I. J. Computer Network and Information Security, 2012, 4, 30-38
Published Online May 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.04.04

An Enhanced Dynamic Mutual Authentication Scheme for Smart Card Based Networks

Dr. S. Santhosh Baboo
Assistant Professor, Department of Computer Science, D.G. Vaishnav College, Arumbakkam, Chennai-600 106, Tamilnadu. India. E-mail: santhos2001@sify.com

K. Gokulraj
Research Scholar, Centre for Research, Bharathiar University, Coimbatore-641 046, Tamilnadu. India. E-mail: gokulrajk@yahoo.co.in

***Abstract*—**Network security is the prevailing and challenging factor in computer communications. Computer security and communication security are interrelated and essential features in the internetworking system. Network security is ascertained by many factors like authentication, authorization, digital signatures, cryptography, steganography etc. Among them authentication is playing an important role in networked communications, where the communicating partners are to be identified each other legitimately. Authentication process ensures the legitimacy of the communicating partners in networked communication. In an authentication process, the originator of the communication and the respondent transact some identification codes to each other, prior to start of the message transaction. Several methods have been proposed regarding the authentication process for computer communication and smart card based networks from time to time. We introduced a new scheme to enhance and ensure the remote authentication through secure and dynamic authentication using a smart card, which is relatively a different approach. This scheme discusses the authentication procedure for smart card based network systems. This article introduces a dynamic authentication scheme, which includes a number of factors, among them the password, password index, and date of modification are important factors, which decide the dynamicity in authentication. The static approach authentication schemes are vulnerable to different types of attacks in networked communication. This dynamic authentication scheme ensures the authentication, confidentiality, reliability, integrity and security in network communications. This article discusses the implementation of this scheme and to analyze the security and performance factors to ensure the dynamic mutual authentication and to enhance the security features in authentication for smart card based networks.

***Index Terms*—**Dynamic Mutual Authentication, Smart Card, Confidentiality, Reliability, Integrity, Network Security.

I. INTRODUCTION

Smart card based authentication scheme is a mechanism, which is used to access the remote server using electronic smart cards. Smart card based network communications are prevailing in the internetworking domain and it is an emerging and essential approach in modern networked communications. The increase in network communication causes for the increase of communication threats. In smart card based authentication systems, vulnerability attacks arise from unknown resources, which cause the user to feel insecure in computer network communications [27]. The existing authentication methods using smart cards are not reliable beyond a certain extent. A remote authentication scheme allows both the user and the server to identify the genuine transacting partners over an existing network communication channel [25]. The secret data and information could be transacted 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, and Mobile Networks. The main aim of the remote authentication scheme is to identify and verify the authenticated smart card holder and to identify the authenticated remote server [26]. The most reliable and secure form of electronic identification of genuine communicating partners is a smart card based remote authentication scheme which is widely accepted method. This scheme helps both the user and the remote server to identify the communicating partners and to interact themselves through the computer networked communicating systems. The proposed scheme emphasizes the Dynamic Mutual Authenticity, Confidentiality, Integrity, Reliability, and Security between the communicating partners over an insecure communication channel. The entire content of this paper is organized as follows: The review of literature has been discussed in the section-II, the proposed dynamic mutual authentication scheme has been discussed in the section-III, implementation of the proposed authentication scheme has been discussed in the section-IV, security and performance analysis of

the implemented authentication scheme has been discussed in the section-V, and the conclusion arrived from this implemented work has been discussed in the section-VI

II. RELATED WORKS

The researchers and academicians have proposed Numbers of research ideas about the remote authentication schemes from time to time. A password authentication scheme with the insecure communication channel was proposed by [1] in 1981. A remote password authentication scheme based on ElGamal's signature scheme was analyzed by [2] in 1994. Password authentication schemes with smart cards was analyzed by [3] in 1999. A new remote user authentication scheme using smart cards was proposed by [4] in 2000. The Cryptanalysis of a remote user authentication scheme using Smart cards was analyzed by [5] in 2000. Examining smart card security under the threat of power analysis attacks was analyzed by [6] in 2002. A remote authentication scheme using smart cards with forward secrecy was analyzed by [7] in 2003. A modified remote user authentication scheme using smart cards was analyzed by [8] in 2003. The Cryptanalysis of a modified remote user authentication scheme using smart cards was discussed by [9] in 2003. A New remote user authentication scheme with smart cards was suggested by [10] in 2004. An Efficient remote user authentication scheme based on the generalized ElGamal signature scheme was proposed by [11] in 2004. The Cryptanalysis of security enhancement for the timestamp-based password authentication scheme using smart cards was discussed by [12] in 2004. An Efficient password authenticated key agreement using smart card was proposed by [13] in 2004. The Man-in-the-middle attack on the authentication of the user from the remote autonomous object was analyzed by [14] in 2005. A password authentication scheme over insecure Networks was analyzed by [15] in 2006. The Cryptanalysis of two improved password authentication schemes using smart cards was discussed by [16] in 2006. A novel remote user authentication scheme using bilinear pairings was suggested by [17] in 2006. A Remote password authentication scheme with smart cards and biometrics was analyzed by [18] in 2006. An efficient and complete remote user authentication scheme using smart cards was proposed by [19] in 2006. A forward secure user authentication scheme with Smart Cards was analyzed by [20] in 2006. An improved efficient remote user authentication scheme was proposed by [21] in 2007. The Two-factor mutual authentication based on smart cards and passwords was analyzed by [22] in 2008. A more efficient and secure dynamic ID-based remote user authentication scheme was proposed by [23] in 2009. A Variant-based Biometric Authentication Scheme Based on Rotor Machine for Home Security was analyzed by [24] in 2009 to avoid the fingerprint template stolen and to immune network attacks for smart home applications through security, in which the user encrypts and alters the biometric template arbitrarily. A Multifactor Hash Digest Challenge-Response Authentication Scheme for Session Initiation Protocol was proposed by [25] in 2010. A New Secure Remote User Authentication Scheme with Smart Cards was proposed by [26] in 2010 to overcome flaws and to provide essential security requirements. A Secure Dynamic Authentication Scheme for Smart Card based Networks was proposed by [27] in 2010 to overcome the possible network security threats and to ensure the authentication, confidentiality, reliability, integrity, and security using dynamic authentication scheme.

III. PROPOSED DYNAMIC MUTUAL AUTHENTICATION SCHEME

A secure dynamic authentication scheme is a new method of remote user authentication and server authentication scheme for smart card based network systems, which is introduced for enhancing the authentication, and security features in existing smart card based applications in network communications. In this scheme, the factors like User Identity (U_{ID}), User Password (U_{PW}), User Password Index (U_{PWI}), User Date of Registration (U_{DR}), User Date of Modification (U_{DM}), Date of Expiry of the Smart Card (D_E), Account Number (N_{AC}), Type of Account (T_{AC}), and Bank Code (B_C) are taken as important factors to strengthen the authentication scheme. Among them, User Password(U_{PW}), User Password Index(U_{PWI}), User Date of Modification(U_{DM}) are the three factors which will vary dynamically for each time of successful user login process with the remote authentication server to ensure the dynamic authentication. The notations used in this authentication scheme are shown in Table-1. This authentication scheme consists of phases namely Registration phase, Login phase, and Dynamic Mutual Authentication phase. These phases are discussed as follows:

A. Registration Phase

In this phase, the user registers with the remote server based on the manual account created details, when a new account is to be created for electronic networked communications are required. 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 (U_{ID}), User Name (U_N), User Password (U_{PW}), User Password Index (U_{PWI}), User Date of registration (U_{DR}), and User Date of Modification (U_{DM}), Date of Expiry of the Smart Card (D_E), Account Number (N_{AC}), Type of Account (T_{AC}), and the Bank Code (B_C). Among them, the three important factors like User Password (U_{PW}), User Password Index (U_{PWI}), and User Date of Modification (U_{DM}) are dynamic factors whose values

will vary for each successful login phase. Whenever, the user registers to create a new account for electronic transactions, the above said factors and their values are intimated to the user by the server immediately after the successful registration phase. The user will have to use these factors during the login phase and dynamic mutual authentication phase. The steps of transaction between the User and the remote Authentication Server are discussed as follows:

Step 1: The user places the Registration Request to the Authentication Server of a Bank with the details namely User Name (U_N), User Account Number (N_{AC}), Type of Account (T_{AC}), and the Bank Code (B_C) as:

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

Table-1 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	Secret Keys
DH( )	Diffie-Hellman Key Exchange Function
hf( )	Hash Function
E( )	Encryption Function
D( )	Decryption Function
-	Nil
XOR	Exclusive OR operation
SCR	Smart Card Reader

Step 2: The remote Authentication Server computes the User Identity (U_{ID}) by taking the factors namely User Name (U_N), User Account Number (N_{AC}), Type of Account (T_{AC}), Bank Code (B_C), Date of Registration of the Smart Card (D_R), and Date of Expiry of the Smart Card (D_E). User Name (U_N) is a string of characters, which are converted into ASCII codes (C_C) of each character and all these character codes are EX-ORed with one another to generate the User name code (U_{NC}) which is given as:

$$U_{NC} = [C_{CH1} \oplus C_{CH2} \oplus C_{CH3} \oplus \ldots \oplus C_{CHn}]$$

Step 3: The User Name Code (U_{NC}) is now combined along with other factors like User Account Number (N_{AC}), Type of Account (T_{AC}), Bank Code (B_C), Date of Registration of the Smart Card (D_R), and Date of Expiry of the Smart Card (D_E). All these factors are EX-ORed with each other and then the User Identity (U_{ID}) is created using one-way hash function hf( ) as given below:

$$U_{ID} = hf(U_{NC} \oplus N_{AC} \oplus T_{AC} \oplus B_C \oplus D_R \oplus D_E)$$

Step 4: Then the Server creates the User Temporary Password (T_{PW}), and User Temporary Password Index (T_{PWI}) as given below:

T_{PW} = 6 Digit Unique Number
T_{PWI} = 6 Digit Index of the T_{PW}

The Authentication Server intimates the User Identity (U_{ID}), User Temporary Password (T_{PW}), and User Temporary Password Index (T_{PWI}) to the user in person or over a secure communication channel. The Server writes the User Identity (U_{ID}), along with U_{NC}, N_{AC}, T_{AC}, B_C, D_R, D_E, g, and p factors into the Smart Card memory, and then it is handed over to the user in person or secure communication channel. The above steps of transactions are shown in the Fig.1.

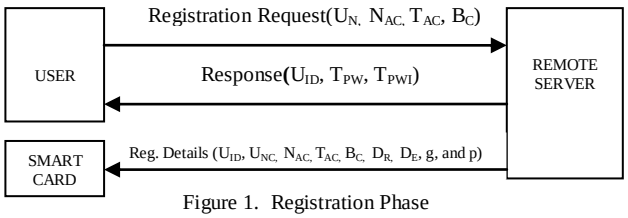

Figure 1. Registration Phase

B. Login Phase

In this phase, the User logon with the remote Authentication Server through the Smart Card Reader (SCR) system. When the user inserts the smart card into 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 using smart card. Then the machine compares the entered U_{ID} and the available U_{ID} from the database. 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 steps of authentication between the

server and the user. The authentications steps among the User, the Smart Card Reader (SCR), and the Authentication Server are shown in the Fig.2.

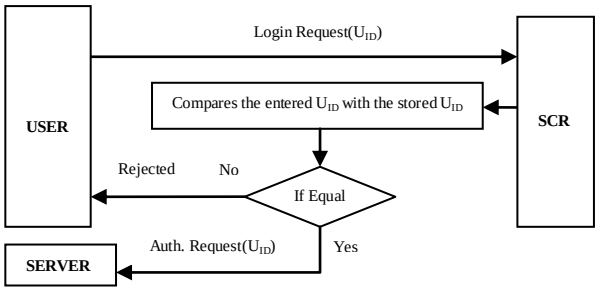

Figure 2. Login Phase

C. Dynamic Mutual Authentication Phase

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

Step 1: The server generates the server tokens as (t1, t2, t3, t4) and sends them to the user using Diffie-Hellman key exchange method DH( ) to determine the secret keys (sk1, sk2, sk3, sk4) respectively, by the user using the same DH( ) method. In turn, the user generates user tokens as (t5, t6, t7, t8) and sends them to the server using DH( ) method to determine the secret keys (sk1, sk2, sk3, sk4) respectively, by the server using the same DH( ) method.

Step 2: The server determines the secret key sk1, computes the component $hf(N_{AC} \oplus sk1)$, and sends this component to the user. In addition, 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 new 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 rejects this step and stops further steps of authentication. Else, the user computes the component $hf(T_{PWI} \oplus sk1)$, and sends it to the server.

Step 4: The server verifies the received Temporary Password Index (T_{PWI}) initially, and User new Password Index (U_{PWI}) from next authentication phase, with the computed Temporary Password Index (T_{PWI}) initially, and User Password Index (U_{PWI}) from next authentication phase using the secret key sk1, and if both the values do not match, then the server rejects this step and stops further steps of authentication. Else, the server determines secret key sk2, computes the component $hf(U_N \oplus sk2)$, and sends it to the user. In addition, the server asks the user to enter the Temporary Password (T_{PW}) initially, and User new 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 rejects this step and stops further steps of authentication. Else, the user computes the component $hf(U_{PW} \oplus sk2)$, 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 server rejects this step and stops further steps of authentication. Else, the server determines the secret key sk3, computes the component $hf(D_M \oplus sk3)$, and sends it to the user. In addition, the server asks the user to enter the New Password Index (N_{PWI}).

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

Step 8: The server decrypts and determines the New Password Index (N_{PWI}) using the secret key sk3, stores the New Password Index (N_{PWI}) in its database, determines secret key sk4, computes the component $hf(B_C \oplus sk4)$, and sends it to the user. In addition, the server asks the user to enter the New Password (N_{PW}).

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

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

The above steps of authentication between the Server and User are shown in Fig.3

IV. IMPLEMENTATION

The proposed work has been implemented using Java with MS-Access as the backend on Windows Platform with the Hardware and Software Configurations used as follows: The Hardware configuration used in this implementation work are:

The Intel Intel(R) Core(TM) 2 E7500 Processor with the operating frequency 2.93 GHz, the Main Memory used is 1.96 GB RAM with 2.93GHz frequency, and the SATA 500 GB Hard Disk Drive. The software configurations used are: 32-Bit Microsoft® Windows XP Operating System, the Java is used as Front End, and the Microsoft-Access 2007 is used as backend. Each step of the implemented result has been verified with the above said steps of authentication, and all the steps of the implemented dynamic mutual authentication scheme perform the mentioned operations effectively.

V. ANALYSIS AND DISCUSSION

A. Security Analysis

The types of security threats overcome by this dynamic mutual authentication scheme are given as follows:

1) Off-line Password Guessing Attack
2) Server Spoofing Attack
3) Replay Attack
4) Modification Attack
5) Bucket Brigade Attack
6) Forward Secrecy Attack
7) Denial of Service Attack
8) Mutual Authentication Attack
9) Smart Card Loss Attack
10) Smart Card Duplication Attack

B. Performance Analysis

Table-2 shows the different smart card authentication schemes and the Methods, Operations, and the Security features adopted by these schemes. This table shows that the Juang [13] scheme uses Hash method, and performs 1 XOR operation, 4 Exponentiation operations, 5 Hash functions, 3 Encryption operations, and 3 Decryption operations, totally 15 computations. The Ping Wang *et al.* [24] Scheme uses Hash method, and performs 4 Exponentiation operations, 2 Hash functions, 4 Encryption operations, and 4 Decryption operations, totally 14 computations. The Fan *et al.* [18] Scheme uses Hash method, and performs 3 XOR operations, 1 Exponentiation operation, 4 Hash functions, 3 Encryption operations, and 4 Decryption operations, totally 15 computations. The Liaw et al. [19] Scheme uses Hash method, and performs 2 XOR operations, 4 Exponentiation operations, 2 Hash functions, and 6 Encryption operations, totally 14 computations. The Proposed Scheme uses Hash and Diffie-Hellman key exchange methods, and performs 12 XOR operations, 6 Hash functions, 2 Encryption operations, and 2 Decryption operations, totally 22 computations. In addition to that, the proposed scheme provides Dynamic Authentication, Confidentiality, Reliability, Integrity, and Security in authentication steps. Therefore, the proposed scheme provides more security features than the other discussed authentication schemes for smart card based networks. The above table of information is shown in the Fig.4.

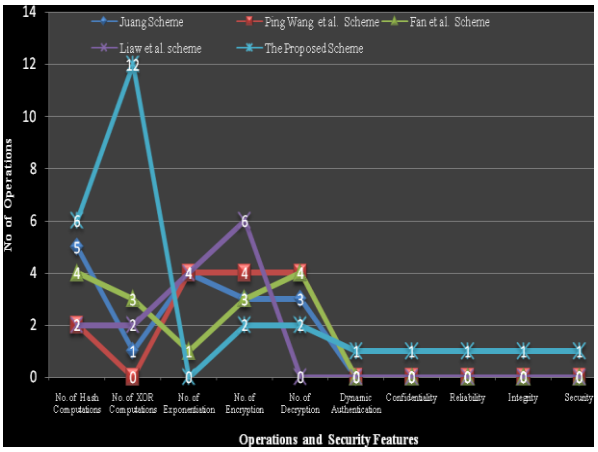

Figure 4. Analytical Graph of Various Smart Card Authentication Schemes

Table-3 shows the processing time(in nano seconds) for various operations performed based on the hardware and software configurations used for implementing this dynamic authentication scheme. This table shows that, the average processing time for XOR operation is 16062.625(ns), the average processing time for Exponentiation operation is 25312.375(ns), the average processing time for Hash function is 638665.8333(ns), the average processing time for the Encryption operation is 5091263(ns), and the average processing time for Decryption operation is 8306123(ns). From this table it is to be noted that the XOR operation consumes the minimum time 16062.625(ns) when compared to all the other operations. The above table of information is shown in the Fig.5.

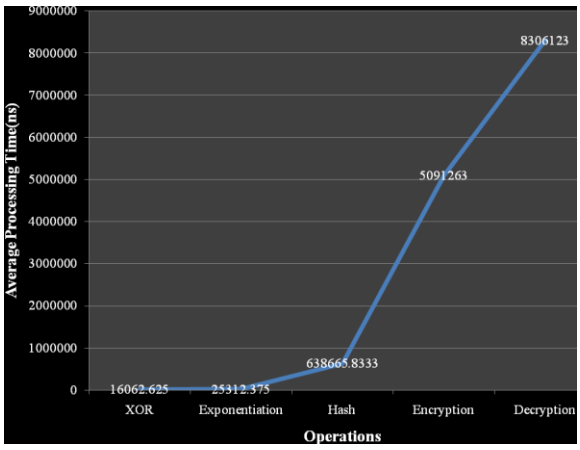

Figure 5. Processing Time For Various Operations

Table-4 shows the Methods, Operations and the Total Processing Time(in nano seconds) for different Smart Card authentication schemes along with the proposed dynamic authentication scheme based on the

hardware and software configurations used in the implementation of this authentication scheme. This table shows that the total processing time of the Juang [13] Scheme is 43502799.29(ns), the total processing time of the Ping Wang *et al.* [24] scheme is 54968125.17(ns), the total processing time of the Fan *et al.* [18] Scheme is 51126444.58(ns), the total processing time of the Liaw et al. [19] Scheme is 31958284.42(ns), and the total processing time of the proposed scheme is 30819518.5(ns). From this table, it is to be noted that the Proposed Scheme processing time is comparatively much lesser than the other mentioned smart card authentication schemes. Therefore, the efficiency of this proposed scheme is much better than the other discussed authentication schemes. The above table information is shown in Fig.6.

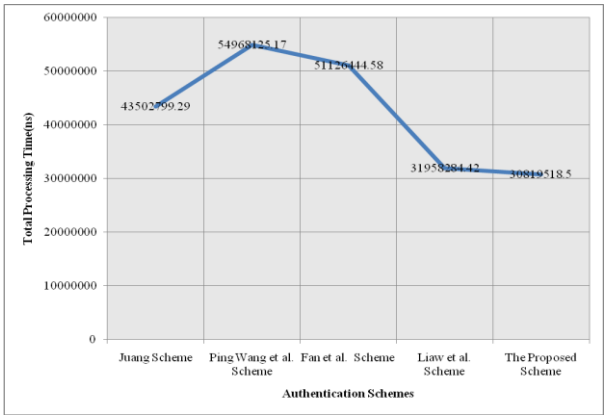

Figure 6. Smart Card Authentication Schemes and Their Total Processing Time

Table-5 shows that the proposed scheme Total Processing time differs from Juang [13] Scheme by 12683281(ns), 24148607(ns) when compared with Ping Wang *et al.* [24] scheme, 20306926(ns) when compared with the Fan *et al.* [18] Scheme, and 1138766(ns) when compared with Liaw et al. [19] Scheme respectively.

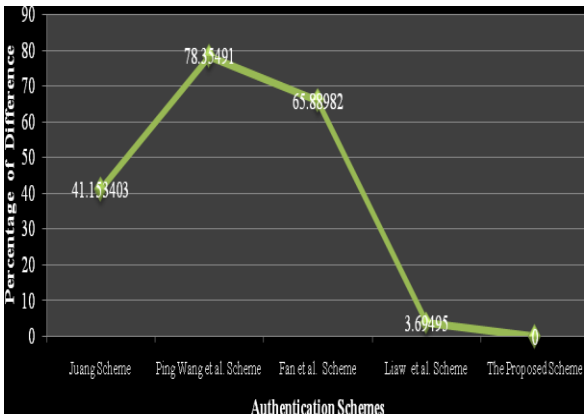

Figure 7. Percentage of Difference in Processing Time of Smart Card Authentication Schemes

Fig.7 shows that the proposed authentication scheme performs better than the Juang [13] Scheme by 41.153403%, 78.35491% than the Ping Wang *et al.* [24] Scheme, 65.88982% than the Fan *et al.* [18] Scheme, and 3.69495% than the Liaw et al. [19] Scheme respectively in terms of Total Processing Time. This shows that the proposed scheme consumes less processing time, when compared with the other mentioned authentication schemes. Therefore, the proposed authentication scheme performs much better than the other compared and discussed smart card authentication schemes.

VI. CONCLUSION

This article discussed the Enhanced Dynamic Mutual Authentication Scheme with different smart card based authentication schemes. This scheme enhances the Dynamic Authentication and security features like Confidentiality, Reliability, Integrity and Security during the authentication process in Computer Network Communications using Smart Card. This authentication scheme has been implemented and each step of the implemented result has been verified with the discussed dynamic authentication steps. The security analysis shows that the proposed scheme provides more security features and overcomes all the discussed security attacks or threats because of the dynamicity in authentication steps. The performance analysis shows that the proposed scheme takes much less computation time than the other discussed smart card authentication schemes. Due to these features, the proposed scheme is a well-secured scheme for smart card based dynamic mutual authentication in computer network communications.

REFERENCES

[1] L. Lamport, "Password authentication with insecure communication", Communications of the ACM, Vol. 24, pp. 770-772, 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, 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, 2000.

[6] T. S. Messerges, E. A. Dabbish, and R. 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 smart cards with forward secrecy", IEEE Transactions on Consumer Electronics, 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, 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, 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, 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, 2004.

[13] W. S. Juang, "Efficient password authenticated key agreement using smart card", Computer & Security, 23, pp. 167–173, 2004.

[14] 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.

[15] 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.

[16] 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, 2006.

[17] 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.

[18] C. I. Fan, Y. H. Lin and R. H. Hsu, "Remote password authentication scheme with smartcards and biometrics", IEEE GlobalTelecommunications Conf., 1-5, 2006.

[19] H.T. Liaw, J.F. Lin, W.C. Wu, "An efficient and complete remote user authentication scheme using smart cards", Mathematical and Computer Modeling, vol. 44, pp. 223– 228, 2006.

[20] 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, 2006.

[21] 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, 2007.

[22] G. Yang, D.S. Wong, H. Wang, X. Deng, "Two-factor mutual authentication based on smart cards and passwords", Journal of Computer and System Sciences, Vol. 74, No. 7, pp. 1160- 1172, 2008.

[23] 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.

[24] Ping Wang and Chih-Chiang Ku, "A Variant-based Biometric Authentication Scheme Based on Rotor Machine for Home Security", Journal of Medical and Biological Engineering, Vol. 29(5), pp. 272-275, 2009.

[25] S. Santhosh Baboo and K. Gokulraj, "A Multifactor Hash Digest Challenge-Response Authentication Scheme for Session Initiation Protocol", Journal of Network Protocols and Algorithms, Vol. 2, No.4, P.30-39, 2010.

[26] 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.

[27] S. Santhosh Baboo and K. Gokulraj, "A Secure Dynamic Authentication Scheme for Smart Card based Networks", International Journal of Computer Applications, Vol. 11, No.8, pp. 5-12, 2010.

Table-2 Methods, Operations, and Security Features Used by Different Smart Card Authentication Schemes

Methods, Operations, and Security	Juang Scheme	Ping Wang *et al.* Scheme	Fan *et al.* Scheme	Liaw *et al.* Scheme	The Proposed Scheme
Methods	Hash	Hash	Hash	Hash	Hash, DH
Operations	HF, XOR, EXP, ENC, DEC	HF, EXP, ENC, DEC	HF, XOR, EXP, ENC, DEC	HF, XOR, EXP, ENC	HF, XOR, ENC, DEC
No. of XOR Computations	1	-	3	2	12
No. of Exponentiation	4	4	1	4	-
No. of Hash Computations	5	2	4	2	6
No. of Encryption	3	4	3	6	2
No. of Decryption	3	4	4	-	2
Dynamic Authentication	-	-	-	-	Applicable
Confidentiality	-	-	-	-	Applicable
Reliability	-	-	-	-	Applicable
Integrity	-	-	-	-	Applicable

Table-3 Processing Time for Various Operations

Operations	Processing Time(in nano seconds)								
	1	2	3	4	5	6	7	8	Average
XOR	52804	10470	8580	6693	7616	17190	9552	15596	16062.625
Exponentiation	11741	1429	622	1009	139162	22271	2546	23719	25312.375
Hash	3422464	108570	68951	62550	60158	109302	-	-	638665.8333
Encryption	8604183	1578343	-	-	-	-	-	-	5091263
Decryption	12345926	4266320	-	-	-	-	-	-	8306123

Table-4 Operations and Processing Time for Various Smart Card Authentication Schemes

Methods, Operations, and Total Processing Time	Juang Scheme	Ping Wang *et al.* Scheme	Fan *et al.* Scheme	Liaw *et al.* scheme	The Proposed Scheme
Methods	Hash	Hash	Hash	Hash	Hash, DH
Operations	HF, XOR, EXP, ENC, DEC	HF, EXP, ENC, DEC	HF, XOR, EXP, ENC, DEC	HF, XOR, EXP, ENC	HF, XOR, ENC, DEC
XOR Computations	1	-	3	2	12
Exponentiation	4	4	1	4	-
Hash Computations	5	2	4	2	6
Encryption	3	4	3	6	2
Decryption	3	4	4	-	2
Total Processing Time (in nano seconds)	43502799.29	54968125.17	51126444.58	31958284.42	30819518.5

Table-5 Comparison Table for Total Processing Time, Difference in Total Processing Time, and Percentage of Differences of various Smart Card Authentication schemes

Processing Time, Difference in Time, and % of Difference in Time	Juang Scheme	Ping Wang *et al.* Scheme	Fan *et al.* Scheme	Liaw *et al.* scheme	The Proposed Scheme
Total Time (in nano seconds)	43502799.29	54968125.17	51126444.58	31958284.42	30819518.5
Difference in Time (in nano seconds)	12683281	24148607	20306926	1138766	-
Percentage of Difference	41.153403	78.35491	65.88982	3.69495	-

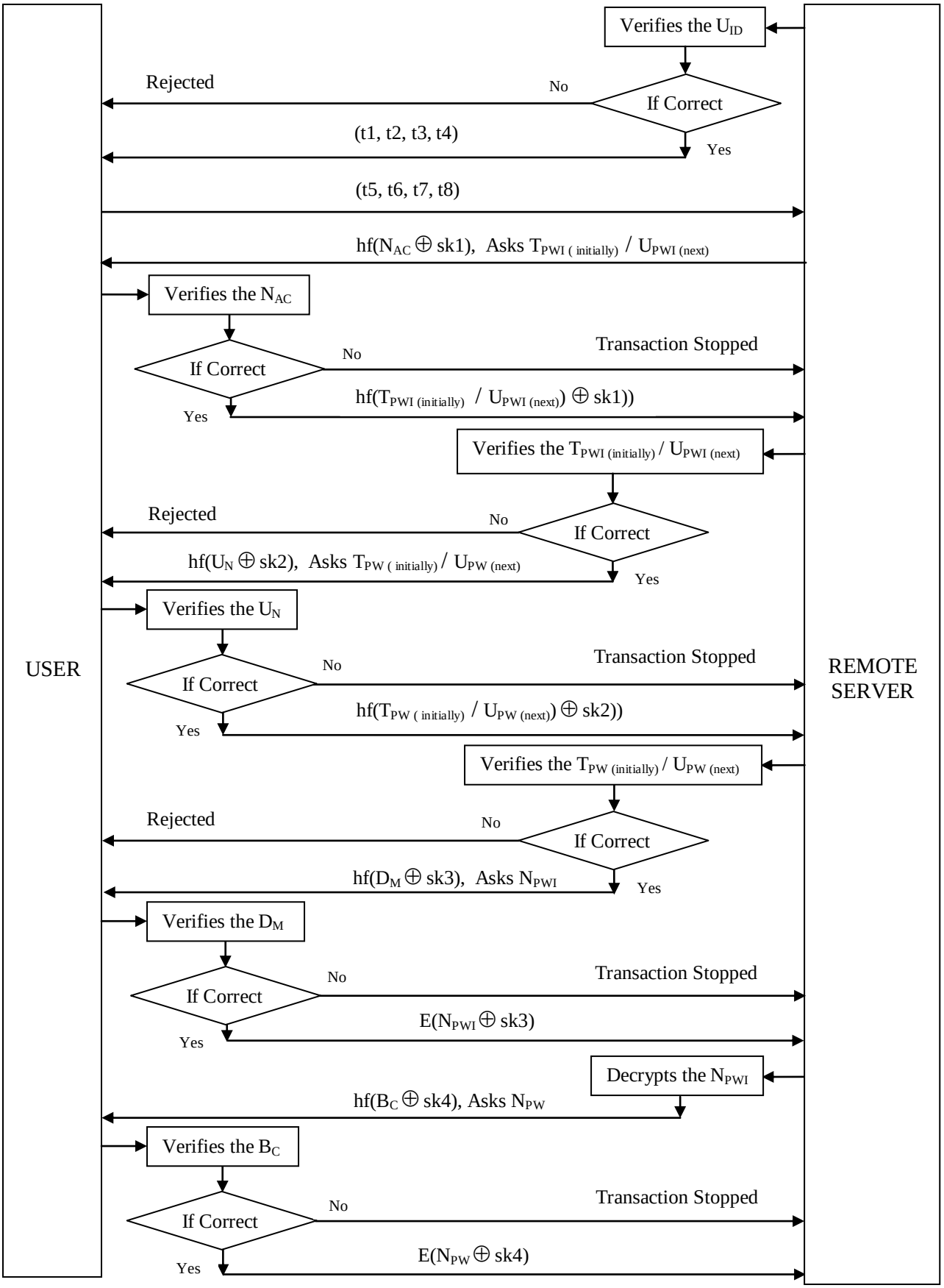

Figure 3. Dynamic Mutual Authentication Phase