Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.623 – 632

RESEARCH ARTICLE

Implementation of Single Sign-On Mechanism for Distributed Computing

MS. Rinky G. Chhatwani[1]
M.E 2nd yr, PRMCEAM, Badnera
rinkychhatwani@gmail.com [1]

Dr.D.G.Harkut[2]
H.O.D, PRMCEAM, Badnera
dg.harkut@gmail.com [2]

Abstract: With wide spreading of distributed computer networks, it has become popular to allow users accessing various network services offered by distributed service providers. It is usually not practical by asking one user to maintain different pairs of identity and passwords for different service providers, since this could increase the workload of both users and service providers as well as the communication overhead of networks. So, for this it requires a single sign-on authentication mechanism that is a single login for multiple service providers, which would not increase the workload. There are various attacks and parameters that need to be considered while providing security to authentication system. In this paper, we provide a comprehensive review of existing work done on Single sign-on. Then for security of single sign-on, what parameters and attacks should be covered. Next, Implementation of Single Sign-on for distributed computing using user-id and password along with biometric verification. Then security analysis is done. Next, we present the comparison and lastly we conclude, specifying the future work.

Keywords: Authentication, Soundness, Anonymity, Single sign-On, Biometrics, security

1. INTRODUCTION

In insecure network environments, Communication securely through open network is one of the common necessities. Cryptography is one of the primary tools for providing better security. The primary goals or aspects of security are data confidentiality, data integrity, and authentication [42]. Single Sign-on means that after obtaining a credential from a trusted authority, each legal user can use this single credential to authenticate itself and then access multiple service providers.

Three methods can be used for secure Single Sign-On.

1. Cryptography based.
2. Using Smart Card.
3. Biometric based.

There are various methods that are smart based and are advantageous. Some input is given from the smart card and nonces are used that is any randomized number is used. There are other methods in which biometrics and smart card are used are advantageous too. In Biometric and smart card based method, biometric input through some hardware device is fed along with the smart card input and then some cryptography is applied and processing is done. In our paper, we are taking input that is user-id and password along with the biometric verification. We are combing concepts from different paper and applying.

Two important concepts come while security for Single Sign-On is concerned. Soundness and Credential Privacy [20][24]. Soundness means that an unregistered user without a credential should not be able to access the services offered by service providers. Credential privacy guarantees that colluded dishonest service providers should not be able to fully recover a user's credential and then impersonate the user to log in other service providers.

While providing security various parameters that need to be considered such as mutual authentication, Password Change phase, User anonymity, User untraceability. There are attacks that should be verified [11] [31] [39] –

- Impersonation attack
- Replay attack
- Denial of service attack
- Credential privacy attack.

Initiator anonymity and Initiator untraceability are the concepts that should be focused for better security [48][7]. Initiator anonymity says that only the server knows the identity of the user with whom he is interacting, while any third party cannot do this. Initiator untraceability is a stronger property than initiator anonymity and requires that any adversary should be not only infeasible to infer the identity of the initiator but also prevent from linking one (unknown) user interacting with the server to another transcript. In other words, the adversary is not able to tell whether he has seen the same user twice.

Kerberos is also an authentication scheme that we should concentrate on [22], but if this unproven symmetric mechanism is used to authenticate users, lead to potential security weakness. As authentication of users is of major concern that is soundness, more improved mechanisms should be used. In method, the phases used are the same for the all the three schemes but the input feed is different and the processing is different. Section 2, introduces related work done on Single Sign-On mechanisms. Section 3 discusses the parameters and attacks that should be considered to see that better security is provided. Section 4 illustrates the implementation of single sign-on mechanism. Section 5, shows the security analysis that is carried out. Section 6, describes the comparison done and lastly section 7, concludes this paper with some suggestions for future work.

2. RELATED WORK

In 2012, C. C. Chang et al. [9], have presented an interesting RSA based SSO scheme based on one-way hash functions and random nonce to solve the weakness of timestamp and to decrease the overhead of the system. It is highly efficient in computation and communication cost. Here the parameters taken are Computation cost and Communication cost. Chang-Lee scheme is actually insecure to impersonation attack; this was found out by authors in [20].

In 2013, G. Wang et al. [20], showed that Chang Lee scheme is insecure by applying credential recovering attack and impersonation attack without credentials. The first attack Credential recovery attack which compromises credential privacy, allows a malicious service provider, who has successfully communicated with a legal user twice, to recover the user's credential and then to impersonate the user to access resources and services offered by other service providers. In the other attack that is the impersonation attack without credential compromises Soundness, an outsider without any credential may be able to enjoy network services freely by impersonating any legal user or a nonexistent user.

In 2008, W. Juang et al. [47], the authors have used Elliptic curve cryptosystem and key agreement. It does not provide user anonymity. The main merits include, a user can freely choose and change password, it is a nonce-based scheme that does not have a serious time-synchronization problem, servers and users can authenticate each other. It can provide identity protection, session key agreement, and low communication and computation cost by using elliptic curve cryptosystems and can prevent the insider attack and offline dictionary attack.

In 2010, X. Li et al. [48], has presented a remedy to by addressing the initiator in traceability property. The trick is to randomize the transmitted data in a manner that the adversary over the channel cannot link different conversations and that the communicating parties can recognize the received messages. It is believed that in traceability property should also be addressed in the design of authentication schemes for wireless communications. The authors used hash function and, symmetric encryption and decryption. Parameters that were checked for security analysis were Mutual authentication, session key agreement, initiator anonymity, Initiator intractability.

In 2011, A.K. Das, [2], shows that the improved scheme provides strong authentication with the use of verifying biometric, password as well as random nonce generated by the user and the server. The author has explained the proposed scheme in four phases that is the registration phase, login phase, authentication phase and password changing phase. Protect against attacks like masquerading server attacks, parallel session attacks, lost smart card attack.

In 2012, G. Dong et al. [25], the authors analyzed that the Das's scheme [2], is insecure against the user impersonation attack, the server masquerading attack, the off-line password guessing attack and insider attack, authors have found out these security weaknesses in Das's scheme. They have not proposed the enhanced scheme.

In 2010, 2012 , Eun-Jun Yoon et al. [29] [32], the authors have shown that the paper proposed by Kim, Lee and Yoon, two ID-based password authentication schemes without passwords or verifying tables, with smart card and fingerprints is insecure and vulnerable to impersonation attack. In the next paper, the authors have showed that Khan-Zhang's biometric remote user authentication scheme is vulnerable to a privileged insider's attack and Parallel session attack. So the authors have proposed a new robust authentication scheme using bit-wise exclusive-OR (XOR) operation and collision-free one-way hash functions as main cryptographic operations without additional requirements such as using server's public key and digital signatures. This scheme can withstand various attacks like replay attack, guessing attack, insider attack and impersonation attack and also provides mutual authentication, secure password change function without helping of the remote server. This scheme is useful for wire/wireless environment and for smart card based schemes as it provides security, reliability and efficiency.

3. PARAMETERS AND ATTACKS CONSIDERED FOR BETTER SECURITY

In order to check the security of our Single Sign-On Mechanism the parameters considered confirm that the security is not hindered.

3.1 Parameters-

A. Mutual Authentication

Mutual authentication is that the user and
the server are authenticated at the same time. Mutual authentication is to establish the agreement between the user and the server, so that the user and the server agree upon a common hey known as session key.

B. Initiator Anonymity

Initiator anonymity is an important property that should be addressed [7] [15]. It says that only the server knows the identity of the user with whom he is interacting, while any third party cannot do this [27]. If the Trusted Third Party (TTP) concept is considered, to each access to service providers a user will use different IP addresses of the service providers to enjoy different services, and the authentication party will give the required data, so in this way the user is anonymous to the service provider also.

C. Initiator Untraceability.

Initiator untraceability, is the stronger property than initiator anonymity. It means that the adversary can neither know who the initiator is, nor whether the two conversations originate from the same initiator. This is an important property that needs to be concentrated on. In simplest term, it requires that any adversary should be prevented from linking one (unknown) user interacting with the server to another transcript. Namely, the adversary is not capable of telling whether he has seen the same user twice.

D. Password Change Phase.

Password change phase is necessary phase that should be included in the methodology as the user needs to update password so as to agree on a new same password to the authentication party through the log-in phase in advance. It should be included as every time the message is send new hash code is generated of the new password and then that password is used during login.

3.2 Attacks is To Be Prevented-

A. Impersonation Attack

An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate in a system or in a communication protocol. So, as the identity is obtained the illegal user tries to modify a login request massage, but the illegal user will be unable to acquire the data so no modification will be done and the address should be detected.

B. Credential privacy attack.

A masquerade attack is through the use of stolen logon IDs and passwords, is the type of attack where the attacker pretends to be an authorized server of a system in order to gain access to it or to gain greater privileges than they are authorized for. This process takes place during login phase and authentication phase. To masquerade as the legitimate server, an attacker attempts to make the forged reply message which can be masqueraded to the user when receiving the user's login request message.

C. Replay attack.

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary, who intercepts the data and retransmits it [21] [47] [49].

D. Denial of service attack

In a denial of service attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses [17]. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

4. IMPLEMENTATION OF SINGLE SIGN-ON MECHANISM

In this section, we present along with user-id and password, biometric based secured user authentication scheme. In our work, we are using One-way hash function and AES Encryption/Decryption algorithm. This work is divided into 3 parts: 1-Client side, 2- Authentication party, 3- Server side. The notations use in the scheme and phases are described below.

The Notations:

Ri – Receiver; **PWi** – generated by AP; **Si** – Server;
AP – Authentication party; **PW***- Password choose by Receiver.

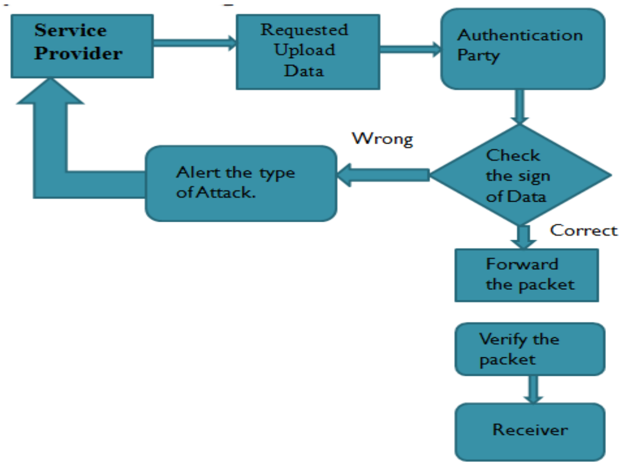

Fig 4.1 System Flow Diagram

There are various phases in which the method is carried out:

- Registration Phase
- Login Phase
- Authentication Phase
- Password changing Phase.

A. **Registration Phase-** In the registration Phase of our work, Receiver R opens the file and registers himself/herself to the authentication party by giving input his user-id and face through data set that is stored in the folder. Here we are doing it by simulation. The authentication party provides the password to the receiver. So the AP computes the hash of UDi and password and stores in it. This is done via a secure channel as the random number that is nonce is added in the message along with the face Biometric. This hash code of UDi and PWi and face data is stored at the AP.

B. Login Phase- Receiver R wants to login in the System to get the service, this phase provides the facility of a secure login request to authentication Party AP.

When the receiver inputs the UDi and PWi along with the face data, the authentication party calculates the hash of the user-id and password and mix the message with the face data along with the random number and the message digest created is checked with the message digest stored at the AP. If it is correct then the receiver is the legitimate user else it terminates the login phase and asks to login again. If the receiver is the legitimate user then, next the IP address is asked of the service provider and the receiver IP address.

C. Authentication Phase –

Receiver authentication- After the login request is done at that time of login the authenticated party authenticates the receiver.

AP already has the list of file name and its sign created. Authentication party asks the receiver of file data needed from the server (Application) through the IP address and also gives his own IP address. One application is of File operation and chat. If the receiver is login, he is online to both the smaller applications that is the file operation and chat both. AP asks the receiver of the file needed.

Server Authentication- As the AP has the list of the File name along with AES encryption/Decryption sign generated. When the AP asks the server for the file, file data stored in the database of the server sends the requested encrypted file along with the random number that is known only to the legitimate server. File is send to the AP. AP does the AES decryption sign. If the sign is same and random number is same that is stored in the AP and the time is also noted then the server is the legitimate server. Server and receiver both are authenticated by the authentication party (AP).

D. **Password Change Phase -** This phase provides the facility of update password by the receiver R, if receiver R wants change his/her password PW_i to PW*.

First the receiver has to login through his old password. Then there is option for change password, the receiver then inputs his new password and the receiver is free to choose any password as his PW*. Once its updated, receiver is now free to login by his new password. Now every time he is login, this new password is used for creating hash and every time the message is sends. Whole further processing is done through this password.

5. SECURITY ANALYSIS

To overcome disadvantages Soundness and Credential Privacy, there are various parameters that need to be considered while providing security and our work covers all these parameters.

- Mutual authentication
- Password Change phase
- User anonymity
- Initiator Traceability

There are **attacks** that should be verified.

- Impersonation attack
- Credential Attack
- Replay attack
- Denial of service attack

Our work provides prevention against all these attacks. In our work overcome these attacks and to cover all these parameters algorithms used are

- One-way hash Function
- AES Encryption/Decryption.

5.1 Impersonation Attack:

An illegal user tries to fool the server in believing his identity.

Prevention:

- IP address is used for detection.
- Adversary login as the legal user IP address, writes correct service provider IP address and request the file that is needed. Here, the filename that is uploaded at the AP is checked with the IP address of the legal user.
- The attacker write his IP address to where the data is to be received, that IP address is matched with the legal user IP address and detected. The location of the adversary is updated at the authentication party.
- Through the IP address the attacker is detected.

5.2 Credential Privacy:

Credential privacy is that the dishonest service provider should not be able to recover user credential.

Prevention:

- Here, authenticated party is used in between the client and the server, server do not know who the legitimate user is. So he will not be able to give wrong service to the receiver.
- User is also not allowed to modify any file; he has the permission to read the file. If the user is modifying the file he is the attacker.
- When the user tries to modify the file, he feels like he is modifying the file, because the original file is seen. It visualizes that the attacker is writing on the file but actually the file is not modified. This trial of modifying the file is updated at the AP.

5.3 Replay attack:

This is an attack in which an adversary intercepts the data and retransmits it at valid time window.

Prevention:

- Trick is to use random no/code that is nonce in the transmitted data every time the message is being transmitted.
- Every time the message is transmitted a different random code is added to the message.
- This random number can be said as the secret key.
- The random number generated is of 32 bit and is added to the message at the end.
- Initiator untraceability: Prevention from linking the message send in communication. This is covered by using the Random number.

5.4 Denial of Service (DOS) Attack:

An adversary inputs wrong identity and password and wants to send invalid login request massage continuously to keep server busy.

Prevention:

The presented work assumes that the adversary can try to attack the system and keep the server busy. So the system is already prevented by taking precaution to not to allow the server to get overloaded.

Adversary is allowed to input wrong identity and password for 3 attempts, after that number of entering the attempts is exceeded and he is not allowed to input further for next attempt. The prevention is taken that the server is not overloaded, so only 3 attempts are allowed.

6. COMPARISON

Following table represents the summary of parameters and attacks covered by various authors in papers. N.P in the table is for not provided, authors in the papers have not explained or not discussed about the specific type of attack or parameter. As we can analyse that no paper has prevented all the attacks and parameters. The main parameter that is not covered by most of the papers is Initiator anonymity and Initiator untraceability. In our proposed work we have covered these parameters also.

Table 1 Security Properties between different papers

Method Used - Parameters, Attacks	Bio-smart card [2]	Bio- smart card [42]	Smart card [47]	Bio-smart card [51]	Our Scheme
Mutual Authenticat-ion	No	N. P	N. P	Yes	Yes
Initiator Anonymity	N. P	No	Yes	N.P	Yes
Initiator Untraceability	N. P	No	No	N.P	Yes
Password Change Phase	Yes	Yes	Yes	No	Yes
Impersonation Attack	No	Yes	N.P	Yes	Yes
Against DOS attack	Yes	Yes	No	Yes	Yes
Replay Attack	Yes	Yes	Yes	No	Yes
Credential privacy attack	No	Yes	N.P	Yes	Yes

7. CONCLUSION

Most Single sign-on schemes suffer from various security issues and are vulnerable to different attacks In this paper, we have discussed existing work done on SSO and parameters that should be considered, attacks that should be prevented to provide security to SSO scheme. We have implemented User-id and password along with biometric based SSO authentication scheme. We have applied One-way hash function and AES Encryption/Decryption algorithm for the file operation that is to the application. We have presented Security analysis of how the attacks are prevented and parameters are covered. We have also given comparison of different papers with our proposed approach. Future work is to improve Soundness disadvantage and to prevent more other attacks along with these attacks.

REFERENCES

[1]A. Menezes, P. van Oorschot, and S. Vanstone, 1996, “Handbook of Applied Cryptography”. Boca Raton, FL: CRC Press.

[2]A.K. Das, 2011,“Analysis and Improvement on an efficient biometric-based remote user authentication scheme using smart cards”, IET Information Security, vol. 5, no. 3, pp. 541–552.

[3]Arul Princy.A1, Vairachilai.S, 2013,“A Survey on Single Sign-On Mechanism for Multiple Service Authentications”, International Journal of Computer Science and Mobile Computing, Vol. 2, Issue.12, December 2013, pg.40 – 44.

[4]B. Dodson, D. Sengupta, D. Boneh and L. M. S. Secure, 2010, “Consumer-friendly web authentication and payments with a phone”. In: Pro. of the Second International ICST Conference on Mobile Computing, Applications, and Services (MobiCASE).

[5] C. C. Chang, S. C. Chang and Y. W. Lai, 2010, “An Improved Biometrics-based User Authentication Scheme without Concurrency System”, International Journal of Intelligent Information Processing, vol. 1, no. 1, pp. 41-49.

[6] C. C. Lee, T. H. Lin and R. X. Chang, 2011, “A Secure Dynamic ID based Remote User Authentication Scheme for Multi-Server Environment using the Smart Cards”, Expert System with Applications, vol. 38, pp. 13863-13870.

[7] C. S. Bindu, P. C. S. Reddy and B. Satyanarayana, 2008, “Improved Remote User Authentication Scheme Preserving User Anonymity”, International Journal of Computer Science and Network Security, vol. 8, no. 3, pp. 62-66.

[8] C. W. Lin, C. S. Tsai and M. S. Hwang, 2006, "A New Strong-Password Authentication Scheme Using One-Way Hash Functions", Journal of Computer and Systems Sciences International, vol. 45, no. 4, pp. 623-626.

[9] C.-C. Chang and C.-Y. Lee, 2012,"A secure single sign-on mechanism for distributed computer networks". IEEE Trans. Ind. Electron., 59(1): 629-637.

[10] Champakamala S, Prof Anjan K, Prof KArunakar K, 2013, "Privacy Preserving Multifactor authentication schemes in a Distributed Environment: An Overview", www.ijirs.com,ISSN 2319-9725, Vol.2, Issue 6, june.

[11] Chun-Ta Li and Cheng-Chi Lee, 2011.A robust remote user authentication scheme using smart card, Information Technology and Control, Vol.40, No.3.

[12] Chun-Ta Li, 2009. "An Enhanced Remote user authentication scheme providing mutual authentication and key agreement with smart cards", volume: 1, 517-520, international conference on information assurance and security.

[13] Chun-Ta Li, Min-Shang Hwang, 2010, "An efficient biometrics-based remote user authentication scheme using smart card", Journal of network and Computer Applications, Vol.33, no.1, pp. 1-5.

[14] D. Hankerson, A. Menezes, and S. Vanstone, 2003, "Guide to Elliptic Curve Cryptography". Berlin, Germany: Springer-Verlag.

[15] D. Hughes and V. Shmatikov, 2004, "Information hiding, anonymity and privacy: A modular approach," J. Comput. Secur., vol. 12, no. 1, pp. 3–36, Jan.

[16] Da-Zhi Sun, Jin-Peng Hual, Ji-Zhou Sun, Jian-Xin Li, Jia-Wan Zhang, member, IEEE, and Zhi-Yong Feng, 2009, "Improvement of Juang et al's password- authenticated key agreement scheme using smart cards", IEEE Transactions on Industrial Electronics, 56(6).

[17] De-Song Wang, Jean-Ping Li, 2011. "A novel authentication scheme based on fingerprint biometric and nonce using smart card". Vol. 5 No. 4.

[18] Enrique Otero Muras, Elisardo Gonz´alez Agulla, Carmen Garc´ıa Mateo, and Jos´e Luis Alba Castro, "Biometrics for Web Authentication: an Open Source Java-Based Approach", vol.62, No.1-2.

[19] Feng Hao, Ross Anderson, and John Daugman, 2006, "Combining Crypto with Biometrics Effectively", IEEE transactions on computers, vol. 55, No. 9, Sep.

[20] Gulin Wang, Jianghan Yu,and Qi Xie, 2013, "Security analysis of a single sign-on mechanism for distributed computer networks", 9(1): 294-302.

[21] Hyun-Sung Kim, Il-Soo Jeon, Myung-Sik Kim, 2011, "Enhanced biometrics-based remote user authentication scheme using smart cards", vol. 8 no 2, Journal of security engineering.

[22] J. G. Steiner, C. Neuman, and J. I. Schiller, 1988, "Kerberos: An authentication service for open network systems". In: Proc. Usenix Conference, pp. 191-202.

[23] J. Y. Liu, A. M. Zhou and M. X. Gao, 2008, "A New Mutual Authentication Scheme based on Nonce and Smart Cards", Computer Communications, vol. 31, pp. 2205-2209.

[24] J. Yu, G. Wang, Y. Mu. 2012. "Provably secure single sign-on scheme in distributed systems and networks". In. Proc. 11th IEEE International Conference On Trust, Security and Privacy in Computing and Communication (TrustCom'12), pp 271-278, IEEE Computer Society.

[25] Jacob Bellamy-McIntyre, Christof Luterroth, Gerald Weber, 2011, "OpenID and the Enterprise: A Model-based Analysis of Single Sign-On Authentication", IEEE computer society.

[26] Jean Jacob, Mary John, 2013. "Security enhancement of single sign on mechanism for distributed computer networks", vol. 3, Issue. 3, pp-1811-1814.

[27] Jingquan Wang, Guilin Wang and Willy Susilo, 2013,"Anonymous single sign-on schemes transformed from group signatures", International conference of intelligent networking and collaborative systems.

[28] Jingquan Wang, Guilin Wang, and Willy Susilo, 2013, "Secure Single Sign-on Schemes Constructed from Nominative Signatures", PP-620-627.

[29] Justie Su-Tzu Juan, Ming-Jhengli, 2010, "New Cryptanalysis of an ID-based Password Authentication Scheme using Smart Cards and Fingerprints", International Journal of Engineering Science and Technology Vol. 2(11), 6840-6844.

[30] K. Atasu, L. Breveglieri, and M. Macchetti, 2004, "Efficient AES implementations for ARM based platforms," in Proc. ACM Symp. Appl. Comput., pp. 841–845.

[31] Kee-Young Yoo, Eun-Jun Yoon , and Sung-Ho Kim ,2012, "A Security Enhanced remote user authentication scheme using smart cards", International Journal of Innovative Computing, Information and Control, vol. 8,no.5(B), pp. 3661-3675.

[32] Kee-Young Yoo, Eun-Jun Yoon, 2012, "A Robust and flexible biometrics remote user authentication scheme, International Journal of Innovative Computing", Information and Control, Volume 8, Number 5(A), pp. 3173-3188.

[33]Li X, Niu J-W, Ma J, Wang W-D, Liu C.-L. 2011, "Cryptanalysis and further improvement of a biometric-based remote user authentication scheme using smart cards", Journal of network and computer applications; 34(1):73-79.
[34] M. Bellare and P. Rogaway, 1995, "Provably secure session key distribution—The three party case," in Proc. 27th Annu. ACM Symp. Theory Comput. , pp. 57–66.

[35] M. Burrow, M. Abadi, and R. Needham, 1990, "A logic of authentication," ACM Trans. Comput. Syst., vol. 8, no. 1, pp. 18–36, Feb.

[36] M. L. Das, A. Sxena and V. P. Gulathi, 2004, "A Dynamic ID-based Remote User Authentication Scheme", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 629-631.

[37] Michel Abdalla, David Pointcheval, 2005, "Simple Password-Based Encrypted Key Exchange Protocols", in Springer-Verlag, Volume 3376, pages 191-208, Feb.

[38] Nils Fleischhacker1, Mark Manulis2, and Amir Azodi, , 2012, "Modular Design and Analysis Framework for Multi-Factor Authentication and Key Exchange", IACR.org, Vol. 3386, pages 65–84.

[39] P.Premchand2, A.Govardhan, Mohammed Misbahuddin, 2008, "A smart card based remote user authentication scheme", Journal of Digital Information Management ‰ Volume 6 Number 3, pp.256-261.

[40] R. Suganya1, A.K. Sathiya Bama, 2013, "Parallel Encryption Technique Combined With Secure Single Sign-On Mechanism for Distributed Computer Networks", International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 8, August 2013, pg 115 – 119.

[41] Rajaram Ramasamy, Amutha Prabakar Muniyandi, 2009, "New Remote Mutual Authentication Scheme using Smart Cards", Transaction on Data Privacy 2 ,PP. 141—152.

[42] S. S. Sonwanshi, R. R. Ahirwal, Y. K. Jain, 2012, "An efficient smart card based remote user authentication scheme using hash function", IEEE students' conference on electrical, electronics and computer science, 1-4.

[43] Sadiq Almuairfi, Parakash Veeraraghavan and Naveen Chilamkurti, 2011, "IPAS: Implicit Password Authentication System", International Conference on Advanced Information Networking and Applications.

[44] Sandeep Kumar Sood, 2012, "An Improved and Secure Smart Card Based Dynamic Identity Authentication Protocol", International Journal of Network Security, Vol.14, No.1, PP.39-46.

[45] Saru Kumari, Muhammad Khurram Khan, 2013, "An Improved Biometrics-Based Remote User Authentication Scheme with User Anonymity", Hindawi Publishing Corporation BioMed Research International Volume 2013, Article ID 491289, 9pages.

[46]Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K. Jain, , 2004, "Biometric Cryptosystems: Issues and Challenges", Proceddings of the IEEE, Vol.92, No.6, June.

[47] W. Juang, S. Chen, and H. Liaw, 2008, "Robust and efficient password authentication key agreement using smart cards", IEEE Trans. Ind. Electron, 15(6): 2551-2556.

[48] X. Li, W. Qiu , S. Zheng, K. Chen, and J. Li, 2010. "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards", IEEE Trans. Ind. Electron, 57(2): 793-800.

[49] Xiao-Min Wang ,Wen-Fang Zhang , Jia-Shu Zhang , Muhammad Khurram Khan, 2007, "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards", Computer Standards & Interfaces, 507 – 512.

[50] Xinyi Hunag, Y. Xiang member, IEEE, Ashley Chonka, J. Zhou, and R. H. Deng Senior member, IEEE, 2010, "A generic framework for three-factor authentication: Preserving security and privacy in distributed systems", IEEE Transactions on Parallel and Distributed System.

[51] Younghwa An, 2012,"Security Analysis and enhancement of an efficient biometric-based remote user authentication scheme using smart cards", Journal of Biomedicine and Biotechnology.

[52] Younghwa An, G. Dong, G. Gu, Yongin-Si, Gyounggi-Do, 2012, "Security Weaknesses of a biometric-based remote user authentication scheme using smart cards", International Journal of Bio-Science and Bio-Technology, 4(3)