GENERATING A KEY FOR AUTHENTICATION PURPOSE USING BIO-METRIC DATA & SMART CARD FOR UNSECURE CHANNEL

Sunil Sharma, Shobhit University, Meerut
Raju Singh, Shobhit University, Meerut

ABSTRACT

In this fast developing world there is a need of information inters change between the system and user in different part of the world. The information interchange requires a high degree of confidentiality and authentication. The authentication technique provides the authenticity of person or system. There are a number of authentication techniques are available to authenticate the system. In this world the authentication system uses Bio-metric data, any card system, PIN system and password. These systems are not very much secure to provide authentication. So, we proposed a biometric Authentication system which uses the finger print and a Smart Card which generates a unique message Authentication code to authenticate the system and access the information over the internet.

Keywords- *Message Authentication code, Finger prints, Smart card, Encryption, Decryption.*

INTRODUCTION

The Bio-metric data are used as to identify the person from one to another. These data are used as to provide authentication in number of application areas. Any data is transmitted over the internet or unsecure channel is encrypted form. It takes confidentiality and authentication to provide reliability to sender. The message Authentication code is a function which append with Cipher text. This code produces a fixed size value at sender and server receives this fixed sized value and checks their validity. If it is matched with the value already stored in the server. Then server gives permission to access otherwise it discard it. If any intruder has known our code function it can easily access our system. The biometric information is useful information for the purpose of authentication. The authentication code generated with the help of finger prints & a special key function is used to generate authentication code is stored in smart card.

Bio-metric Information: Any information related with human body physiological or behavior, which can uniquely distinguish from one to another. Such as finger prints, palm, Irish, heartbeat, thumb stroke etc.

Extraction of information from finger prints: there are some techniques which are used to extract [5] minuate point from finger print

a) *Histogram technique*
b) *Binarization*
c) *Morphological technique.*

In this process we use Morphological techniques to extract minuate point.

LITERATURE SURVEY

In 1981, Lamport [10] first proposed a remote password-based Authentication scheme that could authenticate remote user over an insecure channel. In this Scheme Lamport uses the time based stamp control. When user interact with the system the system can generate a key at that time send to the server, and server generate key at that time match with it , if it is same it authenticate the user otherwise discard the user.

In 1984, Shamir[15] first proposed ID-based cryptosystem. This cryptosystem consist of ID and password When user interacts with system they enter their ID and their password if it is same. In 1990, Hweng, chen and Laig[5],proposed a non-interaction password Authentication scheme without a password table.

In 2002[11], Lee kyu 1/100 proposed a finger print-based user Authentication scheme using a Smart Card. Their scheme would strengthen security by verifying the Smart Card owner's finger prints. In 2003[7], Lee and 1/60 proposed two ID-based password Authentication serves without password or verifications tables with Smart Card and Fingerprints.

PROPOSED WORK

We are proposed a new bio-metric system used for Authentication of user between the user and system using fingerprint and Smart Card .It comprises three phases.

- **Registration phase:**

1. *Take the fingerprints of user*
2. *Extract Minuate point using Morphological Technique*
3. *After extraction of these values.*
4. *Store their values in server as user ID.*
5. *Give a Smart Card to the user with 'n' no of login attempt.*

   Smart Card no: - ***ABCD10'N'***

   N → *no. of attempt provided for user.*

   N → *1 .....100.*

   The server system stores the user finger print and Smart card Information with no. of login attempt.

- **Login phase:**

1. *User first touches their finger Impression to the system as an ID.*
2. *After verification of User ID with server*
3. *Server Display User Registration Information*
4. *Then He insert his smart card*
5. *His cards generate a key and server check this key.*
6. *The card system generates a key with the help of card identity and no. of login attempt.*

   *Key= (card identity) *login attempt*

- **Verification phase:**

a. *The server checks the key generated by card system is correct, it provides authorized login.*
b. *After successful login, the updates it stored value of no. of login attempt reduces by one.*

c. Card system also update this value over the card no. of login attempt reduced bt one.

Every attempt the value of key is changed and it more security to system of Authentication.

CONCLUSION

In this proposed scheme the Authentication is provided by the means of biometric information and Smart card system. A finger print of a person is unique in this world. Secondly, the authentication is provided card system is also secured because after every successful login attempt the key value generated by **the** card system is charged. Any intruder cannot guess such type of key generation because he does not know the no. of login attempt done by the user.

SCOPE FOR FURTHER RESEARCH

In this proposed scheme, the number of login attempt is a main function. This function generates the unique key pattern using biometric information .The future scope of this system is used any other system which provides Authentication with biometric system.

REFERENCES

Lamport L. (1981): "Password Authentication with insecure communication of the ACM" vol.24 no.11 PP.770-772.

Shamir A. (1984): Identity based cryptosystem and signature scheme,Advances in cryptology-crypto 84,LNCS 196 springer-verbig PP.47-58.

Hwang T. chen 1/1 Lain C.S.(1990): Non-interactive password Authentication without password table ,IEEE region 10 conferences on computer and common system PP.429-431.

Lee J.K. kyn S.k.yoo K.X. (2002): finger print-based remote user Authentication scheme using Smart card ,electronics letters vol.88 no.12 PP.554-555.

Kim H.S.Lee S.W.Yoo k.x.(2003): id password based Authentication using Smart Card & finger prints,ACM SIGOPS operating system review vol.87,no.4 PP.32-41.

Authors would like to extend their heartfelt thanks to the academic and infrastructural support received from their respective Dept./University.