A SECURED PRIVACY AUTHENTICATION WITH RECOVERY

Dr.M.Newlin Rajkumar[1], V.Dhurka[2]

[1]*Assistant Professor, Department of CSE, Anna University Regional Centre, Tamilnadu, India.*

[2]*PG Scholar, Department of CSE, Anna University Regional Centre, Tamilnadu, India.*

Abstract - ***Every person has his own data and needs it to be secure, so authentication and acceptance were found to be essential. Most web based applications are based on password level authentication only. Since passwords are easily prone to be attacked, a better authentication is needed. The biometrics and the biometric way of authentication came to existence but this also suffered from the drawback of excess hardware and complex mechanisms. This paper presents a simple and efficient user authentication approach based on OTP with four digit pin number. When the user logins into the system, the login password is matches with database and if they match, the user is identified as a legitimate user. Further, an OTP is generated and sent to the user. The user enter the OTP along with four digit pin. If this combined OTP and four digit pin is matched with database, user is authenticated. This achieves better authentication and efficiency. If user forget their password, recovery phase is available. In this phase user have to answer the query which is based on the image that is displayed by server. If the answer is matches, then password reset link will send to user's mail id.***

Key Words: *Password, Authentication, OTP*

1. INTRODUCTION

The quest for a reliable and convenient security mechanism to authenticate a computer user has existed since the inadequacy of conventional password mechanism was realized, first by the security community, and then gradually by the public. With the increasing use of the Internet as a business and social tool, it is becoming more important that secure access to sensitive and personal information can be provided. A type of network attack is Password Guessing attack. Here a legitimate users access rights to a computer and network resources are compromised by identifying the user id/password combination of the legitimate user. Password guessing attacks can be classified into two. Brute Force Attack: A Brute Force attack is a type of password guessing attack and it consists of trying every possible code, combination, or password until you find the correct one. This type of attack may take long time to complete. A complex password can make the time for identifying the password by brute force long. Dictionary Attack: A dictionary attack is another type of password guessing attack which uses a dictionary of common words to identify the user's password. Several large scale password leakages exposed users to an unprecedented risk of disclosure and abuse of their information. This shook the public confidence in the security of the current information infrastructure; the inadequacy of password based authentication mechanisms is becoming a major concern for the entire information society.

Biometrics, the application of statistical analysis to identify individuals through their biological or physiological characteristics, is emerging as a key aspect in new security systems. Using biometrics, it is possible to avoid pitfalls encountered with traditional security systems where users are required to keep information, such as passwords, safe. Biometric data can be classified as physiological or behavioral. The biometric system improves upon the security level provided by password matching while greatly reducing the risk of dictionary-based attacks. Biometric authentication is much efficient in authenticating the legitimate user but has the drawback that it uses extra specialized hardware. This kind of specialized hardware, which is basically too high cost, cannot be afforded by everyone. Moreover to use this hardware, extra complex mechanisms are required which also creates the environment which is costly in terms of time and resources. In this paper, a signature verification system is used in addition to the standard password match to identify a legitimate user. The system can be customized to multiple Internet-based applications requiring secure authentication. The system uses no specialized equipment, requiring only an Internet capable computer with a keyboard, a mouse, and a Java compliant browser; other systems require specialist equipment such as scanners (e.g., fingerprint, iris, retinal) and microphones.

2. BACKGROUND

In the existing system, there many password leakages exposed to users to an unprecedented risk of disclosure and misuse their information. These types of password-based authentication mechanisms is becoming a major concern for varieties of security based applications. Also some attacks namely called, password guessing attacking has become more concern for the users, while accessing the some of the sensitive application like Bank transaction, Train Booking and Online Shopping. Password leakages will reduce the customer's transaction in the Banking Environment. And also these password guessing attacks will allow hackers to access the account easily. Sometimes, the password guessing attacks will lead to the blocking of the customer's account and that will lead the customer's dissatisfaction. Also the user can enter into phishing site by which the user's sensitive information will be accessed by the hacker and they can use it on behalf of the user.

The Biometric way of authentication came into existence due to the lack of authentication mechanisms. The biometric systems employ extra specialized hardware and complex mechanisms for authentication which makes the task costly in terms of time, memory and other resources. The finger print recognition system requires a finger-print scanner to perform the task and carrying the scanner everywhere is tedious and it is not much practical to use it everywhere by a common man. Similarly, the voice recognition system, face recognition system, palm scanning suffers from the similar type of problems.

Here, in this type of authentication there is no need for additional hardware. Cost also low.

3. PROPOSED SYSTEM

In proposed system we using OTP (One Time Password) along with four digit pin for login purpose. The OTP is send to users' mobile phone. If they lost their mobile they no need to waste their time for buying new sim. Instead of that server will send the OTP to their mail id.

4. BLOCK DIAGRAM

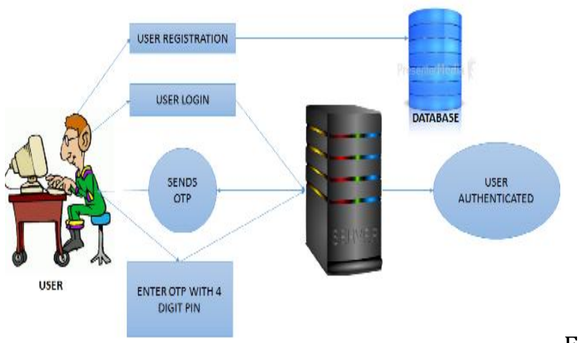

Fig 1: Block diagram for user login

There is also another block diagram for recovery phase.

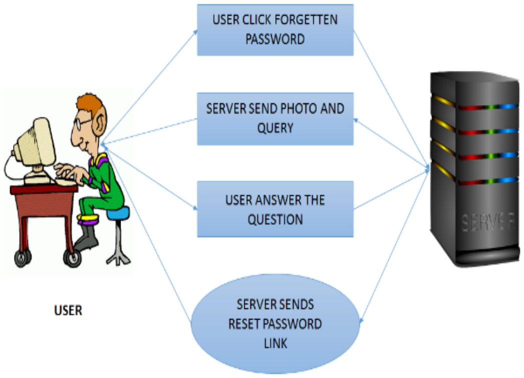
USER CLICK FORGETTEN PASSWORD
SERVER SEND PHOTO AND QUERY
USER ANSWER THE QUESTION
SERVER
USER
SERVER SENDS RESET PASSWORD LINK

Fig 2: Block diagram for user recovery

5. MODULES

The proposed system has four modules. They are,

1. Registration
2. OTP generation
3. Verification
4. Recovery

5.1 Registration

This module implements the Client interface by which the Client can interact with the Application. To access the Application, the Client User has to register their details with the Application Server. They have to provide their information like Name, Password, Date of birth, Mobile Number, Email id, Address, photo for recovery phase etc. This information will be stored in the database of the Application Server. The User is allowed to the access the application only through the provided Interface.

5.2 OTP generation

In this phase one time password is generated and sent to user's mobile phone. If the user lost their mobile phone user can request to send the OTP to their mail id. They no need to wait till they buy new sim.

5.3 Verification

In the verification phase, the server will verify the user when they login into the system. The Server will verify the password provided by the User during login time. If the password is not matched, then the Server will not allow the User to access their account. Once the User had provided their password correctly, the Server will generate the Session Key which is the One Time Password using Secure Random Number generation algorithm and send it to the User Mobile phone/Email id. Once the User received their session key in their Mobile phone/Email id, they have to provide the OTP along with their four digit pin number. Then the server validate those detail and allow the user to access their account.

5.4 Recovery

The recovery phase is used when user forget their password. To ensure that legitimate user click the forgotten password we use one method. User have to answer the question regarding the image displayed in the screen. If they gave correct answer, the password link will be sent to user's mail id.

6. CONCLUSION

Now a days so many people hacking the others social website password and banking password. Try to avoid those type of hacking this paper proposes a new kind of authentication which also very easy to authenticate and consumes less time comparing other type of authentication.

REFERENCES

[1] Anand Sharma and Vibha Ojha. "Password based authentication" Philosophical Survey, IEEE. 2010.

[2]B.Ives, K.R.Walsh, and H.Schneider, "The Domino effect of password reuse," communication ACM, vol.47, no. 4, 2004, pp. 75-78.

[3]B. Parno, C. Kuo, and A. Perrig, "Phoolproof phishing prevention," Financial Cryptography Data Security, 2006, pp. 1–19.

[4] B.Pinkas and T. Sander, "Securing passwords against dictionary at- tacks," in CCS '02: Proc. 9th ACM Conf. Computer Communications Security, New York, ACM, 2002, pp. 161–170.

[5] B.Schneier, "Two-Factor Authentication: Too Little, Too Late," in inside Risks 178, Communications of the ACM, 48(4), April 2005.

[6] C. Yue and H. Wang, "Session Magnifier: A simple approach to secure and convenient kiosk browsing," in Proc. 11th Int. Conf. Ubiquitous Computing, ACM, 2009, pp. 125–134.

[7] D. Weirich and M. A. Sasse. Pretty good persuasion: a ¯rst step towards e®ective password security in the real world. In Proc. of NSPW 2001, pages 137{143, New York, NY, USA, 2001. ACM Press.

[8] E. Gabber, P. B. Gibbons, Y. Matias, and A.J.Mayer. How to make personalized web browsing simple, secure, and anonymous. Financial Cryptography, page 1732, 1997.

[9] J. Bunnell, J. Podd, R. Henderson, R. Napier, and J. Kennedy-Mo®at. Cognitive, associative and conventional passwords: Recall and guessing rates. Computers and Security, 16(7):641{657, 1997.

[10] J. Picciotto and J. Epstein. A comparison of Trusted X security policies, architectures, and interoperability. In Proceedings of the Eighth Annual Computer Security Applications Conference, December 1992.

[11] K. Bicakci N. Baykal, "Infinite length hash chains and their applications" In: Proceedings of 1st IEEE Int. Workshops on Enabling Technologies: Infrastructure for Collaborating Enterprises WETICE'02, 2002, pp. 57-61.

[12] T. Holz, M. Engelberth, and F.Freiling, —Learning more about the underground economy:Acase-study of keyloggers and dropzones, Proc. Computer Security ESORICS 2009, pp. 1–18, 2011.