International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

OTP Intense Cryptography and Palm Vein Voguish on Online Transaction

E. Meena[1], Dr. G. Ravi[2]
[1]Research Scholar, Department of Computer Science, Jamal Mohamed College, Tiruchirappalli, Tamilnadu, India
[2]Associate Professor & Head, Department of Computer Science, Jamal Mohamed College, Tiruchirappalli, Tamilnadu, India

ABSTRACT

Online-Transaction (OLT) is a widespread data processing system in today's initiatives that simplify and accomplish transactions-oriented applications using computer networks such as the internet. The online transactions are based on the one -time password (OTP), which is transmitted over an untrusted communication channel (internet). Security for the OTP is essential in order to prevent the reply occurrences during the transactions. In the existing system, RSA algorithm involves 2048 bits key size in order to achieve 112 bits security level. But in the proposed, Triple Data Encryption Standard (3DES) which performs 56-bit key size multiplies by three times of DES for high level security. In order to overcome these above inconsistencies and to develop a robust security model OTP using Biometrics is combined with cryptography. This paper proposes better security models with 3DES that engenders adequate block size value and aggrandize security of OTP using palm-vein as biometric**.**

Keywords: Online Transaction (OLT), One-time password (OTP), Triple Data Encryption Standard (3DES), Palm vein Biometric

I. INTRODUCTION

Nowadays everyone habits e-commerce application for trade-off the products like trendy online shopping. E-commerce is commonly engraved as Electronic Commerce. Electronic commerce is the term which is used to designate the activities of the business process over the communication channel. Electronic commerce is a way of responsibility business over large electronic networks such as the Internet. E-commerce platform appeals on various applications tools like E-commerce, Electronic Fund Transfer (EFT), e-banking, Processing the online transactions, Electronic Data Interchange (EDI), Automated information gathering systems and inventory management system etc. E-commerce greatly assists transactions between companies and consumers (B2C), between one company and another (B2B), and between individual consumers (C2C). It can also contract with transferring of software, accessing the video games, or downloading data from the articles or the journals.

In the Digital era, all these e-commerce solicitations are interconnected through the internet channel, which deals with private bank details of the customers and sharing of information to the other parties. The security should be providing to 1) the client's personal information and 2) to protect against the fraud [1]. The security disputes like data confidentiality, data authentication, Non-repudiation. To overwhelm these security issues, Cryptography with Biometric features can be applied. The Biometric is a phenomenon which is used for measuring the unique features of an individual, five of the most generally used physical biometrics patterns such as facial expression, voice, fingerprint, eye retina or iris, palm-vein for peculiar Identification purpose.

Cryptography with biometric progresses a sturdy security model for the e-commerce applications. The Biometric mechanism in the Cryptography contains two phases: a) Enrollment and b) Verification. During the Enrollment stage, a designated biometric feature from the individual is attained as a sample. In the verification stage, an updated biometric sample is assimilated. The main objectives of the Biometric features in the cryptography mechanism are: i) Identification and ii) Authentication [2]. The biometric

identification method is the process of matching individual personal features to the outsized set of system users. And the Biometric authentication process deals with verifying that the individuals are an authorized person or not [3] [4].

Cryptography is a secured system which is used to renovate the text to imperceptible format, which cannot be fragmented easily by the third party. This Mechanism delivers exceptional security to the information which is transmitted to the other user of the communication channel in this digital world. The proposed algorithm is used for enhancing the security of the One Time Password with 3DES by palm vein as a Biometric feature. The major objective of using 3DES is to establish secret key, which deals the highest security per bit by engendering key size that is used for Cryptography technique.

II. RELATED WORKS

The OTP is used as a multi-factor authentication method. D. Mahto and D. K. Yadav have proposed an approach that increases the security level of OTP. They have used the ECC algorithm and the palm vein biometric. It provides a double layer protection in an online transaction. Since the execution cost of palm vein biometric is high, it limits the number of users of the proposed system.

Dindayal Mahto, Dilip Kumar Yadav, came out with an idea of incorporating the OTP mechanism with ECC algorithm for the e-commerce transaction. They also planned to implement a biometric parameter and used the palm vein of the user, where the OTP and the user palm vein are placed on two different servers with no connection to each other. No recovery mechanism is in place when the password is forgotten or the mobile number is lost [5]. Biometric features are used to generate the private keys. Since cryptographic keys can be generated as and requisite from the individual's biometrics unique characteristics, so it reduces the efforts of storing the cryptographic keys anymore and that develops strong secure and safe network. The following are the some of the suggested approaches [6].

The palm-vein imaging typically requires infrared illumination which is one component of multi-spectral illumination for the multispectral palm print imaging. Therefore, the multispectral palm print images essentially secure palm-vein details. However, as compared to the bi-spectral approaches, such as in multispectral methods [9] introduce a significant amount of additional computations (which often adds to the cost of the device) while accomplishing very little or marginal performance improvement.

Yingbo Zhou and Ajay Kumar proposed two new approaches to enhance the performance of palm-vein-based identification systems. The proposed methodology attempts to more effectively accommodate the potential deformations, rotational and translational changes by encoding the orientation conserving features and utilizing a novel region-based matching scheme. Furthermore, it evaluates the performance improvement in both verification and recognition scenarios and analyzes the influence of enrollment size on the performance and also related for its superiority using single image enrollment on two different databases [10].

III. ONE TIME PASSWORD (OTP)

Nowadays most of the e-commerce transactions are executed with the help of one-time password (OTP). It is used to overcome the replay attack or eavesdropping on the communication channel. Now, most of the e-commerce applications use OTP to process the online transactions. But this OTP is transmitted over the communication network called the Internet.

OTP is a password that is valid for a single login session for a transaction, on the computer system or other cardinal devices. OTPs help to evade several issues that are accompanied with password – based authentication. In this process, the isolated details such as login id and password can be easily hacked or easily obtain by hackers/ frauds. This process should secure the account transfers creating by OTP. The OTP generated by systems and send to the user's updated mobile no. or system mail id. This OTP is the double layered protection apart from the user's id and passwords. This OTP can assist to use the user's information not matched to the system information like as the user place, type of transactions then also OTP creation to open accounts for further process. The OTP is one of the trends in online transactions.

IV. TRIPLE DATA ENCRYPTION STANDARD (3DES)

Triple DES (3DES) is termed as a Triple Data Encryption Standard, which is generating the Triple Data Encryption Algorithm (TDEA) symmetric key block cipher. It uses the Data Encryption Standard (DES) cipher algorithm triple times to each data block. The original DES cipher's key size of 56 bits was typically sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES which is shown in Figure.1 provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

Advantages of 3DES

- 3DES is easy to implement (and accelerate) in both hardware and software.
- 3DES is pervasive: most systems, libraries, and protocols comprise support for it.

A.Encryption

$$C= E_{K3}(D_{K2}(E_{K1}(P)))$$

Initially, the 3DES encrypts with K_1, *decrypt* with K_2, and then encrypt with K_3.

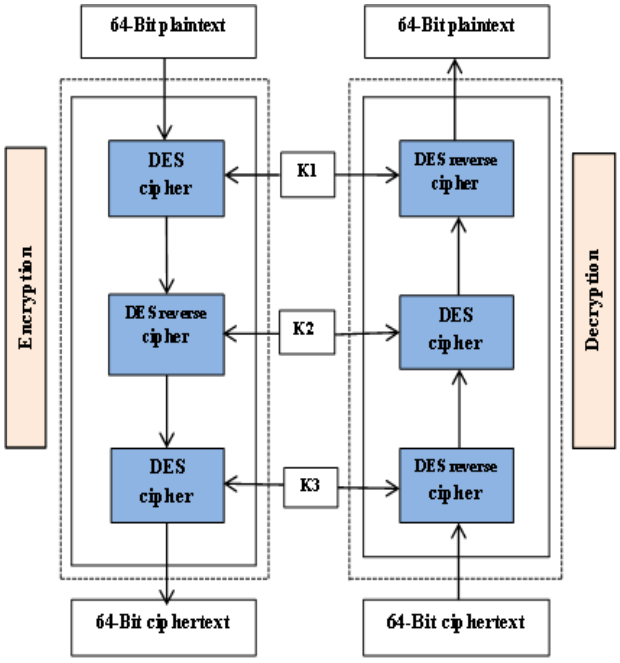

Figure 1. Triple DES

B. Decryption

$$P = D_{K1}(E_{K2}(D_{K3}(C)))$$

i.e., 3ES decrypt with K_3, *encrypt* with K_2, and then decrypt with K_1.

Each triple encryption encrypts with one block of 64 bits of data.

In each case, the middle operation is the inverse of first and last key. The strength of the algorithm is when using the keying option 2 and sends backward compatibility with DES with keying option 3.

B. Key Generation

The standards describe three keying options:

Keying option 1

All three keys are independent.

Keying option 2

K_1 and K_2 are independent, and $K_3 = K_1$.

Keying option 3

All three keys are same, i.e. $K_1 = K_2 = K_3$.

Keying option 1 is the robust, with $3 \times 56 = 168$ independent key bits.

Keying option 2 delivers less security, with $2 \times 56 = 112$ key bits. This option is robust than single DES encrypting twice, e.g. with K_1 and K_2, because it protects against meet-in-the-middle attacks.

Keying option 3 is equal to DES, with only 56 key bits. It provides backward compatibility with DES because the first and second DES operations terminate out.

Each DES key is technically stored or transferred as 8 bytes, each of odd parity, so a key bundle requires 24 bytes for option 1, 16 for option 2, or 8 for option 3.

D. 3DES modes

The 3DES implementation unit supports the following modes:

• ECB (electronic code book)

• CBC (cipher block chaining)

In addition to these modes, the DEU can compute Triple-DES. Triple-DES is an extension to the DES

algorithm in which every 64-bit input block is sorted out three times.

V. PALM VEIN BIOMETRIC

Palm vein technology is also called as the vascular technology in a biometric. It identified over the comparisons of the patterns of blood vessels which is an evident surface of the skin. In this biometric the identification the basic information's and vein blood vessel patterns recorded by CCD behind the surface and already stored in the main systems, this data are processed, compressed and digitalized for the subject.

Figure 2. Pam Vein Scanner

This palm vein technology is growing in popularity. There is no hindrance for capturing the blood vessel patterns and there is no effect on the variation in the color of the skin, because due to the absence of hair on the palm. In this biometric technique, haemoglobin flows over veins measurements are used [7].

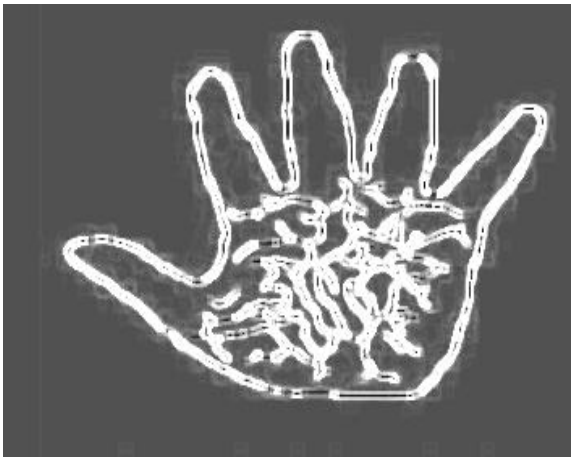

Figure 3. Extracted Palm Vein

By using a palm vein pattern sensor it as shown in the Figure.2 the blood vessels patterns which have deoxidized haemoglobin are taken. These blood vessels patterns, with a unique image is generated for the palm which is shown in the Figure.3 and these images are used for creating keys for the user network model.

VI. PROPOSED MODEL

Palm vein technologies are one of the auspicious new advances which are intensely secure. It is the world's first contactless individual ID framework that uses the vein patterns in human palms to affirm an individual's identity. The palm vein image of each individual is converted into data points which are cannot be easily depredation, and then it also encoded and stored by the software and registered along with the other details in his profile as a reference for future comparison at the time of transactions.

In an RSA algorithm, key generation is slow and it also performs slow singing process and decryption. But the proposed algorithm of 3DES, the encryption method is related to the one in unique DES but applied 3 times to increase the encryption level. Here is a comparison of key size for the existing and proposed model.

The architecture of the proposed model is shown in the Figure.4. In this paper, the palm vein features of the Bank customer/clients are used to generate the secret keys, and then these keys are essential in the 3DES technique in order to provide the data communication security during the transmission of the OTP from the Bank transaction server to the customer.

A. Steps of Proposed Methodology

Following are the steps of the proposed methodology. There is also the encrypted and decrypted data will perform the very high level of security over the communication channel for transferring information. Palm vein technology is highly secure, efficient and voguish in this digital world.

1) OTP is generated by the Bank Server.
2) OTP as a plain text that is encrypted for the given input.
3) An Encryption will process under the functions of 3DES with biometric
4) The generated cipher text is sent to the user's mobile over the communication channel.
5) The User gets the cipher text.

6) At the receiver end, the encryption module is executed and decryption will be processed with the help of 3DES and biometric.

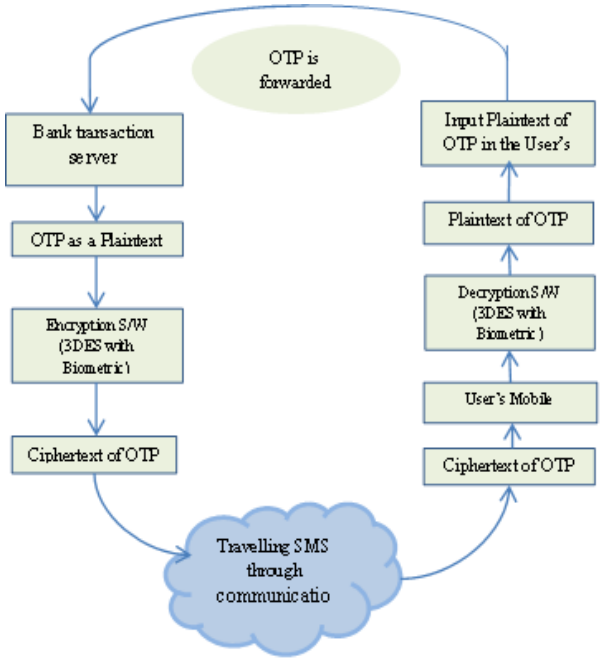

Figure 4. Architecture of Proposed Model

7) The original plain text which is generated at the user's end that is entered as an input for the transaction of the input box for the OTP.

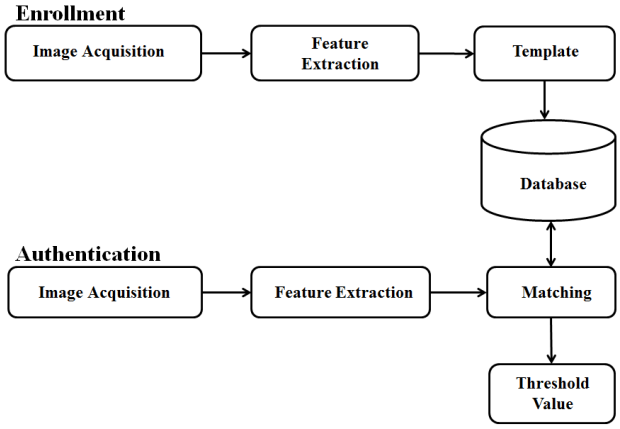

Figure 5. Enrollment and Authentication

During the registration purpose, all the user's palm vein features are scanned through the sensor unit and then the same is filtered for enrollment. This palm vein features are used for an authentication process. The Biometric mechanism requires the enrollment of the users and then it further deals with another process like verifications and identifications which are shown in Figure.5.The functions such as image acquisition, feature, extraction, and matching will be performed in this proposed model.

VII. RESULT

Many of the symmetric cryptography infrastructures have problems like key management, sharing of the keys, etc. In this proposed method, these security issues can be prevented. Palm vein has excellent features like universality, permanence, uniqueness, and accuracy.

TABLE.1 Generation of OTP using 3DES

NO	Message (OTP)	Mode	Encryption (Base 64)	Decryption (OTP)
1	2789	ECB	m+gL6O+EbEA=	2789
2	3593	ECB	kTpdbiBTgRk=	3593
3	9012	ECB	TXVX1ebWtJc=	9012

The triple DES algorithm performs with 64 bit block size value for both encryption and decryption. And it evaluates ECB mode as shown in the Table .1.

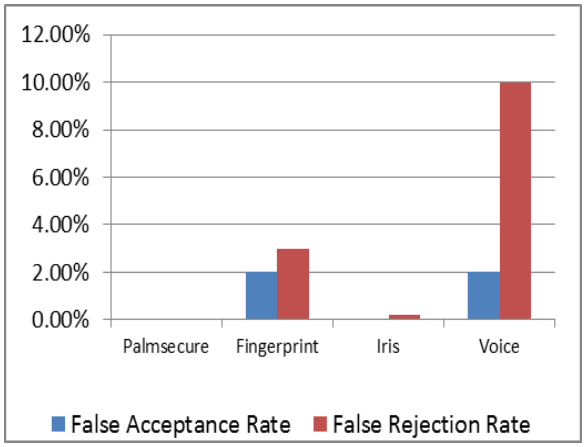

Figure 6. Comparison of various biometrics

The comparisons of various biometrics are represented in Figure.6 which shows palm vein is highly secure than other biometric technologies.

VIII. CONCLUSION

This paper proposes palm vein authentication with cryptography. This technology is highly protected because it secures the information which is confined within the body. It is also a robust and secure model represented for the OTP with the help of 3DES and palm vein as a biometric feature. 3DES is an algorithm which provides high confidentiality and throughput. The major advantage of 3DES consists of low power consumption and triple layer security. Furthermore, the palm vein technology is contactless feature gives it a hygienic advantage over other biometric authentication technologies. The proposed model enhances the disadvantages of the existing system of the e-commerce and it can also be valid for the other type of secure data, which are based on the SMS.

IX. REFERENCES

[1]. Ganesan R. and Vivekanandan K. A secured hybrid architecture model for internet banking (e-banking). Journal of Internet Banking and Commerce, 14(1):1-17, 2009.

[2]. 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.

[3]. Andrew Teoh Beng Jin, David Ngo Chek Ling, and Alwyn Goh. Personalized cryptographic key generation based on Face Hashing. Computers& Security, 23:606-614, 2004.

[4]. Dindayal Mahto and DilipKumar Yadav. Network security using ECC with Biometric. In Karan Singh and Amit K. Awasthi, editors, Quality, Reliability, Security and Robustness in Heterogeneous Networks, 853. Springer Berlin Heidelberg, 2013.

[5]. Dindayal Mahto, DilipKumar Yadav. Computing for Sustainable Global Development (INDIACom) 2015; 1737 - 1742.

[6]. 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.

[7]. NELSON Mike, WRIGHT Tim, and ASHIDA Ken. Fujitsu's palm secure-based e-pose system for school cafeteria. Fujitsu scientific and technical journal, 43(2):236-244, 2007. Eng.

[8]. Ding, Yuhang Ding, Dayan Zhuang and Kejun Wang, "A Study of Hand Vein Recognition Method", The IEEE International Conference on Mechatronics & Automation Niagara Falls, Canada, July 2005, pp. 2106-2110.

[9]. J.-G. Wang, W.-Y. Yau, A. Suwandy, and E. Sung, "Person recognition by fusing palmprint and palm vein images based on "Laplacianpalm" representation," Pattern Recognit., vol. 41, pp. 1514-1527, Oct. 2007.

[10]. Yingbo Zhou and Ajay Kumar, Senior Member, IEEE, "Human Identification Using Palm-Vein Images", IEEE Transactions on Information Forensics and Security, vol. 6, no. 4, December 2011.

[11]. P. Ghosh and R. Dutta, "A new approach towards Biometric Authentication System in Palm Vein Domain"