Volume No:2, Issue No:7 (December-2016) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

A Secure Biometrics based Authentication for Multi-Server Environments using Smart Cards

D.Chandra Preethi
PG Student,
Dept of CNIS,
G.Narayanamma Institute of Technology and Science,
Hyderabad, Telangana, India.

Dr.N.Laxmi Manasa
Associate Professor,
Dept of CNIS,
G.Narayanamma Institute of Technology and Science,
Hyderabad, Telangana, India.

ABSTRACT:

Smartcard based authentication scheme has been widely utilized for numerous transaction-oriented services like electronic currency exchange, social insurance payment and e-commerce payment charge in modern society. If a remote user desires to use numerous network services, he/she should use his/her identity and password at these centers. It is very long and tiresome work for users to register number of servers. In order to resolve this problem, numerous multi-server authentication systems recently have been proposed. But these schemes are insecure against various cryptographic attacks or inefficiently designed for high computation prices. Furthermore, these schemes don't provide robust key agreement performance which can provide flawless forward secrecy.

Based on these motivations, this paper proposes a new efficient secure biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem (ECC) without verification table and to fit multi-server communication environments. This paper provides Security in Wireless Communication network and E-Commerce Application like E-Banking and transaction oriented Services. Our Project using Secure Biometric based Multi-Server Authentication Protocol using smart cards protect the sensitive information against a malicious adversary, a variety of security services like mutual authentication, user credentials privacy and SK-security.

KEYWORDS:

RFID, Fingerprint, Authentication, Smart card, Multi-server, Biometrics, Elliptic curve cryptography, Keys.

INTRODUCTION:

Authentication scheme is a fundamental and important subject for network security because it is usually used to protect sensitive and important information or restrict the access of precious resources for legal privileged users only. In general, there are two main purposes for authentication schemes to achieve. 1) An authentication scheme should give mutual authentication. That is, not only a legal user is able to authenticate remote server, but also the server has the flexibility to authenticate the user. 2) When authenticating with one another, a session key is generated to encrypt/decrypt all communicating messages between the user and server.

As there's speedy development of the wireless communication networks and e-commerce applications, like e-banking and transaction-oriented services, there's a growing demand to safeguard the user’s credential privacy. Now-a-days internet banking is becoming popular. Banks have actively encouraged this cost-saving trend by persuading customers to sign on. Customers attracted by on-line banking convenience, appear mostly unconcerned regarding identity theft and phishing email scams. In fact, most customers appear to believe that internet banking is quite safe and simple.

Net banking system is well-known technology generally employed by people to hold out a variety of personal and business money transactions and/or banking functions by using fingerprint recognition technique. The net banking system has become very popular with the general public for their availability and general user friendliness.

LITERATURE SURVEY:

A. Biometric identification A. Jain, L. Hong, and S. Pankanti.

Biometric systems allow routine recognition of persons based on physical or behavioral features that belong to a certain person. Each biometric feature has its restrictions and no biometric system is perfect, thus uni-modal biometric systems raise a variety of problems. To over satisfying few mentioned inconvenient and limitations and to increase the level of security the multimodal biometric systems are used.

B. The advantages of elliptic curve cryptography for wireless security K. Lauter

Elliptic curve cryptography has changed from interesting theoretical alternative to cutting edge technology adopted by increasing number of companies. There are two reasons for this development: one is that ECC, which is oldest, and has withstood a generation of attacks.

C. On the security of public key protocols D. Dolev and A. C. Yao:

Recently, the use of public key encryption to provide secure network communication has received considerable attention. Such public key systems are usually effective against passive eavesdroppers that merely tap the lines and try to decipher the message. It's been noticed, however, that an improperly designed protocol could be vulnerable to an active saboteur, who may impersonate another user or alter the message being transmitted. In this paper, we formulate many models in which the security of protocols is can be discussed precisely. Algorithms and characterizations that can be used to determine protocol security.

OBJECTIVES:

In the existing internet banking system, user can log on and can view his/her account details, loan details etc. Customer didn’t have the facility of online transaction oriented services. Thus to overcome these drawbacks we have a tendency to move to the new system.Net banking system allows customers of a financial organization to conduct financial transactions on a secure web site operated by the institution, which can be a retail or virtual bank, credit union or building society.

Disadvantages:

- Security is less.
- We need to go to the bank for exchanging foreign money, so there will be a waste of time.
- Because of hacking and rise of identity theft internet banking customers should have trust that their account information and personal information are safe.

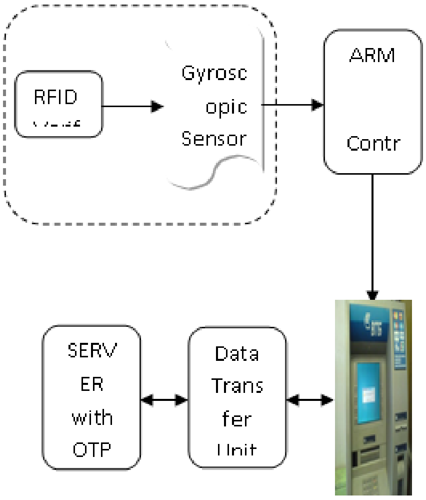
PROPOSED SYSTEM:

In this proposed system, we propose a new biometrics based multi-server authentication protocol using smart card and ECC. We also created the new generation ATM machine which can be accessed by RF-enabled ATM card with 3D position primarily based key generation. Working of RFID card with the gyroscopic sensor was controlled by controller module in which Key generation did base on MEMS axis. It generates a verified OTP, and using MAC implementation OTP will be sent to requested user as SMS.

Advantages:

- By using this method malfunctions are avoided.
- Our transactions will be much secured.
- Multiple banks databases are interconnected with high security.

ARCHITECTURE DIAGRAM:



ALGORITHM:

MD5 Algorithm Description:

Message-Digest (Fingerprint) algorithm is a special function that transforms input of (usually) arbitrary length into output (so-called “Fingerprint” or “Message-digest”) of constant length. We imagine the bits of the message written down as follows:

m_0 m_1 ... m_{b-1}

Computing the message digest of the message is performed in the following five steps:

Step 1: Append padding bits:

The message is "padded" (extended) so its length (in bits) is congruent to 448, modulo 512. That is, the message is extended so it is just 64 bits of being a multiple of 512 bits long. Padding is usually performed, even if the length of the message is already congruent to 448, modulo 512. A single "1" bit is appended to the message, then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448, modulo 512. In all, at least one bit and at the most 512 bits are appended.

Step 2: Append Length:

A 64-bit representation of b (the length of the message before the padding bits were added) is appended to the result of the previous step. In the unlikely event that the b is greater than 2^{64}, then only the low order 64 bits of are used. (These bits are appended as two 32-bit words and appended low-order word first.) At this point the resulting message (after padding with bits has a length that is an exact multiple of 512 bits). Equivalently, this message has a length that is an exact multiple of 16 (32 bits) words. Let M [0…N-1] denote the words of resulting message, where N is a multiple of 16.

Step 3: Initialize MD Buffer:

A four-word buffer (A, B, C, D) is used to compute the message digest. Here each of A, B, C, D is a 32-bit register. These registers are initialized to the following values in hexadecimal, low-order bytes first):

word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98
word D: 76 54 32 10

Step 4: Process Message in 16-Word Blocks:

We first define 4 auxiliary functions that each take as input three 32-bit words and produce as output one 32-bit word.

F(X,Y,Z) = XY v not(X) Z
G(X,Y,Z) = XZ v Y not(Z)
H(X,Y,Z) = X xor Y xor Z
I(X,Y,Z) = Y xor (X v not(Z))

In each bit position F acts as a conditional: if then Y else Z. The function F could have been defined using + rather than v since XY and not(X)Z will never have 1's in the same bit position.). If the bits of X, Y, and Z are independent and unbiased, the each bit of F(X, Y, Z) will be independent and unbiased. The functions G, H, and I are similar to the function F, in that they act in "bitwise parallel" to produce their output from the bits of X, Y and Z, in such a fashion that if the corresponding bits of X, Y, and Z are independent and unbiased, then each bit of G(X,Y,Z), H(X,Y,Z), and I(X,Y,Z) will be independent and unbiased. Note that the function H is the bit-wise "xor" or "parity" function of its inputs. This step uses a 64-element table T[1 ... 64] constructed from the sine function.

Let T[i] denote the i^{th} element of the table, which is equal to the integer part of 4294967296 times abs(sin(i)), where I is in radians.

Triple DES (Data Encryption Standard):

Descriptions:

Triple DES uses a "key bundle" which comprises three DES keys, K1, K2 and K3, each of 56 bits. The encryption algorithm is:

Cipher text = E_{k3} (D_{k2} (E_{k1}(plaintext)))

I.e., DES encrypts with K1, DES decrypt with k2, then DES encrypt with K3. Decryption is the reverse:

Plaintext = D_{k1}(E_{k2}(D_{k3}(cipher text)))

I.e., decrypt with K3, encrypt with k2, then decrypt with K1. Each triple encryption encrypts one block of 64 bits of data. In each case, the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying options two, and provides backward compatibility with DES with the keying option.

TRIPLE DES ALGORITHM:

In cryptography, Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a complete new block cipher algorithm. Triple DES uses a "key bundle" which comprises three DES keys, K1, K2 and K3 each of 56 bits (excluding parity bits). The encryption algorithm is:

Cipher text = E_{K3}(D_{K2}(E_{K1}(plaintext)))

Step 1: DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3. Decryption is the reverse:

Plaintext = D_{K1} (E_{K2}(D_{K3}(cipher text)))

Step 2: decrypt with K3, encrypt with K2, then decrypt with K1. Each triple encryption encrypts one block of 64 bits of data.

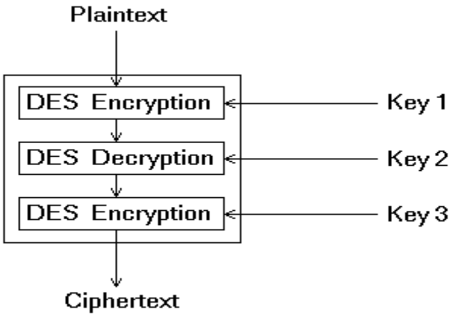


Fig: Triple DES

Elliptic Curve Cryptography:

ECC was first proposed by Koblitz and Miller, and its security was based upon the difficulty of Elliptic Curve Discrete Logarithm Problem (EDCLP). Compared with Public Key Cryptosystem (PKC), ECC offers a better performance because it can achieve the same security with a smaller key size. For example, 160-bit ECC and 1024-bit RSA have the same security level in practice. Thus, ECC-based authentication schemes are more suitable for smart cards and mobile devices than PKC-based ones. An elliptic curve is a cubic equation of the form as follows:

$$y^2+axy+by=x^3+cx^2+dx+e \qquad (1)$$

where a, b, c, d, and e are real numbers. In an elliptic curve cryptosystem (ECC), the elliptic curve equation is defined as the form of

$$E_p(a, b): y^2=x^3+ax+b (\text{mod } p) \qquad (2)$$

Over a prime finite field F_p, where a, b $\in F_p$, p>3, and $4a^3 + 27b^2 \neq 0 (\text{mod } p)$. Given an integer s$\in F^*_p$ and a point P $\in E_p$ (a, b), the point multiplications s P over E_p (a, b) can be defined as

$$sP = \{P + P + \cdots + P \text{ (s times)}\} (3)$$

Generally, the security of ECC relies on the difficulties of the following problems.

Definition 1 Given two points P and Q over E_p (a, b), the elliptic curve discrete logarithm problem (ECDLP) is to find an integer s $\in F^*_p$ such that Q=s P.

Definition 2 Given three points P, s P, and t P over E_p (a, b) for s, t $\in F^*_p$, the computational Diffie–Hellman problem (CDHP) is to find the point st P over E_p (a, b).

Definition 3 Given two points P and Q = s P +t P over E_p (a, b) for s, t $\in F^*_p$, the elliptic curve factorization problem (ECFP) is to find two points s P and t P over E_p (a, b). Up to now, there is no algorithm to be able to solve any of the above problems.

MODULES:

Finger Print Enrolment:

Fingerprint Enrolment is a method of registering user's biometric data for verification purposes. The quality of the fingerprint Enrolment is essential for the performance of the matching algorithm. The number of false rejects is very much dependent on the quality of the enrolled fingerprint template.

User Authentication:

In user authentication module, one-time password (OTP) is generated during registration process. One-time password is generated by random number generation algorithm. That password is sent to the user's mobile number for authentication. After that the user should give that one-time password to access internet banking process.

Finger Print Verification:

In fingerprint verification process the user application sends the fingerprint image of the person being verified. In finger print enrollment module, the user's finger print is stored in the database in fpt format. In verification process the user will give their finger print which is compared with the finger print that is already stored in the database by using SDK tool. If the finger print matches, then only the user will access their internet banking process.

Key Pair Generation:

In this module the public key and private key is generated for every user to access their banking process. The user's information is encrypted by using public key and private key. AES (Advanced Encryption Standard) algorithm is used for encryption and decryption.

Security Verification:

In security verification module, user's public key and private key is verified by the admin. All users may know every user's public key and only particular user is aware of the private key. The encrypted data is decrypted by using key pairs. The generated key pair is verified in this module.

Fund Transfer:

In this module, the users account is managed by the admin. The user can transfer, withdraw, deposit amount to any other account by using the key pairs and one-time password. One user can transfer money to another user by using public key and private key.

Log Maintenance:

This module is maintained by the admin. It shows each user's information and details about amount deposit, withdraw, transfer to another account. Every user's details, information and what they used in internet banking process is viewed by the admin.

CONCLUSION:

In this paper, we've addressed security problem for internet banking. In this we are implementing finger print reorganization technique for high security by using this finger print sensor the user only can authorize and can able to login, the unauthorized user can't able to login, and in this paper we are encrypting the fingerprints and storing into the database in this way we are providing high security for the net banking system. In this way if we use biometrics can provide high security.

REFERENCES:

[1] A piece by Miles Brignal, verified by Visa theme confuses thousands of web shoppers, cash news &amp; options, The Guardian, 2007.http://www.guardian.co.uk/money/2007/apr/21/creditcards.debt 03.12.2009.

[2] D. He, "Security flaws in a biometrics-based multi-server authentication with key agreement scheme," IACR Cryptology ePrint Archive, pp. 1–9, 2011, http://eprint.iacr.org/2011/365.pdf.

[3] E. J. Yoon and K. Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," The Journal of Supercomputing, vol. 63, no. 1, pp. 235–255, 2013.

[4]JCB international website, E-Commerce resolution J/Secure.http://www.jcbglobal.com/english/solution/ec.html 03.12.2009

[5] J. L. Tsai, N. W. Lo, and T. C. Wu, "Novel anonymous authentication theme exploitation good cards," IEEE Transactions on Industrial science, vol. 9, no. 4, pp. 2004–2013, 2013.

[6] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," IEEE Wireless Communications, vol. 11, no. 1, pp. 62–67, 2004.

[7]MasterCard Secure Code, master card Security: Safe &amp; Secure on-line looking. http://www.mastercard.com/us/personal/en/cardholderservices/se cure code/index.html 03.12.2009

[8]S. Kumari and M. K. Khan, "Cryptanalysis and improvement of 'a robust smart-card-based remote user password authentication scheme'," International Journal of Communication Systems, vol. 27, no. 12, pp. 3939–3955, 2014.

[9] Q. Xiao, Security problems in identity verification, Workshop on info Assurance and Security. us academy, West Point, NY, USA: Proceedings of the IEEE, 2005.

[10] Verified by Visa, a straightforward Arcanum protected identity checking service. http://www.visaeurope.com/merchant/handlingisapayments/cardnotpresent/verifiedbyvisa.jsp 03.12.2009.