International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064

A Three-Factor Authentication Scheme in ATM

Prashant R. Avhad[1], R. Satyanarayana[2]

[1]Department of Electronics and Telecommunication
Dr. D. Y. Patil College of Engineering, Talegaon Pune, India

[2]Assistant Professor, Department of Electronics and Telecommunication
Dr. D. Y. Patil College of Engineering, Talegaon, Pune, India

Abstract: ***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 An Improved Three-Factor Authentication Scheme Using Smart Card with Mobile Protection An Improved Three-Factor Authentication Scheme Using Smart Card with Mobile Protection systems, various resources and services need protection from unaccredited use. Remote authentication is the most commonly used method to determine the identity of a remote client. This paper explore a systematic approach for authenticating clients by three factors, namely password, smart card, face recognition and GSM. 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. 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.***

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

1. Introduction

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 authentication for bank account transactions where in such transaction we need to have more security we are using RF id for embedded security and face recognition 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 modeled 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.
c) 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].

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.

The following are certain flaws

A. Server Side Attack
During authentication phase, the two biometric strings obtained during registration and login phase are taken to the server for matching. So the authentication of the user depends only upon the matching algorithm that decides the score. So if an attacker attacks the matching algorithm to make false decisions, the server gets compromised and illegal user can gain access to the system. Also, the keys for encryption and decryption are stored in the server which can be obtained easily by an attacker.

B. Not Truly Three-Factor Scheme
To make the scheme a truly three-factor authentication scheme, all the three factors should be utilized efficiently in the authentication process. The password is not checked properly at the client side. Instead it is directly encrypted during login phase without checking with the encrypted value stored in the card and send to the server for decision making. The procedure follows in such a way that the password has no particular contribution or role in increasing the efficiency of the scheme.

C. Vulnerabilities in Password Hashing
During hashing process, the password is actually combined with a vector and converted into a complex format. The disadvantage in this case is that if this hashing vector is compromised, the entire password could be revealed. In Fan-Lin scheme, at the server side during authentication, the hashed passwords obtained during registration and login phase are taken for matching. At this time when an attacker tries to compromise the system, he can obtain the hashed passwords and break the scheme. Also no password checking is performed at the client side.

D. Attack by an Adversary
Consider that an attacker obtains the biometric of a legitimate user and enters the wrong password. Since password is not checked at client side, the rest of the operations like extracting the random number r from the sketch stored in the card given by r = A(Si (r), Si*) will be performed. With this r the password will be hashed and taken to server. If the attacker obtains the random number, he can obtain the original password of the user by decrypting the stored details in the card. Otherwise, if he compromises the matching algorithm, he can enter the network as a legitimate user.

E. Security Vulnerabilities Due to Insecure Channel
In a remote user authentication scheme, some information are openly transmitted through the insecure channel so that any attacker can intercept the insecure channel and then this intercepted information can be used to construct any fabricated information. Previously we have used smart cards. The biggest problem facing smart cards is security and the problem is twofold. 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 that holds responsibility for the card. If the cash balance is wiped clean by a memory failure, which 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

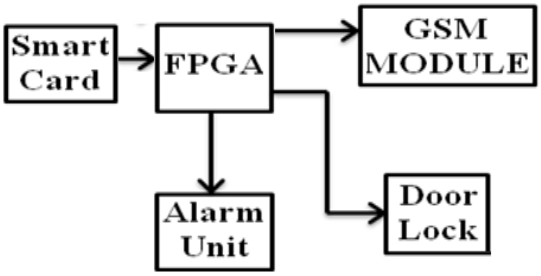

Figure 1: Proposed Authentication Block Diagram

3.1 Smart Card
Now we are using RFID tags are 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. 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 RF id for embedded security and face recognition for biometric security and GSM communication for password security.

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 enters the same password then further process is going on, if password enters is wrong then it will block the user at that stage itself.

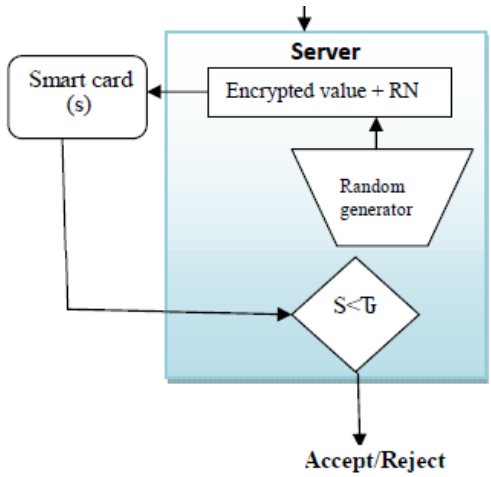

Figure 2: Proposed Authentication Architecture

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

4.1 Existing System

- At present We Are Using Single Card or the Individual Card for the Different Banks Like ICICI, AXIS, HDFC, Etc.,
- The Pin Number in the Negative Behind the Card
- There will be a only one PIN Number

4.2 Proposed System

- All The Bank Must Be in the Single Card
- The Pin No is not present in the Negative
- There Will be Three Passwords
- PIN No and Authentication Password, Finger print

References

[1] J. K. Lee, S. R. Ryu, and K. Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," *Electron. Lett.*, vol. 38, no.12, pp. 554–555, 2002.
[2] C. H. Lin and Y. Y. Lai, "A flexible biometrics remote user authentication scheme," *Comput. Standards Interfaces*, vol. 27, no. 1, pp. 19–23, 2004.
[3] H. S. Kim, J. K. Lee, and K. Y.Yoo, "ID-based password authentication scheme using smart cards and fingerprints," *ACM SIGOPS Operating Syst. Rev.,* vol. 37, no. 4, pp. 32–41, 2003.
[4] Bhargav-Spantzel, A. C. Squicciarini, E. Bertino, S. Modi, M. Young, and S. J. Elliott, "Privacy preserving multi-factor authentication with biometrics," *J. Comput. Security*, vol. 15, no. 5, pp. 529–560, 2007.
[5] Chun-I-Fan and Yi-Hui-Lin, "Provably secure remote truly threefactor authentication scheme with privacy protection on biometrics," *IEEE Trans. Information Forensics and Security,,* vol. 4, no. 4, pp. 933-945, Dec 2009.
[6] K. Awasthi and S. Lal, "An enhanced remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 583-586, 2004.
[7] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629-631, 2004.
[8] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards,"*IEEE Transactions on Consumer Electronics*, vol. 46, pp.28-30, 2000.
[9] D. P. Jablon, "Strong password-only authenticated key exchange," *ACM Computer Communications Review*, vol. 26, no. 5, pp. 5-26, 1996.
[10] L. Lamport, "Password authentication with insecure communication," Communications of ACM, vol. 24, pp. 770-772, 1981.
[11] C. C. Lee, L. H. Li, and M. S. Hwang, "A remote user authentication scheme using hash functions," ACM Operating Systems Review, vol. 36, no. 4, pp. 23-29, 2002.
[12] Maneesh Upmanyu, Anoop M. Namboodiri, Kannan Srinathan, and C. V. Jawahar, "Blind Authentication: A Secure Crypto-Biometric Verification Protocol", *in*

IEEE Transaction on Information Forensics and Security, vol.5, No. 2, June 2010.

[13] Harlay Maria Mathew, Pandit Samuel J Gundapu, S. Benson Edwin Raj, Jeeva Flora Angeline S" An Improved Three-Factor Authentication Scheme Using Smart Card with Biometric Privacy Protection" in IEEE Conference, 2011