Intensify the security of One Time Password using Elliptic Curve Cryptography with Fingerprint for E-commerce Application

Deepak Yadav¹, Dhiraj Malwe², K. Shıvam Rao³, Puja Kuma⁴, Puja Yadav⁵, Prerana Deshmukh⁶

Department of Computer Technology
PCE, Nagpur, Maharashtra, India

Abstract:
Security of one-time password (OTP) is crucial as a result of these days most of the e-commerce transactions are performed with the assistance of this mechanism. OTP is employed to counter replay attack/eavesdropping. Replay attack or eavesdropping is one type of attacks on network-connected computing environment or isolated computing setting. For achieving 112 bits of security level, Rivest Shamir and Adleman (RSA) formula desires key size of 2048 bits, whereas Elliptic Curve Cryptography (ECC) desires key size of 224-255 bits. Another issue with most of the present implementation of security models is storage of secret keys. Cryptographical keys are usually unbroken in en-secured manner that may either be guessed/social-engineered or obtained through brute force attacks. This becomes a weak link and leads integrity problems with sensitive information in a very security model. To beat the on top of drawback, biometries is combined with cryptography for developing sturdy security model. This paper suggests an increased security model of OTP system using ecc with fingerprint biometric. This model conjointly suggests higher security with lesser key size than different prevailing public key crypto-model. The cryptographical keys are not needed to memorize or keep anyplace; these keys are generated as and once required.

Keywords: Biometrics, Elliptic Curve Cryptography (ECC), One-Time Password, Online Banking, Fingerprint.

I. INTRODUCTION

Electronic-commerce (E-commerce) is shopping for and marketing of product using data and communication technology. It includes order accepted, order evaluating, supply of order, billing, and also the transfer of cash [9], we have a tendency to live in digital arena, wherever most of the business dealings is performed with the assistance of pcs and computer networks. pc networks offer platform to try and do e-commerce tasks, on-line banking, and sharing of data and lots of additional among a fraction of seconds with the parties who is also set in any places of the digital world. the safety is needed for twin functions. They are, i) to guard customers’ privacy ii) to guard against fraud [21]. Whereas quite 2 parties communicate to every alternative then they worry regarding confidentiality, knowledge authentication, nonrepudiation etc [17], as so to mitigate these problems, we are able to apply cryptography with biometric options. Biometrics is technique for measuring distinctive personal options, like a subject’s face, voice, palm-vein, fingerprint, gait, retina, or iris for private recognition. It provides distinctive options to acknowledge an individual. Human being has been recognised by its look, gait, and voice for thousands of years. Whereas examination with current identification/recognition/authentication systems, biometrics excels in providing robust security model. Cryptography could be a mathematical technique of reworking text to intangible type, that can’t be simply broken by eavesdropper/cracker. It provides excellent electronic communication security during this digital world, provided keys size ought to be as per business norms. There are several researches, who have recommended that biometry provides competent technique for characteristic and authenticating a personal, since it's been tried as reliable and universally acceptable identification and authentication ways in several application areas [3], the recognition of biometry and cryptography provides foundation to the knowledge security for turning into a standard selection among all applications areas for enhancing their security systems. The identification and authentication of a personal using cryptography and biometry, provides high assurance in its security model. [14], [31], we have a tendency to plan associate degree formula for enhancing the safety of OTP exploitation computer code with palm-vein biometric. the key influence of computer code compared to current public key cryptography like RSA, is that it offers higher security per bit with smaller key size [2]. Since computer code has smaller key size, therefore it additionally reduced the computation power, memory and information measure..

II. RELATED WORK

The main downside of uneven cryptography is that the management of personal key. There mustn’t be any way to access somebody else’s non-public key. It must store in such an area that is protected against unauthorized accessing, this is often prone to attack of hackers/crackers/eavesdropper. This creates huge downside in any security model, so it is resolved by the employment of biometrics. non-public key is generated directly by the biometrics options. Since cryptological keys is generated as and once needed from subject’s biometrics distinctive options, therefore there's no any demand of storing cryptological keys any longer and therefore network becomes safer and safe.

III. OBJECTIVES

The objectives of proposed work are as follows:
1) To develop a security system to overcome the drawbacks of the earlier security system.
2) The system attempts to enhance the security of OTP via fingerprint biometric.
3) The system also helps increase security in e-commerce applications.

IV. METHODOLOGY

1) Flowchart of the system

A. Steps of the proposed methodology Following are the steps of the proposed methodology:
1) Bank Transaction 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 communication channel to the user’s mobile.
5) User mobile 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.

B. Method for generating public key and private key
First of all users’ fingerprint options are scanned through fingerprint pattern scanner then same are filtered for registrations purpose referred to as enrolment and later fingerprint options are used for authentication. Biometric technique needs enrolment of user’s first then additional task like authentication using verification and identifications are done as shown within the Fig.4. To get personal key, we tend to take the fingerprint of the user and generate its hash value with the assistance of MD5 scientific discipline hash function. This resultant hash value is the personal key of the user. Suppose this price is da for user Alice and dB for user Bob.

Now to generate public key in ECC with the help with this private key is as follows:
1) Both users choose the same big prime number ‘p’ and the elliptic curve parameters ‘a’ and ‘b’ such that they fulfill the requirements for the curve formulas number (4) and (5) 2) Now choose any one point G(x, y) from this elliptic curve. The G becomes base point of the curve. 3) Compute PA = dA * G(x, y); This PA is called the public key of user Alice.

To generate public key of user Bob same operation can be performed with the help of the private key of user Bob.

C. OTP Message Encryption
Bank Transaction server generates OTP to be sent to the user Bob, the generated OTP message m gets encoded as a points Pm (x, y) as shown in the Fig. 5. The points Pm get encrypted as a cipher text and later at receiver-end get decrypted. Once mapping of points [22] with user OTP characters on elliptic curve are done, then the encryption of the message are performed as given below steps:
1) Encryption Module encodes the OTP m as Pm = (x, y)
2) The module chooses a public variable, k=20. 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 (xy). The decoding is simple: m=floor((x-1)/k).

The cipher text is a pair of points: Cm = k * G, Pm + k * PB

D. OTP Message Decryption

For Message decryption Bob has to follow following steps:
1) Bob does multiplication on pair’s first point by his secret key and then does subtraction of result from the second point: =Pm + k * PB - db * k * G =Pm + k(dbG) - db(k * G) =Pm
2) The message Pm is the required message of Bob, which is sent by Bank Transaction Server is shown in the Fig. VI-D.
3) Bob enters plain text of OTP in the Bank Transaction Input screen and then transaction gets executed.

VI. CONCLUSION

In this paper, a really secure communication of the OTP within the network is illustrated with the assistance of ECC and fingerprint biometric. The main advantage of ECC is that it needs terribly less key size and provides high level of security with cheaper biometric recognition system. Fingerprint biometrics provides contact-less and non-invasive and simple to use system. Nowadays e-commerce business is growing terribly quickly. Most of the banking systems use OTP within the type of plain-text for the cash dealing of e-commerce business that is incredibly insecure and completely hooked in to the Short Message Services (SMS) providing communication client/server. The projected model enhances the disadvantage of this ecommerce dealing system. The projected model can also be used for the other sort of secure electronic communication systems that are communicated through SMS.

VII. ACKNOWLEDGEMENT

First and foremost we want to thank our Guide Asst. Prof. Prerana Deshmukh for constant encouragement. With great
pleasure and gratefulness we extend our deep sense of
grateful to Dr. Nita Thakre, HOD, Computer technology,
Priyadarshini College of Engineering. Lastly we wish each
and every person involved in making our dissertation
successful.
Thank You

VIII. REFERENCES

[1]. Dindayal Mahatao and Dilip Kumar Yadav “Enhancing
Security of OTP using ECC with biometric” Institute of
Electrical and Electronics Engineers February 2015

[2]. Nandini C. and Shylaja B. Efficient cryptographic key
generation from fingerprint using symmetric hash functions.
Research and Reviews in Computer Science, International

[3]. N. Haller. The s/key one-time password system. Network

[4]. Yoichi Shibata, Masahiro Mimura, Kenta Takahashi, and
Masakatsu Nishigaki. A study on biometric key generation
from fingerprints: Fingerprint-key generation from stable
feature value. In Security and Management, pages 45–51,
2007.

[5]. Koblitz N. Elliptic curve cryptosystems. Mathematics of