PERFORMANCE OF MULTI SERVER AUTHENTICATION AND KEY AGREEMENT WITH USER PROTECTION IN NETWORK SECURITY

NAGAMALLESWARA RAO. DASARI[1]
Research Scholar
CSIT Department
St.Mary's College of Engg. & Tech.,
Hyderabad, India.

VUDA SREENIVASARAO[2]
Professor & Head
CSIT Department
St.Mary's College of Engg. & Tech.,
Hyderabad, India.

Abstract: Using smart cards, remote user authentication and key agreement can be simplified, flexible, and efficient for creating a secure distributed computers environment. Addition to user authentication and key distribution, it is very useful for providing identity privacy for users. In this paper, we propose novel multi server authentication and key agreement schemes with user protection in network security. We first propose a single-server scheme and then apply this scheme to a multi-server environment. The main merits include:
(1) The privacy of users can be ensured; (2) a user can freely choose his own password; (3) the computation and communication cost is very low; (4) servers and users can authenticate each other; (5) it generates a session key agreed by the server and the user; (6) our proposed schemes are Nonce-based schemes which does not have a serious time synchronization problem.

Keywords: Network security, privacy protection, session key, smart card, user authentication

1. INTRODUCTION:

For obtaining permitted services by service providers in a network environment, the user must legally login to the provider's server. In general, the user transmits a message of user authentication to the server, and then the server must be able to verify the identity of the user and give him the right of using permitted services. Typically, the user passes a password as a secret token to the server. The server first checks if the user's identity and the password are matching. The server rejects the user's request if his Identity or the password is not matching. If the password is matching, the server give the user the right for using the permitted services. In 1981, Lamport first proposed a password authentication scheme at the both ends of the communication. Since then, many schemes have been proposed to point out its drawback and improve the security and efficiency of Lamport's scheme. Only passing a password for authenticating between the user and the server is not enough, since it is less safety and is easily tapped by the adversary. Before two parties can do secure communication, a session key is needed for protecting subsequence communications. Also, using smart cards, remote user authentication and key agreement can be simplified, flexible and efficient for creating a secure distributed computers environment. It is also useful for providing identity privacy for the users.
In 2004, Juang proposed two efficient authentication and key agreement schemes for single server, and multi server environments. But both Juang's schemes have no ability of anonymity for the user. Yang et. al. Proposed user identification and key distribution scheme with the ability of privacy protection but we point out it is less efficient because of using public-key cryptosystems. For basically security and efficient requirements, the following criteria are important for remote user authentication and key agreement schemes with smart cards.

C1. Privacy protection: When the user authenticates successfully to the server, the adversary can not derive the user's identity.

C2. Freely chosen password: Users can freely chosen and change their passwords for protecting their smart cards.

C3. Low computation and communication cost: Since capacity and communication constrains of smart cards, they may not offer a powerful computation capability and high bandwidth.

C4. Mutual authentication: Servers and users can authenticate each other.

C5. Session key agreement: Servers and users must negotiate a session key for subsequent Communications.

2. AUTHENTICATION:

Authentication systems can be categorized according to the number of identification factors required to ascertain identity.

- Single-factor authentication uses user ID/password combinations to prove identity.
- Two-factor authentication requires two components, usually a combination of something the user knows (Such as a password) and something the user possesses (such as a physical token Secure ID card).
- Three-factor authentication adds a biometric, a measurement of a human body characteristic.

The more authentication factors used, the more secure the process. However, the more factors you add, the more you add complexity, cost, and management overhead. Every scenario will offer a different break-even point in the trade-off between simplicity and security.

Single-factor authentication with user ID and password is the most common authentication system today. It's easy to administer, familiar to users, and can provide a high level of security if strong password procedures are enforced. Legacy password systems have had some challenges, however, since multiple strong passwords are very hard for users to remember. The recommendations in this section will show how this problem can be minimized with a "Single Strong Password" system.

Tokens such as smartcards and Secure ID cards are added as a second factor in many authentication systems—requiring that the user have physical possession of the token. An attacker would similarly have to have possession of the user's token in order to gain system access. The higher level of authentication comes with additional system cost, however, due to the necessary tokens and token readers. In addition, tokens can be easily lost, which can present a high administration overhead for reissuing. Biometric factors for authentication measure characteristics of the user's body such as fingerprint, handprint, retina, iris, or voice characteristics. Biometric measurements are a useful additional factor and add an even higher level of authentication security. A biometric authentication system entails a measurement proving whom the person actually is, rather than proving they have something such as a token or proving that they know something such as a password. Unfortunately, biometric measurements are not 100 percent effective; with the present state of the technology, it is possible to register false positives and false negatives. Biometric authentication systems also require biometric readers at system access points, adding new system costs. Strong cryptographically-based authentication can be provided through the use of digital certificates issued to users and stored on tokens or within the user's computer memory. Cryptographic algorithms are used to ensure that a particular certificate has been legitimately issued to the user. A Public Key Infrastructure is used to enable the issuance and maintenance of digital certificates. Strong cryptographically-based systems provide very stringent authentication. However, these systems are expensive and incur additional management overhead. Therefore, they are currently being adopted only in very secure environments.

2.1. Authorization:

Once authenticated, authorization mechanisms control user access to appropriate system resources. Authorization can be categorized according to the granularity of control; that is, according to how detailed a division is made between system resources. Fine-grained authorization refers generically to a system where access is controlled to very fine increments, such as to individual applications or services.

Authorization is often "role based" whereby access to system resources is based on a person's assigned role in an organization. The System Administrator role may have highly privileged access to all system resources whereas the General User role would only have access to a subset of these resources. Finer grained authorization can be applied to define other roles, such as a Human Resources Administrators role that has exclusive access to confidential HR databases, and an Accounting role that has exclusive access to accounting systems.

Authorization may also be "rules based" whereby access to system resources is based on specific rules associated with each user, independent of their role in the organization. For example, rules may be set up to allow Read Only access or Read/Write access all or certain files within a system, or access only during certain times or from certain devices.

2.2. Authentication and authorization protocols :

Several protocols have been commonly adopted for authentication services. The RADIUS protocol (Remote Authentication Dial In User Service – IETF RFC2865) is widely used to centralize password authentication services. Originally designed to authenticate remote dial-in users, the RADIUS protocol has been adopted for general user authentication services. Recently, the LDAP (lightweight directory access protocol – IETF RFC2251) has been finding extensive use in authentication and authorization systems. LDAP provides a convenient method for storing user authentication and authorization credentials. RADIUS authentication servers are often coupled with credential storage in LDAP directories to provide centralized authentication and authorization. When a user attempts to access a particular application on such a system, the application queries the user for authentication credentials

and forwards them to the centralized system. The RADIUS server then checks the presented credentials against those stored in the LDAP database, and also queries the LDAP database for authorization rule information. The authentication results (pass or fail) are returned to the application along with authorization rule information for the particular user. Authorization rules are then enforced at the application to allow the user to access particular data or services. From an end-user perspective, these authentication and authorization systems should be automatic and easy to use.

2.3. Authentication and authorization recommendations:

Nortel Networks recommends the following general principles to be followed when implementing enterprise authentication and authorization systems:

- Use a uniform access management system for end users, network operators, partners and customers, with the appropriate level of authentication and resource access authorization to meet business needs.
- Use a centralized authentication mechanism to facilitate administration and remove the need for locally stored passwords, which tend to be static and weak.
- Use a centralized authorization system, tightly coupled with authentication system, with appropriate granularity for the enterprise.
- Enforce strong, complex rules for all passwords.
- Securely store all passwords in one-way encrypted (hashed) format.
- Maintain simplicity to the extent appropriate, for maximum ease of use, ease of administration, and compliance.
- Securely log authentication and authorization events for audit purposes.

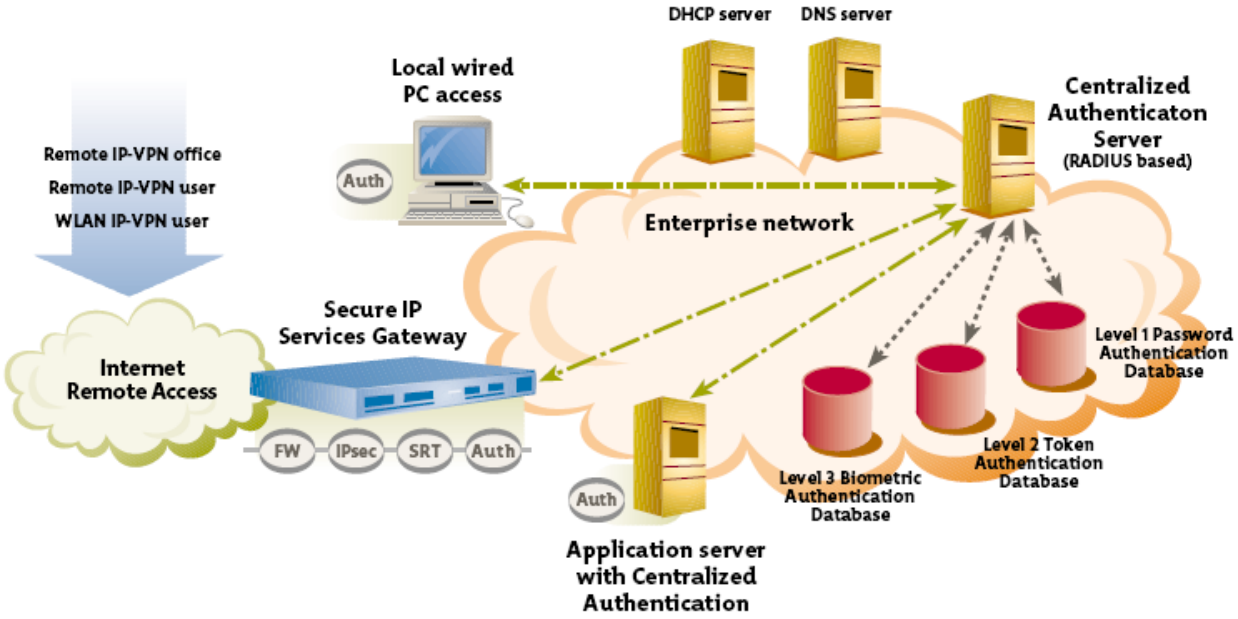

Fig: Secure authentication and authorization reference model

3. NETWORK SECURITY IN THE REAL WORLD:

This section demonstrates this multi-level security framework in action for several real-world scenarios:

- Securing the campus network
- Securing the data center
- Securing the remote office

3.1. Securing the campus network:

In this context, the term “campus” describes a corporate headquarters or large regional office where the network uses a mix of technologies, products, and applications, and serves a large user population. The campus network presents a challenging security picture because of the diversity of elements to protect:

• **Servers**, including departmental servers for user access and file sharing, central application servers such as finance and databases, and Web servers for either public Web or Intranet applications.
• **Operating systems**, typically multiple versions of multiple operating systems running on servers and clients.
• **Network devices**, including routers, Layer 4-7 load-balancing switches, Layer 3 core switches, Layer 2 distribution switches, and wireless LAN access points.
• **Security devices**, such as firewalls, VPN gateways, intrusion-detection and anti-virus servers, SSL accelerators, authentication servers, and content filtering servers.

3.2. Securing the data center:

The typical enterprise data center supports mission-critical applications and houses a high concentration of capital-intensive resources and confidential data—all connected to the inherently insecure Internet as well as internal users. That means securing the data center presents some unique requirements for failsafe security without compromising performance and availability for users. The need increases as enterprises discover new ways to exploit high-performance, Internet-empowered data centers:
• **Ensure business continuity.** Massive processing throughput and transport bandwidth now make it feasible to store primary and duplicate sets of critical data in multiple data centers, in real time—to extend business continuity services, real-time storage mirroring, and live backup across service provider networks.
• **Support critical business applications.** Enterprises use data centers to host business applications, implement firewalls or virtual private networks, provide storage services and content delivery of static and streaming media, and more.
• **Produce economies of scale on infrastructure.** Enterprises can consolidate or outsource data center functions, to centralize critical computing resources, create virtual data centers that span multiple locations, and reduce operational costs without the performance penalty or security concerns typically associated with remote access.

3.3. Securing the remote office:

In this context, the term "remote office" refers to any remote workplace that requires persistent, two-way communication with the enterprise—for locations as diverse as a telecommuter's home office or a major regional office. Connecting remote offices is a significant network cost in many industries, such as retail banking, health care, and government. Traditionally, remote offices were connected to the enterprise network using various LAN technologies and multi-protocol routers, working into frame relay networks with ISDN circuit-switched backup. VSAT satellite terminals have also been widely deployed—for instance, for credit card validation in the retail industry. Four major developments are transforming the remote office networking scenario: (1) the convergence on Ethernet as the LAN standard, (2) universal acceptance of IP as the protocol of choice, (3) the Internet, and (4) a growing list of Layer 2 and 3 VPN services. However, these developments also introduce a variety of security challenges, particularly for "extended" and "open" enterprises.

4. NOTATIONS :

We first define the notation used in this paper. Let "X → Y: Z" denote that a sender X sends a message Z to a receiver Y , $E_k(m)$ denote the cipher text of m encrypted using the secret key k of some secure symmetric cryptosystem [17], $D_k(c)$ denote the plaintext of c decrypted using the secret key k of the corresponding symmetric cryptosystem [17], "||" denote the conventional string concatenation operator and ® denote the bitwise exclusive-or operator. Let h be a public one-way function.

4.1. Single Server Authentication Scheme:

In [8], Juang proposed a user authentication and key agreement scheme using smart cards with much less computational cost and more functionality. The major drawbacks of this scheme are that it does not provide the user anonymity functionality and it is not suitable for multi-server environments.
Let S denote the server, U_i denote user i. Also, let x be the secret key kept secretly by the server S. Let IDi be a unique identification of Ui.

The scheme is as follows.

4.1.2. Registration Phase: Assume u_i submits his identity ID_i and his password PW_i to the server for registration. If the server accepts this request, he will perform the following steps:

Step 1: Compute U_i's secret information $v_i = h(ID_i||x)$ and $w_i = v_i$ ® PW_i.

Step 2: Store ID_i and w_i to the memory of a smart card and issue this smart card to U_i.

4. 1.3. Login and Session Key Agreement Phase: After getting the smart card from the server, U_i can use it when he logins in the server. If U_i wants to login to S, he must attach his smart card to a card reader. He then inputs his identity ID_i and his password PW_i to this device. Assume that N1 is a nonce chosen by U_i and N2 is a nonce chosen by S_j for freshness checking. Assume that ruk is a random number chosen by U_i and rs_k is a random number chosen by S_j for generating the session key $k_i = h(rs_k||ru_k||v_i)$. The following protocol is the ith login with respect to this smart card.
Step 1: $U_i \rightarrow S$: N_1, ID_i,E_{vi} (ru_i, $h(ID_i|| N_1)$);

Step 2: $S \rightarrow U_i$: E_{vi} ($rs, N_1 + 1, N_2$);

Step 3: Ui→ S: Eki ($N_2 + 1$).

4.2. Multi-Server Authentication Scheme:

In [9], Juang proposed a user authentication and key agreement scheme using smart cards for multi-server environments with much less computational cost and more functionality. The major drawback of this scheme is that it does not provide the user anonymity functionality. There are three kinds of participants in this scheme: users, servers and a registration centre. In this scheme, assume that the registration centre can be trusted. The registration centre examines the validity of login users and then issues a smart card to eligible users. The user only has to register at the registration center once and can use services provided by various servers. Let RC denote the registration centre, S_j denote server j, and U_i denote user i. Let UID_i be a unique identification of U_i and SID_j be a unique identification of S_j . Also, let x be the secret key kept secretly by RC, and $w_j = h(x||SID_j)$ be the secret key shared by S_j and RC. The shared secret key w_j can be computed by RC and sent to S_j after he registered at RC. The proposed scheme is as follows.

4.2.1. Registration Phase:

U_i submits his identity UID_i and his password PW_i to RC for registration. RC then performs the following steps:
Step 1: Compute Ui 's secret information $v_i = h(x||UID_i)$ and $\mu_i = v_i \circledR PW_i$.

Step 2: Store UID_i and μ_i to the memory of a smart card and issue this smart card to U_i.

Step 3: Compute the shared secret key $v_{i,j} = h(v_i||SID_j)$ between U_i and S_j , and send the encrypted secret key E_{wj} ($v_{i,j}$,UID_i) to each S_j . Upon receiving E_{wj} ($v_{i,j}$,UID_i), S_j stored it in his encrypted keys table.

4.2.2. Login and Session Key Agreement Phase:

After getting the smart card from RC, U_i can use it to login into S_j . Assume that N_1 is a nonce chosen by U_i and N_2 is a nonce chosen by S_j for freshness checking. Assume that ru_k is a random number chosen by U_i and rsk is a random number chosen by S_j for generating the session key $sk_k = h(rs_k||ru_k||v_{i,j})$. The following protocol is the kth login with respect to his smart card.
Step 1: $U_i \rightarrow S_j$: $N_1, UID_i, Ev_{i,j}$ (ru_k, $h(UID_i||N_1)$);
Step 2: $S_j \rightarrow U_i$: $Ev_{i,j}$ ($rs_k, N_1 + 1, N_2$);
Step 3: $U_i \rightarrow S_j$: Esk_k ($N_2 + 1$).

4.2.3. Shared Key Inquiry Phase:

In Step 3 of the registration phase, RC will send the encrypted shared secret key
E_{wj} ($v_{i,j}$,UID_i) to each S_j . Upon receiving the message, he will store it in his encrypted shared key table. If he do not want to manipulate this table, the shared key can be inquired from RC when it is needed. The following protocol can be inserted between Step 1 and Step 2 of the login and session key agreement phase when Sj needs the shared key.
Step 1': $S_j \rightarrow RC$: N_3, UID_i, SID_j ;

Step 1": E_{wj} ($v_{i,j}$,$N_3 + 1$).

4.3. User Authentication and Key Distribution Scheme :

Yang et al. proposed a user authentication and key distribution with user anonymity [21] based on factoring, discrete logarithm and hash functions. The major drawbacks of this scheme are that it has a time-synchronization problem, and the computation and communication cost is still high. There are three kinds of participants in this scheme: a Smart Card Producing Center (SCPC), service providers (servers) and users. Let U_i denote user i, P_j denote service provider j. This scheme consists of two phases: (1) the key generation phase and (2) the anonymous user identification phase.
Their proposed scheme is as follows:

4.3.1. The key generation phase: The SCPC does the following to set up system parameters.

1) Chooses two large primes p and q, computes n = pq, randomly selects a number e and computes d, where $ed \equiv 1 \bmod \Phi(n)$ and $\Phi(n) = (p-1)(q-1)$.
2) Chooses an element $g \in Z^*_n$ which is a generator of both Z^*_p and Z^*_q .
3) Publishes (e, n, g) as public system parameters and keeps (d, p, q) secret.
4) Sends to each registered user U_i or service provider P_i a secret token $S_i \equiv (ID_i)^d \bmod n$, where ID_i is
The identity of U_i or P_i. The anonymous user identification phase: If U_i wants to request a service from P_j , they then performs the following steps:
Step 1: U_i Sends the service request to P_j for requesting services from P_j .
Step 2: Upon receiving the request, P_j chooses a random number k and computes
$z \equiv g^k S_j^{-1} \bmod n$ and sends z to U_i.
Step 3: Upon receiving z, U_i chooses a random number t and does the following computations:
$a = z^e ID_j \bmod n$,
$K_{ij} = a^t \bmod n$,
$x = g^{et} \bmod n$,
$s = g^t S_i^{h(x||T)} \bmod n$,
$y = E_{Kij}$ (IDi),

where T is the current timestamp and $K_{i,j}$ is the common session key. U_i then sends (x, s, y, T) to P_j .

Step 4: Upon receiving the message in Step 3, P_j checks the timestamp T . If it is old, he aborts the
protocol. Otherwise, he then obtains the common session key $K_{ij} = x^k \bmod n$ and then decrypts y as
$ID_i = D_{Kij}$ (y) and verifies

$$xID_i^{h(x||T)} ?= s^e \bmod n.$$

If the verification passes, then the service request is granted.

5. SINGLE SERVER AUTHENTICATION AND KEY AGREEMENT WITH USER ANONYMITY:

In this section, we propose an efficient single server user authentication and key agreement scheme with privacy protection. The concept used in this section will be used in the next section to construct an efficient multi-server user authentication and key agreement scheme with privacy protection. Let ID_i be a unique identification of user i. Also, let x be the master secret key kept secretly by the server S.

5.1. The Proposed Scheme

The proposed scheme is as follows.

5.1.1. Registration Phase:

Assume U_i submits his identity ID_i and his password PW_i to the server S for registration. If S accepts this request, he will perform the following steps:
Step 1: Compute U_i's secret information $\alpha_i = h(x||ID_i)$ and $\beta_i = \alpha_i$® PW_i. Compute the pseudo identification number $\lambda_{i,1} = h(\alpha_i ||ID_i||1)$ and records ($k = 1$, $\lambda_{i,1}$, ID_i) in an identification table

Step 2: Store IDi, $\lambda_{i,1}$, k = 1, and β_i to the memory of a smart card and issue this smart card to U_i or send them secretly to U_i.

5.1.2. User Authentication and Session Key Agreement Phase:

If U_i wants to log into S anonymously, he must attach his smart card to a card reader. He then inputs his identity ID_i and his password PW_i to this device. The following protocol is the kth login with respect to this smart card.

Step 1: $U_i \rightarrow S : N_1, \lambda_{i,k}$,$E_{\alpha i}$ (ru_k, $h(N_1||ru_k|| \lambda_{i,k}$));

Step 2: $S \rightarrow U_i : N_2, E_{\alpha i}$ (rs_k,$h(rs_k||N_1||N_2)$);

Step 3: $Ui \rightarrow S : E_{skk}$ ($N_2 + 1$).

.5.2. Performance Considerations:

We evaluate the efficiency of our scheme and Juang's scheme in Table 1. First, we assume the block size of secure symmetric cryptosystems is 128 bits and the output size of secure one way hashing functions is 128 bits. Because both our proposed single-server scheme and Juang's scheme are based on symmetric key cryptosystem, the performance is very well. In our scheme and [8], the password length only 128 bits is required. Our proposed scheme needs 384 bits for the user authentication. Both ours and Juang's scheme [8], the computation cost for registration is only needed one hash operation. The computation cost are aggregated operation numbers, including encryption operations, decryption operations or hashing operations. The encryption and encryption operations may be asymmetric or symmetric cryptosystem. In the login and session key agreement phase of our scheme, three symmetric key encryptions, three symmetric key decryptions and seven hash operations are required. In that of Juang's scheme [8], only three symmetric key encryptions, three symmetric key decryptions and three hash operation are required. The computation cost of the login and session key agreement is not including cost of generating session key. Although our proposed scheme has a little high communication and computation cost than Juang's scheme [8], but our scheme have more complete functionality. The functionality comparison between our proposed scheme and related scheme is given in Table 2. Compared

6. MULTI- SERVER AUTHENTICATIONS AND KEY AGREEMENT WITH USER ANONYMITY:

There are three kinds of participants in our multi-server protocol: a key distribution centre, service providers (servers) and users. Let KDC denote the trusted key distribution centre, U_i denote user i, S_j denote service provider j. Let UID_i be a unique identification of U_i and SID_j be a unique identification of service provider j. Also, let x be the master secret key kept secretly by the key distribution centre KDC and $\delta_j = h(x||SID_j)$ be the secret key shared by S_j and KDC. The shared secret key δ_j can be computed by KDC and sent secretly to S_j after he registered at KDC.

6.1. The Proposed Scheme:

The proposed scheme is as follows.

6.1.1. Registration Phase:

Assume Ui submits his identity UIDi and his password PWi to KDC for registration. If KDC accepts this request, he will perform the following steps:
Step 1: Compute Ui's secret information _i = h(x || UIDi) and _i = _i _ PWi.

Step 2: Store UIDi, and _i to the memory of a smart card and issue this smart card to Ui or send them
secretly to Ui.

6.1.2. Shared Key Inquiring Phase:

If Ui wants to use the services provided by Sj, he must inform Sj to query the shared key i,j from KDC in advance. KDC will compute i,j = h(_i _SIDj),where _i is shared key with Ui, and then sends i,j to Sj. They will perform the following steps:
Step 1: Ui ! Sj : N1,UIDi;
Step 2: Sj ! KDC : N0 1, SIDj,E_j (UIDi, h(UIDi || SIDj || N0 1));
Step 3: KDC ! Sj : E_j (i,j , h(UIDi || SIDj || N0 1 || i,j));
Step 4: Sj ! Ui : Ei,j (N1 + 1).

6.2. Performance Considerations:

In this subsection, we present a efficiency comparison among our proposed scheme, Yang et al.'s scheme [21] and Juang's scheme [9]. The comparison is given in Table 3. We also assume that n in Yang et al.'s scheme [21] that has the same assumption with Lin et al.'s scheme [13] is of 1024 bits in order to make the discrete logarithm problem infeasible. Moreover, we also assume both the output size of secure one-way hashing functions and the block size of secure symmetric cryptosystems are 128 bits. In our scheme and Juang's scheme [9], the memory needed in the smart card is 256 bits. In [21], However, the memory needed in the smart card is 1024 bits since their scheme based on the intractability of the discrete logarithm problem. The communication cost of the user authentication of our scheme and Juang's scheme [9] is 384 and 256 bits respectively. In [21], the communication cost for the authentication is 5 × 1024 bits. In our scheme and Juang's scheme [9], the computation cost of registration is one hash operation. In that phase, that is two exponentiation operations in Yang et. al.'s scheme. In our scheme, the computation cost of the shared key inquiring phase is needed three symmetric key encryptions, three symmetric key decryptions, five hash operations and one exclusive-or operation. In Juang's scheme [9], that is needed two symmetric key encryptions, two symmetric key decryptions, two hash operations. That phase of Yang et al.'s scheme [21] is not required. The computation cost of anonymous user identification in our scheme is three symmetric key encryptions, three symmetric key decryptions and seven hash operations. The computation cost of user identification in Juang's scheme [9] is three symmetric key encryptions, four symmetric key decryptions and three hash operations. The computation cost of anonymous user identification in Yang et al.'s scheme [21], nine exponential operations, one symmetric key encryptions, one symmetric key encryptions, and two hash operations are required.

7. CONCLUSIONS:

In this paper, we have proposed two user authentication and key agreement schemes with privacy protection for single server and multi-server environments. Regarding the single-server scheme, it is more simple and efficient. Regarding the multi-server scheme, users only need to register one time and can use all provided services by service providers. Both our proposed schemes have the ability of privacy protection. Our schemes also have low communication and computation cost for user authentication by only using symmetric cryptosystems and one-way functions. Also, our schemes successfully solve the serious time-synchronization problem in a distributed computers environment since our proposed schemes are nonce-based.

8. REFERENCES:

[1] S. Bellovin and M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," in Proceedings of IEEE Symposium on Research in Security and Privacy, pp. 72-84, 1992.
[2] M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication," ACM Transactions on Computer Systems, vol. 8, no. 1, pp. 18-36, 1990.
[3] Y. Chang and C. Chang, "Authentication schemes with no verification table," Applied Mathematics and Computation, vol. 167, pp. 820-832, 2005.
[4] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. IT-22, no. 6, pp. 644-654, 1976.
[5] C. Fan, Y. Chan, and Z. Zhang, "Robust remote authentication scheme with smart cards," Computers & Security, vol. 24, pp. 619-628, 2005.
[6] M. Hwang, C. Lee, and Y. Tang, "A simple remote user authentication scheme," Mathematical and Computer Modelling, vol. 36, pp. 103-107, 2002.
[7] T. Hwang and W. Ku, "Repairable key distribution protocols for internet environments," IEEE Transactions on Communications, vol. 43, no. 5, pp. 1947-1950, 1995.
[8] W. Juang, "Efficient password authenticated key agreement using smart cards," Computers & Security, vol. 23, no. 2, pp. 167-173, 2004.
[9] W. Juang, "Efficient multi-server password authenticated key agreement using smart cards," IEEE Transactions on Consumer Electronics, vol. 50, no.1, pp. 251-255, 2004.
[10] W. Juang and W. Nien, "Efficient password authenticated key agreement using bilinear pairings," in the 16th Information Security Conference, pp. 214-221,Taichung, Taiwan, June 2006.
[11] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, pp. 770-772, 1981.
[12] A. Lenstra, E. Tromer, A. Shamir, W. Kortsmit, B.Dodson, J. Hughes, and P. Leyland, "Factoring estimates for a 1024-bit RSA modulus," in Advances in Cryptology (Asiacrypt'03), LNCS 2894, pp. 55-74, Springer, New York, 2003.
[13] I. Lin, M. Hwang, and L. Li, "A new remote user authentication scheme for multi-server architecture," Future Generation Computer Systems, vol. 19, pp.13-22, 2003.
[14] W. Ku and S. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 204-207, 2004.
[15] R. Merkle, "One way hash functions and DES," in Advances in Cryptology (Crypt'89), LNCS 435, pp. 428-446, Springer, New York, 1989.
[16] NIST FIPS PUB 180-2, Secure Hash Standard, National Institute of Standards and Technology, U. S. Department of Commerce, DRAFT, 2004.
[17] NIST FIPS PUB 197, Announcing the Advanced Encryption Standard (AES), National Institute of Standards and Technology, U. S. Department of Commerce, Nov. 2001.
[18] D. Seo and P. Sweeney, "Simple authenticated key agreement algorithm, Electronics Letters, vol. 35, pp. 1073-1074, 1999.

[19] P. Syverson, "A taxonomy of replay attacks," in Proceedings Computer Security Foundations Workshop
VII, vol. CSFW 7, no. 14-16, pp. 187-191, 1994.
[20] C. Yang, T. Chang, and M. Hwang, "Cryptanalysis of simple authenticated key agreement protocols," IEICE Transactions on Fundamentals, vol. E87-A, no. 8, pp. 2174-2176, 2004.
[21] Y. Yang, S. Wang, F. Bao, J. Wang, and R. Deng, "New efficient user identification and key distribution
scheme providing enhanced security," Computers and Security, vol. 23, no. 8, pp. 697-704, 2004.

9. AUTHOR PROFILE:

Nagamalleswara Rao Dasari received B.Tech., degree in Computer Science and Information Technology from JNTU in 2006. He is a research scholar in CSIT department, St.Mary's Engg. College, Hyderabad, Andhra Pradesh, India. His research interests include Network Security ,Cryptography, Data Mining.

Vuda Sreenivasarao received his M.Tech degree in Computer Science & Engg from the Satyabama University, in 2007.Currently working as Professor & Head in the Department of Information Technology(IT) at St.Mary's college of Engineering & Technology, Hyderabad, India. He is Currently Pursuing the PhD degree in CSIT Department at JNT University, Hyderabad, India. His main research interests are Data Mining, Network Security, and Artificial Intelligence. He has got 10years of teaching experience .He has published 12 research papers in various international journals. He is a life member of various professional societies like MIACSIT, MISTE.