ISSN: 2321-7782 (Online)
e-ISJN: A4372-3114
Impact Factor: 6.047

Volume 5, Issue 10, October 2017

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Survey on E- Commerce Applications

Raka Bisen[1]
Information Technology Department,
Ssgmce , Shegaon
Shegaon444203 – India

Shrutika Gandhi[2]
Electrical Engineering Department,
Ssgmce, Shegaon
Shegaon444203 – India

***Abstract:** Nowadays E-commerce applications are facilitating users to access resources spread at different places. The reach of people has increased and has shortened the horizon. In the completion of an e-commerce application there can be many threats and attacks scenarios possible. So security must be intact at every step in this process. A very challenging aspect of e-commerce application is user authentication which is secured and remote user authentication technique is used for backing up. Schemes presently available for remote user authentication like smart card based, password based, dynamic id based and cookie based authentication. The various authentication techniques of remote user authentication used in e-commerce applications these days are analysed here.*

***Keywords:** Remote User Authentication, E-commerce, Single Server, Multi server, Attack.*

I. INTRODUCTION

In today’s technological era of Information technology, information is spread on the network. For simplicity and security information we need advanced techniques of authentication. With the advancement of technology a very challenging task is a authenticating a legitimate user is. Remote user authentication is a method of verifying the authenticity and legitimacy of a user over an insecure network by remote server through many user authentications is a method of verifying the authenticity and legitimacy of a user over an insecure network by remote server through many techniques. It is a very tough task, because here communication is over an insecure open channel. [1] A remote password authentication scheme will be useful if it will meet some needed requirements as like it must follow the multi server’s single point registration technique [2]. No verification table will be present at server, user’s must be allowed to choose their password freely and the scheme must withstand the guessing and replay attack. Presently many conventional password based authentication technique, smart card based techniques and dynamic Id-based techniques are proposed in single server architecture, [3– 6],[9]. In multi-server environment but these techniques are not sufficient for authentication in multi-server environment. Because in multi-server architecture resources are spread on various servers, so these conventional technique may lead to password compromise and many more complexity. Number of multi-server remote user technique are proposed [16–24],[26]. On the basis of three parameters: Security, Efficiency and Cost, the various techniques and schemes can be compared.

A comparative analysis of various remote user authentication schemes presently used in Ecommerce applications and also discusses the various attacks possible, while authenticating a user remotely are presented in this paper. Then a comparative analysis of various current remote user authentication techniques has been presented. The two broad categories are first Single server Authentication and second Multi server Authentication. Then various techniques used under these schemes, their shortcomings and possible attacks are available here.

II. Attacks in Remote user Authentication

In terms of computer an attack is any attempt of unauthorized access to a system to expose, alter, disable, gain, manipulate, destroy, or copy the information present there so that the whole system get stuck. The various possible attacks in remote user authentication techniques are discussed as follows.

A. *Password Guessing Attack*: Users generally select very common and easy passwords for their ease of convenience. Same password is even used for different systems. If even one of the passwords is guessed by the attacker than the whole system is attacked. In simple password based authentication this is very common.

B. *Replay Attack*: Intruder captures the authenticated data passively and retransmits it latter to gain authorised benefits. The server is replayed by same message to achieve illegal benefits.

C. *Modification*: Modification attack means an attack modifying the content of verification table stored in server by an unauthorised person to misuse or corrupt the system. This is possible in case of verification table based remote password scheme. [6].

D. *Stolen Verifier Attack*: The attacker use the stolen verifier to impersonate as legal user in login phase after stealing the password verifier from the verification table.

E. *Server Spoofing Attack*: The sensitive data of user is gathered by setting up fake server. The useful information of user gets passed to the spoofed server because here user is unable to differentiate between the original and spoofed server. So to withstand this mutual authentication condition must be achieved in multi-server remote user authentication process.

F. *Smart Card Lost Attack:* The attacker can guess or change the user's password, and can act as a legal user if and only if smart card is losed by the user.

G. *Dictionary Attack:* Offline and online dictionary attack are two types of dictionary attack. In online dictionary attack, the attacker tries to login the server. For this he needs to guess password in dictionary order. And in offline dictionary the password is guessed by the attacker from the intercepted authentication messages.

H. *Man-in-the-middle Attack*: Here between user and client the attacker have its presence. So he is benefited by all the authentication messages that are passed through him and hence can act as client or as server as per requirement.

III. literature Survey

A. Single server remote user authentication Techniques

1) *Password based Authentication*: User authentication in computer systems has been a cornerstone of computer security for decades. The concept of user id and password is cost effective and efficient method of maintaining a shared secret between a user and computer system. User holds an ID and compatible password along with it. The user has some ID and corresponding to that a password is given. Storage of password is done in verification table and if Id is entered the password is checked at the server whether ID exists or not. But this scheme is vulnerable to stolen verifier attack. To overcome such scenario Lamport first proposed a password based remote user authentication scheme [6]. This is a verification table based approach. But if an intruder gets access to the server then the contents of the verification table can be easily modify, which results in modification attack. Many other approaches of verification table [3][4] were proposed. Hash functions and cryptographic operation based on strong algorithms such as data encryption standard (DES) were used. Cryptographic operations provide much higher level of security to password based authentication.

2) *Smart Card based Authentication*: To get rid of the problem of storing verification table in the server, an improved smart card based password authentication scheme came into existence. Smart cards are portable modest computing devices with programmable data store and certain tamper- resistance capabilities. They are embedded in plastic cards that looks like a

traditional magnetic stripe credit - card.. So it can store data corresponding to the user, which will help in authenticating the user. Smart card is more adaptable and preferred these days due to their less cost, portability and, capability of performing cryptographic operations. However, this solution is still vulnerable to attacks. Smart cards can store values. Card carriers are able to decide with whom to share data and with whom to transact business and use their cards only with those vendors they choose to trust. Most common form of smart cards is register- based, stored-value card. These can store personal digital certificates for use with SET protocol and other authentication -based protocols [Ghosh,1998].{ Initially, when this scheme was applied [7][8] it was found that, information stored inside the card can be extracted by observing the power consumption of the card or physically exposing the chip inside it. Also off line password dictionary searches were possible. Like [9] highlights and removes the forgery attack possible in [7][8], provided the information stored in smart card is disclosed. However, [9] says that if data is extracted from the card by an internal user, then impersonation attack is possible. [3] Overcomes the demerits of [9] and proposed an efficient strong smart card based password authentication protocol. It fulfils not just the minimum requirements of efficient remote user authentication but also advanced requirements like efficiency and mutual authentication.} So smart card provides a good, efficient and convenient mode of authentication but it has limitations also. So for using smart card in remote user authentication some criteria must be satisfied [5] [10]:

- Authentication server should not maintain any verification table or password table.
- Users should be able to easily choose and change their password.
- While designing the system, the low power and limited memory capacity of smart card must be considered. So that the computation and communication cost consumed by the system should be very low
- The authentication messages communicated should not reduce the entropy of the password.
- Mutual authentication condition must be satisfied to overcome server spoofing attack.
- Attacker cannot be able to extract data stored in the smart card, to gain access to the system
- Session key agreement must be there for protecting subsequent communication.

3*) Dynamic Id based authentication*: Password and smart card are widely used to provide two- factor authentication and user anonymity are two schemes of dynamic id based authentication. Many static Ids based remote user authentication schemes mainly doesn’t allow changing and choosing their passwords and user login. In dynamic Id cards, users are able to change and choose their passwords freely, and do not maintain any verifier table. Hence this scheme is more secure against ID- theft and resists reply attacks, forgery attack, guessing attack, insider attack and stolen verifier attacks. Since three parameters are now required for authenticating the user: possessing the smart card, knowing the identity, and knowing the password [35]. Das et al [11] first introduced dynamic ID based remote user authentication scheme. The security is based on one way hash function which is infeasible to inverse. But [12] [4] highlights the demerits of the Das et al.’s scheme. This is password insensitive because here any random password is acceptable to authenticate the user. So it is password insensitive. This scheme does not fulfil the basic need of authentication schemes. The weaknesses of other schemes proposed in it are smart card loose problem, forward security cannot be achieve, link ability attack, off-line password guessing attack, compromise of identity problem and cloning of smart card problem.4) Cookie Based authentication: Cookie is a piece of data stored in user’s hard drive or RAM, by the browser he is using. These are some relevant information about the user. Which is often need to be entered by the user on a particular browser. Full information about a user by a website on user’s system can be obtained by cookie. Information is stored by it on user system so repeatedly insertion of information is not needed. Cryptographic operations like message authentication code, message digest, digital signatures, and encryption are applied for securing the cookies. [17] Network threats, end-system threats and cookie harvesting threats are three possible attacks on cookies. The security services are Integrity, Authentication, and Confidentiality which are provided by cookies. Cookie can provide three authentication methods these are, Address based, Password based and Digital Signature Based.

a*) Address-based authentication:* user's system's IP Address is used as an authentication parameter. In this technique user's IP address is obtained by cookie issuer which is same as a web server and put this variable in address based cookie. Web server who has the saved IP address is matched with the user's present IP address and if it gets matched then the server considers an authenticate user otherwise it rejects. Weakness of this scheme are not feasible if the IP address of user's system is dynamically defined and not possible if the user access the website with different system. So this scheme is unprotected to IP Spoofing.

b*) Password-based authentication*: This scheme supports dynamic IP address and also supports proxy servers, to withstand server spoofing. The password inserted by the user into the system is transferred from web browser to the server and stored in password cookie as hashed password. User wants to access the server's accepting password cookies. This is verified by matching saved hash password at server with hash of entered password. However this scheme is unguarded to dictionary attack.

c*) Digital-signature-based authentication: The* public key cryptography technique is used here. DSA7 or RSA8 digital signature schemes can be used for user authentication when the public key of user is known to the web server .software is brought into use the additional browser that can generate a digital signature of time stamp generated by user's system. For example if a user want to access a remote server knowing his private key, the signature based cookie is created by users system having digital signature of time stamp generated by his system using its private key. Then the user can be authenticated by any server knowing user's public key, if he will access that server by using user's signature based cookie.

B. Multi Server Remote User Authentication Techniques: Internet has become essential part of our daily life. With the rapidly developing internet age the resources that are spread over the network on many different servers around the world are needed by the users. A user will need, repetitive login to various remote servers and a lot many sets of ID and password also need to be remembered by the user, if the conventional scheme of password authentication will be applied to the multi-server environment. Which is not achievable and must lead to compromise of ID and password. And anonymity preserving is a very important issue with the rapid use of remote user authentication in e-commerce applications. , Single Point Registration criteria must be satisfied in order to make multi-server environments user-friendly [1][2]. Many multi server authentication schemes have been proposed using various authentication techniques [10] [18–22].

1*) Session key agreement protocol*: In this protocol the concept of session key is used. The participating clients authenticate with each other and in order to protect the confidential data to be transmitted, a session key is generated. This scheme provides both authentication and confidentiality. [23] Abashing function and symmetric-key cryptosystem which is totally dependent on efficient multi-server user authentication and key agreement protocol were proposed by Juang. The secrete key is received by the user from the service provider in a shared key inquire phase is proposed, and hence each registered server's load to maintain the encrypted key table is reduced. Here smart card is not used to check identity and password in login phase. It also doesn't satisfy the criteria of user friendly password change phase. Password change phase require the registration centre. These things make it unprotected to online guessing attack, after losing the smart card. This scheme is also unguarded to offline dictionary attack, if the secret parameters stored in the smart card are extracted. It lacks efficiency also. Latter [24] an efficient and secure multi-server password authentication scheme using smart cards is proposed by Chang. Some of the important requirements of multi-server password authentication like: Choose and change password at will, Lower computation, Security, Mutual authentication, Single registration, Session key agreement are satisfied by it. But the computation cost of key agreement and the authentication phase can be decreased here. In login phase and key agreement phase in this scheme the errors in password are unable to found and is detected in only in authentication phase. Latter [20] proposed the improvement of this scheme.

2) *Neural Network Based Authentication*: This uses a pattern classification technique of identifying a legitimate user. The first neural network based password authentication schemewasproposedin1990.Latteronvariousproposalcame [25][26] into existence . The technique initially used was: the time interval between each character is collected while user is typing. It is treated as input vector in neural network. Latter in 2001 [6], proposed a remote password authentication scheme for multi-server architecture using neural networks. This is also an artificial neural network based pattern classification system for password authentication system. In this scheme, users are free to choose their password. Verification table is absent here. By using neural network, the particular user is classified. This scheme is not feasible because its time taking and cost effective for the maintenance and training of the neural network for the users.

3) *Dynamic ID Based Authentication: The* need of modern e-commerce application is user's anonymity. The full proof authentication system can be hampered if static Identity leaks out some information of the user. Hence the need of technology in present information era is dynamic ID based authentication. Many papers [22][25] [27][28] were proposed on this technique. In [22] for multi-server authentication scheme, only hash function is used. In this scheme third party is not at all needed to update the password. But it is unable to satisfy all the necessities of multi-server. But efficient computation is still achieved by the scheme. Latter [25] proposed a smart card based dynamic ID authentication technique. Here two level servers are used. These two servers are assigned as service provider and controller servers .These are used to distribute user's authentication information among them. Dynamic ID is a combination of random nonce and user's information stored in smart card. The computation cost of the scheme is very less.

4) ECC Based Authentication: The strength of any scheme is measured on basis of the three parameter: Security, cost and efficiency. Authentication scheme based on public key cryptosystem are difficult to compromise because of inherent strength of public key system. It is very expensive and time consuming because of heavy exponential calculation. Public key is not a feasible technique because as the present day requirement is the hand held mobile devices having very low power and having reach to all technologies. Symmetric cryptographic parameters are inexpensive with respect to computation cost but are much simpler to forge as that of public key cryptosystem parameter. In comparison to other public key system, maximum security per bit for a given key size is provided by Elliptic Curve Cryptosystem. Many papers [29] on ECC based authentication have been proposed. [29]This paper presents improved ECC algorithm with increased safety performance. The security by using three improvement factors over basic ECC and RSA is enhanced here. These are: optimizing squared remaining determination, private key update transformation optimization and optimizing point product operation. With small key size of this algorithm gives same security level was proposed here.

5) *Biometric Based Authentication*: A security process that relies on the unique biological characteristics of an individual to verify that he is who is says he is, called as Biometric authentication. It compares a biometric data capture to stored, confirmed authentic data in a database. Authentication is confirmed when both samples of biometric data match. Typically, it's used to manage access to physical and digital resources such as buildings, rooms and computing devices.

IV. Conclusion

In this paper the various present day remote user authentication techniques are mentioned, which are being implemented to successfully run the modern e-commerce applications. We have observed the various threats possible in these schemes .In this paper all analytical study of weakness, security analysis and attacks of various existing techniques in the area of remote user authentication is done here.

References

1. Iuon-Chang Lin, Min-Shiang Hwang, and Li-Hua Li, "A new remote user authentication scheme for multiserver architecture", Future Generation Computer Systems, vol.19, pp.1322, (2003).
2. Li, Li-Hua, Iuon-Chang Lin, and Min-Shiang Hwang. "A remote password authentication scheme for multiserver architecture using neural networks." Neural Networks, IEEE Transactions on, vol.12, no.6, pp.14981504,(2001).

3. Evans Jr, Arthur, William Kantrowitz, and Edwin Weiss. “A user authentication scheme not requiring secrecy in the computer.” Communications of the ACM, vol.17, no.8,pp.437-442, (1974).

4. Lennon, Richard E., Stephen M. Matyas, and Carl H. Meyer. “Cryptographic authentication of time-invariant quantities.” Communications, IEEE Transactions on, vol.29, no.6,pp.773-777, (1981).

5. Song, Ronggong. “Advanced smart card based password authentication protocol.” Computer Standards and Interfaces, vol.32, no.5, pp.321-325,(2010).

6. Lamport, Leslie. “Authentication of password with insecure communication.”Communications of the ACM, vol.24, no.11, pp.770-772, (1981).

7. Xu, Jing, Wen-Tao Zhu, and Deng-GuoFeng. “An improved smart card based password Authentication scheme with provable security.” Computer Standards and Interfaces, 31.4 (2009),pp.723-728

8. Lee, Narn-Yih, and Yu-Chung Chiu. “Improved remote authentication scheme with smart card.” Computer Standards and Interfaces, vol.27, no.2,pp.177-180, (2005).

9. Lee, Sung-Woon, Hyun-Sung Kim, and Kee-Young Yoo. “Improvement of Chien et al.’s remote User authentication scheme using smart cards.”Computer Standards and Interfaces, vol.27, no.2, pp.181-183, (2005).

10. Juang, Wen-Sheng. “Efficient multi-server password authenticated key agreement using smart cards.” Consumer Electronics, IEEE Transactions on50, vol.1, pp.251255,(2004).

11. Das, ManikLal, AshutoshSaxena, and Ved P. Gulati. “A dynamic ID-based remote user authentication scheme.” Consumer Electronics, IEEE Transactions on, vol.50, no.2,pp.629-631,(2004). [12] Awasthi, Amit K. “Comment on a dynamic ID-based remote user authentication scheme.” arXiv preprint cs/0410011 (2004).

12. Liao,I-En,Cheng-ChiLee,andMin-ShiangHwang.“Security enhancement for a dynamic ID- based remote user authentication scheme.” Next Generation Web Services Practices, 2005, NWeSP 2005.International Conference on.IEEE, 2005.

13. Zhai, Jingxuan and Cao, Tianjie and Chen, Xiuqing and Huang, Shi. “Security on Dynamic ID-based Authentication Schemes” International Journal of Security and Its Applications,vol.9,no.1, pp.387-396, 2015.

14. D. Wang, C.-g. Ma, P. Wang, and Z. Chen, “Robust smart card based password authentication scheme against smart card security breach”, Cryptology ePrint Archive, Report (2012)/4392012.

15. X. Li, J. Ma, W. Wang, Y. Xiong, and J. Zhang, “A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments”, Mathematical and Computer Modelling, vol. 58, no.12, pp.85-95, (2013).

16. Park, Joon S., and Ravi Sandhu. ”Secure cookies on the Web.” IEEE internet computing 4 (2000): 36-44.

17. Lin, Iuon-Chang, Min-Shiang Hwang, and Li-Hua Li. “A new remote user authentication scheme for multiserver architecture.” Future Generation Computer Systems, vol.19, no.1, pp.13-22, (2003). [19] Tsaur, Woei-Jiunn, Chia-Chun Wu, and Wei-Bin Lee. “An enhanced user authentication scheme for multiserver internet services.” Applied Mathematics and Computation,vol.170, no.1, pp.258-266,(2005).

18. Tsai, Jia-Lun. “Efficient multi-server authentication scheme based on one-way hash function without verification table.” Computers and Security, vol.27, no.3, pp.115-121, (2008).

19. Hu, Lanlan, XinxinNiu, and Yixian Yang. “An efficient multi-server password authenticated key agreement scheme using smart cards.” In Multimedia and Ubiquitous Engineering, 2007.MUE’07. International Conference on, pp. 903-907. IEEE, 2007.

20. Liao, Yi-Pin, and Shuenn-Shyang Wang. “A secure dynamic ID based remote user authentication scheme for multi-server environment.” Computer Standards and Interfaces, vol.31, no.1, pp.24-29, (2009).

21. Juang, Wen-Sheng. “Efficient multi-server password authenticated key agreement using smart cards.” Consumer Electronics, IEEE Transactions on, vol.50, no.1, pp.251255, (2004).

22. Chang, Chin-Chen, and Jung-San Lee. “An efficient and secure multi-server password authentication scheme using smart cards.” In Cyberworlds, 2004 International Conference on, pp. 417-422.IEEE, 2004. [25] Sood, Sandeep K., Anil K. Sarje, and Kuldip Singh. “A secure dynamic identity based authentication protocol for multi-server architecture.” Journal of Network and Computer Applications 34, no. 2 (2011): 609-618.

23. Obaidat, M. S., and D. T. Macchairolo. “A multilayer neural network system for computer access security.” Systems, Man and Cybernetics, IEEE Transactions on 24, no.5, pp.806-813,(1994).

24. Hsiang, Han-Cheng, and Wei-Kuan Shih. “Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment.” Computer Standards and Interfaces, vol.31, no.6, pp.1118-1123, (2009).

25. Leu, Jenq-Shiou, and Wen-Bin Hsieh. “Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards.” Information Security, IET 8, no.2 pp.104-113, (2014).

26. Wei, Xianmin, and Peng Zhang. “Research on Improved ECC Algorithm in Network and Information Security.” International Journal of Security and Its Applications, vol.9, no.2,pp.29-36, (2015).

27. Baruah KC, Banerjee S, Dutta MP, Bhunia CT. An Improved Biometric-based Multi-server Authentication Scheme Using Smart Card. International Journal of Security and Its Applications. 2015;9(1):397-408.

28. Mishra, Dheerendra, Ashok Kumar Das, and SouravMukhopadhyay. ”A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards.” Expert Systems with Applications 41, no. 18 (2014): 8129-8143. Harvard

29. Li, Chun-Ta, and Min-Shiang Hwang. ”An efficient biometrics-based remote user authentication scheme using smart cards.” Journal of Network and computer applications 33, no. 1 (2010): 1-5. Harvard

30. Li, Xiong, Jian-Wei Niu, Jian Ma, Wen-Dong Wang, and Cheng-Lian Liu. ”Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards.” Journal of Network and Computer Applications 34, no. 1 (2011): 73-79.

31. Chuang, Ming-Chin, and Meng Chang Chen. ”An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics.” Expert Systems with Applications 41, no. 4 (2014): 1411-1418.

32. Neha , DrKakaliChatterjee "Authentication Techniques For E-Commerce Applications: A Review".