MF-Secure: Multifactor Security Framework for Distributed Mobile Systems

S. Rithika Saranya and S. Ravimaran

Abstract—**With the advent of mobile technology and its novel applications, mobile based online payment method has become popular in the online business environment, increasing the market potential of the business. This has also led to do purchase by customers from anywhere, any time. The volume of mobile transactions has also demanded for a better security model in the system. The traditional internet based services gives authentication based security in text oriented format. Due to theft of mobile Devices or user identity, the third party person may access the resources. To ensure the security and protection from unauthorized user within distributed mobile system, we have proposed a new approach called mf-secure through single sign-on which provides user authentication by multi factors such as password, digital signature, RFID and biometrics which yields better authenticated service to the mobile clients. This approach is evaluated through simulation which shows enhanced security in distributed mobile system.**

Index Terms—Authentication, biometrics, digital signature, transaction.

I. Introduction

In business environment the mobile based online payment method increases their market tree to worldwide. The traditional internet based services gives authentication based security in text oriented format. Due to theft of mobile devices or user identity, the third party person may access the resources. The fundamental requirement of any online mobile banking applications is a security to protect user confidential data. Financial institutions providing online services and offering internet based products should be secure and efficient methods of authentication to protect data of their customers. Accessing today's web-based services always requires a username and password to authenticate the user identity. This is a significant vulnerability since the password can be captured by man in the middle attack and later used for making illegal access to the user account. The user authentication method used by current online payment systems is not adequate and secure. Thus it is possible for an unscrupulous user to use credit card number or account details stolen from valid user. Financial agencies considered single-factor authentication is not sufficient for user authentication and insecure for high-risk financial transactions which involve access to customer information or the online fund transfer to other parties using web browsers or cell phones. The single factor authentication does not support all the security requirements, major drawbacks of single factor authentication are System relies on password authentication only, Easily deducible with public domain cracking software utilities, Weakness of the system: Password is encrypted and Needs to traverse insecure medium (Interception and decryption),This makes it vulnerable to passive attacks, Rigid and strict password requirements, so difficult to remember passwords and this leads to storing of an e-copy of the password on the computer at easily accessible locations. In order to support our claim single factor authentication is vulnerable to various attacks. We would like to highlight the key points of the published guidelines of FFIEC (Federal Financial Institutions Examination Council).The FFIEC Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. In previous section the proposed framework clients' biometric characteristics are kept secret from servers. This not only protects user privacy but also prevent a single-point failure from undermining the authentication levels of other services. They introduced a various points related to need of stronger authentication for Internet banking services So, we need Multifactor Authentication technique to ensure the security and protection from unauthorized user within distributed mobile system, In proposed system we introduce a new approach called mf-secure through single sign-on which provides user authentication by multifactor such as password, digital signature, RFID and biometrics which yields better authentication service to the mobile clients. This approach is evaluated through simulation which shows enhanced security in distributed mobile system.

The Multifactor Authentication is a technique for users to authenticate themselves using two or more authentication, generally this method has been implemented for large devices which are more capable in terms of power and processing capabilities, some commonly available systems uses combination of something the user possesses such as a security token (e.g., security smart card), and something the user knows (e.g., password). Another very popular multifactor authentication technique is biometrics. Our approach suggests that Multifactor Authentication technique can be a secure authentication in a distributed mobile system. The following sections of this paper is organized as : Section 2 Background and Related work, section 3 propose MF-Secure Framework, section 4 provides performance evaluations and finally the section 5 gives conclusion.

Manuscript received June 20, 2012, revised July 17, 2012.

The authors are with computer science and Engineering, M.A.M College of Engineering, Tiruchirappalli, Tamilnadu, India (email: s.rithi89@mamce.org, ssg_ravimaran@mamce.org)

DOI: 10.7763/IJFCC.2012.V2.121

II. Background And Related Work

Numerous endorsement protocols have been proposed to participate biometric authentication with password authentication and/or smart-card authentication. Biometric authentication adds a new paradigm in user authentication which, unlike conventional approaches, is not based on what an individual knows or possesses, but on some characteristics of the individual itself. J.K. Lee, S.R. Ryu, and K.Y. Yoo, Designed an authentication system which does not need a password table to authenticate registered users. Instead, smart card and fingerprint are required in the authentication [1]. However, due to the analysis given in [2] Lee et al.'s scheme is insecure under conspiring attack. Lin and Lai [3] showed that Lee et al.'s scheme is vulnerable to masquerade attack. Namely, a legitimate user (i.e., a user who has registered on the system) is able to make a successful login on behalf of other users. An improved authentication protocol was given by Lin and Lai to fix that flaw. The new protocol, however, has several other security vulnerabilities.

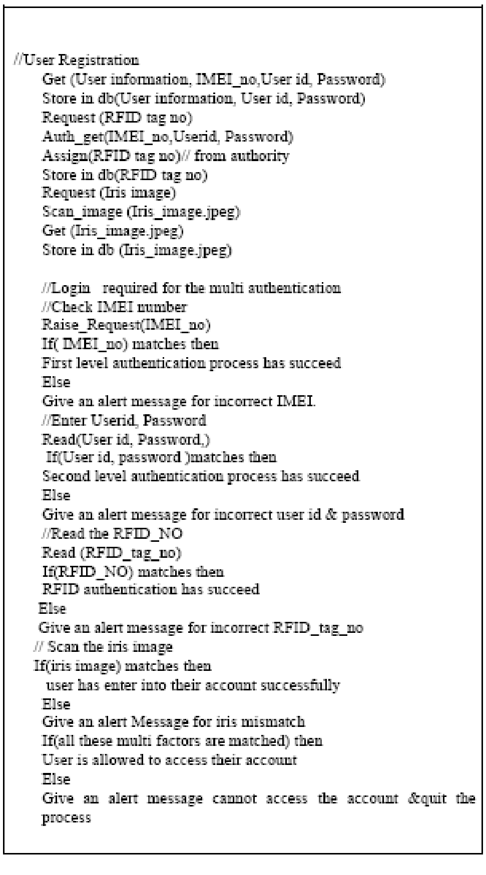
First, Lin-Lai's scheme only provides client authentication rather than mutual authentication, which makes it susceptible to the server spoofing attack [4].

Second, the password changing phase in Lin-Lai's scheme is not secure as the smart card cannot check the correctness of old passwords [5].

Third, Lin-Lai's scheme is insecure under impersonation attacks due to the analysis given by Yoon and Yoo [8], who also proposed a new scheme. However, the new scheme is broken and improved by Lee and Kwon [7]. In [6], Kim et al. proposed two ID-based password authentication schemes where users are authenticated by smart cards, passwords, and fingerprints. However, Scott [9] showed that a passive eavesdropper (without access to any smart card, password or fingerprint) can successfully login to the server on behalf of any claiming identity after passively eavesdropping only one legitimate login. Bhargav-Spantzel et al. proposed a privacy preserving multifactor authentication protocol with biometrics [10]. The authentication server in their protocol does not have the biometric information of registered clients. However, the biometric authentication is implemented using zero knowledge proofs [11], which requires the server to maintain a database to store all users' commitments and uses costly modular exponentiations in the finite group. Password authentication schemes with smart cards have a long history in the remote user authentication environment. So far different types of password authentication schemes with smarts cards [12]-[13] have been proposed. This scheme [14] does not maintain the password table to check the validity of the login request. However, the biometric database could put client privacy at risk.

However, the biometric database could put client privacy at risk. In order to protect client privacy, Fan and Lin [15] proposed a three-factor authentication scheme with privacy protection on biometrics. The essential approach of their scheme is as follows: 1) During the registration, the client chooses a random string and encrypts it using his/her biometric tem-plate; 2) the mobile environment. It is more frequently required in areas such as provides security in the distributed mobile system. The Multifactor Authentication is a technique for users to authenticate themselves using two or more authentication, generally this method has been implemented for large devices which are more capable in terms of power and processing capabilities, some commonly available systems uses combination of something the user possesses such as a security token (e.g., security smart card), and something the user knows (e.g., password). Another very popular multifactor authentication technique is biometrics. Our framework does not rely on any trusted devices to verify the authentication factors, which also meets the imperfect feature of distributed mobile system where devices cannot be fully trusted. We have taken an example bank application for a mf-secure in that proving authentication for online money transaction in mobile that which process has been shown in the following sections. Rresult (called sketch) is stored in the smart card; and 3) During the authentication, the client must convince the server that he/she can decrypt the sketch, which needs correct biometrics (close to the biometric template in the registration. Very recently, Li and Hwang [16] .There are no satisfactory solutions for three factor authentication properties which have been studied intensively in smartcard based password authentication. To provide more secured authentication in a distributed mobile system we have introduce a new approach called mf-secure through single sign-on which provides user authentication by multi factors such as password, digital signature , RFID and biometrics which yields better authentication service to the mobile clients.

TABLE I: Pseudo Code for MF-Secure



```
//User Registration
    Get (User information, IMEI_no,User id, Password)
    Store in db(User information, User id, Password)
    Request (RFID tag no)
    Auth_get(IMEI_no,Userid, Password)
    Assign(RFID tag no)// from authority
    Store in db(RFID tag no)
    Request (Iris image)
    Scan_image (Iris_image.jpeg)
    Get (Iris_image.jpeg)
    Store in db (Iris_image.jpeg)

    //Login   required for the multi authentication
    //Check IMEI number
    Raise_Request(IMEI_no)
    If( IMEI_no) matches then
    First level authentication process has succeed
    Else
    Give an alert message for incorrect IMEI.
    //Enter Userid, Password
    Read(User id, Password,)
     If(User id, password )matches then
    Second level authentication process has succeed
    Else
    Give an alert message for incorrect user id & password
    //Read the RFID_NO
    Read (RFID_tag_no)
    If(RFID_NO) matches then
    RFID authentication has succeed
   Else
   Give an alert message for incorrect RFID_tag_no
  // Scan the iris image
  If(iris image) matches then
     user has enter into their account successfully
    Else
    Give an alert Message for iris mismatch
    If(all these multi factors are matched) then
    User is allowed to access their account
    Else
    Give an alert message cannot access the account &quit the
    process
```

III. Mf- Secure Approach

Password authentication is one of the simplest and the most convenient authentication mechanisms to deal with secret data over distributed mobile environment. It is more frequently required in areas such as computer networks, wireless networks, remote login systems, operation systems, and database management systems. To be critical, most of the existing schemes are vulnerable to various attacks and fail to serve all the purposes an ideal password authentication scheme should. A reliable and accurate identification or verification technique can be designed using biometric technologies. Biometric authentication employs unique combinations of measurable physical characteristics fingerprint, facial features, iris of the eye, voice print, hand geometry, vein patterns, and so on that cannot be readily imitated or forged by others. In this framework we introduce a new approach called **mf-secure** through single sign-on which provides user authentication by multifactor such as password, digital signature, RFID and biometrics which yields better authentication service to the mobile clients. This approach has mainly provides security in the distributed mobile system. The Multifactor Authentication is a technique for users to authenticate themselves using two or more authentication, generally this method has been implemented for large devices which are more capable in terms of power and processing capabilities, some commonly available systems uses combination of something the user possesses such as a security token (e.g., security smart card), and something the user knows (e.g., password). Another very popular multifactor authentication technique is biometrics. Our framework does not rely on any trusted devices to verify

The authentication factors, which also meets the imperfect feature of distributed mobile system where devices cannot be fully trusted. We have taken an example bank application for mf-secure in that proving authentication for online money transaction in mobile, process has been shown in the following sections.

A. Mf-Secure Architecture

Mf-secure architecture process has been done in single sign-on. The client has to enter some authentication process before proceeding to online money transaction. First the client has to register the password, iris image, user information, personal id. Then the information used to login (i.e.) username and password and they are used to scan their iris image and enter the RFID-No if these authentication are matches then the client used to access their account else they can't access their account. The process of mf-secure architecture has been explained in following section.

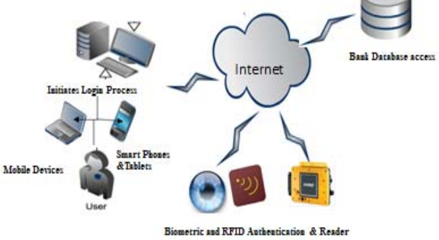


Fig. 1. MF-secure architecture

1) Chronic to Ac: Before we enter into the network, first the user must chronic (register) to the ac server. In this process, user scans their images and move to the various ridging operation. After biometric operation, the user registers their RF-ID no. After completion of operation, the user registers their particulars.
2) Ac Authentication: After chronic process completed, the user sign in to the Ac server. Ac server verifies the general authentication process by verifying user name and Password. Then, Biometric authentication process is work on. And, RF-ID authentication can be done through entering the id number.
3) User's Repository: The authenticated user can posit their data's and files to the server. AC queries a server with the data which the user wants and the server Implements the queries and server response to the ac according to the query.
4) AC's Query to server: AC queries a server with the data which the user wants and the server implements the queries and server response to the ac according to the query.
5) Respond *from server and Re – Encryption:* AC masks decryption keys and re encrypts the results from the server with the masked decryption keys.
6) *Providing Access to the User:* After getting the Encrypted data from the Ac Server, Users get their access to use the applications.

The multifactor authentication process pseudo code has shown in table 1.Initally the user has to register their personal information such as personal id, password, IMEI (Mobile id) and iris image. When the user wants to login, first user has to enter their user id & password. Then the system verifies it and if it success static user id and password then user has enter into next authentication process. In this user id, password alone not enough for authentication so we are going for next authentication process is RFID. In this user has to enter RFID that is the user has to enter the IMEI NO. It is mainly used to give sms alert to the user in case of fraud detection. RFID contains RFID tag and reader that which the user has to enter their information in database. The main purpose of RFID tag or transponder (derived from transmitter/responder) is to provide the information that identifies the person or object, and is carried or implanted. The information is usually in the form of an alphanumeric word. This information is authentication process by verifying user name and their Called an identifier, and that of each tag is unique. Tags vary in size, and their size mainly depends on the size of the antenna on the tag. Then RFID reader or transceiver (derived from transmitter/receiver). It supplies energy to the tag in the form of RF electromagnetic waves. It then receives the signal from the tag. It usually contains an interface that allows it to communicate with a data processing system. Then the system verifies it and if it get success then the system has precede next process for authentication. Next process the user has to enter the biometric information. Biometric authentication human physical and behavioral characteristics are used to verify the identity of the biometrics authentication which is used to scanning the iris image. Iris image is one of the most heavily used and actively studied biometric technologies. A person's iris is fully developed within 18 months after birth, and is protected by eyelashes, eyelids and the retina. Its shape hardly changes so that it has higher consistency compared to other biometric characteristics. Its higher uniqueness in shape than a face or fingerprints ensures that an authentication system using the iris is immensely reliable. Personal identification using iris is recognizing it. Firstly, the system performs the function of obtaining the iris image suitable to iris recognition. The second part is comprised of two stages: extracting the iris area from the image and creating image from an input device is the first stage of personal identification using the iris. The device is comprised of a camera to capture the image and lighting the image sensors to grab correct iris patterns. In particular, the device is closely related to the system's overall performance. Unlike face recognition, close-up photographing is since an eye is smaller than a face. In the case of close-up photographing, it is difficult to set a clear focus due to low depth of field. To obtain a clear image, the shutter speed of a camera and the degree of security is concerned. Again the system verifies the iris image if it is matches then the user can successfully login their account and access their account securely. These are the process that is involved in the multifactor authentications.

IV. Advantages

In single factor the system relies on password authentication only so it's easily deducible with public domain cracking software utilities. Hence single factor authentication does not require more security. In two factor authentication client has a valid smart card and correct password in which it provides a strong security guarantees than password authentication, it could also fail if both authentication factors are compromised then attacker has successfully obtained the password and the data in the smart card. In three factors authentication previous research is introduced to incorporate the authentication based on password, smart card and biometrics but it's confusing and far from satisfactory. Hence comparing with these authentications we introduce multifactor authentication approach in which the process has been done on single -sign on and provides more security in distributed mobile systems.

V. Conclusion

Preserving security and privacy is a challenging issue in distributed mobile systems. This paper makes a step forward in solving this issue by proposing mf-secure framework authentication to protect services and resources from unauthorized use. The authentication is based on password, biometrics, RFID and digital signature. The analysis shows that the framework satisfies all security requirements on multifactor authentication. In future we should analyze to implement this work in mobile which have the internal device of Irish recognizer for give efficient authentication (90%).

References

[1] J. K. Lee, S. R. Ryu, and K.Y. Yoo, "Fingerprint-Based Re-mote User Authentication Scheme Using Smart Cards," E*lec-tronics Letters*, vol. 38, no. 12, pp. 554-555, June 2002.

[2] C. C. Chang and I. C. Lin, "Remarks on Fingerprint-Based Remote User Authentication Scheme Using smart Cards," *ACM SIGOPS Operating Systems Rev*, vol. 38, no. 4, pp. 91-96, Oct. 2004.

[3] C. H. Lin and Y. Y. Lai, "A Flexible Biometrics Remote User Authentication Scheme," *Computer Standards Interfac-es*, vol. 27, no. 1, pp. 19-23, Nov. 2004.

[4] M. K. Khan and J. Zhang, "Improving the Security of 'A Flexible Biometrics Remote User Authentication Scheme," *Computer Standards Interfaces*, vol. 29, no. 1, pp. 82-85, Jan. 2007.

[5] C. J. Mitchell and Q. Tang, "Security of the Lin-Lai Smart Card Based User Authentication Scheme," *Technical Report RHULMA20051*, Jan. 2005.

[6] H. S. Kim, J. K. Lee, and K.Y. Yoo, "ID-Based Password Authentication Scheme Using Smart Cards and Finger-prints," *ACM SIGOPS Operating Systems Rev*, vol. 37, no. 4, pp. 32- 41, Oct. 2003.

[7] Y. Lee and T. Kwon, "An improved Fingerprint Based Remote User Authentication Scheme Using Smart Cards," in *Proc. Int'l Conf. Computational Science and Its Applications (ICCSA)*, 2006.

[8] E. J. Yoon and K.Y. Yoo, "A New Efficient Fingerprint Based Remote User Authentication Scheme for Multimedia Systems," in *Proc. Ninth Int'l Conf. Knowledge-Based Intelli-gent Information and Eng*, Systems (KES), 2005.

[9] M. Scott, "Cryptanalysis of an ID-Based Password Authentication Scheme Using Smart Cards and Fingerprints," *ACM SIGOPS Operating Systems Rev*, vol. 38, no. 2, pp. 73-75, Apr. 2004.

[10] A. B. Spantzel, A.C. Squicciarini, E. Bertino, S. Modi, M. Young, and S. J. Elliott, "Privacy Preserving Multi-Factor Authentication with Biometrics," *J. Computer Securi-ty*, vol. 15, no. 5, pp. 529-560, 2007.

[11] S. Goldwasser, S. Micali, and C. Rackoff, "The Know-ledge Complexity of Interactive Proof-Systems," *SIAM J. Computing*, vol. 18, no. 1, pp. 186-208, Feb. 1989.

[12] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electronic,* vol. 46, no. 1,pp. 28-30, 2000.

[13] C. C. Chang and S. J. Hwang, "Using smart cards to authenticate remote passwords," *Computers and Mathematics with applications,* vol. 26, no.7, pp. 19-27, 1993.

[14] J. J. Shen, C. W. Lin and M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electronic,* vol. 49, no. 2, pp. 414-416, May 2003.

[15] C. I. Fan and Y. H. Lin, "Provably Secure Remote Truly Three-Factor Authentication Scheme with Privacy ProtectiononBiometrics," *IEEE.*

[16] C.T. Li and M. S. Hwang, "An Efficient Biometrics-Based Remote User Authentication Scheme Using Smart Cards," *J. Network and Computer Applications*, vol. 33, no. 1, pp. 1-5, 2010.

S. Rithikasaranya has received her B.E in Computer Science and Engineering from Mookambigai college of Engineering, Anna University of Technology, Chennai, Tamil Nadu, and India in 2010. Currently she is pursuing M.E in computer science and Engineering, M.A.M College of Engineering, Tiruchirappalli, Tamilnadu, India. Her research interests in network security,

S. Ravimaran has received his B.E. in computer science and engineering from National Institute of Technology, Tiruchirapalli, India in 1997 and his M.E.computer science and engineering from Periyar Maniammai College of Technology, Vallam, Tanjore, Anna University, Chennai, Tamil Nadu, India in 2004.Since 2007 he has been a research scholar, pursuing a Ph.D.at Anna University, Tiruchirappalli, Tamilnadu, India. Since January 1992 to December 1999, He was worked as a SENIOR FACULTY CUM HEAD in Academic Courses Techno Services Pvt Limited, Tiruchirappalli, Tamilnadu, India. From December 1999 he was worked as a LECTURER, SENIOR LECTURER, ASSISSTANT PROFESSOR and currently he is working as a Professor and HEAD, Department of Computer Science and Engineering, M.A.M. College of Engineering, Tiruchirappalli, Tamil Nadu, India. He has published papers such as A Transaction Processing System for Sharing Mobile Databases in Wireless Environment in National Conference on Recent Trends in Information Technology at RVS College of Engineering and Technology in March 2010.Another paper titled Performance Analysis in Data Replication in Distributed Data base Environment was Published in National Conference on Networking and Database NCND organized by PABCET, on 17 -18 Mar 2005. His research interests are mobile computing. Professor S.Ravimaran was a member of IEEE and IEEE Computer Society,ISTE, CSI and Institution of Engineers