A Review Study of Juang Approach with Overview of Improved Proposed Approach for Multisever Authentication and Key Agreement with User Protection

Amita Jangid
Mtech Scholar, Dept of CSE
Arya College of Engineering & Information Technology
SP- 42 RIICO Industrial Area, Kukas, Jaipur, Rajasthan, India

Vishal Shrivastava
Professor, Dept of CSE
Arya College of Engineering & Information Technology
SP- 42 RIICO Industrial Area, Kukas, Jaipur, Rajasthan, India

ABSTRACT
Use of smart card makes remote user verification and key agreement easy, elastic to making a secure scattered system environment. It is very important to provide user privacy protection in authentication phase. In this paper, we are describing the performance comparison of Jung approach for multiple server authentication and key agreement schemes with user protection in network security with our proposed approach. First we are describing the juang approach then overview of our approach with comparison. All the areas those can be improved by us are also defined. Our approach is works for single server as well as multi sever environment. According to our analysis the juang approach is open to the element, leak-of-verifier attack and session key discovery attack and smart card loss attack. We are saving data into the server table in form of digital identity, smart card is removed by us, and so the new approach is safe from smart card loss attack.

General Terms
This paper describes the Juang approach for multiserver authentication and key agreement. It defines the limitation of his approach than the overview of improvements can be done by us to make this approach more secure and cost effective with user protection.

Keywords
User verification, session key, comparison, key size, smart card, network security

1. INTRODUCTION
The user must login to access the services provided by the server. For login user send his username and password to the server through a protected path. In this case for to check the authenticity of the user sever reads the message send by the user and verifies his identity and password, if the identity and password matches then server gives rights to access all services provided by itself otherwise user not allowed to access the services. In previous paper we study the Juang approach for multi server authentication and key agreement problem and we figure out its limitation and improvement areas. So in this paper we shall describe the overview of our proposed approach and comparison of performance with Jung approach. Juang scheme is efficient for authentication and key agreement but the drawback of the scheme; it has no ability of anonymity for the user. we can make it more secure and cost effective. The following points must be considered for user authentication and key conformity phase.

a. Confidentiality shelter: In the phase of authentication the opponent can not constrain the identity of the user.

b. Generously choose password: All uses are free to change password and select his password by himself.

c. Less communication and computation cost: The smart card is costly and it is not offers a powerful computation capability so we are removing the smart card from our approach.

d. Mutual authentication: Server authenticate user mutually.

e. Session key contract: Each server and user must establish a session before communication [7, 8].

Usually in all scheme each user needs to register many servers and memorize more than one identities and passwords. This is not convenient way for the users. To make it easy to use many approaches are proposed for multi server authentication. In these entire new schemes only one time login works for many severs. User need not to register on all the servers. These are the following criteria for security of the session key generation phase.

a. **Session key safety**: Session key must be shared with the user and server only securely

b. **Forward confidentiality**: Session key must have some time out feature. The long driven session key is unsecure that is used before for other sessions. For each new session new key must be generate.

c. **Known-key security:** The old session key can not determine the new session key.

2. STUDY OF JUANG APPROACH
Juang approach is smart card based approach for remote logins to multi server environment. This approach is weak beside smart card lost problems, leak-of-verifier attack. To remove all recognized security terrorization in their mechanism, we shall propose an improved version this approach.

Notation used in Juang algorithm "A → B: C" denote A is sender B is message and C is receiver, E y(c) denote that secure key y is used to encrypt the chipper text c. D y(m) denote the secrete key y is used to decrypt the plaintext m corresponding symmetric cryptosystem[13], "||" denote the string concatenate operator and ® denote the bitwise exclusive-or operator. h denote the hash function.

2.1 Juang Approach for Single Server Authentication

Juang scheme is based on the smart card which is describing below this scheme is for user authentication and key agreement with high communication cost and more functions. [8] Following notations are used here. Ui stands for ith user. IDi stands for unique identity of user. x is the secrete key. S stands for server. PW is the password for a user login.

2.1.1 Registration Phase

User sends a message to the server of his identity IDi and password PW for registration [8] If sever accepts his request than below steps are processed:

Step 1: Sever generate secrete keys for user ui vi = h(IDi||x) and wi = vi ® PWi.

Step 2: In this step IDi and wi is loaded into the memory of smart card. That card issue to the user.

2.1.2 Login and Session Key Agreement Phase

User first attaches his smart card to the device then submits his id and password to the reader device. Both server and user choose nonce value N1 and N2 for fresh login check step. For generate the session key a random number rsk chosen by server and ruk chosen by user then the session key is generated ki = h(rsk||ruk||vi). Then below steps are processed for it login:

Step 1: Ui → S: N1, IDi,Evi (rui, h(IDi|| N1));

Step 2: S → Ui: Evi (rs,N1 + 1,N2);

Step 3: Ui→ S: Eki (N2 + 1).

2.2 Multi Server Authentication Scheme

This scheme is proposed by Juang for multi server authentication and key agreement which is based on smart card. Users, servers and a registration centre are the participants of this scheme. It is assumed that the registration centre is trusted. In this scheme user has to register only one time to access the different services provided by the different servers. Let RC stands for the registration centre, Sj denote server j, and Ui denote user i. Let UIDi be a unique identification of user i and SIDj stands for unique identity of server Sj. X is assume to be a secrete token kept by registration center securely. Registration center generates the secret key wj = h(x||SIDj) that is shared with registered servers securely. This key further used in communication.

2.2.1 Registration Phase

User sends a message to registration center RC sever which message conations user identity UIDi and user password PWi. Below steps are performed by the registration center for ith user registration.

Step 1: RC generates the two secret keys for user i one is vi =h(x||UIDi) and other is µi = vi ® PWi.

Step 2: Then user identity and µi is loaded to the memory of smart card than that is useful for the user. That card is issue to the user.

Step 3: For establish communication between each user and server RC generates a shared secret key which is shared between users and severs. The key is vi,j = h(vi||SIDj). And then RC sends encrypted key Ewj (vi,j ,UIDi) to each sever after receiving this encrypted key, severs saves this key into its database.

2.2.2 Login and Session Key Agreement Phase

User first attaches his smart card to the device then submits his id and password to the reader device. Both server and user choose nonce value N1 and N2 for fresh login check step. For generate the session key a random number rsk chosen by server and ruk chosen by user then the session key is generated ki = h(rsk||ruk||vi). Then below steps are processed for it login:

Step 1: Ui → Sj : N1,UIDi,Evi,j (ruk, h(UIDi||N1));

Step 2: Sj → Ui : Evi,j (rsk,N1 + 1,N2);

Step 3: Ui → Sj : Eskk (N2 + 1).

2.2.3 Shared Key Inquiry Phase

As we have seen in step 3 of registration phase of multi sever environment RC sends a encrypted key Ewj (vi,j ,UIDi) to each sever that key is saved by all severs databases, so for removing the efforts to save that key on each server we can verify this key from registration center only. It can be fetch directly from the RC. So the below steps can be processed between step 1 and step 2 of login and session key agreement phase when it requires the shared key [10].

Step 1: Sj → RC : N3,UIDi, SIDj ;

Step 2: Ewj (vi,j ,N3 + 1).

2.3 Inadequacy of Juang scheme

These are some drawbacks of this scheme it does not provide the user secrecy functionality and it is not function properly for multi server environments. Juang's scheme lacks efficiency, and each server needs to additionally protect and securely maintain an encrypted key table. According to my analysis the key size is very large. The output block size of secure key can reduce. This can be more secure by using other cryptographic functions.

3. OVERVIEW OF OUR PROPOSED APPROACH

First we shall define the improvements we can do in the above scheme. Following are the improvements those we have consider in our proposed scheme.

- **a.** The secure key size can be reducing by using the other cryptographic technique.
- **b.** We are using 3DES in place of hash function which is more secure and required the less block size. So security is another factor that we shall improve.
- **c.** We can make only one time registration to login to multiple sever. By using a single digital identity and password user can access the multiple services provided by the different severs.
- **d.** We are removing smart card in our proposed scheme so the user is saved from smart card loss attack. We are storing the user's login details in sever in form of digital identity securely.
- **e.** Cost and time consumption can be reduce.

These are the area we can improve in our approach. Now let's discuss the overview of our proposed approach.

4. PROPOSED APPROACH

We proposed an improved version of Juang user authentication and key agreement scheme that is more efficient, less computational, more secure and required less

memory block size. This proposed scheme is suitable for single server and multi server environment. Our scheme also has low communication and computation cost for user authentication by only using symmetric crypto systems using 3DES which more secure technique. Also, this new scheme successfully solves the user protection and security problem in a multiple sever system since our proposed scheme is based on 3DES.Description of proposed improvements in Juang user authentication and key agreement scheme. In place of one simple hash function we are using 3DES which is more secure and required less memory block size. It provides addition security and control over user.

It is an efficient approach for user authentication and key agreement with controlled security attacks using 3DES algorithm. The same approach used for single server will be use to build an efficient multiple servers system. The keys generated by the sever for each user is saved on sever in digital identity form. The user login to user by entering its digital identity which is securely sent to the user. If the identity is correct server allows users to login to sever otherwise not.

In case of multiple server environment the registration center manages all severs and users. A key distribution centre, service providers (servers) and users are the participants of this protocol.

The registration center compute the secrete key and send that key to each sever after register at registration center. That key is generated using highly secure 3DES algorithm which less in size in comparison of Juang scheme and more secure. This key is also saved on registration Center. Each severs also save the same key in tables securely.

To login the user must register on registration center user enter its identity and password. The sever generates its secure key using 3DES algorithm and sends that key to the each sever to verify the users identity when the same user will login to registered server. After successful registration the user can login to sever. User chooses a nonce value and server also chooses a nonce value for freshness checking. Then user enter its details sever checks his identity by applying some secure encryption decryption techniques. If the details matches with the digital identity stored by the server then user gets successful login otherwise not ale to login the sever.

This is the overview of our proposed approach we shall describe the detail of each steps of our approach for single server as well as multiserver environment. The algorithm steps we shall describe in our next paper.

5. COMPARISONS OF PERFORMANCE ANALYSIS

We estimate the competence of our scheme and Juang's scheme. Juang's scheme is based on the hash function, and our scheme is based on the 3DES cryptosystem so the performance of our approach is better than Juang approach. In our scheme secrete key length is less than Juang scheme. For compute the computation cost of registration phase we can see the Juang approach [8], needs only one hash function and in our scheme one 3DES function needed that makes secrete keys more secure and less memory size required. The computation cost is base on the aggregation of encryption and decryption operations. Our approach requires four encryptions and four decryptions in login phase. In Juang approach [8], only three encryptions, four decryptions and five hash functions needed. We have removed the smart card also saving all the data on sever in form of digital signatures securely which is cost effective and safe from smart card loss attack.

Our approach taking more time than juang approach but the use of 3DES in place of hash function makes our approach more secure. The secure key length size is small than Juang approach so the processing time is less and key is more secure than Juang mechanism. The overall performance of our approach is better than Juang approach with high security and user protection.

Table 1 Comparison of performance analysis on basic of different parameters

Algorithm	Block Size (bits)	Security level	Cost	Time consume
3DES	64	High	Less	High
Hash function	128	Less	High	Less

6. CONCLUSION

In this paper, we have discussed the improvements done in juang approach and overview of our proposed approach for multiple server and single server user authentication and session key establishment. In our approach only one time registration required to access the multiple services provided by the servers. Our approach is more secure required less cost and ease of use.This new approach also have low communication and Computation cost for user authentication by only using 3DES algorithm. It also solves the serious time-synchronization problem in a multi server environment. Our scheme required less memory size. Less cost because smart card is removed in our approach so we are safe from smart card loss attack.

7. FUTURE WORK

We will provide the implementation of each step of our new approach. In this paper we have only discuss the overview of our approach. It is an improved version of Juang approach which is more secure. That approach will take less memory to store the user secrete keys and less computational work require. It will store the user login information securely in server tables in form of digital identity by doing this smart card loss problem can be removed.

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 authenticationscheme," Mathematical and Computer Modelling, vol. 36, pp. 103-107,2002.

[7] W. Juang, "Efficient password authenticated key agreement using smart cards," Computers & Security, vol. 23, no. 2, pp. 167-173, 2004.

[8] Lamport, "Password authentication with insecure communication,"Communications of the ACM, vol. 24, pp. 770-772, 1981.

[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] 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.

[11] I. Lin, M. Hwang, and L. Li, "A new remote user authenticationscheme for multi-server architecture," Future Generation ComputerSystems, vol. 19, pp.13-22, 2003.

[12] 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.

[13] W. Juang and W. Nien, "Efficient password authenticated keyagreement using bilinear pairings," in the 16th Information SecurityConference, pp. 214-221,Taichung, Taiwan, June 2006.