© 2016 IJSRST | Volume 2 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Multi Server Authentication System Based On Palm Vein Authentication and Secured OTP Using ECC

Yugapriya. R, Vijayanandhini. E, Seetha. J

Department of Information Technology, Dhanalakshmi College of Engineering, Chennai, Tamil Nadu, India

ABSTRACT

There is no proper security is implemented in online bank transaction even though lot of mobile user's presence. These textual passwords are easily hacked by the attackers using Guessing attacks and Shoulder Surfing attacks. To provide data communication security while sending the (OTP) One Time Password form bank transaction to customer using Elliptic Curve Cryptography (ECC) technique. The bank transaction server generates OTP and encrypts the OTP with ECC. To generate private key, we take the palm vein of the user and generates its hash value. The hash value is private key of user. During the authentication process, server sends the encrypted OTP to user. Then the user decrypt the OTP based on giving its private key. The user will be registering their palm vein and can select 3 different web portals like face book, gmail and twitter. After successful verification of palm vein user can select any one of the above set sample web sites so that the corresponding web sites gets login without its password.
Keywords: OTP-One time password, ECC-Elliptic curve cryptography, Palm vein, Biometric Authentication

I. INTRODUCTION

Electronic-commerce (E-commerce) is buying and selling of product using information and communication technology. It includes order accepting, order evaluating, supplying of order, billing, and the transfer of money. We are living in digital arena, where most of the business transaction is performed with the help of computers and computer networks. Computer networks provide platform to do e-commerce tasks, online banking, and sharing of information and many more within a fraction of seconds with the parties who may be located in any places of the digital world. The security is required for dual purposes. They are, i) to protect customers' privacy ii) to protect against fraud. While more than two parties communicate to each other then they worry about confidentiality, data authentication, non repudiation etc. In order to mitigate these issues, we can apply cryptography with biometric features. Biometrics is technique for measuring unique personal features, such as a subject's face, voice, palm-vein, fingerprint, gait, retina, or iris for personal recognition. It provides unique features to recognize an individual. Human being has been recognized by its appearance, gait, voice for thousands of years. While comparing with prevalent identification/ recognition/authentication, biometrics excels in providing strong security model. Cryptography is a mathematical technique of transforming text to intangible form, which can't be easily broken by eavesdropper/cracker.

It provides excellent data communication security in this digital world, provided keys size should be as per industry standard. There are many researches, who have suggested that biometrics provides competent technique for identifying and authenticating an individual, since it has been proved as reliable and universally acceptable identification and authentication methods in many application areas. The popularity of biometrics and cryptography provides foundation to the information security for becoming a common choice among all applications areas for enhancing their security . The identification and authentication of an individual using cryptography and biometrics, provides high assurance in its security model. We proposed an algorithm for enhancing the security of OTP using ECC with palm-vein biometric. The major influence of ECC compared to prevalent public key cryptography such as RSA, is

that it offers higher security per bit with smaller key size. Since ECC has smaller key size, hence it also reduced the computation power, memory and bandwidth. This research article has been organized as follows.

Out of many types of attacks, there is a type of attack on computing environment connected to the network, is replay attack/eavesdropping, which obtains legitimate user's credential such as login-id and password. Once the credentials are captured by attackers, then same are used to get accessed into the legitimate user's account to do some mischievous works. To get rid of this type of attack, an OTP is used. OTP has operations in both sides of the networks. On the client/user side, the appropriate OTP must be generated and displayed. On the server/host side, the server must be able to verify the OTP received from client side and permits the secure exchanging of the user's confidential information.

II. METHODS AND MATERIAL

ECC-Elliptic curve cryptography Algorithm

1. Server generates OTP.
2. Encryption module gets OTP as its input in a plain-text.
3. Encryption module generates cipher-text against plain-text of OTP.
4. Cipher-text gets transmitted over the channel to the user's cellphone.
5. User cellphone gets cipher-text.
6. Decryption module at recipient-end gets executed in a decryption enabled devices and plain-text gets generated.
7. The plain-text generated in the step 6, entered as input for OTP for the transaction in the input box of OTP.

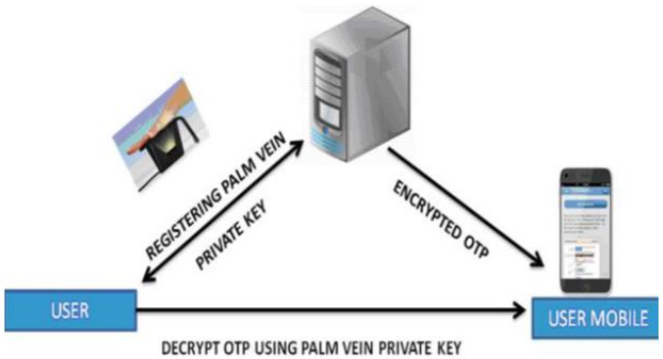

Figure 1. Architecture Diagram

III. RESULT AND DISCUSSION

Features	RSA	ECC
Efficiency	Low	High
Security	Low	High
Confidentiality	Less	More
Chances of hacking	More	Less
Throughput	Not accurate	Accurate

Figure 2. Palm Vein Authentication

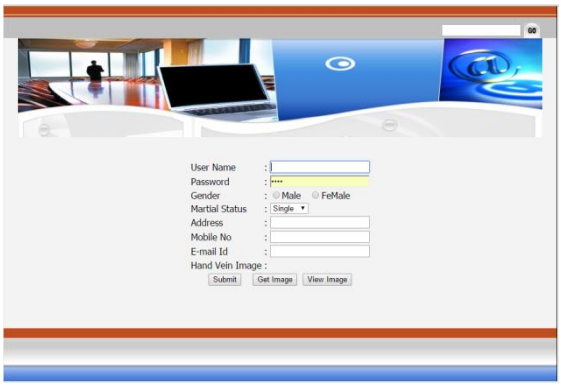

Figure 3. Registration

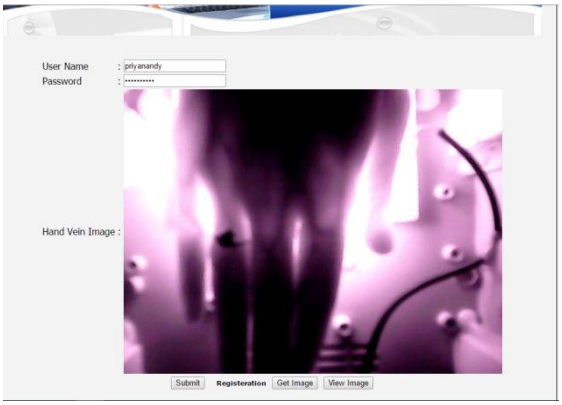

Figure 4. Login

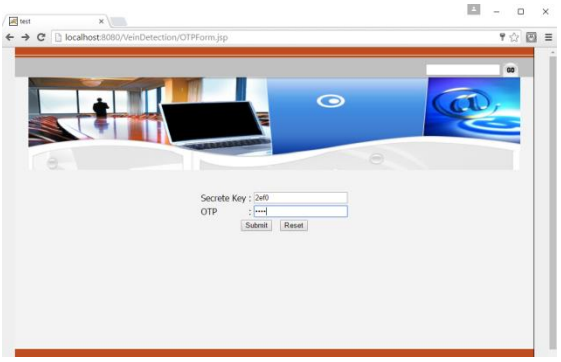

Figure 5. OTP

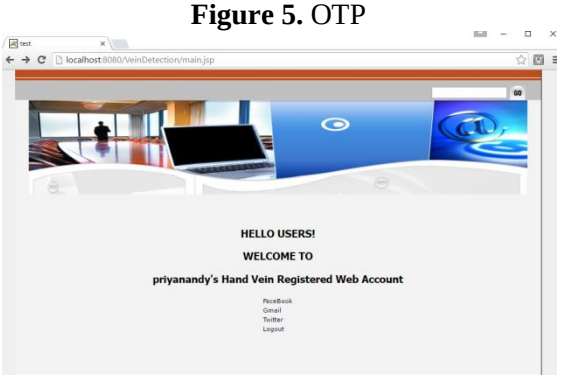

Figure 6. Opening Three Web Portals

IV. CONCLUSION

A very secure communication of the OTP in the network is illustrated with the help of ECC and palm vein biometric. The main advantage of ECC is that it requires very less key size and gives high level of security with cheaper biometric recognition system. Palm vein biometrics provides contact-less, hygienic and noninvasive and easy to use. At present e-commerce business is growing very rapidly. Most of the banking systems use OTP in the form of plain-text for the money transaction of e-commerce business, which is very insecure and totally dependent on the Short Message Services (SMS) providing communication client/server. This model enhances the drawback of the present ecommerce transaction system. This model also can be employed for any other type ofsecure data communication systems, which is communicated through SMS.

V. FUTURE ENHANCEMENT

The implemented method has generated private key from fused image and also elliptic curve parameters to find the elliptic curve and public key associated with the user.

This method can fatherly develop to generate the digital signature by using ECDSA and can also be merged with steganography.

VI. REFERENCES

[1] Lucas Ballard, SenyKamara, and Michael K. Reiter. The practical subtleties of biometric key generation.

[2] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid. Recommendation for key management part 1: General (revision 3). NIST Special Publication 800-57, pages 1–147, July 2012.

[3] Nandini C. and Shylaja B. Efficient cryptographic key generation from fingerprint using symmetric hash functions. Research and Reviews in Computer Science, International Journal of, 2(4), 2011.

[4] B. Chen and V. Chandran. Biometric based cryptographic key generation from faces. In Digital Image Computing Techniques and Applications, 9th Biennial Conference of the Australian Pattern Recognition Society on, pages 394–401, Dec 2007.

[5] W. Diffie and M.E. Hellman.New directions in cryptography. Information Theory, IEEE Transactions on, 22(6):644–654, Nov 1976.

[6] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Christian Cachin and JanL. Camenisch, editors, Advances in Cryptology- EUROCRYPT 2004, volume 3027 of Lecture Notes in Computer Science, pages 523–540. Springer Berlin Heidelberg, 2004.

[7] HaoFeng and Chan Choong Wah. Private key generation from online handwritten signatures. Information Management & Computer Security, 10(4):159–164, 2002.

[8] S.P. Ganesan. An asymmetric authentication protocol for mobile devices using elliptic curve cryptography. In Advanced Computer Control (ICACC), 2010 2nd International Conference on, volume 4, pages 107– 109, March 2010.