ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Secure Smart Card Based Remote User Authentication Scheme for Multi-server Environment

Archana P.S, Athira Mohanan

M-Tech Student [Cyber Security], Sree Narayana Gurukulam College of Engineering Ernakulam, India

ABSTRACT: In a network environment the number of server providing the facilities for the user is usually more than one since the authentication protocols for multi-server environment are required for practical applications. There are a number of methods proposed for multi-server environment. Many of these methods achieve mutual authentication by sending encrypted or hashed secret information across the network which make them vulnerable to various Man-In-The-Middle attacks. In this paper we propose a secure smart card based remote user authentication scheme for multi-server environment. The proposed scheme use both smart card and biometric information for authentication. Smart card stores some sensitive data corresponding to the user that assist in user authentication. Our scheme not only supports multi-server environments but also achieves many security requirements. The security analysis of this method proves that the method is strong enough to prevent many attacks.

KEYWORDS: Multi-Serve; Smart card; Mutual Authentication

I. Introduction

With the rapid growth of Internet technologies, the system providing resources to be accessed over the network often consists of many different servers around the world. When a user requests a server's service, he must pass an examination of user authentication. Through this user authentication process, the server can determine whether the user can use the services provided by the server. When a user uses a service in a server, the transmitted messages between the user and the server must be kept secret. With the growing popularity of the multi-server architecture, authentication schemes designed for the multi-server architectures have been investigated and designed by many researchers. Among all of the schemes, password based authentication schemes with smart card are the most popular, mainly due to their strong security and simplicity. Basically, smart card authentication schemes consist of three phases namely; registration phase, login phase and authentication phase. The registration phase is invoked whenever new user registers in the server. Upon receiving the registration request, server issues a smart card to user by storing the necessary parameters into smart card memory. The login phase and authentication phase are invoked at the time when user login into the server. After receiving the login request, server checks the validity of the login request to authenticate the user.

II. Related work

Authentication is the primary step in any secure transaction. To achieve this, any of the multi-server authentication schemes can be used. Multi-Server authentication scheme enables a user to obtain services from multiple servers after registering with a registration Center (RC). Many researchers have come up with different authentication schemes designed specifically for a mutli-server environment because of its growing popularity. In a network environment, when a user requests a server's service, he must pass an examination of user authentication. Through this user authentication process, the server can determine if the user can use the provided services and the exact access rights of this user in these services. When a user uses a service in a server, the transmitted messages between the user and the server must be kept secret. They must negotiate a session key to be used for protecting their subsequent communications. Since a remote user authentication scheme proposed by Lamport [7] to authenticate a remote user over an insecure channel, several schemes have been proposed to improve functionality, security, and efficiency [2, 3, 4, 6, 8, 21, 22, 23, 24, 25].Due to the cryptographic capacity and portability, smart cards have been widely used in many e-commerce applications. As mentioned in [4, 8], the following criteria are crucial for remote authentication and session key agreement schemes using smart cards.

Among all of the schemes, password based authentication schemes with smart card are the most popular due to their strong security features and simplicity. W.-S. Juang[1] proposed a password authenticated key agreement using smart cards. Liao and Wang [17] pointed out that, Juang's scheme neither updates user's password without the help of registration Center nor provide the smart card for the mechanism of checking identity and password in the login phase. Thus, it will easily suffer online guessing attack after losing the smart card. Besides, if the secret parameters of the smart card are extracted with some ways, Juang's scheme cannot withstand offline dictionary attack. They proposed a dynamic ID based remote user authentication scheme for multi-server environment. Hsiang and Shih [18] proved that Liao and Wang's scheme fails to provide mutual authentication. They improved Liao and Wang's dynamic identity based smart card authentication protocol for multi-server environment. However, Sood et al. [19] found that Hsiang and Shih's protocol is susceptible to replay attack, impersonation attack and stolen smart card attack. The scheme of Sood et al [19] does not provide mutual authentication between the user and the server, which means that a user has no way to verify the validity of the service providing server. Chen et al.[5] then proposed robust smart card based remote user password authentication scheme. But the scheme cannot really ensure forward secrecy, and the validity of the password is verified by the server, so if the user inputs a wrong password in login phase, it will waste unnecessary communication and computation cost [20].

In this paper, a secure smart card based mutli-server mutual authentication scheme is proposed based on smart card, password and biometrics. This scheme successfully establishes a session key between the user and the server. This scheme also satisfies the security properties such as resistance to replay attack, resistance to masquerade attack, resistance to DoS attack, resistance to insider attack.

III. PROPOSED METHOD

In this section, we propose an efficient multi-server password authenticated key agreement scheme using smart cards. There are three kinds of participants in our protocol: users, servers and a registration centre. In this scheme, we assume the registration center can be trusted. The registration centre examines the validity of login users and then issues a smart card to eligible users. The user only has to register at the registration center once and can use services provided by various servers. The proposed method consists of two phases:

- Registration phase
- Login and mutual-authentication phase
- Password change phase

Out of Band Authentication (OOB) is one of the main key features of this scheme. For OOB sms services can be used. The security functionality of the proposed method will be further analyzed. The notations used in this method are summarized in Table 1.

A. *Registration Phase:*

If any user U_i wants to get services from the available servers under the control of Registration Center (RC), First all the users must undergo registration phase. Let the servers be S = $S_1 ... S_j ... S_n$, As a first step the user U_i selects a user identity id_i and a password $pw_{i,}$ then send id_i, $h(pw_i)$ to the Registration Center (RC). After verifying the uniqueness of the identity the RC sends a unique key k_i to the user U_i for further communication. The key k_i send using the OOB service such as sms. The user U_i then select a secret sec and then compute the actual password npw_i for the user U_i, $npw_i = h\ (id_i \oplus h(pw_i||sec))$. Then input the biometric characteristics of the user such as finger print by using proper device. Then the user sends pw_i, id_i and BIO encrypted with the key k_i through secure channel. After getting this message the Registration Center(RC) become capable of calculating npw_i, RC then generated a smart card for the user U_i along with BIO, id_i, npw_i, k_i. The Registration Center(RC) sends the details such as k_i, id_i, P_{ij} and npw_i to the corresponding servers those selected by the RC for providing services to the user U_i.. P_{ij} is the service period of a server S_i for any user $U_{i.}$ The registration phase is shown in Fig.1.

DOI: 10.15680/IJIRCCE.2015. 0310120

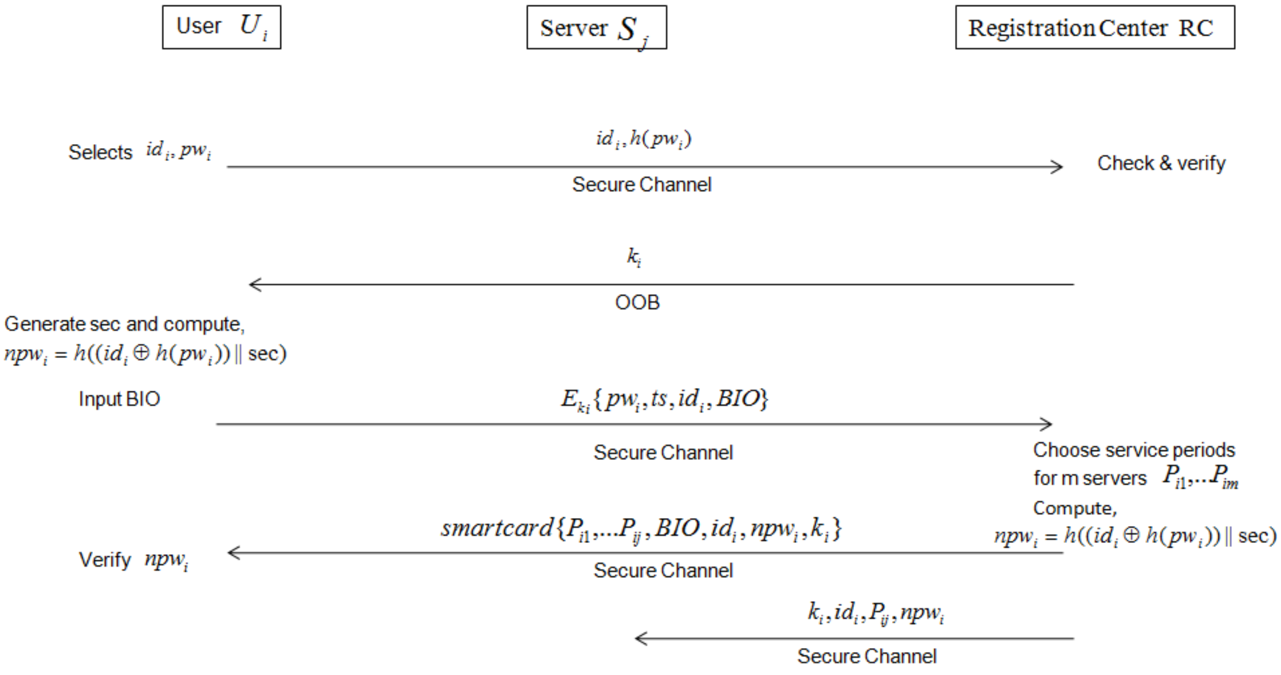

User U_i
Server S_j
Registration Center RC
Selects id_i, pw_i
$id_i, h(pw_i)$
Secure Channel
Check & verify
k_i
OOB
Generate sec and compute,
$npw_i = h((id_i \oplus h(pw_i)) \| \sec)$
Input BIO
$E_{k_i}\{pw_i, ts, id_i, BIO\}$
Secure Channel
Choose service periods for m servers $P_{i1},..P_{im}$
Compute,
$npw_i = h((id_i \oplus h(pw_i)) \| \sec)$
$smartcard\{P_{i1},...P_{ij}, BIO, id_i, npw_i, k_i\}$
Verify npw_i
Secure Channel
k_i, id_i, P_{ij}, npw_i
Secure Channel

Fig. 1 Registration Phase

B. *Login and mutual-authentication phase:*

When a user U_i want to access the services of any server S_j, login and mutual-authentication phase is invoked. The user swipe the smart card for the local system verification. During local system verification the biometrics entered in the smart card is compared with the sample taken from the user at the time of login attempt, this helps to prevent the system from Man-In-The-Middle attacks. The local system sends the id_i along with the P_{ij} and time stamp ts encrypted with the secret key k_i. After receiving this message the server S_j generates a onetime key key_{ij} to the user through sms to the mobile phone. Then the local system sends $MAC_{keyij}(BIO)$, ts, id_i, npw_i to the server S_j encrypted with the key k_i. When the server get this details, the server S_j computes $MAC_{keyij}(BIO)$, and then compares it with the received $MAC_{keyij}(BIO)$, hence we can say that the user U_i is authenticated to the server S_j. As a next step server S_j calculates k_{ssi} as $h(npw_i \oplus key_{ssi})$ and then send id_i and ts encrypted with k_{ssi} to the user U_i. After receiving it the user decrypt the message by calculating the key key_{ij}. Then verify id_i and also check the time stamp ts. The existence of ts helps to check the freshness of the message. As a result we can say that the server S_j is authenticated to the user U_i. So the mutual authentication is completed, Session key is discarded when the session expires. The mutual authentication phase is depicted in Fig.2.

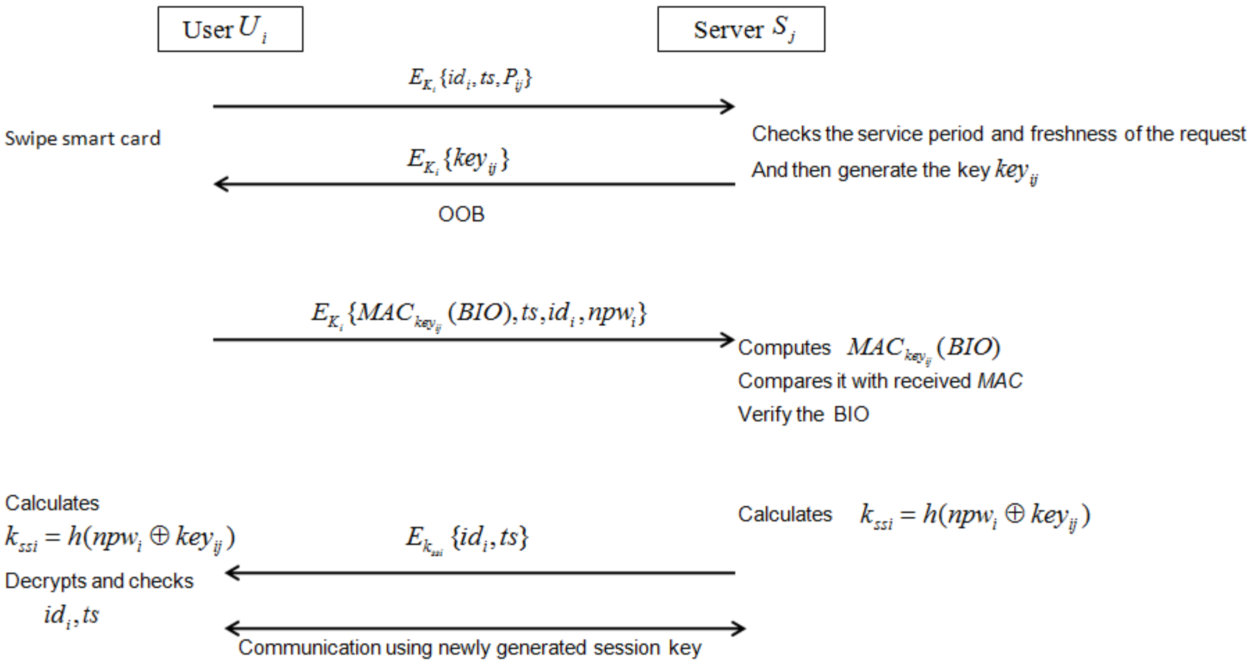

User U_i
Server S_j
$E_{K_i}\{id_i, ts, P_{ij}\}$
Swipe smart card
Checks the service period and freshness of the request
And then generate the key key_{ij}
$E_{K_i}\{key_{ij}\}$
OOB
$E_{K_i}\{MAC_{key_{ij}}(BIO), ts, id_i, npw_i\}$
Computes $MAC_{key_{ij}}(BIO)$
Compares it with received MAC
Verify the BIO
Calculates
$k_{ssi} = h(npw_i \oplus key_{ij})$
$E_{k_{ssi}}\{id_i, ts\}$
Calculates $k_{ssi} = h(npw_i \oplus key_{ij})$
Decrypts and checks
id_i, ts
Communication using newly generated session key

Fig. 2 Login & Mutual Authentication Phase

C. *Password change phase:*

This procedure is invoked whenever a user wants to change his password. In this procedure, the user can easily change his password with minimum number of steps as shown in fig.3.

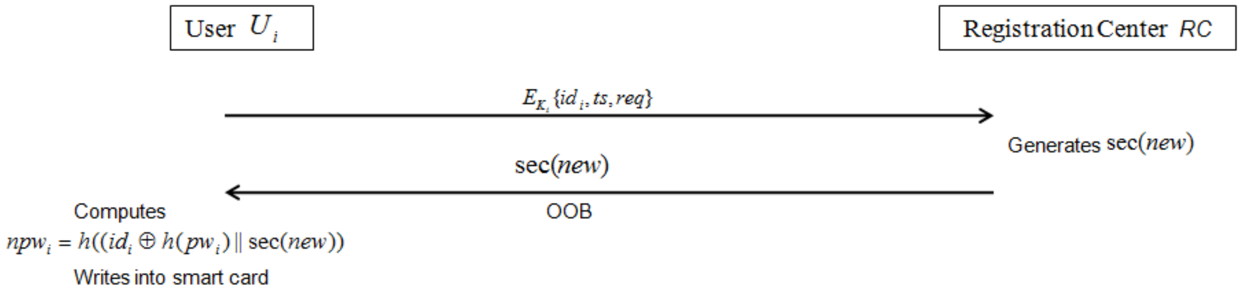


Fig. 3 Password Change Phase

IV. Security Analysis

This section provides the security analysis of the proposed scheme against other multi-server schemes. Table 1 shows the Comparison of our scheme with other multi-server schemes.

A. *Mutual Authentication:*

To achieve mutual authentication the client must prove its identity to the server and also the server prove its identity to the user. In our proposed protocol mutual authentication is achieved, which is explained in the login and mutual authentication phase of the proposed system.

B. *Simple & secure password modification:*

The proposed scheme provides simple and very secure password modification method. If the smart card and the password are stolen by any intruder, he/she cannot able to masquerade as a legitimate user because during the time of local system verification the biometric characteristics stored in the smart card is compared with the login users biometric characteristics. The password modification phase is very simple and secure, the OOB transfer of sec(new) helps to improve the security.

C. *Fast error detection:*

In this scheme the error detection is very effective and fast

D. *Insider attack resistance:*

An insider attack is a malicious attack performed on a network/computer system by a person who has an authorized system access. The biometric detail of the user helps to avoid such kind of attacks.

E. *Forgery attack resistance:*

The OOB communication and biometric checking helps to avoid all kinds of forgery attacks because, the biometric character is completely different for any two persons. And also the OOB communication can be consider as a secure communication.

F. *Three factor security*:

In this proposed system we will make use of three factors such as password, smart card and the biometric characteristics for the authentication.

Table 1

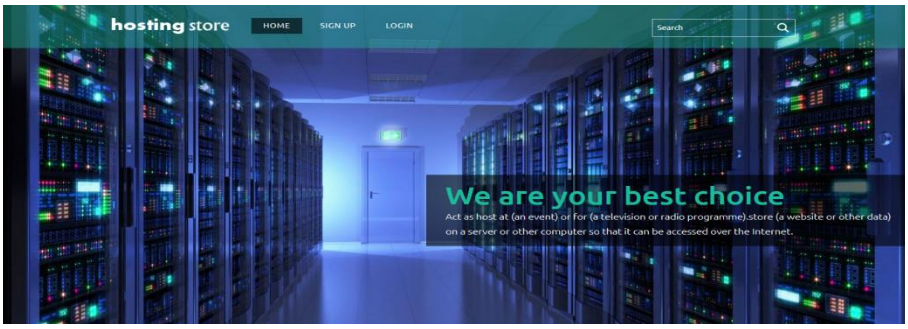
Comparison with other multi-server schemes

	Our	Juang et al.	Tsai	Liao et al.	Yoon et al.
		(2004)	(2008)	(2009)	(2010)
C1	Yes	Yes	Yes	No	Yes
C2	Yes	No	No	Yes	Yes
C3	Yes	No	No	Yes	Yes
C4	Yes	No	No	No	No
C5	Yes	Yes	Yes	Yes	No
C6	Yes	No	No	No	Yes

C1: Mutual-authentication C2: Simple & secure password modification
C3: Fast error detection C4: Insider attack resistance
C5: Forgery attack resistance C5: Three factor security

V. Simulation Results

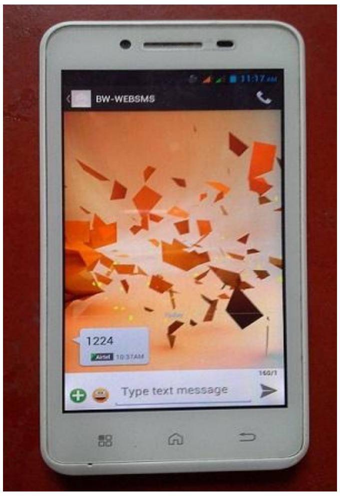
This section describes the details of the proposed protocol implementations. We implemented the protocol by using .Net programming. For Out-of-Band Authentication we use SMS. The fig.4 shows the home page of the implemented scheme.

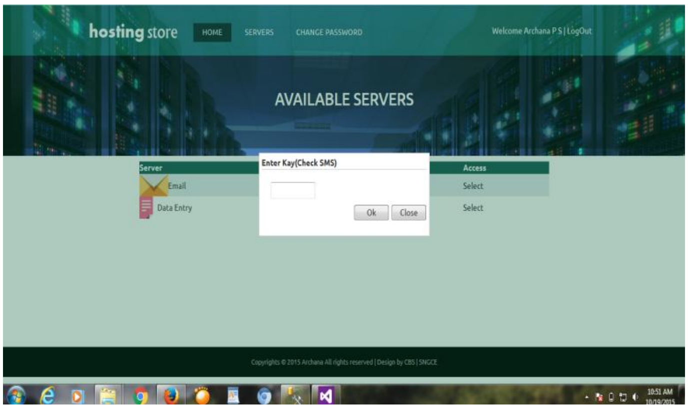


Act as host at (an event) or for (a television or radio programme).store (a website or other data) on a server or other computer so that it can be accessed over the Internet.

Fig.4 Home Page

The sample of OOB authentication SMS is shown in fig.5.





Server	Access
Email	Select
Data Entry	Select

Fig.5. SMS through phone .

Fig.6. Key Generation

After registration phase the valid user get smart card. By using this smart card and the biometric characteristics he/she can communicate with the servers allocated by the RC. After authentication user get a home page with information about the available servers. The user can select the server. When the user clicks into the select button he/she get a new key through SMS. After entering the key the user can start using the server. All these operations are shown in the fig.6.

VI. Conclusion And Future Work

In this paper, a secure smart card based remote user authentication scheme for multi-server environment is proposed. Through analysis it has been proved that the proposed scheme is strong enough to prevent different attack. The proposed scheme archives mutual authentication and session key agreement. A comparison with other schemes shows that the proposed scheme is more secure than the other related schemes.

In the future, we will propose a cryptanalysis scheme to prove that our authentication mechanism is secure and discuss the biometric matching issue in detail.

REFERENCES

1. Wen-Shenq Juang (2004") Efficient Multi-server Password Authenticated Key Agreement Using Smart Cards." IEEE Trans-actions on Consumer Electronics, pp. 251255.
2. C. Chang and T. Wu, "Remote Password Authentication with Smart Cards, "IEE Proceeding-Computers and Digital Techniques, Vol. 138, No. 3, pp. 165-168, 1991.
3. C. Chang and S. Hwang, "Using Smart Cards to Authenticate Remote Passwords," Computers and Mathematics with Application, Vol. 26, No. 7, pp. 19-27, 1993.
4. H. Chien, J. Jan, and Y. Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card," Computers and Security, Vol. 21, No. 4, pp. 372-375, 2002.
5. Chen BL, Kuo WC, Wuu LC (2012). Robust smart-card-based remote user password authentication scheme, International Journal of Communication Systems.
6. M. Hwang and L. Li, "A New Remote User Authentication Scheme Using Smart Cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, pp. 28-30, February, 2000.
7. L. Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, Vol. 24, pp. 770-772, 1981.
8. W. Juang, "Efficient Password Authenticated Key Agreement Using Smart Cards," Computers & Security, in press, 2004
9. L. Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, Vol. 24, pp. 770-772, 1981.
10. Li Bai, Saroj Biswas, Albert Ortiz and Don Dalessandro (2006)." An Image Secret Sharing Method," In Prec. of the 9th International Conference on Information Fusion.
11. Juang, Wen-Shenq (2004). "Efficient multi-server password authenticated key agreement using smart cards." IEEE Transaction on Consumer Electronic, 50(1), 251–255.
12. Tsai, J. L. (2008)." Efficient multi-server authentication scheme based on one-way hash function without verification table." Computers & Security, 27(3–4), 115–121.
13. Liao, Y. P., & Wang, S. S. (2009)." A secure dynamic ID based remote user authentication scheme for multi-server environment." Computer Standards & Interfaces, 31(1), 24–29.
14. Yoon, E.-J., & Yoo, K.-Y. (2010). Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. Journal of Supercomputing, 1–21.
15. Jia-Lun Tsai, Nai-Wei Lo, Tzong-Chen Wu (2013)." A new password-based mutli-server authentication scheme robust to password guessing attacks." Wireless Pers Communication, Springer.
16. Ming-Chin Chuang, Meng Chang Chen (2014). "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics." Journal of Expert Systems with Applications, pp. 1411-1418.
17. Yi-Pin Liao, Shuenn-Shyang Wang (2009)." A secure dynamic ID based remote user authentication scheme for multi-server environment". Journal of Computer Standards Interfaces, pp. 24-29.
18. Han-Cheng Hsiang, Wei-Kuan Shih (2009). "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment", Journal of Computer Standards Interfaces, pp. 24-29.
19. Sandeep K. Sood, Anil K. Sarje, Kuldip Singh (2011)."A secure dynamic identity based authentication protocol for multi-server architecture," Journal of Network and Computer Applications , pp. 609-618.
20. Xiong Li, Jianwei Niu, Muhammad Khurram Khan, Junguo Liao (2013). "An enhanced smart card based remote user password authentication scheme." Journal of Network and Computer Applications, pp. 1365-1371.
21. W. Juang, C. Lei and C. Chang, "Anonymous Channel and Authentication in Wireless Communications," Computer Communications, Vol. 22, No. 15-16, pp. 1502-1511, 1999.
22. W. Yang and S. Shieh, "Password Authentication Schemes with Smart Cards," Computers and Security, Vol. 18, No. 8, pp. 727-733, 1999.
23. H. Sun, "An Efficient Remote User Authentication Scheme Using Smart Cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 4,pp. 958-961, November, 2000.
24.] K. Tan and H. Zhu, "Remote Password Authentication Scheme with Smart Cards," Computer Communications, Vol. 18, pp. 390-393, 1999.
25. S. Wang and T. Chang, "Smart Card Based Secure Password Authentication Scheme," Computers and Security, Vol. 15, No. 3, pp.231-237, 1996.
.