Access Security Implementation towards the Information System of Research, Publication and Community Service

Kodrat Iman Satoto[1], Kurniawan Teguh Martono[2] , Rizal Isnanto[3], and Rinta Kridalukmana[4]

[1] Computer Engineering, Diponegoro University, Semarang, 50275, Indonesia

[2] Computer Engineering, Diponegoro University, Semarang, 50275, Indonesia

[3] Computer Engineering, Diponegoro University, Semarang, 50275, Indonesia

[4] Computer Engineering, Diponegoro University, Semarang, 50275, Indonesia

Abstract

Information System refers to a very essential part in the development of an organization. Institute for Research and Community Service (LLPM) of UNDIP is one of organizations that manage the activities of research, publication and community service. The existence of a computer-based information system used to manage these activities is highly needed purposely to facilitate in the process of management, storing and distribution of information. Considering how important an information system is, the access security is deemed essential. One of the ways to do so is by implementing the encryption process towards the information related to the username and passwords.

In this research, the method of designing the software used is software development life cycle. It includes five phases including needs analysis, design, implementation, testing and maintenance. Each of phases is implemented entirely to go to the following phases.

The result of this research is the encryption using MD5 and added by using Salt as a key combination successfully implemented and able to be used to open the access of information system.

Keywords: ***Encryption, Information System, Security.***

1. Introduction

The advance of computer technology at the moment has emerged a change in all aspects where an organization moves. All lines in an organization today require a role of a computer technology. LPPM, Institute of Research and Community Services, of Diponegoro University, Indonesia is one of organizations implementing the advanced technology of computer in its operational. One of the implementations of computer technology is used to manage the data of research activities, publication and community service. The need for information for an organization is becoming something critical in view of its influence in taking a policy.

Today, information system has been a strategic part for organization. Such system is able to give a contribution effectively to harmonizing the business process to a strategy of an organization purposely to achieve the improvement of productivity and effectiveness [1]. IS (Information System) is a key component to obtain a success of an organization [2]. It functions to gather, process, and store, analyze and distribute the information to other parties for certain purpose.

On the other hand, the computer crime rate – particularly the one related to the information system will be increasing for the following factors:

1. The increase of the computer-network and information technology-based business application
2. Decentralization and distributed server causing more systems to be handled.
3. The improvement of users' competence on computer making them to try to play and discharge system being used.
4. The accessibility of software used to attack computer and computer network.

Hence, it is deemed critical to obtain a number of ways to secure the information system. A number of processes to secure information system can be done by conducting the encrypting process on the data or by encrypting on the application programs. Another method that can be done by using an additional component is firewall. This paper is designed to discuss about the process of information security by using encryption on the username data and

password that will be used when accessing the information system of research, publication and community service.

2. Literature Review

2.1 Information System

Information system is the data gathered, classified and processed in such manner to be a unity of information that is related and support to each other – thus producing valuable information for those obtaining it. Today, information system has been the backbone of all organizations. Say, a bank is not able to process a payment or government is not able to collect the tax, hospital is unable to treat the patients or supermarket is unable to manage the goods supply on the display without a support from information system. In short, most of all sectors both in education, health, finance, and manufacturing and in large-scale or small scale business system highly require information system. Certainly, information, for some reasons, now plays an essential role in the development of an organization [3].

Computer-based information system comprises some components including hardware, software, database and people involved [4]. Information system is divided into four types arranged in a pyramid. The lowest type is Transaction Process System, Management Information System, Decision Support System and the last type is Executive Information system. Figure 1 illustrates the types of information system

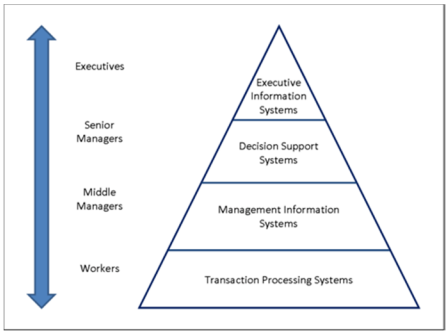

Figure 1. Hierarchy of the type of Information System

From Figure 1, it can be explained as follows:

1. Transaction Processing Systems (TPS) is the computerized information system developed to process the large scale data for a transaction in an organization. An example of TPS is the record of data from sales, salary and purchase.
2. Information System Management is a system of planning for a part of internal control of a business including the use of human, document, technology and procedure by management accounting to solve any business problems regarding, for example, product expense, service or a business strategy.
3. Decision Support Systems (DSS) refers to a set of certain classes of computerized information system supporting any activities of business or organization decision making. DSS designed correctly is an interactive software-based system designed to assisting the decision makers to compile the information that is useful from the raw data, document, and personal knowledge to identify and solve any problems in making a decision.
4. Executive Information System (EIS), also known as Executive Support System (ESS), is an interactive computer–based system that makes it possible for any executives to access the data and information. Hence, it is possible to identify the problem, explore the solution, and become a base in a strategic planning process.

2.2 Information System Security

In view of how important the information system is, it then leads to more increasing potential of threat towards the information system. A threat for information system can be divided into two – active and passive. The active threat can include any frauds and crime towards computer. Meanwhile, a passive threat can include the failure of system, human error and natural disaster.

To secure the information, it can be done by coding process towards the original information. Encryption is a process making a change from an understandable code to be the one unable to be understood (unreadable). Encryption can be interpreted as a code or chipper. A coding system uses a table or a dictionary that has been defined to replace a word from information or as a part of information sent. A chipper uses an algorithm that can code all data stream of bit from a message to be an unintelligible cryptogram [5]. The management towards security can be seen from the side of risk management. To managing any threat in an information system, Risk Management Model has been made then [6]. In this model, there are three components that can give a contribution to Risk, those are Asset, Vulnerabilities, and Threats. Table 1 shows the contribution to Risk in information system.

Table 1. Risk Contribution

No	Name of Components	Example
1	Assets	Hardware, software, documentation, data , communication, environment, human
2	Vulnerabilities	Software bugs, hardware

		bugs, tapping, crosstalk, unauthorized users, storage media
3	Threats	Users, terrorist, accidents, crackers

Figure 2 shows a encrypting process of information

Figure 2. Encryption Process [7]

Figure 2 shows how an encrypting process in sending a message "Hello!" when a message is sent to a transmission media. Then the message is camouflaged to prevent the tapper unable to obtain the original information. Then, when the information is accepted, the camouflaged information will be retranslated – thus making the authorized message accepter is able to read the point of the message sent.

Any kinds of algorithm are used to improve the security of information system. One of algorithms used in this case is by using MD5 (Message Digest 5). MD5 Algorithm accepts an input in the form of message with a random size and results in a message digest that is 128 bit in length. The MD5 algorithm uses the function of HASH in which the function accepting the input string with a random length will convert it to be an output string with the same length [8]. The function of HASH can accept any strings. If the string states a message, then the randomized message of M sized freely is compressed by the function of HASH H through the equation 1.

$$h = H(M) \quad \text{.....(1)}$$

where the output of function HASH can be also called as HASH value or message digest. In equation (1), h is a hash value or message digest from the function H for the input M[9]. The process of making message digest using algorithm of MD5 is shown in Figure 3.

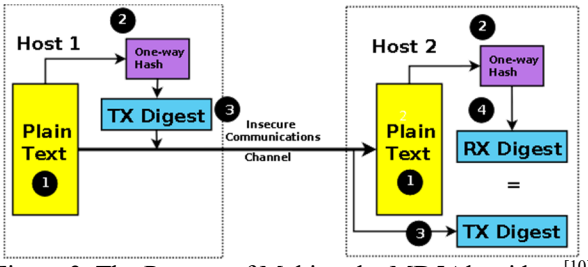

Figure 3. The Process of Making the MD5Algorithm [10]

The steps of making message digest in broad line can include as follows:

1. The addition of bit-bit padding bits)
2. The addition of the long value of initial message
3. Initialization of buffer MD.
4. The message management in the 512-bit block.

2.3 MVC

In developing the computer-based information system, the use of framework is highly helpful in the process in making it. One of the frameworks that can be used in the development is CodeIgniter. Using the framework of CodeIgniter, then this process that is done does not need to be started from the beginning. Each function used has been provided in the library present in the framework of CodeIgniter.

The concept applied in the framework of CodeIgniter is by using the MVC (Model, View, and Controller) concept. In this development process, this division is aimed to separate each part in the display design process, connection with the database and other processes. Model is a part to represent the data that will be used by application as the business process associated towards it. By sorting it as a separated part, as in data accommodation, data, persistence, and manipulating process, it can make it separated with other part of application. View is a layer that contains an entire detail from the implementation of user interface. In this layer, the graphic component provides the representation of the internal process of application and leads the path of user interaction to the application. Meanwhile, the final part is Controller, a connector between Model and View. The Controller consists of class and functions processing any request from the View into the data structure in the Model. The Controller also cannot contain the code to access database. It acts to provide any variables that will be displayed on view, calling model to do an access to the database, providing error management, doing a logic process from the application and making validation or checking towards the input. Figure 4 illustrates the basic correlation of Model-View-Controller.

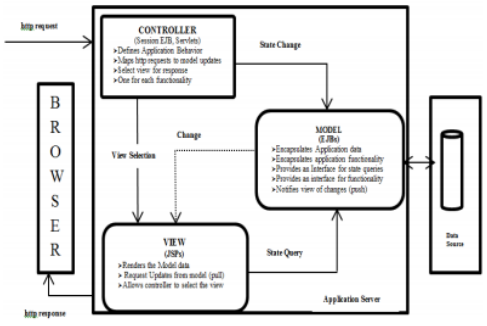

Figure 4. Correlation of Model, View, and Controller[11]

3. Method

To obtain an accountable result of a research, a structured method is highly needed. In this research, SDLC (Software Development Live Cycle) method was used. It was more emphasized on the design of security of Information System at the access level of login. The phase conducted in this research is illustrated in Figure 5.

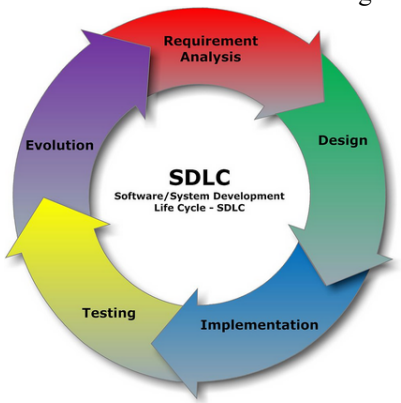

Figure 5. Model SDLC.

1. The phase of need analysis in this research is presented in Table 2

Table 2. Need Analysis of the System

No	Need	Remark
1	Username	Used as an evidence in accessing the system. Information security of username is required. Hence, encrypting process is needed.
2	Password	As a key to open or enter in the information system of research, publication and community service. To secure the data of password, then the encrypting process is needed.
3	Access Level	To determine the area of user access into the information system of research, publication and community service.

The next phase was the structure design of database for the rights of access and the login display design. Table 3 presents the design display from the data structure that would be used in storing the rights of access towards the information system or research, publication and community service.

Table 3. The Design of Field Structure in Database

No	Field	Type	NULL
1	id_user	Int(4)	
2	nidn	Varchar(20)	
3	user	Varchar(32)	
4	pass	Varchar(32)	
5	level	Int(1)	
6	email	Varchar(32)	
7	Faculty	Int(2)	
8	Time	timestamp	
9	status	Int(1)	

Field username and password are the data that have been encrypted using MD5Algorthm added by modification of keyword. Meanwhile, the display of login page is shown in Figure 7.

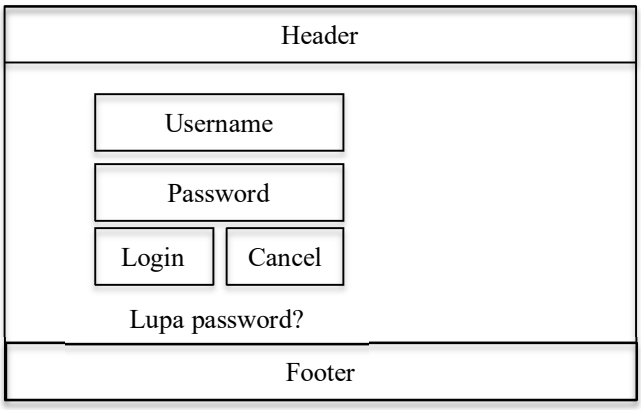

Figure 7. Design of Login Display

2. Implementation is a phase of making program code with a design that has been described in Figure 7. The phase of the database implementation using the commands as follows.

```
CREATE TABLE IF NOT EXISTS `user` (
`id_user` int(4) NOT NULL AUTO_INCREMENT,
`nidn` varchar(20) NOT NULL,
`user` varchar(32) NOT NULL,
`nama` varchar(50) OT NULL,
`pass` varchar(32) NOT NULL,
`level` varchar(25) NOT NULL,
`email` varchar(100) NOT NULL,
`fakultas` int(2) DEFAULT NULL,
 `jurusan` int(3) DEFAULT NULL,
`status` int(1) NOT NULL,
`waktu` timestamp NOT NULL
DEFAULT URRENT_TIMESTAMP
ON UPDATE CURRENT_TIMESTAMP,
PRIMARY KEY (`id_user`),
UNIQUE KEY `username` (`user`),
UNIQUE KEY `NIDN` (`nidn`))
ENGINE=MyISAM
DEFAULT CHARSET=latin1
AUTO_INCREMENT=74;
```

3. The next phase is to do a system testing. The testing used a white-box testing. It was aimed to figure out whether the code and algorithm used has been suitable.
4. The final phase was by doing an evolution process or the development to the newer system.

4. Implementation and Testing

4.1 Implementation

The implementation of Table user in the database is shown in Figure 8.

	Field	Type	Collation	Attributes	Null
	id_user	int(4)			No
	nidn	varchar(20)	latin1_swedish_ci		No
	user	varchar(32)	latin1_swedish_ci		No
	nama	varchar(50)	latin1_swedish_ci		No
	pass	varchar(32)	latin1_swedish_ci		No
	level	varchar(25)	latin1_swedish_ci		No
	email	varchar(100)	latin1_swedish_ci		No
	fakultas	int(2)			Yes
	jurusan	int(3)			Yes
	status	int(1)			No
	waktu	timestamp		on update CURRENT_TIMESTAMP	No

Figure 8. The Implementation of Table User in dbms MySQL

The login process in this information system is shown in Figure 9.

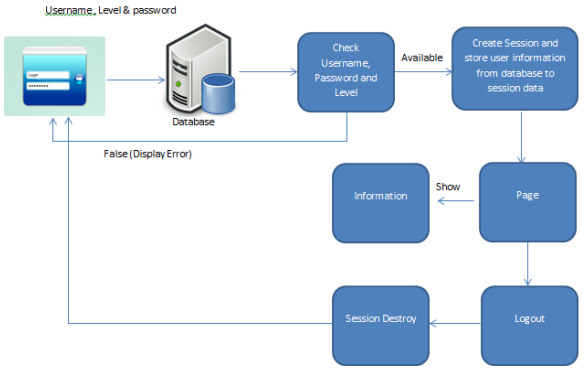

Figure 9. Diagram of Login Process Flowchart

The explanation in Figure 9 is as follows:

1. User does login first before accessing the entire system
2. Data or information sent to the database is given an encrypting process and would be matched with the data or information in the database.
3. IF the data is not proper, then the message about the error in the form of login will be displayed.
4. Any proper data or information would be given session and can access the page addressed in accordance with its access level.
5. Click the logout, then it would replace the status session and would be taken back to the initial page.

The program cuts used to do an encrypting process of a data as well as user information when checking the validation of the data in the database.

```
<?php
class User extends CI_Model
{
    function login($username,$password,$level)
    {
        $this->db->select('id_user,user,pass');
        $this->db->from('user');
        $this->db->where('user',$username);
        $this->db->where('pass',MD5($password));
        $this->db->where('level',$level);
        $query=$this->db->get();
        if($query->num_rows()==1)
            {
                return $query->result();
            }
        else
            {
                return false;
            }
    }
}
?>
```

The system testing was conducted in the local computer environment using the server apache and MySQL database united in the program of XAMPP. Figure 10 shows the result of the testing on the initial page display from the information system of research, publication and community service.

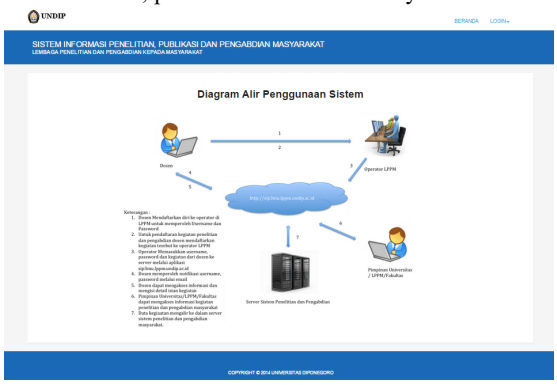

Figure 10. The Display of Initial Page

The Display of initial page in Figure 10 contains information about how information system works. Figure 11 shows a display for the proper login process in accordance with the level of access owned.

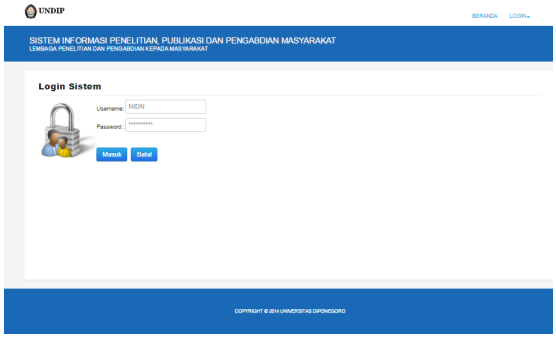

Figure 11. The Display of Login Page

4.2 Testing

The test of white-box and black-box for the login process. Berikut ini adalah potongan program pada model login.

```
[1]  <?php
[2]  class User extends CI_Model
[3]  {
[4]    function login($username,$password,$level)
[5]    {
[6]              $this->db->select('id_user,user,pass');
[7]              $this->db->from('user');
[8]              $this->db->where('user',$username);
[9]              $this->db->where('pass',
                      md5($password.md5($password)));
[10]             $this->db->where('level',$level);
[11] $query=$this->db->get();
[12] if($query->num_rows()==1)
[13] {
[14] return $query->result();
[15] }
[16] else
[17] {
[18] return false;
[19] }
[20] }
[21] }
[22] ?>
```

Cyclomatic Complexity that has been resulted in is shown in Figure 12.

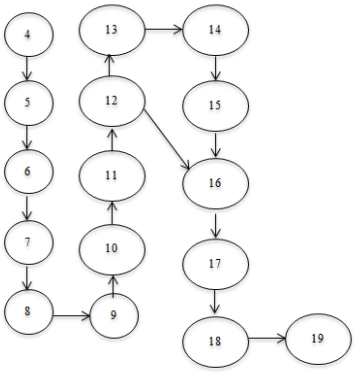

Figure 12. Cyclomatic Complexity

From Figure 13, it is found two paths of testing. The path I is when the testing passes the point of 4-5-6-7-8-9-10-11-12-13-14-15. Meanwhile, the path II is a test passing the 4-5-6-7-8-9-10-11-12-16-17-18-19.

Path I is a scenario of testing when the data to be entered was a correct data. For this, the program would continue to display the page that is suitable with the access rights. Meanwhile, Path 2 is the result when the input data was wrong. Then, it would go to the login page and give information about the error message.

To test the functionality of the login system in the application of information system of research, publication and community service is shown in Table 4.

Table 4. Testing Result of Black Box

Testing	Expected Result	Testing
The testing of the login form with the correct password, username and level	Login is successful suitable with access rights	Successful
Testing on the login form with the erroneous username data, correct password and level.	Login is failed	Successful
Testing on the login form with erroneous username data and password but correct level	Login is failed	Successful
Testing on Login Form with erroneous username data, password and level.	Login is failed	Successful
Testing on the login Form with correct username data, erroneous password and correct level	Login is failed	Successful
Testing on the login form with correct username data, but erroneous password and level.	Login is failed	Successful

5. Conclusion

The results of the testing using the Black Box and White Box are as follows:

1. Encryption using MD5 and added by Salt as a key combination were successfully implemented and can be used as a key to open the access of Information System.
2. Testing scenario using white-box produced two access paths for correct input data and wrong data.
3. Scenario or the expected result from the Black Box testing showed a result with the successful value. Thus, the functionality of work system is in line with the scenario.
4. The security of username password and access level are guaranteed by using encryption of MDS added with the slat as the key combination

References

[1] M. Oussama, T. Amal, T. Mohammed, Towards a New Maturity Model for Information System, International Journal Computer Science and Issue, Volume 12, Issue 3, May 2015.
[2] M. Elmaallam, A. Kriouille, "Towards A Model of Maturity For IS Risk Management", International Journal of Computer Science & Information Technology (IJCSIT) Volume 3, No 4, August 2011.
[3] https://mitpress.mit.edu/sites/default/files/titles/content/9780262015387_sch_0001.pdf accessed 26/08/2015
[4] E. Turban, Leidner, et.al, Information Technology for Management, John Wiley & Sons, 2007
[5] https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201107_en.pdf accessed 27/08/2015
[6] Gary Stoneburner, Alice Goguen, and Alexis Feringa, *Risk Management Guide forInformation Technology Systems*, National Institute of Standards and Technology Special Publication 800-30, Juliy 202
[7] https://www.digicert.com/ssl-cryptography.htm
[8] Steven M. Bellovin and Eric K. Rescorla, Deploying a New Hash Algorithm, in: Proceedings of the Network and Distributed System Security Symposium, NDSS 2006, San Diego, California, USA, The Internet Society, 2006
[9] http://www.zytrax.com/tech/survival/encryption.html accessed 10/09/2015
[10] Rajeev Sobti, G.Geetha, Cryptographic Hash Functions: A Review, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, March 2012
[11] Raheela Nasim, Software Architectures: A Comparative Study for Web Based Applications, IJCSI International Journal of Computer Science Issues, Vol. 11, Issue 4, No 1, July 2014

Kodrat Iman Satoto He got his bachelor and magister degree from Department of Electrical Engineering, Gadjah Mada University in 1991 and 1999, respectively. At the moment, he is a lecturer in Department of Electrical Engineering, Diponegoro University, Semarang since 1993. The research fields he elaborates include database, computer network, and technology and information system.

Kurniawan Teguh Martono, He graduated from undergraduate program of State University of Semarang)in 2006 and graduated from postgraduate program of Electrical Engineering of Bandung Institute Technology (ITB) in 2008. He is a lecturer at Computer System at Engineering Faculty of Diponegoro University, Semarang

Rizal Isnanto, completing undergraduate and postgraduate (S2) at the Department of Electrical Engineering, Gadjah Mada University, Yogyakarta in a row in 1994 and 2002. Now he is taking the Doctoral Program at the Department of Electrical Engineering and Information Technology at the same university. In addition, He is still active as a lecturer in the Department of Electrical Engineering and Computer Systems Studies Program, University of Diponegoro, Semarang.

Rinta Kridalukmana, He got his title as Computer Bachelor from Department of Information System in Stikubank Semarang in 2003 and Magister title from STEI ITB (School of Electrical Engineering and Informatics, Bandung Institute Technology) in 2007. At the moment, he is one of the members of Association for Computing Machinery and a lecturer at the Program of Computer System Engineering, Diponegoro University since 2011. The research field is in Information System, Mobile application and integration data.