INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SPECIAL ISSUE FOR
NATIONAL LEVEL CONFERENCE
"RENEWABLE ENERGY
RESOURCES & IT'S APPLICATION"

THREE LEVEL SECURITIES USING MULTISERVER AUTHENTICATION

MR. ANAND A.BIHADE, MR.YOGESH BHUYAR

Assistant professor, COETA, Akola.

Accepted Date: 12/03/2016; Published Date: 02/04/2016

Abstract: In this paper, we propose three levels server authentication system with user protection in network security. We first propose a single-server system and then apply this technique to a multi-server system. Addition to user authentication and key distribution, it is very useful for providing privacy for users. The key factors include. The privacy of users can be secured. A user can freely choose their own password.

Keywords: Network Security, Privacy Protection, Session Key, Smartcard.

Corresponding Author: MR. ANAND A.BIHADE

Co Author: MR.YOGESH BHUYAR

Access Online On:

www.ijpret.com

How to Cite This Article:

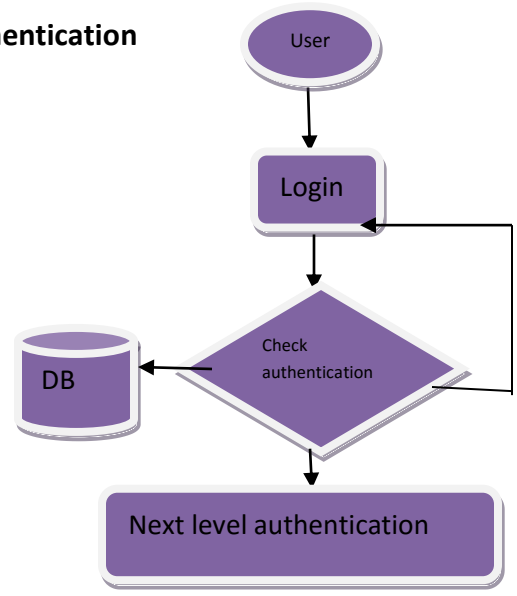
Anand A. Bihade, IJPRET, 2016; Volume 4 (8): 122-127

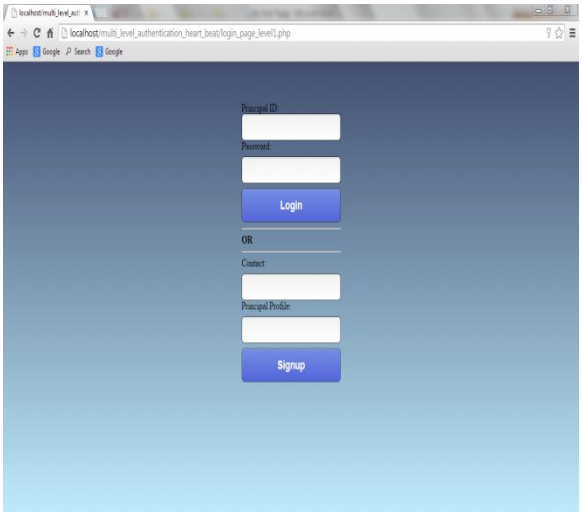
PAPER-QR CODE

INTRODUCTION

In order to provide security to the network and to the data. In ths paper we provide three levels of security. In first level of authentication is carried out by simple user id and password enter by user and password check in data base if match the can access the secure data. Only passing a password for authenticating between the user and the server is not sufficient, since it contain less amount safety and is easily hack by the intruders. In second level Before two parties can do secure communication, a session key is required for protecting subsequence communications. Also, using smart cards, remote user authentication and tokens are generated which contains client ip,server ip,client id,login time and time to leave. Security against proxy .In the first level of authentication is use to detect if the login request is coming via proxy server. In third level of authentication heart beats and eye retina are scan and toke key is generated with a session key for a specified time. Password authentication scheme at both the point of the communication. Since then, Password authentication scheme at both the point of the communication. Since then, many technique have been proposed to point out its drawback and improve the security and efficiency of Lamport's scheme.[3] Only passing a password for authenticating between the user and the server is not sufficient, since it contain less amount safety and is easily hack by the intruders. Before two parties can do secure communication, a session key is required for protecting subsequence communications. Also, using smart cards, remote user authentication and key agreement can be simplified, flexible and efficient for creating a secure distributed computers environment. It is also useful for providing identity privacy for the users.

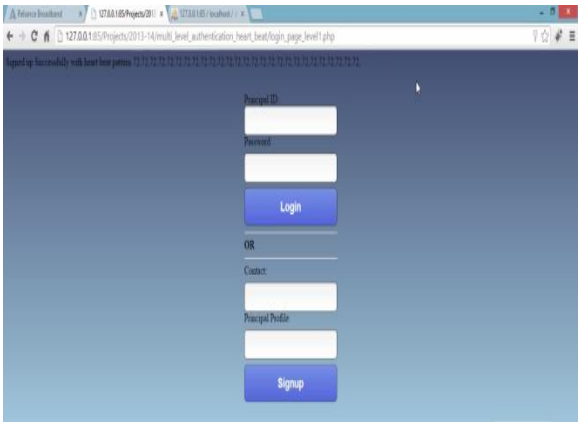
First Level of Authentication





In this level user id and password are entered by the user. Password is stored in the database. Once the user id and password entered by the user it is check in the database if the user id and password are match in the database then it is proceed to the next level. In first level of authentication security against proxy server is check. In this level of authentication is used to detect if the login request is coming via proxy server. Suppose user click on login at 3.10 pm the and sends the login reguest at 3.15 pm and login request process at 3.18pm then there is a chance that request might come from proxy server.

Second Level of Authentication.



In second level after login tokens are generated which provide the time limit if the time exit then the threshold limit the session exit.

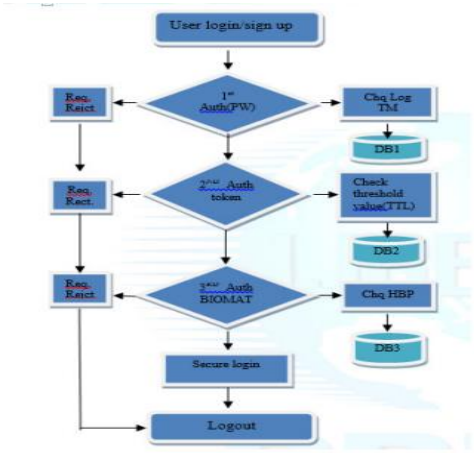
After the tokens are generated and are match in the database with the time give the it proceed to the next level. Then the secret key is generated. Which is the entered into the user id, password and the token generated with the secret key. After all the passes are match then next level is open.

Fig: Token generated

After the token then single client id is generated which is haves a time line of 5 minutes which expires after time limit.

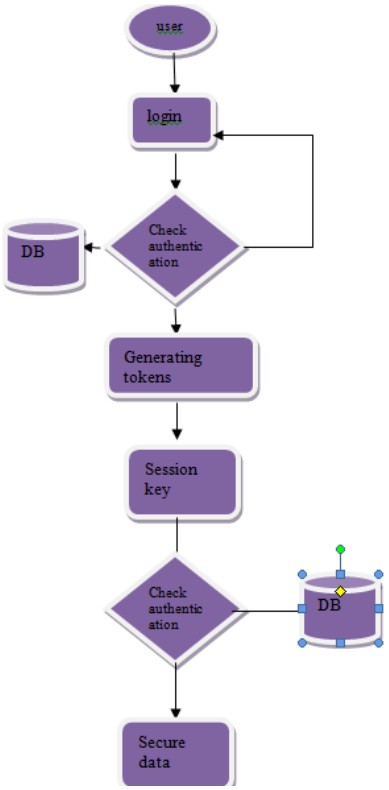
Three Way Authentication:

Security with Heart Beat while sign up the heartbeat of the user is saved in the database. So while login we record the Heart Beat of the user and compare it with save pattern to find the difference or variance. If variance is less than threshold than the user is login else logout. The security tokens generated contains client ip, client id, server ip, login time, TTL. (Time to leave) If the current ip address and the client ip matches with the ip address in the ticket it is suppose that user is not under attack but if the current ip and ip present in the ticket generated does not match the user is logout



Heartbeat Measurement

Heart rate measurement indicates the soundness of the human cardiovascular system. This project demonstrates a technique to measure the heart rate by sensing the change in blood volume in a finger artery while the heart is pumping the blood.



CONCLUSIONS:

In this paper we have presented authentication using multiserver in order to obtain data securely to avoid any attack on it various levels of authentication is begin use in order to apply authentication process to various server. Regarding the multi-server scheme, users only need to register one time and can use all provided services by service providers. Both our proposed schemes have the ability of privacy protection.

REFERENCES:

1. M. Alzomai, '' Identity Management: Strengthening One Time Password Authentication Through Usability ''. May 2011.

2. H.C. Kim, H.W. Lee, K. S. Lee , M.S. Jun, '' Design of One-Time Password Mechanism using Public Key Infrastructure''.978-0-7695-3322-3/08 © 2008 IEEE DOI 10.1109/NCM.2008.77.

3. J.L. Tsai, “Efficient multi-server authentication scheme based on one-way hash function without verification table”, Computers & Security, Vol. 27, No. 3-4, pp. 115-121, May- June 2008.

4. Y.P. Liao, S.S. Wang, “A secure dynamic ID based remote user authentication scheme for multi-server environment”, Computer Standards & Interfaces, Vol. 31,

5. 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.

6. M. Burrows, M. Abadi, and R. Needham, “A Logic of Authentication,” ACM Transactions on Computer Systems, vol. 8, no. 1, pp. 18-36, 1990.

7. Y. Chang and C. Chang, “Authentication schemes with no verification table,” Applied Mathematics and Computation, vol. 167, pp. 820-832, 2005.

8. W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory, vol. IT-22, no. 6, pp. 644-654, 1976.