SECURE THREE FACTOR AUTHENTICATION SCHEME WITH MOBILE PROTECTION

PRASHANT R.AVHAD1, R.SATYANARAYANA2

1,2 Department of Electronics and Telecommunication, Dr. D.Y. Patil College of Engg., Talegaon, Pune, India

praschantravhad@gmail.com; sathyva.sintre@gmail.com

ABSTRACT

This paper explore a systematic approach for authenticating clients by three factors, namely password, smart card, face recognition and GSM (OTP). A Three-Factor Authentication Scheme Using Smart Card with Mobile Protection systems, various resources and services need protection from unauthenticated use. A generic and secure framework is proposed to upgrade two-factor authentication to three-factor authentication. The conversion not only improves the information assurance at low cost but also protects client privacy in distributed systems. The configuration is easy to implement. This paper proposes an authentication method which is based not only on the password and the user ID but also on the biometric input and the OTP as part of the security within different. However, this authentication scheme is unprotected to imitation attacks and middle man attacks. An attacker could impersonate authorized users to login and access the remote server.

Full papers are expected to be between 6 pages (minimum) and 8 pages (normal maximum) in length. Please use this as a template for your paper.

Keywords: Smart Card, Three Factor Authentication, GSM, RFID etc.

1 INTRODUCTION

Three-factor authentication method was introduced as advancement to two-factor authentication schemes in remote authentication. The three factors used in authentication are a smart card, password and a biometric. The authentication is based on the characteristics of these three factors. To improve the security in the remote authentication, biometric was introduced. Due to the uniqueness and the characteristics of biometrics, they are quite suitable for user authentication and also reduce the drawbacks inherited from passwords and smart cards [13].

Authentication is considered as the first step of security requirement for any grid environment against probable threats. This paper proposes an authentication method which is based not only on the password and the user ID but also on the biometric input and the OTP. We are going to use three factor authentications for bank account transactions. Where in such transaction we need to have more security we are using RFID for embedded security and face reorganisation for biometric security and GSM communication for password security. In remote authentication schemes, the remote system gains information about the identity of the communicating Person or device. Since the introduction of Lamport’s scheme [10], several new proposals and improvements on two-factor remote systems authentication [6, 7, 8, 9, 11] have been proposed. Lamport proposed a password authentication scheme to provide authentication between the users and the remote server. Since then, many password-based remote user authentication schemes have been proposed. In a smart card (RFID) based password authentication scheme, the smart card takes the password and Secret pin from the users as input, computes the login message and sends the login message to the server. The server checks the validity of the user’s login message. In the mutual authentication situation, not only the server can verify the user but also a user can verify the server.

The adversary is modelled as follows:
(a) The adversary can tap the communication channel between the users and the server during the login and authentication phase.
(b) The adversary either can extract the information by obtaining the smart card or can get a user’s password and Finger print. The adversary cannot do both, or the adversary can login the server as a legitimate user

2. RELATED WORK

Chun-I-Fan and Yi-Hui-Lin in their paper Provably Secure Remote Truly Three Factor Authentication Scheme with Privacy Protection on Biometrics [5] tries to prove such a three-factor authentication scheme that is suitable in smart card environment as well as avoids most of the disadvantages of previously proposed three-factor authentication schemes. The scheme proves to have many advantages. The authors claim that the scheme is a truly three-factor authentication scheme that also provides privacy protection to biometrics. They claim that their scheme is immune to password loss, offline dictionary attack and biometric loss. Also they claim that the biometric and password are checked at the server without revealing its actual value to the server. No databases or tables are utilized at server side so as to improve the security by avoiding database attacks at server. Also unlike previous three-factor authentication schemes [1, 2, 3, 4], no complex computational procedures are adopted in their scheme. But still there are certain loopholes in their scheme that can break the entire scheme.
even without obtaining any of the user identity information. There are different weaknesses in the Fan-Lin scheme. The scheme aimed to achieve truly three-factor authentication by authenticating at the server. Even if the scheme is called a truly three-factor one, its performance is inefficient.

Several three-factor authentication schemes have been proposed in the literature [14], [15], Lee et al. [16] proposed a fingerprint-based remote user authentication scheme using smart cards in 2002. In the scheme, users insert their smart cards into card readers and then input their fingerprints and passwords in the login phase. The fingerprint will be checked according to the fingerprint template stored in the card and some parameters will be randomly generated from the user’s fingerprint minutiae. The scheme was, however, broken by Line et al. [18] and by Chang et al. [20]. Lin et al. [18] discovered that a registered user could create many valid pairs of identities and passwords to masquerade as other legal users. Chang et al. [20] pointed out that Lee’s scheme is unworkable and cannot resist a conspiring attack. Kim et al. [15] proposed an ID-based password authentication scheme using smart cards and fingerprints in 2003. This scheme has also been shown to be insecure, however, because an attacker can impersonate a legal user [27]. Another scheme was proposed by Lin et al. in 2004 [18]. This scheme combines passwords and fingerprint minutiae templates into super passwords and allows passwords to be changed off-line. This system has also been found to be unsafe. The password change operation is vulnerable because smart cards cannot check the correctness of old passwords [25]. In addition, the scheme is vulnerable to an impersonation attack [14]. Yoon et al. proposed an improvement that solves this problem. Their improved scheme was itself broken by Lee et al., who also proposed a further improved scheme in 2006 [17].

This most recent scheme has not yet been broken, but it still, like other methods, lacks a means of checking on biometrics in the server’s sides. Bhargav-Spantzel et al. proposed a privacy preserving multifactor authentication protocol with biometrics [19]. The factors they used are a fingerprint, a random string, and a password or other personal identifiers, and they are combined together to form a cryptographic key for verification. The server cannot know the factors due to zero-knowledge proofs being included. However, the server must maintain a commitment database to record all users’ commitments which contain biometric data and random strings for the server to verify these factors. Besides, it is not suitable for smart-card environments since each of the users should perform modular exponentiation computations in the authentication phase. However, in biometric-based authentication, the above idea should be performed on the client side rather than on the server side [26] for the protection of biometrics against the server. If we want the server to perform the secret-extracting algorithm for truly three-factor authentication, it should know the input biometric sample. And after executing the secret-extracting algorithm, the server also obtains the embedded secret. The secret can recover the original biometric template with the public sketch. Therefore, the technique of [21], [22], [23], and [24] is not sufficient to solve our problem because it does not consider privacy protection for biometric data against the server when the operations about biometrics are performed in the server’s side. Our proposed scheme matches biometrics in the server and considers the strong privacy of biometrics. Since all of the above previous schemes perform the checking of biometrics in the cards, the server must trust the smart cards to properly handle the task. But an adversary can skip the checking process in the smart cards without the remote server noticing. Previously we have used smart cards. The biggest problem facing smart cards is security and the problem is two fold. The first issue is that not all smart cards are in fact secure. VISA and MasterCard developed a new standard, SET, in early 1996 in an attempt to get the entire industry on a standard of encryption. Additionally, there are standards such as DES which have been around for years, usable in all forms of encryption which are being used in smart cards. But still some smart cards are not inviolate. Mondex, a maker of banking smart cards, solves this problem by making its transactions possible only between Mondex cards. But in order for smart cards to reach their full potential, they must be able to interact with a host of interfaces. And they must do so securely. The second issue with security involves public perception of the technology. People must believe that the cards are secure. This depends to a great extent upon actual security, but people must also be convinced of it. And once people are comfortable that the card is secure, they must still be confident.

A third issue concerns who holds responsibility for the card. If the cash balance is wiped clean by a memory failure, who is liable, the person or the bank? If a transaction is not recorded, where are the lines drawn? Currently companies have begun to write out agreements in order to draw boundaries, but these will have to be ones which consumers are comfortable with in order for people to begin to use smart cards. The final problem which smart cards will face in their move to diffuse extensively involves product complements. While smart cards themselves are fairly cheap, card readers are not (costing between $50 and $200). However, in an effort to make smart cards more pervasive, companies such as Netscape and Microsoft are proposing putting software in packages they make. Additionally, Gemplus has created a new pocket reader and other companies are considering adding readers to keyboards.
3. PROPOSED MODEL

![Proposed Authentication Block Diagram](image)

3.1 Smart Card: Now we are using RFID tags as devices that stores a unique number but has no processing capability. It is more like a radio-based RFID bar code used mostly for chips are identification (hence much smaller than smart chips “radio frequency identification”). It can work even in water, air.

3.2 FPGA: Field Programmable Gate Array. It will sense that RF signal and send one interrupt from FPGA to PC where in Matlab

3.3 GSM: Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. A GSM modem is a wireless modem that works with a GSM wireless network. A wireless modem behaves like a dial-up modem. The main difference between them is that a dial-up modem sends and receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves.

In this first we are going to identify the person by using active RF ID tag, depending upon the RF signal which is connected to the FPGA it will sense that RF signal and send one interrupt from FPGA to PC where in Matlab we are going to compare the face image in that folder, here we already having data base related to the received FPGA signal, if the selected image is in data base then person is authorized if not person is not authorized. If person authorized means then it will go for third level of authentication, if person is not authorized then buzzer will blow to alert the security. In third level security here we are using GSM communication to send one time password, if the person enter the same password then further process is going on, if password enter is wrong then it will block the user at that stage itself.

![Proposed Authentication Architecture](image)

The proposed scheme consists of client side, terminal side and server side. In client side we sense the biometric data (for example iris) using a sensor. In terminal side, we perform image processing operation for extracting feature vectors and then this feature vector is converted into a single vector using SVD (Single Vector Decomposition) [12]. Then the vector is encrypted using a strong public key encryption (example RSA Algorithm). This encrypted value is send to the server. At server side, a random number, generated using a random generator, is added to the encrypted value and public key which gives the advantage of protecting the server side authentication process. For example, if an intruder tries to compromise the server, still we can be effective in protecting the biometric data as it is randomized with the random number. Now the randomized value is product with the encrypted value which results in the value S. Then the value S is passed to the smart card storage. Using the smart card, the value S is compared with a range of threshold which makes the decision.
4. COMPARISON
Existing system
- At present we are using a single card or the individual card for different banks like ICICI, AXIS, HDFC, etc.
- The PIN number in the negative behind the card
- There will be only one PIN number

Proposed system
- All the banks must be in the single card
- The PIN number is not present in the negative
- There will be three passwords
- PIN no and authentication password, fingerprint

5. RESULTS
I. Identify the person by using an RFID card, then using Matlab compare the face image.

II. If the person is authorized, then it proceeds to the next authentication.

III. Select the bank from which you want to debit money.

IV. Enter the PIN number for that particular bank.

VI. Then window is open where they ask for amount withdraw & other options such as checked balance.
V. If person is not authorized then buzzer will blow to alert the Security.

CONCLUSIONS

There are many schemes that deal with three-factor authentication process, but they are unable to deal with both Client & Server side Security. By using this three factor authentication there we provide both security. The configuration is easy to implement. However, this authentication scheme is unprotected to imitation attacks and middle man attacks. Hence our proposed scheme gives advantage of protecting information from the user except the required identity.

ACKNOWLEDGEMENTS

I would like to thank all the staff members of E&TC Department of Dr. D. Y. Patil College of Engineering, Ambi for their valuable guidance and support.

REFERENCES