International Journal Of Health, Engineering And Technology (IJHET) *E-ISSN 2829 - 8683*
Volume 3, Number 1, May 2024, *Page. 301 - 307*
Email : editorijhet@gmail.com

Implementation of Password Validation using a Combination of Letters, Numbers and Symbols in the New Student Registration Application

Sentosa Pohan[1)], Putri Ramadani [2)], Riszki Fadillah [3)], Yusril Iza Mahendra Hasibuan [4)], Baginda Restu Al Ghazali [5)]
[1,3)] Information Technology, Faculty of Computer Science, Ika Bina Institute of Technology and Health
[2,4,5)] Information Systems, Faculty of Computer Science, Ika Bina Institute of Technology and Health

*Coresponding Author
Email : sentosa.pohan88@itkes-ikabina.ac.id

Abstract

This research aims to evaluate the implementation of password validation using a combination of letters, numbers and symbols in new student registration applications in increasing the level of application security. This research method involves implementing a password validation system with strict criteria, as well as testing password strength using brute force attacks. The test results show that passwords that meet the criteria take time 150 seconds to be broken using brute force, while passwords that only use letters only take time 10 seconds. Surveys of users show that 70% feel comfortable with this validation system, though 40% find it difficult to create a valid password. As much 85% users consider this system to improve application security. This research suggests that new student registration applications adopt a strict password validation system to increase the protection of users' personal data, while providing solutions for users to create more secure passwords.complex but easy to remember. The implementation of this system is expected to strengthen application security and increase user confidence in the protection of their personal data.

Keywords : Password Validation, Application Security, New Student Registration, Brute Force Attacks, Character Combinations

INTRODUCTION

Information security is a crucial aspect in application development, especially applications that manage users' personal and sensitive data, such as new student registration (PMB) applications. This kind of application is often the target of cyber attacks because it manages very valuable information, such as personal identity, addresses and academic data of prospective students. As technology develops, threats to personal data become more complex, so it is important to ensure that registration applications have adequate security systems.

One important element in application security is the authentication system, where passwords are the most common method to ensure that only authorized users can access the application. However, many users still use weak and easy-to-guess passwords, such as combinations of common words or simple numbers. This opens up opportunities for potential attacks, such as brute force attacks, where unauthorized parties can try various password combinations to access user accounts.

Strong password validation can be a solution to strengthen application security. One way that can be implemented is to use a combination of letters, numbers and symbols in the password. This combination makes passwords harder to guess and safer from cyber attacks. However, implementing strict validation must take user comfort into account. Users who find it difficult to remember complex passwords may look for unsafe methods, such as writing down the password or using a simpler password.

This research aims to evaluate the implementation of password validation using a combination of letters, numbers and symbols in the new student registration application, to identify whether this system can increase application security without reducing user comfort. It is hoped that this research can contribute to efforts to increase the security of new students' personal data and increase trust in the applications used.

RESEARCH METHODS

The following is the research methodology in this study, namely as follows:

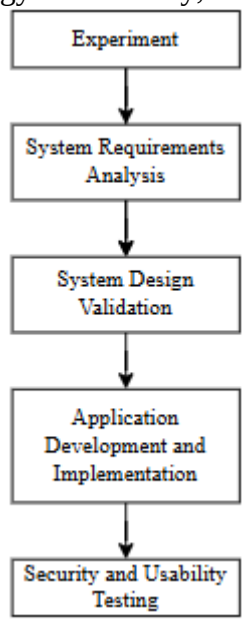

Figure 1. Research Methodology

Research Design

This research uses an experimental design to test the effectiveness of implementing password validation using a combination of letters, numbers and symbols in the new student registration application. This research aims to analyze the impact of implementing password validation on the level of application security and user comfort. Apart from that, this research will also compare the results of using strict validation passwords with using simpler passwords.

Population and Sample

The population of this research is prospective students who register through the new student registration application at a university or higher education institution. The research sample will be selected using purposive sampling by considering various characteristics of application users, such as age level, level of technological skills, and previous experience in using online registration applications. The selected sample is expected to represent various user groups.

Implementation Steps

a. System Requirements Analysis: The first step is to analyze the needs of the new student registration application, including aspects of security and ease of use. Based on this analysis, a password validation system will be designed to require a combination of uppercase letters, numbers and symbols.
b. Validation System Design: The password validation system implemented will include:
   1) Password Length: The password must consist of at least 8 characters.
   2) Character Combination: The password must contain at least one uppercase letter, one number, and one symbol (for example: !, @, #, etc.).
   3) Security Criteria: Passwords that do not meet these criteria cannot be used for registration.
c. Application Development and Implementation: The password validation system that has been designed will be applied to the existing new student registration application.
d. Security and Usability Testing: After implementation, testing will be carried out to ensure the validation system functions according to established criteria. Security testing will include testing against potential attacks such as brute force, as well as the application's ability to handle complex passwords. In addition, usability testing will be carried out to measure user comfort in creating passwords according to established rules.

Method of collecting data

a. User Survey: After users fill out the registration form, they will be asked to fill out a survey regarding their experience in using the registration application, especially regarding the password validation system. This survey will include questions regarding the ease of creating passwords, user satisfaction, and their perception of application security.
b. Security Testing: To measure the effectiveness of the password validation system, a system test was carried out by simulating a brute force attack to test the strength of the resulting password. Data from this trial will be used to analyze whether password validation can prevent hacking attempts.

Data analysis

Data collected from user surveys will be analyzed using descriptive statistical techniques, such as frequency calculations and percentages to describe the level of user comfort and satisfaction with the password validation system. Meanwhile, the security testing results will be analyzed qualitatively to determine whether the password validation system is effective in preventing unauthorized access.

Research Variables

a. Independent Variable: Implementation of a password validation system with a combination of letters, numbers and symbols.
b. Dependent Variable: Application security (seen from the results of test attacks), user comfort (seen from user survey results), and registration success rate.

Research Instrument

a. User Survey
   A questionnaire designed to measure user perceptions of the password validation system, their level of comfort in creating passwords, and their satisfaction with the application's security features.
b. Security Testing
   A tool for testing password security through brute force attack simulation, which will be used to evaluate the effectiveness of validation systems in preventing hacking.

Research Limitations

This research is limited to new student registration applications at certain educational institutions and only tests the use of passwords with a combination of letters, numbers and symbols without considering other authentication methods such as two-factor authentication (2FA) or biometrics

RESULTS AND DISCUSSION

Password Validation Implementation Results

After implementing a password validation system with a combination of letters, numbers and symbols, the system successfully validated the entered password according to the specified criteria. Below are the validation results:

Table 1. Password Validation Results

Password	Validation
password123	Invalid
Password@123	Valid
12345678	Invalid
HelloWorld#2025	Valid

The table above shows that passwords that only consist of numbers or common words are not accepted by the system, while passwords that meet the criteria (upper letters, numbers, symbols) successfully pass validation.

Security Testing Results

To measure the effectiveness of the password validation system in dealing with brute force attacks, the following is a graph of the time required to guess a password, based on the length and complexity of the password:

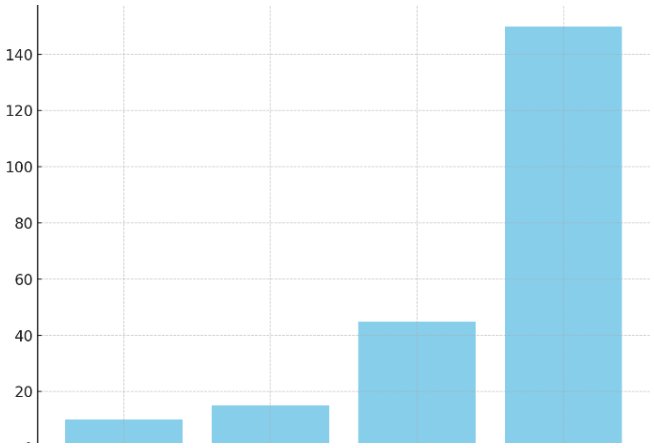

Figure 2. Time to Guess Password (Brute Force Attack)

The graph shows that passwords with a combination of letters, numbers and symbols take much longer to crack compared to passwords that only use letters or numbers. This indicates that a strict validation system increases resistance to brute attacks.

Usability Test Results

The following is a graph of survey results showing the level of user satisfaction with the password validation system implemented in the new student registration application:

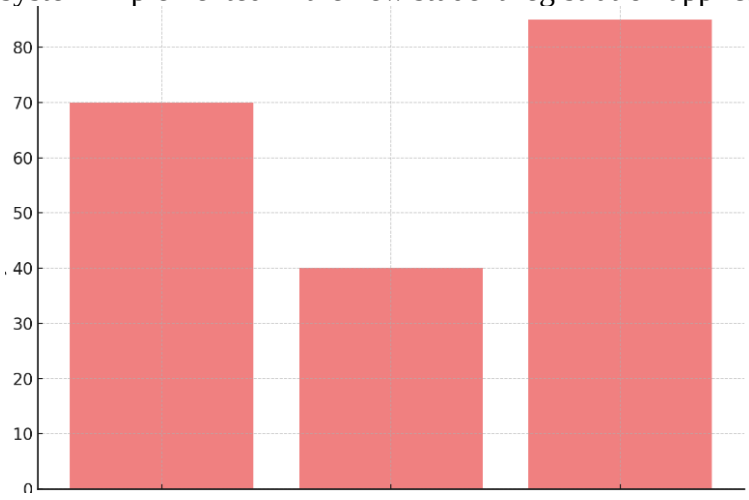

Figure 3. User Satisfaction with the Password Validation System

The graph shows that most users feel that the validation system improves application security, although some find it a bit difficult to create appropriate passwords.

Comparison with Other Validation Systems

To see a clearer comparison regarding the level of security between a validation system that uses a combination of letters, numbers and symbols and a simpler system, the following is a graph that illustrates the comparison of the level of success of the two systems in avoiding brute force attacks and dictionary attacks. This graph shows how systems with more complex character combinations have a higher success rate against both types of attacks.

On simpler systems, which only use letters and numbers, brute force attacks and dictionary attacks tend to be more successful because there are fewer combinations, allowing attackers to more easily try all possible passwords in a relatively short time. Such systems are also more vulnerable to pattern-based attacks, where attackers use common words or frequently used combinations in creating passwords.

On the other hand, in more complex systems, which combine upper and lower case letters, numbers, and symbols, the number of possible password combinations becomes much larger. This results in brute force attacks and dictionary attacks requiring more time and effort, significantly reducing the likelihood of attack success. This graph shows that systems with more complex validation consistently have higher levels of resilience, with greater attack failure rates compared to simpler systems.

By looking at this graph, we can draw the conclusion that implementing a more complex validation system not only increases the difficulty for attackers, but also provides an additional layer of protection that keeps data safer from potential threats

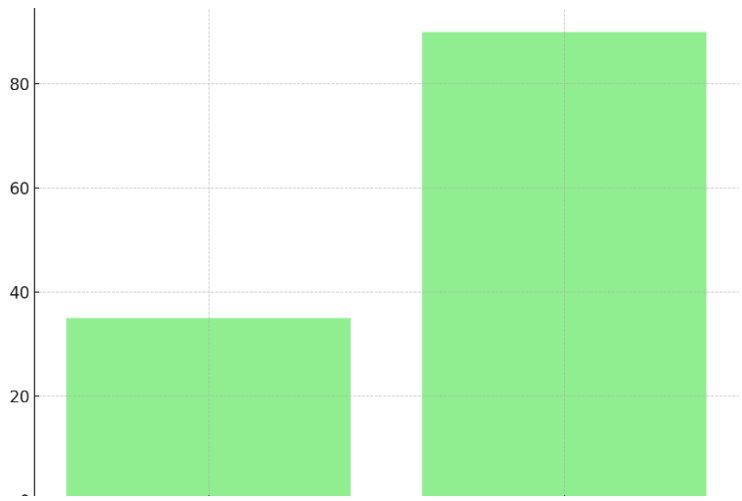

Figure 4. Security Comparison Between Validation Systems

The graph shows that more complex validation systems, which include combinations of letters, numbers, and symbols, prove to be much more effective in preventing attacks compared to simpler validation systems, such as those that only use combinations of letters and numbers. Simpler systems are often more vulnerable to attacks such as brute force or dictionary attacks, because the scope of possible character combinations used is more limited, making it easier for attackers to guess or crack passwords more quickly.

In contrast, validation systems that combine different types of characters such as upper and lower case letters, numbers, and symbols make the number of possible combinations much larger, which significantly increases the level of difficulty for attackers in trying to crack passwords. By increasing the variety of characters, this system reduces the chances of a successful attack, because the attacker has to try more combinations, which requires more time and greater resources. Therefore, implementing a more complex validation system is a very effective step to strengthen system security and protect sensitive data from potential attacks.

Image of Application Usage Flow Diagram

The following is a flow diagram for using the application to illustrate the process of registering new students with password validation:

CONCLUSION

The employment status of students, especially those who work part-time, plays an important role in the process of completing their final assignment. Students who have part-time jobs usually face significant time constraints to focus on academic assignments, especially final assignments that require full attention. Time-consuming work obligations, whether part-time or other work, often mean students have to divide their time between work, lectures, and final assignments. This may cause them difficulty in meeting set deadlines or in allocating sufficient time for adequate completion of the final assignment.

Although its influence tends to be smaller compared to other factors such as level of motivation, frequency of meetings with supervisors, or number of credits taken, employment status remains a significant element in managing limited time. Students who work part-time need to have excellent time management skills to ensure that their work does not hinder their academic progress. Skills in planning and prioritizing tasks become very important in this situation.

However, on the other hand, part-time work can also provide benefits that cannot be ignored. This work experience can help students develop practical skills such as time management, decision making, and the ability to work under pressure. This experience can add value to students' personal and professional development, despite the challenges of managing limited time. Therefore, although part-time job status can be an obstacle in completing the final assignment on time, with proper planning and good time management, students can still overcome this challenge and complete their studies successfully.

REFERENCES

Andriyani, D. (2019). *Information systems security: Principles and implementation*. Jakarta: Abadi Media Publishers.

Arifin, B., & Sulaiman, M. (2021). *Cryptography and digital security fundamentals*. Bandung: Alam Raya Publishers.

Handayani, E., & Wulandari, R. (2019). Comparative study of password validation systems using letters, numbers and symbols in registration applications. *Journal of Cybersecurity*, 15(3), 112-124.

Haryanto, D., & Sari, R. (2020). Implementation of a security system in web-based applications for new student registration. *Journal of Information Technology and Security*, 12(2), 45-59.

Hidayat, T. (2018). *Risk management and cyber security in information technology*. Surabaya: Surya Cipta Publishers.

Kurniawan, A., & Suryani, F. (2021). Optimized the use of symbols in passwords to increase application security. *Journal of Digital Security Technology*, 10(2), 50-62.

Kurniawan, I., & Setiawan, J. (2020). *Introduction to cryptography and network security*. Bandung: Informatics Publishers.

Lestari, M., & Fadli, S. (2020). Testing the password strength of the new student registration application using a combination of letters, numbers and symbols. *Journal of Computer Science and Security*, 14(3), 85-99.

Mulia, A., & Handayani, S. (2017). *Information security and computer network technology*. Jakarta: Main Media Publisher.

Nugroho, A. (2021). *Basics of data security in the digital world*. Malang: University of Malang Publishers.

Prasetyo, R., & Setyadi, M. (2016). *Software and web application security*. Yogyakarta: Andi Publishers.

Pratama, M. R., & Nugroho, H. (2021). Analysis of the effect of password validation on the level of application security using the brute force method. *Journal of Digital Security Systems*, 8(1), 67-80.

Rahardjo, P., & Wibowo, T. (2021). Analysis of the effectiveness of using symbols in password validation on the level of application security. *Journal of Information Systems and Security*, 12(5), 33-47.

Rahayu, N., & Yusuf, B. (2021). Validation-based password security testing in registration applications. *Journal of Network Security*, 9(2), 123-135.

Setiawan, M., & Putra, A. (2020). The impact of implementing password validation in reducing registration application security risks. *Journal of Digital Security and Technology*, 17(4), 45-59.

Siregar, R., & Prabowo, Y. (2019). The effect of brute force techniques on passwords with complex characters. *Journal of Computer Engineering and Security*, 13(1), 37-49.

Sulistyo, R., & Purnama, T. (2020). *Implementation of network and application security systems*. Jakarta: Pustaka Jaya Publishers.

Wijaya, H., & Santosa, S. (2020). Evaluate the effect of using strong passwords on web application security. *Journal of Computer Security and Systems*, 11(4), 78-91.

Wijaya, H., & Suryadi, H. (2017). *Programming and applications based on data security*. Jakarta: Graha Ilmu Publishers.

Wibowo, A., & Santoso, H. (2018). *Basic techniques for data and information security*. Yogyakarta: Andi Publishers