SECURITY & THREATS RELATED TO ONLINE ELECTRONIC TRANSACTIONS

HARSHIL.B.JANI
M.TECH(D.C),INDUS UNIVERSITY

Abstract— *Secure electronic transaction (SET) is a significant-commerce protocol designed to improve the security of creditcard purchases. In this paper we discuss various securitymeasuresand protocols which are used till date and are still usedfor the security of online transaction in which electronic cashflows from buyer to the supplier or merchant. Various issuesdiscussed in this paper are SET protocol, Authenticated and KeyAgreement for P2P-Based Networks, Mutual Authenticationbetween Cardholder and Merchant, Biometric Mechanism for enhanced Security of Online Transaction, Using a Mobile Deviceto Enhance Customer Trust in the Security of RemoteTransactions, Digital content mediator for secure P2P onlinetransactions,Sensitive Data Transfer Security Model finally wewill see the SMS-Based Authentication Scheme.*

KEYWORDS— *Digital content mediator, Authentication, P2PBased Networks, Secure electronic transaction (SET), SensitiveData,M-commerce.*

I.INTRODUCTION

Protocols in cryptography allowpeopletocommunicate securely across an open network, even in the presence of otheragents. Such protocols are hard to design and many of researchers have developed ways of finding errors or proving that the protocol is correct. The verification of the registration protocols of Secure electronic transaction (SET), a large and

important protocol lforelectroniccommerce,proposedbyVisaand MasterCard and is a industry standard. SET presents twomajor challenges to previous methods.

- It involves many levels of encryption, using many combinations of symmetric cryptography, asymmetric cryptography&hashing.
- It does not assume that each agent has his own privatekey so that the only problem which is remained is the distribution of the public keys, but allows cardholders to decide their asymmetric key
- ➢ .The first challenge comes from SETs is how to use digital envelopes. One part of a digital envelope is the main body of the message.
- ➢ The other part contains that key and is encryptedwith the recipient's public encryption key. The two parts may have some common data, possibly hashed, in order to confirmthat they are tied together. This combination of symmetric andasymmetric encryption can be considered more efficient thanusing asymmetric cryptography alone and it makes a protocolmuch harder to decide.

(2)The second challenging aspect of theSET protocols is the possibility for cardholders and merchants to make public/private key pairs as they want for theirelectronic credentials.

II. SET REGISTRATION PROTOCOLS

Everyone normally pay for goods purchased over theInternet by giving the merchant their credit card details. To prevent this information from unwanted people from stealing the card number, the message undergoes a session of the securesockets layer (SSL) protocol. In this arrangement thecardholder and merchant should trust each other. That requirement is undesirable even in face-to-face transactions,but over the internet it has risks.
- The cardholder is protected from eavesdroppersbutnot from the merchant itself. Some merchants are dishonest. They do not protect the sensitive information.
- The merchant also needs to be protected and shouldhave some protection against dishonest cardholders who supply an invalid credit card number.It seems contrary to popular belief that it is the merchant who has the most to lose from fraud. Law in many countriesprotects the cardholder. The aspect of registration of merchant as well as cardholder is dealt with here. First figure shows theregistration of cardholder and the second one registrationof merchant.
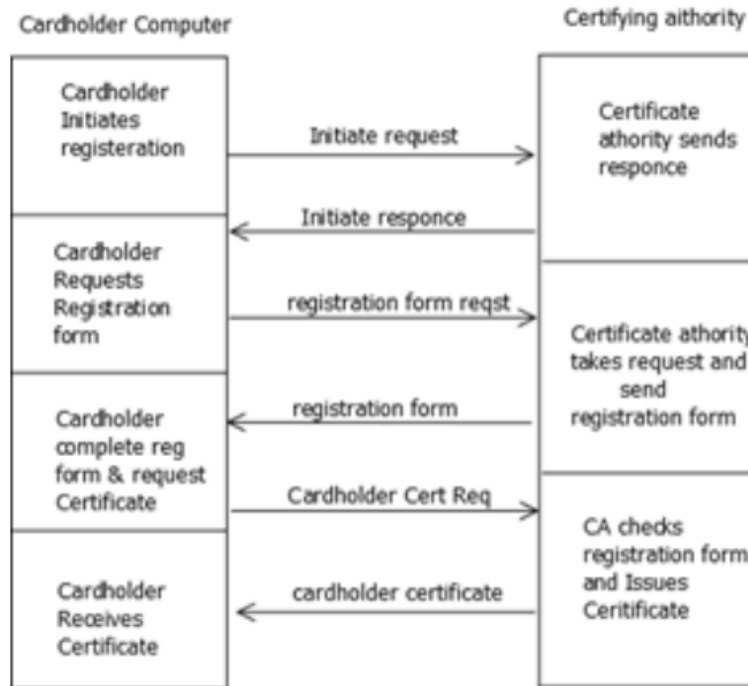
Figure1: Cardholder Registration
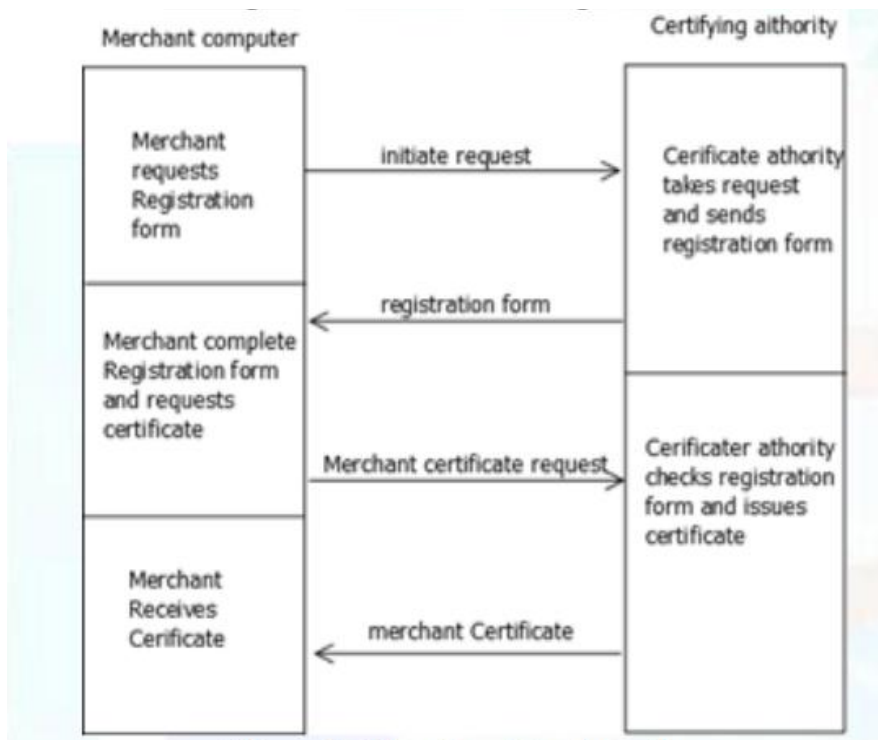
Figure2: Merchant Registration

III. SENSITIVE DATA TRANSFER SECURE.

In the study of barcodes work related to sensitive datatransfer secure (SDTS) algorithms is proposed by many authors for security and applications of the same. The revisedmodel of SDTS is below provides the benefits of the following.

• Firstly, this makes the system more complex becausethe changes made are at byte level and thus, it is very difficult to predict by the hackers that what exactly is happening.

• Secondly, this provides tightly coupled securitybecause the complexity of the system is increased to larger extent.

Figure3: Sensitive data transfer secure

SDTS model is converting the secure information into barcodes first, this information converting can be done by pixel manipulations and then convert the barcode image into bytearrays they may be even odd byte array. Finally, it encrypts the bytes using standard RSA algorithm. The detail view of the model is shown in figure is the revised model.

➢ With Reference:
to the online transaction processing apps, the information to be
processed is not sent over the network in unsecured manner,but a security key corresponding to the information
is picked

from database table to secure the real time data or informationfrom being exposed on the network or to the people who arenot intended to view it. Then secure/secret key before exposingto the network is processed under various layers and convertinginto unreadable form. A quick response barcode is created forthe key and then it is splittedinto two identical barcode likeimages which is also called False Images. Each false image isconverted to a byte array it may be even or odd. Each byte
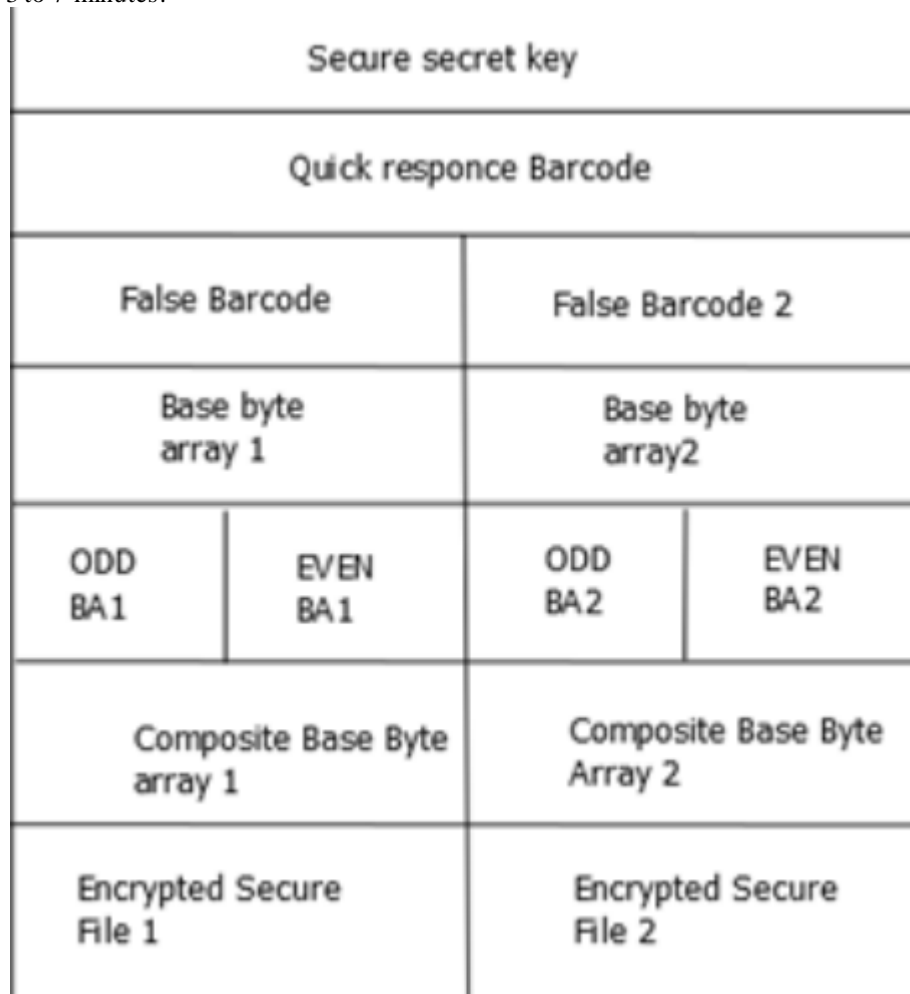
array is further splitted into two;

• picking all the odds together

• picking all evens together.

Then these odds and evens are combined and the sequenceis formed. We want to change the information completely in apredefined manner such that it gets tougher to identify theinformation within the arrays. The transformed array is then encrypted using the RSA algorithm

➢ . The two encrypted secure files are sent over thenetwork secured or unsecured network with some random time difference of 3 to 7 minutes.

Secure secret key	
Quick responce Barcode	
False Barcode	False Barcode 2
Base byte array 1	Base byte array2
ODD BA1 / EVEN BA1	ODD BA2 / EVEN BA2
Composite Base Byte array 1	Composite Base Byte Array 2
Encrypted Secure File 1	Encrypted Secure File 2

➢

Figure4: Top view of SDTS

A. Onsite Transaction Procedure

This is the scenario where the cardholder is physicallypresent at the merchant's site or shop and gives his smartcard at the merchant's terminal after selecting the goods andservices to purchase. Onsite transaction steps are as follows.
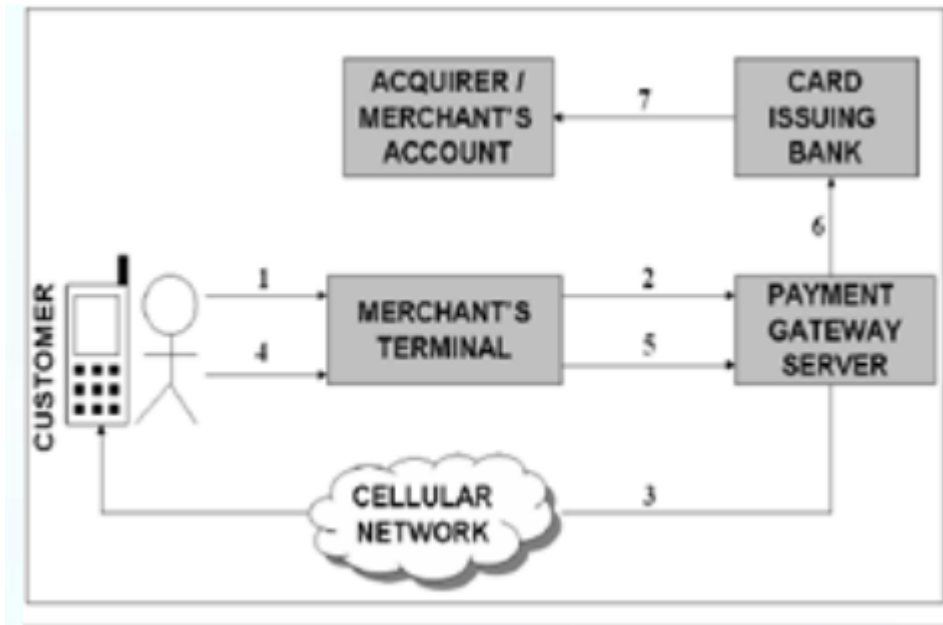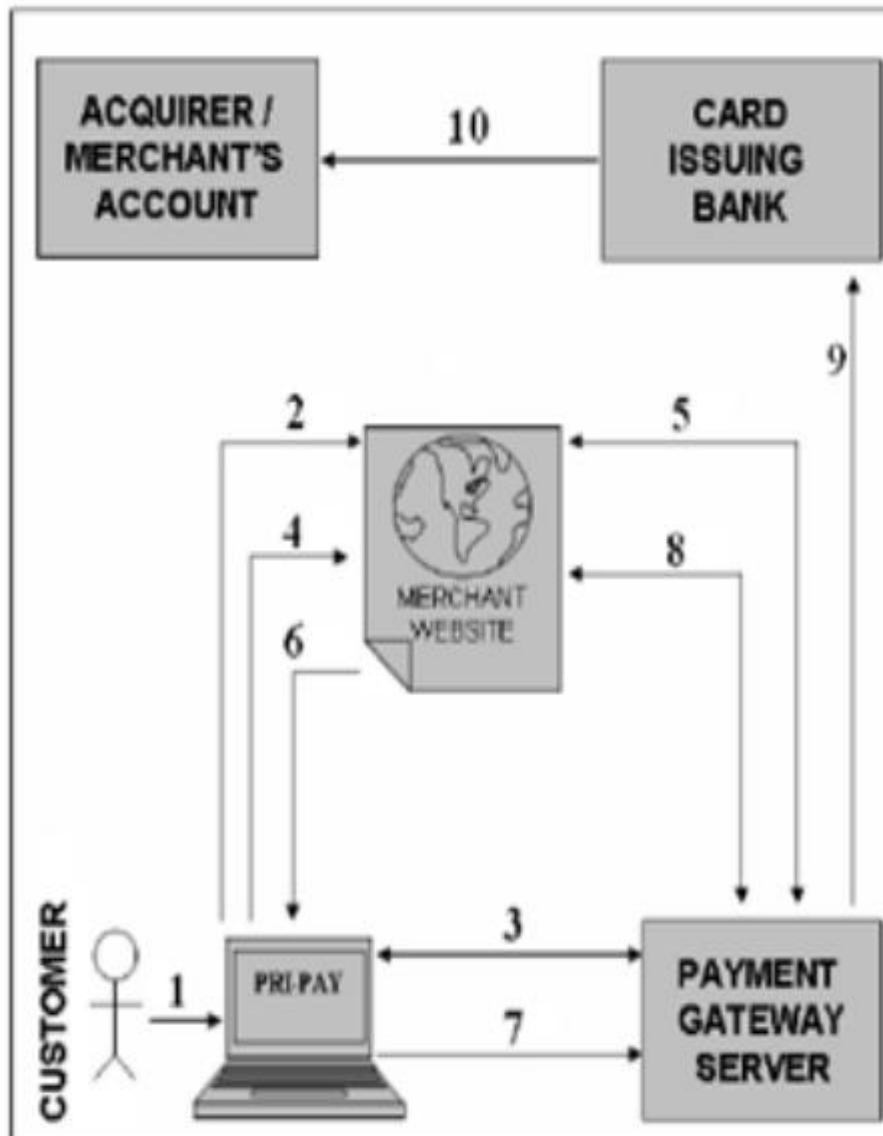
Figure5: Onsite transaction Procedure

Following steps customer should be Aware:

1. Customer/cardholder gives his smartcard at themerchant's terminal. Merchant accountant feeds payment details and then brings the smartcard nearthe smartcard reader.

2. Credit card details are encrypted using public keyof the payment gateway and sent to GS throughthe merchant's terminal.

3. GS after authorizing the credit card details of thecardholder sends a one-time password to the mobile device of the cardholder through thecellular network.

4. Cardholder enters the one time password obtainedon his mobile device on to the merchant'sterminal.

5. Now the complete transaction information is sent from the merchant's terminal to GS.

6. GS after finally authorizing the cardholder passesthe payment details to the issuing bank.

7. After verifying the payment information issuingbank transfers the respective funds to the merchant's account or the acquirer.

B. Online Transaction Procedure

We explain working of software Pri-pay. Pripaymainlyconsists of two parts a Pri-pay browser and an Authentication module. Pri-pay can be accessed only by the legitimate userhaving the PIN or a user defined password. Online transaction steps are as follows as:

Figure6: Online transaction Procedure

1. Customer starts Pri-pay on his terminal. He is then asked to enter a secret password or a PIN to access the system.
2. After successful entry of the password/PIN, customeropens the Pri-pay browser where he visits the
merchant's website and places the order
3. The OTP system in the Authentication module of Pripay synchronizes itself with the payment gateway
server (GS).
4. An initial request draft, Req Draft is createdautomatically by Pri-pay and encrypted using the
public key of the payment gateway
5. Merchant sends the received Req Draft to GS. GS after verifying the customer notifies the merchant about
authenticity of the customer.
6. Merchant then creates a transaction bill, TransBill
which is: TransBill = EnCrypt [(Merchant ID,Merchant's Acc. No. , Payment details), PRMER.
7. Customer verifies the order information and then Authentication module of Pri-pay sends T_ID obtained from the
merchant to GS for merchantauthentication.
8. GS sends T_ID to the corresponding merchant andmerchant in turn sends the TransBill to GS. GSdecrypts the
TransBill using merchant's public key and authorizes the merchant and notifies the customer
of merchant is authenticated.
9. GS then sends payment details and customer's details
(credit card number) to the issuing bank.
10. Issuing bank after verifying the payment transfers the requested funds to the merchant's account/acquirer

and both, customer and the merchant are notified of the transaction status.

C. PRI-PAY SECURITY FEATURES:

Working of the software, we have already described pripay and now, we elaborate the structure of Pripay along with its security features. The use case diagram of the prepay software is shown in figure. Use-Case Diagram of Pri-pay
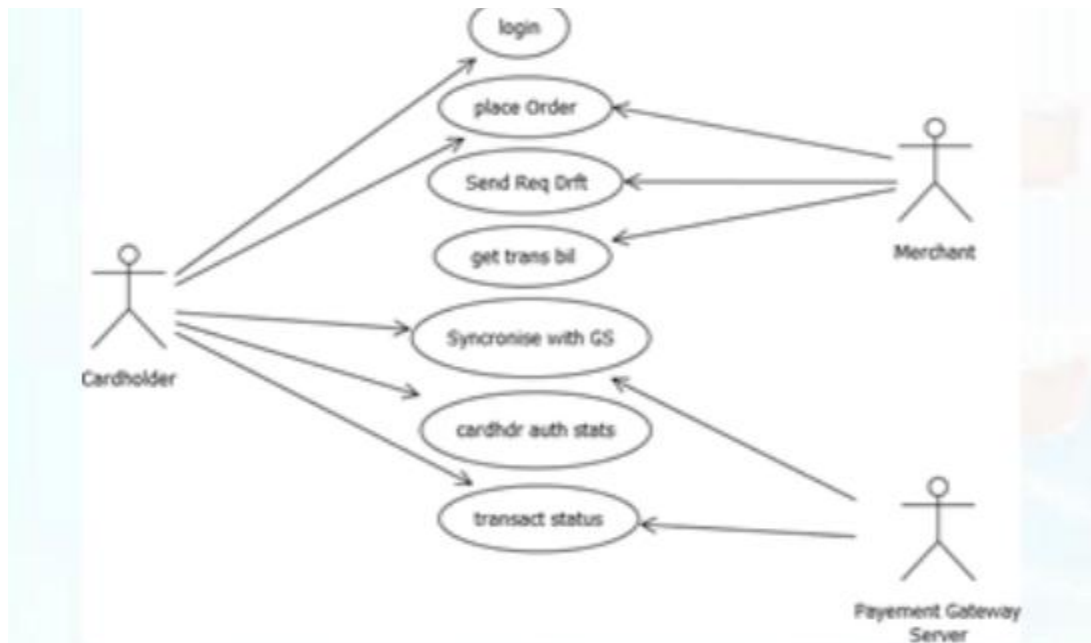
Figure7: Use case Diagram

D. *Biometric Authentication*

Another concept for the security of online electronic transaction security is use of Biometric. Biometrics operation is very common application for identification. Across the world many researchers have worked in the similar area. Biometrics

the system validates a person's identity by comparing the captured biometric data with data stored system database. In such a system, an individual who wants to be recognized claims an identity, usually via a PIN Personal Identification Number), a user name, a smart card, etc., and the system conducts a one to one comparison to determine whether the person is true or not. The aim is to prevent multiple people from using the same identity and thus achieving security of the system:

(1)**verification mode:**

In verification mode the system validates a person's identity by comparing individual data with PIN NO.

2) **Identification mode:**

In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to many comparison to search an individual's identity without the person having to claim an Identity.
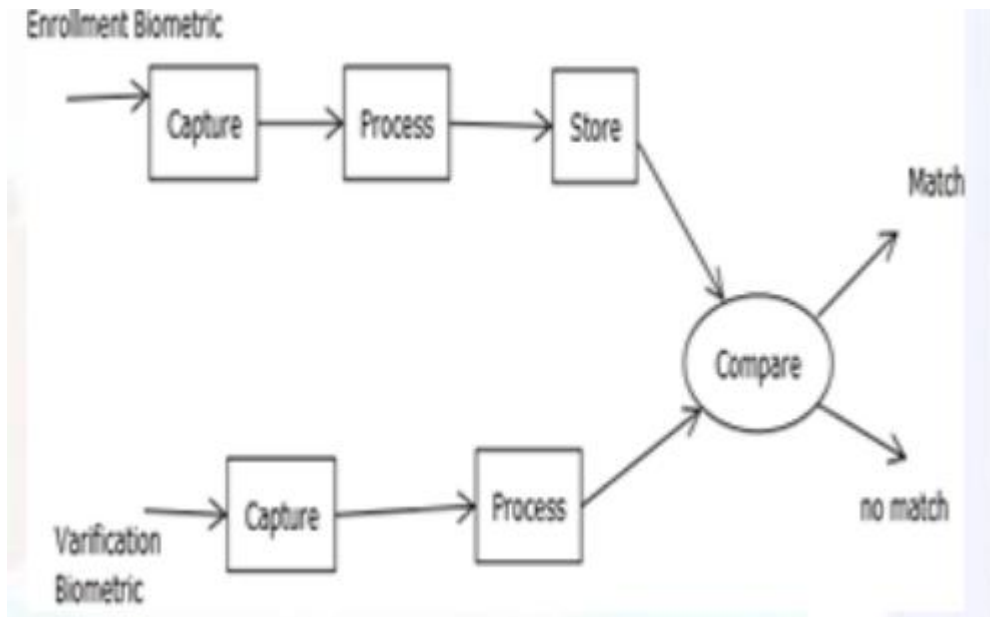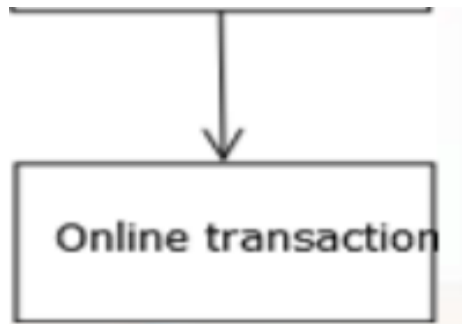
Figure8: Biometric Enrollment and Verification Process

IV. **SECURED FINGERPRINT PAYMENT SYSTEM**

The solution involves the use a biometric authenticationmechanism. A payment application would be installed onto android device, for authentication finger print is taken at run time.
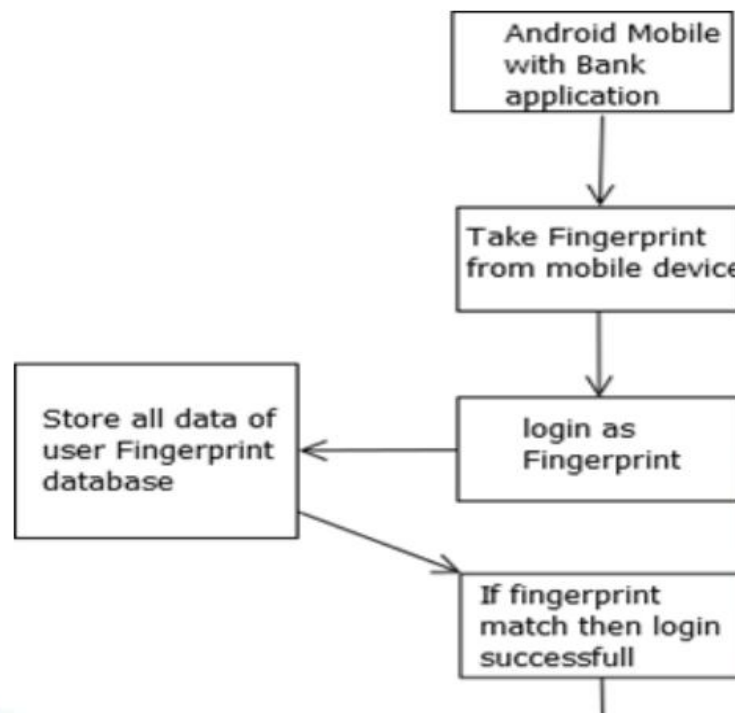
Figure9: Biometric Authentication

The finger print template would be captured by the phoneand compared against a stored template on a database server.The fingerprint template is encrypted by using the RSA algorithms or any other encryption algorithm and sends it to the Bank. Fingerprint is used for the login purpose for the bankapplication on mobile. Mobile will act as a client in this systemand the bank website will act as a server in this system. Oncefingerprint is taken as a login by mobile device, it sent to theserver for matching as request, and server send the replymessage.

If it is matching then only login will be successfuland user can do the transaction otherwise user will not be given access to online electronic transaction and this security of system will be achieved.

V. CONCLUSION:& FUTURE WORK

(1)Privacy and Security are the two major factors that affectNcostumers trust in electronic transaction. Therefore companies or websites or organizations that offer and sell their products orservices online should put more efforts in positively influencing their costumers perceptions of privacy and security.Computer system security is a worldwide problem that is affecting private as well as corporate users of IT.
(2)Informationtechnology users should be informed and should takeresponsibility for the security of resources that they are usingand building.
(3)Accordingly, they should play an active role inprotecting their privacy. All other security systems aregenerally based on cardholder authentication but ignore themerchant verification which makes the transaction systemvulnerable to merchant attacks which should be taken care ofand Internet related frauds such as site cloning, merchantcollusion etc.
(4) In biometric run time fingerprint would be captured for mobile transaction and it should not stored already in the mobile device so it provides more security and not stolen by third party.
(5) Authentication request and reply should be in in the encrypted form. This gives the better level of security mechanism for mobile payment system..

REFERENCES:

[1] AsafShabtai,YuvalFledel, UriKanonov, Yuval Elovici, ShlomiDolev (2010), "Google Android: A Comprehensive Security
Assessment." IEEE security and Privacy.
[2] MachigarOngtang, Stephen McLaughlin, William EnckandPatrick M c D a n i e l (2009) "Semantically Rich ApplicationCentric Security in Android" Annual Computer SecurityApplications Conference.
[3] FadiAloul, Syed Zahidi, Wassim El-Hajj (2009) "Two Factor Authentication Using Mobile Phones"
[4] A. Levi, and C.K. Koc, CONSEPP: convenient and secure
electronic payment protocol based on X9.59, Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17thAnnual, 2001, pp. 286-295.
[5] C. Joris, P. Bart, and V. Joos, Combining World Wide Web andWireless Security, Proceedings of the IFIP TC11 WG11.4 FirstAnnual Working Conference on Network Security: Advances in Network and Distributed Systems Security, Kluwer, B.V., 2001.
[6] K.s. Vorapranee, and J.M. Chris, Using GSM to enhance ecommerce security, Proceedings of the 2nd international workshop on Mobile commerce, ACM Press, Atlanta, Georgia,
USA, 2002.
[7] Lee Heng Wei; Osman, M.A.; Zakaria, N.; and Tan Bo,"Adoption of Ecommerce Online Shopping in Malaysia," IEEE
7th International Conference on e--BusinessEngineering(ICEBE), pp. 140 – 143, Jan. 2011.

[8] Fengying Wang; Caihong Li; Zhenyou Wang; and Zhen Cheng,"Security Scheme Research of Digital Products Online

Transactions," IEEE International Conference on Automation

and Logistics (ICAL), pp. 1521 – 1525, Sept. 2008.

[9] Ion, M.; Koshutanski, H.; Hoyer, V.; and Telesca, L., "RatingAgencies Interoperation for Peer-to-Peer Online Transactions,"Second International Conference on Emerging SecurityInformation, Systems and Technologies (SECURWARE), IEEE,pp. 173 – 178, Sept. 2008.

[10] Hong-Jun Guan, "The Research of SET-Based ElectronicPayment System Model," International Conference on EBusiness and Information System Security (EBISS), IEEE, pp. 1– 4, June 2009.

[11] Jihui Chen; XiaoyaoXie; and Fengxuan Jing, "The Security ofShopping Online," International Conference on Electronic andMechanical Engineering and Information Technology (EMEIT),IEEE, pp. 4693 – 4696, Sept. 2011.

[12] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: Challenges and opportunities," IEEENetw., vol. 24, no. 4, pp. 13–18, Jul./Aug. 2010.

[13] D. Niyato, P. Wang, W. Saad, and A. Hjorungnes, "Controlledcoalitional games for cooperative mobile social networks,"IEEE Trans. on Vehi. Tech., vol. 60, no. 4, pp. 1812–1824, May2011.

[14] M. Ge, K.-Y. Lam, X. Wang, Z. Wan, and B. Jiang, "VisualSec:A secure message delivery scheme for online social networksbased on profile images," in Proc. IEEE GLOBECOM, 2009,

[15] S. Buchegger and A. Datta, "A case for P2P infrastructure for social networks—Opportunities and challenges," in Proc.

WONS, 2009, pp. 161–168.

[16] S. Buchegger, D. Schioberg, L. H. Vu, and A. Datta,"PeerSoN—P2P social networking: Early experiences and insights," in Proc. SocialNets,2009, pp. 46–52.

[17] L. Ching, V. Vijay, W. Yan, and P. Vineet, Trust enhanced security for mobile agents, E-Commerce Technology, 2005.

CEC 2005. Seventh IEEE International Conference on, 2005,pp. 231-238.

[18] R. Lars, and J. Sverker, Simulated social control for secureInternet commerce, Proceedings of the 1996 workshop on Newsecurity paradigms, ACM Press, Lake Arrowhead, California,United States, 1996.

[19] N. Kreyer, K. Pousttchi, and K. Turowski, StandardizedPayment Procedures as Key Enabling Factor for Mobile Commerce, University Library of Munich, Germany, 2002.

ABOUT AUTHOR:

Author:
Harshil.B.Jani
janiharshil091@gmail.com
M.tech[ELECTRONICS & COMMUNICATION Engineering.,]
INDUS UNIVERSITY
AHMEDABAD