Two Factor Authentication Using Token and TAC

Nurul Salimah Binti Mohamed Ismail
Universiti Kuala Lumpur
UniKL MIIT
Kuala Lumpur, Malaysia
nurulsalimah@s.unikl.edu.my

Herny Ramadhani Mohd Husny
Universiti Kuala Lumpur
Unikl MIIT
Kuala Lumpur, Malaysia
herny@unikl.edu.my

***Abstract*— Nowadays single authentication is not secure anymore and easy to be hacked. The widely used authentication to secure the account from unauthorized parties make two-factor authentication a strong authentication. This paper presents the development of two-factor authentication using USB Token and TAC that received through email. The process includes developing requirement model, prototype construction and usability testing. The objective of this study are to develop strong authentication that used combination of USB Token and TAC as a two-factor authentication. The Prototyping Model methodology is used as the process flow for this project.**

Keywords—***Two Factor Authentication, Token, TAC.***

I. INTRODUCTION

This project is about Two-Factor Authentication (2FA) to add more security to the system. 2FA is an extra layer of security. When two-factor authentication is enable, the user need to provide a combination of two authentication like something that the user knows, such as password and something that the user has, such as biometric like fingerprint or face recognition [2]

This project is use Token as a two-factor authentication. The Token is used in addition to or in place of a password and the second authentication that is TAC is send through Email to the user to login into the account. User have to perform both authentication to login into the account. The TAC can be used only for one login, after user logout from the account the previous TAC cannot be used anymore to login again. To login again, user need to get new TAC.

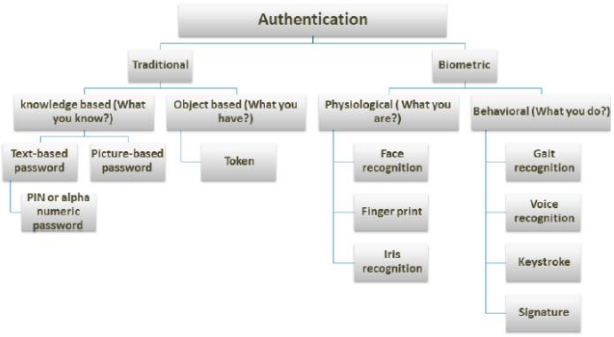


Figure 1: Classification of authentication techniques

II. RESEARCH OBJECTIVE

The main objective of this project is to develop two-factor authentication using Token and TAC, to protect authentication from third parties access and to implement a security protocol, which required all authorized users to perform two forms of authentication to access the account.[1]

III. METHODOLOGY

A. Methodology Uses

Prototype model is used as a methodology in developing this project. The phase of the development are done sequentially starting with the project planning phases, followed by analysis and design phase, implementation phase and system phase.

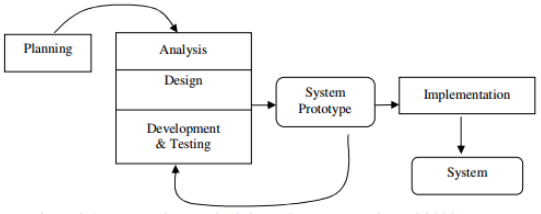


Figure 2: Prototype Model Phase

e-ISSN: 2550-1550

B. *Methodology Explains*

Project planning is the first phase of this project. In the project planning phases, the work that needed to be complete to development this project has been identified. In order to complete the development, the project has been separated into several tasks. Gantt chart has been created in order to schedule the project and identified the time needed to complete every task. By creating the Gantt chart, the time was well managed and the project will ensure to complete in timely manner.

The analysis phase of this project is more about research data. In the analysis phases of this project, the problems that caused user account easy to get hacked by hackers make losing of data and misused the user account. This project has identified that using single authentication are not secure anymore. This project concentrated on preventing user data from being hacked and safe from account misuse.

The development of the system as stated before will reducing account misuse problem and account hacked problem from happened. This project is using two-factor authentication to secure the user account. This project using USB token as a first authentication and TAC as second authentication to login into the account. The TAC will send through email to user.

After user successfully perform the both authentication then user can access into their account, this will keep the account safe from being hacked.

The hardware and software that needed in this project development were identified. The Java will be used as the programming language.

In system prototype phase, the potential of developing this project have been confirm. Using normal authentication such as password are not secure and have a lot of problem such as hacked the account and steal user data. This is because of the security of single authentication is not strong enough and easy to be hacked.

Thus, this project bring a secure authentication that used two-factor authentication using USB token and TAC that hard to be hacked because TAC is send through email.

The implementation phase is the last phase of this project development. This is a part where the design is turned into a functional system. The implementation phase divided into three (3) major phase that is coding and database phase, testing phase and installation phase.

In the coding and database phases, the program code is written to make up the system that wants to build and database for user information is created in order to restore user information, for the programming language, source code will be used by the NetBeans IDE 8.2 while for databases, the PHP-MY Admin will be used.

A second phase is the testing phases. This phase is started after the coding and database phase completed. At this phase, the system will be tested to find and correct any error that occur. This phase also will determine either the system is success or not.

The last phase is the installation phases. In this phase, the two-factor authentication using USB Token and TAC will be connected to database to receive user's information to login into the website account. The installation phases are the end of the system development.

System is the last phase for this project. In this phase, the system will be maintain for better performance to avoid any error occur or any attack happen to the system. The system will always being monitor for safety.

IV. PROTOTYPING/PRODUCT DEVELOPMENT

This chapter will discuss on detail each stage of prototype development phases include the message structure to retrieve data from the database and also the prototype technique propose to handle the both authentication which is USB Token authentication and TAC authentication. In the requirement phase, we have come out with the several diagrams that represent the user requirements. The main propose is to show the system looks like, design the system-model diagrams and interface of the system.

a) Prototype System Design

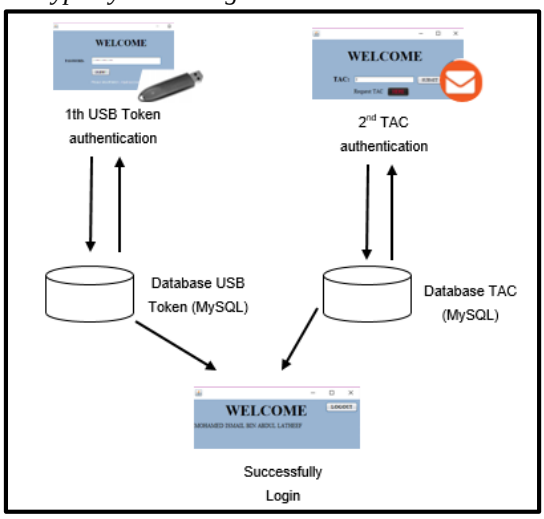


Figure 3: Solution Prototype platform Hardware/Software

The solution to this is to place two-factor authentication that used USB token for first authentication and TAC for second authentication. For USB token user have to insert USB dongle in computer or laptop USB port and then open the website that the user wants to login. User have to key in the Token that user set for that website to perform first authentication.

After first authentication success user have to perform the second authentication by clicking the TAC request button to request the TAC. Email is use instead of SMS to make the authentication more secured. The TAC is send through users email, user have to key in the TAC in the second authentication page and click submit. The TAC is only valid for 5 minutes. If the user did not use the TAC before 5 minutes, the TAC will be expired and user have to request for new TAC.

For main project module, we were trying to code it in Netbenas and Java language as a Two Factor Authentication. The prototype for system was fully developed. The application

will be control by authorized user, which is the one who own the USB token and have rights to access the authentication. All information and Token History will be stored in the database in MySQL database. For example, the user request the TAC and the TAC will be stored in database but the TAC is only valid for single use only. That is mean every time user want to perform the second authentication have to request new TAC.

V. TESTING AND RESULT

A. *Introduction to Testing Method*

In this chapter, all the output from the testing phase will be discussed. After the system was fully integrated, the system went through an extensive testing with various type of data. From the test conducted, every output and result of the system was verified. The result were directly corresponding to the objective of the system that was defined earlier in the introduction.

B. *Usability Testing Result Phase*

This phase is focuses on process of executing a program or system intent of finding error. During the development, the developer must check functionality of the system and check the system to make sure the system successfully integrate with USB Token and TAC to verify the authentication validation to perform the Login. The evolution of a Prototype Development for Two Factor Authentication using USB token and TAC.

- *Test Organization*

Test Organization is a part that must to take by the developer to test the overall system functional. The developer have to confirm that the system can run in any web platform and can access the login with this system. Person who involve for this testing is the system developer and user. The system developer involves in testing, interpret and document the result of test cases and user act as independent test observer, ensure that the developer executes test according and observed result according to expected result.

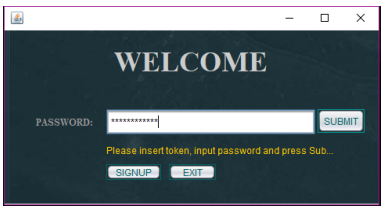
- *Output from Testing Phase*

As referred to the testing phase, many outputs and result from the testing phase were expected in the system. It has been tested that for the system is achieved. There are several working interfaces created for the system.

1. Registration Output

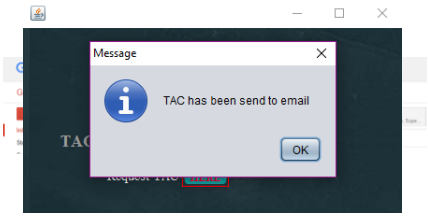
This figure show the registration for new Token and email to send the TAC to user email when user wants to perform the second authentication. User that want to use difference password for difference website have to register first.

2. Token Authentication Output



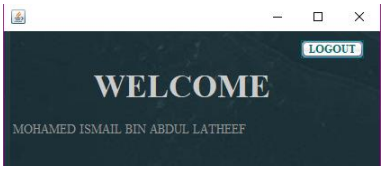
User have to use the Token that user register to perform this authentication.

3. TAC Authentication Output



In second authentication, user have to click the HERE button to receive TAC. The TAC will send to user email. User have to open their email to see the TAC to perform the second authentication. The TAC is valid for five (5) second.

4. Login Output



This is the final output. After first authentication and second authentication successful, user can access the system.

e-ISSN: 2550-1550

- *Test Case Result*

In this phase, the test case result does by the developer to testing the system. The error message show when users enter wrong information that not fulfil the system requirement. If the Token and TAC is incorrect, the system was unable to proceed to second authentication and the authentication will be not success.

VI. CONCLUSION

In conclusion, the proposed of this project had been successfully developed where it allows admin to access the Login with Two Factor Authentication using USB Token and TAC that receive through Email. This project has achieved the objective that are to develop a prototype for Two Factor Authentication using USB Token and TAC. Even though the objective have been achieved, there are still some limitation of this prototype which is if the user lost the USB token, they cannot perform the authentication.[2]

VII. RECOMMENDATION

There are several things that need to be done on this project and can be improve the Two Factor Authentication using USB Token and TAC. For future recommendation, we believe that the project could be more useful if it allows the system automatically detect the Token and TAC. So that user no need to type the Token and TAC. The system will auto detect and fill the Token and TAC to the system. User just have to click submit after the system detect the Token and TAC. Currently, the system allow user the key in the Token and TAC. Moreover, the security measures should be implemented for a more reliable system.

REFERENCES

[1] Aloul, F., Zahidi, S., & El-Hajj, W. (2009). Two factor authentication using mobile phones. In Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on (pp. 641–644). IEEE.

[2] Awang, M., Mohamed, M., Mohamed, R., Ahmad, A., & Rawi, N. (2017). A Pattern-Based Password Authentication Scheme for Minimizing Shoulder Surfing Attack. International Journal on Advanced Science, Engineering and Information Technology, 7(3), 1049–1055.

[3] Bergamasco, S., Bon, M., & Inchingolo, P. (2001). Medical data protection with a new generation of hardware authentication tokens. In Mediterranean Conference on Medical and Biological Engineering and Computing. Citeseer.

[4] Fang, X., & Zhan, J. (2010). Online banking authentication using mobile phones. In Future Information Technology (FutureTech), 2010 5th International Conference on (pp. 1–5). IEEE.