

Web-based attendance system with OTP implementation

Luai Ahmed Haidar Al-Mesbahi
 School of Technology
 Asia Pacific University of Technology
 and Innovation (APU)
 Kuala Lumpur, Malaysia
 TP047128@mail.apu.edu.my

Julia Juremi
 School of Technology
 Asia Pacific University of Technology
 and Innovation (APU)
 Kuala Lumpur, Malaysia
 julia.juremi@staffemail.apu.edu.my

Mohamed Shabbir Hamza
 School of Technology
 Asia Pacific University of Technology
 and Innovation (APU)
 Kuala Lumpur, Malaysia
 mohamed.shabbir@staffemail.apu.edu.my

Abstract— Technology have changed our world in many ways possible and it has changed the concept of the way we live by computerizing most of the tasks that we do on regular bases such as the way of taking attendance of the students. Attendance Management System is a web based system developed for maintaining the attendance of the student on the daily basis in any constitution. Here the staffs, who are handling the subjects, will be responsible to mark the attendance of the students. Each staff will be given with a separate username and password based on the subject they handle. An accurate report based on the student attendance is generated here. This system will also help in evaluating attendance eligibility criteria of a student. Report of the student’s attendance on weekly and monthly basis is generated.

Keywords—OTP, 2 factor authentication, logging, privacy, confidentiality

I. INTRODUCTION

According to a research which was done by [1] for developing a new attendance system where implementing two factor authentications is the best solution which could be implemented in terms of securing the login function of the system. The research paper shows how using a standard algorithm of login into any system could be very dangerous and possibly could harm the system in terms of getting hacked easily. The online web application system should be designed only with newest tech of graphical user layouts by which it means the simplicity, light weighted pages and flexible to all sizes screens and many more. In addition, the system uses the Bootstrap model to through the user's intuitive experiences.

It has become a standard of the university that all students must go to 80% of class in each subject course in the semester so that they will be qualified to attend the final exam and pass the module. To make sure that only authorized people could access the system makes it accurate since no one can access and manipulate the student’s attendance data to increase the student’s attendance. This can be happened by securing the process of logging into the system to check whether the user is the one allowed to access the system or not and to do so OTP will be the best option. Adding a second layer of security will require the user to authenticate by a username and password and if he/she succeed that another way of authentication is needed by entering the SMS code received to verify that this users is allowed to get access. Fig.1 shows the example of web module for an online attendance system. This computerized system permits the parents of the students to monitor and catch up on the attendance of their kids whenever

and anyplace continuously by using of the web-interface system. Also, it allows the guardians of the students to have reports of their students' attendance through E-mail [1].

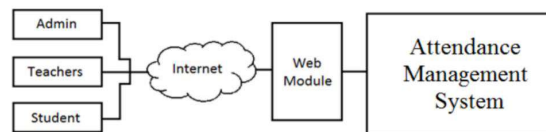


Fig. 1. Prototype of Web Attendance System

II. INTEGRATION OF OTP WITH WEB-BASED SYSTEM

A. One Time Password (OTP)

One-time Passwords (OTP) will help to increase current user IDs and passwords with an added authentication layer to improve security for all authorized users. The explanation is that the OTP will also have to be breached if a password were stolen, as well to obtain entry. Its method of authentication is called two factor authentication, a better form of authentication. This One-time password or OTP as illustrated in Fig.2 could be used for only one-time access such as accessing any system the user is required to enter this one-time password to authenticate that he/she is authorized to get access [2]. This OTP is not saved in the database of the system so it is impossible to save it since it will be generated every time the users require logging into the system. Cell phones have been very popular in modern days. Despite the rise in services for customers in diverse industries, misuse of knowledge has often risen. To make the verification system more protected from security breaches, the OTP method is a powerful solution for verifying user authentication in a specific field [3].

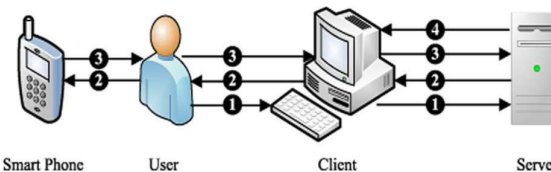


Fig. 2. One Time Password (OTP)

B. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. Advanced encryption

standard (AES) was Announced in 2000 by (NIST) National Institute of Standards and technology to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 rounds depending on key size. It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications [4][5]. These steps used to encrypt 128-bit block

- The set of round keys from the cipher key.
- Initialize state array and add the initial round key to the starting state array.
- Perform round = 1 to 9: Execute Usual Round.
- Execute Final Round.
- Corresponding ciphertext chunk output of Final Round

III. SYSTEM ARCHITECTURE

The proposed system will be running in a very secure environment using multi security layers that protect user information from various attacks and cybercriminal daily threats. The main security features of the system are focusing on the user privacy and the Login process by using the OTP method, the website will ask the user to provide the OTP code that consists of 6 digits, when request for logging into the system.

Moreover, this system has designed to be a full function Attendance management system such as adding students, staff and admins, recording the student’s attendance, login and logout, as well as the users can edit his own profile. In addition, an admin will have full access to add, edit, delete Intakes and Courses into the system and the staff will be assigned to an Intake so that he only can add, edit, delete the students assigned into that intake. Furthermore, this website will be secure from the attacks by using SSL/TLS (HTTPS) connection as well as database will be encrypted to compile the security features.

The main features which the developer has focused into is the process of logging into the system especially for the users of the system such as the admin and staff because those accounts will have access to most of the system access and could see and modify the students information. Securing the process of logging into the system by adding another layer of security such as OTP will enhance the security in the system since even if the users credential has been leaked of hacked still another process of authentication is needed to make sure that the user of the account is the one authorized to get the access.

This system has three level of access (Admin, Staff, Student): In this system developer has added one level of access to the system by the developer to perform some daily functions that help the company in managing their resources such as updating the daily income and the distance spent to determine the proper time to send the vehicle to the service department. Fig. 3 shows the system architecture for the proposed system.

A. System Architecture

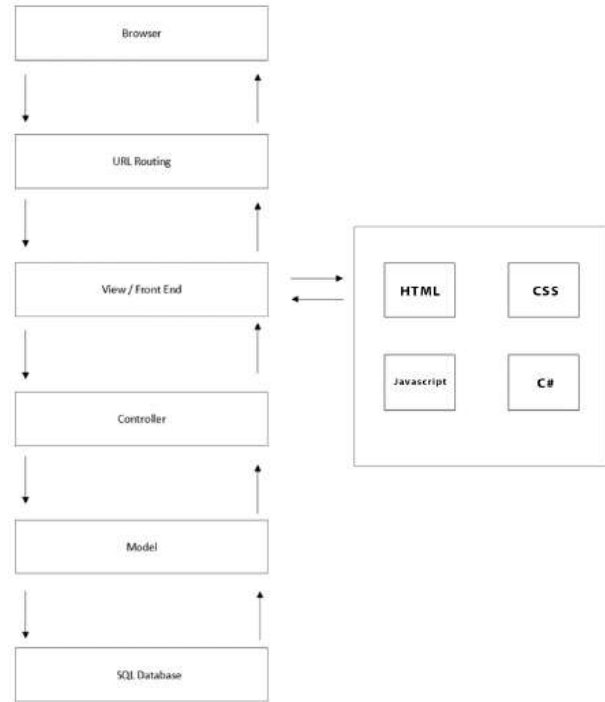


Fig. 3. System Architecture

The Admin is able to surf the application with the help of browser, Microsoft Edge, Chrome, Firefox Mozilla, and Brave; any of these is recommended for better performance. The browser then routes the URL of system and front end/ View is accessed. View is controlled by Controllers. Controllers goes through model to the database from which the data are fetched.

B. Login With OTP

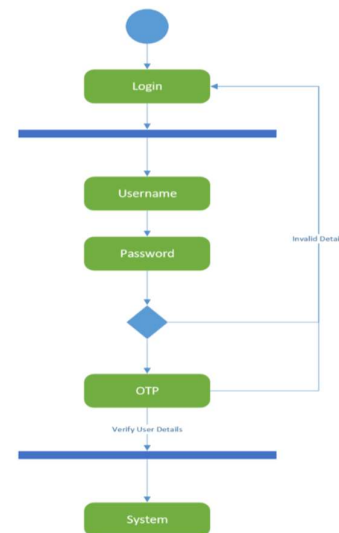


Fig. 4. Login Page with OTP

The login page as illustrated in the activity diagram in Fig.4 will be have a username and password textbox for the system user to enter his credentials in order to get access to

the attendance system. In addition, the student can get his password in case he forgot using the forgot password function. After the user logs into the system successfully a one-time password is send to the users registered email to verify that the user is authorized to access the system and no other person is accessing his account.

C. System Interfaces

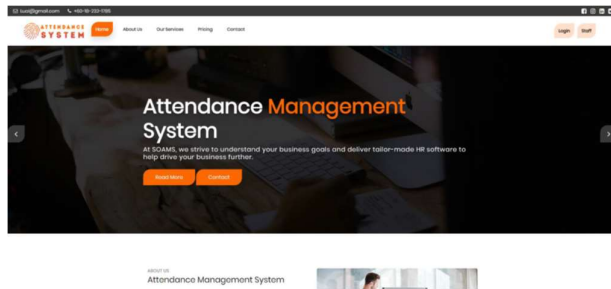


Fig. 5. Homepage of the Attendance System

Fig. 5 above shows the home page of the Secured Online Management System The home page also consists of the slide show that give since of the interface design as well as the company mission and vision that give short briefing about the company goals and objectives.

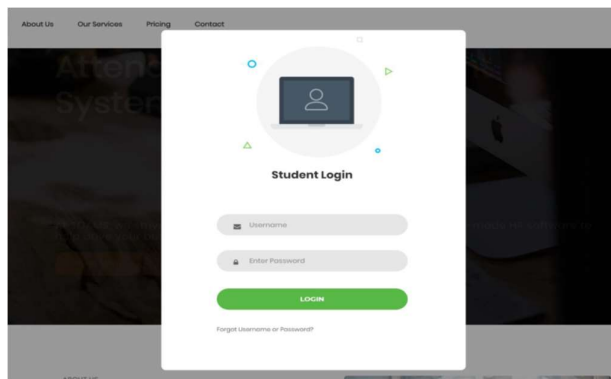
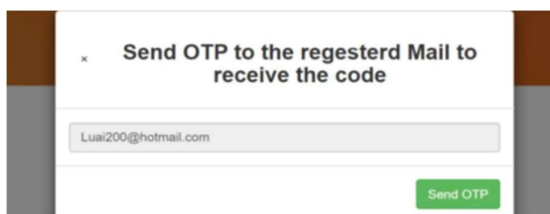


Fig. 6. Student Login Page

The login page contains several actions that the user can take and the login page also has many scenarios, If the user has completed the registration process, the user will be able to login by providing Username and password and login as normal login, the other scenario is that if the user forgot his password the system can send the users details after the users provide the email registered in the system.

Fig. 7 shows the screenshots for the OTP verification process which will be send and verify through email.



OTP

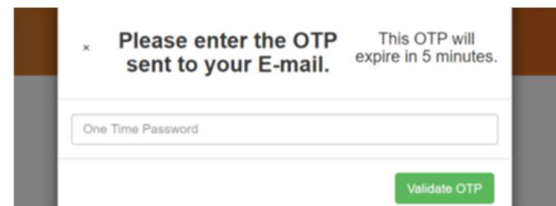
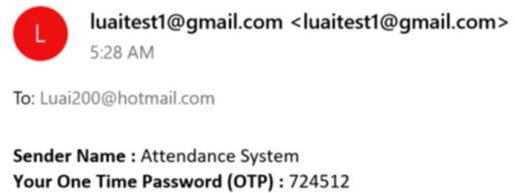


Fig. 7. OTP Verification Page and Process

Fig.8 shows the total student in each course by selecting the intake and course desired, if any field is left empty the system will required to fill in that field first and the last scenario is that if no student is registered yet the system will display no student registered. the add attendance page will require the staff to enter the course chosen in the intake assigned too and if the staff tried to enter the select button without choosing the course a massage will be displayed for the staff asking to select course first. After the staff selects the desired course the list of students will be displayed with the date of the attendance recorded.

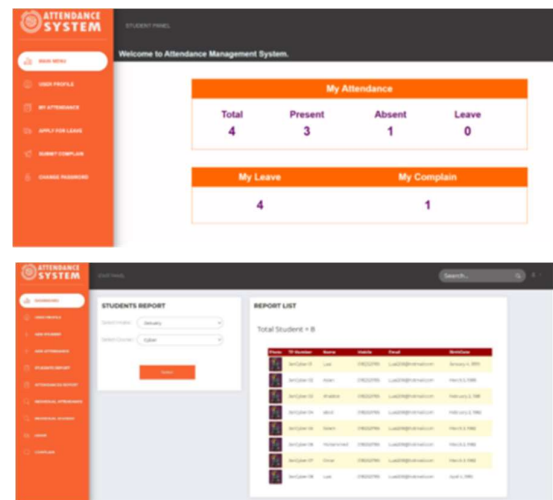


Fig. 8. Student attendance report

IV. UNIT TESTING & USER ACCEPTANCE TESTING

In the face of all testing the researcher has good test output evaluation results. Several results have been shown in Fig.9. After checking the unit test, the researcher noticed that any part of the secure online attendance system functions without any problems. The developer found that there were a few areas without operation, so that a consistency so reliability check needed to allow development. The developer has now implemented some improvements to indicate signs of

improvement and eliminate deformities. The project has been collecting some consumer feedback about what they would like to learn later by utilizing product approval research. It will encourage the creator to change the program to make the customer feel more comfortable with the program and pleased.

Test Case ID	Test Conditions	Description	Expected Result
TC3	Enter OTP: Empty	Leave the field of the verify OTP empty	Please fill out this field
TC3	Enter OTP: 12	Enter the OTP wrong	Wrong OTP
TC3	Enter OTP: 546381	Enter Correct OTP	Correct OTP and give access to the user
TC3	After OTP expire	This OTP will expire in 5 minutes.	Wrong OTP

Test Case ID	Test Conditions	Description	Expected Result
TC8	Course: Empty Date: Empty	Leave all the field empty	Total Attendance = 0
TC8	Course: Cyber Date: Empty	Leave the Date field empty	Total Attendance = 0
TC8	Course: Cyber Date: 01/01/1999	Fill in all the Date and course fields but there is no attendance recorded on that date	Total Attendance = 0
TC8	Course: Cyber Date: 01/01/2020	Show the attendance List of the students in the selected course	Show total attendance list

Tester: Jubair Al-Nazi											
Position: Security researcher											
Date: 10/08/2020	Location: Parkhill Residence										
Time Start: 05:00 PM	Time End: 5:20 PM										
No.	Category	Scale									
		1	2	3	4	5	6	7	8	9	10
1	Flexibility of using secure online attendance website.										✘
2	Clarity of website components.										✘
3	Alignment of Content.										✘
4	website design										✘
5	Over all GUI Impression.										✘
6	Adequacy of Functionality.										✘
7	Prevalence of Errors.										✘
8	security features										✘
Comments: the security of the system is well worked on in addition to the functionality of the system											

Tester: Abdulmalek Alshugga											
Position: Developer											
Date: 09/08/2020	Location: Parkhill Residence										
Time Start: 12:40 PM	Time End: 1:10 PM										
No.	Category	Scale									
		1	2	3	4	5	6	7	8	9	10
1	Flexibility of using secure online attendance website.										✘
2	Clarity of website components.										✘
3	Alignment of Content.										✘
4	website design										✘
5	Overall GUI Impression.										✘
6	Adequacy of Functionality.										✘
7	Prevalence of Errors.										✘
8	security features										✘
Comments: The system is achieving all the objectives mentioned and everything works perfectly. The security part in the website is okay and working accordingly											

Fig. 9. Sample of Unit Testing and User Acceptance Testing

IV. CONCLUSION

The implemented system has several of functionalities and features such as OTP and password encryption but still more improvements can be made with the proposed system such as right now it's only web based compatible and only works using the browser. The second limitation is that the implemented system can only record the attendance once and cannot update once it is made. Lastly, all the admin and staff who has control over the implemented system have full exposure and this could result in issues. Since the system is controlled by humans, there is a higher risk of errors occurring because people are most prone to produce them. Human activity may also slow down the cycle of functioning as opposed to artificial sensors.

REFERENCES

- [1] J. Jacob, K. Jha, P. Kotak, "Mobile attendance using Near Field Communication and One-Time Password," International Conference on Green Computing and Internet of Things (ICGCIoT), pp. 1298-1303. IEEE, 2015.2015.
- [2] Posb., One Time Password (OTP) for Online Transactions. Retrieved from posb: <https://www.posb.com.sg/personal/support/card-transaction-otp.html>, 2019.
- [3] Aujla, G. S., A REVIEW OF ONE TIME PASSWORD MOBILE VERIFICATION. Trans Steller, 6.K. Elissa, 2014. Rouse, M., RSA algorithm (Rivest-Shamir-Adleman). Retrieved from searchsecurity:<https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>, 2017.
- [4] Su, N., Zhang, Y.: Research on data encryption standard based on AES algorithm in Internet of Things environment. In: 3rd Information Technology, Networking Electronic and Automation Control Conference, 15–17 Mar 2019.