International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 10, October - 2013

Security of Online Electronic Transactions

Nikhil Khandare Dr. B. B. Meshram

Department of Computer Engineering
VeermataJijabai Technological Institute, Mumbai400019

Abstract: Secure electronic transaction (SET) is a significant e-commerce protocol designed to improve the security of creditcard purchases. In this paper we discuss various security measures and protocols which are used till date and are still used for the security of online transaction in which electronic cash flows from buyer to the supplier or merchant. Various issues discussed in this paper are SET protocol, Authenticated and Key Agreementfor P2P-Based Networks, Mutual Authenticationbetween Cardholder and Merchant, Biometric Mechanism for enhanced Security ofOnline Transaction, Using a Mobile Device to Enhance Customer Trust in the Security of RemoteTransactions, Digital content mediatorfor secure P2P online transactions, Sensitive Data Transfer Security Model finally we will see the SMS-Based AuthenticationScheme

Index Terms: Digital content mediator, Authentication, P2P-Based Networks,Secure electronic transaction (SET), Sensitive Data, M-commerce

Introduction

Protocols in cryptography allow people to communicatesecurely across an open network, even in the presenceof other agents. Such protocols are hard to designand many of researchers have developed ways of finding errors or proving tht the protocol is correct. The verification of the registration protocols of Secure electronictransaction (SET), a large and important protocol for electronic commerce,proposedby Visa and MasterCard and is a industry standard. SET presents twomajor challenges to previous methods.

- It involves many levels of encryption, using many combinationsof symmetric cryptography,asymmetric cryptographyand hashing.
- It does not assume that each agent has his own privatekey so that the only problem which is remained is the distribution of thepublic keys, but allows cardholders to decide their asymmetric key.

The first challenge comes from SETs is how to usedigital envelopes.One part of a digital envelope is the main body of the message. The other part containsthat key and is encryptedwith the recipient's public encryptionkey. The two parts may have some common data, possiblyhashed, in order to confirm that they are tied together. This combinationof symmetric and asymmetric encryption can be consideredmore efficient than using asymmetric cryptography alone and it makes a protocol much harder to decide. The second challenging aspect of the SET protocols is thepossibility for cardholders and merchants to make public/privatekey pairs as they want for their electronic credentials.

SET REGISTRATION PROTOCOLS

Everyone normally pay for goods purchased over the Internet bygiving the merchant their

IJERT

credit card details. To prevent this information from unwanted peoplefrom stealing the card number, the message undergoesa session of the secure sockets layer (SSL) protocol. In this arrangementthe cardholder and merchant should trust eachother. That requirement is undesirable even in face-to-face transactions, but over the internet it has risks.

- The cardholder is protected from eavesdroppers but notfrom the merchant itself. Some merchants are dishonest. They do not protect the sensitive information.
- The merchant also needs to be protected and should have some protection against dishonest cardholderswho supply an invalid credit card number.

It seems contraryto popular beliefthat it is the merchant who has the most tolose from fraud. Law in many countries protects thecardholder. The aspect of registration of merchant as well as cardholder is dealt with here. First figure shows the registration of cardholder and the second one show registration of merchant.

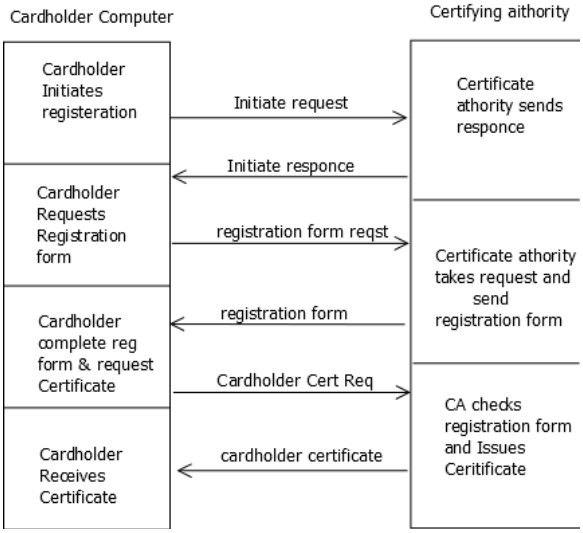

Figure1: Cardholder Registration

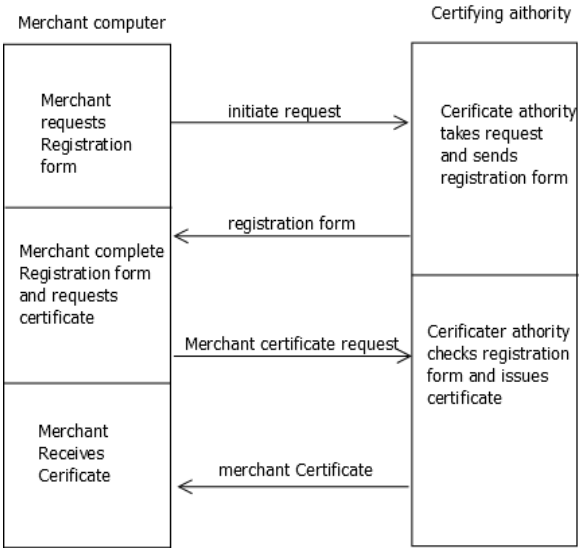

Figure2: Merchant Registration

SENSITIVE DATA TRANSFER SECURE.

In the study of barcodes work related to sensitive data transfer secure (SDTS)algorithms is proposed by many authors for security and applications of the same. Therevised model of SDTS is below provides thebenefits of the following.

- Firstly, this makes the system morecomplex because the changes made are at byte level and thus, it is very difficult to predict by thehackers that what exactly is happening.
- Secondly, this provides tightly coupled security becausethe complexity of the systemis increased to larger extent.

IJERT

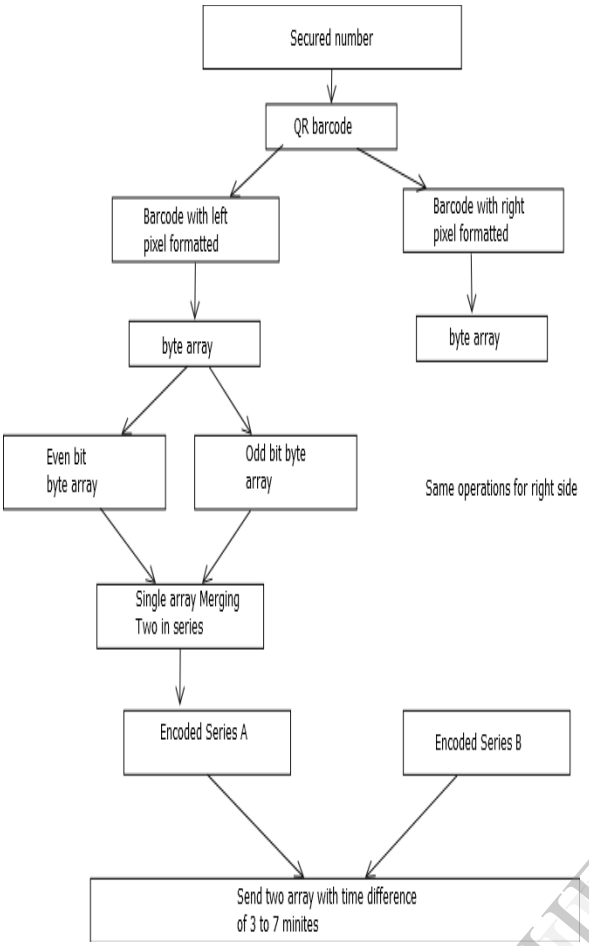

Figure3: Sensitive data transfer secure

SDTS modelisconverting the secure information into barcodes first, this information converting can be done bypixel manipulations and then convert the barcode image intobyte arrays 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 transactionprocessing apps, the information to be processedis not sent over the network in unsecured manner, but a security key corresponding to the information is picked from database table tosecure the real time data or information from being exposed on thenetwork or to the people who are not intended to view it.Then secure/secret key before exposing to the network isprocessed under various layers and converting into unreadable form. A quick response barcode is created for the keyand then it is splitted into two identical barcode like images which is also calledFalse Images. Each false image is converted to a byte array it may be even or odd.Each byte array isfurther splittedinto two;

- picking all the odds together
- picking allevens together.

Then these odds and evens are combined and the sequence is formed. We want to change the information completely in a predefinedmanner such that it gets tougher to identify the informationwithin the arrays. The transformed array is then encrypted using the RSAalgorithm. The two encrypted secure files are sent over thenetwork secured or unsecured network with some random time difference of 3 to 7 minutes.

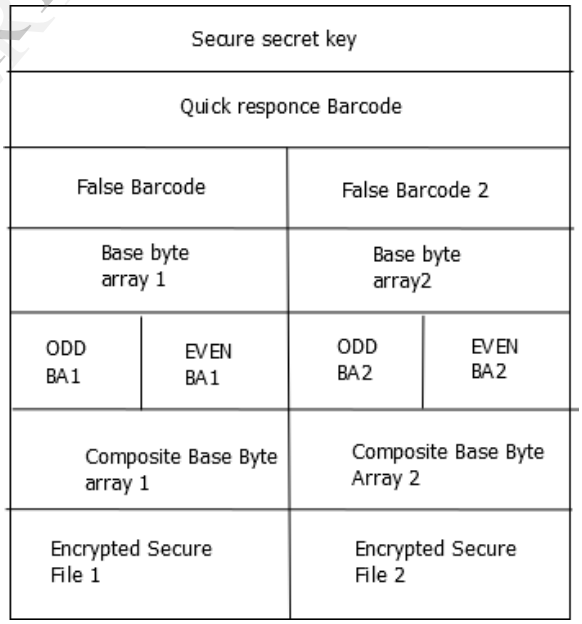

Figure4: Top view of SDTS

Onsite Transaction Procedure

This is the scenario where the cardholder is physicallypresent at the merchant's site or shop and gives his smartcard at themerchant's terminal after selecting the

IJERT

goods and services topurchase. Onsite transaction steps are as follows.

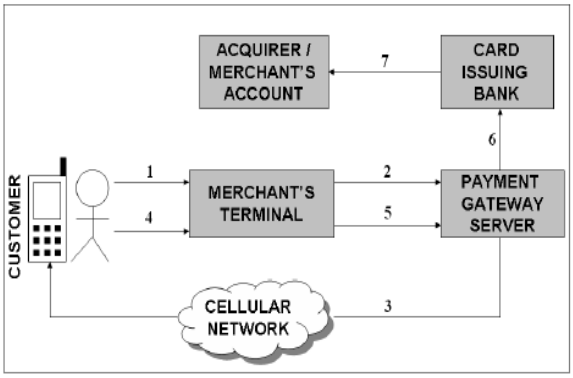

Figure5: Onsite transaction Procedure

1. Customer/cardholder gives his smartcard at themerchant's terminal. Merchant accountant feeds payment details and then brings the smartcardnear the smartcard reader.
2. Credit card details are encrypted using public key ofthe payment gateway and sent to GS through themerchant's terminal.
3. GS after authorizing the credit card details of thecardholder sends a one time password to the mobile deviceof the cardholder through the cellular network.
4. Cardholder enters the one time password obtained onhis mobile device on to the merchant's terminal.
5. Now the complete transaction information is sent fromthe merchant's terminal to GS.
6. GS after finally authorizing the cardholder passes thepayment details to the issuing bank.
7. After verifying the payment information issuing bank transfers therespective funds to the merchant's account or theacquirer.

Online Transaction Procedure

We explain working of software Pri-pay. Pripaymainly consists of two parts a Pri-pay browser and anAuthentication module. Pri-pay can be accessed only by thelegitimate user having the PIN or a user defined password.Online transaction steps are as follows

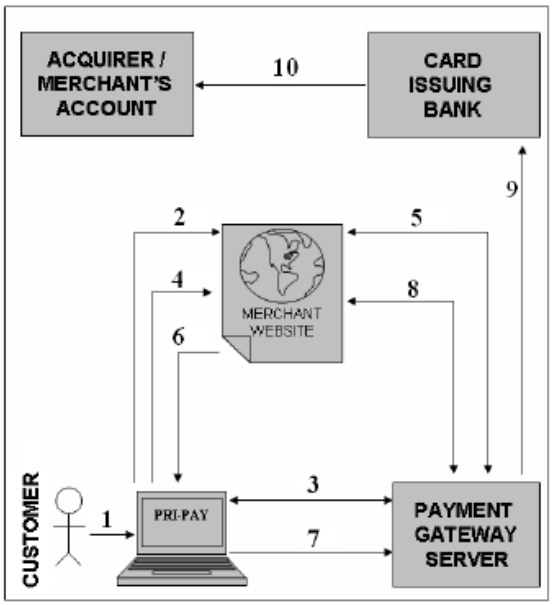

Figure6: Online transaction Procedure

1. Customer starts Pri-pay on his terminal. He is thenasked to enter a secret password or a PIN toaccess the system.
2. After successful entry of the password/PIN, customeropens the Pri-pay browser where he visits themerchant's website and places the order.
3. The OTP system in the Authentication module of Pripaysynchronizes itself with the payment gatewayserver (GS
4. An initial request draft, ReqDraft is createdautomatically by Pri-pay and encrypted using the publickey of the payment gateway.
5. Merchant sends the received ReqDraft to GS. GS afterverifying the customer notifies the merchant aboutauthenticity of the customer.
6. Merchant then creates a transaction bill, TransBillwhich is:

TransBill = EnCrypt[(Merchant ID ,Merchant's Acc. No. , Payment details) , PRMER.

7. Customer verifies the order information and thenAuthentication module of Pri-pay sends T_ID obtainedfrom the merchant to GS for merchant authentication.

IJERT

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 andauthorizes the merchant and notifies the customer ofmerchant 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 requestedfunds to the merchant's account/acquirer and both,customer and the merchant are notified of thetransaction status.

Pri-pay Security Features

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

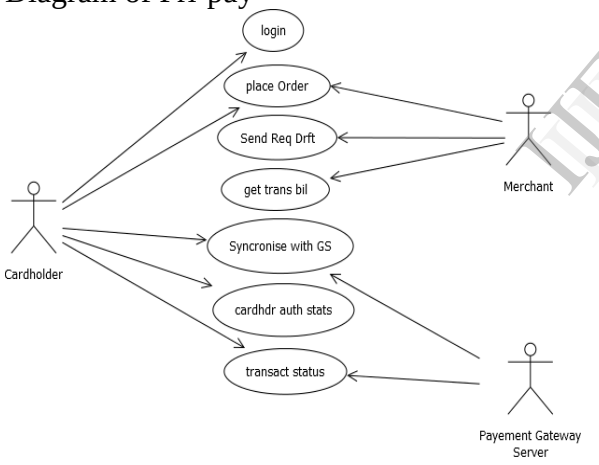

Figure7: Use case Diagram

A. Biometric Authentication

Another concept for the security of online electronic transaction security is use of Biometric. Biometrics operation is very common application foridentification. Across the world many researchers have worked in the similararea. Biometrics identify people by measuring

- Some aspectof individual characteristics such as your handgeometry or fingerprint, some deeply ingrained skill.
- Other behavioral characteristic such as your handwrittensignature.
- Something that is a of the two such as yourvoice.

Biometric authentication technologies such asface, finger, hand, iris, and speaker recognition areused largely today and are already in use.A biometric system is mainly a pattern recognition systemthat operates by taking biometric data from an person,extracting a feature from the data, and comparing extracted features with data stored in the database.Biometric system operates in two modes verification mode or identification mode.

1) Verification mode:

In the verification mode, the system validates a person'sidentity by comparing the captured biometric data with data stored system database. In such asystem, an individual who wants to be recognized claims anidentity, usually via a PIN Personal Identification Number), auser name, a smart card, etc., and the system conducts a one to one comparison to determine whether the person is true ornot. The aim is to prevent multiple people from using the same identity and thus achieving security of the system.

2) Identification mode:

In the identification mode, the system recognizes an individualby searching the templates of all the users in the database for amatch. Therefore, the system conducts a one-to-manycomparison to search an individual's identity without theperson having to claim an Identity.

IJERT

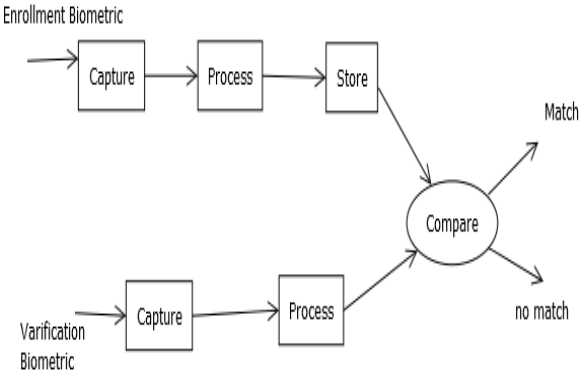

Figure8:Biometric Enrollment and Verification Process

SECURED FINGERPRINT PAYMENT SYSTEM

The solution involves the use a biometric authenticationmechanism. A payment application would be installed onto aandroid device, for authentication fingerprint is taken at runtime.

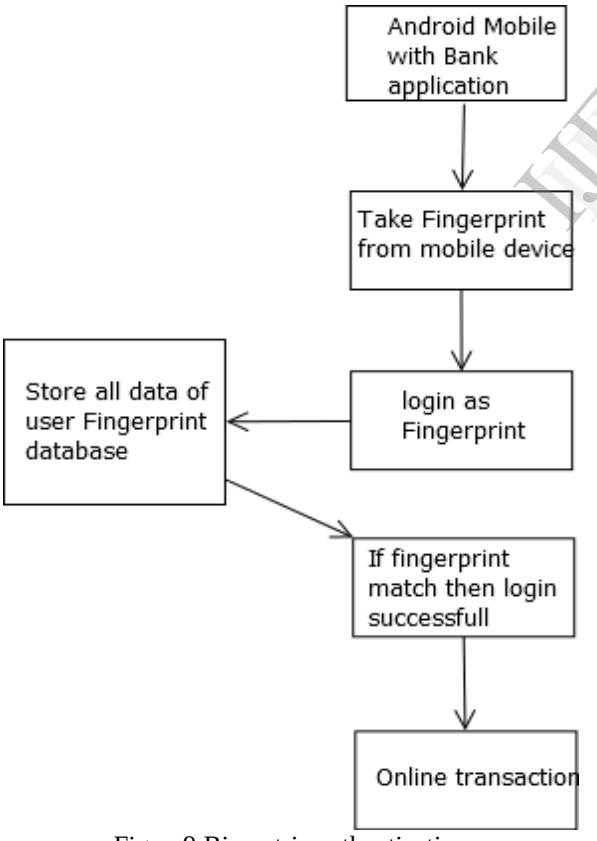

Figure9:Biometric authentication

The finger print template would be captured by thephone and compared against a stored template on a databaseserver.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 system and the bank website will act as aserver in this system. Once fingerprint is taken as a login by mobile device, itsent to the server for matching as request, and server send thereply message. If it is matching then only login will besuccessful and user can do the transaction otherwise user will not be given access to online electronic transaction and this security of system will be achieved.

Conclusion& Future Work

Privacy and Security arethe two major factors that affect costumers trust in electronictransaction. Therefore companies or websites or organizations that offer and sell theirproducts or services online should put more efforts in positively influencing their costumers perceptions of privacy and security. Computer system security is a worldwideproblem that is affecting private as well as corporateusers of IT. Information technologyusers should be informed and should take responsibilityfor the security of resources that they are using and building.Accordingly, they should play an active role in protectingtheir privacy.Allother security systems are generally based on cardholderauthentication but ignore the merchant verification whichmakes the transaction system vulnerable to merchant attacks which should be taken care of and Internet related frauds such as site cloning, merchantcollusion etc.In biometric run timefingerprint would be captured for mobile transaction and it should not stored already in themobile device so it provides more security and not stolen bythird party. Authentication request and reply should be in in theencrypted form.

IJERT

This gives the better level of securitymechanism for mobile payment system.

References:

[1] AsafShabtai,YuvalFledel, Uri Kanonov, Yuval Elovici, ShlomiDolev(2010), "Google Android: A Comprehensive Security Assessment." IEEEsecurity and Privacy.
[2] MachigarOngtang, Stephen McLaughlin, William Enck and Patrick Mc D a n i e l (2009) "Semantically Rich Application-Centric Security in Android" Annual Computer Security Applications Conference.
[3] FadiAloul, Syed Zahidi, Wassim El-Hajj (2009) "Two Factor Authentication Using Mobile Phones"
[4] A. Levi, and C.K. Koc, CONSEPP: convenient andsecure electronic payment protocol based on X9.59,Computer Security Applications Conference, 2001. ACSAC2001. Proceedings 17th Annual, 2001, pp. 286-295.
[5] C. Joris, P. Bart, and V. Joos, Combining World WideWeb and Wireless Security, Proceedings of the IFIP TC11WG11.4 First Annual Working Conference on NetworkSecurity: Advances in Network and Distributed SystemsSecurity, Kluwer, B.V., 2001.
[6] K.s. Vorapranee, and J.M. Chris, Using GSM to enhancee-commerce security, Proceedings of the 2nd internationalworkshop on Mobile commerce, ACM Press, Atlanta,Georgia, USA, 2002.
[7] Lee Heng Wei; Osman, M.A.; Zakaria, N.; and Tan Bo, "Adoption of EcommerceOnline Shopping in Malaysia," IEEE 7th InternationalConference on e--Business Engineering(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., "Rating AgenciesInteroperation for Peer-to-Peer Online Transactions," SecondInternational Conference on Emerging Security Information, Systemsand Technologies (SECURWARE), IEEE, pp. 173 – 178, Sept. 2008.
[10] Hong-Jun Guan, "The Research of SET-Based Electronic PaymentSystem Model," International Conference on E-Business andInformation System Security (EBISS), IEEE, pp. 1 – 4, June 2009.
[11] Jihui Chen; XiaoyaoXie; and Fengxuan Jing, "The Security of ShoppingOnline," International Conference on Electronic and MechanicalEngineering and Information Technology (EMEIT), IEEE, pp. 4693 – 4696, Sept. 2011.
[12] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for onlinesocial networks: Challenges and opportunities," IEEE Netw., vol. 24,no. 4, pp. 13–18, Jul./Aug. 2010.
[13] D. Niyato, P. Wang, W. Saad, and A. Hjorungnes, "Controlled coalitionalgames for cooperative mobile social networks," IEEE Trans. on Vehi.Tech., vol. 60, no. 4, pp. 1812–1824, May 2011.
[14] M. Ge, K.-Y. Lam, X. Wang, Z. Wan, and B. Jiang, "VisualSec: A securemessage delivery scheme for online social networks based on profileimages," in Proc. IEEE GLOBECOM, 2009, pp. 1–6.
[15] S. Buchegger and A. Datta, "A case for P2P infrastructure for socialnetworks—Opportunitiesand challenges," in Proc. WONS, 2009,pp. 161–168.
[16] S. Buchegger, D. Schioberg, L. H. Vu, and A. Datta, "PeerSoN—P2Psocial networking: Early experiences and insights," inProc. SocialNets,2009, pp. 46–52.
[17] L. Ching, V. Vijay, W. Yan, and P. Vineet, Trustenhanced security for mobile agents, E-CommerceTechnology, 2005. CEC 2005. Seventh IEEE International Conference on, 2005, pp. 231-238.
[18] R. Lars, and J. Sverker, Simulated social control forsecure Internet commerce, Proceedings of the 1996 workshopon New security paradigms, ACM Press, Lake Arrowhead,California, United States, 1996.
[13] N. Kreyer, K. Pousttchi, and K. Turowski, StandardizedPayment Procedures as Key Enabling Factor for MobileCommerce, University Library of Munich, Germany, 2002.

IJERT

About Authors:

Author1:
Nikhil Khandare
M.tech Computer Engineering
And
Teaching Assistant
VeermataJijabai Technological Institute
Matunga Mumbai 400019

Author2:
B. B. Meshram
Professor & Head
Department of Computer Engineering
and Information Technology
VeermataJijabai Technological Institute
Matunga Mumbai 400019

IJERT