the mechanism of transforming a pixel value to 1 if the value is larger than the mean intensity value of the current block (16x16) to which the pixel belongs .

4. 4. Roi Extraction By Morphological Operations

Two Morphological operations called 'OPEN' and 'CLOSE' are adopted. The 'OPEN' operation can expand images and remove peaks introduced by background noise. The 'CLOSE' operation can shrink images and eliminate small cavities. The bound is the subtraction of the closed area from the opened area. Then the algorithm throws away those leftmost, rightmost, uppermost and bottommost blocks out of the bound so as to get the tightly bounded region just containing the bound and inner area.

4.5. Minutiae Points Extraction

Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. uses an iterative, parallel thinning algorithm. In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3x3). And finally removes all those marked pixels after several scans. After the fingerprint ridge thinning, marking minutia points is relatively easy. For each 3x3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending. Suppose both the uppermost pixel with value 1 and the rightmost pixel with value 1 have another neighbor outside the 3x3 window, so the two pixels will be marked as branches too. But actually only one branch is located in the small region. So a check routine requiring that none of the neighbors of a branch are branches is added.

4.6. False Minutia Removal

The preprocessing stage does not totally heal the fingerprint image. For example, false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking are not totally eliminated. Actually all the earlier stages themselves occasionally introduce some artifacts which later lead to spurious minutia. These false minutia will significantly affect the accuracy of matching if they are simply regarded as genuine minutia. So some mechanisms of removing false minutia are essential to keep the fingerprint verification system effective.

4.7. Key Generation From Minutiae Points

In this Section we explain the **Key Generation Algorithm** Assumptions
Kl → length of the AES key
Mp → Minutiae point set
Kl → Key length
Np → Size of Minutiae point set
S → Seed value
Sl → seed limit.
m → (x,y) – co-ordinate of a minutiae point
Kv → Key Vector

Step 1 : The Extracted minutiae points are represented
as
$Mp = \{ mi \}i=1,\ldots, Np$

Step 2 : The initial key vector is defined as follows,
$Kv = \{ xi : p(xi) \}\ i=1, \ldots.., Kl$
Where
$p(x) = Mp[I \% Np] + Mp[(i+1) \% Np] + S$
$i=1,\ldots. , Kl$

Step 3 : Initial value of S is equal to total Number of Minutiae points. The value of S will be dynamically changed as follows
$S = Kv (i) \% Sl , -1 < i< Kl$

Step 4 : Initial key vector (Kv) is converted in to a
matrix Km of size Kl / 2 * Kl / 2

$Km = (aij)\ Kl / 2 * Kl / 2$

Step 5 : A intermediate key vector is generated as
follows
$KIV = \{ Ki : (m(ki) \}\ i=1,\ldots. Kl$
Where
$m(k) = | Aij | ,$
$Aij = Km\ i,j : i+size,j+size , -1 < i< Kl/2$
Aij is a submatrix formed from the key matrix.

Step 6 : Final key vector is formed is
$Sv = \{ 1, \text{ if } KlV [i] > mean(KlV) ,0 \text{ otherwise } \}$

5. CONCLUSION

From the above discussion I have proposed a method of securing VoIP communication using Encryption and a novel approach for fingerprint based cryptography system. The crypto keys have been generated using fingerprint patterns, which is stable through out person's lifetime.

Since it creates more complexity to crack or guess the crypto keys. This approach has reduced the complicated sequence of the operation to generate crypto keys as in the traditional cryptography system. It can generate more complex keys with minimum amount of time complexity, which is aptly suited for any real time cryptography.

6. REFERENCES :

[1]. B. Goode, “Voice Over Internet Protocol (VOIP)”. Proceedings of thee IEEE, VOL. 90, NO. 9, Sept. 2002.

[2]. “Breaking Through IP Telephony “ http://www.nwfusion.com/reviews/2004/0524voipsecurity.html

[3]. “Voice over Internet Protocol” from http://en.wikipedia.org/wiki/Voice_over_IP

[4]. “ Cisco IP Phones Compromise “ http://www.syssecurity.com/archive/papers/The_Trivial_Cisco_IP_Phones_Compromise.pdf.

[5]. “ Security Risk Factors in IP Telephony Based Networks “ http://www.syssecurity.com/archive/papers/Security_Risk_Factors_with_IP_Telephony_based_Networks.pdf

[6]. “Security Testing of Protocol Implementations at the University of Finland “ http://www.ee.oulu.fi/research/ouspg/protos/

[7]. Announcing the “ADVANCED ENCRYPTION STANDARD (AES)” – Federal Information, Processing Standards Publication 197,November 26, 2001

[8]. “Advanced Encryption Standard “ from http://en.wikipedia.org/wiki/Advanced_Encryption_ Standard

[9]. D.Maio and D. Maltoni, “Direct gray-scale minutiae detection in fingerprints “. IEEE Trans. Pattern Anal. And Machine Intell., 19(1):27-40, 1997

[10]. L.C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui. “Intelligent biometric techniques in fingerprint and face recognition.”, 1999, the CRC Press

[11]. Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K.Jain “Biometric Cryptosystems Issues and Challenges” Proceedings of the IEEE 2004.

[12]. “GaborFilter”from http://en.wikipedia.org/wiki/Gabor_filter

[13]. “Fingerprint Minutiae Extraction Based On FPGA and MatLab”, Víctor López Lorenzo, Pablo Huerta Pellitero, José Ignacio Martínez Torre, Javier Castillo Villar, http://www.escet.urjc.es/~phuerta/pdf/dcis_2005.pdf

[14]. “New Fingerprint Image Enhancement Using Directional Filter Bank” Sang Keun Oh, Joon Jae Lee*, Chul Hyun Park, Bum Soo Kim, Kil Houm Park School of Electrical Engineering, Kyungpook National University, SEOUL 702-701, Daegu, Korea , http://wscg.zcu.cz/wscg2003/Papers_2003/J37.pdf