Information Technology Studies Journal (ITECH)
Vol 2 (2) 2025 : 182-196

IMPLEMENTATION OF COMBINATION METHOD ON PASSWORD FOR USER ACCESS IN BANK OPERATIONAL ENVIRONMENT

PENERAPAN METODE KOMBINASI PADA PASSWORD UNTUK AKSES USER DI LINGKUNGAN OPERASIONAL BANK

R Fitria Rachmawati
Universitas Ibn Khaldun Bogor
*fitria@uika-bogor.ac.id

**Corresponding Author*

ABSTRACT
The development of information and communication technology has now progressed so rapidly and become an inseparable part of human life. The use of this technology has driven rapid business growth, because various information can be easily obtained and presented sophisticatedly, such as compiling electronic documents, performing calculations, sending and reading e-mails, searching for all kinds of information on the internet, and chatting are daily activities that utilize information and communication technology. These positive impacts do not always last well, on the other hand, other parties have thoughts that with bad intentions seek profit by breaking the law. This study explains the scope of information system ethics in terms of the use of passwords as a support for privacy security for system users in the bank's operational environment. The theory used in this study covers the scope of information system ethics, theories related to passwords used in the bank's operational environment. The results of this study are expected to provide deeper knowledge to the general public, and especially in the bank's operational environment, about the importance of information system ethics in terms of implementing combination methods on passwords for user access in the bank's operational environment.
Keywords: Information System Ethics, Password Security, Information and Communication Technology, Data Privacy, Bank Operations

ABSTRAK
Perkembangan teknologi informasi dan komunikasi saat ini telah berjalan begitu cepat dan menjadi bagian hidup manusia yang tidak dapat dipisahkan. Pemanfaatan teknologi tersebut telah mendorong pertumbuhan bisnis yang pesat, karena berbagai informasi dapat diperoleh dengan mudahnya dan disajikan dengan canggih, seperti menyusun dokumen elektronik, melakukan penghitungan, mengirim dan membaca e-mail, mencari segala macam informasi di internet, chatting merupakan aktivitas sehari-hari yang memanfaatkan teknologi informasi dan komunikasi. Dampak positif tersebut tidak selalu berlangsung baik, di sisi lain timbul pikiran pihak-pihak lain yang dengan itikad tidak baik mencari keuntungan dengan melawan hukum. Penelitian ini memaparkan tentang cakupan etika sistem informasi dalam hal penggunaan password sebagai penunjang keamanan privasi bagi pengguna sistem di lingkungan operasional bank. Teori yang digunakan dalam penelitian ini meliputi tentang cakupan etika sistem informasi, teori terkait password yang digunakan di lingkungan operasional bank. Hasil penelitian ini diharapkan akan dapat memberi pengetahuan lebih dalam lagi kepada masyarakat umum, dan khususnya di lingkungan operasional bank tentang pentingnya etika sistem informasi dalam hal penerapan metode kombinasi pada password untuk akses user di lingkungan operasional bank.
Kata Kunci: Etika Sistem Informasi, Keamanan Password, Teknologi Informasi dan Komunikasi, Privasi Data, Operasional Bank

1. INTRODUCTION

The development of information and communication technology has now progressed so rapidly and become an inseparable part of human life. The use of information technology has driven rapid business growth, because various information can be obtained easily and presented sophisticatedly, such as compiling electronic documents, performing calculations,

sending and reading e-mails, searching for various kinds of information on the internet, chatting and many more, all of which are daily activities that utilize information and communication technology, through long-distance relationships utilizing telecommunications technology can be used as material for carrying out the next business steps. The parties involved in the transaction do not need to meet face to face, only enough through computer and telecommunications equipment.

These positive impacts do not always last well. On the other hand, sometimes there are thoughts from other parties with bad intentions and are irresponsible to seek profit by violating the law on the use of information and communication technology, which means committing violations and crimes. The integration of computer technology into society brings major changes, almost in all aspects of human life. Changes occur in the way people think, both in problem-solving efforts, planning, and decision-making. Changes that occur in the way people think as one of the consequences of technological developments, more or less will influence the implementation and how people view ethics and norms in their lives.

In the field of information systems, not all information systems are always successful in their use and implementation. In practice, there are various real-life cases that demonstrate security gaps and ethical violations in the use of information systems. One example is the case of account theft, which differs from physical theft because the perpetrator only needs to capture the user ID and password without taking any tangible items. The primary goal of this theft is usually to obtain specific information, not to steal assets directly. As a result, victims are often unaware of the loss, but the impact is felt when the information is used by irresponsible parties. In many cases, the burden of account usage fees is actually borne by the legitimate account owner. One real-life example occurred at an ISP (Internet Service Provider), where two internet cafes in Bandung were found to be using stolen accounts for their activities.

A similar case rocked the Indonesian banking industry, perpetrated by Steven Haryanto. He created fake websites that resembled the original BCA Internet Banking service. Through these fake websites, if customers mistyped the official website address, their identities, such as user IDs and PINs, could be stolen. Approximately 130 customers were reported to have fallen victim to this data theft. Although Steven claimed his goal was to raise public awareness of mistyped website addresses, the impact was still serious, as many BCA customers reported losing money due to transactions they did not initiate.

This type of crime is classified as a form of misuse of user IDs and passwords by unauthorized parties, which falls into the categories of unauthorized access and hacking-cracking cybercrime. These crimes are referred to as "gray crimes" because perpetrators often claim educational or experimental motives, yet still violate information system laws and ethics. The targets of these crimes can be categorized as cybercrime against property (attacking property rights) and cybercrime against persons (attacking individuals). This phenomenon demonstrates the importance of understanding information system ethics and implementing strong cybersecurity, particularly regarding the use of user IDs and passwords in high-risk environments such as banking and internet service providers.

Several factors influence the continued occurrence of cases of information technology abuse, including human behavior and weaknesses in the system. From a user perspective, some computer users are unaware that all forms of computer access and information system use require ethics. When these systems are used, they are often not well-received by their users. Behavioral aspects need to be incorporated into the development and use of these systems. From a system perspective, not all application systems currently provide a facility to determine strong, medium, and weak password categories as a reference that can reduce the level of privacy insecurity for system users in bank operational environments.

The development of crimes in the use of computer technology is increasingly diverse along with the development of existing technology. Starting from hacking or accessing computers by unauthorized people but not causing damage to the system, cracking or breaking

into computer systems for the purpose of damage, carding or stealing credit card numbers online, data diddling or falsification of data, social engineering or deceiving employees to gain access, spoofing or stealing passwords through falsified login pages, spreading viruses, and so on. Related to the use of passwords, the question arises: is it possible for someone to know another person's password and use it without the knowledge of the more authorized person? To answer the above question, of course, very much depends on the conditions and level of the problem, and very much depends on each case that occurs. Perhaps for some people, the problem of password use is not too concerning, but in reality, the impact of password misuse can be felt. In fact, there have been many incidents simply because of password creation errors, such as passwords that are easily guessed by unauthorized people, thus giving rise to actions to misuse the password itself for purposes that are not in accordance with the authority and regulations that should be.

In general, as humans, wherever and under any circumstances, we desire protection of privacy, security, and a sense of security in all our daily activities, including the use of computer technology. Naturally, every user expects that whatever they do with computer technology will be secure and free from the possibility of being damaged, stolen, or misused by unauthorized parties.

The importance of ethics in the field of information systems is very influential in the use of computer technology which is currently increasingly advanced rapidly, society must begin to pay attention and realize the importance of ethics in computer use, especially because of human awareness that computer use that is not in accordance with information system ethics can interfere with the privacy rights of each individual. As discussed by Richard Mason, that ethics in information systems includes PAPA, namely; Privacy, Accuracy, Property, and Access. Related to passwords, the creation and use of good and correct passwords, namely knowing several categories of strong passwords, medium password categories, and weak password categories, is expected to be a recommendation so that users can increase their attention to privacy security issues in the bank's operational environment.

Seeing the bad impact that can be caused by the misuse of computer technology, and in an effort to increase user knowledge to be more ethical in the field of information systems, especially in terms of password use, it is necessary to conduct research by providing more in-depth knowledge through the application of combination methods on passwords for user access in the bank's operational environment.

The main problem in this research is that not all users have a deep understanding of information system ethics, especially regarding the use of secure passwords. Many users are unable to distinguish between strong, medium, and weak password categories, so there are still risks to system security and data privacy. Furthermore, in the operational environment of banks there are no facilities available to help users determine the level of password strength, which has the potential to create vulnerabilities to unauthorized access. Based on these problems, this research seeks to answer the question of how to explain and provide users with an understanding of how to determine the categories of strong, medium, and weak passwords in accordance with the principles of information system ethics in the operational environment of banks.

This study aims to provide a deeper understanding of the application of information system ethics through the use of secure passwords in bank operational environments. The purpose of this study is to improve the ethical culture in the use of information systems by implementing passwords that comply with the principles of data security and privacy, and to determine the level of user knowledge, understanding, concern, and attention to the use of secure and ethical passwords.

The results of this study are expected to provide benefits in the form of increased user understanding of how to create and use good and correct passwords, by identifying strong, medium, and weak password categories as a reference for protecting privacy and access rights.

Furthermore, this study is also expected to provide an overview of secure password creation techniques through simulations of various password categories, so that they can be effectively implemented in banking operations to strengthen information system protection.

2. LITERATURE REVIEW

1. Privacy, Accuracy, Property, Accuracy, abbreviated as PAPA.

PAPA, according to Richard Mason in Mcleod and Schell (2004, p. 318), identifies four community rights over computers, including the right to privacy, accuracy, ownership, and access.

a. Privacy

Privacy concerns an individual's right to protect personal information from access by others who are not authorized to do so.

Case Example:

(1) Junk mail

A privacy issue related to the implementation of an information system is the case of a marketing manager who wanted to monitor his subordinates' emails because he believed they were more likely to interact with personal emails than with customers. Although the manager had the authority to do so, he violated his subordinates' privacy.

b. Accuracy (Accuracy)

Computers are believed to be capable of achieving levels of accuracy unattainable by non-computer systems. Accuracy of information is a crucial factor for any information system. Inaccurate information can be disruptive, detrimental, and even dangerous.

Case example:

(1) The loss of her social security number experienced by Edna Rismeller (Alter, 2002, p. 292)

(2) The case of the United States missile detection error.

c. Property (Ownership)

Protection of property rights currently being promoted is known as IPR (intellectual property rights). Intellectual property is regulated through three mechanisms:

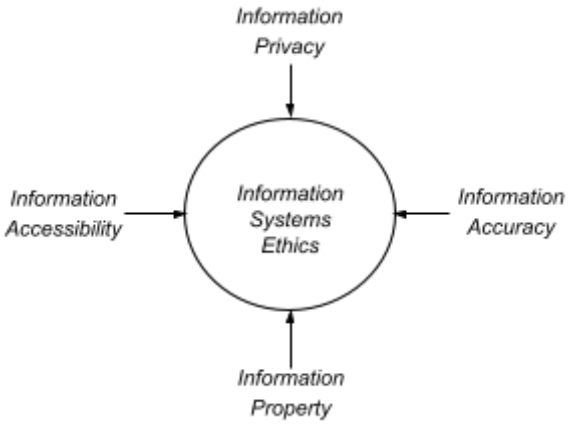
(1) Copyright,

(2) Patents, and

(3) Trade secret.

d. Access

The focus of access issues is on providing access for all groups. It is hoped that information technology will not be a barrier to accessing information for certain groups, but rather support access for all.



Gambar 2.1. Cakupan etika sistem informasi menurut Richard Mason

2. Computer Ethics

According to James H. Moor in Mcleod and Schell (2004, p. 271), computer ethics is an analysis of the nature and social impact of computer technology, as well as how to formulate appropriate policies to use this technology ethically.

a. Reasons why computer ethics is important.

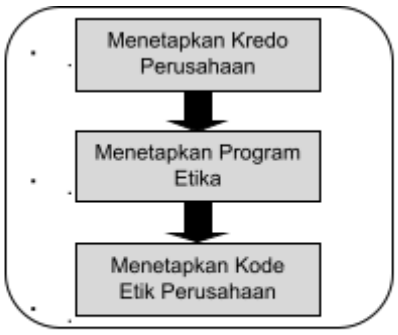
There are three main reasons for the high public interest in computer ethics, namely: logical malleability, transformation factors, and invisibility factors. James H. Moor in McLeod, Raymond., and George Schell (2004, p. 272)

1. Logical flexibility.
   James H. Moor defined logical malleability as the ability to program a computer to do whatever we want. Computers work exactly as their programmers instruct them to, and this ability can be frightening.
2. Transformation factor.
   The reason for this concern about computer ethics is that computers can drastically change the way we do things. We can see similar transformations in all types of organizations.
3. Invisible factors.
   The third reason for public interest in computer ethics is because all of a computer's internal operations are hidden from view.

b. Implementing Ethical Culture

The task of top-level managers is to ensure that ethical concepts reach all members of the organization, from top managers down to all employees at the grassroots level. Corporate executives use three stages to establish these ethical concepts. The first stage is establishing a corporate credo; the second stage is implementing ethics programs; and the third stage is establishing corporate codes.

Figure 2.2 below shows the relationship between these three stages. (McLeod, Raymond., and George Schell, 2004, p.271)



Gambar 2.2. Hubungan dari ketiga tahapan dalam menerapkan budaya etika.

(1) Company understanding

A short, but clear statement of the values the company will uphold.ObjectiveThe purpose of forming a corporate understanding is to provide information to the public, both inside and outside the company, regarding the ethical values held by the company.

The following table illustrates an example of corporate governance from Security Pacific Corporation, a Los Angeles-based bank. Security Pacific's management recognizes that

business is built on both internal and external commitments. (McLeod, Raymond, and George Schell, 2004, p. 271)

Table 1
Example table of company understanding from Security Pacific Corporation.

1. Commitment to customers	2. Commitment to employees	3. Commitment from employees to Security Pacific
4. Commitment from employees to employees	5. Commitment to society	6. Commitment to shareholders

(2) Establishing an Ethics Program

An effort consisting of various activities designed to provide employees with direction on how to implement the company's philosophy. These activities are typically provided in several sessions during orientation for new employees. During these sessions, specific discussions focus on ethical issues. (McLeod, Raymond, and George Schell, 2004, p. 271)

(3) Establishing a Company Code of Ethics.

Every company has its own code of ethics. Sometimes these codes are adapted from specific industry codes. (McLeod, Raymond, and George Schell, 2004, p. 271)

3. Password

A password is a term that can be described as the last line of defense in a data or information security system. It is part of the authentication process (the validation process when entering a system). Passwords are kept secret from unauthorized access, and those seeking access are tested to determine whether they are worthy of access. In concrete terms, one of the common ways used to secure a system is to regulate user access to it through a mechanism of truth matching (authentication) and granting access rights (access control).

A password is a secret code typically used to perform authentication, a process used to confirm whether someone has permission to access confidential information or data. Passwords are always kept secret, known only to individuals or groups authorized to access the protected data or information. People who lack access but need the information often attempt to obtain it (Thor, 2008, p. 2).

Passwords were originally used as a means of bypassing city security (of course, this was often the case during wartime). However, in modern times, people use them to protect Automated Teller Machines (ATMs), credit cards, online banking, operating systems like Windows, and even computers themselves. (Thor, 2008, p. 2)

The password itself doesn't have to be a standard sentence or word. It can use numbers, uppercase letters, lowercase letters, or special keyboard characters like punctuation marks or "Extended ASCII" symbols like ệ and Φ. (Thor, 2008, p. 3).

Here is a table that gives more information about Extended ASCII. The words found in the column name also mean: (1) Dec (Decimal). A group of numbers as many as three digits that can be used as another name of the character. (2) Hex (Hexa Decimal). Just another form of a number. If the number we know is the number in 10's consisting of 0123456789, then the Hexa number is the number in 16's consisting of 0123456789ABCDEF. (3) Char (Character) or form to be produced. (Thor, 2008, p.3)

It's also quite easy to do. If you're using a keyboard on your PC, type Alt+128 on the Numlock Pad (numbers-
If the numbers on the right side of the keyboard form a small box, you will get a capital C with a tail like the character in the upper left corner of the image on the next page. (Thor, 2008, p. 3)

a. How passwords work in login systems.

One way to implement this mechanism is through the use of passwords. A simple example is when using a computer, the user is required to go through an authentication process by entering their user ID and password. This information is then compared with data in the system. If both matches (are valid), the prospective user is allowed to log in; if not, a failure message appears, as shown in Figure 2.3.

Figure 2.3. How passwords work in the login system

After the authentication process, users are granted access rights according to their level of privileges. This access control is usually grouped into categories. There are regular users, guests, and administrators with privileged privileges. These groups are tailored to the needs and responsibilities of each user. For example, in a university environment, there are usually groups of students, staff, employees, lecturers, the rector, and administrators. Meanwhile, in a business environment, there are groups of finance, engineers, auditors, marketing, directors, and so on. In a bank's operational environment, there are groups for frontliners, back office, international banking operations, marketing, internal audit, human resources division, operations managers as supervisors for the operational section, and so on.

However, a password doesn't necessarily mean a string of words; of course, a password that isn't a meaningful word will be more difficult to guess. Additionally, a password is often used to describe something more accurately called a passphrase. Passwords are sometimes also used in a form that only contains numbers; one example is a Personal Identification Number (PIN). Passwords are generally short enough to be easy to remember.

b. Good password

The criteria for a good password are actually quite simple, limited by only two requirements: it should be easy for the owner to remember, and at the same time, difficult for others or those who are not authorized to know it to guess. However, in practice, these requirements are difficult to implement. Most passwords that are easy for the owner to

remember tend to be easy for others. Meanwhile, a password that is considered secure because it is difficult for unauthorized people to guess tends to be difficult for the owner to remember. Therefore, a special technique is needed to choose a password that is both secure because it consists of a difficult-to-guess character arrangement, and easy for the owner to remember.

c. Ideal Password criteria

A good password is recommended to have the following characteristics:

(1) Consisting of a minimum of 8 characters, where in principle the more characters the better, it is recommended that a relatively secure password consists of 15 characters.

However, according to (Thor, 2008, p. 15), a strong password is determined by the complexity of the words it contains. Even if you use 20 characters, if your password is "JunaediPratama," or your own name, it will be easy for someone to guess.

But that doesn't mean using a name as a password is the worst. Using a name as a password is certainly one of the best ways to prevent forgetting your own name, as it's unlikely you'll forget it. However, it should be made a little more complex so it's not easy to guess. For example, by adding numbers to replace vowels in the password, making it "Jun43d1Pr4t4m4" (Thor, 2008, p. 15).

(2) Use a random mix of different types of characters, namely: uppercase letters, lowercase letters, numbers, and symbols;

(3) Avoid passwords that consist of words that can be found in a language dictionary;

(4) Choose a password that is somehow easy to remember; and,

(5) Do not use the same password for different systems.

d. How to secure passwords (Thor, 2008, p.15)

(1) Use Minimum number of characters.

A strong password is determined by the complexity of its words. Even if you use 20 characters, but your password is "Junaidi Pratama," which is your own name, it's still easy for someone to guess.

But that doesn't mean using a name as a password is the worst. Using a name as a password is certainly one of the best ways to prevent forgetting your own name, as it's unlikely you'll forget it. However, it should be made a little more complex to make it difficult to guess. For example, by adding numbers to replace vowels in the password, making it "Jun43d1Pr4t4m4."

(2) Use of password(s) that are considered strong.

Besides using numbers and making your password longer than the minimum number of characters considered strong (or exceeding the minimum number of 12 characters), another way you can protect yourself from password theft is by adding punctuation marks or Extended ASCII symbols such as ĉ to your password.

(3) Change the password regularly.

Changing your password regularly or periodically at least once every 6 months is one of the best security measures.

(4) Recognizing secret question(s)

(5) Avoid using default password(s)

(6) Encryption

In short, encryption is a technique that changes information (in the form of writing) into something that cannot be understood by others, by using a mathematical key. Other people will never understand the meaning of the words that have been changed (scrambled) by the encryption process if they do not have the key. The key to the encryption process can be a rule, number, direction, word or sentence. A simple analogy, for example, I want to encrypt the sentence "I want to eat" and the key is a mathematical calculation of the 8x8 Matrix, maybe the sentence will be something like "9xKKLA%ASNK 401v" (who knows?). Some

examples of the most widely used encryption in the world of information security are RSA, MD5, and SHAL.

3. METHODS

3.1. Research Design

The following is a flowchart of the research design as seen in the image:

Gambar 3.1. Bagan Alir Desain Penelitian

1. Identification of problems
   Explain the problem being researched clearly, in detail, and in accordance with the problem being researched.
2. System design and implementation.
   Carry out the design creation using the method used, then the results of this system design are implemented by installing the hardware and software.
3. System testing.
   Conducting trials or testing before the system is actually used.
4. System feasibility test
   After the system trial is carried out, a system feasibility test is carried out. This system feasibility test aims to determine whether the system is suitable for use by users.

3.2. Data Collection Methods

In compiling this thesis, several methods were employed to obtain and collect comprehensive data for this research. The methods used to obtain the data are as follows:

a. Observation
   Observation is a technique or approach to obtain primary data by directly observing the data object. (Jogiyanto, 2008, p.89).

Things observed from this observation include:

(1) The observation location was carried out in the bank's operational environment, including in the back office (savings checking and financing operations), frontliner (Teller and Customer Service), and Personnel.
(2) Questionnaire/Survey:

Respondents were provided with a facility to complete questionnaires online via a local area network. Observations were made directly when a system user entered a password in the new user registration menu.

To gather the opinions of system users in the bank's operational environment regarding their knowledge of password usage, a survey was conducted using a questionnaire. The questionnaire was designed with 10 questions, each of which measured employee knowledge regarding passwords.

b. Interview
   The interview was conducted by asking the source directly questions that were closely related to how to input passwords into the application system.
c. Library Research
   In this case, the author collects materials from books or theories that can support the writing of this thesis.
d. Searching or looking for theories on internet pages that are considered representative to support this research.

All methods require detailed, complete, accurate, and clear recording. To achieve completeness, accuracy, and clarity of data, data recording must be accompanied by:

a. The name of the data collector
b. Date and time of data collection
c. Data collection location
d. Additional information on data/terms/respondents

All items asked in all data collection methods must align with the research problem formulation and/or hypothesis. Therefore, the process of decomposing research variables into sub-variables, dimensions, and research items is a process that must be carried out carefully. This decomposition process also facilitates the measurement and data collection process. This decomposition process is known as the operationalization of research variables, as shown in Figure 3.2.

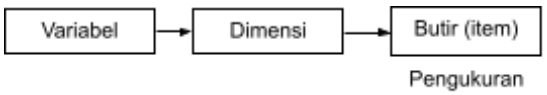


Figure 3.2. Process of operationalizing research variables.

3.3. Data Analysis Methods

1. Likert scale

Attitude scale or Likert scale is an information gathering technique that measures attitudes. According to Best (1977, p.191-192) in Tukiran Taniredja and Hidayati Mustafidah (2011, p.136) states that this Likert scale asks respondents to answer a question with very good (SB), good (B), sufficient (C), less good (KB), not good (TB). Each data. Each answer is associated with a number or value, for example SB = 5, B = 4, C = 3, KB = 2, and TB = 1. This is also in accordance with Muller's opinion in the book by Tukiran Taniredja and Hidayati Mustafidah (2011, p.136) namely 'In scoring positively stated Likerts "strongly agree" receives 5 points, "agree" 4 points, and so on'.

2. Combinatorial

In creating passwords, combinatorial theory is used, and to test the strength of the password, guessing is done when entering the password using a mathematical combination formula.

Combinatorial is a branch of mathematics that deals with calculating the number of possible arrangements of objects without having to enumerate all possible arrangements. In general, there are two main principles in combinatorial theory:

a. Rule of product.

If an event P and Q occur simultaneously (under the same conditions), then the number of possible events is equal to P x Q.

Example of Multiplication Rule Formula 1:

Two representatives from class A went to the lecturer to protest the exam scores. The representatives chosen were 1 man and 1 woman. How many ways can the two representatives be chosen?

The example of the Multiplication Rule Formula 1 above can be explained as follows:

65 x 15 = 975 dear

b. Rule of sum.

If an event P and Q occur where P and Q are not carried out simultaneously (under different conditions), then the number of possible events is equal to P + Q.

Example of the Multiplication Rule Formula 2:

A class president will be elected in class A. Only 1 person (male or female, no gender bias). The number of men in class A = 65 people and the number of women = 15 people. How many ways can the class president be elected?

The example of the Multiplication Rule Formula for 2 above can be explained as follows:

65 + 15 = 80 ways

3. Combination

Combinations are a special form of permutation. While permutations take the order of occurrence into account, combinations ignore the order of occurrence.

Combination formula-**r**(number of unordered elections elements taken from fruit element), symbolized by

Combin $C(n,r)$ atau $\binom{n}{r}$:

$$C(n,r) = \frac{n!}{r!\,(n-r)!}$$

Example of Combination Formula 1:

We will try to guess the password input by as many as 4 digits, the number of characters is 4 digits, so how many ways are there to guess 2 digits from the 4 digits of letters and numbers?

Example of Combination Formula 1 above can be explained with:

n = 4, r = 2, eyes $C(4,2) = \frac{4!}{2!(4-2)!} = \frac{4!}{2!\,.2!} = 6\ Ways$

Example of Combination Formula 2:

An experiment was conducted to input a 3-digit password with only numeric characters. So, how many ways are there to guess the 3-digit password?

The example of the 2 Combination Formulas above can be explained as follows:

T1	T2	T3
111	211	311
112	212	312
113	213	313
121	221	321
122	222	322
123	223	323
131	231	333
132	232	331
133	233	332

From the solution to question number 2 above, we can see that the number of passwords with a total of 3 characters (only numbers) can be guessed with 27 guesses from a combination of numbers between 1, 2 and 3, with the following details:

a. T1 = Stage 1 guess 9 times
b. T2 = Stage 2 guesses totaling 9 times
c. T3 = Stage 3 guesses totaling 9 times

The number of possible combinations is 27, which is obtained from 9 x 3 = 27.

4. Simple Correlation

Data analysis in this study uses simple correlation analysis, namely a set of statistical techniques used to measure the closeness of the relationship (correlation) between two variables.

Correlation Coefficient Formula (r),

$$r = \frac{n(\sum XY) - (\sum X)(\sum Y)}{\sqrt{\left[n(\sum X^2) - (\sum X)^2\right]\left[n(\sum Y^2) - (\sum Y)^2\right]}}$$

4. RESULT AND DISCUSSION

Based on the results of testing the questionnaire data using the simple correlation analysis method as in table 4.2.

Table 3
Calculation of user knowledge data against password

No	Code	1	2	3	4	5	6	7	8	9	10	QTY
1	RS175	4	5	4	3	3	5	5	5	1	3	38
2	RS074	5	5	4	1	1	2	5	5	1	2	31
3	RS546	5	5	4	1	1	3	5	5	2	4	35
4	RS059	5	5	5	2	1	3	5	4	1	4	35

5	RS048	5	5	5	5	4	5	5	5	5	5	49
6	RS536	5	5	5	1	1	2	5	5	1	2	32
7	RS361	5	5	5	3	3	2	2	5	1	5	36
8	RS560	5	5	5	4	3	3	5	5	1	3	39
9	RS268	5	5	5	4	5	5	5	5	3	4	46
10	RS607	5	5	5	3	1	2	5	5	3	3	37
11	RS217	5	5	5	2	1	2	5	5	1	3	34
12	RS728	5	5	5	3	3	2	5	5	2	4	39
13	RS238	4	4	4	2	1	2	5	5	1	5	33
14	RS542	5	5	5	2	3	3	5	4	3	5	40
15	RS480	5	4	4	2	2	3	5	5	1	3	34
16	RS718	5	4	4	3	3	3	5	5	1	3	36
17	RS876	5	4	4	3	3	4	5	5	2	4	39
18	RS584	5	4	5	3	2	3	5	5	2	4	38
19	RS261	5	5	5	2	1	2	4	5	1	4	34
20	RS347	5	4	4	2	4	3	5	4	1	4	36
												741

No.	X	AND	X^2	XY	AND^2
1	4	38	16	152	1444
2	3	31	9	93	961
3	4	35	16	140	1225
4	4	35	16	140	1225
5	5	49	25	245	2401
6	3	32	9	96	1024
7	4	36	16	144	1296
8	4	39	16	156	1521
9	5	46	25	230	2116
10	4	37	16	148	1369
11	3	34	9	102	1156
12	4	39	16	156	1521
13	3	33	9	99	1089
14	4	40	16	160	1600
15	3	34	9	102	1156
16	4	36	16	144	1296
17	4	39	16	156	1521
18	4	38	16	152	1444
19	3	34	9	102	1156
20	4	36	16	144	1296
	76	**741**	**296**	**2861**	**27817**

$$r = \frac{20(2861) - (76)(741)}{\text{QUOTE } [20(296) - (76)^2]\,[20(27817) - (741)^2]}$$

$$r = \frac{904}{\text{QUOTE } [144][7259]} = 0{,}884196$$

The test was conducted on employees in the bank's operational environment and yielded positive results using the correlation coefficient calculation, indicating a direct and positive relationship between the two variables. A correlation value of 0.884196 indicates a strong relationship between the two variables. The average user already knows that password usage in the system is essential for data security, and they also feel a need for knowledge about passwords.

5. CONCLUSION

Based on the results and discussion in this development research, it is known that the implementation of password in the operational environment of Bank Muamalat Indonesia, Tbk, Jakarta Operational Head Office, especially in several sections such as financing operations,back office, frontliner, and personnel department, shows that employees feel they have an interest and need for deeper knowledge about password. This is especially related to

understanding category testing.password, which is expected to help improve ethical culture in the field of information systems, especially in the banking operational environment.

As suggestions for further system development, there are several things that can be done to optimize the system's role and the benefits experienced by internal parties, both the bank and the employees involved. First, further research is needed on the application of the combination method password for user access to positively impact system security. Second, decision-makers in the banking sector need to ensure they have sufficient information relating to the problem description and factors influencing the implementation of information system security. Third, the development of an online questionnaire (online questionnaire) that already exists should be expanded by involving employees from various other operational parts of the bank as respondents, so that the data obtained can be more accurate, comprehensive, and reflect the actual conditions in the bank's operational environment.

6. REFERENCES

Ali Pangera, Abas & Ariyus, Dony. 2008. Sistem Operasi. Andi. Yogyakarta.

Arikunto, Suharsimi. 2006. Prosedur Penelitian Suatu Pendekatan Praktik. Rineka Cipta. Yogyakarta.

Kadir, Abdul. 2003. Pengenalan Sistem Informasi. Andi. Yogyakarta.

HM, Jogiyanto. 2007. Sistem Informasi Keperilakuan. Andi. Yogyakarta.

IBISA. 2011. Keamanan Sistem Informasi. C.V Andi Offset. Yogyakarta.

McLeod, Raymond and P.Schell, George. 2004. Sistem Informasi Manajemen. Management Information System. Ninth Edition. Prentice Hall, New Jersey.

McLeod, Raymond and P.Schell, George. 2008. Sistem Informasi Manajemen, Edisi 10. Management Information System, 10th ed. Prentice Hall, New Jersey.

Setiawan, Agus. 2007. Pengantar Sistem Komputer. Edisi Revisi. Informatika. Bandung.

Taniredja, Tukiran dan Mustafidah Hidayati. 2011. Penelitian Kuantitatif. C.V ALFABETA. Bandung.

Thor. 2008. Hacker's Biggest Secret : Zero-knowledge Password. PT. Elex Media Komputindo. Jakarta.

Wahyono, Teguh. 2006. Etika Komputer dan Tanggung Jawab Profesional di Bidang Teknologi Informasi. Andi. Yogyakarta.