International Journal of Smart Sensor and Adhoc Network

Volume 1 | Issue 4 Article 3

April 2012

A Fuzzy Implementation of Biometrics With Five Factor Authentication System For Secured Banking

S. Hemamalini
Department of Computer Science and Engineering, Affiliated to Anna University, Alpha College of Engineering, Thirumazhisai, Chennai., hemamaliniiii@yahoo.co.in

M. L. Alphin Ezhil Manuel
Département of Computer Science and Engineering, Alpha College of Engineering, Thirumazhisai, Chennai, alphinezhilmanuel@gmail.com

`

A Fuzzy Implementation of Biometrics With Five Factor Authentication System For Secured Banking

S. Hemamalini & M. L. Alphin Ezhil Manuel
Department of Computer Science and Engineering, Alpha College of Engineering, Thirumazhisai, Chennai.
Email: hemamaliniiii@yahoo.co.in, alphinezhilmanuel@gmail.com

Abstract - Remote authentication is the most commonly used method to determine the identity of a remote client. Secure and efficient authentication scheme has been a very important issue with the development of networking technologies. In a Generic Framework for Authentication, preserving security and privacy in distributed systems provide three factors for authentication of clients. This paper investigates a systematic approach for authenticating clients by five factors, namely RFID card, PIN, biometrics, One Time Password (OTP) and keypad ID. The conversion not only significantly improves the information assurance at low cost but also protects client privacy in distributed systems.

Keywords – *Authentication; Distributed systems; Security; Privacy; PIN; RFID card; Biometrics.*

I. INTRODUCTION

In a distributed system, various resources are distributed in the form of network services provided and managed by servers. The five authentication factors used are

1. RFID card
2. PIN
3. Fingerprint
4. OTP
5. Keypad with Keypad ID

Most early authentication mechanisms are solely based on password. While such protocols are relatively easy to implement, passwords (human generated passwords in particular) have many vulnerabilities. As an example, human generated and memorable passwords are usually short strings of characters and (sometimes) poorly selected. By exploiting these vulnerabilities, simple dictionary attacks can crack passwords in a short time. Due to these concerns, hardware authentication tokens are introduced to strengthen the security in user authentication. RFID card-based password authentication provides two-factor authentication, which requires the client to have a valid smart card and a correct password. While it provides stronger security guarantees than password authentication, it could also fail if both authentication factors are compromised (e.g., if an attacker has successfully obtained the password and the data in the smart card). Another existing authentication mechanism is biometric authentication where users are identified by their measurable human characteristics, such as fingerprint can be easily obtained without the awareness of the owner. In this case OTP and Keypad ID further improve the system's assurance. This motivates the five-factor authentication, which incorporates the advantages of the authentication based on, RFID card, PIN, Fingerprint, OTP and Keypad ID.

1.1 Motivation

The motivation of this paper is to investigate a systematic approach for the design of secure five-factor authentication with the protection of user privacy. Five-factor authentication is introduced to incorporate the advantages of the authentication based on PIN, RFID card, fingerprint OTP and keypad ID. A well designed five-factor authentication protocol can greatly improve the information assurance in distributed systems. However, the previous research on three-factor authentication is confusing and not satisfactory.

1.2 Security Issues

The existing three-factor authentication protocols are flawed and cannot meet security requirements in their applications. Even worse, some improvements of those flawed protocols are not secure either. The research history of five-factor authentication can be summarized in the following diagram.

NEW PROTOCOLS→ BROKEN→ IMPROVED PROTOCOLS→ BROKEN AGAIN→ ENHANCED PROTOCOLS→ SECURE.

1.3 Privacy Issues

Along with the improved security features, five-factor authentication also raises another subtle issue on how to protect the biometric data. The authentication factors are not only the privacy information of the owner, but also closely related to security in the authentication process. As biometrics cannot be easily changed, the breached biometric information (either on the server side or the client side) will make the biometric authentication totally meaningless. However, this issue has received less attention than it deserves from protocol designers. We believe it is worthwhile, both in theory and in practice, to investigate a fuzzy implementation for five-factor authentication, which can preserve the security and the privacy in distributed systems.

1.4 Related Work

Several authentication protocols have been proposed to integrate biometric authentication with password authentication and/or smart-card authentication. An improved authentication protocol was given by Lin and Lai to fix that flaw. The new protocol, however, has several other security vulnerabilities. [1] Xinyi Huang, Yang Xiang, Jianying Zhou and Robert H. Deng proposed to authenticate clients by three factors namely password, smart card and Biometrics. Fan and Lin [2] 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 template; 2) The result (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). As we shall show shortly, our fuzzy implementation employs a different approach. The client in our framework uses his/her Finger impression, RFID card and the PIN for authentication purpose. The Main Server will generate One Time Password (OTP) and send it to the User's Mobile number when the finger impression does not match exactly with the existing finger impression in the database. The keypad id is provided to the user during Account Registration. This leads to a fuzzy implementation of biometrics with five-factor authentication system for secured banking from a generic framework for three factor authentication: preserving security and privacy in distributed system.

2. Preliminaries

This section reviews the definitions of RFID card-based authentication, five-factor authentication, fingerprint recognition and fuzzy logic.

2.1 RFID card-based authentication

Radio-frequency identification (**RFID**) is the use of a wireless non-contact radio system to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking. Some tags require no battery and are powered by the radio waves used to read them. Others use a local power source. The tag contains electronically stored information which can be read from up to several meters (yards) away. Unlike a bar code, the tag does not need to be within line of sight of the reader and may be embedded in the tracked object.

2.2 Five-Factor Authentication

Five-factor authentication is very similar to three factor based authentication, with the only difference that it requires OTP and keypad ID as an additional authentication factor.

2.3 Fingerprint Recognition

Fingerprint recognition technologies analyze global pattern schemata on the fingerprint, along with small unique marks known as minutiae, which are the ridge endings and bifurcations or branches in the fingerprint ridges.

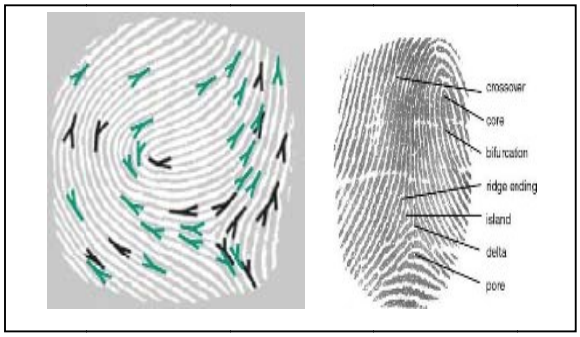

Fig.1.1 Fingerprint minutiae

The data extracted from fingerprints are extremely dense, where density explains why fingerprints are a very reliable means of identification. Fingerprint

recognition systems store only data describing the exact fingerprint minutiae whereas images of actual fingerprints are not retained. Fingerprint scanners may be built into computer keyboards or pointing devices (mice), or may be stand-alone scanning devices attached to a computer.

2.4 Fuzzy logic

Fuzzy logic is a form of many-valued logic, it deals with reasoning that is approximate rather than fixed and exact. In contrast with traditional logic theory, where binary sets have two-valued logic: true or false, fuzzy logic variables may have a truth value that ranges in degree between 0 and 1. Fuzzy logic has been extended to handle the concept of partial truth, where the truth value may range between completely true and completely false.

2.5 One Time Password (OTP)

The purpose of a one-time password (OTP) is to make it more difficult to gain unauthorized access to restricted resources, like a computer account. Traditionally static passwords can more easily be accessed by an unauthorized intruder given enough attempts and time. By constantly altering the password, as is done with a one-time password, this risk can be greatly reduced.

2.5.1 OTP over SMS

A common technology used for the delivery of OTPs is short message service (SMS). Because SMS is a ubiquitous communication channel, being available in all handsets and with a large customer-base, SMS messaging has the greatest potential to reach all consumers with a low total cost of ownership.

RSA Algorithm:

The RSA algorithm is the most commonly used encryption and authentication algorithm. The generation of OTP using RSA algorithm is as follows

Key generation: Select random prime numbers p and q, and check that p!= q

Compute modulus n = pq

Compute phi, Φ = (p - 1)(q - 1)

Select public exponent e, $1 < e < \Phi$

such that gcd (e, Φ) = 1

Compute private exponent d = e^{-1} mod Φ

Public key is {n, e}, private key is d

Encryption: c = m^e mod n

Decryption: m = c^d mod n

Digital signature: S= $H(m)^d$) mod n,

Verification: m' = s^e mod n,

If m' = H (m) signature is correct.

H is a publicly known hash function.

3. A Fuzzy Implementation of Biometrics with Five Factor Authentication System

3.1 Registration:

Every user has to register in the bank in order to become an authorized user. The registration procedure is as follows:

1. The customer must have to provide their basic information like username, address, contact information, email id, photo proofs and other required information.
2. We assume that there is a device for extracting the fingerprint template and carrying out all calculations in a fuzzy extractor. This step does not involve any interaction with the authentication server.

3.1.1 Customer Verification Techniques

Customer verification is a related but separate process from that of authentication. Customer verification complements the authentication process and should occur during account origination. Verification of personal information may be achieved in three ways:

•**Positive verification:** To ensure that material information provided by applicant matches information available from trusted third party sources. More specifically, a financial institution can verify a potential customer's identity by comparing the applicant's answers to a series of detailed questions against information in a trusted database (e.g., a reliable credit report) to see if the information supplied by the applicant matches information in the database. As the questions become more specific and detailed, correct answers provide the financial institution with an increased level of confidence that the applicant is who they say they are.

Logical verification: To ensure that information provided is logically consistent with the telephone area code, ZIP code and street address.

• **Negative verification:** To ensure that information provided has not previously been associated with fraudulent activity. For example, applicant information

can be compared against fraud databases to determine whether any of the information is associated with known incidents of fraudulent behavior. In the case of commercial customers, the sole reliance on online electronic database comparison techniques is not adequate since certain documents (e.g., bylaws) needed to establish an individual's right to act on a company's behalf is not available from databases. Institutions still must rely on traditional forms of personal identification and document validation combined with electronic verification tools.

3. The information provided are then stored in the database of the server after all verification. Once the information registered is true then the Server generates a RFID card which contains all the information related to the user. The client is given RFID card, PIN number and Keypad ID along with the keypad to perform the transaction.

As in the existing authentication protocols, we assume the registration phase is performed in a secure and reliable environment, and particularly the device is trusted for its purpose. After a successful registration, the client will have a RFID card, keypad with keypad ID and the initial PIN.

3.2 Login-Authentication

The client first inserts the RFID card into a card reader which will extract the data. After that, the client enters the PIN and his/her fingerprint data. A fingerprint scanner is used for extraction at this phase. The login procedure is as follows

1. The PIN that the user enter should match with already existing one in the database otherwise the user cannot proceed further.
2. Once the PIN matches perfectly the user has to give his/her fingerprint on the fingerprint scanner. Fuzzy logic is applied as soon as the fingerprint is obtained on the fingerprint scanner. If the fingerprint matches exactly (100%) with existing fingerprint in the database then the user will be allowed for transaction.
3. If the obtained fingerprint matches less than 60% with the existing fingerprint in the database, transaction cannot be performed.
4. If the fingerprint of the user is partially true (60%-99%) then OTP will be generated automatically and sent to the real user's mobile using "RSA" algorithm.
5. The generated OTP must be entered using the keypad which is already updated with the keypad ID.
6. The user is allowed for transaction if the OTP matches perfectly.

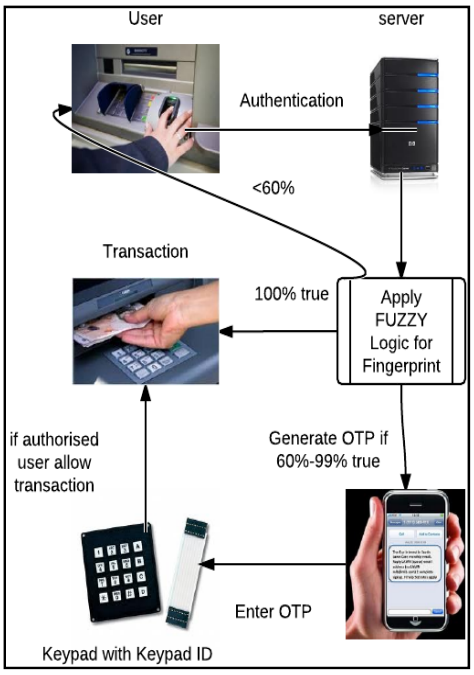

Fig.1.2 Login-Authentication Overview

This completes the description of the 5-Factor-Login-Authentication protocol in our work.

3.3 PIN-Change

After a successful login, the client can change his/her PIN. The server allows the client to change the old PIN with new PIN and updates the data in the RFID card accordingly.

3.4 Fingerprint-Selection

Similarly, one can change the fingerprint (using any one of the 5 fingers) used for authentication. To do so, the client has to record fingerprints of all the fingers in the database. The change of selected fingerprint will be updated in the RFID card automatically.

CONCLUSION

Preserving security and privacy is a challenging issue in distributed systems. This paper makes a step forward in solving this issue by proposing a fuzzy implementation of biometrics with five-factor authentication to protect services and resources from unauthorized use. The authentication is based on password, RFID card, OTP, fingerprint and keypad ID. Our work not only demonstrates how to obtain secure five-factor authentication from three-factor authentication, but also addresses issues of biometric authentication in distributed systems (e.g., client

privacy). The analysis shows that the work satisfies all security requirements on five-factor authentication and has several other practice-friendly features. The future work is to fully identify the practical threats on five-factor authentication and develop concrete five- factor authentication protocols with better performances.

REFERENCES

[1] Xinyi Huang, Yang Xiang, Jianying Zhou and Robert H. Deng, "A Generic framework for three factor authentication: Preserving security and privacy in distributed systems" IEEE Trans. Parallel and distributed system Vol. 22, no. 8, pp. 1390-1397, August 2011.

[2] C.-I. Fan and Y.-H. Lin, "Provably Secure Remote Truly Three- Factor Authentication Scheme with Privacy Protection on Bio- metrics," IEEE Trans. Information Forensics and Security, vol. 4, no. 4, pp. 933-945, Dec. 2009.

[3] C.H. Lin and Y.Y. Lai, "A Flexible Biometrics Remote User Authentication Scheme," Computer Standards Interfaces, 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] H. Tian, X. Chen, and Y. Ding, "Analysis of Two Types Deniable Authentication Protocols," Int'l J. Network Security, vol. 9, no. 3, pp. 242-246, July 2009.

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

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

[8] 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.

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

[10] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, "Biometric Cryptosystems: Issues and Challenges," Proc. IEEE, Special Issue on Multimedia Security for Digital Rights Management, vol. 92, no. 6, pp. 948-960, June 2004.

[11] C.-I. Fan and Y.-H. Lin, "Provably Secure Remote Truly Three- Factor Authentication Scheme with Privacy Protection on Bio- metrics," IEEE Trans. Information Forensics and Security, vol. 4, no. 4, pp. 933-945, Dec. 2009.

[12] 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.

[13] P.C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Proc. Int'l Cryptology Conf. (CRYPTO), pp. 388-397, 1999.

[14] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), pp. 523-540, 2004.

[15] M.-H. Lim and A.B.J. Tech, "Cancelable Biometrics," Scholarpedia, vol. 5, no. 1, p. 9201,2010

[16] T.S. Messerges, E.A. Dabbish, and R.H. Sloan, "Examining Smart-Card Security under the Threat of Power Analysis Attacks," IEEE Trans. Computers, vol. 51, no.5, pp.541-552, May 2002.

[17] Y.Dodis, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), pp. 523-540, 2004.

❑❑❑