Biometric and ID Based User Authentication Mechanism
Using Smart Cards for Multi-Server Environment

U. S. Pandey1 and Vibha Kaw Raina2
1School of Open Learning, Delhi University,
2B.I.T MESRA Ranchi Extension centre NOIDA
1us_pandey@hotmail.com and 2kawvibha@yahoo.com

ABSTRACT
Since the number of servers in distributed network environment is more than one, the authentication protocols are required for multi server environment are required for practical applications. With the rapid development of Internet service, more and more network architectures are used in multi server environments. This paper proposes a new efficient and secure multi server authentication scheme based on one way hash function without verification table to minimize the complexity of hash operation among all users and fit multi server communication environment. Compared with related multi server authentication schemes, the proposed scheme has strong security.Due to the presence of double authentication i.e. biometrics and user id and password.

KEYWORDS
Multi server, Authentication scheme, Smart card, one way hash function.

1. INTRODUCTION
With the rapid progress in the wireless mobile communication technologies, increasing number of services are provided through the internet instead of the traditional manner. The system providing resources to be accessed over the network often consists of many different servers through out the world. The distribution of the remote system hardware in different places makes the user access the resources more efficiently and conveniently. In 1981, Lamport [1] first proposed an authentication scheme for single server architecture in insecure networks. However, Lamport scheme require the server to maintain a verification table for remote users. So, important information can be cracked by hackers. To eliminate the security problems and reduce the communication and computation costs ,variety of single server authentication schemes using one way hash functions have been proposed .[2,3,4,5]
Recently, more and more schemes are used in multi server environments without verification tables. In such multi server network architecture, a network user must prove to the servers that he is the legitimate user before he can get any service from the various servers. In conventional password authentication schemes, each network user does not only need to log into various remote servers repetitively but also needs to remember various user id’s and passwords. This is very insecure because id’s and passwords can be leaked or hacked easily. Another problem in using the traditional remote login methods to authenticate a user is that the server often uses a verification tablet that stores user’s id and password. Therefore, the server requires extra memory space to store the verification table and these schemes will be partially or totally broken if the verification tables are stolen by adversary. Moreover, any user who wants to access different servers must repeat registration to each server and makes the scheme inefficient.
A secure and efficient remote user authentication scheme for multi server environment usually meets the following requirements [6].
1. Single Registration: User only must register at the registration center once and can use all the permitted services in eligible servers.
2. Change password securely and freely. It allows the user to change his password freely after assuring his legality.
3. Mutual authentication and Key agreement. It allows the user and the servers to authenticate one another and negotiate the session key to protect the transmitting message.
4. Low computation and communication costs. Due to the power constraints and small flash memory of smart cards, they may not provide a powerful computation capability and high bandwidth.
5. No verification table. No, verification or password table is stored in the server.
6. Security. The authentication scheme must be able to resist all kinds of attacks so that it can be applied in the real worlds.
In this paper we propose a “Biometric and user id based authentication mechanism using smart cards for multi-server environment.” This mechanism provides a new efficient and secure multi server authentication scheme based on ID and biometric using one way hash function. The proposed scheme can resist guessing attacks, replay attacks, stolen verifier attacks, server spoofing attack, registration centre spoofing attack, impersonation attack, security of session key, security of secret key, mutual authentication.
The remainder of this paper is organized as follows: Some related work is given in Section 2. The proposed scheme is presented in Section 3, while Section 4 discusses the security and efficiency of the proposed scheme. The conclusion is given in Section 5.

2. RELATED WORK
Due to the widespread applications of Internet services, the study of remote user authentication scheme for multi server environment has received considerable attention and some schemes have been proposed. Sun proposed a system where no password table is required to keep in a system for verifying the legitimacy of the login users [7]. Sun further proposed a revised version to significantly reduce the communication and computation costs[4]. In order to deal with ID-theft problems, Das proposed a dynamic ID-based remote user authentication scheme using smart cards [8]. The revised version of the Das’s scheme is provided by Chien and Chen to conquer the weakness of the protection of user’s anonymity [9]. Besides the protection of user privacy against outside attacks, Kim et al.’s effort [10] is to guarantee user privacy against a remote server and further provide traceable anonymity authentication. In addition, since a number of server providing the facilities for users is usually more than one, remote user authentication schemes used for multi server architectures, rather than single server. Li et al. [5] presented a remote password authentication scheme for multi server environments in which the password authentication system is a pattern classification system based on an artificial neural network. An efficient solution with much less computational cost and key agreement is given in Juang’s work [11]. Liao and Wang [12] indicated that a threat to user privacy is caused by the use of static ID for password authentication. Instead, a secure dynamic ID-based scheme to achieve user’s anonymity is proposed in their work. A shared secret value among servers is not secure against server spoofing attack and impersonation attack [13].

3. PROPOSED SCHEME
This section introduces the proposed multi-server authentication based on one way hash function. The proposed scheme is composed of three phases which are the server registration phase, user registration phase and authentication phase. The notations used in this paper are as follows:

- **Si**: The Server;
- **Ui**: The User;
- **RC**: The Registration Centre;
- **ID, Pwd**: Ui’s identity and password, respectively;
- **Bi**: Biometric template of Ui;
- **SIDi**: Si’s identity;
- **x**: Ui’s secret key maintained by the registration centre.

### 3.1 SERVER REGISTRATION PHASE

![Figure 1. Server Registration Phase](image)

**Step 1**: When the server Si wants to register and becomes a new legal server, Si freely chooses his identity SIDi and submits it to the registration centre through a secure channel.

\[
\text{Si} \rightarrow \text{RC} : \text{SIDi}
\]

**Step 2**: RC computes \( h(\text{SIDi} || y) \) and sends back to Si through secure channel.

\[
\text{RC} \rightarrow \text{Si} : h(\text{SIDi} || y)
\]

### 3.2 USER REGISTRATION PHASE

![Figure 2. User Registration Phase](image)

**Step 1**: When User wants to register and become a new legal user, Ui freely chooses his identity ID, password pwd, biometric template Bi and a random nonce K and submits ID,pwd,Bi ⊕ K to RC through a secure channel.

- **y**: Si’s secret key maintained by the registration centre.
- **K,N**: Random nonces;
- **h(.)**: Exclusive – or (XOR) operation;
- **| |**: Concatenation operation;
- **A → B:M**: A sends a message M to B;

Where \( h(\cdot) \) is a secure one way hash function; \( N \) is a random nonce; \( K \) is a shared secret value among servers; \( Bi \) is biometric template of the user; \( SIDi \) is the identity of the user; \( x \) is the secret kept in a system for verifying the legitimacy of the login users.
Biometric and ID Based User Authentication Mechanism Using Smart Cards for Multi-Server Environment

Ui ➔ RC: ID,pwd,Bi ⊕ K

Step 2: RC computes user authentication key M=h(ID||x) and C=M ⊕ Pwd ⊕ Bi ⊕ K.

Then, RC stores C and h(.) into smart card and issues it to user Ui through a secure channel.

RC ➔ Ui: Smart card

Step 3: Upon receiving the smart card, Ui enters K into his/her smart card.

3.3 AUTHENTICATION PHASE

After server registration phase of the proposed scheme, the following steps are then performed during the authentication phase:

Step1: When user Ui wants to login to a server Si, Ui inserts smart card into a card reader and enters his personal biometrics Bi, along with ID and Pwd. The card reader extracts M by computing C ⊕ Pwd ⊕ Bi ⊕ K, generating a random nonce NU and computes L1=h(M||NU)=h(h(ID||x)||NU). Then, Ui sends ID, NU, L1 to Si.

Ui ➔ Si: ID, NU, L1

Step 2: Upon receiving the message in Step 1, Si generates a random nonce NS and computes L2 = h(h(SIDi||y)||NS). Then, Si sends ID, NU, L1, SIDi, NS, L2 to RC.

Si ➔ RC: ID, NU, L1, SIDi, NS, L2.

Step 3: Upon receiving the message in Step 2, RC computes L1’ = h(h(ID||x)||NU) and L2’ = h(h(SIDi||y)||NS) and then checks whether L1=L1’ and L2=L2’ respectively. If they are equal, Si computes session key V = h(h(SIDi||y)||NS||NU) the ephemeral secret key W = h(h(ID||x)||NU||NS) for Ui and Si, L3 = V ⊕ W and L4 = h(V||W) . Then, RC sends L3 and L4 to Si.

RC ➔ Si: L3, L4.

Step 4: Upon receiving the message in Step 3, Si computes V’=h(h(SIDi||y)||NS||NU) and extracts the ephemeral secret key W by computing L3 ⊕ V’. Then, Si computes L4’ = h(V’||W) and checks whether L4=L4’. If they are equal, Si computes the shared session key, SK=(h(SIDi||W||NU||NS) and L5=h(W||SK). Finally, Si sends NS and L5 to user.

Si ➔ Ui: NS, C5

Step 5: After receiving the message in Step 4, Ui computes the secret key W = h(h(ID||x)||NU||NS) and the shared session key, SK = h(ID||SIDi||W||NU||NS). Then, user computes L5’=h(W||SK) and checks whether L5=L5’. If they are equal, Ui computes L6=h(W||SK||NS) and sends it to Si.

Ui ➔ Si: L6

Step 6: Upon receiving the message in step 5, Si computes L6’=h(W||Sk||NS) and checks whether L6=L6’. If they are same then Si confirms the legality of user. As a results, Ui and Si can use shared secret session key, SK=h(ID||SIDi||W||NU||NS) in private communication.

4. SECURITY ANALYSIS

In this section, security analysis of the proposed scheme is given as follows:

4.1 RESIST GUESSING ATTACKS

In the proposed scheme, the online password guessing attack will fail, since in Step 3 of Authentication Phase, RC can authenticate Ui. The offline password guessing attack the Pwd is only used for protecting the corresponding smart card, and no verifiable information is encrypted by passwords. Also, the secret value of C=M ⊕ Pwd ⊕ Bi ⊕ K is stored in Ui’s smart card. Only the legal user Ui has his / her password Pwd can extract the user authentication key M by computing C ⊕ Pwd ⊕ Bi ⊕ K and then use his / her smart card. Therefore, the proposed scheme can resist guessing attacks.

4.2 RESISTS REPLAY ATTACKS

In the proposed scheme, the replay attacks fail because the messages transmitted in the authentication phase is provided by the random nonces NC, NS and the shared session key SK and the shared secret value W, can embed the SK and W in the hashed messages L5=h(W||SK) generated by Si of Step 4 of Authentication Phase and L6=h(W||SK||NS) generated by Ui of Step 5 of Authentication phase respectively. Therefore, the proposed scheme can resist replay attacks.

4.3 RESISTS STOLEN - VERIFIER ATTACKS

In the proposed scheme Si and RC do not store any verification table, hence can resist stolen-verifier attacks.

4.4 RESISTS INSIDERS ATTACKS

Since Ui registers to RC by presenting Pwd ⊕ Bi ⊕ K. The insider of RC cannot directly obtain Pwd without knowing the value of Bi as well as random nonce K. Therefore, the proposed scheme can resist insider attacks.

4.5 RESISTS SERVER SPOOFING ATTACKS

It is impossible for an attacker to masquerade as Si to cheat Ui or RC. Because none of the servers store any user authentication key h(ID||x) in it, none of the servers can authenticate Ui. If Si wants to authenticate, Si must be authenticated by the RC first, and then obtain the user
authentication key h(ID||x) from RC. If an attacker wishes to cheat RC, they must have h(SIDi||y). Therefore, the proposed scheme can resist server spoofing attack.

4.6 RESISTS REGISTRATION CENTER SPOOFING ATTACKS
It is impossible for an attacker to masquerade as the registration center RC, because every server Si has a h(SIDi||y). Si can use h(SIDi||y) to verify the identity of RC. Therefore, the proposed scheme can resist registration centre spoofing attack.

4.7 RESISTS IMPERSONATION ATTACKS
It is impossible for an attacker to masquerade as a legal user Ui. To successfully perform an impersonation attack, the attacker requires h(ID||x) to generate authentication messages correctly. All authentication messages between Si and Ui are protected by h(ID||x). To avoid Si get h(ID||x), RC sends the ephemeral secret key W=h(h(ID||x)||NU||NS) to Si. The ephemeral secret key W is generated by the random nonce NU and NS, so this key is different in each authentication process. When an attacker obtains an ephemeral secret key to masquerade as a legal user. Therefore, the proposed scheme can resist impersonation attacks.

4.8 PROVIDES SECURITY OF SESSION KEY
A session key SK is generated from W=h(h(ID||x)||NU||NS). The parameter values are different in each session, and each is only known by Si and Ui. Whenever the communication ends between Ui and Si, the key will immediately self-destruct and will not be reused. When Ui re-enters the system, a new session key will be generated for encrypting all the messages between Si and RC. Therefore, assuming the attacker has obtained a session key, Ui will be unable to use this session key to decode the information in other communication processes. Because the random nonce NS and NU are both generated randomly, a known session key cannot be used to calculate the value of next session key. Additionally, since the value of nonce is very large, attackers cannot directly guess the value of nonce to generate the session key. Therefore, the proposed scheme provides the security of session key.

4.9 PROVIDES THE SECURITY OF EPHEMERAL SECRET KEY
The ephemeral secret key W=h(h(ID||x)||NU||NS) is used to help Si to authenticate Ui. When Ui re-enters the system, the ephemeral secret key W is regenerated during the authentication process. Therefore assuming the attacker has obtained an ephemeral secret key W by cracking Si, an attacker will be unable to use this key to authenticate Ui in other authentication processes. Because the random nonce NU is generated randomly and very large, it is impossible to use a known ephemeral secret key W to calculate the value of next ephemeral key. Therefore, the proposed scheme provides the security of the ephemeral secret key.

4.10 PROVIDES THE MUTUAL AUTHENTICATION
In the proposed scheme, the agreed session key SK is generated between Ui and Si for ith session. In step 3 of authentication phase after Rc receives the ID,NU,L1,SIDi,NS and L2 from Si, he/she two hash values L1 and L2 are correct. Since each random nonce NC and NR are hashed with the user authentication key h(ID||x) shared between Ui and RC and the server authentication key h(SIDi||y) shared between Si and RC respectively, RC will believe that the ith random nonces NC and NR was originally sent from A and B respectively. In step 4 of authentication phase, after Si receives the message L3 and L4 from RC, he/she will check of the hash value of L4 is correct. Since. Since the hashed message included the shared secret value h(SIDi||y). Si will believe L3 and L4 were originally sent from RC. In step 5 of authentication phase, after Ui receives the message NS and L5 from Si, he/ she will check if the hash value of L5 is correct. Since the hashed message include h(ID||x) and SK, Ui will believe NS and L5 was originally sent from Si. In step 6 of authentication phase after Rc receives the message L6 from Ui, he / she will check if the hash value of L6 is correct. Since the hashed message included W and SK, Ui believes L6 was originally sent from Ui. Therefore, the proposed scheme provides the mutual authentication.

4.11COMPARISON WITH OTHER SCHEMES
The security comparison between the proposed scheme and other multi server user authentication schemes are summarized in Table below:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No verification table</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Single registration</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Prevention of guessing attack</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Prevention of replay attack</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Prevention of stolen verifier attack</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Prevention of insider attack</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Prevention of server spoofing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Prevention of RC</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Prevention of impersonation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mutual authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Biometric and ID Based User Authentication Mechanism Using Smart Cards for Multi-Server Environment

<table>
<thead>
<tr>
<th>User friendly</th>
<th>Yes</th>
<th>Yes</th>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic user authentication key</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Double user authentication</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Table 1. Comparison between the proposed scheme and other schemes:

5. CONCLUSION
This paper proposed a secure and convenient double authentication i.e. biometrics and password authentication scheme with key agreement and mutual authentication. Also, this scheme is based on one way hash function without verification table to minimize the complexity of hash operation among all users and fit multi server communication environment. This proposed scheme is beneficial for different M-Commerce applications good level of security. Moreover, an integrated management environment for authentication, key agreement and authorization is required for practical applications that are proposed in the paper.

REFERENCES
Shared Information: $h(.)$

Information held by $Ui$: ID, Pwd, Smart card ($C=M\oplus Pwd\oplus Bi\oplus K,K,h(.)$).

Information held by $Si$: $(SIDi,h(SIDi||y))$.

Information held by $RC$: $x,y$.

### Authentication Phase

1. **Enter ID, Pwd, Bi**
2. **Extract $C=M\oplus Pwd\oplus Bi\oplus K$**
3. **Generate random $NU$**
4. **Compute $L1=h(M||NU)$**
5. **Generate random $NS$**
6. **Compute $L2=h(h(SIDi||y)||NS)$**
7. **Compute $L1'=h(h(ID||x)||NU)$**
8. **Compute $L2'=h(h(SIDi||y)||NS)$**
9. **Verify $L1'=L1$**
10. **Verify $L2'=L2$**
11. **Compute $V=h(h(SIDi||y)||NS||NU)$**
12. **Compute $W=h(h(ID||x)||NU||NS))$**
13. **Compute $L3=V\oplus W$**
14. **Compute $L4=h(V||W)$**
15. **Compute $V'=h(h(SIDi||y)||NS||NU)$**
16. **Extract $W=L3$**
17. **Compute $L4'=h(V'||W)$**
18. **Verify $L4'=L4$**
19. **Compute $SK=h(ID||SIDi||W||NU||NS)$**
20. **Compute $L5=h(W||SK)$**
21. **Verify $L5'=L5$**
22. **Compute $L6=h(W||SK||NS)$**
23. **Compute $L6'=h(W||SK||NS)$**
24. **Verify $L6'=L6$**

**Shared Session key between $Ui$ and $Si$: $SK=h(ID||SIDi||W||NU||NS)$**