

Webpage Login System

Ms. Chetana Kawale^{*1}, Mr. Dhiraj V. Patil²

Professor, Department of Computer Applications, SSBT's COET, Jalgaon Maharashtra^{*1}

Research Scholar, Department of Computer Applications, SSBT's COET, Jalgaon Maharashtra, India²

Abstract: The Web page login system is a web-based application intended for online registration. The main objective of this application is to make it interactive and its ease of use and provide security. It would make information of students / employees and selection about their category easier. The application also provides a multiple option feature so that a user can fill proper information. The main emphasis lies in providing a user-friendly search engine for effectively showing the desired results. With the rapid evolution of the wireless communication technology, user authentication is important in order to ensure the security of the wireless communication technology. Password play an important role in the process of authentication. Due to the issues, there are many solutions has been proposed to improve the security of wireless communication technology. In this paper, the previously proposed solution will be used to enhance the security of the system. The solution adopted is the one-time password, hashing and two-factor authentication. In this context, we have tried to explain how we have aimed to bring security to a common online system. And how we have limited the number of users with the help of the login system. And we have brought restrictions to those who are outside abusers. In short, we have made it clear how we can strengthen the login system in the future.

INTRODUCTION

1.1 Backgrounds

Authentication is an activity to authenticate the person credential that wishes to perform the activity. In the process of authentication, the password enter by the user will be transmitted along the traffic to the authentication server in order to allow the server to grant access to the authorized user. When the password is transmitted, the attackers will try to sniff into the network to obtain data that include the user's password. Currently, there is rainbow table which able to trace the password with the hash algorithm to obtain the user's password. Once the password is succeeded to be decrypted, the attackers can use the user credential to do something illegal such as fraud others which will cause the user lost in credit. According to Pagliery (2014), there is 47% of the American adults account been hacked in that year. Their personal information is exposed by the hackers. Due to the problem exists, there are more people no longer trust that password will be able to protect their online account. According to Suleiman (2017), some of the attackers will sell the email account that is been hacked to others to gain profit.

1.2 Overview of a System

A Web page Login (Form) system is a web-based application that allows students to fill and enter information at select time, about won info. Here is an overview of the various components of a student management (Form) system and Traditional system, which was mainly paper-based, required a large amount of space to store information. It limits the exchange of information, updating and causes loss of documentation. A collaborative work in this system becomes rigid and degrades performance. This project on the student information management system is one complete information management solution for students and staff of any educational institution. A webpage login system is the process that a user credentials are shared on the Web to gain access to some protected (or otherwise private) content. The steps in this flow are a user sends some credentials to a server, which compares it with the database, creates a session and gives you back a temporary session that later is used to match against its own database when you resume your browsing. The system exploits both front-end technologies such as HTML for form generators and back-end scripts, languages, and databases to process data and to ensure security.

1.3 Physical Documentation System

The drawbacks of physical based document there are significant costs, inefficiency, exposure to environment and security threat along with potential data corruption. Physical documents are hard to organize, protect and retrieve compared with digital records posing significant threat for any business.

- **Time is wasted:** Workers may squander hours each workweek rummaging around in files or piles in search of lost documents. Carrying, sorting and picking up manually is too boring and will make precious time wasted.
- **Not enough scalability:** As the business grows so does the paperwork and therefore needs more storage space and

more staff. Less collaboration: Sharing physical papers with remote workers or between teams is slow and doesn't work, so communication is harder and decisions take longer. Human error: People will make mistakes when they write down information on paper, like using old versions of documents, entering data wrong or writing illegible handwriting.

- **Security:** There are some problems like theft or misuse of physical authority, which leads to irregularities in transactions. And the important information that is in the hands of the thief or misuser is not properly disposed of, which is why there is a possibility of a lot of loss.
- **Mental pain:** What happens on one occasion that you have to stand in a crowd to do paperwork and have to go around the room, which causes physical pain?
- **Money fraud:** What happens in physical documentation is that we give our documents to the officer but for some reason they do not give our documents for further processing. Then it happens that our important work gets interrupted and due to inconvenience of further work, financial fraud also occurs. Therefore, online document upload is an affordable option.

1.4 Problem Statement

Authentication is an activity to authenticate the person's credentials to perform the exercise. In the process of authentication, the password entered by the user will be transmitted along the traffic to the authentication server to allow the server to grant access to the authorized user. When the password is transmitted, the attackers will try to sniff the network to obtain data that includes the user's password. Currently, a rainbow table can trace the password with the hash algorithm to receive the user's password. Once the password is succeeded to be decrypted, the attackers can use the user credential to do something illegal, such as fraud which will cause the user to lose credit. According to a report, many accounts have been hacked yearly due to weak authentication systems. Hackers expose their personal information. Due to this problem exists, there are more people who no longer trust that passwords will be able to protect their online accounts. Some of the attackers will sell the email account that has been hacked to others to gain profit. It is vital to protect our accounts because our credit is priceless. It is hard to trace the attackers in the cyber world. A secure login system is needed to ensure cyber safety. Therefore, this project would like to provide alternative ways to log in to a plan because the current login system needs to be more secure.

1.5 Goals and Objectives

Login system is web based application .it use to fill form online .its use full for student and other Department and Login system stores and management the filling record workload, personal information, record, and more. It's a means of streamlining the work and tracking all the data generated by category, consolidating everything into one system rather than multiple records.

- No Crowds
- No Pressure.
- Saves time and Security
 - The main objective is to implement a secure login authentication system with two factor authentications. Using the concept of two-factor authentication could help increase the login system's strength. The attacker will need to pass through the next barrier of defines to success to log in. This system will help to enhance the login authentication system.
 - Apart from that, the third objective will be to generate a one-time password offline. This will help perform the login procedure if there is a limited connection of Wi-Fi or the mobile signal is weak. It will help the user who lives in the countryside and has a weak phone signal.

1.6 User Interface

The user interface is the part of the system that user interact with. It typically includes a home page, form page, checkbox and user account page. Login management system is software which is helpful for students as well as the school authorities and other sector. In the current system all the activities are done manually. It is very time consuming and costly. Our student management system deal with the various activities related to the students

1.7 window

The login window for an online form system typically includes the following elements:

Username/Email field: This is where the user enters their registered username or email address.

Password field: This is where the user enters their password. For security reasons, the password field usually displays dots or asterisks instead of the actual characters.

Forgot Password link: This link allows users to reset their password if they forget it. Login button: This button submits the user's login information and logs them into the system

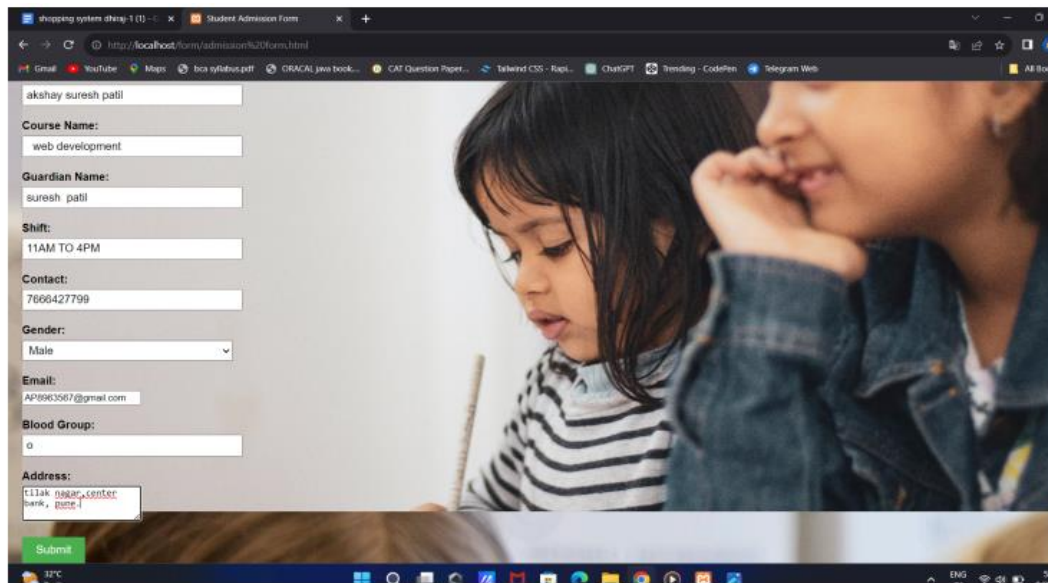


Figure 1 home page

1.8 Database Design

The purpose of the database is to handle information as an integrated whole. A database is a collection of interrelated data stored with minimum redundancy to serve may include users quickly and effectively. After designing input and output, the analyst must concentrate on database design on how data should be organized around user requirements. The general objective is to make information access easy, quick, inexpensive, and flexible for other users. During the database design, the following purpose is concerned-

- Controlled Redundancy
- Data Independence
- Accurate and Integrating
- Recovery from failure
- Privacy and Security
- Ease of learning and use

1.9 Database connection using Php my admin

We use xampp server and php myadmin for database connection User fill form and this infer mention store in our database in tabular format we create database.

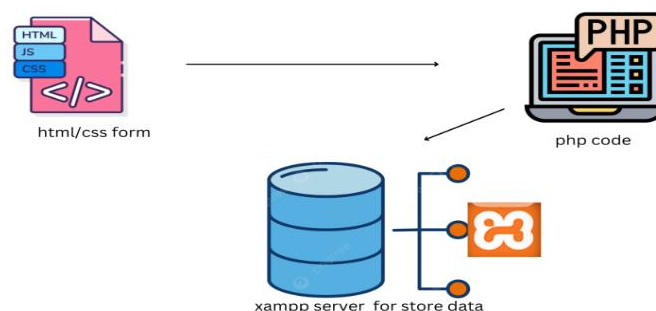


Figure 2

1.10 Challenges

- Availability: The system should always be available, meaning the user can access it using the website. A replacement page will be shown in case of a hardware failure or database corruption. Also, in case of a hardware failure or database corruption, backups of the database should be retrieved from the website data folder and saved by the administrator.
- Performance: The system is interactive, as users can post and reply to the existing posts. The data loading is fast because in the database the posts & replies of those posts are saved.
- Reliability: As the system provides the right tools for problem-solving, it is made so that the system is reliable in its operations and for securing sensitive details.

LITERATURE REVIEW

In this world of online, there are various methods to open locks and login, but in the future we can come up with a stronger login method and I am sure that this method will not be misused. The above study is based on the following source and in this study, more information about the webpage login system can be found.

1) Khan, W.Z.; Xiang, Y.; Aalsalem, M.Y.; Arshad, Q. Mobile phone sensing systems: A survey. *IEEE Commun. Surv. Tutor.* 2012, 15, 402–427. Mobile phone sensing is an emerging area of interest for researchers as smart phones are becoming the core communication device in people's everyday lives. Sensor enabled mobile phones or smart phones are hovering to be at the center of a next revolution in social networks, green applications, global environmental monitoring, personal and community healthcare, sensor augmented gaming, virtual reality and smart transportation systems. More and more organizations and people are discovering how mobile phones can be used for social impact, including how to use mobile technology for environmental protection, sensing, and to leverage just-in-time information to make our movements and actions more environmentally friendly. In this paper we have described comprehensively all those systems which are using smart phones and mobile phone sensors for humans good will and better human phone interaction.

2) Dasgupta, D.; Nag, A.K.; Roy, A. Adaptive Multi-Factor Authentication System. This book provides the state-of-art account of authentication technologies which covers not only basic authentication methodologies but also emerging technologies which are yet to be deployed and adopted by industry. This book is the outcome of last 5 years extensive literature review on authentication, research, and project implementation of specific authentication technologies. Specifically, the concept of negative authentication

3) Kumar, S.A.; Ramya, R.; Rashika, R.; Renu, R. A Survey on Graphical Authentication System Resisting Shoulder Surfing Attack. In *Advances in Artificial Intelligence and Data Engineering*; in today's modern world, security is a major concern. To provide security, the most widely recognized authentication methods are credentials, OTP, LTP, etc., and these methods are more prone to brute-force attack, shoulder surfing attack, and dictionary attack.

4) Li, Y.; Yun, X.; Fang, L.; Ge, C. An Efficient Login Authentication System against Multiple Attacks in Mobile Devices. *Symmetry* 2021. Access management of IoT devices is extremely important, and a secure login authentication scheme can effectively protect users' privacy. However, traditional authentication schemes are threatened by shoulder-surfing attacks, and biometric-based schemes, such as fingerprint recognition and face recognition that are commonly used today can also be cracked. Researchers have proposed some schemes for currenattacks, but they are limited by usability. For example, the login authentication process requires

5) Patel, J.; Patel, A. A Survey on Different Authentication Schemes for Session Passwords. *Int. J. Sci. Res. Sci. Eng. Technol.* 2015 to provide the security mainly authentication and authorization is given to the system. For that purpose mostly textual passwords are being used. Now day's graphical passwords are also available. The password schemes those are being used by now Days are mostly textual password and the graphical password (pattern matching), textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing.

6) Narayanan, A.; Shmatikov, V. Fast dictionary attacks on passwords using time-space tradeoff. In *Proceedings of the 12th ACM conference on Computer and communications security— CCS*. Human-memorable passwords are a mainstay of computer security. To decrease vulnerability of passwords to brute-force dictionary attacks, many organizations enforce complicated password-creation rules and require that passwords include numerals and special characters.

METHODOLOGY

The structure of the working system is an important step for research work because it is through the working system that we reach our work. In this chapter, we saw that there are parts of the working system and its evidence is through its structure. And through this evidence and work, the working method is studied.

1 System Requirement

There is 2 device that requires respective system requirement. For the laptop requirement suggested will be as listed as below.

- 1) OS Window XP and later/Mac OS
- 2) RAM 2GB

3) Processor Intel's dual-core Core i3-4130

4) Hard drive 1GB of free space

Apart from system requirement of the laptop, the project also requires a list of system requirement for the mobile. The suggested requirement is stated as shown below. CPU type Intel Pentium 4 RAM 1GB OS Android 6.0 above Version 1GB of free space Memory 500MB

2 Xampp Server

Database XAMPP helps a local host or server to test its website and clients via computers and laptops before releasing it to the main server. It is a platform that furnishes a suitable environment to test and verify the working of projects based on Apache, Perl, MySQL database, and PHP through the system of the host itself.

3 Methodology Development Model

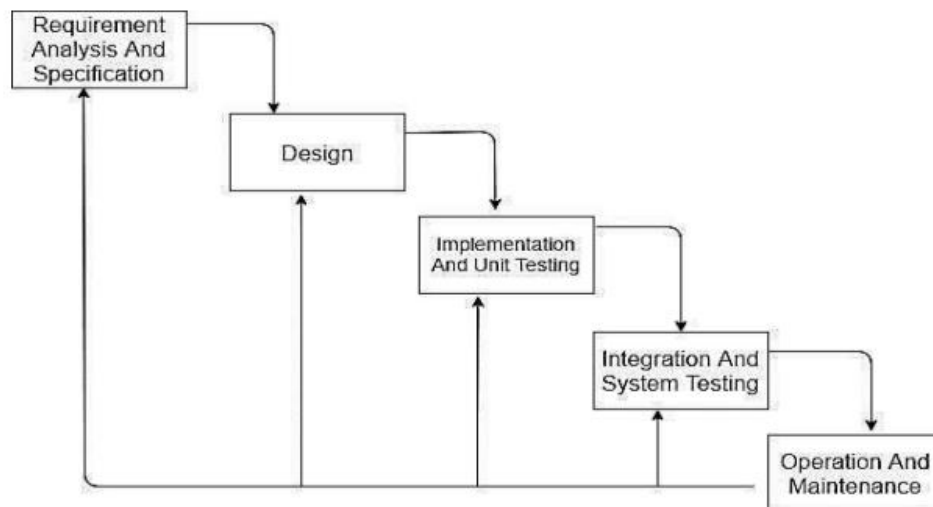


Figure 3 water fall model

- **Requirement Gathering and analysis** – All possible requirements of the system to be developed are captured in this phase and documented in a requirement specification document.
- **System Design** – the requirement specifications from first phase are studied in this phase and the system design is prepared. This system design helps in specifying hardware and system requirements and helps in defining the overall system architecture.
- **Implementation** – with inputs from the system design, the system is first developed in small programs called units, which are integrated in the next phase. Each unit is developed and tested for its functionality, which is referred to as Unit Testing.
- **Integration and Testing** – All the units developed in the implementation phase are integrated into a system after testing of each unit. Post integration the entire system is tested for any faults and failures.
- **Deployment of system** – Once the functional and non-functional testing is done; the product is deployed in the customer environment or released into the market.
- **Maintenance** – There are some issues which come up in the client environment. To fix those issues, patches are released. Also to enhance the product some better versions are released. Maintenance is done to deliver these changes in the customer environment.

CONCLUSION

Conclusion what do I mean by a review of the work done. And the final result of the work done. So in this way we understand the outline and working method of the work method through the conclusion, as well as we get an idea of the tools and methods needed to get the final result. So in this way we have used this method in our project. In the web page login system, we concluded that how much we can strengthen this login system and how much we can increase its security. How do we solve the continuous fraud? In the future, we can use high-quality technology in this system so that. No one will have any problem or fraud while working online in the future. And the personal information of the user will also be confidential.

REFERENCES

- [1]. Khan, W.Z.; Xiang, Y.; Aalsalem, M.Y.; Arshad, Q. Mobile phone sensing systems: A survey. *IEEE Commun. Surv. Tutor.* 2012, 15, 402–427
- [2]. Dasgupta, D.; Nag, A.K.; Roy, A. Adaptive Multi-Factor Authentication System. U.S. Patent 9,912,657, 2018
- [3]. Li, Y.; Yun, X.; Fang, L.; Ge, C. An Efficient Login Authentication System against Multiple Attacks in Mobile Devices. *Symmetry* 2021,
- [4]. Kumar, S.A.; Ramya, R.; Rashika, R.; Renu, R. A Survey on Graphical Authentication System Resisting Shoulder Surfing Attack. In *Advances in Artificial Intelligence and Data Engineering*; Springer: Berlin/Heidelberg, Germany, 2021
- [5]. Patel, J.; Patel, A. A Survey on Different Authentication Schemes for Session Passwords. *Int. J. Sci. Res. Sci. Eng. Technol.* 2015,
- [6]. Narayanan, A.; Shmatikov, V. Fast dictionary attacks on passwords using time-space tradeoff. In *Proceedings of the 12th ACM conference on Computer and communications security—CCS*.
- [7]. Gupta, P.; Gupta, P. Multibiometric Authentication System Using Slap Fingerprints, Palm Dorsal Vein, and Hand Geometry. *IEEE Trans. Ind. Electron.* 2018