Journal of Information & Communication Technology
Vol. 10, No. 1, (Spring 2016) 65-81

IMPROVEMENT OF A DYNAMIC ID BASED REMOTE USER PASSWORD AUTHENTICATION KEY AGREEMENT SCHEME WITH VERIFIABLE PASSWORD UPDATE FOR WIRELESS COMMUNICATION

Hina Memon[1]
Institute of Mathematics and Computer Science, University of Sindh ,Jamshoro, Sindh ,Pakistan
Imran Memon[2]
College of Computer Science, Zhejiang University
Qasim Ali Arain[3]
Department of Software Engineering, MUET Jamshoro, Pakistan
Farman Ali Mangi[4]
Department of Physical Electronic, University of Electronic Science and Technology of China
Deedar Ali Jamro[5]
Department of Physics and Electronics Shah Abdul Latif University Khairpur, Pakistan

ABSTRACT

The security and authentication of the mobile user are challenging problem, seamless mobile users roaming over a wireless network are extremely desirable. In 2011, Khan, has given a concept of Dynamic ID based user Authentication that is going to assert their scheme has security strength. In this manuscript, we pointed that khan scheme was not fastened to certain attacks such as impersonation attacks, man and middle attack, spoofing attack, exhaustion attack launch by an adversary at any time. An adversary got sensitive information inserted in smart cards; their strategy was completely divided up. Furthermore, the proposed scheme did not offer user's anonymity because it was lacking with the concept of revocation, key exchange, and secret renewal for users. We suggest a scheme is robust and it has the strong security measurements, our scheme does not only protecting above mentioned security problems but also offered other advantages. We have introduced a new feature by taking appropriate advantage of user authentication schemes for wireless communication. It will acquire the critical information enclosed inside the smart card however the user password of the owner remains anonymous to the attacker. Finally, we performed analysis and has proved that our scheme has outperformed the other schemes based on smart card authentication.

Key Words: LBSS, Localization, Range-Free, Continuous Query, Road Network

INSPEC Classification : A9555L, A9630, B5270

---

1 Hina Memon : hinamemon@gmail.com
2 Imran Memon : Imranmemon52@zju.edu.cn
3 Qasim Ali Arain : Arainqasim_ali_arain@yahoo.com
4 Farman Ali Mangi : farman.mangi@salu.edu.pk
5 Deedar Ali Jamro : deedar.jamro@salu.edu.pk

1. INTRODUCTION

The rapid proliferation of wireless network and micro electromechanical systems, so it is very easy for the user to enjoy the particular services from multiple servers by using their personal digital assistant from anywhere (Imran Memon, 2015). Meanwhile, it is of utmost importance to ensure that a system's services will not be consumed by unauthorized users in a fraudulent manner. Among numerous methods available for validating a remote user, password based authentication is one of the greatest effective approaches.

Previously authentication schemes were depending on password based schemes. It is comparatively easy to implement passwords have various vulnerabilities (Mohammad Sabzinejad.et.al, 2014). Three factor authentications are quite safe to smart card based password authentication only modification is that it needs biometric appearances as more authentication. However biometric authentication factor is the most people would not like to discuss about it, but it has its own significance. Moreover by considering the intense cases, may lead to the dis-functioning of hands, eye damage and damage of vocal cord etc. however the implementation cost is too much high. So for that reason it can be deduces that the three factor authentication was bit costly then two factor authentication.

In 2004, password based authentication scheme with anonymous use to wireless environment proposed by Zhu et al..(Zhu, J., & Ma, J., 2004). However this technique may not achieve the desired results and could not achieve mutual authentication and forgery attack and susceptible to perfect backward pointed by Lee et al.(Lee, C.-C., Hwang,2006). However, another more authenticated anonymous scheme has been proposed in 2006 by Wei et al. (Hongfeng Zhu, XinHao,2000).Subsequently, Wu et al.(Chia-Chun et.al,2008) investigated Lee et al.'s technique, verified that it could not accomplish user privacy, regressive privacy in 2008. Further, secure and authentication schemes are proposed that claim that this scheme user anonymity ,backward secrecy achieved both for wireless communication environment proposed by Wu et al. (Lee, J.-S., Chang,et.al,2009) and Lee et al.(Wang, C.-H,et.al,2009) demonstrated that Wu et al.'s scheme fails to does not offer user anonymity. Wang et al.(Jeon, W,et.al,2012) after that they proposed an established the same scheme. Be that as it may. Jeon et al.(Khan MK,et.al,2011) showed that Wang et al.'s scheme is vulnerable to a malicious attacker cloud not offer user anonymity. Khan et al.(Khan MK,et.al,2011)schemes, real life implementation recognized that there were various practical drawbacks (Wang YY,et.al,2009). All contributions in recent papers support our works.

In this paper, we show that khan et al.'s proposed scheme practical implementation drawbacks and were not providing the security (Wang YY, et.al, 2009). An impersonation attack is proposed by Ku and man and middle attack, spoofing attack, exhaustion attack can be an effective attack on these schemes (Qi Xie, Bin Hu, et.al, 2015). Our proposed scheme, to need operations on mobile users is just one asymmetric encryption/decryption operation. Due to this reason, it's more appropriate for low power and resource limited mobile devices. It involves four message exchanges between the mobile user, remote server and local server. The communicational efficiency should be improved due to this feature. It's more suitable for lower bandwidth mobile environment. Our schemes improved to enhance security of Khan et al.'s scheme. Our strategy would not only preserve the original scheme merit but also meet all requirements of other recently proposed schemes (Imran Memon, et.al, 2015).

In our scheme, a mobile user can freely change his/her password of the smart card without the help of the home agent. We demonstrate that previously proposed scheme can withstand offline password tracking attack and user impersonation attack. Also, our proposed scheme can detect an incorrect password in the login phase immediate. We also show that our proposed scheme is well suitable for mobile environments, and manifest the advantages of our scheme as compared to the recently schemes.

2. REVIEW OF KHAN ET AL.'S SCHEME

In the following discussion, we thoroughly review Khan et al.'s technique which comprises of five parts. These can be work as under (Su R, Cao ZF, 2010):

2.1 Registration phase

This part has been stimulated every time the user U_iinitially get connected or re connected to the validation server S. Moreover the following steps are being executed to cover the process of the registration.

(i) U_iChooses his ID_i and PW_i and produceaarbitrary number r and will calculate RPW = h(r || PW_i).
(ii) U_i used to suggest his ID_i and RPW to the S over a protectedcommunication channel.
(iii) S Would confirm the registration estimonial U_i and verify either the selected ID_i is previously in the system or not. If ID_i already presents in the system, Swould inform U_i to select a new ID_i . Moreover, S would verify the authentication record of U_i and if U_i is a novice user then it would setS value of N = 0, or else if U_i is re-connecting in the database then the value of S sets the value of N=1 and place these values of ID_i and N in the system.
(iv) S-ComputesJ=$\oplus$(r || IDU) where IDU= (ID_i || N) .
(v) S-Computes L =J RPW.

(vi) Hence S will issue smart card to U_i which might have the values of L and y over a protected communication channel.

(vii)U_i securely places random values r in the smart card and Needs not to remember its value (David Basin and CasCremers 2014).

2.2 Login phase

During login phase when U_i needs to get login into S, it will need to put his smart into the terminal and needs to inputs his ID_i and PW_i.So it will have to perform the following procedure:

It needs to calculate RPW =h(r || PW_i).and L =J ⊕ RPW in which random values r is robustly stored in the smart card.

(ii) It will then get the latest timestamp value T_i and calculatesC_1 = h(T_i || J).

(iii) It will then need to generate a random number d which will calculates an secret ID of U_i by AID_i ID_i = h(yT_i || d).

(iv) After login procedure,U_i sends login message m = {AID_i,T_i,d,C_1} to S for the verification procedure(Cheng-Chi Lee,et.al,2014).

2.3 Authentication phase

While getting the request for login message m= {AID_i, T_i , d, C_1}, theverification end server Sconfirms its validity by the following procedures:

(i) it will Authenticate the legitimacy of time interval in between T_i and T′. If (T′ - ≥ ΔT , then S would refuse the request for login and inform U_i that the time span has been expired and no further processing would be done.

(ii) Computes ID_i = AID_i h(yT_i || d)and verify if ID_i will belong to a legitimate user's ID, if yes then it will allow further operations, in other case it will blocked the operation and intimates U_i about it.

(iii) it will confirm the value of N in the system and calculates = (ID_i || N) .

(iv) it will calculates J=h(x || IDU)and confirm either h(T_i || J) = C_1. However if these two values are same then U_i would be a confirm user and S will admit the login request, in the other case the login request would get rejected and user will get informed regarding the verdict.

(v) During the procedure of mutual authentication, Swould acquires the latest time span T_s and would calculates C_2 = h ⊕ ⊕ T_s) and after that would send the mutual authentication message {C_2,T_s }to U_i.

(vi) However after getting the mutual authentication message, U_i authenticate the time span amongT_i andT″, where T″, is the time span when mutual authentication message was acknowledged. If(T″ - T_s) = T , then U_i would discards the message and has to end the operation, however in the other case step (vii) is being performed.

(vii) Now U_i would verify either h(C ⊕ ⊕ T_s) = C_2. If the pervious condition get true then, U_i validate S in another case a login request would be cancelled by U_i.

(viii) However at this stage ,U_i and S would share the symmetric session key S_k = (C_2 ⊕ J) for executing more function while inside a session (Florian Bergsma , et . al , 2014).

2.4 Password-change phase

During this phase, smart card has to execute the following operations while not interacting with remote server S:

i) Computes RPW^*= h (r PW_i) and J^* = ⊕ RPW^* . If J=J^* hold, then U_i would get permitted to alter the password, however in other case password-change procedure is terminated.

(ii) It will calculates $= \oplus \ RPW \oplus \ RPW^{*} \ h(r \parallel PW_i')$ and would change the pervious old value of L with the fresh value. Hence the new password would get changed successfully and this phase is ended (KadhimHayawi, et.al, 2015).

2.5 Lost smart card revocation phase

In case of lost or stolen of smart card, U_i requests S for its revocation. S First validates the U_i by his secret credentials, e.g. mother's maiden name, date of birth, national ID card number, or some other values known to U_i. After validating the revocation request, S changes the value of N to revoke the smart card. In every case of stolen or loss of smart card, the value of N is increments by one. Later on, U_i can re-register to S without changing his ID_i (Jiliang Zhang,et.al,2015).

3. CRYPTANALYSIS OF KHAN'S SCHEME

During this discussion, it has been assumed that there is a weak Adversary, who can eavesdrop the communication over the internet. It has the ability to forge the messages and block the messages which are being transmitted over the internet, however at the same it has also some additional information to discover the information placed in smart cards (Yong Wang, et.al, 2015).

3.1 Impersonation attack

The first impersonation attack works in the following way. If an attacker has stolen MU's smart card, the attacker can impersonate MU to access the service on the foreign network. The detailed description of this attack is as follows. The attacker inserts MU's smart card into the device and enters the fake password $PW^{*} = 0$. The smart card computes $n^{*} = r \oplus PW^{*} \ h(N \parallel ID_{HA}) \oplus h(N \parallel ID_{MU})$[19]. From step 1 in the first phase of the scheme of, obviously, the attacker can obtain n^{*} by eavesdropping. The attacker can obtain the message. Thus, the attacker can obtain MU's $\{ID_{MU}, h(N \parallel ID_{HA}), ID_{HA}\}$ password $PW_{MU} = n^{*} \oplus ID_{MU} \oplus h(N \parallel ID_{HA}) \oplus ID_{HA}$. After that, with MU's real identity and password, the attacker can use MU's smart card to impersonate MU to access service in any foreign network. In addition, the schemes in is not efficient in password authenticate.

3.2 Address spoofing attack

An acquire a unique address without DAD. If a malicious mobile user spoofs a good mobile user's address to flood a false message (for example, a DAD message), its neighbor mobile users first receive the false message. Since the neighbor mobile users cannot authenticate the malicious mobile user, they abandon the false message. Therefore, the flooding of a false message is prevented. In the same way, if a malicious mobile user spoofs an address to communicate with a good mobile user, then the good mobile user will disrupt the communication with the malicious mobile user because it cannot authenticate the malicious mobile user.

3.3 Address exhaustion attack

If a malicious mobile user requests an address from a neighbor mobile user, then the neighbor mobile user will decline the request because it cannot authenticate the malicious mobile user. 1) False address conflict attack; if a malicious mobile user broadcasts an address conflict message, and then its neighbor mobile users first receive the message. Because the neighbor travelling users cannot authenticate the malicious mobile user, they abandon the address conflict message. Moreover, this protocol achieves the address configuration without DAD, so it does not employ an address conflict message to ensure an assigned address' uniqueness. Therefore, if a mobile user receives an address conflict message, then it can determine that the message comes from a malicious message. In this way, the flooding of a false address conflict message is prevented.

4. PROPOSED SCHEME

4.1 Registration phase

A user Uiget registered at the server (S) by the following procedures:

Step 1:

U_i g S: {ID_i, d0}

A userUichooses an identity of user ID_i, a password pw_i, and arbitrary dig$\in Z_p^*$[, and calculates d0 = h(pw_i || ID_i) N. Next, U_i sends {ID_i, d0} to the Server (S) by a protected network.

Step 2:

S g U_i: Smart card

S Computes A_i = h(ID_i || r), c = $\oplus$ d0 , and places {c , x , p, Q, h()} to a smart card. Then server notify the smart card to U_i by a protected network.

Step 3:

U_i g Smart card: {d1, d2}

U_i computes d1 $\oplus$ N, d2=h(ID_i||pw_i), and replaces c with {d1,d2} in the smart card. The nonce N might not be stored in the card.

In the same way, the remoteserver RSjget registered at the S. Sj chooses and directsto a remote server $RSID_j$. Then the remote server sends back {Bj, x, p, Q, h()} to a protected communication network, when Bj=H(r||SID_j).

So we can define the login procedure, verification and key agreement part as following.

4.2 Login phase

When U_i attempts to login a remove server RSU_j, U_i put that smart card inside a card reader and key in the identity of a user ID_i and password PW_i.

Step 1:
The card calculates $h(ID_i||pw_i)$ and confirmeither it is equivalent to the stored d2. However if these two are not same , it will end the session. Moreover it will move forward to the next step.

Step 2:
After U_i inputs the remove server identity $RSID_j$, the smart card computes A_i=d1 $h(pw_i||ID_i)$. Hence the card would select an arbitrary value ri and computes

$Q_i1 \equiv T_{r_i}(x)$ mod p, $Q_i2 \equiv T_{r_i}(Q)$ mod p, $X1 = h(Q_i2)$ ID_i, $X2 = h(A_i||RSIDj||Q_i1||Q_i2||X1)$.

Step 3:
Smart card g RSj: {Qi1, X1, X2}

Step 4:
Here in this case RSUj would select an arbitrary value rj and computes

$Qj1 \equiv T_{r_j}(x)$ mod p, $Qj2 \equiv T_{r_j}(Q)$ mod p,

$Y1 = h(Qj2) \oplus RSIDj$, $Y2 = h(Qj1||Qj2||Qi1||Y1||X2||Bj)$.

Step 5:
Sj g remove server : {Qi1 X1, X2, Qj1, Y1, Y2}
RSj sends {Qi1,X1,X2, Qj1,Y1,Y2} to the Server (S).

4.3 Authentication and key agreement

Step 1:

Upon receiving {Qi1, X1, X2, Qj1, Y1, Y2}, the remove server computes

$Qi2^* \equiv T_r(Q_{i1})$ mod p, $IDi^* = h(Qi2^*)$ X1, $Ai^* = h(IDi^*||r)$,
$Qj2^* \equiv T_r(Q_{j1})$ mod p, $RSIDj^* = h(Qj2^*)$ Y1, $Bj^* = h(r||RSIDj^*)$.

Step 2:

The remote server confirms if
$X2 = h(Ai^*||RSIDj^*||Qi1||\ Qi2^*||X1)$, $Y2 = h(Qj1||Qj2^*||Qi1||Y1||X2||Bj^*)$. However if any of them might not true, remote server would discard the login invitation. In other case, the IPv6 calculates
$Zi = h(Qi1||Qj1||RSUIDj^*||Ai^*||X2)$, $Zj = h(Bj^*||Qi1||Qj1||Zi)$.

Step 3:

IPv6 g RSj: {Zi, Zj}
The remote server sends {Zi,Zj} back to the RSj.

Step 4:

Remote server RSjwill confirm either the equation Zj=h(Bj||Qi1||Qj1||Zi) holds. If it is the case, RSjwould select a vibrant identity CIDi and a cessation date t So that the user is permissible to login the remote server RSj. Then RSUj calculates R=h(CIDi||Bj||t) $\oplus$ h($T_{r_i}(Q_{i1})$),Rj=h(Zi|| $T_{r_j}(Q_{i1})$ ||CIDi||t||R).

Step 5:

RSj g Ui: {Qj1,Rj, CIDi,t,R}

Step 6:

The smart card first computes Zi*=h(Qi1||Qj1||RSIDj||Ai||X2), and checks whether Rj=h(Zi*|| $T_{r_i}(Q_{j1})$ ||CIDi||t||R).
So if the above condition might get true, then the smart card would calculate V= R $T_{r_i}(Q_{j1})$,
Ri=h(RSIDj||Qi1||Qj1||V||),d=h(RSIDj||pwi||IDi||t) $\oplus$ V
and stores {RSIDj,d,CIDi,t}.
So at the end , the smart card would calculates the session key SK= h($T_{r_i}(Q_{j1})$ ||RSIDj).

Step 7:

Ui g RSj: {Ri}
The card sends {Ri} to the RSj.

Step 8:

Remote server first checks whether

Ri=h(RSIDj||Qi1||Qj1||h(CIDi||Bj||t)|| $T_{r_j}(Q_{i1})$).

If this condition get true , RSj might get calculates the session key SK= h($T_{r_i}(Q_{j1})$ ||RSIDj).

4.4 Login phase on a subsequent login

After Ui has completed the login verification process to the RSj, Ui might get login to RSj and by doing zero interaction with the remote server. This technique can escape the blockage of the remote server. We define in the succeeding login procedure as following. Ui places his card inside a reader and key in his identity IDi, password PWi and the identity RSIDj.

Step 1:
The card calculates h(IDi||pwi) and confirms either it is equivalent to the kept d2. So if these two values are equivalent then it will remain continue to the next phase and if not equal then process might end there.

Step 2:
The smart card calculates V = d $\oplus$ h(RSIDj||pwi||IDi||t) .
Then it might select ri and computes
Qi1 mod p, X1=V Qi1, X2=h(CIDi||RSIDj||Qi1||X1).

Step 3:
Smart card ?RSUj: {CIDi, t, X1, X2}
The request {CIDi, t, X1, X2} is sent to RSj.

4.5 Authentication and key agreement phase on a subsequent login

Step 1:

As the message get arrived {CIDi, t, X1, X2}, Sjwould confirm either it is authentic.

If true, Sj calculates Qi1*=h(CIDi||Bj||t) X1. Then RSj checks whether X2=h(CIDi||RSUIDj||Qi1*||X1).

Step 2:
If the given condition becomes true, RSj select an arbitrary value and computes

Qj1 $\equiv T_{r_j}(x)$ mod p,Y1= h(Qi1*|| h(CIDi||Bj||t)) $\oplus$ Qj1,

Y2=h(Qj1|| Qi1*|| h(CIDi||Bj||t)||Y1|| $T_{r_j}(Q_{i1})$).

Step 3:
RSUj g Ui: {Y1, Y2}

Step 4:
The smart card first calculates Qj1*= h(Qi1*||h(CIDi||Bj||t)) $\oplus$ Y1 and checks whether

Y2= h(Qj1*||Qi1|| h(CIDi||Bj||t)||Y1|| $T_{r_i}(Q_{j1}^{*})$).
However if the condition become true, the smart card calculates V= R $\oplus$ $T_{r_i}(Q_{j1})$
Ri=h(RSIDj||Qi1||Qj1*||h(CIDi||Bj||t)||Y1|| $T_{r_i}(Q_{j1}^{*})$).

At the end, the card will calculates the session key SK= h($T_{r_i}(Q_{j1}^{*})$ ||RSIDj).

Step 5:
Ui g RSUj: {Ri}

Step 6:
The service remote server checks whether the equality holds

Ri=h(RSIDj||Qi1||Qj1||h(CIDi||Bj||t)||Y1|| $T_{r_j}(Q_{i1})$).

If the condition become true, Sj would calculates the session key SK= h($T_{r_j}(Q_{i1})$ ||RSIDj).

4.6 Password change phase

If U_i needs o get alter his password, U_i would place the smart card into machine, then key in the identity ID_i and previous password pw_i. And U_i would rise an apprise demand. Then the card calculates d2*=h(IDi||pwi) and checks whether d2* equals to the stored d2. If they are not equal, it terminates. Otherwise, it accepts the update request. Ui chooses a new password pwi new. Then the smart card computes

d1new = d1 $\oplus$ h(pw_i||ID_i) $\oplus$ h(pw_i new ||ID_i),d2 new =h(ID_i||pw_i new),
and replaces { d1,d2 } with {d1new ,d2 new}.

4.7 Revocation phase

The stole of smart card, U_i could request S for its revocation. S verifies the user's credentials and checks whether d0=h(pw_i||ID_i) N. Next, U_i sends {ID_i, d0} is in the registration table. We note that pw_i is the original password in the registration phase. If d0is valid, S delete U_i's registration information including d0 in the registration table. Ui can change his/her IDior ? pw_i.

5. SECURITY ANALYSIS

In this scenario, we are going to analyze and design a technique which is related to security and that is going to prove various security properties. Following are the advantages of our scheme over others.

5.1 Mutual Authentication

According to our technique, it has to be assume that the remote server and Local Server are jointly authenticated. However in our authentication process, remote server would be responsible to authenticate Mu ; in turns, remote server would help Local Server and LBSs to verify each other. Our perceptive is depends upon BAN logic to confirm that the given technique is going to provide mutual verification forMc-remote server

andMU-local server.
However, Muis clear to know that the value of r is new. By receiving m_4, it validates $V_2 = h(r'_2 \| SR^{*\prime} \| SR \| aP.x \| ID_{BTS})$. However If V_2 comes to be legal, Mu beliefs that V_2 will comes from remote server moreover it is only remote server who can calculate $SR = h(r \| s)$by using its long-term secrets. Because ID_ is in V_2, Mu also beliefs that Local Server is honest. At this stage, Mu and remote server would have confidence that their correspondent is authentic. As the remote server would support local server to validate Mu, both Local Server and Mc would also jointly validated.

5.2 Perfect Forward Secrecy

Our proposed technique will uses ECDH (Elliptic Curve Diffie-Hellman) to deliver flawless forward privacy. remote server and Local Server would responsible to calculate the session key $K_{MF}=h(abP.x)$, However a,bwould be spawned newly for each session. Moreover it does not looks good to derive either a or b from aPandbP, respectably. So by considering the ECDH, It can be inferred that it would be computationally hard problem to speculateab P to provide aPandbP. Nevertheless, there is no attacker who can deduce the session key K_{MF} for any given session even though after conceding long-term secrets of Mcand remote server .

5.3 Achieve Anonymity

According to our protocol, There has been remote server authenticates Mu by authenticating its $PID_{MU} = h(ID_{MU} \| b_2)$. However the values in the given message m_2 from LOCAL SERVER to remote server may not contain ID_{MU}, however it only contains its hash value PID_{Mu} inDID_{Mu}. Moreover the secure hash function is being used, so it's very difficult for LBSs to reveal ID_{MU} from PID_{MU}. Nevertheless, ID_{MU} will never be directed in the form of plaintext. While only PID_{MC} would be directed over uncertain channel in $DID_{MU} = PID_{MU} \oplus h(r \| s)$. However it would be bit difficult for Remote server or an snooping antagonistA to develop ID_{MU} from DID_{MU}.

5.4 Attain Untraceability

By the end of the verification phase,r has been allocated a fresh value $r^* = r_1 \oplus r_2$, while r1, r2 are newly spawned by Mu and remote server server , correspondingly; However it would lead to the conversion of $h(r \| s)$ and $DID_{MU}=PID_{MU} \oplus h(r \| s)$. Therefore, the values that are being generated from Mu may not remain the same. However, LOCAL SERVER and Amight not know either the information from two different sessions originates from the identical Mu or not.

5.5 To Restrain Revelation of User's Password

In our given scheme, the client's password would only need to calculate PW_{MU} = h(pw_{MU} || b_1), and hence there might not be any critical information which is associated with PW_{MU} by any message sent from Mu. Moreover no invader might get PW_{MU} by snooping the communication channel.

5.6 To Restrain Man-in-the-middle Attack

In previous scheme there might be different loopholes and it might suffer because of multiple kinds of man-in-the-middle attacks and it does not verify aP and bP properly. However in our technique,Mcwill have to be confirm that aPmust originates from BTS, and Local Server must have to authenticate that bPmust originates fromMc. However remote server would deliver Local Server by V3=h(r || r*)So that it might get verified by bP. Moreover when m_4would be received fromMu, hence Local Server would calculate the session key K_{MF} and might practicesV_3 to validate it by making comparisons withh(K_{MF} || V3)contrary to the acquired value of C_{MF}. Moreover when mobile client is considered, then smart card might get authenticateaP since aP.x is confined in V2 = h(r2 || SR* || SR || aP.x || ID_{FA}) that would be directed from LBSs. However If Mu and remote server would already get validated, ThenMuwould be sure that aP indeed comes from Local Server.

5.7 To restrain Replay Attack

During this scenario for each session the values r, r1, r2, a,b being created, however the parameter values of all messages are associated to them. Moreover these values might get authenticated by Mu, LOCAL SERVER, and remote server; while an attacker would not cheat any authentic user by restating old messages.

5.8 To Restrain Stolen Verifier Attack

In this scenario an invaderAhave conciliations with remote server server 's catalogue, however it might acquire DID_{MU} =PID_{MU} $\oplus$ h(r || s), and VID_{MU} = h(r || PID_{MU}). Moreover, if LBS unable to have long-term secret s , it will unable to calculate SR=h(r || s) which might be used in calculating R2, V2. So it might be get difficult to pretense as local serveras it might do in previous scheme.

5.9 To Restrain Smart Card Lost Attack

During this scenario if user Awould acquire a authentic smart card of ID_Mu, Then is able to recover b1, b2, randP SR=h(r | $\oplus$) PW_{MU}, wherever PW_{MU} =h(PW_{MU} || b1). However the invader may not have information of PW_{MU} to calculate PW_{MU}. Until it does not have password, Amight notoriginate SR=h(r || s)that might play an important role in validation. So by misplacing smart card might not compromise the safety of the system.

	Khan et al.[11]	Wang et al.[12]	Wen et al.[13]	Ours
User anonymity	Yes	No	Yes	Yes
Prevention of insider attack	No	Yes	Yes	Yes
Prevention of impersonation attack	No	No	Yes	Yes
No password table	Yes	Yes	Yes	Yes
Communication overhead	High	High	Low	Low
Session key establishment	Yes	No	Yes	Yes
Session key is updated periodically	No	No	Yes	Yes
Energy consumption	Low	High	Low	Low
Prevention of fraud	Yes	Yes	Yes	Yes
Prevention of replay attack	Yes	No	Yes	Yes
highly efficient in password authentication	Yes	No	No	Yes
Single registration	Yes	Yes	Yes	Yes
No verifier table	Yes	Yes	Yes	Yes
The password is changed by the user freely	Yes	Yes	Yes	Yes
The password is chosen by the user freely	No	No	No	Yes
Providing the authentication scheme when a user is located in his/her local server	Yes	No	No	Yes
Secrets update	No	No	Yes	Yes
Revocation	No	No	Yes	Yes
Security	No	No	No	Yes

Table 1: Security Comparison

Schemes	Computation cost on user side
Khan et al.[11]	$10th + 3t_{sym}$
Wang et al.[12]	$6th + 2t_{sym}$
Wen et al.[13]	$5th + t_{sym}$
Ours	$8th + 2t_{se} + t_{mexp}$

Table 2: Performance Comparison

6.PROPOSED SECURITY AND PERFORMANCE ANALYSIS ARCHITECTURE

We have conclude the main safety structures of our technique and have compared its robustness and security features with khan et al, Wang et al.'s and Wen et al schemes. However after having a detail analysis it has been revealed that our technique is much more authentic and robust than the other schemes proposed in literature. However n Table 2 it has been evident that our scheme require hashing operation fewer than Khan et al.'s scheme since our technique might present privacy and session key calculation which must need extra processes to increase the safety of the application. Moreover it can also be inferred that the calculation overhead and communication cost of the given scheme is much better than the other schemes in terms of boosted security structures which are essential for fulfilling a consistent and truthful remote user verification system.

CONCLUSIONS

Researcher has discovered certain drawbacks in terms of security and robustness in recently proposed smart card based verification schemes for wireless communication environments. Moreover an authentic and robust scheme has been proposed in order to falsify the issues in terms of security and robustness in smart card systems. Our proposed scheme based on dynamic ID based remote user password authentication key agreement system, Moreover the Performance and security analysis has revealed that our given technique is much more authentic against multiple attacks, and it is evident from the results that it is best solution for wireless communication environments.

ACKNOWLEDGMENT

We are finally thankful to the editor, reviewers and IBT especially who provided us with the opportunity to publish our research paper in this esteemed journal.

REFERENCES

Imran Memon. (2015) authentication user's privacy: an integrating location privacy protection algorithm for secure moving objects in location based services. wireless pers, commun DOI,pp.121-125.

Mohammad Sabzinejad Farash, Mahmoud AhmadianAttari.(2014) Cryptanalysis and improvement of a chaotic map-based key agreement protocol using Chebyshev sequence membership testing. Nonlinear Dynamics,Volume 76, Issue 2, pp 1203-1213.

Zhu, J., & Ma, J. (2004) A new authentication scheme with anonymity for wireless environments. IEEE Transactions on Consumer Electronics, 50(1), Volume 76, Issue 2, pp 1203-1213

Lee, C.-C., Hwang, M.-S., & Liao, I.-E.(2006) Security enhancement on a new authentication scheme with anonymity for wireless environments, IEEE Transactions on Industrial Electronics, 53(5),pp.1683–1687.

Hongfeng Zhu, XinHao.(2000) A provable authenticated key agreement protocol with privacy protection using smart card based on chaotic maps.Nonlinear Dynamics,pp.48.

Chia-Chun, W., Lee, W.-B., &Tsaur, W.-J.(2008) A secure authentication scheme with anonymity for wireless communications,IEEE Communications Letters, 12(10), pp.722–723.

Jing, X., & Feng, D. (2009) Security flaws in authentication protocols with anonymity for wireless environments, ETRI Journal, 31(4), pp.460–462.

Lee, J.-S., Chang, J. H., & Lee, D. H. (2009) Security flaw of authentication scheme with anonymity for wireless communications, IEEE Communications Letters, 13(5), pp.292–293.

Wang, C.-H., Wei, T.-C., Lee, P.-C., & Wu, C.-C.(2009) An improvement of secure authentication scheme with full anonymity for wireless communications. In Proceedings of the 2nd international conference on interaction sciences: information technology, culture and human, ACM. ,pp. 115–118,

Jeon, W., Kim, J., Lee, Y., & Won, D.(2012)Security analysis of authentication scheme for wireless communications with user anonymity. In Information technology convergence, secure and trust computing, and data management, Berlin: Springer, pp. 225–231.

Khan MK, Kim SK, Alghathbar K.(2011) Cryptanalysis and security enhancement of a 'more efficient and secure dynamic ID-based remote user authentication scheme'. Computer Commun;34(3),pp.305–309.

Wang YY, Liu JY, Xiao FX, Dan J.(2009) A more efficient and secure dynamic ID-based remote user authentication scheme, Computer Commun volume4 (32), pp.583–585.

Fengtong Wen, XueleiLi.(2012)An improved dynamic ID-based remote user authentication with key agreement scheme, Computers and Electrical Engineering volume38, pp. 381–387.

C.C. Lee, M.S. Hwang, I.E. Liao.(2006) Security enhancement on a new authentication scheme with anonymity for wireless environments, IEEE Transactions on Consumer Electronics 53 (5) ,pp. 1683–1687.

Qi Xie, Bin Hu, Ting Wu. March .(2015) Improvement of a chaotic maps-based three-party password-authenticated key exchange protocol without using server's public key and smart card, Nonlinear Dynamics ,Volume 79, Issue 4, pp 2345-2358.

Imran Memon , Ling Chen ,Abdul Majid ,Mingqi Lv , Ibrar Hussain, Gencai Chen.(2015) Travel Recommendation Using Geo-tagged Photos in Social Media for Tourist, Wireless Personal Communications, pp.1347-1362.

Imran Memon , Mohammed Ramadan Mohammed , Rizwan Akhtar ,Hina Memon , Muhammad Hammad Memon , Riaz Ahmed Shaikh.(2014) Design and Implementation to Authentication over a GSM System Using Certificate-Less Public Key Cryptography (CL-PKC).Wireless Pers Commun volume.79,pp.661–686.

Su R, Cao ZF.(2010) An efficient anonymous authentication mechanism for delay tolerant networks, Computer Electrical Eng volume (36), pp.435–41.

David Basin, CasCremers.(2014) Know Your Enemy: Compromising Adversaries in Protocol Analysis. Transactions on Information and System Security (TISSEC) , Volume 17 Issue 2,pp.29.

Cheng-Chi Lee, Der-Chyuan Lou, Chun-Ta Li, Che-Wei Hsu. April (2014) An extended chaotic-maps-based protocol with key agreement for multi-server environments, Nonlinear Dynamics, Volume 76, Issue 1, pp. 853-866.

Philipp Richter, Mark Allman, Randy Bush, Vern Paxson. (2015) A Primer on IPv4 Scarcity, SIGCOMM Computer Communication Review , Volume 45 Issue

2,pp.39-45.

Johannes Götzfried, TiloMüller.Mutual. (2014) Authentication and Trust Bootstrapping towards Secure Disk Encryption, Transactions on Information and System Security (TISSEC) , Volume 17 Issue 2,pp.789-810.

Florian Bergsma, Benjamin Dowling, Florian Kohlar, JörgSchwenk, Douglas Stebila.(2014) Multi-Ciphersuite Security of the Secure Shell (SSH) Protocol.CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security,pp.41-48.

KadhimHayawi, AlirezaMortezaei, Mahesh V. Tripunitara.(2015) The Limits of the Trade-Off Between Query-Anonymity and Communication-Cost in Wireless Sensor Networks, CODASPY '15: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy Ziming Zhao, Gail-JoonAhn, HongxinHu. Picture Gesture Authentication: Empirical Analysis, Automated Attacks, and Scheme Evaluation, Transactions on Information and System Security (TISSEC), Volume 17 Issue 4, pp.30.

MalihehShirvanian, NiteshSaxena. (2014) Wiretapping via Mimicry: Short Voice Imitation Man-in-the-Middle Attacks on Crypto Phones.CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security,pp.90-95.

Jiliang Zhang, Yaping Lin,(2015) Gang Qu.Reconfigurable Binding against FPGA Replay Attacks.Transactions on Design Automation of Electronic Systems (TODAES) , Volume 20 Issue 2,pp.45.

Arpan Roy, SantonuSarkar, RajeshwariGanesan, GeetikaGoel.(2015)Secure the Cloud: From the Perspective of a Service-Oriented Organization.Computing Surveys (CSUR) , Volume 47 Issue 3,pp.954-956.

Yong Wang, Yun Xia, JieHou , Shi-mengGao , Xiao Nie , Qi Wang.(2015) A fast privacy-preserving framework for ontinuouslocation-based queries in road networks, Journal of Network and Computer Applications, pp.5357–73.