A Review on Single Sign-On Mechanism for Distributed Computing

Dr. D. G. Harkut[1]
H.O.D, PRMCEAM, Badnera

Ms. Rinky G. Chhatwani[2]
M.E 2nd yr, PRMCEAM, Badnera

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, we discuss the various ways and mechanisms through which single sign-on is carried out to provide security to authentication scheme from illegal users and dishonest service providers. At last, we proposed Single Sign-On mechanism that is Biometric and smart card based using one way hash function and exclusive OR operation.

Keywords: *Authentication, Single sign-On, Attacks, Soundness.*

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 [18]. Single Sign-on means that after obtaining 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.

Two important concepts come while security for Single Sign-On is concerned. Soundness and Credential Privacy [8][10]. 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, Session key agreement, Computation cost. There are attacks that should be verified for the parameters [3] [14] [17] –

- Impersonation attack
- Server masquerading attack
- Insider attack
- Replay attack
- Denial of service attack
- Stolen smart card attack.

Initiator anonymity and Initiator untraceability are the concepts that should be focused for better security [23]. 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, 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 various ways and mechanisms through which Single Sign-On is carried out. Section 5 concludes this paper with some suggestions for further improvement.

2. RELATED WORK

Papers on Cryptography

In 2012, C. C. Chang et al. [2], 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 [8].

In 2013, G. Wang et al. [8], 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.

Papers on cryptography with smart card

In 2008, W. Juang et al. [21], 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 his own 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. [23], 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, S. S. Sonwanshi, et al. [18], has used the one-way hash function and exclusive OR operation to develop our scheme. A hash function must be able to withstand all known types of attack. This one-way hash function protect the most important value like as identity, password and server secret key. It's computationally infeasible to reversible. The proposed scheme satisfies all necessary requirements and withstands the various possible attacks, this mechanism provides security against attacks like Denial of service attacks, impersonation attack, replay attacks, Attack on server secret key.

Paper on Biometric with smart card

In 2011, A.K. Das, [1], 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 [1], 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. [13] [15], the authors have shown that the paper proposed by Kim, Lee and Yoo, two ID-based password authentication schemes without passwords or verifying tables, with smart card and fingerprints is insecure and vulnerable to impersonation attack. They said that the bio information pays a very important role in the user authentication schemes. 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 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. Let *A* mean the user, *B* mean the server, and *A, B share a common session key Sk*. If there is an *Sk* such that *A* believes $A \leftarrow Sk \rightarrow B$ and *B* believes $A \leftarrow Sk \rightarrow B$ for the transaction, we can say that the mutual authentication is finished between A and B [21].

B. Session Key Agreement

It is an interactive method in which for two or more parties needs to share some session key in secret. Attributes of key agreement protocols are known session key, forward secrecy [22]. At each run of key agreement protocol, user and server should produce a unique secret key and achieves its goal even in face of adversary is successful in achieving the previous session keys. The goal is even if one key compromise at one point should not expose the key of another point. Forward secrecy says that the secrecy of previous session keys is not affected even if long-term secrets of one or more entities are compromised.

C. Initiator Anonymity

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 [11]. If the Trusted Third Party (TTP) concept is considered, to each access to a service provider a user will use a different temporary identity to authenticate himself to the TTP and TTP then forwards the users request to service provider. So, the service provider knows only the temporary identity of the user not the real identity, so in this the user is anonymous to the service provider also.

D. 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.

E. 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 session key with the server through the log-in phase in advance. If user U wants to change his password from PW to PW*, user U inserts the smart card into card reader and keys in ID and PW* then the card reader checks that the user is legitimate user or not, if yes then asks the user to enter new password, then the card reader does the further processing in smart card.

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 secret key so no modification will be done. In this way impersonation attack can be prevented.

B. Server masquerading 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. But to do so the attacker requires the secret key, which is not known to the attacker and so it prevents this attack.

C. Insider attack.

The insider attack is when the user's password is obtained by the server in the registration phase [18] [21]. Therefore user password should not be known to the server. So, here the trick used to prevent the Insider attack is to use random number that is nonce and send in the massage that is hashed. So the server will be unable to get the user password.

D. **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 [9] [24] [21]. This attack can also be prevented using nonce. Two nonces are used one by the user and the other by the server.

E. Denial of service attack

In a denial of service attack [6], the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. 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. There are various measures to prevent this attack, one of them is that in login phase the card reader checks the valid user id and password [18], so it prevents the attack during this process.

F. Stolen smart card attack.

Suppose the user's smart card has been lost or stolen and the attacker can breach the information which is stored in the smart card [24]. The attacker cannot use this card until he gets the valid user id and password. It is not possible for the attacker to get the secret information along with the valid user id and password both at the same time as the message is hashed. Therefore stolen smart card attack can be prevented.

G. Attack to server secret key.

The privileged insider leaks the server secret key publically. For that the attacker needs the user id and password from the login message, but will be unable to get it because it is in hashed message, which the attacker is unable to know. In this way, attack to server secret key can be prevented from the adversary.

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 will cover these parameters also.

Table 1 Security Properties between different papers

Method Used Parameters, Attacks	Bio-smart card [1]	Bio-smart card [18]	Smart card [21]	Smart card [23]	Bio - smart card [26]
Mutual Authentication	Yes	N. P	N. P	Yes	Yes
Key Agreement	N. P	N. P	Yes	Yes	N. P
Initiator Anonymity	N. P	No	Yes	Yes	N. P
Initiator Untraceability	N. P	No	No	Yes	N. P
Password guessing Attack	No	Yes	Yes	Yes	Yes
Against DOS attack	Yes	Yes	No	Yes	Yes
Insider Attack	No	Yes	Yes	Yes	Yes
Impersonation Attack	No	Yes	N. P	N. P	Yes
Server Masquerading Attack	No	Yes	N. P	N. P	Yes
Password Change Phase	Yes	Yes	Yes	Yes	No

4. Single Sign-On Mechanisms

Secure and efficient authentication scheme has been a very important issue with the development of networking technologies. Consequently, user authentication plays a crucial role in distributed computer networks to verify if a user is legal and then can be granted to access the services requested. To prevent bogus servers' users usually need to authenticate service providers. Single Sign-On is an authentication scheme that enables a legal user with a single credential to be authenticated by multiple service providers in distributed computer networks. Single Sign-on (SSO) mechanism has been introduced so 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. User authentication has been widely used in distributed computer networks to identify a legal user who requires accessing network services. Figure 4.2 illustrates the basic structure in flow data will be carried out.

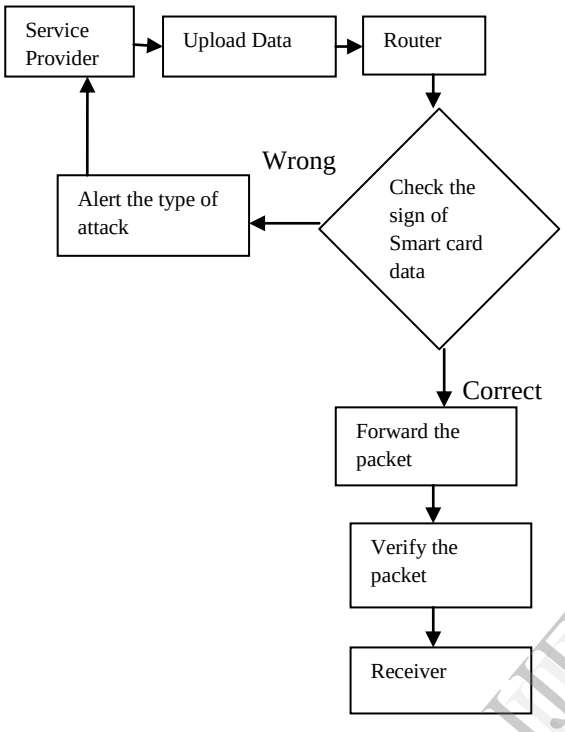

Figure 4.1 Basic structure

There are various phases in which the method is carried out and it is almost the same for all methods, but processing done in it is different by different authors.

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

4.1 Available Single Sign-On Mechanisms

In three main ways the Single Sign-On can be done is by

- Cryptography based Single Sign-On.
- Smart Card based Single Sign-On.
- Biometric based Single Sign-On.

The authors have also proposed papers based on combining these three Single Sign-On Mechanisms in different ways. As the main goal is to have secure Single Sign-On authentication scheme, various methods are being developing now a days in different domains. Figure 4.1 shows the methods of Single Sign-On mechanism.

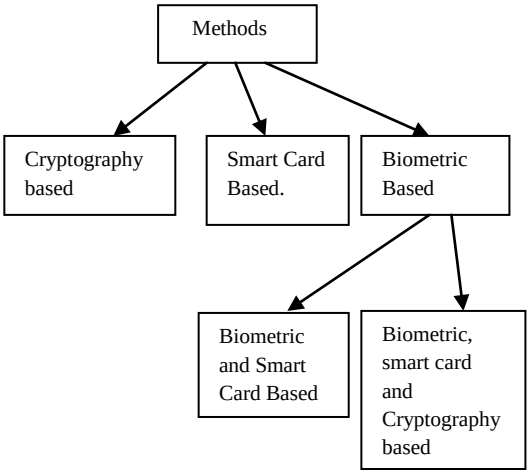

Figure 4.2 Types of SSO Mechanism.

Cryptography Based SSO: In this method, various cryptography based algorithms are used RSA algorithm [8], Elliptic curve cryptosystem [21], AES encryption [12] are used. Messages are encrypted and send to the receiver side, at the receiver they are decrypted and the process is done in four phases.

Smart Card Based SSO: In this smart card based method , user inserts smart card into the card reader and submits user id and password card reader computes and checks that the feed data is the same, if yes then further processing is done and message is hashed and send to the server [4].

Biometric based SSO: Biometric is used in SSO mechanism as biometrics is more advantageous because of its properties. It provides better security as is required for the authentication phase. User inputs the personal biometrics on the input device, if the biometric does not match the template that is stored in the system then no further procedure is carried out.

Biometric and Smart Card Based SSO: User inputs the personal biometrics input and inserts smart card in card reader and the card reader input that is user id and password is inserted. The template is matched which is stored in the system and according to result further procedure is carried [5].

Biometric, Smart Card and Cryptography based SSO: The purpose behind using these all three is to provide better security to Single Sign-On scheme. Biometrics key cannot be lost or forgotten, cannot be guessed and have various other advantages. The main motive of our proposed scheme is that to make the better and secure remote user authentication scheme with biometric, smart card in public open network. The current open network is vulnerable to various attacks.

Using one way hash function and Exclusive OR is very advantageous, as most important value like as identity, password and server secret key is protected by one way hash function. Using one way hash function and Exclusive OR operation most of the possible attacks are prevented. For Initiator anonymity and untraceability property nonce's will used. All papers have not addressed this property as it should be addressed for authentication scheme along with preventing all possible attacks. For this, biometric input is given by the user through the biometric device and user inserts smart card into card reader and inputs user id and password, this data is checked with the template stored in the system. If the template is matched then one way hash function is applied with the Exclusive OR operation and nonce is added during communication link of messages. It is well said that one way hash function along with Exclusive OR operation withstand all possible attacks [28].

5. 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. Next, we discuss various mechanisms through which SSO can be carried out and also proposed "Biometric, smart card based SSO scheme" using one way secure hash function and Exclusive OR operation with its security analysis compared over other SSO schemes. Currently, we are designing and implementing "Biometric, smart card based SSO scheme" using hash function and Exclusive OR operation. Future work is to improve the parameters considered.

6. REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

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

[7] 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).

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

[9] 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*.

[10] 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.

[11] 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.

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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.*

[18] 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.

[19] 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 http://dx.doi.org/10.1155/2013/491289.*

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

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

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

[27] Yu-heng Wan, Ding Wang, Chun-guang Ma, Lan Shi, 2012, *On the Security of an Improved Password Authentication Scheme Based on ECC*, Information Computing And Applications, Springer, LNCS , Volume 7473, pp181-188.
http://link.springer.com/chapter/10.1007/978-3-642-34062-8_24

[28] Zi- Yao Cheng, Yun Liu, Chin-Chen Chang, and Chen-Xu Liu, 2013, *A novel biometric-based remote user authentication scheme using quadratic residues*, 3(4).