International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010
1793-8201

Application of Automatic Variable Password Technique in Das's Remote System Authentication Scheme Using Smart Card

C. Koner, *Member, IACSIT*, C. T. Bhunia, *Sr. Member, IEEE* and U. Maulik, *Sr. Member, IEEE*

***Abstract*— Remote systems authentication schemes need more research and investigation due to increasing of hackers and attacks with the population of wired and wireless traffic. All of the popular remote user and system authentication schemes are fixed authentication and provides only entity authentication, not provides any data authentication. Recently Das proposed a flexible remote systems authentication scheme using smart card [8] that checks authenticity of user as well as remote system.**

In this paper, we show that Das's scheme is not withstand the modification attack, reverse XOR attack and adversary system attack. We have proposed Modified Das's scheme which serves as entity authentication as well as data authentication. We have applied Automatic Variable Password technique (AVP) to make the password unbreakable by changing it session to session. Application of AVP made the Das's scheme a Time Variant Authentication scheme that checks the authenticity of remote user time to time. We show that how Modified Das's scheme defenses modification attack, reverse XOR attack and adversary system attack.

***Index Terms*—Automatic Variable Password, Remote user, Remote system, Smart card, Time Variant Entity and Data Authentication.**

I. Introduction

Remote user authentication in sending information is a great research challenge. Remote user authentication is made of two types – Entity Authentication and Data Authentication. In Entity Authentication remote system checks the authenticity of remote user by the entity (e.g. password, smart card etc) of user before the transmission of user message. Authenticity is verified by the theory of public key cryptography. But Data Authentication remote system checks the authenticity of remote user by user message after receiving the message.

Chandan Koner is an Assistant Assistant Professor in the Department of Computer Science and Engineering, Bengal Institute of Technology and Management, Santiniketan, P.O. Doranda, West Bengal, Pin-731236, India., he is pursuing PhD course. He is member of IACSIT and IAENG. (Phone No.+91-9434535556, email: chandan_durgapur@yahoo.com)

Chandan Tilak Bhunia is an Director, Bengal Institute of Technology and Management, Santiniketan, P.O. Doranda, West Bengal, Pin-731236, India. He is a Senior Member of IEEE and FIE.

(Phone No. +91-9434033157, email: ctbhunia@vsnl.com)

Ujjwal Maulik is currently a Professor in the Department of Computer Science and Technology, Jadavpur University, Kolkata, India. He is a Senior Member of IEEE.

(Phone No. 91-33-24131766, email: ujjwal_maulik@yahoo.com).

Many different Data Authentication [1-3] and Entity Authentication [4-8] are studied separately in literature.

Remote password authentication scheme using smart card was first proposed by Chang and Wu in 1993 [5]. After that, several new remote user password authentication schemes with smart card have been proposed. Remote user authentication using smart card, introduced by Hwang and Li in 2005 [6], is an application of ElGamal's cryptosystem [7]. After that, few public-key based authentication techniques have been invented and improved. But all of the techniques check only the authenticity of user but can not check the authenticity of system. In 2006, Das et al [8] developed a flexible remote user authentication scheme using smart card that authenticates user as well as remote system.

The entire remote user authentication schemes are fixed authentication (no time variant authentication) and provide only Entity authentication, not providing any Data authentication. This motivates us to develop a scheme that will serve as data authentication as well as entity authentication. The Automatic Variable Password (AVP) technique [9] can be applied by changing the password from session to session to make the password unbreakable. In this paper, we proposed Modified Das's scheme which is application of AVP technique that will check the authenticity of user time to time throughout the accessing of the remote server and it serves as a data authentication as well as entity authentication. We also show that Das's scheme is vulnerable to different attacks and how brilliantly Modified Das's scheme defenses those attacks and enhances the efficiency of the scheme.

II. Review Of Das's Remote System Authentication Scheme

Das's Remote System Authentication is a mutual authentication scheme, which authenticates the remote user as well as the remote system. The user chooses a password (PW_i). The user has no private or public key but the remote system has a primary secret key (x) and a secret number (y). This scheme consists of three phases: registration phase, authentication phase and password change phase.

In the registration phase, the user U_i submits PW_i to the remote system (RS) for registration. The RS computes $N_i = h(PW_i,ID_i) \oplus h(x)$ and personalize a smart card with the parameters h(.), N_i, $h(PW_i,ID_i)$ and y.

The authentication phase is divided into two parts, namely

the User authentication and the RS authentication.

In user authentication phase, U_i insert his smart card and submits ID_i and PW_i. The smart card checks PW_i and ID_i with the stored ones in smart card. If they are correct, the smart card computes $DID_i = h(PW_i, ID_i) \oplus h(y \oplus Tu)$, where Tu is timestamp of U_i 's system and $C_i = h(Ni \oplus y \oplus Tu)$. Send (DID_i, C_i, Tu) as login request to the RS. RS receives the login request at time Ts and authenticates the U_i by the following way. If the time interval between Tu and Ts is the expected valid time interval for the transmission delay, then RS computes $h(PW_i, ID_i) = DID_i \oplus h(y \oplus Tu)$ and $C_i^* = h(h(PW_i, ID_i) \oplus h(x) \oplus y \oplus Tu)$. If $C_i^* = C_i$, the user is authentic.

In RS authentication phase, RS computes $X_i = h(h(PW_i, ID_i) \oplus h(x) \oplus Tu \oplus Ts^*)$ where Ts* is timestamp of RS's system and sends (X_i, Ts^*) to the user. Let the user receives the response at time Tu*. If the time interval between Tu* and Ts* is a valid time interval then computes $X_i^* = h(Ni \oplus Tu \oplus Ts^*)$. If $X_i^* = X_i$, then the RS is authentic.

III. Cryptanalysis Of Das'S Scheme

We present a cryptanalysis of Das's remote system authentication scheme in this section. Das showed that, although his scheme is secured from replay, stolen verifier, impersonation, guessing and denial-of-service attack but his scheme is still vulnerable to modification attack, reverse XOR attack and adversary system attack. We demonstrate these attacks.

（i） Modification attack: As the remote system checks the authenticity of user before the transmission of message. Remote system does not verify the authentication of user by user message after receiving the message. So an adversary can change user message in the transmission of user message. Hence Das's scheme is suffer from modification attack.

（ii） Reverse XOR attack: During the registration phase, the secret key x has to be applied. Now based on the reversible property of XOR operation, if the primary secret key of remote system (x) is hacked and user password (PW_i) is guessed, then nonce, N_i can be easily obtained. Hence Das's scheme is vulnerable to the reverse XOR attack.

（iii） Adversary system attack: Suppose the processors in remote system and card reader are very hasty and the transmission of data between user and server is happening in very speedily. In this type of communication, the timestamp of user Tu in user authentication phase and the timestamp of server Ts* in remote system authentication phase will be equal. During remote system authentication phase, remote system sends X_i [$= h(N_i \oplus Tu \oplus Ts^*)$ or $h(h(PW_i, ID_i) \oplus h(x) \oplus Tu \oplus Ts^*)$] to the user over a public channel. As Tu and Ts*are same so $X_i = h(N_i)$. Again suppose an adversary has stolen the user smart card for one time and just extract the N_i and mode of hash function is known to him so he can easily compute X_i which is h(x). Now if the adversary is also a user and accessing another server then he can send X_i to the user by that illicit sever over the public channel before the original server sent. Then user can easily certify that server as an authentic server and communicates with that illicit server. The adversary, thus, can trick the user by connecting him with a wrong server. Das's scheme is therefore insecure from the adversary system attack.

IV. Modified Das'S Remote System Authentication Scheme

Modified Das's Remote System Authentication Scheme is mainly divided into two parts, namely, Entity Authentication Phase and Data Authentication Phase. The Entity Authentication Phase checks the authenticity of the remote user time to time by user password. The Data Authentication Phase checks the authenticity of the remote user by applying cryptography (Digital signature) on the user sending message. The Entity Authentication Phase is further subdivided into four parts, namely, User Enrollment Phase, User Login Phase, User Accessing Phase and Remote System Authentication Phase. Data Authentication Phase is also subdivided into three parts, namely, Key Generation Phase, Data Sending Phase and Data Receiving Phase.

A. Entity Authentication Phase

1) User Enrollment Phase

This phase is invoked whenever a user U_R wants to register to the remote system S_R. The U_R chooses a password PW_1 and identifier ID and submits it to the S_R. After receiving enrollment request, the S_R performs the following operations.

DUE1: Computes, $N = h(PW_1 \oplus ID \oplus x)$, where x is a primary secret key of S_R, h(.) is a one-way hash function and $\oplus$ is a bitwise concatenation operator.

DUE2: Personalizes a smart card C_S with the parameters h(.), N, PW_1, ID, E, D and y, where y is the secondary secret number stored in each registered user's smart card, E is the encryption key and D is the decryption key generated by remote system by applying RSA algorithm.

DUE3: Sends the C_S to the U_R in a secure channel.

User Login Phase

When the U_R wants to login to the S_R then the following steps are executed. This part is executed only once when the U_R wants to login to the S_R. U_R inserts his C_S and keys his identity ID and password PW_1'. The C_S verifies the entered ID and PW_1' with the stored ones in C_S. If the ID and PW_1 are correct, the C_S executes the following steps,

DUL1: Computes, $D = h(PW_1 \oplus ID \oplus x) \oplus h(y \oplus Tu)$

DUL2: Computes, $C = h(N \oplus Tu \oplus y)$

Then send (D, C, Tu) as login request to the S_R. Upon receiving the login request at time Ts, the S_R authenticates the U_R the following steps,

DUL3: Computes, $h(PW_1 \oplus ID \oplus x) = D \oplus h(y \oplus Tu)$

DUL4: Computes, $C^* = h(h(PW_1 \oplus ID \oplus x) \oplus y \oplus Tu)$

If $C = C^*$, the S_R accepts the login request and gives permission to the U_R to send the data.

2) User Accessing Phase

User accessing phase is executed to check authenticity of U_R when U_R is accessing the S_R. This phase is executed at a

regular interval during the time of accessing the S_R by U_R.

Let T_P is timestamp of S_R when the U_R starts to access the S_R and at a ΔT regular interval the S_R wants to verify the authenticity of U_R.

Now let $T_P + (\Delta T + \ldots\ldots\ldots\ldots\ldots\ldots) = T_P'$

Assume the U_R's message M which is sent to the S_R, is a continuous bit stream. C_S divides the M into different blocks of fixed size as the length of PW_1 in Date sending phase of Data authentication phase. Let the message blocks are M_1, M_2, M_3,……., M_n.

The C_S generates modified blocks by the following way,

$PW_2 = PW_1 \oplus M_1$,

$PW_3 = PW_2 \oplus M_2$,

So, $PW_n = PW_{n-1} \oplus M_{n-1}$

Thus the password at i^{th} position will be,

$PW_i = PW_{i-1} \oplus M_{i-1}$

$PW_i = PW_{i-2} \oplus M_{i-2} \oplus M_{i-1}$ and therefore

$PW_i = PW_1 \oplus M_1 \oplus M_2 \oplus \ldots\ldots\ldots\ldots \oplus M_{i-2} \oplus M_{i-1}$

The C_S sends PW_i blocks simultaneously as message blocks to S_R. The C_S also uses PW_i blocks one by one for every authentication checking execution after every ΔT regular interval.

DUA1: The S_R sends $< T_P'>$ as an authentication query to the C_S through a public channel after every ΔT regular interval.

DUA2: After receiving the authentication query, the C_S asks the U_R to enter the ID and PW_1.

DUA3: Then the U_R enters his ID' and PW'_1.

DUA4: The C_S validates the entered ID' and PW'_1 with the stored ones in C_S. If the ID and PW_1 are correct then executes the following steps, otherwise terminates the accessing,

DUA4.1: Computes, $D' = h (PW_i \oplus ID \oplus x) \oplus h (y \oplus T_P')$

DUA4.2: Computes, $C' = h (N \oplus y \oplus T_P')$

DUA4.3: Send (D', C', T_P') as authentication request to the S_R through a public channel.

DUA5: After receiving the authentication request, the S_R authenticates the U_R the following steps,

DUA5.1: Computes, $h (PW_i \oplus ID \oplus x) = D' \oplus h (y \oplus T_P')$

DUA5.2: Computes, $C'^* = h (h (PW_i \oplus ID \oplus x) \oplus y \oplus T_P')$

DUA5.3: Checks whether $C' = C'^*$. If it holds, then gives permission to access again otherwise terminates the accessing.

3) Remote System Authentication Phase

Remote system authentication phase is executed to check the authenticity of S_R. The correctness of the S_R is checked in this phase and executed when authenticity of U_R is passed correctly.

DRA1: Computes, $X= h ((h (PW_1 \oplus ID \oplus x) \oplus h(Tu)) \oplus h(Ts^*)$ where Ts^* is the timestamp of S_R.

DRA2: Send (X, Ts^*) to the U_R over a public channel.

The smart card computes $X^* = h ((N \oplus h (Tu)) \oplus h(Ts^*)$ and checks whether $X=X^*$ or not. If $X = X^*$, then S_R is authentic and U_R starts accessing the resources.

B. Data Authentication Phase

1) Key Generation Phase

Key Generation Phase is executed after receiving the enrollment request of U_R by S_R in parallel with user enrollment phase of Entity authentication phase. This phase is executed only once for one U_R. In this phase the S_R performs the following steps,

DKG1: Generates Encryption Key (E) and Decryption Key (D) by RSA algorithm.

DKG2: Stores E and D into C_S with other parameters h(.), N, PW_1, ID and y.

2) Data Sending Phase

Data sending phase is executed after the User login phase of Entity authentication phase. In this phase the C_S performs the following steps,

DDS1: Divides the M into different message blocks of fixed size as the length PW_1. Let the message blocks are M_1, M_2, M_3,……., M_n.

DDS2: Sends the Decryption key D to the S_R through a public channel.

DDS3: Sends first message block M_1 and the Digital Signature of M_1 (Calculated the Hash of M_1 then encrypts it by E) to the S_R.

DDS4: Generates PW_2, PW_3,……,PW_n blocks by the above theory.

DDS5: Sends PW_2, PW_3,……,PW_n blocks and Digital Signature of them to the S_R through a public channel without waiting for authentication query from S_R. When S_R sends authentication query after a ΔT regular interval then stops the sending of PW_i. After authentication checking if S_R gives permission to access then sends PW_i blocks again simultaneously.

DDS6: If receives any request for sending any block again from S_R, then immediately sends it.

3) Data Receiving Phase

Data receiving phase is executed after receiving the first message block M_1 and the Digital Signature of M_1 from the U_R, the S_R executes the following steps,

DDR1: Decrypts the Digital Signature of M_1 by D and calculates the hash of M_1. Then compares Digital Signature of M_1 and hash of M_1. If they are same, confirms that M_1 was sent from authentic U_R. If they are not same, rejects M_1.

DDR2: Then receives and decrypts the Digital Signature of PW_2, PW_3,……,PW_n by D and calculates the hash of them simultaneously. After that compares each decrypted block PW_i with their hash. If any block is not same, rejects it.

DDR3: If any block is rejected then sends a request to C_S for sending it again.

Now S_R gets M by the following theory,

$M_2 = PW_2 \oplus PW_3$,

$M_3 = PW_3 \oplus PW_4$,

So, $M_n = PW_n \oplus PW_{n+1}$

V. Security Analysis Of Modified Das's Scheme

We analysis that how Modified Das's scheme is protected from the various security parameters. We discuss the defense of the scheme from the various attacks by which previous techniques are suffered.

Modification attack: In Modified Das's scheme the remote system checks the authenticity of user on user message after

the transmission of message. If an adversary alters the authentic user message during the transmission of message, the remote system can easily identify it. Hence Modified Das's scheme is not suffer from Modification attack.

Reverse XOR attack: In this authentication scheme, N [= h(PW⊕ ID⊕ (x)] is computed in the registration phase. If PW is guessed and mode of hash function is leaked by an adversary, he never gets N because N is a function of four parameters PW, ID and x. Hence Modified Das's scheme is undoubtedly not vulnerable to the reverse XOR attack.

Adversary system attack: In remote system authentication phase, remote system sends X [=((h (PW⊕ ID⊕ x) ⊕ h (Tu)) ⊕ h(Ts)] to the user over a public channel. For a very first system where Tu and Ts are same X will not be equal to the h (N). So if an adversary extracts the N by stoling the user smart card for one time and mode of hash function is known to him then he never gets X. So the user always authenticates a correct server. Hence Modified Das's scheme is firmly secured from the adversary system attack.

VI. Experimental Results And Discussion

Suppose U_R submits the following password and identifier to the S_R,

User Password (PW_1): User'sAuthentication

User Identifier (ID): IdentityofRemoteUser

Suppose S_R generates Encryption and Decryption key by RSA algorithm in the following way,

Let, two large prime numbers P=13 and Q=19.

So, N=13×19=247

Encryption Key (E) = 31 and Decryption Key (D) = 7

Suppose U_R sends a message of 1600 bits to the S_R,

User Message (M): "Authentication in sending information is a research challenge. Time Variant Authentication technique will check the authenticity of user for time to time throughout the accessing of the remote server."

M =

```
41757468656e7469636174696f6e20696e207365
6e64696e6720696e666f726d6174696f6e206973
20612072657365617263682063686163616c6c616e67
65652054696d652056617269616e742041757468
656e7469636174696f6e20746563686e69717565
2077696c6c20636865636b207468652061757468
656e7469636974796f662075736572206666f72
2074696d6520746f2074696d65207468726f7567
686f7574207468652061636365737369696e67206f
662074686520726d6f7465207365727665722e
```

A. Results of Entity Authentication

The C_S generates the following new passwords after receiving every authentication query from S_R,

PW_2: 1406111a421d351c170911071b0743081a491c0b

PW_3: 7a627874253d5c727166636a7a732a6774697578

PW_4: 5a035806404e391303050b4a191b4b0b18081b1f

PW_5: 3f2d785229235c335564792378753f2b597d6f77

PW_6: 5a430c3b4a42285a3a0a59571d165745300c1a12

PW_7: 7a34655726624b325f693277697e326551796e7a

PW_8: 1f5a113e450b3f4b7f0654571c0d5717711f0108

PW_9: 3f2e7853202b4b245f723d3a792d237f0370746f

PW_{10}: 57410d27005f23417f135e591c5e50166d175400

B. Results of Data Authentication

Digital Signature of Message of Das's Scheme is given below,

DF =

```
c4a659b0cd0506e24d7c7c18534076cb4f33c7c1
e95f634bdcc11ed63d47a29747753a9c8270d731
7a3c7883c1ca000a544cccc9af4fbd631bf5007a
6b7a2fc508054adc5aab03510142943407a2a62a
be39a369d0d7ee2ff201c6acca9a0939b2cdc7
c806e7a6528209681e15e22fc75aa700dad29da8
60ca01d8e6934601540b3ac0b0e16a5739cf5d41
92314ed220d9f69ae082284e1202ddd984e8ec38
5a1add2131437673 42a693b7c2d0d6af82b693
ec665224121b7744ddb78ec067ee3d30d354c07c
```

Digital Signature of Message of Modified Das's Scheme is given below,

DT =

```
c4a659b0cd0506e24d7c7c18534076cb4f33c7c1
9c216ae63a892bb099922d3d8eeae1b88fd6a6b8
8118af4271aaa7919b48edc52e0bbbe2083bcd45
31a7d426115abe54ef3c45f2271e89b2dd2342f1
d1dd7d367a6965578b4cba86a6eb835526e89f4a
c37eb3ddf4b61ac9a06328092fa89d4d2c6616af
e18a90cac3ebbc458de30d475a5e3c838b0bbaaf
4a7d7e55d79991a0da1d9067c3e56e8cae384aeb
03bc6ec795369ca116509022b770b9d27916f52e
0f0aecc6b150a117766cef50497d899c46b16e51
```

VII. Experimental Analysis Das'S Scheme And Modified Das'S Scheme

This section discusses the analysis of experiment results of the Das's scheme and Modified Das's scheme. We compare the techniques using three parameters: Distance, Redundant Character and Redundant Pair Character. Distance is defined as the summation of modulus of deviation between characters of plain text and cipher text. Redundant character measures the same character if they are in same position in plain text and cipher text. Redundant Pair character measures the pair of character if they are in same position in plain text and cipher text.

A. *Das's scheme*

(i) Distance = Deviation of M and DF = ∑ Deviation of m_{ij} from df_{ij} = 1937.

The probability of authentication depends on the distance. Smaller distance increases the probability of authentication failure.

(ii) Redundant Character: If (m_{ij} = df_{ij}) then the character is redundant. Here 28 characters are redundant out of 400 characters. So the probability of redundant character is 28/400. The probability of redundant character increases the probability of authentication failure.

(iii) Redundant Pair Character: If ($m_{ij}m_{i+1j+1}$ = $df_{ij}df_{i+1j+1}$) then the characters are redundant pair. Here 3 characters are redundant pair out of 200 characters. So the probability of redundant pair character is 3/200. The probability of redundant pair character increases the probability of authentication failure.

B. *Modified Das's scheme*

(i) Distance = Deviation of M and DT = ∑ Deviation of m_{ij} from dt_{ij} = 1979.

The probability of authentication depends on the distance. Smaller distance increases the probability of authentication failure.

(ii) Redundant Character: If (m_{ij} = dt_{ij}) then the character is redundant. Here 20 characters are redundant out of 400 characters. So the probability of redundant character is 1/20. The probability of redundant character increases the probability of authentication failure.

(iii) Redundant Pair Character: If ($m_{ij}m_{i+1j+1}$ = $dt_{ij}dt_{i+1j+1}$) then the characters are redundant pair. Here 1 character is redundant pair out of 200 characters. So the probability of redundant pair character is 1/200. The probability of redundant pair character increases the probability of authentication failure.

VIII. Comparative Study By Result

This section discusses comparison between the Das's scheme and Modified Das's scheme. We compare the techniques by the following parameters.

A. *Comparison by Distance*

The distance is lower in Das's scheme than Modified Das's scheme this means that the probability of authentication failure is more in Das's scheme. The distance is higher in Modified Das's scheme this means that the probability of authentication failure is lower Modified Das's scheme. Comparing by distance, we conclude that Modified Das's scheme is the more efficient authentication scheme.

B. *Comparison by Redundant Character*

The no of redundant character is lower in Modified Das's scheme than Das's scheme that means the probability of authentication failure is lower in Modified Das's scheme than Das's scheme. Comparing by redundant character, we conclude that Modified Das's scheme is the more efficient authentication scheme.

C. *Comparison by Redundant Pair Character*

The no of redundant character is lower in Modified Das's scheme than Das's scheme that means the probability of authentication failure is lower in Modified Das's scheme than Das's scheme. Comparing by redundant character, we conclude that Modified Das's scheme is the more efficient authentication scheme.

IX. Conclusion

In this paper we have discussed the proposed Modified Das's remote system authentication scheme which checks the authenticity of remote user time to time and provides entity authentication as well as data authentication. This scheme is very fast operating since our proposed algorithm tested under C-programming. Therefore, this authentication method can be applied in real time basis for all sort remote network.

It has lot of advantages which are specifically listed below:

(i) This technique enjoys the advantages of Data Authentication as well as Entity Authentication.

(ii) An encrypted user message is sent to the remote system.

(iii) Insulated from modification attack, reverse XOR attack and adversary system attack..

(iv) User authenticity as well server authenticity is checked efficiently.

(v) Many users with same login identity can not able to log in.

(vi) Any user password database is not required in remote sever.

In future, we are exposing to find out more advanced realistic solution in the field of remote user and system authentication.

References

[1] C. T. Bhunia, *Information Technology Network and Internet*, New Age International Publishers, India, 5th Edition (Reprint), 2006.

[2] Charlie Kaufman, Radia Perlman and Mike Speciner, *Network Security: Private Communication in Public World*, Pearson Education, India, 2nd Reprint, 2003.

[3] Atul Kahate, *Cryptography and Network Security*, Tata McGraw Hill, India, Sixth Reprint, 2006.

[4] L. Lamport, "Password authentication with insecure communication." *Communication. ACM*, Vol. 24, No. 11, pp. 770-772, 1981.

[5] C. C. Channg and T. C. Wu, "Rmote password authentication with smart cards", *IEEE Proceeding-E*, Vol. 138, no. 3,pp. 165-168, 1993.

[6] 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, February 2000.

[7] T. ElGamal, "A public key based cryptosystem and a signature scheme based on discrete algorithms", *IEEE Transactions on Information Theory*, Vol. 31, No. 4, pp. 469-472, 1985.

[8] M.L.Das, "Flexible and Secure Remote Systems Authentication Scheme Using Smart Cards". *HIT Transaction on ECCN*, Vol. 1, No.2, pp.78-82, April 2006.

[9] C.Koner, C.T.Bhunia, U.Maulik, "An Efficient and Reliable Time Variant Three-Entity and Data Authentication of Remote User Using Smart card" on *ITNG09, IEEE Computer Society, USA* pp487-491.