RESEARCH ARTICLE OPEN ACCESS

Database Security Two Way Authentication Using Graphical Password

Kamlesh Gupta[#1], Arshad Malik[#2], Shamal Pawar[#3] , Jijnasa Patil [*4]
[#]*Dept. Of Computer Engineering,Veermata Jijabai Technological Institute Mumbai, Maharashtra (India)*
[*]*Assistant Professor, Dept. Of Computer Engineering,Veermata Jijabai Technological Institute Mumbai, Maharashtra (India)*

ABSTRACT
As data represent a key asset for today's organizations. The problem is that how to protect this data from attackers, theft and misuse is at the forefront of any organization's mind. Even though today several data security techniques are available to protect database and computing infrastructure, many such as network security and firewalls tools are unable to prevent attacks from insider. Insider is a person working in organization who can try to access the sensitive data. This paper proposes a two-way authentication method which fuses knowledge-based secret and personal trait information.

I. INTRODUCTION

Human factors are often considered the weakest link in a computer security system. Patrick, et al. [1] point out that there are three major areas where human computer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the authentication problem.

The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember [2]. Unfortunately, these passwords can also be easily guessed or broken. According to recent new computer world article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords [3]. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts [4, 5].

To address the problem with tradition user name and password authentication, we will focus on alternative using two way authentication using graphical password and one time password.

II. BACKGROUND

2.1 Classification of Current Authentication Methods

A. Token based Authentication

It is based on something that user possess. For example Smart Cards, a driver's license, credit card, a university ID card etc. It allows the users to enter the username and password which allocate the token to the user and allow the user to access

The resources without entering the username and password. Once their token has been obtained, the user can offer the token - which offers access to a specific resource for a time period - to the remote site [6]. Many token based authentication systems also use knowledge based techniques to enhance security [7].

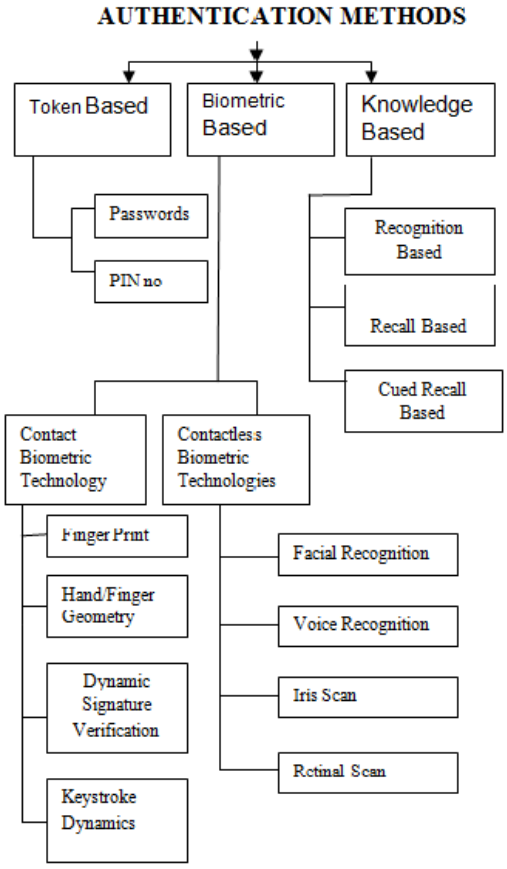

Figure1 Classification of Authentication [8]

B. **Biometric Based Authentication**

It is based on "Something you are". Biometrics is the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. It uses physiological or behavioral characteristics like fingerprint or facial scans and iris or voice recognition to identify users. A biometric scanning device takes a user's biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information a computer can interpret and verify. A biometric-based authentication system may deploy one or more of the biometric technologies: voice recognition, fingerprints, face recognition, iris scan, infrared facial and hand vein thermo grams, retinal scan, hand and finger geometry, signature, gait, and keystroke dynamics. Biometric identification depends on computer algorithms to make a yes/no decision [8]. It enhances user service by providing quick and easy identification.

C. **Knowledge Based Authentication**

Knowledge based techniques are the most extensively used authentication techniques and include both text based and picture based passwords. Knowledge-based authentication (KBA) is based on "Something You Know" to identify you For Example a Personal Identification Number (PIN), password or pass phrase. It is an authentication scheme in which the user is asked to answer at least one "secret" question. KBA is often used as a component in multifactor authentication (MFA) and for self-service password retrieval. Knowledge based authentication (KBA) offers several advantages to traditional (conventional) forms of e-authentication like passwords, PKI and biometrics [8].

III. DESIGN

This security mechanism provides better security to database. It solves the problem having with traditional username and password authentication.

3.1 System Flow

Figure 2 shows the system flow of proposed authentication system. Flow chart diagram shows the system flow when user try to login the system. User enter the user name then system will show random images include the image submitted by user during its registration process. If user select the correct image system send one time password(OTP) to user on their registered cell phone. User will enter OTP on system which define that user is authenticated user.

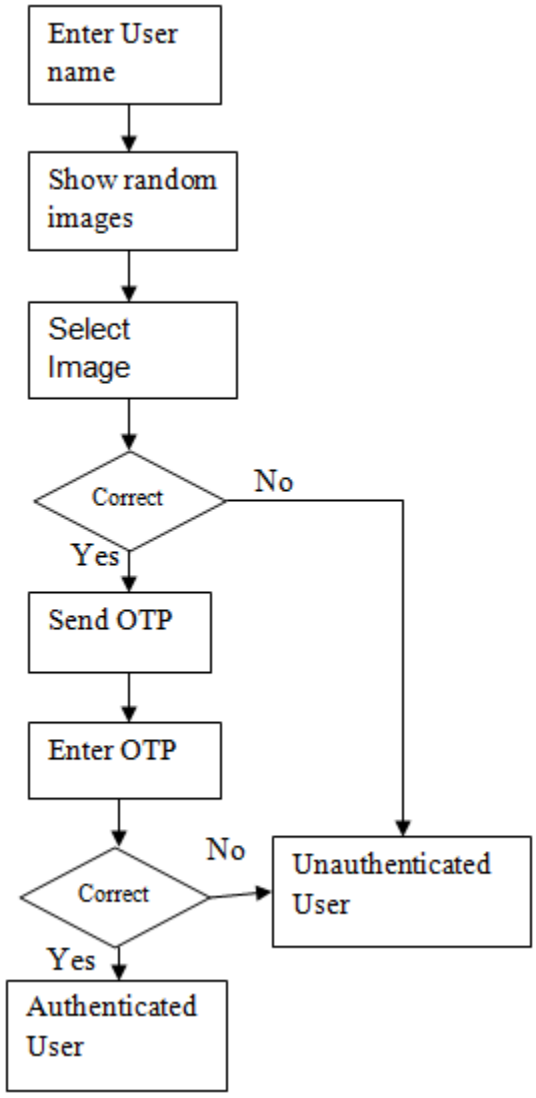

Figure 2: System View

IV. IMPLEMENTATION DETAILS

4.1 Registration

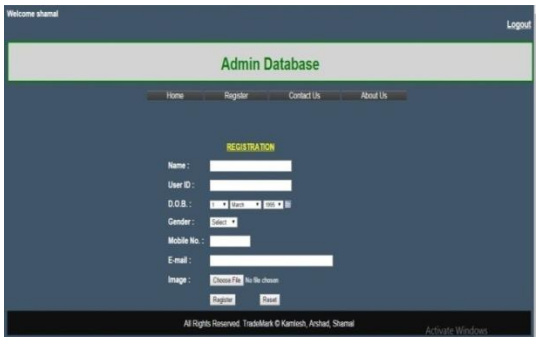

Figure 3: Registration Page

In registration process the user submit their information contain full number, E-mail Id, Image (any random image which will further used for verification in during login process). Image

submitted by user during registration process is used as graphical password. User has to remember image which he/she has submitted because system uses image as password.

V. Login Process

A. Enter Username

In login process initially system will show enter user id page. User has to enter the user id which have registered and proceed for verification.

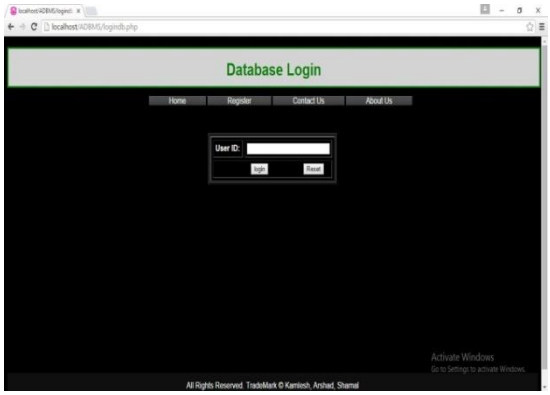

Figure 4: Enter username page

B. Graphical password selection

Figure 5: Graphical password selection

In this step system shows the random images. As shown in figure 5. System shows the random images including one image which has submitted by user as graphic password in registration process. If user select correct image, system send the one time password (OTP) to users registered number otherwise ask again to select the image and if second time also user failed to select correct image system block the system and send SMS to user that unauthorized person tried to access account. As shown in figure 6.

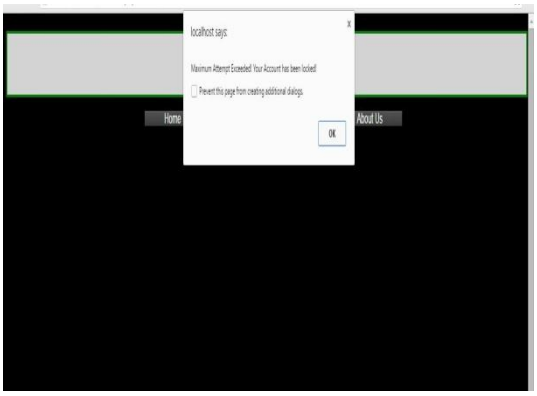

Figure 6: Exceed the change to login

C. One Time Password

When user passes the graphical password selection step, system sends OTP to user. User has to enter OTP got on cell phone via SMS. User has to enter the OTP to system as shown in figure 7.

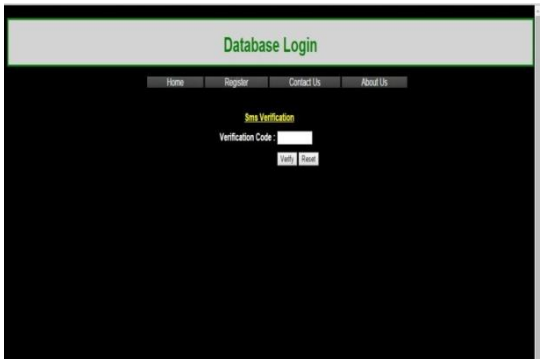

Figure 7: Enter OTP

VI. CONCLUSION

Database Security has become the important aspect in information technology. There are many authentication methods each with its advantages and disadvantages. Using picture as password is becoming popular but very less research has done in this area. Proposed system is combination of graphical password and One Time password (OTP) which provide dual secure mechanism for system. It is difficult to pass two steps of checking of authenticity. Our system aims to provide more security to system but it also has some limitations and issues comes with drawbacks of guessing of picture in graphical password and OTP such as user has activated do not disturb or some mobile network issues.

REFERNCES

[1]. A. S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA, 2003.
[2]. A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999.
[3]. K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.
[4]. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.
[5]. M. Kotadia, "Microsoft: Write down your passwords," in ZDNet Australia, May 23, 2005.
[6]. Token Based Authentication: http://www.w3.org/2001/sw/Europe/events/foafgalway/papers/fp/token_based_authentication/ [last visited on 02/05/11].
[7]. Approaches to Authentication:http://www.e.govt.nz/plone/archive/services/see/see-pki-paper-3/chapter6.html?q=archive/services/see/see-pki-paper-3/chapter6.html [Last Visited on 15/05/2011].
[8]. Kailas I Patil, Jaiprakash Shimpi, A Graphical Password using Token, Biometric, Knowledge Based Authentication System for Mobile Devices,
[9]. International Journal of Innovative Technology and Exploring Engineering 4, March 2013.