Application Mail Tracking Using RSA Algorithm As Security Data and HOT-Fit a Model for Evaluation System

Ginanjar Setyo Permadi[1,*], *Kusworo* Adi[1,2], *Rahmad* Gernowo[1,2]

[1]Master Program of Information System, School of Postgraduate School, Universitas Diponegoro
[2]Physic department, Faculty of Science and Mathematics, Universitas Diponegoro

Abstract. RSA algorithm give security in the process of the sending of messages or data by using 2 key , namely private key and public key .In this research to ensure and assess directly systems are made have meet goals or desire using a comprehensive evaluation methods HOT-Fit system .The purpose of this research is to build a information system sending mail by applying methods of security RSA algorithm and to evaluate in uses the method HOT-Fit to produce a system corresponding in the faculty physics. Security RSA algorithm located at the difficulty of factoring number of large coiled factors prima, the results of the prime factors has to be done to obtain private key. HOT-Fit has three aspects assessment, in the aspect of technology judging from the system status, the quality of system and quality of service. In the aspect of human judging from the use of systems and satisfaction users while in the aspect of organization judging from the structure and environment. The results of give a tracking system sending message based on the evaluation acquired.

1 Introduction

Letter is communication in writing containing a information would be delivered or sent by one party to another individually or organization, company, and the office. The utilization of technology in assist with the send a message/ data is part of information system. System information can be defined as a means to present information in such manner that beneficial for recipients for the purpose present information to decision-making on planning, organizing, control operations subsystem an enterprise, and presenting synergy organization on a process [1].

Mail delivery system over the internet from various hardware and software components that include the sender's client computer, server, client and server computer with the required software and services are installed on each client [2]. The use of the mail delivery system is not only used to communicate between users but also between users and other organizations online services [3]. Organizations such as academic institutions or business companies typically manage their own mailing system, providing everyone with an address post mail in mail server by using the mailing list [4].

Mail Tracking is a way to monitor the delivery of a mail to the recipient or destination of the shipment. Most of the tracking technology using some form of digital records to reveal the exact time and date of the mail has been opened or received, as well as the IP address of the recipient [5]. In a mail tracking information system development needs must be viewed from a supporting factor for the creation by choosing the method of development of the system.

In this study add Algorithm Rivest Shamir Adleman (RSA) to provide security of a message or data in the process of delivery. RSA has two keys, a public key and a private key. RSA security located in the difficulty of a large number of factors being the prime factors [6]. With the addition of the RSA can give a sense of security in the process of sending data over the internet then it needs the addition of an algorithm or method in the construction of a data security system.

As for previous research about the implementation of digital signatures for security systems for authentication data mail tracking sender or signer of the letter, and based on one letter if signed by n sender verification should be done as much then n times. If all n Verify valid value means have penetrated the security tier n in terms of verification. Conversely, if one or more of the results invalid and verification or fail then the recipient can find out if the letter is received is not authentic and or one or more of the signatories of the letter was not the one who actually signed the letter. In the previous research for the correct letter, it sends the same letter maker directly without any changes from others.

* Corresponding author: ginanjar.s.permadi@gmail.com

To ascertain and assess directly whether the system has been made already achieve the goal or desire, in this research adds a method evaluation system. There are many methods to do the evaluation system, in this study using the method of human, organization and technology fit (HOT-fit). HOT-fit approach discusses the important components of the information system (SI), i.e., human, organizational and technological, and conformity between them using a comprehensive approach, sustainability and systematically to analyze the key components of the system, development, use, and net profit [7].

Based on government regulation republic of Indonesia No. 82 in 2012 about organizing systems and electronic transactions mentioned in article 1 paragraph 6 and 7 containing about understanding electronic information which is the set of electronic data (sounds, images, maps, photos, e-mail, electronic data Interchange, telegram) and understanding electronic documents that have a sense of any electronic information are made, forwarded, transmitted, received, or stored in the form of analog, digital, optical, electromagnetic, or similar ones, which can be seen, displayed, and/or heard through a computer or electronic systems. The use of e-mail has also stated in the Legislation of the Republic of Indonesia number 11 Year 2008 Electronic information and Transactions About article 5 and 6, which contains Information about electronic and/or electronic documents and/or the results of the print is legitimate and legal evidence of electronic information and/or electronic documents are considered valid throughout the information contained in it can be accessed, displayed, secured unity , and socially so that explains a situation.

With information from the Government of the Republic of Indonesia and the Republic of Indonesia that has been described above, making the system mail tracking in the systematic study of can help and contribute directly to provide information with a message or mail in send. This will give advantage in the proposed system can be run in an organization or company. So making the mail tracking system using RSA and HOT-Fit is expected to optimize the performance in terms of data transfer or messages, so that the information will be shared or posted can be easily on the monitor.

2 Theoretical Framework

2.1. Mail Tracking

Mail tracking is the way or method to monitor sending message to recipients sent in a system .The grooves of delivery systems message that is , messaging transmits a message be kept in a database mail server messaging and system continue the sending of messages to mail server the purpose of delivery , then the system give notice incoming messages to recipients of a message [2]. As for explanation structure / a groove system of process of shipping mail on Figure 1.

Fig 1. Flowchart of mail

Based on a groove system the e-mails and then in system that built this users can do tracking message sent have been opened, passed on, status of the message has been in verification, and status message on process. Messaging to know a response from recipients message to a message that which had been shipped. Figure 2. Drawing a groove delivery and response system.

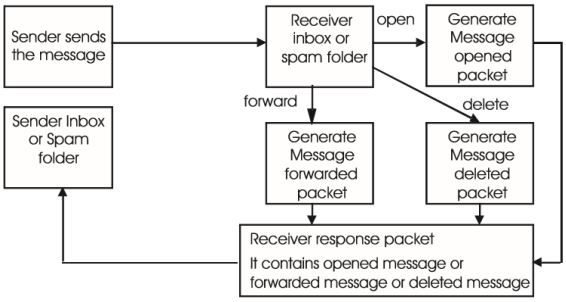

Fig. 2. Mail Message and Response Flowchart Diagram

2.2. Algorithm RSA

Including algorithm RSA algorithm asymmetry, namely the algorithms having 2 key, public key and private key. Security RSA algorithm located at the difficulty of factorization number of large coiled factors prima. Factorization is conducted to gather private key. During factorization number of large coiled factors prima has not been found the algorithms that good, so long as it security rsa fixed guaranteed [6]. Key to do in such a way that a decryption key may not be easy deduced of the encryption key public, as a in Figure 3.

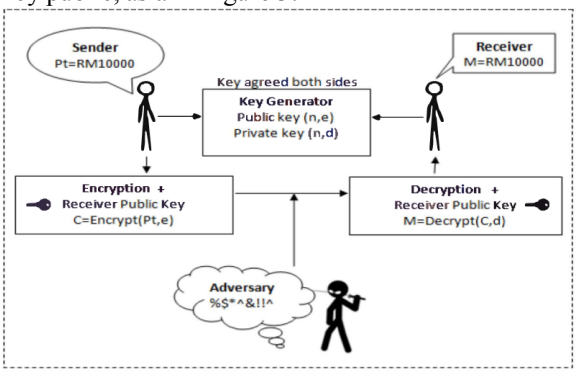

Fig. 3. RSA encryption algorithm

2.2.1 Key Generation Process

a. Select two parameters, namely p and q, these two parameters must be random prime number
b. Compute $n = p \times q$.
c. Compute $\Phi(n) = (p - 1)(q - 1)$.
d. Choose the exponent k if : GCD (h(id), phi (n)) = 1 Else, looping the process 1 to 6 and until k=1

e. Compute $d = e$ -1 mod $\Phi(n)$
f. Public key : (e, n)
g. Private key : (d, n)

2.2.2 Encryption Process

a. use public key (e, n).
b. Choose plainteks M, $0 \leq M \leq n$ -1 .
c. Compute $C = M\ e$

2.2.3 Decription Process

a. Use private key (d, n)
b. Compute $M = C\ d$ mod n.

2.2.4 Hash Function

Hash function is one of a mathematical function, who takes a long variable string input, called pre-image and convert them to a string output by long fixed and usually smaller consisting of letters and digits look random (binary data written in hexadecimal notation), called message digest [8].

Function hash one direction (one-way hash function) is hash function who works one direction, which is a hash function who can calculate message of pre-image digest, but is very difficult to count pre-image of message digest.

2.5 Evaluation System

Evaluation research is to collect , analyze , and presenting information which is useful about the object evaluation , rating them by comparing it with an indicator evaluation and the results should be used to evaluate and making decisions on the object evaluation.

Function evaluation system in this case to assess the implementation of delivery systems message may be accepted or need of improvements to systems. Methodology data collection using evaluation system with the spread of questioner directly based on an indicator variable model evaluation selected system.

2.5.1 HOT-fit Model

The framework of human, organization, technology-fit (HOT-fit) model was a development of success of the information system delone and mclean. Model evaluation explain all of the components that contained in information system, "human" assessment or in view of the use of (use of system) relating to the use, training, experience, knowledge, hope, the reception and rejects the. "organization" who feel system of organization the structure and organization environment associated with management planning, control system , support management, and financing. While in terms of "technology" can be seen from system quality, quality of information, and services [9].

HOT-fit has 3 aspects and different perspectives in every aspect. In aspect of technology, there are three dimensions: (1) system mention status; (2) the quality of information; (3) quality of service. In aspect of people, there are two dimensions: (1) use; system and (2) satisfaction users. In the organization, there are two dimensions: (1) structure; and (2) environment.

As for explanation three aspects that side in figure 5 the following [10].

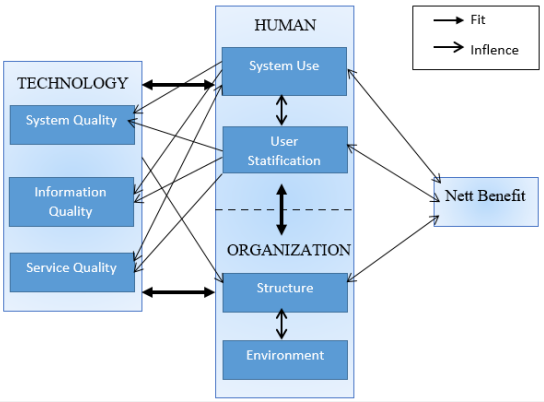

Fig. 5. HOT-Fit Evaluation Framework

3 Result and Discussion

3.1 Information System Sending Mail

The sending of messages information system is a system that provide the services the sending message a message the notification letter, the meeting, and the permission. In building information systems sending mail need data of mail template used at an object research. This system can do tracking message based on the number of letters and display information about a letter of the message timestamp opened, continued, verification status, and the status of being processed.

3.1.1 Algorithm

In this section, the method proposed is RSA algorithm. Figure 6 shows diagram a groove algorithm key power station. The first step in key generation is choose two random prime number for p and q, after that calculate n = p*q. Next step is calculate value of modulo phi(n)=(p-l)*(q-l). User input their email id as a parameter e, and get decimal value for email id using CRC hash function h(id)= hash (e). After that test either GCD (h(id),phi(n)) = \ or not. If value of GCD=\, so that email id can be a public key, and if GCD is not equal to one, the process will be looping from the first step to get new value of modulo until GCD equal to one.

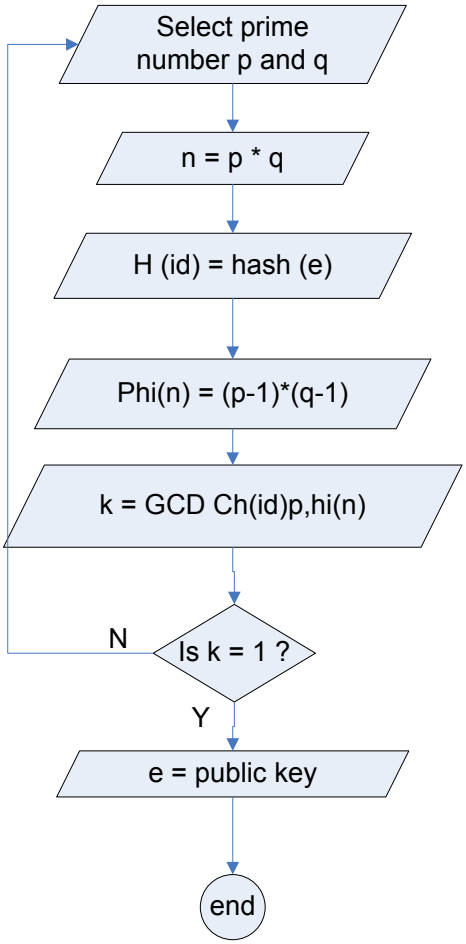

Fig. 6. Flow chart of i-RSA algorithm key generation

Table 1. Showing samples of data which implements RSA algorithm stored in a database.

Table 1. Applied algorithm RSA

Mail Number	Body	Publik Key	Mod Key
SJ/1234/1234	4521031425665177139 4748813461942348316 9508409774...	5	56147513 70746471
SJ/1234/1235	1816691989958088317 0032316292452398393 799954485 ...	5	54330613 89057521
SJ/1234/1236	751333.1506281076143 469.2696393490444714 .5754029...	5	86700716 34754457
SJ/1234/1237	4460713701637443034 1360827509712800700 3498064 11...	5	49342639 9904741
SJ/1234/1238	1741431677165025210 6022005741841916661 6584 14364...	5	25296861 766199

3.1.2 Mail Tracking

Figure 7. Showing menu tracking a message from information systems that built. The first step in do tracking message by inserting number a message to his search string, after that select the search button

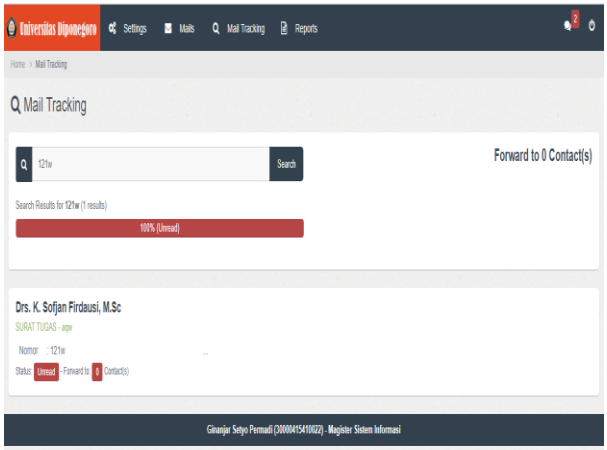

Fig. 7. Mail Tracking

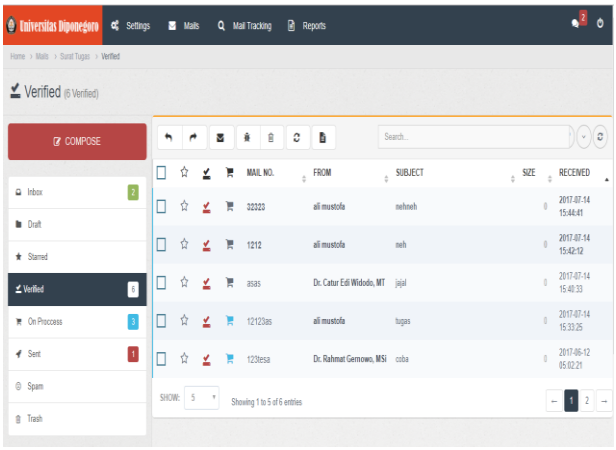

Fig. 8. Status mail

Figure 8. Showing the parts of a feature system can give status message sent. Status the message of status verification and status being processed. If the message has been in verification so menu the

3.2 Evaluation of Applied information system

The final stage is do the analysis afterwards evaluation of the implementation of a system of information the sending of messages which have been made .This research use the model hot fit developed by Yusof et al [7] to assess the success of the implementation of information system the sending of messages. Hot fit model is a model that complete and most according to the condition of the existing problems compared with a model that other.

Then the system will do the search based on the number the letter. The result of the process search

provides information that of the message has been is read with details date and time opened, and information message has forward.

Verification will display messages that was in verification. Where as if message being processed so menu being processed will display messages that has been in the process.

Variable in this research consists of eight variable i.e. quality of a system, quality of information, quality of services, organizational of structure, and use of endogenous variable, satisfaction complainants, organizational environment and benefits.

Model evaluation information system portray a hypothesis the relationship between the factors that directly have an impact on information systems, on the model the evaluation was, the quality of system, the quality of information and quality of service used as a hypothesis to influence the assumption users against the system beneficial (net benefit and easy to use [6]. Hypothesized model developed for the evaluation of information system the sending of messages as follows :

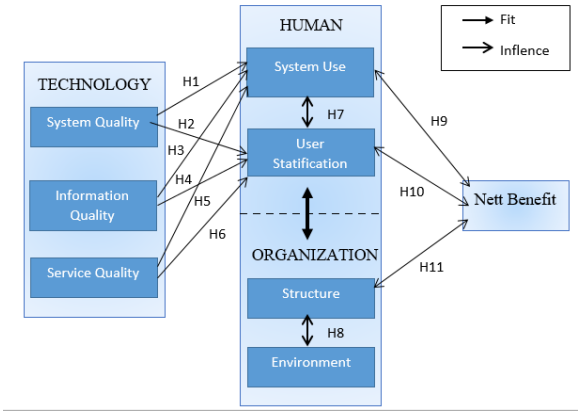

Fig. 7. Evaluation Hypothesis Model

The conceptual framework research can be seen on Figure 7. There are seventeen hypotheses in this research:

1. H1 : system quality has a significant positive effect towards system use.
2. H2 : system quality has a significant positive effect towards user satisfaction.
3. H3 : information quality has a significant positive effect towards system use.
4. H4 : information quality has a significant positive effect towards user satisfaction.
5. H5 : service quality has a significant positive effect towards system use.
6. H6 : service quality has a significant positive effect towards user satisfaction.
7. H7 : system use has a significant positive effect towards user satisfaction.
8. H8 : structure has a significant positive effect towards environment.
9. H9 : system use has a significant positive effect towards net benefits.
10. H10 : user satisfaction has a significant positive effect towards net benefits.
11. H11: environment has a significant positive effect towards net benefits

In evaluation system uses the data collected from questioner granted to information system sending of mail person as respondents. Users is lecturer and employees in the physics faculty Diponegoro University with the total respondents 35 people. Table 2. Show framework evaluation begins with the interpretation of the every aspect on the model hot-fit into one statement measurable, consisting of variable and indicators.

Table 2. Variables and indicator

No	Variables	Indicator
1	System Quality	System easy to use and user friendly System view is not confusing Security system System easy of learning The system rarely errors
2	Information Quality	Accuracy Availability Timeliness Completeness Information easy to read
3	Service Quality	Fast quality and responsive System easy to access
4	System Use	System use to easy for searching information System Use helping work every day System use can help in decision making Level of use
5	Use Stratification	Facilities and features as need of user Need system development Facilities and features according to needs Accurate information User satisfied with system view Over all system liked expectation Easy to use
6	Structure Organization	System is a strategy for performance improvement Always updating hardware or software System has been well planned Institution support implemented system
7	Environment	Assist in submitting letters Improve work efficiency Help make decision Help reach the goal effectively Improve communication between all parts of organization

Table 3. Test results statistic-t

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	Standard Error (STERR)	T Statistics (|O/STERR|)
KI -> KP	0,190418	0,183789	0,073820	0,073820	2,579470
KI -> PS	0,800221	0,811994	0,073040	0,073040	10,955888
KL -> KP	0,632795	0,645636	0,084925	0,084925	7,451253
KL -> PS	0,700640	0,696069	0,115518	0,115518	6,065214
KP -> NB	-0,084379	-0,043700	0,044658	0,044658	1,889464
KP -> PS	-0,526889	-0,534306	0,182610	0,182610	2,885326
KS -> KP	0,221444	0,213358	0,067641	0,067641	3,273805
KS -> PS	0,089517	0,088287	0,026991	0,026991	3,316587
LO -> NB	-0,690410	-0,660785	0,057967	0,057967	11,910355
PS -> NB	-1,114080	-1,001627	0,194129	0,194129	5,738872
SO -> LO	0,882306	0,889061	0,015202	0,015202	58,037257
SO -> NB	2,751230	2,580272	0,234069	0,234069	11,753918

In Table 3. It is a reject hypothesis or accepted based on value from t statistic compared with t table, in this

research have 95% (α =0,05) value t table with significant of degree 95% is 1,77.
Based on result of research t statistic, then can be determined hypothesis test in this research :

Table 4. Result of research hypothesis test

H1	system quality has a significant positive effect towards system use	Accepted
H2	system quality has a significant positive effect towards user satisfaction	Accepted
H3	information quality has a significant positive effect towards system use	Accepted
H4	information quality has a significant positive effect towards user satisfaction	Accepted
H5	service quality has a significant positive effect towards system use	Accepted
H6	service quality has a significant positive effect towards user satisfaction	Accepted
H7	system use has a significant positive effect towards user satisfaction	Accepted
H8	structure has a significant positive effect towards environment	Accepted
H9	system use has a significant positive effect towards net benefits	Accepted
H10	user satisfaction has a significant positive effect towards net benefits	Accepted
H11	environment has a significant positive effect towards net benefits	Accepted

4 Conclusion

In this research has been built information system sending mail by add RSA algorithm in the security of the mail sending process. The output of system is mail status report has been opened and forwarded. Result of the system is evaluated using HOTfit method based on the questionnaire of user system. Evaluation result show that the system has been good implemented in physics faculty Diponegoro University.

References

1. 1 J. J. Y. Chen, M. Z. Wu, *Integrating Extreme Programming with Software Engineering Education*. MIPRO (2015).
2. 2 J. Divya, D. Jagadeesan, G. Asha, *i-manager's Journal on Communication Engineering and Systems* (2016).
3. 3 I. Kounelis, SeadMuftic, J. Löschner, *Secure and Privacy-enhanced E-Mail System based on the Concept of Proxies*. (2014)
4. 4 H. Kim, S-Y. Shin, T. Motomichi, *Proceedings of the Seventh International Conference on Web-Age Information Management Workshops* (WAIMW'06) IEEE. (2006)
5. 5 G. Singh, M. Kaur, International Journal of Advanced Research in Computer Science and Software Engineering, Volume **5**, Issue 1. (2015)
6. 6 H. Delfs, and H. Knebl, *Introduction to Cryptography, Principles and Applications* Second Edition. Springer (2007).
7. 7 M. M. Yusof, HOT-fit Evaluation Framework: Validation Using Case Studies and Qualitative Systematic Review in Health Information Systems Evaluation Adoption. (2008)
8. 8 R. Munir, *Kryptografi,* Bandung: Informatika. (2004)
9. 9 I. P. Ramayasa, Journal of Theoretical and Applied Information Technology. (2015)
10. 10 L.M. Erlirianto, A. H. N. Ali, A. Herdiyanti, The Third Information Systems International Conference. Procedia Computer Science **72** 580 – 587 (2015).
11. H. A. *Fatta, Analisis dan Perancangan* Sis*tem Informasi*. Yogyakarta : Andi. (2007)
12. N. Muhammadi, J.M. Zaini, M. Y. M. Saman, Interational Conference on Control, Automation and Systems (ICCAS 2013) in Kimdaejung Convention Center, Gwangu, Korea. (2013)