MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

SECURED AND EFFICIENT PIN ENTRY METHOD USING ECC

Mr. Sandeep Patil, Mr. Anup Shinde, Mr. Nilesh shinde,
Mr. Shreyas Peadmkar, Prof. Laxmi Madhuri
Computer Engineering, Dr.D.Y.Patil School of Engineering
Lohegaon, Pune, India.

Abstract: *Security of one-time password (OTP) is important because now a days most of the e-commerce transactions are achieved with the help of this device. OTP is used to counter Replay attack/overhearing. Replay attack or overhearing is type of attacks happening network-connected computing environment or isolated computing environment. Alternative problem with most of the current implementation of security models is storing of top-secret keys. Cryptographic keys are regularly kept in un–secured way that can either be solved/social-engineered or obtained through brute force attacks. This becomes a poor link and leads integrity issues of sensitive data in a security model. To overcome the above problem, biometrics is united with cryptography for developing solid security model. This paper suggests enhanced security model of OTP method via ECC using palm vein biometric. This model also suggests better security with lesser key size than additional prevalent public key cryptographic model .The cryptographic keys are not required to remember or keep anywhere, these keys are generated as and when wanted.*

Keywords*: One-Time Password (OTP), Elliptic Curve Cryptography (ECC), Biometrics, Palm Vein.*

1. INTRODUCTION

Electronic-commerce is buying and marketing of product using material and communication technology. It contains order accepting, order evaluating, delivering of order, billing, and the transfer of money. We are living in digital arena, anywhere most of the business transaction is done with the help of computers and computer networks. Computer networks offer stage to do e-commerce tasks, online banking, and sharing of information and several more within a fraction of seconds through the parties who may be set in any places of the digital world. The security is required for twin purposes. They are: I) defend customers' privacy II) to defend against fraud. Although more than two parties communicate to each other then they concern about privacy, data authentication, non-repudiation. In order to alleviate these issues, we can put on cryptography with biometric features. Biometrics is technique for measuring sole personal features, such as a subject's face, voice, palm-vein, fingerprint, gait, retina, or iris for personal recognition. It provides unique features to identify an

individual. Human being has been recognized by its appearance, walk, voice for thousands of years. While comparing with prevalent identification/recognition/authentication systems, biometrics excels in providing solid security model. Cryptography is a mathematical method of transforming text to intangible form, which can't be easily cracked by overhearing/cracker. It provides excellent data communication security in this digital world, providing keys size should be as per industry standard. There are many investigates, who have recommended that biometrics provides competent technique for identifying and authenticating an individual, since it has been proved as reliable and commonly acceptable identification and authentication techniques in many application areas [3]. The acceptance of biometrics and cryptography offers foundation to the information security for becoming a common choice between all uses areas for enhancing their security systems. The identification and authentication of an separate using cryptography and biometrics, provides high guarantee in its security model.

This paper proposed an algorithm for enhancing the security of OTP using ECC (Elliptic Curve Cryptography) with palm vein biometric. The major influence of ECC compared to predominant public key cryptography such as RSA, is that it provide higher security per bit with lesser key size [2]. Since ECC has lesser key size, hence it also compact the computation power, memory and bandwidth.

The problem of asymmetric cryptography is the administration of private key. There should not be any way to access someone else's private key. It needs to store in such a place which is secure from illegal accessing. This is vulnerable to attack of hackers/crackers/ overhearing. This creates large problem in any security model. Thus it can be solved by biometrics. Private Key can be created straight by the biometrics features. Since cryptographic keys can be made as and when required from subject's biometrics sole features, so there is no any requirement of storing cryptographic keys and hence network becomes more secure and safe. Shoulder Surfing is particularly effective in crowded places because it is easy to spot somebody as they. Fill out a form Enter their pin at an automated teller machine or a POS terminal Use a phone card at community pay phone Enter a password at a cybercafé, public or university libraries. Enter a code for a rented locker in a civic place such as swimming pool or airport. Shoulder surfing can also be done at a space by binocular or other vision enhancing device. Inexpensive, minute closed circuit television cameras can be hidden in ceilings ,walls to observe data entry. To avoid shoulder surfing, it is guided to protection paper word or keypad from view by using one's body hand. Keystroke logging (extra often called as "key logging or key loggers") is the action of tracking (or logging) the keys struck on a keyboard, typically in such a manner so that the person using the keyboard is unaware that their actions are being observed. There are numerous key logging methods , ranging from hardware and software based approaches to electromagnetic and acoustic analysis.

2. LITERATURE SURVEY

2.1 One-Time Password (OTP): Out of numerous types of attacks, there is a type of attack on computing environment connected to the network, is replay attack/overhearing, which obtains legitimate user's credential such as login-id and password. Once the credential are took by attackers, then similar are used to get accessed into the valid user's account to do

some mischievous workings .To get rid of this type of attack, an OTP method is used. OTP method has operations in both sides of the networks system. On the client/user side, the appropriate OTP must be made and displayed. On the server/host side, the server must be able to confirm the OTP(One Time Pin) received from client side and licenses the safe exchanging of the user's confidential information [11]

2.2 ECC: In 1985, Neil Koblitz and Victor S. Miller self-sufficiently proposed the use of ECC. Since 1985, there have been a lot of studies regarding ECC. The use of ECC is very attractive for various reasons [8], [17]. The first and probably most main reason is that ECC offers improved security with a smaller key size than any other prevalent asymmetric cryptography.ECC with 160-bit provides equal security to RSA with 1024-bit and ECC with 224-bit provides like security to RSA with 2048-bit [10]. There is high demand of lesser keys sizes especially in software applications running on devices taking memory constraints because lesser key size takes less memory for storing cryptographic keys. ECC wants lesser memory resources than prevalent unequal cryptography. In order to crack ECC, the needs of computation power, fixed twice than that requirements for cracking RSA. It delivers greater level of security due to its complicated mathematical process. ECC's mathematical formulas are more difficult and complex than mathematical formulas Used for predominant asymmetric cryptography. Due to this goal, elliptic curves are considered as effective techniques for cryptographic purposes.

2.3 Palm Vein Biometric: In the palm vein method, vascular designs of user's palm are considered. Complex vascular patterns have many features and that features provides appropriateness for user's authentication [27]. Due to absence of hair in palm there is no obstacle for taking blood vessel pattern, and there is also no effect on changing color of skin. In this biometrics, sizes of hemoglobin flow through veins are used .

3. OBJECTIVE

It could be tiny time consuming to find the letters in the grid. But the main purpose of enhancing the security and solving the problems.

4. PROPOSED SYSTEM

The proposed "Grid Based Authentication" system provides the solution to the problems like "Shoulder Surfing ","Duplicate login pages" ".It improves the security of the web based system and makes it difficult for the attackers to decipher the keyword of the user. Using a palm vein pattern sensor unit is present here the blood vessel pattern having deoxidized hemoglobin is taken, which is displayed and based on the blood vessel pattern, an unique image is generated for palm and this unique image is used for making keys for the user in our model.

5. ADVANTAGES

- Its construction is simple and requires less maintenance.
- Low cost.

- Portable in size and Easy transportable.
- Less Manual Work.

6. SYSTEM ARCHITECTURE

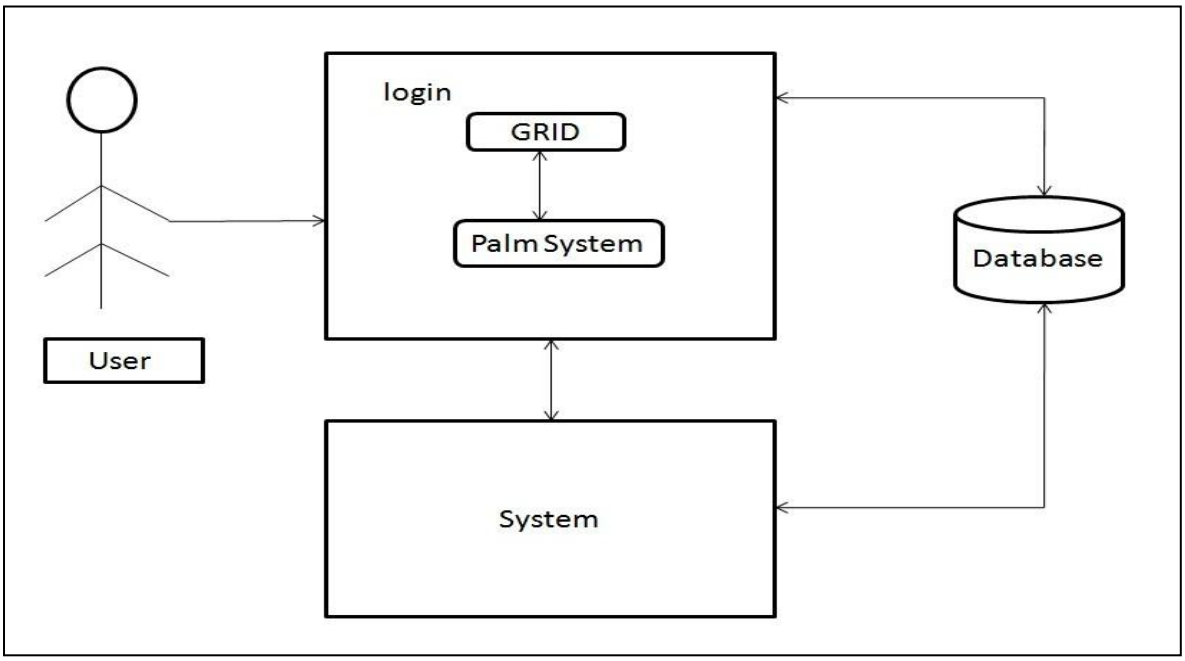

Fig.1: Architecture of proposed system

7. DESCRIPTION

The block diagram of Secured and Efficient PIN Entry Method Using ECC is shown in figure, it consists of a grid based system and palm based system. User can login with either grid or palm based system. By login with a grid system user will receive OTP useful for secure transaction and if user login with palm based system then it will match the image with registered palm image stored in database. Successful matching will give access to user for secure transaction.

8. CONCLUSION AND FUTURE SCOPE

In this paper a very secure communication of the OTP (One Time Pin) in the network is demonstrated with the help of ECC and plain vein biometric. The advantage of ECC is that it requires very fewer key size and gives higher security with cheaper biometric recognition system. contact-less, hygienic as well as noninvasive and informal to use system. At present e-commerce business is increasing very rapidly. Most of the banking organizations use OTP in the form of plain-text for the money business of e-commerce business, which is very unconfident and totally dependent on the Short Message Services (SMS) supplying communication client/server. The proposed model enhances the disadvantage of the present ecommerce transaction system. The proposed model also can be employed for any other type of safe data communication systems, which is connected through SMS.

ACKNOWLEDGMENT

It gives us great pleasure in presenting the project report on 'Secured and Efficient PIN Entry Method Using ECC'. We would like to take this chance to thank our internal guide Prof. Laxmi Madhuri for giving us all the help and guidance we needed. We are really grateful to him for his kind support. His valuable suggestions were very helpful. We are also grateful to Prof. Soumitra Das, Head of Computer Engineering Department, DYPSOE, Lohegaon, Pune and to our Project Co-ordinator Prof. J. L. Chaudhari for their indispensable support, suggestions and motivation during the entire course of the project. In the end special thanks to our Director Dr. S. S. Sonawane who encouraged us and created a healthy environment for all of us to learn in good possible way. We also thank all the educators' staff of our college and technicians for their help in creation this project a successful one.

REFERENCES

[1]. Lucas Ballard, Seny Kamara, and Michael K. Reiter. The practical subtleties of biometric key generation. In Proceedings of the 17th Conference on Security Symposium, SS'08, pages 61–74, Berkeley, CA,USA, 2008.USENIX Association.

[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]. 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.

[5]. Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz. Comparing Elliptic Curve Cryptography and RSA on 8-bit cpus. In Marc Joye and Jean-Jacques Quisquater, editors, Cryptographic Hardware and Embedded Systems - CHES 2004, volume 3156 of Lecture Notes in Computer Science, pages 119–132. Springer Berlin Heidelberg, 2004.

[6]. S. Mohammadi and S. Abedi. ECC-based biometric signature: A new approach in electronic banking security. In Electronic Commerce and Security, 2008 International Symposium on, pages 763–766, Aug 2008.

[7]. Can Wang, Hong Liu, and Xing Liu. Contact-free and pose-invariant hand-biometric-based personal identification system using rgb and depth data. Journal of Zhejiang University SCIENCE C, 15(7):525–536, 2014.