User Authentication: A Three Level Password Authentication Mechanism

Gouri Sankar Mishra¹, Pradeep Kumar Mishra², Parma Nand³, Rani Astya⁴, Amrita⁵
Department of Computer Science & Engineering, SET, Sharda University
¹gourisankar.mishra@sharda.ac.in, ²pradeepkumar.mishra@sharda.ac.in, ³parma.nand@sharda.ac.in, ⁴rani.astya@sharda.ac.in, ⁵amrita.prasad@sharda.ac.in

Abstract. User authentication is one of the cutting edge research to provide access to legitimate users. A number of mechanisms like biometric, image based, graphical based have been implemented. In this research work a three level password authentication is proposed and reported experimental results. From the result analysis it is found that the three level authentication provides reliable security level in comparison to the existing mechanisms.

Keywords. Text-based password, authentication, color-code detection, bot attack recognition, graphical password.

1. Introduction
The paper is based on verification and validation methodology for the user authentication. The proposed system verifies the legitimate user if he or she claims to be. The security system has three levels to crack through, before a successful login. Until now there are already so many different password system but seems to be failed because of bot attacks. Which is why this system mainly focus on bot attack. Out of the three phases, one phase is completely dedicated for bot attack in order to prevent system hack by using bot. Therefore, the proposed system is designed to get the utmost level of security for user authentication.

The application has three phases for the login. The login parameters increase with each level. The user must pass all the phases in order to login into the system successfully that too in first attempt. If in second or third phase the user gives the wrong input then the user will be diverted to first phase instantly. For new users, they can sign up and set the password and color code of their choice. The three phases that are: simple login id and password based security which is basic authentication, after this system will advance to its second phase, which is bot-attack detection, where system will detect if you are a real human user or bot, if passed then third and the final phase will come into action, which is color-code based password authentication. With three completely different phases the chance of breaking into application are negligible. A simple bot attack or fake user can not just break into the system.
The new methodology hybridizes the new technique on the older systems to obtain the advantageous features of both technologies.

The three level security in the proposed system consists textual password, recognition of bot-attack and detection of color code. Previously the textual as well as graphical passwords are used individually whereas in the proposed system it has been combined together for reducing threat of security. In addition the bot attack recognition module provides security from programmed attacks.

2. State of art
These days, many hackers hack the private data of the users for their advantage for example, bank card details etc. There are many security methods are used but still no improving on the secure protection because mostly the existing approaches are easily to crack or hack. For instance, the password is too easy for guessing and loss to someone. The existing systems are having password protection like:-

- Security Questions: User have to choose a question during sign up and set the answer for it. While authentication user need to answer the same question in order to verify his/her identity to the system.
- Old Password: If you do not remember your current password, in that case user can enter the last password that he/she remembers using with the system and can easily gain the access.

3. Challenges of Existing Systems
Problem with password based authentication is this it is old and common and traditional method running since decades to provide basic security. The main problem with text password arises when user create simple password for easy to remember. Thus, passwords are easy to recognize and break. Thus, result into malicious activities.

However, many attempts have been made since years in order to make strong text password. To name a few examples, combination of number, special characters, case sensitive alphabet characters and unique sequence of number and alphabets such that no single alphabet is repeated in consecutive order. This makes these passwords difficult to remember by the users.

Still the problem remains same, a simple computer program code can easily break into even into these complex simple text based passwords. Thus, only password based authentication for system is not secure enough.

4. Proposed Methodology
The proposed methodology contains three levels of verification of identity. In the first level the textual passwords are verified. Textual verification of passwords are one of the primary and existing methodologies widely used for authentication. On successful verification of
textual passwords the user is verified for bot attack. The programmed software may generate different combination of alphabets, symbols and numerals which may successfully go through the textual password verification phase. The bot attack recognition module allows the legitimate users to go for the third level of authentication. In the third level a color code detection module verifies the legitimate users providing the highest level of security. The architecture of proposed methodology is given in Figure 1.

![Figure 1. Three level password authentication system](image)

Followings are the procedures for the users to set their own authentication credentials.

The new users are asked to register by providing the details in the registration form. Then the users are directed to set their password three level passwords. These passwords are required along with each level of authentication as described in the proposed methodology. After successful verification in three levels users can successfully login into the system.

4.1. Level 1: Text-Based Password

The first phase of this application is basic authentication with validations for fields and length. Basic authentication includes entering a user id and user password, that is text based authentication. This is most traditional approach in use since last 3 to 4 decades. The reason for this is that it is very easy to implement, cost effective, simple and familiar to almost everyone. Text password contains case sensitive alphabet characters, numbers, and special symbols too. Combining this becomes a secret pass code for every user, which he or she should never share to anyone.
4.2. Level 2: Bot-Attack Recognition

The second level of this project checks if the claiming user is human or not. As the claiming user can be any robot or well-designed computer program that may be trying to break the system. Thus, it is important to check if the claiming user is really a human or robot.

In this phase, the application displays four random images every time and user will be asked to choose the human image. As rest three images are not of human. As, if the user is any robot or computer program then it will not be able to click on the right image. Thus, if the claiming user is human then only application will allow to pass through this phase and redirect user to the “third phase”

4.3. Level 3: Color-Code Detection

In this level user needs to enter the color code that was set during the time of registration. The password. There are total five colors and user needs to pick any three colors in a particular sequence. Then during the time of log in user will have to enter the same code and in the same sequence. The order of colors will always appear in random order, so user must remember the code, hit and try will simply not work as there are total 120 combinations of color in this security check. Where user will have only one chance to fill the correct order, the moment pattern mismatches user will send back to login.

The overall procedure of authentication is based upon the textual password verification in first level. This verification is static in nature. After successful verification the users are asked to draw a pattern which is dynamic one. This phase restricts the bots to break through the system as the patters are dynamic in nature. Another dynamic verification is employed in the third level for color detection. The three level of authentication can be employed for the sensitive data access systems minimizing the threat of identity theft.

5. Experimentation

To implement the designed methodology, a complete system with all its components are developed. This system contains the front end which the users interact with the system and a backend to keep the data. The verification modules are programmed, tested and evaluated manually.

5.1. Java/JSP (Backend)

Java is an object oriented backend language; it is platform independent which means it is not system oriented. It will convert the source code into the bytecode which is non-readable by human. This bytecode will make the java platform independent.

Java Server Pages also known as JSP is a server side programming language used to develop dynamic content like web pages. JSP have rights to Java API library including read/write. JSP uses tags to write the code in frontend pages. It is the enhanced update of Servlet Technology.

5.2. MySQL (Database)

Database is used to store the large amount of data for the future use in the form of table and files, it gives access to manage retrieve add delete or update the data. In a way we can perform all CURD operations with the help of database in our application. It helps in wide range of applications such as warehousing, e-commerce and logging applications, etc. MySQL is a type of relational database which is purely based on Structured Query Language (SQL).It store the data in the form of tables.
5.3. **HTML5 (Front-end)**

HTML stands for Hypertext Markup Language. HTML5 is the enhanced update of HTML. It is used to write the UI/UX content for any application, does not need extra software to write the code. It develops the web pages using simple language and the built-in tags. HTML creates the static pages. It can add functionality like; music, images etc.

5.4. **CSS3 (Front-end)**

CSS stands for Cascading Style Sheets used to style the content of web pages. It is used to modify the look and feel of the web applications. CSS can make changes like add color, hover effect, set the alignment and margin, add gradient etc. CSS3 is the enhancement of CSS2 having better technology like selectors level 2D and 3D transformation etc.

5.5. **Bootstrap4 (Front-end)**

Bootstrap is a styling framework for HTML and CSS in order to build a website more faster and easier way. It provides HTML and CSS based design templates for font style, Button style, color types, CSS class names, table types, navigation, images, modals, carousels, etc. Apart from HTML and CSS it also gives support to JavaScript. Also for any problem solving, bootstrap has a very large community to provide help.

5.6. **JavaScript (Front-end)**

JavaScript also known as JS is a scripting language which mean it is already interpreted and does not require compiling. It is used to add the functionality to the HTML pages on the client-side like, update the content dynamically, add event listeners etc. JavaScript support object oriented and can render the server side data on client side. In recent years JavaScript has broaden its area now it supports backend language like node.js.

6. **Results**

The experimental results of the 3 tier authentication is found to be achieving 98.39% accuracy. This methodology is also found to be more reliable in comparison to the methodologies previously implemented namely biometric authentication, image based authentication, graphical, shape and text based authentication mechanisms. The comparison of these methodologies are given in Fig.2.

Here the execution is carried out for a 3 tier authentication for an application. The user requires to be authorized to Appeal services from the system. Earlier a user can be attested to the system, he accepts to register with the system for the beginning time. This procedure is called registration. Therefore, for a new user, the user must register with a system and then authenticated before he can request for a service. The first level of authentication is a Text based authentication where a verification is performed using a text.
Figure 2. Comparison of authentication mechanisms

The second level bot attack recognition authentication, where a verification is executed using an human image. And the third level of authentication is a color code detection, authentication, where to choice the three color. Verification is executed to keep up privacy and it provides protection too. User Verification can be ameliorated by employing both text password and structured image. From the analysis of results in can be recommended for the sensitive data accessing systems to deploy three level authentication model.

7. Conclusion
The objective of this research is to improve the security of the system for which a number of published papers are surveyed. It is found from the experimental results that the three level authentication systems provides more security than one way or two way authentication system. Three levels are efficient because user needs to go through three different phases of authentication with the increased difficulty. Firstly we have a simple basic authentication using text based user id and password. Now With the benefit of having three level password authentication we can check a bot and user security code so we cover all three major fields of security. However time complexity can be high but security is also high and there are regions where you can compromise with little bit of time complexity but not at all with data security.

References
[1] C.T. Li and M.-S. Hwang, “An Efficient Biometrics-Based Remote User Authentication Scheme Using Smart Cards,” J. Network and Computer Applications, vol. 33, no. 1, pp. 1-5, 2010.
[2] P.C. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” Proc. Int’l Cryptology Conf. (CRYPTO), pp. 388-397, 1999.
[3] T.S. Messerges, E.A. Dabbish, and R.H. Sloan, “Examining Smart-Card Security under the Threat
of Power Analysis Attacks,” IEEE Trans. Computers, vol. 51, no. 5, pp. 541-552, May 2002.

[4] Y. Dodis, L. Reyzin, and A. Smith, “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data,” Proc. Int’l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), pp. 523-540, 2004.

[5] N.K. Ratha, J.H. Connell, and R.M. Bolle, “Enhancing Security and Privacy in Biometrics-Based Authentication Systems,” IBM Systems J., vol. 40, no. 3, pp. 614-634, 2001.

[6] Security Analysis and Implementation of JUIT-IBA System using Kerberos Protocol, Proceedings of the 7th IEEE International Conference on Computer and Information Science, Oregon, USA, pp. 575-580, 2008.

[7] Richard E. Newman, Piyush Harsh and Prashant Jayaraman, “Security Analysis of and Proposal for Image Based Authentication,” 2005.

[8] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. A Second Look at the Usability of Click-based Graphical Passwords. ACM SOUPS, 2007.

[9] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, A New Graphical Password Scheme Resistant to Shoulder-Surfing.

[10] Z. Zheng, X. Liu, L. Yin, Z. Liu A Hybrid password authentication scheme based on shape and text Journal of Computers, vol.5, no.5 May 2010.

[11] Chris Ullman and Lucinda Dykes, Beginning Ajax (Programmer to Programmer), Paperback, March 19, 2007.

[12] A. Bhargav-Spantzel, A.C. Squicciarini, E. Bertino, S. Modi, M. Young, and S.J. Elliott, “Privacy Preserving Multi-Factor Authentication with Biometrics,” J. Computer Security, vol. 15, no. 5, pp. 529-560, 2007.

[13] S. Goldwasser, S. Micali, and C. Rackoff, “The Knowledge Complexity of Interactive Proof-Systems,” SIAM J. Computing, vol. 18, no. 1, pp. 186-208, Feb. 1989.

[14] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, “Biometric Cryptosystems: Issues and Challenges,” Proc. IEEE, Special Issue on Multimedia Security for Digital Rights Management, vol. 92, no. 6, pp. 948-960, June 2004.

[15] C.-I. Fan and Y.-H. Lin, “Provably Secure Remote Truly Three-Factor Authentication Scheme with Privacy Protection on Bio-metrics,” IEEE Trans. Information Forensics and Security, vol. 4, no. 4, pp. 933-945, Dec. 2009.