IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-02, Issue-12 E-ISSN: 2347-2693

Secure Banking System Using Multi – Factor Authentication

Revathy Menon[1*], Ajisha John[2], Sini Jacob[3], Sneha Divakaran[4] and Diana Davis[5]

[1*,2,3,4,5] *Department of Information Technology*
Jyothi Engineering College, Cheruthuruthy, Thrissur, Kerala, India

www.ijcaonline.org

Received: Dec/02/2014 Revised: Dec/08/2014 Accepted: Dec/23/2014 Published: Dec/31/ 2014

***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

Authentication is the act of confirming the truth of an attribute of a datum or entity. Authentication often involves verifying the validity of at least one form of identification. Secure and efficient authentication scheme has been a very important issue with the development of networking technologies. In a distributed system, various resources are distributed in the form of network services provided and managed by servers [1].

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 [2].

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 systems assurance. This motivates the five-factor authentication, which incorporates the advantages of the authentication based on, RFID card, PIN, Fingerprint, OTP and Keypad ID.

A. 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. Proceedings, and not as an independent document. Please do not revise any of the current designations.

II. EXISTING SYSTEM

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.

Corresponding Author: *Revathy Menon, revathysatheesan@gmail.com*

III. PROPOSED SYSTEM

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.

MODULES OF MULTI – FACTOR AUTHENTICATION

A. *RFID card-based authentication*

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. 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.

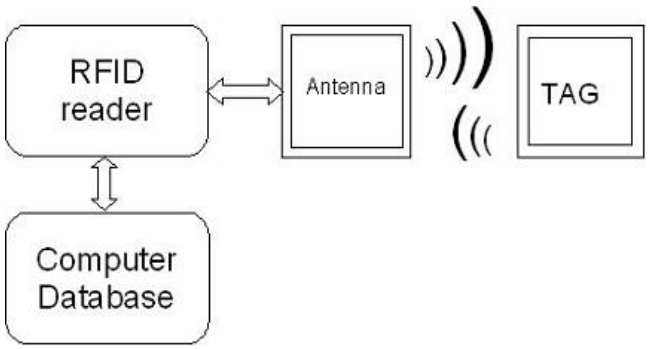

Fig 1: RFID working

B. *PIN*

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

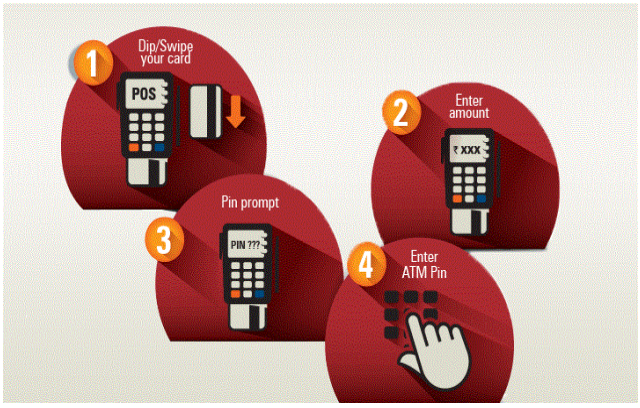

Fig 2: Enter PIN Number

C. *Fingerprint Scanning*

One can change the fingerprint (using any one of the 5 fingers) used for authentication. 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. Fingerprint scanners may be built into computer keyboards or pointing devices (mice), or may be stand-alone scanning devices attached to a computer [3].

Fig 3: Fingerprint Scanning

D. *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.

A common technology used for the delivery of OTPs is short message service (SMS). 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.

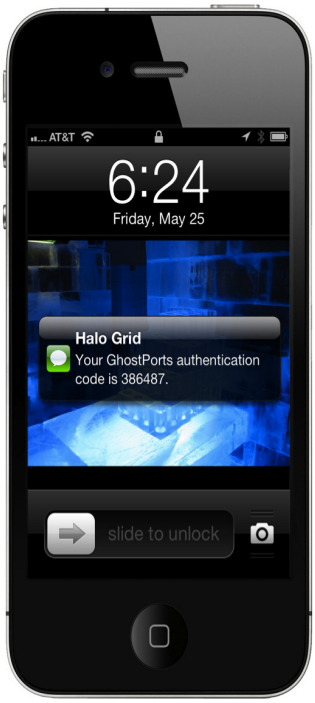

Fig 4: OTP over SMS

E. Keypad with Keypad ID

Keypad id has helped users to protect their username and passwords from being captured by key loggers, spyware and malicious bots. The keypad id is provided to the user during Account Registration [7].

Fig 5: Keypad

F. 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.

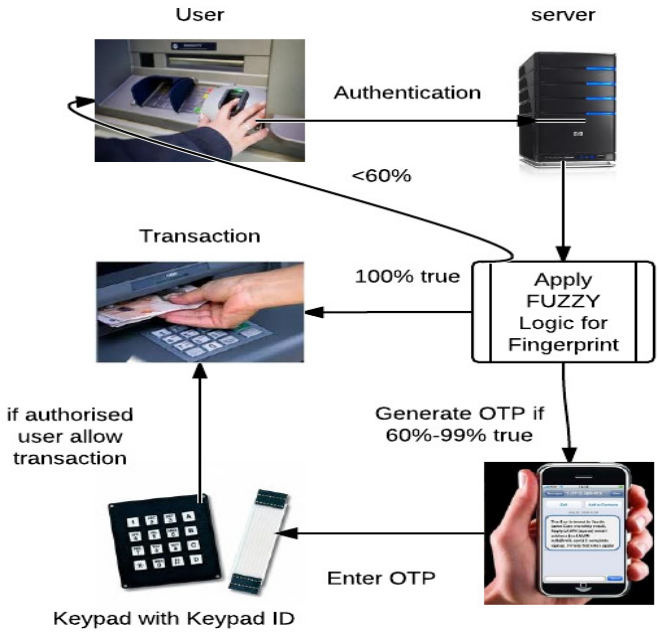

Fig 6: Login – Authentication Overview

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.

IV. 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.

ACKNOWLEDGMENT

We express our gratitude and thank to our Head of our Department Ms. Divya M Menon who have helped us a lot in the successful completion of initial phase of our project. We extend our gratitude and sincere thanks to our project coordinator Ms. Sabna AB who has always given her valuable time for us and also for her moral support. We remember the invaluable support offered by Ms. Diana Davis, our project guide and for his good suggestions and constant encouragement.

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] 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**.

[7] 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**.

