www.sphinxsai.com

International Journal of ChemTech Research
CODEN (USA): IJCRGG ISSN : 0974-4290
Vol.6, No.9, pp 4359-4365, September 2014

RTBCE 2014[12th August 2014]
Recent Trends in Biotechnology and Chemical Engineering

Biometrics Based Key Generation using Diffie Hellman Key Exchange for Enhanced Security Mechanism

M.S.Durairajan[1*], Dr.R. Saravanan[2]

[1]Departmentof Information Technology, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai, India

[2]Computer Science and Engineering, RVS Educational's Trusts Group of Institutions, Dindigul, TamilNadu, India

*Corres.author: M.S.Durairajan

Abstract Security has always been a major concern for authentication over networking. Cryptographic methods solve the problem of security by implementing various methods for key exchange. Shared key is the major constraint established by Diffie Hellman Algorithm for two parties without the prior knowledge of each other over insecure communication channel. This algorithm generates the shared key with the help of receiver's public key and sender's private key. This research paper deals with the usage of finger print as the private key for generating the shared key for enhanced security.

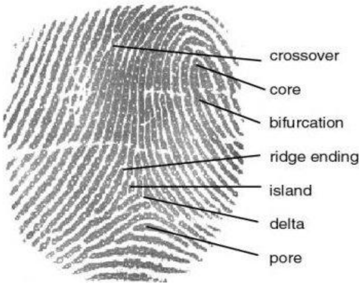
Keywords: Authentication, Diffie-Hellman algorithm, Finger print, shared key

Introduction

Cryptography contains various abstraction levels of security mechanism and it builds the discipline of data encryption and decryption. Network administrator provides authorized access over the network by implementing network security and adoption of its provisions and policies to prevent unauthorized access. Authorization has always been an integral part of the security mechanism. Biometric system of identification uses unique feature of face, hands like iris, retina, finger print, structure of the face to identify a person with a unique characteristic that differentiates the concerned person from others. The system of using finger print as a parameter for authorization provides enhanced security for data transfer over the network. In non-biometric authentication process such as usage of passwords or PIN numbers, depending upon the length of the key, the information is very much vulnerable to unauthorized access by individuals. Longer and random passwords are safer than short words that contain dictionary words. Finger print is an impression left by the friction ridges of a human finger. They are formed in humans in their definitive form before birth and are always unique. Finger prints play an important role in forensic science. Finger print matching methods are categorized into three classes. They are correlation based matching, minutiae based matching and ridge feature based matching. Sergey Tulyakov at al[1] propose to use symmetric hash functions to secure biometric systems. Fuzzy extractor[2] binds random data with biometric data to produce unique keys.

Diffie-Hellman algorithm (DH algorithm) is a way of generating a shared secret key between two people in such a way that the secret key cannot be intruded by observing the communication over an insecure communication channel. The distinguishing feature is that you are not sharing information during the key exchange, you are creating key together. This is particularly useful because you can use this technique to perform encryption with public key of the receiver, and then start encrypting your incoming data with your private key. And even if the incoming data is recorded and later analyzed, there is absolutely no way to figure out what the private key was, even though the exchanges that created it may have been visible[3].

Figure 1: Finger print image



Experimental Setup

Diffie Hellman Algorithm

In Diffie Hellman algorithm, initially there will be one private key and public key this two keys on combination a shared key is generated. In the generation process two common variables are used. The two common variable here we are using as **α** and **q**.

Constraints for the variable **α** & **q**:

- Q-it should be the prime number.
- **α** should be lesser than Q
- α-it should be the primitive root of Q

The mechanism of this algorithm is that we use two common variables such that one is a prime number and the other is primitive root of that prime number. Using these two common variables the private key is selected for both sender and receiver. In this algorithm the public key is generated for both sender and receiver using the private key and the two common variables (Figure- 2)

Figure 2: Key exchange mechanism

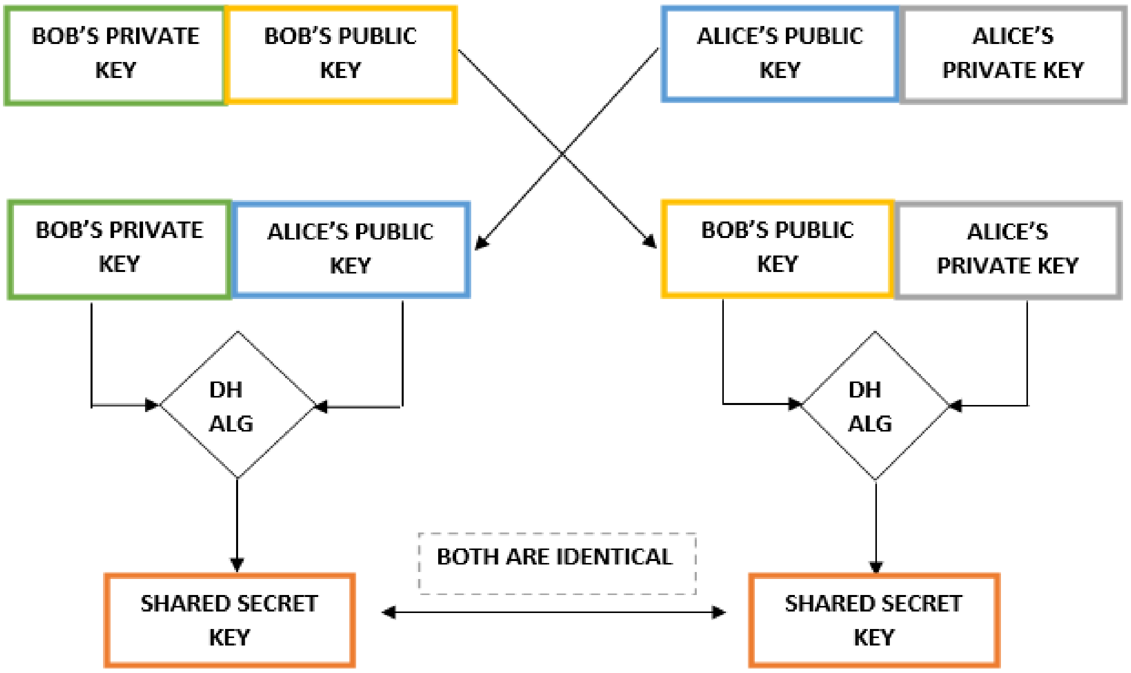
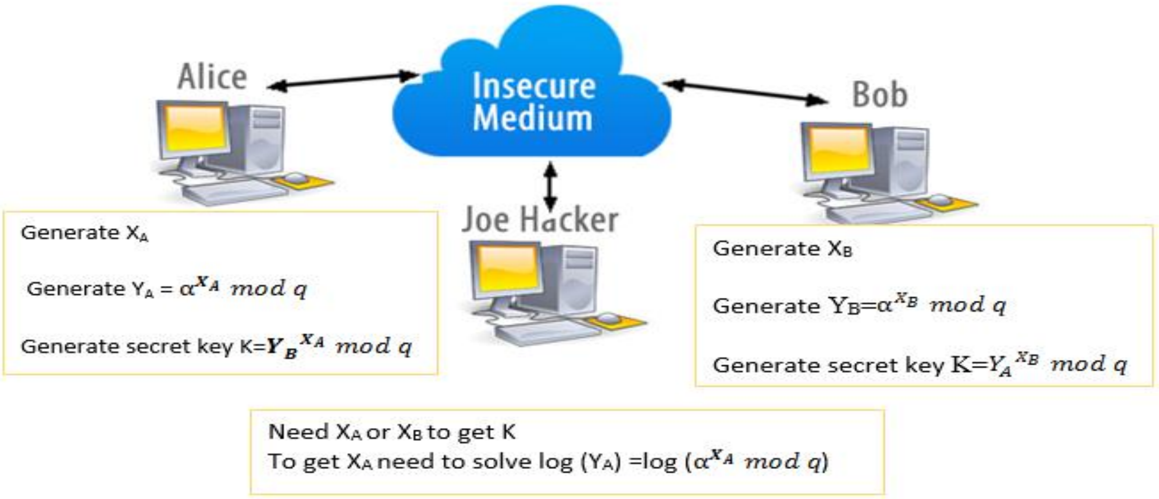


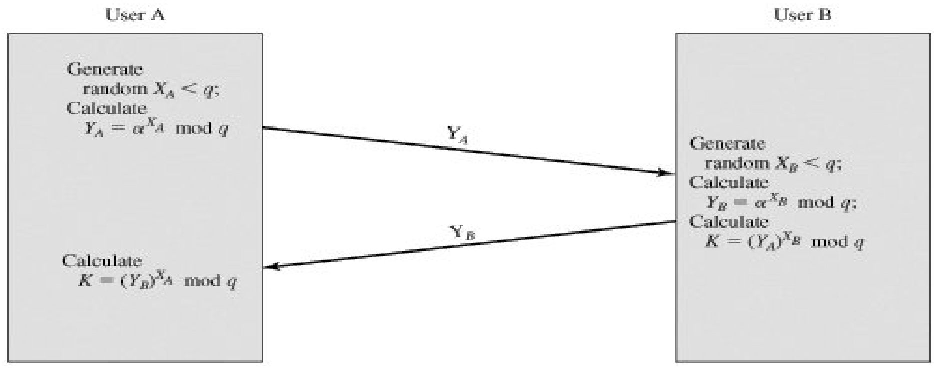
Figure 3: Insecure access to data


Alice
Insecure Medium
Bob
Joe Hacker
Generate X_A
Generate $Y_A = \alpha^{X_A} \bmod q$
Generate secret key $K = Y_B^{X_A} \bmod q$
Generate X_B
Generate $Y_B = \alpha^{X_B} \bmod q$
Generate secret key $K = Y_A^{X_B} \bmod q$
Need X_A or X_B to get K
To get X_A need to solve log (Y_A) =log ($\alpha^{X_A} \bmod q$)

(Figure- 3) shows that the hacker named Joe is trying to get the key to know the data that is being transferred between Bob and Alice.But Joe can get only the two common variable and the public key but not the private to get the shared key. This is the advantage of Diffie-Hellman algorithm [4]. The user sender and receiver need not share the key to each other on a insecure line while transferring data as the shared key generated using the two common variable and the private key is the same for both sender and receiver.

Algorithm

Figure 4: Diffie Hellman algorithm


User A
User B
Generate random $X_A < q$;
Calculate $Y_A = \alpha^{X_A} \bmod q$
Y_A
Y_B
Generate random $X_B < q$;
Calculate $Y_B = \alpha^{X_B} \bmod q$;
Calculate $K = (Y_A)^{X_B} \bmod q$
Calculate $K = (Y_B)^{X_A} \bmod q$

In Diffie Hellman algorithm (Figure- 4), the shared key is generated by combining the sender's private key and receiver's public key in the sender side and the receiver, decrypt the data by using sender's public key and its own private key. The shared key generated by both the parties are same. This can be mathematically proved by taking certain variables for consideration. Let (q) be a prime number and an integer (α) that is a primitive root of (q). Let A and B be the parties who wish to communicate over the network and they generate their shared key respectively. Party A selects a random integer and similarly party B independently selects a random integer and both parties compute the values of (α) and (q). Each party keeps the value of the private key and makes the value visible publicly to the other party. Both the parties compute their shared key. Here X_A and X_B are the private keys of the sender A and receiver B respectively. The public key [Y_A] for party A (sender) is obtained by raising the power of (α) to (X_A) and taking mod for the value obtained with (q) i.e. **[**$Y_A = \alpha^{X_A} \bmod q$ **]**. Similarly the receiver obtains the public key value i.e. [$Y_B = \alpha^{X_B} \bmod q$]. The public key value thus obtained is exchanged between them for the generation of shared key. Party A now generates the shared key by obtaining the product of the sender's private key (**X_A**) and the receiver's public key (**Y_B**) and then by performing the mod function the product with the value of (q) [$\mathbf{K} = \boldsymbol{Y_B}^{X_A} \bmod q$]. Similarly the receiver computes the value of shared key, i.e. [$K = Y_A^{X_B} \bmod q$]

These are the Calculations Performed by the Sender A

$K = (Y_B)^{X_A} \bmod q$
The public key of receiver is used to generate the shared key by the sender.
$= (\alpha^{X_B} \bmod q)\ X_A \bmod q$
Now the value of Y_B is substitued in the above equation,
$= (\alpha^{X_B})^{X_A} \bmod q$
$= \alpha^{X_B X_A} \bmod q$
$= (\alpha^{X_A})^{X_B} \bmod q$
$= (\alpha^{X_A} \bmod q)^{X_B} \bmod q$
The shared key generated by the sender which is identical.
$= (Y_A)^{X_B} \bmod q$

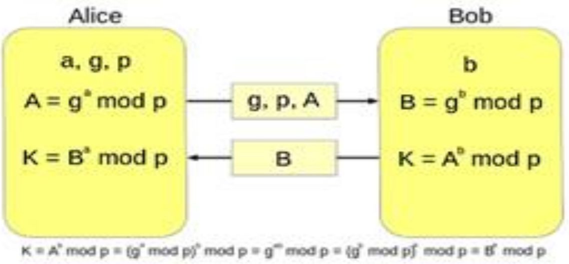
Suppose that user A wishes to set up a connection with user B and use a secret key to encrypt messages on that connection. User A can generate a one-time private key , calculate , and send that to user B. User A can generate a one-time private key , calculate , and send that to user B. User B responds by generating a private value X_B ,calculating Y_B and sending it to the user A. Both the users can now calculate the key. The necessary public values q and α would need to be known ahead of time. Alternatively, user A could pick values for q and α and include those in the first message.

These are the Calculations Performed by the Receiver B

$K = (Y_A)^{X_B} \bmod q$
$= (\alpha^{X_A} \bmod q)\ X_B \bmod q$
$= (\alpha^{X_A})^{X_B} \bmod q$
$= \alpha^{X_A X_B} \bmod q$
$= (\alpha^{X_B})^{X_A} \bmod q$
$= (\alpha^{X_B} \bmod q)^{X_A} \bmod q$
$= (Y_B)^{X_A} \bmod q$

The above calculation performed by the receiver B is similar as done in the sender for the generation of the shared key for encryption (Figure- 5)

Figure 5: Key Generation


Alice
Bob
a, g, p
A = g^a mod p
K = B^a mod p
g, p, A
B
b
B = g^b mod p
K = A^b mod p
K = A^b mod p = (g^a mod p)^b mod p = g^ab mod p = (g^b mod p)^a mod p = B^a mod p

Proof

Sender A → $K= (Y_A)^{X_B} \bmod q$ Receiver B→ $K= (Y_B)^{X_A} \bmod q$

The shared key generated in the sender and the receiver is identical (Figure- 4 & 5)

Proposed System

Among all the recent biometric techniques, the fingerprint is the most successful and secured feature for the personal authentication. This features enable us to use fingerprint authentication system where security is a prime requirement. The following analysis made finger print as a choice of selection (Table- 1).

Here we can use the finger print as the private key for the generation of key for encryption.

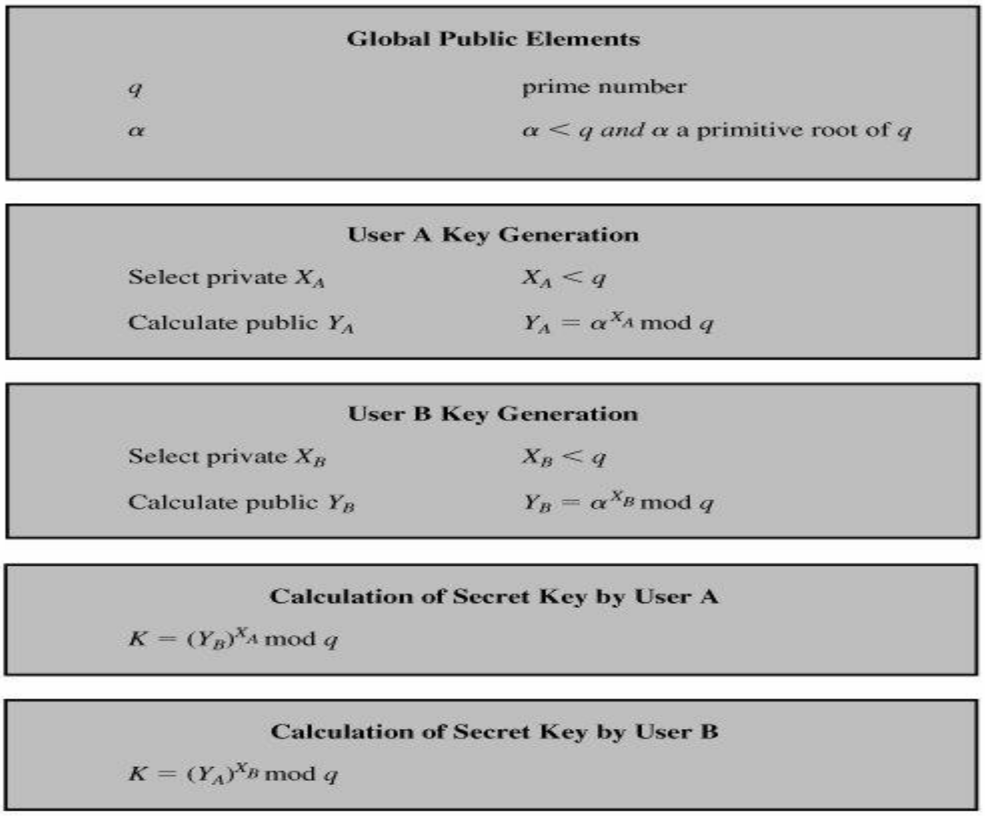
Table 1: Comparison of various biometric technologies

Biometric identifier	Un	Di	Pm	Co	Pf	Ac	Ci
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand Geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Key stroke	L	L	L	M	L	M	M
Signature	L	L	L	M	L	H	H
Voice	M	L	L	M	L	H	H

Un- Universality Pf – Performance Di– Distinct
Ci– Circumvention Pm– Permanence L – Low
Co – Collectability M – Medium H- High

The private key Value is replaced with the value of the finger print. Let us assume the finger print value for the sender A be (β1) and the receiver B be (β2). Hence, in sender side K**=(Y_A)** $^{\beta 1}$ **mod q .** In receiver side **K = (Y_B)** $^{\beta 2}$ **mod q** (Figure- 6, 7 & 8).

Figure 6: Key Generation mechanism



Global Public Elements

q prime number

α $\alpha < q$ *and* α a primitive root of q

User A Key Generation

Select private X_A $X_A < q$

Calculate public Y_A $Y_A = \alpha^{X_A} \bmod q$

User B Key Generation

Select private X_B $X_B < q$

Calculate public Y_B $Y_B = \alpha^{X_B} \bmod q$

Calculation of Secret Key by User A

$K = (Y_B)^{X_A} \bmod q$

Calculation of Secret Key by User B

$K = (Y_A)^{X_B} \bmod q$

Figure 7: Conversion of finger print into binary digits

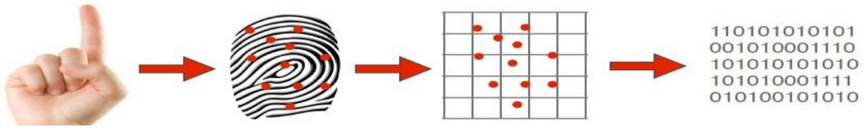
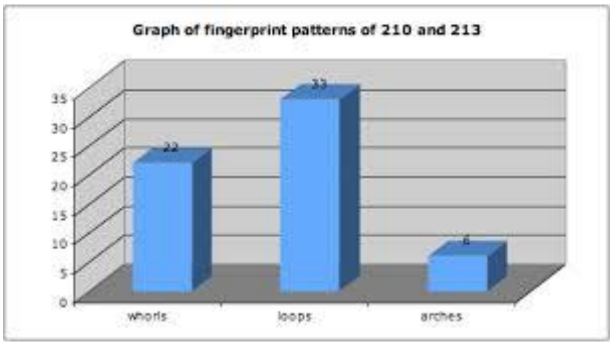


Figure 8: Analysis of Finger print patterns

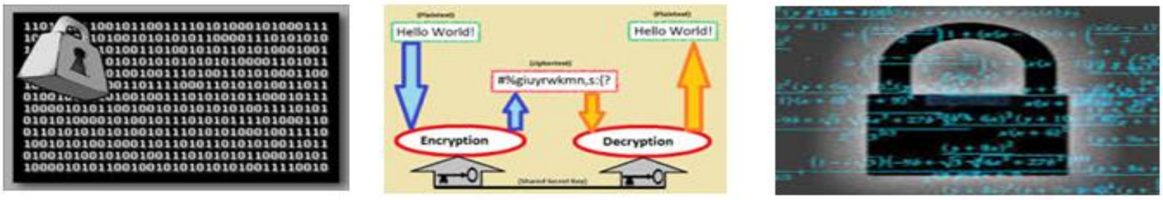


The finger print of the sender and receiver are converted to equivalent decimal value. The decimal value of the finger print obtained from the biometric authentication device which is used as the private key (Figure- 9 & 10).

Figure 9: Conversion of Finger print value into private key

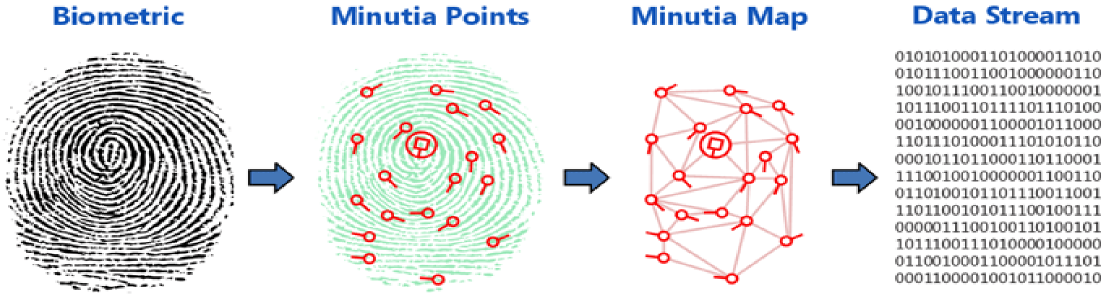
010010101
Decimal number
(private key)

Figure 10: Encryption and Decryption



In biometric this approach is used for exchanging secret key between two parties and ensures both authentication and non-repudiation. Here, Diffie-Hellman based encryption scheme used, instead of transmitting secret key, user's finger print is stored in database, it is retrieved only at the time of authentication, and no one can pose as a sender, because of his finger print identity. This works puts the cryptanalysts under pressure. The use of this novel algorithm in biometric signature creation improves the electronic banking security, as the public and private keys are created without storing and transmitting any private information anywhere over the network (Figure- 11).

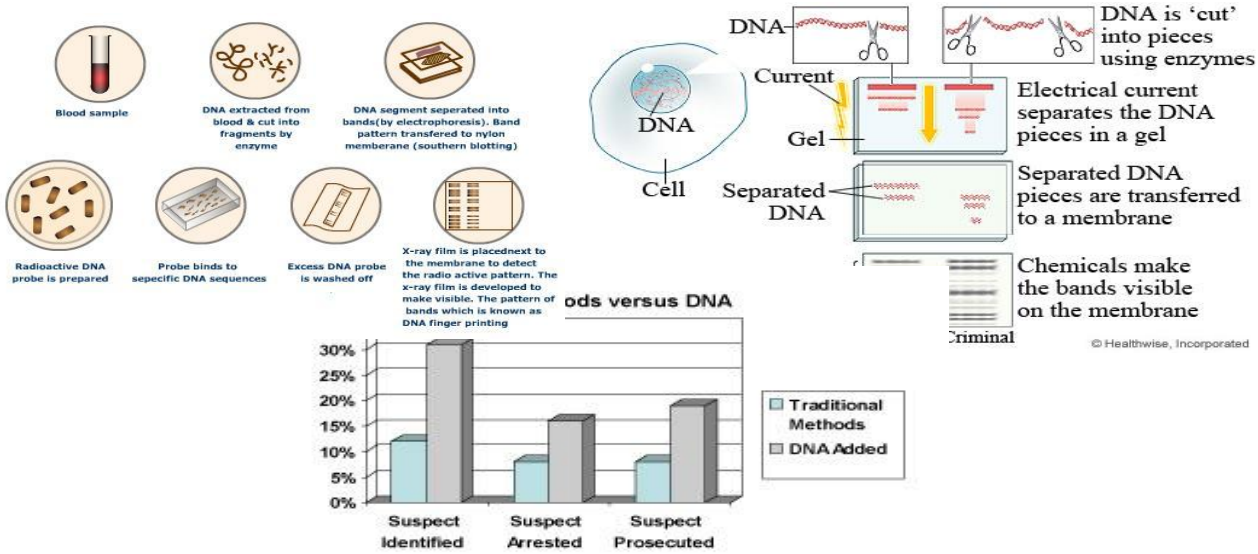
Figure 11: Conversion of finger print to data stream



Conclusion

The above research paper is proposed for enhanced network security. For this analysis, Diffie Hellman algorithm has been implemented which is based on shared key concept. The usage of finger print instead of random number as a private key in the algorithm provides better security for data transfer over the network with high confidentiality. In future to avoid high level security threats we can upgrade the system by having multi parameter security mechanisms such as hybrid combinations of Deoxyribonucleic Acid (DNA) with finger print or with retina (Figure- 12).

Figure 12: Analysis of DNA and retina with finger print


Blood sample
DNA extracted from blood & cut into fragments by enzyme
DNA segment seperated into bands(by electrophoresis). Band pattern transfered to nylon memberane (southern blotting)
Radioactive DNA probe is prepared
Probe binds to sepecific DNA sequences
Excess DNA probe is washed off
X-ray film is placednext to the membrane to detect the radio active pattern. The x-ray film is developed to make visible. The pattern of bands which is known as DNA finger printing
DNA
Cell
DNA
Current
Gel
Separated DNA
DNA is 'cut' into pieces using enzymes
Electrical current separates the DNA pieces in a gel
Separated DNA pieces are transferred to a membrane
Chemicals make the bands visible on the membrane
:riminal
© Healthwise, Incorporated
ods versus DNA
30%
25%
20%
15%
10%
5%
0%
Suspect Identified
Suspect Arrested
Suspect Prosecuted
Traditional Methods
DNA Added

References

1. Sergey Tulyakov, Faisal Farooq, Praveer Mansukhani, Venu Govindaraju, "Symmetric Hash functions for Secure Finger print biometric systems".
2. Y.Donis, L. Reyzin and A.Smith, "Fuzzy Extractors"In security with Noisy Data: Private Biometrics, Secure key Storage and Anti-Counterfeiting, P.Tuyls, B.Skoric and T.Kevenaar, Eds., chpt5,pp.79-77, Springer-Verlag, 2007.
3. William Stallings, "Cryptography and Network Security principles and practices ", third Edition, Pearson Education, 2003.
4. Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography", Invited Paper, 1976.

*****