MultiFactor Authentication by Using Image Processing Techniques

Poosarla Vinay Raj [#1], Pranitha Gadde [*2]

M.Tech Scholar [#1], Assistant professor [*2]

Department of Computer Science & Engineering,
Anil Neerukonda Institute of Technology & Sciences
Bheemunipatnam (Municipality),Sangivalasa - 531162
Vishakapatnam (District), AP (INDIA).

Abstract

User Authentication is the process of confirming the identity. It majorly depends on three factors namely, something you have (Hardware token), something you are (e.g. finger print) and something you know (e.g. password). In this paper we analyse three factors of authentication, text password authentication, image sequence and image template. By providing aforementioned major factors we can increase security level and secure data from third party. As we have conducted several experiments on this three factor authentication, we finally came to a conclusion that this proposed approach is very good at providing security for the large and small scale usage person's in order to hide their valuable data.

Keywords

Security human factors, Authentication, Image password

1. Introduction

Password is an ancient term which can be a word, or image, or string used for the user authentication to provide identity to access data. The password must be kept secret. The only way to secure the user data is by using authentication. The password is a string or special character used for user's authentication to provide more security. Nowadays users are creating their passwords as their date of birth, names, mobile numbers or nickname. Some of the users (systems) store the password as a plain text. It is easy for the hacker to crack a password and in some cases, if we provide more authentication using special characters, users tend to forget the password. In this paper we propose Image authentication thereby, users cannot forgot their password. According to scientific research, the images we see and voices we hear are stored in the left part of the brain cerebral cortex layer which maintains long time memory. Supported by this theory we can confirm that users can remember their image password for long time. In this paper we can provide more authentication to something you know (password) as an outcome, third party cannot crack the password. This in turn enhances image password to be more secure than other password techniques.

2. Related Work and Assumptions

In this section, we mainly discuss the literature which is clearly related with our proposed implementation method in providing data security through three factor authentication.

2.1 Modeling

In this paper the modeling techniques has been classified into three types:

- Text password based authentication

- Image sequence based authentication
- Image template recognition

Text Password based Authentication

The first factor of authentication is text password, text or message is human readable form. Plain text is an input of encryption form and the output in the decryption form for every application or a login form (registration), authentication process first step is the login of the text password. The text password is used to provide the authentication for user. The Gmail, yahoo and many social networking sites provide the text password as the first authentication level and the input is given as the user's name (text). The password is denoted by some special character according to user's requirements and the passwords are created. These passwords provide security only to some extent. The third party users can also crack the password, hack the information. Additionally there are some tools available in online to crack the password. In this paper we have used image processing authentication techniques to provide more security to users in so doing, we are not allowing any third party users to crack the password.

Figure 1. User selects the sequence of images

Image Sequence based Authentication

The image is termed as a visual output. Information available in image form is easily understandable to everyone. Through image processing we can hide and send the data. The second multifactor authentication is the image sequence. In this image sequence we provide password authentication. As we know from our prior discussion that user can forget the text password but not the image there by making it more efficient. In this paper we developed image sequence technique. Initially, user has to upload 8 images in web page. The images user uploads should be identical like route map images of user from one place to another. These eight images together form password. This kind of images make only user identify. The user can select the images on his wish. Once the user selects his sequence order, password can be generated based on the sequence order. The user has only three attempts to provide correct password. This password provides high security and cannot be cracked by unregistered users.

Figure 2. User arranges his password in sequence order

Image Template Recognition

The third factor of authentication is image template recognition. In this paper, we follow image template technique to improve security. We provide set of images to the user that are already stored in the web page. User will select one of the images and draws a pattern on that image as their wish in a recognized manner. This grants the access to the user and now, the user is an authenticated user. Whenever the user tries to login he has to draw the pattern which was given at the time of registration. By this image template recognition technique a more authenticated password is provided.

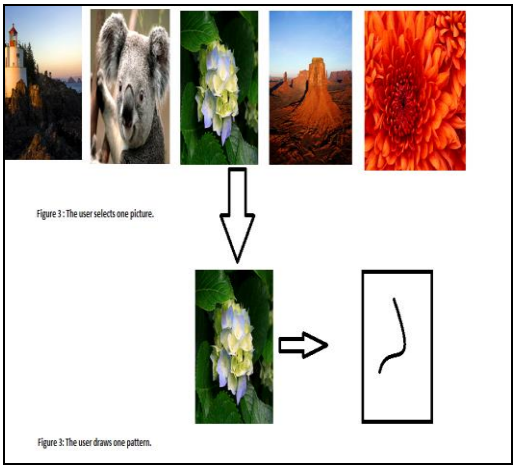

Figure 3. User selects one picture

3. Proposed Algorithms

As mentioned about to implement Image Template we used two algorithms which are related to Image classifications. They are

- Support Vector Machine Algorithm.
- Histogram based Support Vector Machine Algorithm.

3.1 Support Vector Machine Algorithm

Support Vector Machine is practical learning method based on statistical learning theory. This theory was invented by Vladimir N. Vapnik and the current standard incarnation was proposed by Corinna Cortes and Vapnik in 1993 and published in 1995. This theory was used for classification, regression or other tasks. In general, larger the margin, lower the generalization error of the classifier. By using certain calculations for our authentication process this theory can be used like, the pattern which was drawn on the image by the user will be detected by the algorithm and noted the margin values (vectors) of the pattern as a code. These margin values of code will be match with the code which was drawn at the time of login. So, this way we can authenticated our page using support vector machine algorithm.

3.2 Histogram Based Support Vector Machine Algorithm

Histogram Based Support Vector Machine Algorithm is an algorithm that is used for finding suitable representations for the images, and retrieval generally involving comparisons of images. In this paper for our Image template authentication technique this algorithms plays a vital role. As the pattern is drawn on the selected image by the user, that image will be represented as a black and white image and produces a vector calculation for that image. This vector code is calculated by using certain formulas. Based on those vector codes the validation of the user will be done. This algorithm improves the security of our pages and avoids unregistered users.

4. Proposed Implementation Modules

Implementation is a stage where the theoretical design is automatically converted into

practical form. This is mainly divided into following three modules.

4.1 Text Password Module

To login into the web page, the user have to fill the registration form which contains all the details of the user such as, username, first name, last name, email, phone number, date of birth, password and confirm password. Every field has its own validations for example; password must contain one alphabet, one special character and must be a minimum of eight digits. Once the user fills the detail fields they will be stored in the database. To login into the web page, user has to enter his username and password. If the username and password are matched with the database, the user is successfully logged into the web page. User is also provided with forgot password which sends the password to the respective user email. Once the user enters correct username and password, the user is directed to the next web page.

4.2 Image Sequence Module

We implement image sequence technique for the creation of password after the completion of text password, to improve the security level in password creation. Once the user enters the registration fields, the user will be directed to the next page which has fields as discussed later, user has to upload eight images and user will give sequence order to the uploaded eight images. The sequence order is as per the mouse click count on the image. This sequence order is stored in the database as password of the user and whenever the user login in to the page one has to click the same sequence order which was created during registration. The sequence order of images should match with the database, once the password is matched user is successfully logged in.

4.3 Image Template Module

To improve the security to more extent, we implemented a technique of image template which provides much efficient password than text password and image sequence password. Once the user enters the fields in the registration form, the user is directed to the next page wherein, user will be provided with five images, user has to select one image randomly and draws a pattern on that particular image. This image with pattern is treated as password. Whenever user wants to login into the page, firstly he has to enter the username. If the username is a valid username then it will direct to a page which contains the five images and then user has to select one image and draws the same pattern which was drawn at the time of registration. The validation of password will be done by using certain algorithms. If the image password matches the user will be successfully logged in. Every user has only two attempts to login into the page. If the user had more than two wrong attempts, the user will be automatically blocked. In this paper, we implemented three factors of authentication to provide more security to the user and to avoid access from any unauthorized users.

5. Conclusion and Future Scope

Aforesaid are the three factors of authentication to make a password more secure and help users from the unauthorized users. In this paper we have applied image processing technique for the purpose of authentication. As a future enhancement, we can use bio-metric technology as fourth factor of authentication.

6. References

[1] Support Vector Machines for Histogram-Based Image Classification, Olivier Chapelle, Patrick Haffner, and Vladimir N. Vapnik.

[2] Support vector machine From Wikipedia, the free encyclopedia Hsu, Chih-Wei; and Lin, Chih-Jen (2002). "A Comparison of Methods for Multiclass Support Vector Machines", IEEE Transactions on Neural Networks.

[3] Principal component analysis From Wikipedia, the free encyclopedia.

[4] A Simple SVM Algorith S.V.N. Vishwanathan, M. Narasimha Murty.

[5] Image processing with neural networks—a review M. Egmont-Petersena, D. de Ridderb, H. Handelsc.

[6] Lecture M. Unser, EPFLseealsowebsite: http://bigwww.epfl.ch/

[7] FourthFactor Authentication: Somebody You Know John Brainard RSA Laboratories Bedford, MA, USA.

[8] Fast Approximate Correlation for Massive Time-series Data Abdullah Mueen UC Riverside mueen@cs.ucr.edu

7. About the Authors

Poosarla Vinay Raj is currently pursuing his 2 Years M.Tech (CSE) in Department of Computer Science and Engineering at Anil Neerukonda Institute of Technology & Sciences, Bheemunipatnam (Municipality), Sangivalasa, Visakhapatnam. His area of interests includes Information Security.

Pranitha Gadde is currently working as Assistant Professor, in Department of Computer Science and Engineering at Anil Neerukonda Institute of Technology & Sciences, Bheemunipatnam (Municipality), Sangivalasa, Visakhapatnam. Her research interests include Networks Security & Information Security.