文章编号：2096-1472(2016)-10-04-04

多服务器间基于动态身份的身份认证和密钥共识方案

王 牧，亢保元，景东亚
（天津工业大学计算机科学与软件学院，天津 300387）

摘 要：多数的身份认证方案是依赖于单个的认证服务器与用户之间的相互认证，如果一个用户想要使用不同的网络服务，就必须向每一个服务器进行注册。然而要使得用户记住不同的身份和口令是非常困难的。最近，Li et al.分析了Sood et al.提出的多服务器间基于动态身份的认证方案，指出了其中存在的问题并且提出了一个改进的方案。Li et al.声称他们的方案可以保证用户的匿名性，提供了相互认证和共享密钥，并且可以抵抗一些常见的攻击。然而，通过仔细分析之后，我们发现Li et al.的方案容易受到假冒攻击。因此，本文提出了一种高效安全的多服务器间基于动态身份的相互认证和密钥共识方案并给出了安全性分析。

关键词：身份认证；密钥共识；多服务器；安全性
中图分类号：TP393 **文献标识码**：A

An Dynamic Identity Based Authentication and Key Agreement Protocol for Multi-Server Architecture

WANG Mu,KANG Baoyuan,JING Dongya
(*School of Computer Science and Software Engineering*,*Tianjin Polytechnic University*,*Tianjin* 300387,*China*)

Abstract: Most of the authentication protocols rely on the mutual authentication of the single authentication server and the user.If a user wants to use numerous different network services,he/she has to register himself/herself to every service-providing server.In order to solve this problem,various multi-server authentication protocols have been proposed.After analyzing the protocol proposed by Sood et al.,Li et al. pointed out the problems,proposed a new protocol and claimed that the new protocol can provide user with anonymity,mutual authentication,session key agreement and resistance to several common attacks.However,through careful analysis,the paper finds that Li et al.'s protocol is still vulnerable to the impersonation attack.Therefore,the paper proposes an efficient and secure dynamic identity based authentication and key agreement protocol for multi-server architecture,along with security analysis.

Keywords:identity authentication;key agreement;multi-server architecture;security

1 引言(Introduction)

智能卡因为具有低能耗，易携带等特点，已经被广泛应用于电子商务和网络安全协议中。用户把智能卡插入读卡器并提交他的身份和口令，智能卡就可以通过处理这些信息来验证用户的合法性。

随着网络和电子商务技术的发展，许多通过网络提供的服务，比如网上购物，网上缴费等等使得我们的生活越来越便捷。在公共环境中，如何在远程用户连接到服务器之前确认用户的身份显得至关重要。大多数的口令认证协议都是基于一个服务器，这个服务器保存了用户的口令认证信息等。口令认证信息存储在单一的服务器中就会很容易受到泄露或者篡改攻击。多服务器模型的提出很好地解决了这些问题。多服务器模型具有把用户的口令和认证功能分配给不同的服务器的灵活性，因此多服务器模型更具有实际意义。

口令认证在认证方案中是最简单最常见的认证方法，近年来人们提出了很多基于静态身份的口令认证方案来加强安全性和高效性，然而用户可以改变他的口令却不能改变他的身份信息。因此，在通信中，基于静态身份的口令认证协议会泄露关于用户的部分认证信息给攻击者。大多数的多服务器间的认证信息也是基于静态身份的，攻击者可以利用这些信息追踪判定不同的消息请求来自于同一批用户。然而，基于动态身份的口令认证方案在身份和口令的基础上提供了双重认证，所以更适合应用于电子商务中。本文提出了多服务器间带有智能卡的基于动态身份的安全高效的认证方案，在不安全的信道中保证了用户的匿名性，因此可以直接应用于电子商务中。

本文的结构为：第二节介绍了多服务器间安全高效的基于动态身份的身份认证和密钥共识方案的国内外研究现状，

基金项目：本论文得到天津市应用基础与前沿技术研究计划支助，编号为No.15JCYBJC15900.

第三节和第四节回顾了Li et al.的方案并对其进行攻击，第五节我们提出了全新的多服务器间安全高效的基于动态身份的身份认证和密钥共识方案，第六节给出了新方案的安全性分析，第七节是本文的结束语。

2 相关工作(Related work)

Lamport[1]在1981年首先提出了不安全的网络环境中的远程口令认证协议，然而在他提出的协议中，服务器必须存储口令表，这就使得这个协议不能抵抗篡改攻击。Hwang和Li[2]2000年提出了基于ElGamal算法的带有智能卡的远程认证方案，这个方案不要求服务器存储口令表。此后，人们提出了大量带有智能卡的单一服务器认证方案来解决安全性问题(Fan et al.[3],2005；Hwang et al.[4],2010；Lee et al.[5],2005；Li和Hwang[6],2010；Li et al.[7],2011)。

然而，当用户想使用单一的服务器认证协议登录不同的远程服务器时，记住许多不同的口令和身份是很困难的。为了解决这个问题，Li et al.[8]提出了基于神经网络的远程认证协议，这个协议可以适用于多服务器的网络体系，但是这个协议需要巨大的运算量。2004年，Juang[9]提出了一个高效的基于哈希函数的多服务器认证协议。同年，Chang和Lee[10]指出Juang的方案不够高效因为服务器和用户仍需要进行大量的运算和记忆，而且一旦智能卡丢失，这个方案将受到线下猜测攻击。因此Chang和Lee提出了新的远程认证协议，然而他们提出的协议仍然可能受到内部攻击和欺骗攻击。2008年，Tsai[11]提出了一个高效的没有认证表的远程认证方案，这个方案只用到了单向哈希函数计算量小，所以非常适合运用于分布式网络环境中。

然而，以上所有的多服务器间口令认证协议都是基于静态身份的，这就使得攻击者可以追踪到用户的信息。2009年，Liao和Wang[12]提出了多服务器间基于动态身份的远程认证协议，他们声称他们的方案可以抵抗各种攻击并能共提供相互认证。2009年，Hsing和Shih[13]对Liao和Wang提出的方案进行了改进。2011年，Sood et al.[14]指出Hsing和Shih的方案容易受到重放攻击，假冒攻击和智能卡丢失攻击并提出了新方案来解决这些问题。2012年,Li et al.[15]指出Sood et al.的方案容易受到智能卡丢失攻击和信息泄露攻击，也提出了新的方案，他们声他们的方案可以抵抗各种各样的攻击，即使是智能卡丢失，攻击者提取出智能卡中保存的信息，这个方案也是安全的，因为攻击者不可能得到秘密参数 的信息。经过仔细分析，我们发现Li et al.的方案仍然容易受到假冒攻击，因此，本文提出了一个新的多服务器间基于动态身份的认证方案。

3 Li et al.方案的回顾(Overview of Li et al.'s scheme)

本文用到的相关参数如表1所示。我们先回顾Li et al.提出的多服务器间基于动态身份的认证方案。在这个方案中有三个参与者：提供服务的服务器S_j，控制服务器CS和用户U_i。假设控制服务器相当于一个可信的第三方负责用户的注册和相互认证。控制服务器拥有私钥x和一个秘密参数y，当提供服务的服务器S_j用他的身份SID_j向控制服务器注册的时候，控制服务器计算$h(SID_j \| y)$和$h(x \| y)$，并把$h(SID_j \| y)$和$h(x \| y)$通过安全信道提交给提供服务的服务器。方案分为四个阶段：注册阶段、登录阶段、认证和密钥共识阶段、口令改变阶段。

表1 相关参数

Tab.1 Related parameters

符号	含义	符号	含义
U_i	第i个用户	S_j	第j个提供服务的服务器
ID_i	控制服务器	ID_i	用户U_i的身份
P_i	用户U_i的口令	SID_j	S_j的身份
y	CS选取的秘密参数	x	CS的私钥
b	用户注册阶段选取的随机数	CID_i	用户生成的动态身份
SK	共享密钥	N_{i1}	用户智能卡生成的随机数
N_{i2}	随机数	N_{i3}	随机数
$h(\cdot)$	单向哈希函数	$\oplus$	模二加运算
$\|$	级联运算		

4 Li et al.方案的安全性分析(The protocol analysis)

尽管Li et al.声称他们的方案可以抵抗各种各样的攻击，即使是智能卡丢失，攻击者提取出智能卡中保存的信息，这个方案也是安全的，因为攻击者不可能得到x,y的信息。经过仔细分析，我们发现实际情况却不是这样。

4.1 用户假冒攻击

我们假设有一个恶意的用户U_k拥有一个智能卡并提取出智能卡里的信息$(C_k,D_k,E_k,h(\cdot),h(y),b_k)$，这个恶意用户$U_k$根据自己的$ID_k,P_k$可计算出$A_k=h(b_k \| P_k)$，$B_k=D_k \oplus h(ID_k \| A_k)$，从而得出$h(y \| x)=E_k \oplus B_k$。如果一个合法用户$U_i$的智能卡被$U_k$盗取，$U_k$就可以提取出其中的$(C_i,D_i,E_i,h(\cdot),h(y),b)$，当这个恶意用户$U_k$拦截到用户发送的$F_i,CID_i$，就可以计算$N_{i1}=F_i \oplus h(y)$，$B_i=E_i \oplus h(y \| x)$，$A_i=CID_i \oplus h(B_i \| F_i \| N_{i1})$利用这些数据，这个恶意用户$U_k$就可以伪造用户$U_i$的登录信息。首先，$U_k$生成一个随机数$N_{i1}'$，计算$F_i'=h(y) \oplus N_{i1}'$，$P_{ij}'=E_i \oplus h(h(y) \| N_{i1}' \| SID_j)$，$CID_i'=A_i \oplus h(B_i \| F_i \| N_{i1}')$，$G_i'=h(B_i \| A_i \| N_{i1}')$。智能卡把登录请求$(F_i',G_i',P_{ij}',CID_j')$通过公共信道发送给提供服务的服务器$S_j$。收到$U_k$发来的登录

请求之后，S_j选择一个随机数N_{i2}，计算$K_i = h(SID_j \| y) \oplus N_{i2}$，$M_i = h(h(x \| y) \| N_{i2})$，并把信息$(F_i', G_i', P_{ij}', CID_i', SID_j, K_i, M_i)$发送给控制服务器$CS$。当控制服务器$CS$收到登录请求$(F_i', G_i', P_{ij}', CID_i', SID_j, K_i, M_i)$之后，计算$N_{i2} = K_i \oplus h(SID_j \| y)$，$M_i' = h(h(x \| y) \| N_{i2})$并验证$M_i'$等于收到的$M_i$。于是控制服务器$CS$计算$N_{i1}' = F_i' \oplus h(y)$，$B_i = P_{ij}' \oplus h(h(y) \| N_{i1}' \| SID_j) \oplus h(y \| x)$，$A_i = CID_i' \oplus h(B_i \| F_i' \| N_{i1}')$，$G_i'' = h(B_i \| A_i \| N_{i1}')$，并验证$G_i''$等于$G_i'$，控制服务器可以确认用户$U_i$的合法性。综上，恶意用户$U_k$可以进行用户假冒攻击。

4.2 服务器假冒攻击

按照上述做法，这个恶意用户U_k可以计算出N_{i1}, A_i, B_i，当他拦截到提供服务的服务器S_j发给用户U_i的消息(V_i, T_i)之后，U_k计算$V_i' = h(h(A_i \| B_i) \| h(N_{i1} \oplus N_{i2}' \oplus N_{i3}'))$，$T_i' = N_{i2}' \oplus N_{i3}' \oplus h(A_i \| B_i \| N_{i1})$，用户收到信息$(V_i', T_i')$之后计算$N_{i2}' \oplus N_{i3}' = T_i' \oplus h(A_i \| B_i \| N_{i1})$，$V_i'' = h(h(A_i \| B_i) \| h(N_{i1} \oplus N_{i2}' \oplus N_{i3}'))$，并验证$V_i''$等于$V_i'$，智能卡就可以确认控制服务器$CS$和提供服务服务器的合法性。所以恶意用户可以进行服务器假冒攻击。

5 改进的新方案(The proposed scheme)

在这一节，我们提出了一个安全高效的方案，来解决Li et al.方案中的问题。我们的方案同样包括三个参与者，用户U_i、提供服务的服务器S_j、控制服务器CS。控制服务器CS选取一个大素数p，g是Z_p^*的生成元，选取私钥$x \in Z_{p-1}^*$，公钥$y_{CS} = g^x \bmod p$。我们的方案同样分为四个步骤：注册阶段、登录阶段、认证和密钥共识阶段、口令改变阶段。相关步骤如图1所示。

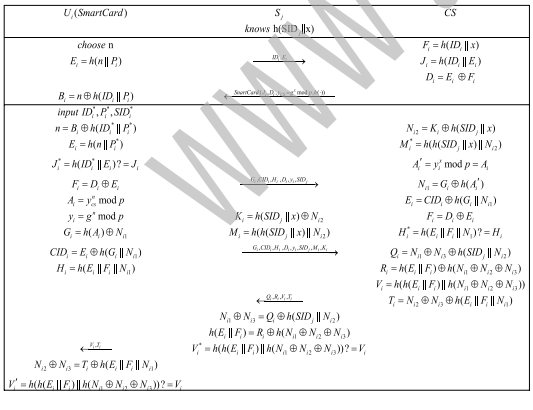

图1 新的方案

Fig.1 New scheme

5.1 注册阶段

用户U_i首先要向控制服务器CS进行注册，注册阶段都是在安全信道中进行。

Step1：用户U_i选取一个随机数n，计算$E_i = h(n \| P_i)$，然后把ID_i, E_i通过安全信道提交给CS。

Step2：控制服务器CS收到ID_i, E_i之后计算$F_i = h(ID_i \| x)$，$J_i = h(ID_i \| E_i)$，$D_i = E_i \oplus F_i$，CS把$(J_i, D_i, g, y_{CS}, h(\cdot))$存储在智能卡中并把智能卡通过安全信道颁发给用户。

Step3：当用户收到智能卡之后计算$B_i = n \oplus h(ID_i \| P_i)$，并把$B_i$保存在智能卡中。最终智能卡存储了$(J_i, D_i, B_i, g, y_{CS}, h(\cdot))$。

提供服务的服务器S_j也要在控制服务器CS进行注册。当S_j用它的身份SID_j向控制服务器注册的时候，CS计算$h(SID_j \| x)$，然后把$h(SID_j \| x)$通过安全信道提交给S_j保存。

5.2 登录阶段

Step1：用户U_i把智能卡插入读卡器中并输入ID_i^*和口令P_i^*以及提供服务的服务器S_j的身份SID_j，智能卡计算$n = B_i \oplus h(ID_i^* \| P_i^*)$，$E_i = h(n \| P_i^*)$，$J_i^* = h(ID_i^* \| E_i)$，并验证$J_i^* ?= J_i$，如果上式成立，就说明$U_i$是一个合法用户。

Step2：验证成功之后，智能卡生成一个随机数N_{i1}，并且计算$F_i = D_i \oplus E_i$，$A_i = y_{CS}^n \bmod p$，$y_i = g^n \bmod p$，$G_i = h(A_i) \oplus N_{i1}$，$CID_i = E_i \oplus h(G_i \| N_{i1})$，$H_i = h(F_i \| E_i \| N_{i1})$，于是智能卡把登录请求$(G_i, H_i, D_i, y_i, CID_i)$通过公共信道发送给$S_j$。

5.3 认证和密钥共识阶段

Step1：收到登录请求之后，S_j选取一个随机数N_{i2}，计算$K_i = h(SID_j \| x) \oplus N_{i2}$，$M_i = h(h(SID_j \| x) \| N_{i2})$，之后$S_j$把登录请求$(G_i, H_i, D_i, y_i, CID_i, SID_j, M_i, K_i)$发送给控制服务器。

Step2：当收到登录请求$(G_i, H_i, D_i, y_i, CID_i, SID_j, M_i, K_i)$后，$CS$开始计算$N_{i2} = K_i \oplus h(SID_j \| x)$，$M_i' = h(h(SID_j \| x) \| N_{i2})$，并且验证$M_i'$是否等于$M_i$，如果验证相等，$CS$可以确认$S_j$的合法性。否则$CS$终止这次请求。

Step3：控制服务器CS计算$A_i' = y_i^x \bmod p = A_i$，$N_{i1} = G_i \oplus h(A_i')$，$E_i = CID_i \oplus h(G_i \| N_{i1})$，$F_i = D_i \oplus E_i$，$H_i^* = h(E_i \| F_i \| N_{i1})$，验证$H_i^*$是否等于$H_i$，如果验证等式成立，$CS$认为用户的身份合法，否则$CS$拒绝这次请求。

Step4：控制服务器CS生成一个随机数N_{i3}计算$Q_i = N_{i1} \oplus N_{i3} \oplus h(SID_j \| N_{i2})$，$R_i = h(E_i \| F_i) \oplus h(N_{i1} \oplus N_{i2} \oplus N_{i3})$，$V_i = h(h(E_i \| F_i) \| h(N_{i1} \oplus N_{i2} \oplus N_{i3}))$，$T_i = N_{i2} \oplus N_{i3} \oplus h(E_i \| F_i \| N_{i1})$，控制服务器$CS$把$(Q_i, R_i, V_i, T_i)$作为相互认证的信息发给$S_j$。

Step5：提供服务的服务器S_j收到控制服务器CS发送来的信息(Q_i, R_i, V_i, T_i)，计算$N_{i1} \oplus N_{i3} = Q_i \oplus h(SID_j \| N_{i2})$，$h(E_i \| F_i) = R_i \oplus h(N_{i1} \oplus N_{i2} \oplus N_{i3})$，$V_i' = h(h(E_i \| F_i) \| h(N_{i1} \oplus N_{i2} \oplus N_{i3}))$，并验证$V_i'$是否等于$V_i$。如果验证上述式子不成立，$S_j$就拒绝这次访问。如果验证上述等式成立，$S_j$就可以确认控制服务器$CS$的合法性，并且$S_j$把$(V_i, T_i)$传送给用户。

Step6：用户收到(V_i, T_i)之后计算$N_{i2} \oplus N_{i3} = T_i \oplus h(E_i \| F_i \| N_{i1})$，

$V_i' = h(h(E_i \| F_i) \| h(N_{i1} \oplus N_{i2} \oplus N_{i3}))$，并验证$V_i'$是否等于$V_i$，如果验证不相等，智能卡就拒绝这次访问。如果验证相等，智能卡就可以确认提供服务的服务器和控制服务器的合法性。

最终，用户U_i，提供服务服务器S_j，控制服务器CS达成了一个共享密钥$SK = h(h(E_i \| F_i) \| (N_{i1} \oplus N_{i2} \oplus N_{i3}))$。相关步骤如图1所示。

5.4 口令改变阶段

当用户U_i想要改变口令的时候触发这个阶段，这个阶段不需要控制服务器CS的参与。用户U_i把智能卡插入读卡器并输入身份ID_i^*和口令P_i^*，智能卡计算$n = B_i \oplus h(ID_i^* \| P_i^*)$，$E_i = h(n \| P_i^*)$，$J_i^* = h(ID_i^* \| E_i)$，并验证$J_i^* ?= J_i$，如果等式成立，用户就可以提交一个新的口令$P_i^{new}$，智能卡计算$E_i^{new} = h(n \| P_i^{new})$，$J_i^{new} = h(ID_i \| E_i^{new})$，$B_i^{new} = n \oplus h(ID_i \| P_i^{new})$，$D_i^{new} = F_i \oplus E_i^{new}$并把$J_i^{new}, B_i^{new}, D_i^{new}$存储在智能卡中替换$J_i, B_i, D_i$。

6 改进方案安全性分析(The proposed protocol analysis)

在我们提出的方案中，即使智能卡中的信息被攻击者提取出来，攻击者也不能利用这些信息成功攻击这个方案，下面是安全性分析的具体细节。

6.1 假冒攻击

在这种攻击中，攻击者需要伪造一个登录请求$(G_i, H_i, D_i, y_i, CID_i)$来假冒合法用户，然而攻击者并不能计算

$$G_i = h(A_i) \oplus N_{i1},\ H_i = h(F_i \| E_i \| N_{i1}),$$

$$D_i = E_i \oplus F_i,\ CID_i = E_i \oplus h(G_i \| N_{i1}),$$

因为攻击者并没有A_i、E_i、F_i。

我们假设用户U_i的智能卡丢失，攻击者可以提取出智能卡中的信息$(J_i, D_i, B_i, g, y_{CS}, h(\cdot))$，但是攻击者得不到$x$，也不能得到用户的$ID_i$、$P_i$、$n$，所以攻击者计算不出$A_i = y_{CS}^n \bmod p$，$E_i = h(n \| P_i)$，$F_i = D_i \oplus E_i$，也就不能利用得到的智能卡进行假冒攻击。

6.2 重放攻击

假设攻击者截获到用户和服务器之间的信息，想要把截获到的信息再次发送给服务器来假冒合法用户。然而，用户计算$G_i = h(A_i) \oplus N_{i1}$，$CID_i = E_i \oplus h(G_i \| N_{i1})$，$H_i = h(F_i \| E_i \| N_{i1})$，控制服务器$CS$计算$Q_i = N_{i1} \oplus N_{i3} \oplus h(SID_j \| N_{i2}), R_i = h(E_i \| F_i) \oplus h(N_{i1} \oplus N_{i2} \oplus N_{i3})$，$V_i = h(h(E_i \| F_i) \| h(N_{i1} \oplus N_{i2} \oplus N_{i3}))$，$T_i = N_{i2} \oplus N_{i3} \oplus h(E_i \| F_i \| N_{i1})$，$K_i = h(SID_j \| x) \oplus N_{i2}$，$M_i = h(h(SID_j \| x) \| N_{i2})$，提供服务的服务器$S_j$计算$K_i = h(SID_j \| x) \oplus N_{i2}$，$M_i = h(h(SID_j \| x) \| N_{i2})$的时候，每次通信都选取不同的$N_{i1}$、$N_{i2}$、$N_{i3}$以保证每次发送的消息都是不同的，所以重放攻击是无效的。

6.3 用户的匿名性

在注册阶段，用户和控制服务器之间是在安全信道中进行通信，可以保护用户的身份。在登录阶段，用户用$CID_i = E_i \oplus h(G_i \| N_{i1})$代替真正的身份来登录，所以攻击者不能得到真正的$ID_i$。在认证和密钥共识阶段，所有的计算都是在$E_i, F_i$的基础上进行的而不是真正的身份$ID_i$。此外用户每次登录的动态身份$CID_i$包含随机数$N_{i1}$，所以用户每次登录的身份是不同的，因此攻击者不能根据登录请求来判断具体是哪一个用户。

7 结论(Conclusion)

在这篇文章中，我们指出了Li et al.的方案容易在用户智能卡丢失的情况下受到用户的假冒攻击。于是，我们提出了一种新的多服务器间安全高效的基于动态身份的身份认证和密钥共识方案，新方案可以满足多服务器间相互认证和密钥共识方案的安全需求。与Li et al.的方案和其他的相关方案相比，我们的方案中控制服务器没有存用户的储任何信息，即使智能卡丢失，攻击者也无法进行假冒攻击。此外，我们的方案保证了用户在通信过程中的匿名性，并提供了安全的共享密钥，计算量也相对较小，所以我们的方案更安全，更高效。

参考文献(References)

[1] Lamport L.Password Authentication with Insecure Communication[J].Communications of the Acm,1981,24(11):770-772.

[2] Hwang M S,Li L H.A new Remote User Authentication Scheme Using Smart Cards.IEEE Transactions on Consumer Electronics,2000,46(1):28-30.

[3] Fan C I,Chan Y C,Zhang Z K.Improved Remote Authentication Scheme with Smart Card[J].Computers & Security,2005,27(2):177-180.

[4] Hwang M S,Chong S K,Chen T Y.DoS-Resistant ID-Based Password Authentication Scheme Using Smart Cards[J].Journal of Systems & Software,2010,83(1):163-172.

[5] Lee S W,Kim H S,Yoo K Y.Efficient Nonce-Based Remote User Authentication Scheme Using Smart Cards[J].Applied Mathematics & Computation,2005,167(1):355-361.

[6] Li C T,Hwang M S.An Efficient Biometrics-Based Remote User Authentication Scheme Using Smart Cards[J].Journal of Network & Computer Applications,2010,33(1):1-5.

[7] Li X,et al.Cryptanalysis and Improvement of a Biometrics-

Based Remote User Authentication Scheme Using Smart Cards[J].Journal of Network & Computer Applications,2011,34(1):73-79.

[8] Li L H,Lin L C,Hwang M S.A Remote Password Authentication Scheme for Multiserver Architecture Using Neural Networks[J].IEEE Transactions on Neural Networks,2001,12(6):1498-1504.

[9] Juang W S.Efficient Multi-Server Password Authenticated Key Agreement Using Smart Cards.IEEE Transactions on Consumer Electronics[J].IEEE Transactions on Consumer Electronics,2004,50(4):251-255.

[10] Chang C C,Lee J S.An Efficient and Secure Multi-Server Password Authentication Scheme using Smart Cards[C]. Proceedings of the 2004 International Conference on Cyberworlds.IEEE Computer Society,2004:417-422.

[11] Tsai J L.Efficient Multi-Server Authentication Scheme Based on One-Way Hash Function without Verification Table[J]. Computers & Security,2008,27(s3-4):115-121.

[12] Liao Y P,Wang S S.A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment[J]. Computer Standards & Interfaces,2009,31(1):24-29.

[13] Hsiang H C,Shih W K.Improvement of the Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment[J].Computer Standards & Interfaces, 2009,31(6):1118-1123.

[14] Sood S K,Sarje A K,Singh K.A Secure Dynamic Identity Based Authentication Protocol for Multi-Server Architecture[J].Journal of Network & Computer Applications, 2011,34(2):609-618.

[15] Li X,et al.An Efficient and Security Dynamic Identity Based Authentication Protocol for Multi-Server Architecture Using Smart Cards[J].Journal of Network & Computer Applications, 2012,35(2):763-769.

作者简介：

王 牧(1990-)，男，研究生.研究领域：信息安全.

亢保元(1965-)，男，博士，教授.研究领域：信息安全.

景东亚(1990-)，男，研究生.研究领域：信息安全.

(上接第17页)

16-17.

[6] FENG Tao,MURTAGH F,FARID M.Weighted Association Rule Mining Using weighted support and significance framework[C].Proc.of the 9th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining,ACM Press,2003:661-666.

[7] 徐嘉莉,陈佳.基于向量的数据流滑动窗口中最大频繁项集挖掘[J].计算机应用研究,2012,29(3):837-840.

[8] AGRAWAL R,SRIKANT R.Fast Algorithms for Mining Association Rules[C].Proc of the 20th International Conference on Very Large Database.San Francisco:Morgan Kaufmann Publishers,1994:487-499.

[9] 徐建民,郝丽维,王煜.数据流频繁项集的快速挖掘算法[J].计算机工程与应用,2008,44(34):142-144.

作者简介：

马连灯(1992-)，男，硕士，硕士生.研究领域：大数据，数据挖掘.

王占刚(1975-)，男，博士，副教授.研究领域：大数据，计算机检测应用，计算机网络安全.

(上接第49页)

Systems,2015,16(3):1148-1161.

[3] Lee S C,Nevatia R.Hierarchical Abnormal Event Detection by Real Time and Semi-Real Time Multi-Tasking Video Surveillance System[J].Machine Vision & Applications,2014,25(1):133-143.

[4] 陈嘉懿,郑巧英,李鲍.RFID通用数据交换平台建设研究[J].图书情报工作,2014,58(23):97-101.

[5] 任杰.公安信息网边界接入平台的设计与实现[D].中山大学, 2011.

[6] 魏启超.信息系统安全等级保护[C].全国信息安全等级保护技术大会会议,2013.

[7] 王其祥.公安信息通信网边界接入平台的设计与实现[D].厦门大学,2014.

[8] 邓洁霖.政务信息资源交换体系技术概述[J].信息技术与标准化,2005(11):28-32.

作者简介：

周俊鹤(1971-)，男，硕士，工程师.研究领域：计算机应用及网络安全，视频监控应用技术研究.

张晓双(1991-)，女，研究生.研究领域：社交网络.