Journal of Engineering and Applied Sciences 12 (Special Issue 12): 9365-9369, 2017
ISSN: 1816-949X

A Secure One-time Password Authentication Scheme Using Elliptic Curve Cryptography with Fingerprint Biometric

Dindayal Mahto and Dilip Kumar Yadav
Department of Computer Applications, National Institute of Technology Jamshedpur,
831014 Jamshedpur, India

Abstract: Internet provides easy and convenient way to do e-Commerce transaction or transfer money from one account to another account using online banking system. In order to complete the transfer process, banking system generates One-Time Password (OTP) and then the generated OTP is sent to authenticate the transaction. If customer enters correct OTP, then transfer gets executed successfully. However, if impostor somehow able to know the customer's online accounts details with password and gets customer's registered Subscriber Identity Module (SIM), then impostor may do online shopping or transfer money successfully as per his will. This study proposes a secure one-time password authentication scheme using Elliptic Curve Cryptography (ECC) with fingerprint biometric in which only the legitimate customer can decrypt cipher OTP and upon decryption, the plain OTP gets appeared and then the customer has to enter the plain OTP into the Banking transaction page to make the transaction successful. Customer generates his/her private and public keys for ECC with the help of his/her fingerprint. This scheme suggests more security with less key length than RSA and there is no need to store any private key anywhere. Private key of the user gets generated when user needs to provide his/her authenticity.

Key words: Biometrics, elliptic curve cryptography, fingerprint, one-time password, customers, online

INTRODUCTION

Currently all the online banking transactions are performed with the help of global communication network system, i.e., internet. Internet provides instant communication platform to do e-Commerce tasks, online banking, sharing of information and many more with parties who may be located in any places of the digital era. However, internet also provides a platform to fraudsters for doing illegal or unethical transactions. The transactions security is required for dual purposes. They are to protect customer's privacy) to protect against fraud (Ganesan, 2009). While more than two parties communicate to each other then they worry about confidentiality, data authentication, non-repudiation, etc. (Mohammadi and Abedi, 2008). In order to mitigate these issues, we can apply cryptography with biometric features.

This study proposes a scheme to generate encrypted and authenticated OTP. The principal attraction of ECC compared to RSA is that it offers higher security per bit with smaller key size (Barker *et al.,* 2012). Since, ECC has smaller key size, hence, it also reduced the computation power, memory and bandwidth.

Literature review: One of the main problems of cryptography is the management of its key. It needs to be stored in such a way that stealing of the same is not possible. It needs to recall easily when requires but if size of it is big, then, recalling problem exists. In order to solve these problems, biometric traits may be used. A private key can be generated with help of biometric traits. As private key can be generated dynamically from one's biometric traits, so, there is no need to store private key anymore and network becomes more secure and safe. Some of the suggested approaches are given by Monrose *et al.* (2001), Feng and Wah (2002), Dodis *et al.* (2004), Teoh *et al.* (2004), Chen and Chandran (2007), Shibata *et al.* (2007), Wang and Plataniotis (2007), Ballard *et al.* (2008), Mohammadi and Abedi (2008), Rathgeb and Uhl (2010), Ogiela and Ogiela (2011) and Mahto and Yadav (2013, 2015a, b, 2017).

One-Time Password (OTP): An OTP is a short message service, used by commercial server to authenticate user's transaction. It is valid for only one transaction and until its usage or 30 min. The OTP system is designed to counter eavesdropping type of attack. There are two sides to the operation of the OTP system. On the client side, the

Corresponding Author: Dindayal Mahto, Department of Computer Applications, National Institute of Technology Jamshedpur, 831014 Jamshedpur, India

appropriate OTP must be generated. On the host side, the server must verify the OTP and permit the secure changing of the user's secret pass-phrase (Haller, 1995) or financial information.

Elliptic Curve Cryptography (ECC): Koblitz (1987) and Miller (1985) independently proposed the use of ECC. The use of ECC is very appealing for various reasons (Shibata *et al*., 2007; Ganesan, 2010). ECC is asymmetric-key cryptography (Diffie and Hellman, 1976) based on the elliptic curves. It is considered that ECC is suitable for small devices as it requires comparatively less or smaller parameters for encryption and decryption than RSA but with equivalent levels of security (Mahto *et al*., 2016). As far as ciphertext length is concerned, the already existing ASCII based cryptography is made more generalized and optimized in the sense of security aspect and the article also proposes maximum length of alphanumeric receiver identity is 40 (Sanyasi and Desai, 2016).

Fingerprint biometric: Finger-prints have been scientifically studied for many years in our society. The characteristics of fingerprints were studied as early as 1600's. Meanwhile, using fingerprints as a means of identification first occurred in the mid-1800's. Sir William Herschel in 1859, discovered that fingerprints do not change over time and that each pattern is unique to an individual. With these findings, he was the first to implement a system using fingerprints and handprints to identify an individual in 1877. By 1896, police forces in India realized the benefit of using fingerprints to identify criminals and they began collecting the fingerprints of prisoners along with their other measurements. Based on the study and analysis of existing authentication models, fingerprint authentication model is justified as best suitable model for Online Database Transaction Processing (OLTP) systems under heterogeneous environment (Rajagopalan and Vidyaathulasiraman, 2007).

MATERIALS AND METHODS

The architecture of the proposed scheme is shown in Fig. 1. In this study, we are using finger-print features of bank customers for generating secret keys and then the keys are used in ECC to provide data communication security while sending the OTP from Bank Transaction Server to customer.

Steps of the proposed methodology: Following are the steps of the proposed methodology:

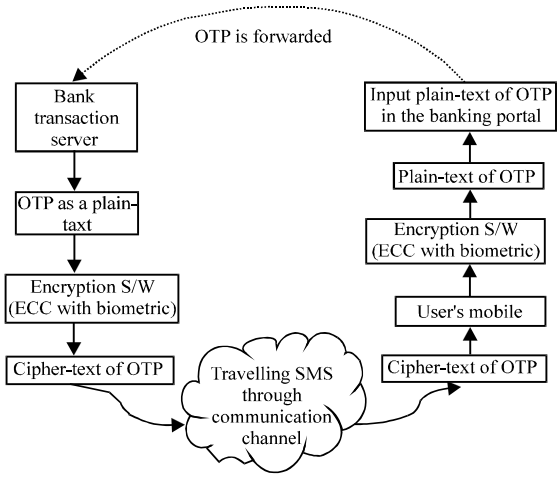

Fig. 1: Architecture of the proposed scheme

- Bank transaction server generates OTP
- Encryption module gets OTP as its input in a plain-text
- Encryption module generates cipher-text against plain-text of OTP
- Cipher-text gets transmitted over communication channel to the user's mobile
- User mobile gets cipher-text
- Decryption module at recipient-end gets executed in a decryption enabled devices and plain-text gets generated
- The plain-text generated in the step-vi, entered as input for OTP for the transaction in the input box of OTP
- If entered plaintext OTP is correct, transaction gets executed otherwise it gets cancelled

Method for generating public key and private key: First of all user's finger-print features are scanned through finger-print sensor unit and then same are extracted for registrations purpose known as enrollment and later these features are used for authentication. Steps for extracting minutia features are shown in Fig. 2. Thisstudy generates message digest of extracted minutia features of the customer's finger-print. The recently generated digest is considered to generate the private key of the customer.

Suppose the private key is d_A for user Alice and d_B for user Bob. Now to generate public key in ECC with the help with the above private keys is as follows: Both user choose the same large prime 'p' and the elliptic curve parameter 'a' and 'b' such that:

$$y^2 \bmod p = (x^3+ax+b) \bmod p \quad (1)$$

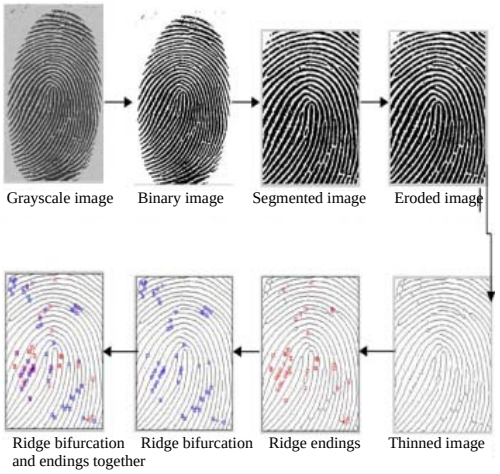

Fig. 2: Steps for feature extraction of a fingerprint

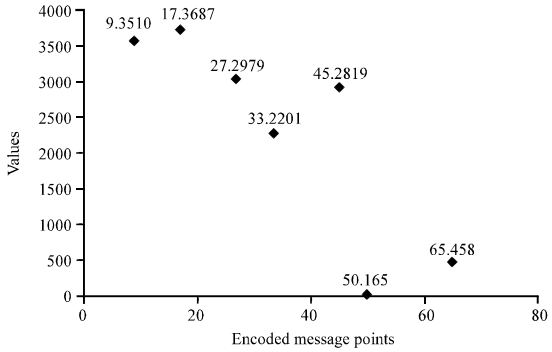

Fig. 3: Plain-text points before encryption

Where:

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

Now choose any one point G(x, y) from this elliptic curve. This point is called the base point of the curve. Compute $P_A = d_A * G(x, y)$, this P_A is called the public key of user Alice. To generate public key of user Bob, above three operations can be performed with the help of the private key of user Bob.

OTP message encryption: Bank Transaction server generates OTP like "32145688" to be sent to the user Bob. After that, first task is to encode the generated OTP message m as a point $P_m(x, y)$ as shown in Fig. 3.

It is the point P_m that will be encrypted as a cipher text and subsequently decrypted. After mapping of points with user OTP characters on elliptic curve, they can encrypt the message by following steps:

- Encryption Module encodes the OTP m as $P_m = (x, y)$
- The module chooses a public variable, k = 20

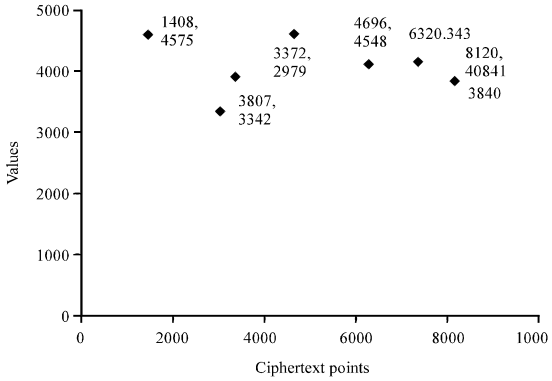

Fig. 4: Cipher-text points after encryption

Compute, x = m*k+i, varying i from 1 to k-1 and try to get an integral value of y. Thus, m is encoded as (x, y). The decoding is simple: m = floor ((x-1)/k). The cipher text is a pair of points: $C_m = k*G$, $P_m + k*P_B$. Encryption module sends this cipher text as shown in Fig. 4 to Bob.

OTP message decryption: For Message decryption Bob has to follow following steps:

- Bob multiplies the first point in the pair by his secret key and subtracts the result from the second point

$$= P_m + k*P_B - d_B*k*G$$
$$= P_m + k(d_B G) - d_B*k*G$$
$$= P_m$$

- The message P_m is the required message of Bob which is sent by bank transaction server is shown in Fig. 3
- Bob enters plain text of OTP in the bank transaction Input screen and then transaction gets executed

RESULTS AND DISCUSSION

The public key infrastructure implementation and encryption/decryption techniques face lots of problems such as key management, key storing, key privacy, etc. Our proposed approach can handle such problems. In the proposed model, digest of key features of finger-print are used as a private key, so that, there is no need to store any private key. The finger-print has lots of merits over other biometrics like it is more user-friendly and cheaper too. Finger-print recognition also has some outstanding features like universality, permanence, uniqueness and accuracy. As we are using ECC, so, we can achieve high level security with very shorter key size. Thus, it also solves the key size problem. ECC requires very complex

mathematical operation because of elliptic curve discrete logarithm problem. Therefore, security strength per bit is also very high.

CONCLUSION

In this study, a secure authentication scheme of an OTP in the communication network is illustrated with the help of ECC and finger-print biometric. The main strength of ECC is that it requires very less key size and gives high level of security. Finger-print is a cheaper biometric recognition system which allows the model to generate keys as and when require and hence no need to store any private key anywhere. At present online transaction is evolving rapidly. Most of the banking systems use OTP in the form of plain-text for the money transaction or transfer which is very insecure and totally dependent on the Short Message Services (SMS) providing communication client/server system. The proposed model enhances the security of one-time password authentication scheme for online transaction system. The proposed model also can be implemented for other SMS-based transaction system which requires higher OTP authentication security.

REFERENCES

Ballard, L., S. Kamara and M.K. Reiter, 2008. The Practical subtleties of biometric key generation. Proceedings of the 17th Symposium on USENIX Security, July 28-August 1, 2008, USENIX Association Berkeley, California, USA., pp: 61-74.

Barker, E., W. Barker, W. Burr, W. Polk and M. Smid, 2012. Recommendation for key management part 1: General (revision 3). Master Thesis, National Institute of Standards and Technology, Gaithersburg, Maryland, USA.

Chen, B. and V. Chandran, 2007. Biometric based cryptographic key generation from faces. Proceedings of the 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications (DICTA 2007), December 3-5, 2007, IEEE, Glenelg, Australia, ISBN:0-7695-3067-2, pp: 394-401.

Diffie, W. and M.E. Hellman, 1976. New directions in cryptography. IEEE Trans. Inform. Theory, 22: 644-654.

Dodis, Y., L. Reyzin and A. Smith, 2004. Fuzzy Extractors: How to generate strong keys from biometrics and other noisy data. Adv. Cryptol. EUROCRYPT, 3027: 523-540.

Feng, H. and C.C. Wah, 2002. Private key generation from on-line handwritten signatures. Inform. Manage. Comput. Secur., 10: 159-164.

Ganesan, R., 2009. A secured hybrid architecture model for internet banking (E-banking). J. Internet Banking Commerce, 14: 1-17.

Ganesan, S.P., 2010. An asymmetric authentication protocol for mobile devices using elliptic curve cryptography. Proceedings of the 2010 2nd International Conference on Advanced Computer Control (ICACC) Vol. 4, March 27-29, 2010, IEEE, Shenyang, China, ISBN:978-1-4244-5845-5, pp: 107-109.

Haller, N., 1995. The s/key one-time password system. Inf., 1: 1-12.

Koblitz, N., 1987. Elliptic curve cryptosystems. Math. Comput., 48: 203-209.

Mahto, D. and D.K. Yadav, 2013. Network security using ECC with biometric. Proceedings of the 9th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, January 11-12, 2013, Springer, Berlin, Germany, pp: 842-853.

Mahto, D. and D.K. Yadav, 2015a. Enhancing security of one-time password using elliptic curve cryptography with finger-print biometric. Proceedings of the 2nd International Conference on Computing for Sustainable Global Development (INDIACom), March 11-13, 2015, IEEE, New Delhi, India, ISBN:978-9-3805-4415-1, pp: 1737-1742.

Mahto, D. and D.K. Yadav, 2015b. Enhancing security of one-time password using elliptic curve cryptography with biometrics for E-commerce applications. Proceedings of the 2015 3rd International Conference on Computer, Communication, Control and Information Technology (C3IT), February 7-8, 2015, IEEE, Hooghly, India, ISBN:978-1-4799-4446-0, pp: 1-6.

Mahto, D. and D.K. Yadav, 2017. Secure online medical consultations using elliptic curve cryptography with iris biometric. Intl. J. Control Theory Appl., 10: 169-179.

Mahto, D., D.A. Khan and D.K. Yadav, 2016. Security analysis of elliptic curve cryptography and RSA. Proceedings of the World Congress on Engineering Vol. 1, Proceedings of the World Congress on Engineering Vol. 1, June 29-July 1, 2016, WCE-Razi Publishing, London, England, UK., ISBN:978-988-19253-0-5, pp: 29-34.

Miller, V.S., 1985. Use of elliptic curves in cryptography. Proceedings of the Conference on Theory and Application of Cryptographic Techniques (CRYPTO'85), August 18-22, 1985, Springer, Berlin, Germany, pp: 417-426.

Mohammadi, S. and S. Abedi, 2008. ECC-based biometric signature: A new approach in electronic banking security. Proceedings of the 2008 International Symposium on Electronic Commerce and Security, August 3-5, 2008, IEEE, Guangzhou, China, ISBN:978-0-7695-3258-5, pp: 763-766.

Monrose, F., M.K. Reiter, Q. Li and S. Wetzel, 2001. Cryptographic key generation from voice. Proceedings of the IEEE Symposium on Security and Privacy (S&P 2001), May 14-16, 2001, IEEE, Oakland, California, USA., ISBN:0-7695-1046-9, pp: 202-213.

Ogiela, M.R. and L. Ogiela, 2011. Image based crypto-biometric key generation. Proceedings of the 3rd International Conference on Intelligent Networking and Collaborative Systems (INCoS), November 30-December 2, 2011, IEEE, Fukuoka, Japan, ISBN:978-1-4577-1908-0, pp: 673-678.

Rajagopalan, S.P. and Vidyaathulasiraman, 2007. A proposed theory of using finger print as the primary tool of biometrical user authentication in an OLTP system under heterogeneous environment. J. Eng. Applied Sciences, 2: 846-848.

Rathgeb, C. and A. Uhl, 2010. Privacy preserving key generation for iris biometrics. Proceedings of the 11th IFIP TC 6/TC 11 International Conference on Communications and Multimedia Security (CMS 2010) Vol. 6109, May 31-June 2, 2010, Springer, Berlin, Germany, pp: 191-200.

Sanyasi, D.R. and A.K. Desai, 2016. Optimizing cipher text size for ASCII based cryptography using Matrices. Intl. J. Multi. Cryptology Inf. Secur., 5: 8-11.

Shibata, Y., M. Mimura, K. Takahashi and M. Nishigaki, 2007. A study on biometric key generation from fingerprints: Fingerprint-key generation from stable feature value. Proceedings of the 26th Conference on Security and Management (SAM'7), July 25-28, 2007, Huntington Press Publishing, Las Vegas, Nevada, USA., pp: 45-51.

Teoh, A.B.J., D.C.L. Ngo and A. Goh, 2004. Personalised cryptographic key generation based on faceHashing. Comput. Security, 23: 606-614.

Wang, Y. and K.N. Plataniotis, 2007. Fuzzy vault for face based cryptographic key generation. Proceedings of the Symposium on Biometrics, September 11-13, 2007, IEEE, Baltimore, Maryland, USA., ISBN:978-1-4244-1548-9, pp: 1-6.