International Innovative Research Journal of Engineering and Technology

ISSN NO:2456-1983

International Conference on Emerging Innovation in Engineering and Technology

ICEIET-2017

Implement The Banking Security Based Key Exchage Protocal And Keystroke Authentication

R.KULOTHUNGAN[1],M.MANIKANDAN[2],K.MURUGANANTHAN[3],P.PRAVEEN[4],

[1,2,3,4]UG Scholar ,B.E. Computer Science and Engineering.

Mr.R.VIJAYABHRATHI[5]

[2]Assistant Professor, Dept. of CSE.

MRK Institute of Technology, Kattumannarkoli.

[5]vijayccn@gmail.com, [1]kulothcharan007@gmail.com,[2]mani95msk@gmail.com,
[3]murugak07@gmail.com,[4]praveen1.cse@gmail.com

ABSTRACT:

An anonymous two factor AKE scheme improve the security of banking services. The Elliptic Curve Cryptography [ECC] based session key allocated the user device for the banking process. User login phase change the keystroke value and the second verification key dynamically on the server. This allows a user and a server to authenticate each other and generate session key for the subsequent communications.

Keyword: AKE Protocol, ECC Algorithm, Keystroke, Multiple Server.

I. Introduction:

Due to the increasing vulnerabilities in cyberspace, security alone is not enough to prevent a breach in banking services, but it also required some potential techniques to improves the security, AKE protocols offers two factor user authentication and mutual authentication .It avoids the vulnerability against lost-smart card attack, de-synchronization attack, password guessing attack in banking process. In this system ensures the users are identified or authenticated based on the way they type on keyboard, when a password is typed, These system contains two types of authentication values, which one is given by bank and other one is generated by the server2 that is stored in smart card . These two values are identify the valid user and smart card value from banking servers. In the user verification phase analyzes the username ,password and keystroke value in server1 .The second phase verifies the smartcard value with the message received by mobile. In this case second value is in dynamic nature it will be changed at every transaction.

II. LITERATURE REVIEW:

Under this topic we are using different kind of paper for improving our project result. The newly added traits on here is, to implement the more than one authentication checks by using AKE protocols and Keystrokes[6][7]. And the ECC algorithm generates the session key for the transaction at the time of inserting a card into a teller machine. In this system using smartcard to stores the value which is generated by server2[23][26][28].These values are dynamically changed in every transaction[3][4].

III. EXISTING SYSTEM:

In an Existing System, a Single server used for the user verification process. Which means the user data are stored in a single banking server .And the symmetric cryptography used for make a secure transaction in this wireless transmission. In this older system are based on the user id verification .But this is not more secure for these type of secure process. Then the unauthorized person each account details easily access the secret pin, From the teller machines.

In this wireless transaction intruders each easily attack the system. 3.1 Disadvantage:

- User details are stored on the single server.
- Transaction is very less.
- Occur the offline attack.

IV. PROPOSED SYSTEM:

In this proposed system user a multiple server to provide strong authentication process. In server1 it stored the pin1, users data and keystroke values. In server2 generates the pin2 and stored it in a smartcard. Which one is inserted into a teller machine and send that same key to uses by message, which is in dynamic nature[13][16][17]. So it provides a two-factor authentication support to avoid vulnerability again guessing. The ECC is used for encryption and decryption process with signature verification. Then the AKE protocol is used to exchange the keys which is generated by server2 and it is also verifies the keystroke of the keyboard when the user type the pin[6].

4.1Advantage:

- Secured the communication process.
- Reduce the problem offline attack.
- Over the problem of user authentication.

V. MODULE DESCRIPTION:

The proposed protocol can allows four modules in this system and description and below.

- Enrollment
- Anonymous User Authentication
- Session Key Agreement
- Online Banking.

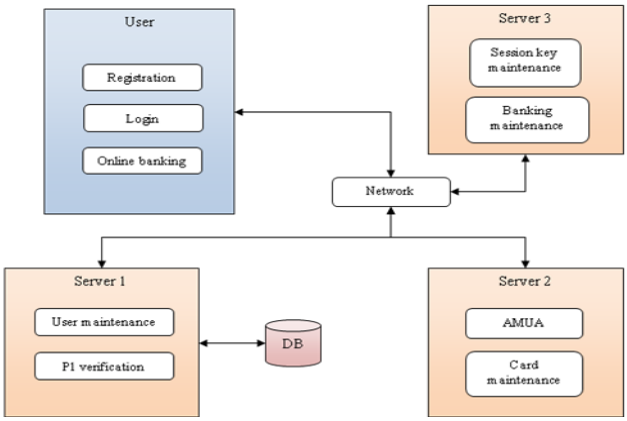

Fig:1

5.1 Enrollment:

This module is for user related operation the important functionalities of this module is described as below. The basic user details are registration by this module the some user details are name, address, first factor, contact no, keystroke value. The next joel for this module is to stroke user details on database and key value on the server database, by both first and second server database respectively.

5.2 Anonymous User Authentication:

In this module, the server method process are held down for example, user verification, user name and password analysis, and also verification of keystroke value. The second import ion process by this module is to verify the second password, which is already built on that smartcard. This second server can also overwrite the value user's smartcard in enemy if these all verification are gives the true result, then the process is execution, correctly.

5.3 Session Key Agreement:

Session key agreement for to establish a new session key for user's after finishing the verification process ,this session key creation is done. This methodology is based on the ECC algorithm or asymmetric algorithm technology to finish this entire process, Then the communication is start between the login user and bank server.

5.4 Online Banking:

This module can handled more precious processor on this entire systems (i.e) the online money transfer can be done by this module . The list of process by this module are, deposit, transaction and other banking process. Here the request and retrieved data can be encryption and decryption relatively it means, the user request can be encrypted to send server and that request is decrypted by server and reterited the needed request for appropriate user query.

VI. CONCLUSION:

In an Existing System the security is a major issue because it uses single server authentication, So the unauthorized person can easily access the security pin and user data from teller machines. But in this proposed system to prevent data from intruders . This is useful for ensure the authentication and presences the privacy details of user in more effective. Here we are using two type of key or password to provides more security of these kind of money transaction.

REFERENCE:

[1] Ducan S.Wong, Guilin Wang, Xiao Tan, Kefei Chen, Liming Fang,"Provably Secure Dynamic ID-based Anonymoustwo –factor Authenticated key Exchange protocol with extended security model," IEEE Transaction on Information Forensics & security ., no.1, Jun.2017.

[2]A.Velanzano, L.Durante, and M.Cheminod, "Review of security issues in industrial network," IEEE Tran.Ind.Inf.,Vol.9,no.1,pp.277-293-2013.

[3]Amin, R., and Biswas, G.P., "DEsine and analysis of bilinear pairing basedutual authentication and key agreement protocol usable in multi-server environment".*wirel.* pers, commun 1-24,2015.

[4]Amin, R.,and Biswes, G.P.,"An improved rsa based authentication and session key agreement protocal usable in tmis". J.Med.Syst 39(8):79,2015.

[5]S.Bhatt and T.Santhanam, "Keystroke dynamics for biomartic authentication –a survey ", in Int.Conf .on PattenRecognition Infirmatics and mobile Engineering .2013 ,pp.17-23.

[6]K.S.killourhy," A science understanding of keystroke dynamics" Ph.D.disseration.Canegie Mellon University,

Jan 2012.

[7]V.C.Gungor,and G.P.Hancke."Industrial wireless sensor network:challenger,design principle and technical approaches",IEEE trans.,Ind.Electron.,vol.56,no.10,pp.4258-4265,Oct.2009.

[8]D.Liu,M.C.Lee,and D.Wu,"A Node-to-Node Location Verification Method ,"IEEE Tran. Ind. Electron., vol.1537,May2010.

[9]G.Wang, J.yu, and Q.Xie, "Security analysis of a sing sign-On mechanism for Distributed Computer Network," IEEE Tran.Ind.Inf.,vol.9,no.1,Jan 2013.

[10]L.Barolli and F.Xhafa,"JXTA-OVERLAY:A P2P platform for distributed,collaborative and ubiqiuitous computing," IEEE Trans.Ind.Electron.,n vol.58.,no6,pp.4784-4791,2012.

[11]Y.Huang, W.Lin, and H.Li "Efficient Implementation of RFID Mutual Authentication protocol", IEEE Tran .Ind.Electron.,vol.59,no.12,pp.4784-4791,2012.

[12]B.Wamg and M.Ma,"Aserver independent authentication scheme for RFID system," IEEE Tran.Ind. Inf ., vol8.no.3, pp.689-696, Agu 2012.

[13] M.Hwang, and L.Li ,"A new remote user authentication scheme using smartcards," IEEE Trans. Consum. Electron.,2000,46(1)28-30.

[14] C.Lee, M.Hwang, and I.Liao,"Security enhancement on a new authentication scheme wuth anonymity for wireless environment ," IEEE Trans. Ind. Electron., vol.53, pp.1683-1687. Oct 2006.

[15] J.J.Shen,C.W.Lin, "Amoditify remote user autnetication scheme using smartcard," IEEE Tran, Consum. Electron., 2003,49(2):414-416.

[16] G.Yang ,D.S.Wang and X.Deng,"Two-Factor mutual authentication based on smartcards and password,"Jounal of computer and syatem ,science 74(7):1160-1172,2008.

[17] C,Ma,D.Wang ,and S.Zhoa ,"Security flaws in two improved remotr user authentication schemes using smartcard,"Int.J.Commun.Syst., DOI:10.1002/dac.2468,2012.

[18] D.He, J.Chen, and J.Hu,"Improvement on a smartcard based password authencation scheme," Journal of Internet Technology, vol.13,no.3,pp.405-410,2012.

[19] Q.Xie,"Improvement of a security enhanced one-time factor authentication and key agreement scheme," Science Iranica,vol.19,pp.1856-1860,2102.

[20] M.Witteman,"Advances in smartcard security ",Information Security Bulletin,"7(2002):11-22,2002.

[21] P.Kocher, J.Jaffe, and B.Jun, "Differential power analysis ," Advance in Cryptology(Cryto'99),pp.388-397,1999.

[22] T.S.Messerges,E.A.Dabbish,and R.H.Sloan," Examining smart card security under the threat of power analysis attacks,"IEEE Tran on Computers , vol.51,no.5,pp.541-552,Jun 2002.

[23] X.X.Li , W.D.Qiu, D.Zheng,K.F.chen,J.H.Li, "Anonymity enhancement on robust and efficient password-authentication key agreement schemes using smart cards," IEEE Trans. Ind., vol.57,no.2,pp.793-800,Feb 2010.

[24] H.Chen, Y.Xion,X.Hong F.Hu and J.Xie,"A survery of anonymity in wireless communication system ," Security Comm.Ntework.2009(2):427-444.

[25]M.L.Das,A.Saxena,and v.p.gulati," A dymanic ID-Based remote user authentication scheme using smartcard: A review ,"Journal of Network and computer Application,35(2012)1235-1248,2012.

[26] D.He ,and H.Hu,"Cryptanalysis of a dynamic ID – based remote user authentication scheme with access control for multiple server environment," IEICE Trans., Inf Sys., Vol.E96-D, no.1,pp.1-3,2013.

[27] Y.Y.Wang, J.Y.Liu,F.X.Xiao, and J.Dan,"Amore efficient and secure dynamic ID-based remote user authencatiation scheme Computer communication ," Security Comm.Networks, vol.6, no.5,pp.585-585-2009.

[28]S.Chaudhry,H.Naqvi,K.Mahmood,H.F.Ahmad and M.K.Khan,"Improved remote user authebtication scheme using Eilliptic Curve Crptogarphy," Wireless Pres.Commun.,DOI 10.1007/s11277-016-3745-3,2016.

[29] S.CHaudhry ,"A secure biometric based multimedia network,"multimed tolls apple., 75.:12705-12725,2016.