ISSN: 0975-858

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Multi Server Authentication System Based on Finger Print and Secured OTP using ECC.

Mythili S, and Nirmalrani V*.

Department of Information Technology, Faculty of Computing, Sathyabama University, Chennai, Tamil Nadu, India.

ABSTRACT

Authentication is the process in which the credentials provided are compared with those in the database of authorized users with an authentication server. The growth of wireless communication network and transaction oriented services has created a demand for the protection of user credentials privacy. The encryption mechanism with the cryptographic keys is enabled to safeguard the data or documents that are exchanged over the e-mail or in commercial transaction. The cryptographic keys that are generated in terms of PIN and passwords are easily forgettable and are vulnerable to attacks. Hence the confidentiality of protecting the cryptographic keys is made efficient by the combination of biometric and cryptography. The use of biometric parameter fingerprint of a human is being used for multi server authentication along with ECC (Elliptic Curve Cryptography) for more security functionality. ECC offers security with smaller key size for faster computation, low power consumption in terms of memory and bandwidth. OTP is a password generated and received through mobile that is valid for a single login session of transaction which is prone to replay or eavesdropping attacks, which are overcome by ECC security systems.

Keywords: Authentication, Authorization, Biometric, ECC, OTP, Security.

**Corresponding Author*

INTRODUCTION

The growth of wireless communication networks paved way for the growth of e-commerce and transaction oriented applications, which includes e-banking, online shopping. Hence the authentication protocols become a major part in the communication systems. Thus there is a need for scalable and efficient mechanisms that well suits for both wired and wireless environments.

An authentication protocol is a cryptographic protocol designed specifically for data authentication among two entities. The security of this layer is most important as it provides a secure communication within the networks. The recent cryptography system is based on mathematical computation in collaboration with the computer practice. Cryptographic algorithms are designed in such a way that the computation of those algorithms is very hard to break or crack the keys used for the transaction.

Encryption key usually use the pseudo-random encryption algorithm to generate the keys, so that only authorized people can view the content or messages that are being transferred. To decrypt the message without the possessing key requires more computational resources and skills are required.

Fingerprints are one form of biometrics that can be used to identify and verify individuals. The analysis of fingerprints is done based on the several comparison features that are characterized as minutia points and ridges.

Elliptic curve cryptography is a public key crypto system based on the elliptic curve structure over finite field. ECC generates keys of smaller size when compared to other crypto system. Elliptic curve are applicable for pseudo random generators, digital signature and encryption. The size of the curve determines the difficulty of the problem. The ECC security is determined by the computation the point multiplication.

OTP are generated by pseudo random generators that are prone to replay attacks. OTP are difficult to memorize and hence they require mathematical technology to work. OTPs avoid issues associated with password based authentication. OTP requires a OTP calculator or a specific cell phone to generate a PIN.

The above technologies are used in a format to generate OTP using ECC along with the fingerprint to prevalent public key cryptography that offers higher security in smaller key size with reduced computation power, memory and bandwidth. The identification and authentication of individual using biometrics and cryptography provide a high level security model.

RELATED WORKS

Vanga Odelu, Ashok Kumar Das and Adrijit Goswami, describe a biometric based authentication system which is enable by the smart card system. The smart card is in-built with the user bio-metric component. This smart card is used for the user authentication. However they failed to propose an alternative when the provided smart card is stolen or broken and by pass the user authentication phase while they login to the bank system [15].

Dindayal Mahto, Dilip Kumar Yadav,came out with an idea of encorportaing the OTP mechanism with ECC algorithm for the e-commerce transaction. They also planned to implement a bio-metric parameter and used the palm vein of the user, where the OTP and the user palm vein are placed in two different server with no connection to each other. No recovery mechanism is in place when the password is forgotten or the mobile number is lost [2].

Yao-Jen Chang, Wende Zhang, and Tsuhan Chen, helped out with a key generation technique using the biometric parameter. They used Face detection to generate the keys. Those generated keys are used for the authententication of the user. Since face is used as parameter, the change in the face reation are not recognized which led to the drawback of this project [17].

A. Jayalakshmi, I. Ramesh Babu, cameout with the solution for secured key generation. Instead of Face detection they used fingerprint to generate keys. The keys are generated based on the minutiae points extracted from the fingerprint captured. The keys generated are stable and can be used on a longer run, which can be easily hacked as the keys are not for a particular session [4].

Swadeep Singh, Anupriya Garg, AnshulSachdeva made an analysis to meet the users cryptographic need. The RSA and ECC algorithm found to be effective which can be used for the session key generation. But when compared to RSA, ECC generated smaller key size that was most suitable for the hand held devices [14].

Yevgeniy Dodis, Leonid Reyzin, and Adam Smith used the idea of fuzzy logic for turning biometric information to keys that are used in cryptographic application. A fuzzy extractor is used to select a random value on the biometric input and an error-tolerant extraction to keep the extracted data closely matching to the original information. This system creates precise and uniformly distributed data [18].

PROPOSED SYSTEM

The existing paper proposes a security system which provides the security mechanism using the smart card enabled using the biometric parameter of the user. The paper fails to ensure the security once the smart card is stolen or lost, as the smart card mapping phase is eradicated. This leads to the data hacking, data leakage, as only the user defined passwords are used for login and transaction which can be easily hacked through shoulder surfing and guessing attacks.

These issues are mitigated by using a cryptographic method with biometric feature to protect customer privacy and against fraudulent activities. While comparing with other authentication systems, biometrics provide a strong security model. Cryptographic algorithm provides a mathematical calculation for transforming text to other form, which can’t be easily hacked by eavesdropper/cracker.

The biometric popularity and cryptography enhance the security system of all application area and became a common choice among most of the users/developers. The user identification using cryptography and biometrics model provides high assurance of security. Hence ECC algorithm is used to generate a Eight digit OTP for enhancing the security with user fingerprint template. The major influence of ECC compared RSA, is that it offers higher security with smaller key size per bit

The network computing environment is prone to replay attack/eavesdropping, which obtains user’s login-id and password. Once the credentials are captured by attackers, it is used to access the user’s account for fraudulent work. An OTP system is used to get away from this type of attack. OTP system works on both the client/user end, for the OTP generation and the server for verifying the OTP and the user authentication.

ARCHITECTURE OF THE PROPOSED SYSTEM

The client interface is used to interact with the end user in front end application, where the clients register themselves with the specified details. The details include Name, Date of Birth, Password, Mobile Number, E-mail ID, etc., which gets stored to the application server. The users are allowed to access the application only by their provided interface.

All the user activities are monitored and verified by the server before storing it to the database. The server establishes a connection to communication with the users to authenticate and update each user activity while they access through the application. In this way the server will prevent the unauthorized user from accessing the application.

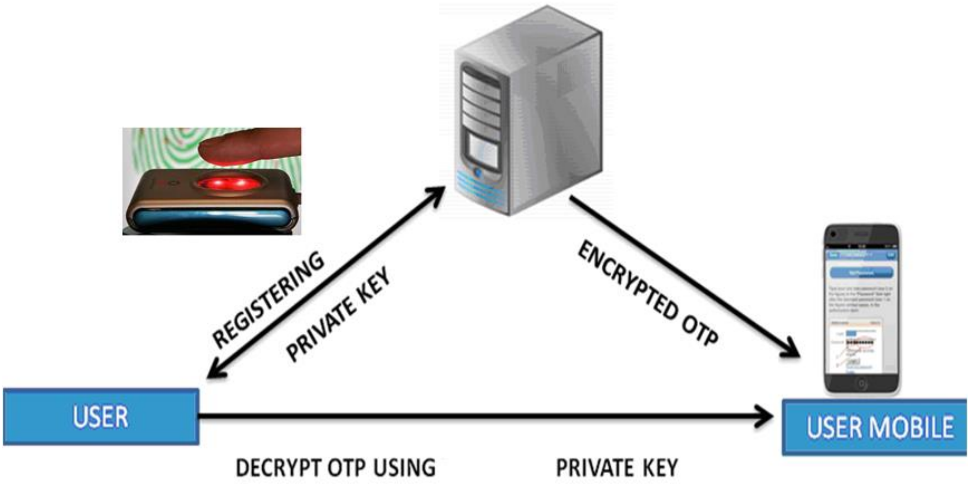

Figure. 1 Proposed System Architecture

IMPLEMENTATION PHASES OF THE PROPOSES SYSTEM

Verification Phase

In the Verification Phase, the Server will verify the User when they login into their account. The Server will verify the Finger print provided by the User while login with the Finger print provided by the User during the Registration Phase. If the Finger print is not matched, then the Server will not allow the User to access their account.

Fingerprint Enrollment

Fingerprint enrollment is the process of capturing the user finger print and storing it in the database. User need to enter their fingerprint twice for the system to process and generate a finger print template. The template is designed using the minutia take from the fingerprint sample and the hash value. Based on the template generated, the user fingerprint is matched each time for authentication

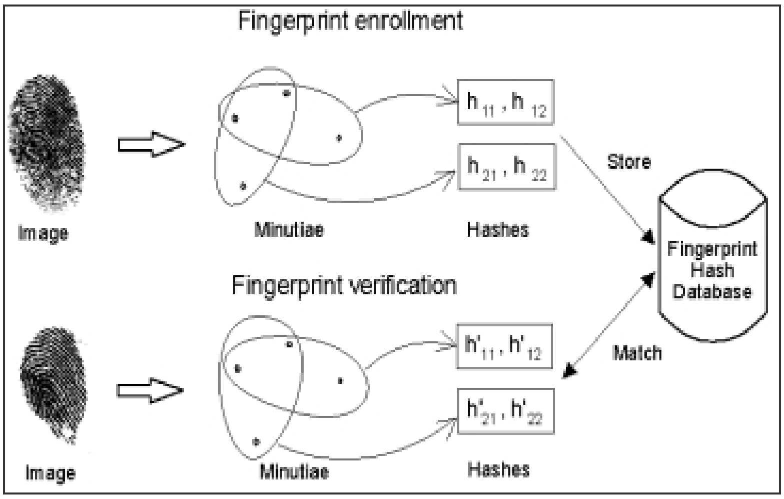

Figure. 2 Fingerprint Template Creation and Matching

Fingerprint Matching

Users provide his finger impression through optical sensor and system generates a template with the impression. It is compared in the finger library for a matching template

The matching is done in two ways:

- 1:1 matching, system compared the live finger impression with specific designated template.
- 1:N matching, or searching, system searches the whole finger library for the matching finger.

In both circumstances, system result is success or failure upon comparison with the template along with its hash value

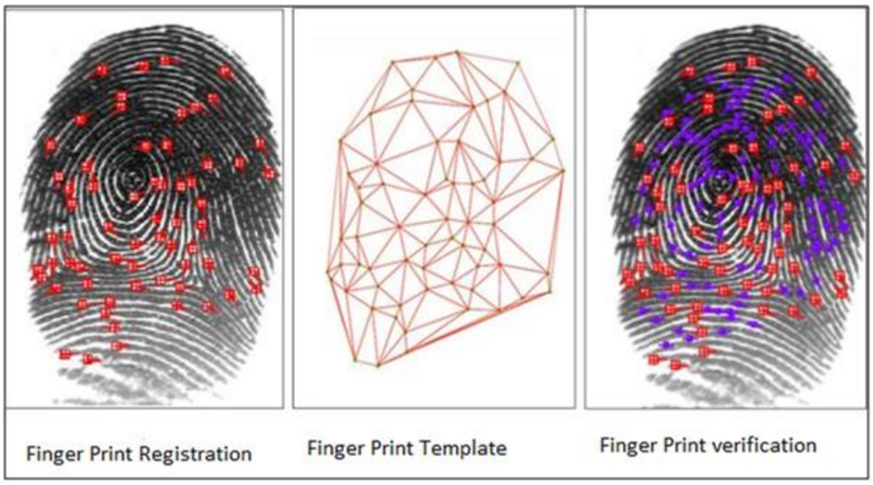

Figure. 3 Fingerprint Verification

OTP Verification Phase

A Onetime password (OTP) is a password that is valid for a single login session for transaction, on computer system or other digital device. OTPs help to avoid several issues that are associated with password – based authentication.

A number of implementations incorporate two factors:

- Authentication by ensuring that the one-time password requires access to an appliaction the user already has.
- Authentication by ensuring that a person require access to something that is known by the person(such as a PIN).

From the input data given by user the bank server send OTP (one time password) to user mobile for further access of account. If any wrong information is provided transaction/access will be denied.

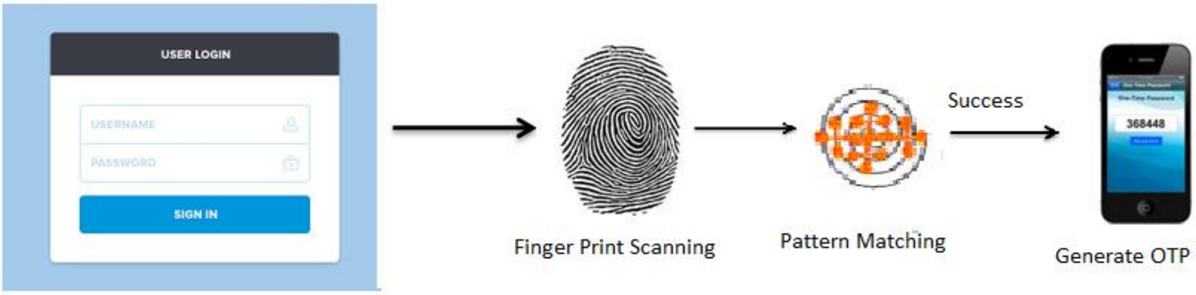

Figure. 4 OTP Generation

ALGORITHMS USED

ECC Algorithm

The ECC algorithm goes in hand with the mathematical calculation of elliptic curve formulae

$$y^2 = x^3 + ax + b \quad \mathrm{mod}\ p$$

Where y, x, a, b are all within the finite point p. also the curve condition has to fulfill the formula

$$4a^3 + 27b^2 \neq 0$$

Key Generation

Key generation is an important part where both public and private key are generated. The sender encrypts the message with receiver's public key and the receiver will decrypt with its private key.

Now, we have to select a number 'p' within the range of 'n'.

Using the following equation we can generate the public key

- Q = p * x
- p = The random number that we have selected within the range of (1 to n-1). x is the point on the curve.
- 'Q' is the public key and 'p' is the private key.

Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve. Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 - (n-1)].

Two cipher texts will be generated let it be C1 and C2.

- C1 = k*P
- C2 = M + k*Q

C1 and C2 will be used for decrypting the original message.

Decryption

We have to get back the message 'm' that was sent to us,

- M = C2 – d * C1

M is the original message that we have send.

Algorithm to get back the message

- M = C2 – d * C1
- Substitute the values of M, C1 and C2 in the formula,
- Hence C2 – d * C1 = (M + k * Q) – d * (k * P)
- = M + k*d*P – d*k*P (canceling out k * d * P)
- = M (Original Message)

Step 1 : select a curve Ep (a,b)
Step 2 : select base point G=(x1,y1) with large order n where nG=O(point of infinity)
Step 3 : A & B select private keys nA<n, nB<n
Step 4 : compute public keys: PA=nAG, PB=nBG
Step 5 : compute shared key: K=nAPB, K=nBPA

Encode and decode

Step 1 : Encode any message M as a point on the elliptic curve Pm
Step 2 : Encrypt the message Pm : Cm={kG, Pm+kPB}, k random int number 1<k<p-1
Step 3 : To decrypt, computes the product of the first point from Pm and his private key, n nB * (kG)
Step 4 : Takes this product and subtracts it from the second point from Pm(Pm + kPB) – [nB(kG)] = Pm + k(nBG) – nB(kG)= Pm

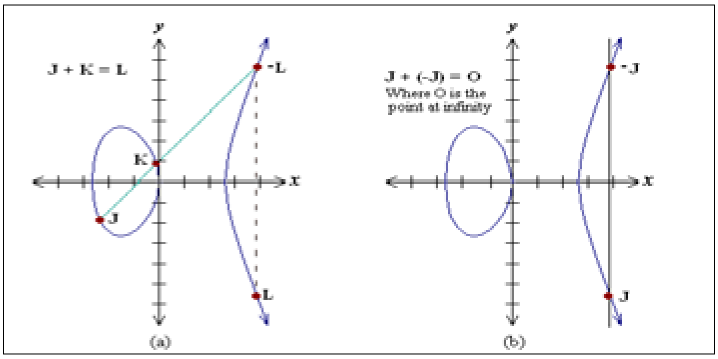

Fig. 5 ECC Curve Generation

PERFORMANCE ANALYSIS[14]

Key Size

Table.1: Key size comparison of ECC and RSA

ECC in bits	RSA in bits
106	512
112	768
132	1024
160	2048
210	3072

Encryption Time

Table 2: Encryption time of RSA and ECC

Algorithm	Encryption Time	Key Strength
RSA	4 ms	Less than 2ms
ECDSA	71 ms	33 ms
RSA	3 ms	5 ms
ECDSA	63 ms	70 ms

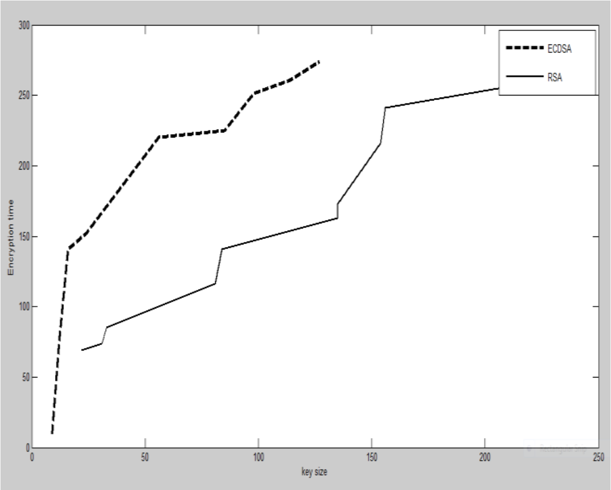

Figure. 6 Encryption Time vs. Key Size

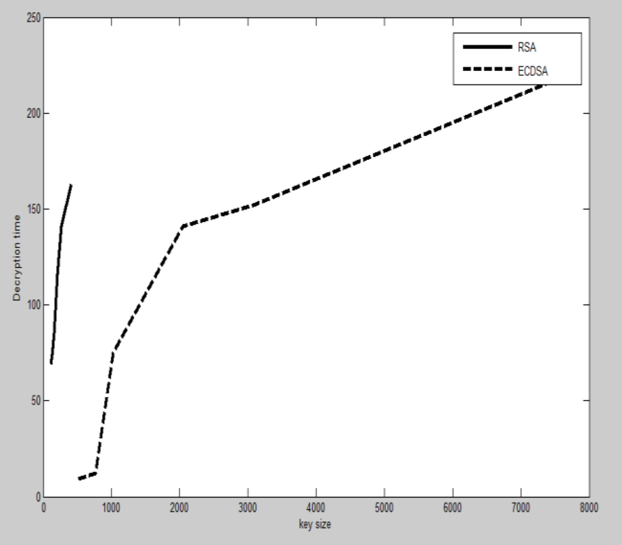

Figure. 7 Decryption Time vs. Key Size

CONCLUSION

Thus this paper has been proven to be more secure than the existing system with the smart card as the biometric parameter is used along with the Elliptic curve cryptography mechanism which generates the smallest key size. The solution offered is more suitable for hand held battery efficient devices that are portable and is in use extensively.

The solution must be used in various field where money transactions are involved like online recharges, ticket booking, payments etc., so that the security can be retained in all transactions where only the user is held responsible even for the wrong transaction. Though ECC generates smaller key size with hard manipulation, the curve generation and security of this algorithm is not fully understood. Hence a better algorithm should be used for security improvements.

ACKNOWLEDGEMENT

We thank Sathyabama University for providing us with various resources and unconditional support for carrying out this work.

REFERENCES

[1] Can Wang, Hong Liu and Xing Liu. Journal of Zhejiang University Science 2014; 15 (7): 525 – 536.

[2] Dindayal Mahto, Dilip Kumar Yadav. Computing for Sustainable Global Development (INDIACom) 2015; 1737 – 1742.

[3] Hao Feng, Chan Choong Wah. Information Management &Computer Security 2002; 10 (4): 159 – 164.

[4] A. Jayalakshmi, I. Ramesh Babu. IOSR Journal of Engineering 2012; 2 (2): 325 – 330.

[5] Lucas Ballard, Seny Kamara and Michael K. Reiter Security Symposium 2008; 61 – 74.

[6] C. Nandini and B. Shylaja. International Journal of Research and Reviews in Computer Science 2011; 2(4).

[7] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz. International Association for Cryptologic Research 2004; 119 – 132.

[8] Nirmalrani V and Sakthivel P. Journal of Pure and Applied Microbiology 2015; 9 (Spl. Edn. 2): 595 – 609.

[9] Nirmalrani V and Sakthivel P. National Conference on Emerging Trends in Information and Communication Technologies 2012; 101 – 107.

[10] Nirmalrani V and Sakthivel P. International Reviews on Computers and Softwares 2014; 9 (11): 1867 – 1874.

[11] Nirmalrani V and Sakthivel P. Journal of Theoretical and Applied Information Technology 2015; 76 (3): 296 – 308.

[12] P.Saravanan and P.Sailakshmi. Journal of Theoretical and Applied Information Technology 2015; 72 (1): 34 – 39.

[13] Sathish Kumar K, Sukumar R, Karthiyayini M. International Journal of Advanced Research in Computer Science & Technology 2014; 2.

[14] Swadeep Singh, Anupriya Garg and Anshul Sachdeva. International Journal of Computer Science and Communication Engineering 2013; Special issue on Recent Advances in Engineering & Technology: 211 – 216.

[15] Vanga Odelu, Ashok Kumar Das and Adrijit Goswami. IEEE Transactions on Information Forensics and Security 2015; 10 (9): 1953 – 1966.

[16] Yao-Jen Chang, Wende Zhang and Tsuhan Chen. International Conference on Multimedia and Expo, 2004; 3: 2203 – 2206.

[17] Yevgeniy Dodis, Leonid Reyzin and Adam Smith. International Association for Crptographic Research 2004; 523 – 540.