A Secure Dynamic Authentication Scheme for Smart Card based Networks

Dr. S. Santhosh Baboo
Reader in Computer Science
D.G. Vaishnav College, Arumbakkam
Chennai-600 106, Tamilnadu, India

K. Gokulraj
Research Scholar
Centre for Research, Bharathiar University
Coimbatore-641 046, Tamilnadu, India

ABSTRACT
Authentication is one of the essential security features in network communication. Authentication process ascertains the legitimacy of the communicating partners in communication. In authentication process, the originator of the communication and the respondent transacts some identification codes of each other prior to start of the message transaction. Several methods have been proposed regarding the authentication process from time to time. Here, we introduce a new authentication scheme based on dynamicity which is relatively a different approach to ensure and enhance the smart card based remote authentication and security. This method discusses about the authentication for smart card based network systems. This method introduces a dynamic authentication scheme which includes number of factors, among them the password, password index, and date of modification are important factors which decides the dynamicity. The static approach authentication schemes are vulnerable to different types of attacks. In order to overcome the threats of the existing approaches, the dynamic authentication scheme is introduced. This scheme ensures the authentication, confidentiality, reliability, integrity and security. The security analysis of this method shows that this scheme is sustainable to the vulnerability attacks during authentication process and provides more security features in networked communications using smart cards.

Keywords
Dynamic Authentication, Smart Card, Reliability, Integrity, Network Security.

1. INTRODUCTION
Smart card based authentication scheme is to access the remote server in an emerging and essential needs in modern communication trend. The increase in network communication causes for increase of vulnerability threats. In smart card based authentication systems, vulnerability attacks quite common which causes the user to feel insecure in network communication. Hence, smart card based authentication is also an important factor in network security to be dealt with carefully. The existing access methods using smart cards are simpler methods, which are not found to be safe. A remote authentication scheme permits both the user and the server to identify the genuine transacting partners over an existing communication channel. The secret data and information could be dealt simply, securely, and conveniently by the remote authentication scheme. The remote authentication scheme plays an important role in application areas like Computer Networks, Wireless Networks, Remote Logon systems, Operating Systems, and Database Management Systems. The main aim of the remote authentication scheme is to identify and verify the authenticated smart card holder with the valid access rights and authenticated remote server. The most reliable and secure form of electronic identification of authentication is smart card based remote user authentication scheme which is widely accepted method. This scheme helps the user to interact with the remote authentication server through the distributed and portable communicating systems which emphasizes the Dynamic Authenticity, Integrity, Reliability, and Security of the transacting partners in an insecure communication channel.

2. RELATED WORK
About remote authentication scheme, number of research ideas have been suggested by the researchers from time to time. [1] proposed a password authentication scheme over an insecure communication channel in 1981. A remote password authentication scheme based on signature scheme was analyzed by [2] in 1994. A password authentication scheme with smart card was analyzed by [3] in 1999. A new remote user authentication scheme using smart cards was analyzed by [4] in 2000. [5] analyzed smart card based remote authentication scheme in 2000. [6] analyzed the security of smart cards under the threat of power analysis attack in 2002. [7] analyzed a remote authentication scheme using smart cards with forward secrecy in 2003. A modified remote user authentication scheme using smart cards was analyzed by [8] in 2003. [9] analyzed the modified remote user authentication schemes in the same year. A new remote user authentication scheme was suggested by [10] in 2004. Then, [11] proposed a remote authentication scheme based on signature scheme using smart card in 2004. [12] analyzed the security enhancement for the time-stamp based password authentication scheme using smart cards in 2004. [13] analyzed the Man-in-the-middle attack in the remote authentication scheme in 2005. [14] discussed the password authentication scheme over an insecure channel in 2006. [15] analyzed two improved password authentication schemes using smart cards in 2006. [16] proposed a novel remote user authentication scheme using bilinear pairings in 2006. A forward secure user authentication scheme was proposed by [17] in 2006. [18]

proposed an improved efficient remote user authentication schemes in 2007 to provide two-factor security. A secure and dynamic ID-based remote user authentication scheme was proposed by [19] in 2009. [20] proposed new secure user remote authentication scheme using smart cards to overcome flaws and to provide essential security requirements in 2010.

3. PROPOSED DYNAMIC AUTHENTICATION SCHEME

A secure dynamic authentication scheme is a new method of remote user authentication scheme using smart card based network systems which is introduced for enhancing the existing authentication and security in smart card based applications in network communications. Here, the factors like User Identity(UID), User Password(UPW), User Password Index(UPWI), User Date of Registration(UDR), User Date of Modification(UDM), Date of Expiry of the Smart Card(DE), Account Number(NAC), Type of Account(TAC), Bank Code(BC) are dealt. Among them User Password(UPW), User Password Index(UPWI), User Date of Modification(UDM) are the three factors which will vary dynamically for each time of user login process with the remote authentication server. This authentication scheme consists of phases namely Registration phase, Login phase, and Dynamic Authentication phase. These phases are explained as follows:

3.1 Registration Phase

In this phase, the user registers with the remote server whenever a new account is created. At the time of registration, the user account is created and the user identity is determined by the authentication server and it is stored in the smart card memory. In this scheme, the authentication server maintains the User Identity(UID), User Name(UN), User Password(UPW), User Password Index(UPWI), User Date of registration(UDR), and User Date of Modification(UDM), Date of Expiry of the Smart Card(DE), Account Number(NAC), Type of Account(TAC), and Bank Code(BC). Among them, the three important factors like User Password(UPW), User Password Index(UPWI), User Date of Modification(UDM) are dynamic factors whose values will vary for each successful login phase. Whenever, the user registers for new account, these factors and their values are intimated to the user immediately after the registration. The user will have to use these factors during login phase and authentication phase. The steps of transaction between the User and the Authentication Server are given as follows:

Step : 1 The user places the Registration Request to the Authentication Server of the Bank with the details namely User Name(UN), User Account Number(NAC), Type of Account(TAC), and the Bank Code(BC) and it is given as follows:

User Registration Request(U_N, N_{AC}, T_{AC}, B_C) **Server**

Step : 2 The remote Authentication Server computes the User Identity(UID) by taking the factors namely User Name(UN), User Account Number(NAC), Type of Account(TAC), Bank Code(BC), Date of Registration for Smart Card(DR), and Date of Expiry of the Smart Card(DE).

User Name(UN) is a string of characters which are converted into ASCII codes(CC) of each character and all these character codes are EX-ORed with one another to generate User name code(UNC) as given below:

UNC = [CCH1 $\oplus$ CCH2 $\oplus$ CCH3 $\oplus$ ….. $\oplus$ CCHn]

Step : 3 The User Name Code(UNC) is now combined along with other factors like User Account Number(NAC), Type of Account(TAC), Bank Code(BC), Date of Registration of Smart Card(DR), and Date of Expiry of the Smart Card(DE) and all these factors are EX-ORed with each other and then the User Identity(UID) is created using one-way hash function hf( ) as follows:

UID = hf(UNC $\oplus$ TAC $\oplus$ BC $\oplus$ DR $\oplus$ DE)

Step : 4 Then the Server creates the User Temporary Password(TPW), and User Temporary Password Index(TPWI) as given below:

TPW = 6 Digit Hexa-Decimal Unique Number

TPWI = 6 Digit Hexa-Decimal Index of the TPW

The Authentication Server intimates the User Identity (UID), User Temporary Password (TPW), and User Temporary Password Index(TPWI) to the user in person or over a secure communication channel. The Server writes the User Identity (UID), along with (UNC, NAC, TAC, BC, DR, DE, g, and p) factors into the Smart Card memory and it is handed over to the user in person or secure communication channel. The above steps of transactions are shown by the fig.1

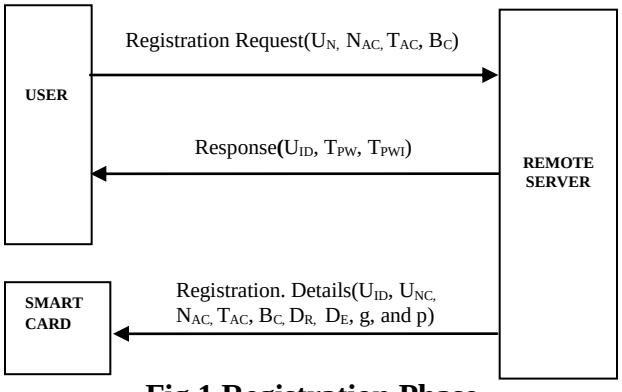

Fig.1 Registration Phase

3.2 Login Phase

In this phase, the User logon to the remote Authentication Server through the Smart Card Reader (SCR) system. When the user inserts the smart card in to the card reader machine, the machine asks the user to enter the User Identity(U_{ID}) code. The user enters the U_{ID} into the card reader machine. Then the machine compares the entered U_{ID} and the available U_{ID} in smart card memory. If both the identity values do not match, then the card reader machine rejects the login request of the user. Else, the card reader machine redirects the control to the authentication server by sending the correct user identity U_{ID}. The authentication server takes over the control for further transaction between the server and user. The transaction among the User, SCR, and Authentication Server are shown in the fig.2

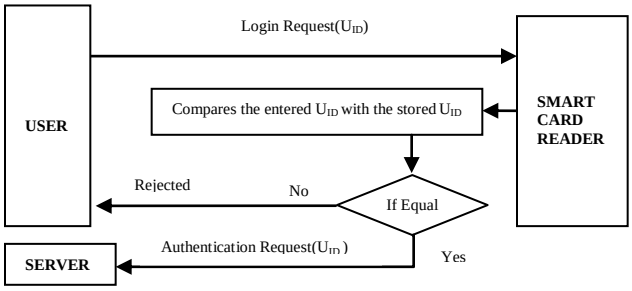

Fig.2 Login Phase

3.3 Dynamic Authentication Phase

In this phase, the server verifies for the genuine user and in turn the user verifies the authentication server. The server verifies the user identity sent by the card reader system and if both the values do not match, then server rejects the authentication request. Else, the transaction between the authentication server and the user are given as follows:

Step 1 : The server sends the server generates the tokens(t1, t2, t3, t4) using DH( ) and sends them to the user for the secret keys(sk1, sk2, sk3, sk4) respectively, which are determined by the user using the same method. In turn, the user generates user tokens(t5, t6, t7, t8) using DH( ) and sends them to the server for the secret keys(sk1, sk2, sk3, sk4) respectively, which are determined by the server using the same method.

Step 2 : The server determines the secret key sk1, computes hf($N_{AC} \oplus$ sk1) and sends this component to the user. Also, the server asks the user to enter the Temporary Password Index(T_{PWI}) initially. From next authentication phase, the server asks the user to enter User Password Index(U_{PWI}).

Step 3 : The user verifies the received Account Number(N_{AC}) with the computed Account Number(N_{AC}) using sk1 and if both the values do not match, then the user stops further transaction. Else, computes the component hf($T_{PWI} \oplus$ sk1), and sends it to the server.

Step 4 : The server verifies this received Temporary Password Index(T_{PWI}) initially, and User Password Index(U_{PWI}) from next authentication phase, with the computed Temporary Password Index(T_{PWI}) using the secret key sk1, and if both values do not match, then the server rejects the login request. Else, the server determines secret key sk2, computes the component hf($U_N \oplus$ sk2) and sends it to the user. Also, the server asks the user to enter the Temporary Password(T_{PW}) initially, and User Password(U_{PW}) from next authentication phase.

Step 5 : The user verifies the received User Name(U_N) with the computed User Name(U_N) using the secret key sk2, and if both the names do not match, then the user stops further transaction. Else, the user computes hf($U_{PW} \oplus$ sk2) and sends it to the server.

Step 6 : The server verifies the received User Password(U_{PW}) with the computed User Password (U_{PW}) using the secret key sk2, and if both the passwords do not match, then the login request is rejected. Else, the server determines the secret key sk3, computes hf($D_M \oplus$ sk3) component, and sends it to the user. Also, the server asks the user to enter the New Password Index(N_{PWI}).

Step 7 : The user verifies the received Date of Modification(D_M) with the computed (D_M) using the secret key sk3, and if both the dates do not match, then the user stops further transaction. Else, computes the Encrypted component E($N_{PWI} \oplus$ sk3), and sends it to the server.

Step 8 : The server receives and determines the New Password Index(N_{PWI}) using the secret key sk3, stores the New Password Index(N_{PWI}), determines secret key sk4, computes hf(Bc $\oplus$ sk4) component, and sends it to the user. Also, the server asks the user to enter the New Password(N_{PW}).

Step 9 : The user verifies the received Bank Code(Bc) with the computed (Bc) using the secret key sk4, and if both the codes do not match, then the user stops further transaction. Else, computes the Encrypted component E(N_{PW} $\oplus$ sk4), and sends it to the server.

Step 10 : The server receives and determines the New Password(N_{PW}) using the secret key sk4, stores the New Password (N_{PW}).

The above transactions between the Authentication Server and User are shown in fig.3

Table1. Notations

U_{ID}	User Identity
U_N	User Name
U_{NC}	User Name Code
U_{PW}	User Password
U_{PWI}	User Password Index
T_{PW}	User Temporary Password
T_{PWI}	User Temporary Password Index
N_{PWI}	User New Password Index
N_{PW}	User New Password
U_{DR}	User Date of Registration
U_{DM}	User Date of Modification
N_{AC}	User Bank Account Number
T_{AC}	User Type of Account
B_C	Bank Code
D_R	Date of Registration
D_E	Expiry Date of the smart card
C_C	Character Code of User Name
g	Common Base of DH( )
p	Prime Number of DH( )
r1, r2, r3, r4	Random Number of a Server
r5, r6, r7, r8	Random Number of a User
t1, t2, t3, t4	Tokens generated by the Server
t5, t6, t7, t8	Tokens generated by the User
sk1, sk2, sk3, sk4	Session Keys
DH( )	Diffie-Hellman Key Exchange Function
hf( )	Hash Function
E( )	Encryption Function
D( )	Decryption Function
-	Nil
CAT	Concatenation
XOR	Exclusive OR operation
SCR	Smart Card Reader

4. SECURITY ANALYSIS

4.1 Off-line Password Guessing Attack

This is a type of attack using which the intruder could guess the password in an off-line communication. If an intruder tries to guess a password to break the security, the password will not match with the guesses. Because, the password is not a static code and it is changed every time when the user logon to the authentication server. This method insists the user to change the password every time when login process is successfully completed with authentication server in order to ensure the dynamic authentication. It ensures the dynamic authentication of the proposed method. Thus, our scheme prevents the off-line password guessing attack.

4.2 Server Spoofing

It is a type of attack in which the attacker acts like the authenticated server to deceive the user. When an attacker tries to spoof the user, attacker asks the Password, Index of the Password from the user. If the user is unaware of this spoofing activity, user enters all the asked information. But, in our scheme, the server has to issue server authentication factors like the User Account Number(N_{AC}), User Name(U_N), Date of Modification(D_M), Bank Code(Bc) of the user, one after the another during the dynamic authentication phase to the user. The intruder cannot respond all these authenticated codes to the user because of the security feature using DH( ), and hf( ) along with the secret keys for each code of transaction and the attacker cannot deceive the user. Hence, server spoofing is resisted by our new dynamic authentication scheme.

4.3 Replay Attack

This attack replays the recorded security codes during the authentication phase between the user and server. When the intruder initiates the replay attack at the user side, the user easily identifies this attack by means of response from the intruder. Since the intruder cannot respond with the correct authenticated codes in replay attack to the user, this attack at user side is not possible. Similarly, When intruder initiates the replay attack at the server side, the attacker has to respond with the User Password(UPW) and User Password Index(UPWI) to the server. Since the user password and its index value dynamically vary for each login phase, all these security codes cannot be responded by the attacker to the server by means of replay attack. Since, the replay information contains the lapsed password, and password index. This is not accepted by the server. So, this method does not permit the replay attack.

4.4 Modification Attack

This attack causes to modify the contents of the authentication code by the attacker. If an attacker tries to modify the contents of the security code, the modification causes for lot of changes due to hf( ) in the received information at the server, and the server will easily identify these changes by comparing the received code with the computed code. Because, whenever the server receives security code, it re-computes the same using hf( ) with the

available data in its table to verify the originality of the received authentication codes. If the computed code and the received code do not agree with each other, the server rejects the login request. Thus, the modification attack is prevented by this method.

4.5 Bucket Brigade Attack

This attack is also known as Man-in-the-Middle attack. In this type of attack, the attacker intercepts the authentication code transaction between the user and the authenticated server. Due to this interception, the attacker may change the entire content of the intercepted code and this code may be retransmitted to the another side of the transaction either at the user or server side. But, anywhere if the intercepted data is altered and retransmitted to the another side of the communicating systems, it is easily identified by the receiving systems by means of re-computation using hf( ) and comparison of the received code with the computed code. It ensures the confidentiality of the authentication system. So, our scheme prevents the bucket brigade attack.

4.6 Forward Secrecy

It ensures the protection of the password and its index value even when the secret key is revealed or stolen. In our scheme, the secret keys are sk1 to sk4. If any of these secret keys are stolen by the attacker, the authentication of the system is not affected. Since, using the stolen secret keys the attacker cannot determine the other authentication codes like User Password (U_{PW}) and User Password Index (U_{PWI}). Besides which, the password and its index values are dynamically changed during each login phase with the authentication server. So, the secret keys stolen are in no way affect the authentication process. Hence, our scheme maintains the forward secrecy.

4.7 Denial of Service Attack

It is an attack by which the required service by the user from the authenticated server is denied by the attacker at the initial or intermittent level of transaction. This scheme does not permit denial of service. Because, the adversary cannot make false attempt of the legitimate user to the authentication server. Even if any false attempt of the legal user is made, the server rejects the login request of that particular session. The future login attempts of the legitimate user are not affected by any of the false attempt made by the attacker. This causes for ensuring the reliability of the proposed method. So, our scheme is free from denial of service attack.

4.8 Mutual Authentication

This is a type of authentication in which both the user and the remote authentication server verify themselves for their legitimate access and authenticity. When the user enters the password index(U_{PWI}) and password(U_{PW}) one after the another, in turn, the server has to respond with User Account Number(N_{AC}), User Name (U_N), User Account Type(T_{AC}), User Bank Code(B_C). It is not possible to the attacker to provide all the mentioned response authentication codes to the user. The attacker cannot determine all these authentication codes. Thus, our scheme adopts mutual authentication to overcome the unknown attacks and for ensuring the security features.

4.9 Smart Card Loss Attack

This attack is possible only when the smart card is lost or stolen. When the smart card is lost, the adversary may misuse the card for masquerading the remote server. If any attempt is made like this, the adversary has to enter the correct User Password(U_{PW}) and Password Index(U_{PWI}) values to the remote authentication server. These code values are not known to the adversary and these values cannot be determined by the adversary. It ensures the integrity of the authentication system. So, our scheme prevents this attack though the smart card is lost or stolen and misused.

4.10 Smart Card Duplication Attack

When the original smart card is lost or stolen, it may be possible to duplicate the original card by the eavesdropper for further login process. Though the card is duplicated, unless otherwise the eavesdropper knows the User Password(U_{PW}) and Password Index(U_{PWI}) value of the legitimate user, the eavesdropper cannot login to the remote authentication server. It ensures the security of the authentication system. Thus, our scheme prevents the smart card duplication attack.

5. DISCUSSION

Table-2 shows that Juang scheme performs 5 hash functions, 4 exponentiation and 6 symmetric encryption operations, totally 15 computations. Lee *et al*. scheme performs 5 hash functions. Yoon *et al.* Scheme performs 10 hash functions and 4 exponentiation operations, totally 14 computations. Wang *et al*. scheme performs 14 Hash functions, 8 XOR operations, 4 exponentiation, and 10 concatenation operations, totally 36 computations. Tian *et al*. scheme performs 15 Hash and 5 XOR operations, totally 20 computations along with that the security feature is ensured. Manoj scheme performs 9 Hash, 12 XOR, and 2 Concatenation operations, totally 23 computations along with that security feature is provided. But, our proposed scheme performs 6 Hash functions, 12 XOR operations, and 2 encryption operations, totally 20 computations. In addition to that, our scheme provides Dynamic Authentication, Confidentiality, Reliability, Integrity, and Security. So, our scheme provides more security features than the other compared smart card based authentication schemes.

6. CONCLUSION

This article introduced a new authentication scheme called Secure and Dynamic Authentication Scheme for Smart Card based Network Systems to enhance the Authentication and to introduce security features like Confidentiality, Reliability, Integrity and Security during the authentication process. The security analysis shows that our scheme overcomes all the discussed security attacks or threats because of the dynamicity in

authentication codes. The table of comparison shows that our scheme provides Dynamic Authentication and more security features. This scheme is a well secured scheme for smart card based authentication in networking systems.

7. REFERENCES

[1] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol.24, pp. 770-772, Nov. 1981.

[2] C. C. Chang and W. Y. Liao, "A remote password authentication scheme based upon ElGamal's signature scheme," Computer &Security, vol. 13, no. 2, pp. 137-144, 1994.

[3] W. H. Yang and S. P. Shieh, "Password authentication schemes with smart cards," Computers & Security , vol. 18, no. 8, pp. 727-733, 1999.

[4] M. S. Hwang, and L. H. Li, "A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 46, no. 1, pp 28-30, Feb. 2000.

[5] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using Smart cards," IEEE Transactions on Consumer Electronics, vol. 46, no. 4, pp. 992-993, Nov.2000.

[6] T. S. Messerges, E. A. Dabbish, and .H. Sloan, "Examining smart card security under the threat of power analysis attacks," IEEE Transactions on Computers, vol. 51, no. 5, pp. 541-552, 2002.

[7] A. K. Awasthi and S. Lal, "A remote user authentication scheme using smarts cards with forward secrecy", IEEE Transactions on Consumer Electronic, vol. 49, no. 4, pp.1246-1248, 2003.

[8] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication Scheme using smart cards", IEEE Transactions on Consumer Electronics, vol.49, no.2, pp. 414-416, May 2003.

[9] K. C. Leung, L. M. Cheng, Anthony S. Fong, and C. K. Chan, "Cryptanalysis of a modified remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 49, no. 4, pp. 1243-1245, Nov. 2003.

[10] K. Manoj, "New remote user authentication scheme with smart cards," IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 597-600, 2004.

[11] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "Efficient remote user authentication scheme based on generalized ElGamal signature scheme," IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 568-570, May 2004

[12] C. C. Yang, H. W. Yang, and R. C. Wang, "Cryptanalysis of security enhancement for the timestamp-based password authentication scheme using smart cards", IEEE Transactions on Consumer Electronics , vol. 50, no. 2, pp. 578-579, May 2004.

[13] C. Y. Yang, C. C. Lee, and S. Y. Hsiao, "Man-in-the-middle attack on the authentication of the user from the remote autonomous object", International Journal of Network Security, vol. 1, no. 2, pp. 81-83, 2005.

[14] I. E. Liao, C. C. Lee, and M. S. Hwang, "A password authentication scheme over insecure Networks", Journal of Computer and System Sciences, vol. 72, no.4, pp. 727-740, 2006.

[15] R. C. Wang and C. C. Yang, "Cryptanalysis of two improved password authentication schemes using smart cards", International Journal of Network Security, vol. 3, no. 3, pp. 283-285, Nov.2006.

[16] M. L. Das, A. Saxena, V. P. Gulati and D. B. Phatak, "A novel remote user authentication Scheme Using bilinear pairings", Computers and Security, vol. 25, no. 3, pp. 184-189, 2006.

[17] B. Wang and Z. Q. Li, "A Forward-Secure User Authentication Scheme with Smart Cards", International Journal of Network Security, vol. 3, no. 2, pp. 116-119, Sep. 2006.

[18] Xiaojian Tian, Robert W.Zhu, and Duncan S. Wong, "Improved Efficient Remote User Authentication Schemes", International Journal of Network Security, Vol.4, No.2, pp.149-154, Mar.2007.

[19] Y. Y. Wang, J. Y. Liu, F. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme", Computer Communications, vol. 32, no. 4, pp. 583-585, 2009.

[20] M. Kumar, "A New Secure Remote User Authentication Scheme with Smart Cards," International Journal of Network Security, vol. 11, no. 2, pp. 88-93, 2010.

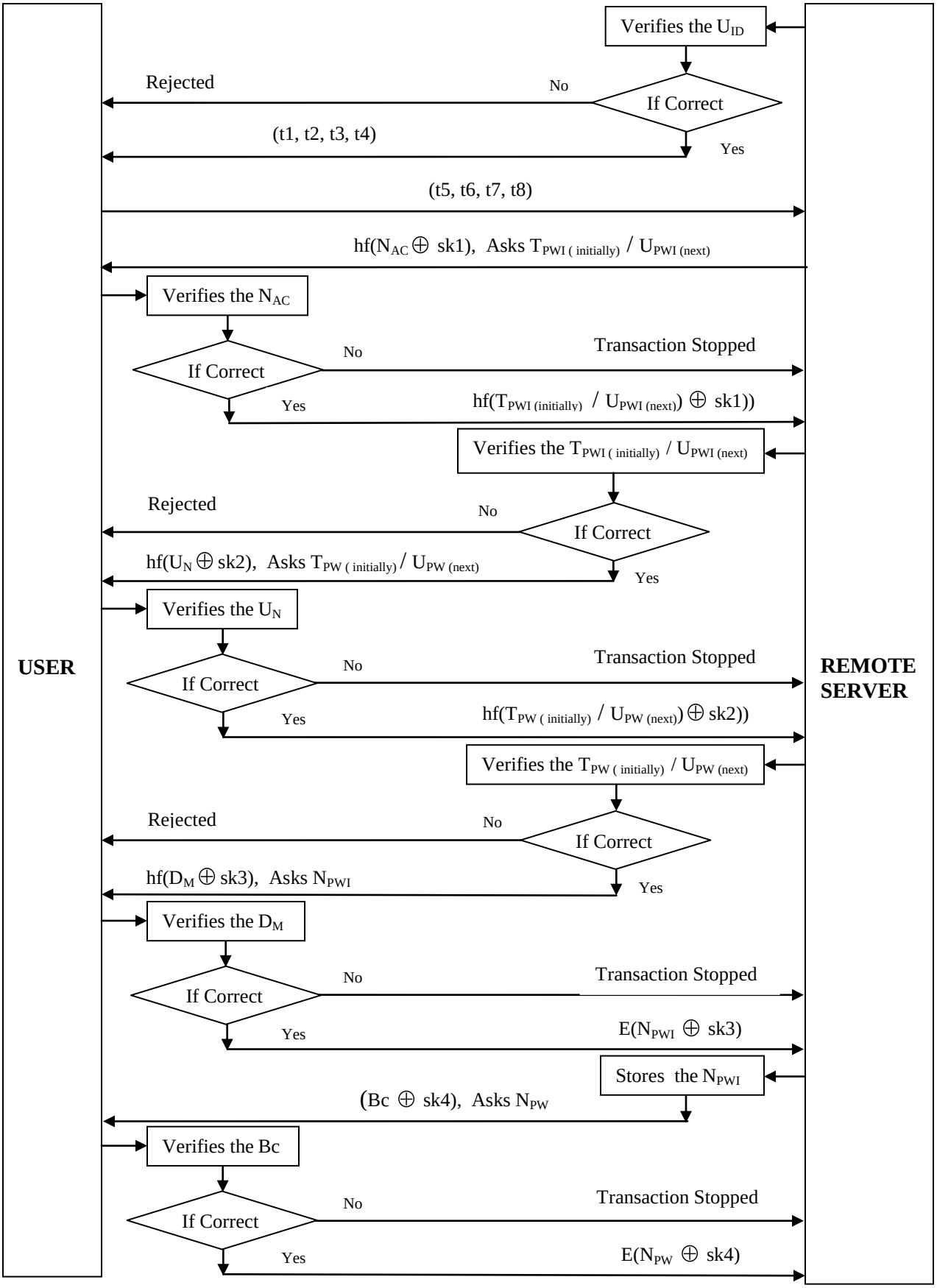

Fig.3 Dynamic Authentication Phase

Table – 2 Comparison of different smart card authentication schemes

Methods, Operations, and Security	**Juang Scheme**	**Lee *et al.* Scheme**	**Yoon *et al.* Scheme**	**Wang *et al.* Scheme**	**Tian *et al.* Scheme**	**Manoj Scheme**	**The Proposed Scheme**
Methods	Hash	Hash	Hash	Hash	Hash	Hash	Hash, DH
Operations	HF,EXP,ENC	HF	HF, EXP	HF,EXP,XOR,CAT	HF, XOR	HF, XOR, CAT	HF, XOR, ENC
No. of Hash Computations	5	5	10	14	15	9	6
No. of XOR Computations	-	-	-	8	5	12	12
No. of Exponentiation	4	-	4	4	-	-	-
No. of Concatenation	-	-	-	10	-	2	-
Symmetric Encryption	6	-	-	-	-	-	2
Dynamic Authentication	-	-	-	-	-	-	Applicable
Confidentiality	-	-	-	-	-	-	Applicable
Reliability	-	-	-	-	-	-	Applicable
Integrity	-	-	-	-	-	-	Applicable
Security	-	-	-	-	Applicable	Applicable	Applicable