TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 19, No. 5, October 2021, pp. 1535~1543
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v19i5.20403

Improvement security in e-business systems using hybrid algorithm

L Sumaryanti[1], Dedy Hidayat Kusuma[2], Rosmala Widijastuti[3], Muhammad Najibulloh Muzaki[4]
[1]Department of Informatics, Universitas Musamus, Merauke, Indonesia
[2]Department of Information Technology, Politeknik Negeri Bayuwangi, Banyuwangi, Indonesia
[3]Department of Agrotechnology, Universitas Musamus, Merauke, Indonesia
[4]Department of Information System, Universitas Nusantara PGRI Kediri, Kediri, Indonesia

Article Info

Article history:

Received Sep 16, 2020
Revised Jul 15, 2021
Accepted Jul 29, 2021

Keywords:

Cryptography
Decryption
E-business security
Encryption
RSA algorithm
Symmetric key

ABSTRACT

E-business security becomes an important issue in the development of technology, to ensure the safety and comfort of transactions in the exchange of information is privacy. This study aims to improve security in e-business systems using a hybrid algorithm that combines two types of keys, namely symmetric and asymmetric keys. Encryption and decryption of messages or information carried by a symmetric key using the simple symmetric key algorithm and asymmetric keys using the Rivest Shamir Adleman (RSA) algorithm. The proposed hybrid algorithm requires a high running time in the decryption process compared to the application of a single algorithm. The level of security is stronger because it implements the process of message encryption techniques with two types of keys simultaneously.

Corresponding Author:

L Sumaryanti
Department of Informatics
Universitas Musamus
Kamizaun Road, Merauke, Indonesia
Email: lilik@unmus.ac.id

1. INTRODUCTION

E-business systems have an important role in transaction management and business processes, and can create a competitive advantage, to compete in marketing and customer service development. Rice milling business is one of the processing industry category businesses [1] which produces rice production that is ready to be marketed, so this business has an important role in the agribusiness system in rice in Indonesia [2]. The need for increased customer service and transaction security, for business process management and presenting information in real-time, has become a new revolution as a breakthrough in utilizing the capabilities of internet technology using e-business [3]. Internet networks have innovated civilization from all directions, and have transformed business processes into a series of electronic-based financial transactions [4]. E-business systems accessed through the internet for business process management, electronic commerce, transactions between business partners, customers, suppliers, and other stakeholders in the company [5]. The development of e-business systems can improve customer service [6], business efficiency, and provide information according to user needs [7], [8]. The opportunity for e-business [9] to become a means of supporting business is the strength of the company is competing in modern markets [10].

Management of business transactions in an e-business system creates various problems, one of which is transaction security [11]. Security guarantees in e-business systems must be provided [12], to maintain the convenience of customers and companies in conducting business transactions. Security implementation can be done through various techniques such as encryption with homomorphic algorithms [13]. Risk control to ensure transaction security in system development with electronic transactions using a quantitative model. Determination of standards and limits of transaction security involving automatic information exchange using a checker model [14]. E-business maturity is a combination of various business processes that involve business structure and activity management, which utilize technology to improve services and convenience in transactions [15]. Security issues become a challenge for electronic transactions involving online communication, so a system that can protect against attacks or misuse of data is needed, as a result of business process complex problems and information exchange vulnerabilities, so a security model with cryptographic techniques is developed [16]. An e-business system is said to be good if it can accommodate all business processes, and meet the information needs of its users [17], share information about products and can directly conduct transactions.

Encryption in cryptography is a process of encoding information that refers to the security of computer-based information content. The digital signature authentication system uses the concept of asymmetric key cryptography, implementing hash functions to ensure document authenticity and integrity. Factors affecting the insecurity of information exchange can arise due to, inexperienced users, weak passwords, or improperly configured security settings [18]. Transaction security in e-business is carried out based on the sequence of activities. Security facilities for selling products and improving services can assist in providing references for information improvement. Two common methods are used to secure and protect the information, namely cryptography and steganography. Information security is very important because it supports the performance of e-business systems, in improving services to customers [19]. Cryptography is a technique of making messages or information secret and can only be accessed by authorized users through an encryption process using a mathematical model to recover secret keys from cryptographic devices [20]. This study aims to improve security in the e-business system for rice milling small and medium-sized enterprises (SMEs) by implementing cryptographic algorithms, which can strengthen passwords on user accounts and hide the exchange of transaction information. Digital transaction security transmitted over computer networks can be secured, using cryptographic techniques, which combine symmetric and asymmetric keys, so that only authorized users can access and view confidential data information, by implementing a hybrid algorithm for message encoding [21]. The proposed hybrid algorithm uses a combination of simple symmetric algorithms and the use of public and private keys by applying the Rivest Shamir Adleman (RSA) algorithm.

2. PROPOSED HYBRID ALGORITHM

Cryptographic techniques are the process of encrypting confidential or private information to maintain the confidentiality of messages, except for authorized users. There are two important components in the data encryption process, namely algorithms and keys. Algorithms are generally published while keys are kept secret to ensure security. The application of cryptography is divided into two types of keys, namely symmetrical and asymmetrical. This study proposes a hybrid algorithm that combines the use of the symmetric key and an asymmetric key simultaneously to encrypt messages. The application of symmetric keys uses a simple symmetric algorithm, and the application of asymmetric keys uses the RSA algorithm, based on two mathematical problems, namely number factorization and modulo operations. The application of this algorithm produces two different keys but connected mathematically [22]. The key for the encryption process is known as the public key and the key used for decryption is the private key. Both are key pairs that will be used in securing messages or information [23], [24]. The steps of the hybrid algorithm are shown in Figure 1, which is described as follows;

- The plaintext is original or initial messages like human language in general.
- Encryption is the process of encoding a message plaintext into ciphertext using a specific algorithm to generate a public key, resulting in messages that have no meaning.
- Decryption is the process of translating the message encrypted (ciphertext) using a private key, thereby producing an understandable message (plaintext).
- Chipertext is a message that has been encrypted and cannot be understood by unauthorized or legitimate users.

Information security by applying a hybrid algorithm consists of two actors, namely the sender and receiver of the message. The message encoding stage begins with plaintext which is the original information that will be sent by the sender of the message, then the symmetric key encryption process is carried out using a simple symmetric algorithm, the results of symmetric key encryption are used in the asymmetric key

encryption process that applies the RSA algorithm [25], and produces a public key. Chipertext can be read by doing the decryption process using a private key and producing plaintext that is still encrypted, then the results are used in the decryption process with a symmetric key to producing the original message or plaintext. The application of the RSA algorithm consists of three main processes, namely key generation, encryption, and decryption [26].

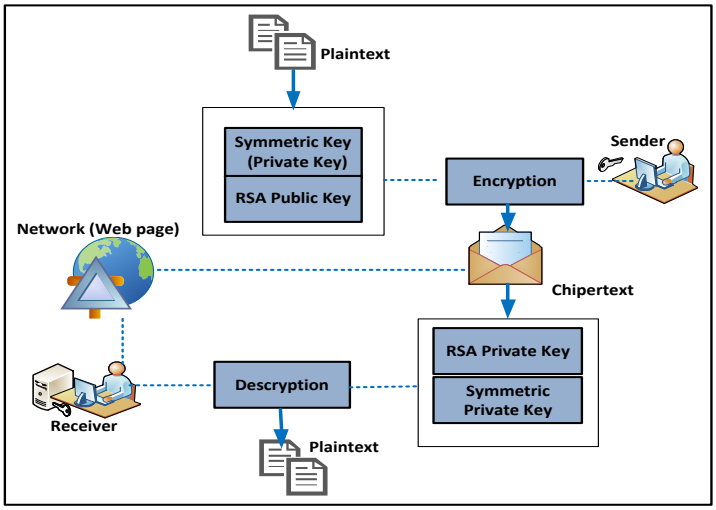

Figure 1. Block diagram of the proposed algorithm

2.1. Simple symmetric algorithm

Application of symmetric key with an encryption and decryption process using the same key [27]. Senders and recipients of messages use the same key model to be able to access information [28]. Symmetric algorithms are most commonly used because they can be combined with other algorithms to increase security, have good hardware and software performance, efficiency, and flexibility [29]. Symmetric key modeling according to alphabetic letters from A to Z, and numeric from 0 to 9, by providing integer initialization for each alphabet and numeric, such as A=1, B=2…., 9=36. Meanwhile, spaces are initialized with the integer 37.

– Encryption technique
a. Make a simple integer initialization for each letter of the alphabet and numeric, assuming I
b. Choose an integer randomly assume it is n
c. Find the value n^{-1} using the mod 37 operation, assume it is k
d. Choose a negative number as a safeguard, assume n_a
e. Find the value of n_a^{-1} using mod 37, assume it is k_1
– Decryption technique
a. The assignment of a value in the form of an integer according to the initialization for each letter in the ciphertext, assume it is I
b. Multiply the value I by the random value selected in the encryption process o get the values of k and k_1
c. Calculate using the 37 modulo operation
d. Find the plaintext with P=(I*k*k1) mod 37

2.2. Application of asymmetric keys using the RSA algorithm

RSA algorithm has a working concept that is factoring two large integers so that it becomes a problem that is difficult and challenging, but the encryption strength lies in the key length, if we add the length or size of the key is the encryption level will also increase gradually [30]. The main use of the RSA algorithm because it is the most secure key exchange mechanism [31], the appropriate domain for the implementation of this algorithm is to secure digital key transport signatures [32]. The stages of the RSA algorithm is described as follows [33].

– Procedure for generating keys
a. Choose two large prime numbers at random p and q, the condition p≠q.
b. Calculate the value of n=p×q.
c. Calculate m=(p-1)(q-1).
d. Select an integer e such that 1<e<m

e. Calculate d to satisfy the congruence relationship d×e=1 mod m; d is stored as a private key
f. The public key is (e, n) and the private key is (n, d).
g. Keep all d, p, q and m values confidential.
– Encryption process, if plaintext P <n, then ciphertext C=P ^{e}mod n.
– The decryption process produces Plaintext: P=C ^{d} mod n

2.3. Hybrid algorithm

The application of a hybrid algorithm is based on the concept of working two key types namely symmetric and asymmetric keys. This algorithm combines the two keys simultaneously on message encryption and decryption process, the merger of two key reasons, in order to improve the security message with the modified algorithm. Several previous studies have implemented several algorithm modifications [34] to improve the security of information exchange using cryptographic techniques. The proposed algorithm works:

– Encryption process

Encoding the original message is called "plaintext", done in the following steps;

a. Plaintext encryption uses a symmetric key, the encryption technique applies a simple symmetric algorithm, with work steps as shown in sub-chapter 2.1.
b. Generating public and private keys for asymmetric keys using the RSA algorithm.
c. The encryption result in point (a) is used as plaintext in the next encryption process by applying the RSA algorithm using a public key, the work steps are shown in sub-chapter 2.2. This process will produce ciphertext.

– Decryption process

a. The translation of ciphertext messages begins with applying an asymmetric key, namely, decryption using the RSA algorithm with a private key, the work steps can be seen in sub-chapter 2.2. The results of the decryption process will produce plaintext that will be used in the next process.
b. Decryption with a symmetric key using a simple symmetric algorithm, the process of translating the message from point (a) with the symmetric private key, which produces plaintext or the original message.

3. RESULTS AND ANALYSIS

3.1. Selection of integer value for plaintext initialization

Implementation of a symmetric key algorithm begins by selecting an integer for each letter of the alphabet and numeric. Determining the value of the integer will be used in the encryption and decryption process by applying the symmetric key. The initialization stages of integer values for alphabetic letters start from A to Z, with integer values ranging from 1 to 26. An example of its application is shown in Table 1. Table 2, it shows the results of selecting integer values for numeric values starting from 0 to 9 and one for the space character. This stage will be used in the next process, namely the encryption and decryption process using a symmetric key.

Table 1. Determination of the integer value for the alphabet (string)

	Plaintext												
String	A	B	C	D	E	F	G	H	I	J	K	L	M
Integer	1	2	3	4	5	6	7	8	9	10	11	12	13
String	N	0	P	Q	R	S	T	U	V	W	X	Y	Z
Integer	14	15	16	17	18	19	20	21	22	23	24	25	26

Table 2. Determination of integer values for numerics

	Plaintext										
Numeric	0	1	2	3	4	5	6	7	8	9	Space
Integer	27	28	29	30	31	32	33	34	35	36	37

3.2. Plaintext for testing samples

The message used as a sample for the implementation of cryptography in e-business systems combines two types of keys, namely symmetric and asymmetric. For symmetric keys using simple keys while asymmetric keys apply the RSA algorithm. Trial sample text message security using "SIMPLE" shown in Table 3. The process of encrypting messages sent by the sender begins by determining the integer value for the sample message to be used based on the references from Table 1. The next step is to create a simple symmetric key and an asymmetric key using the RSA algorithm.

Table 3. Sample messages for the application of the hybrid algorithm

	Plaintext					
String	S	I	M	P	L	E
Integer	19	9	13	16	12	5

3.3. Preparation of simple symmetric key

The steps to generate this key are described in the following steps:

- Choose a random integer, assume n=5.
- Find the inverse of n by applying the mod 37 operation, so that n-1=15 is obtained, verify the inverse result by multiplying two numbers, then mod 37. (5x15 mod 37=1), then the first key (k)=15.
- Again choosing a random negative number, assume na=-3.
- Find the inverse of na=-3 with mod 37 operation, get the value of na-1=12, verify (-3x12 mod 37=1), then the second key k1=12.

Result of the encryption process using simple symmetric key algorithms are shown in Table 4.

Table 4. Encryption using symmetric key algorithm

Plaintext	Integer (I)	C_1= (I*n) mod 37	C_2 = (C_1*n_1) mod 37	Chipertext
S	19	21	11	K
I	9	8	13	M
M	13	28	27	0
P	16	6	19	S
L	12	23	5	E
E	5	25	36	9

3.4. Generate keys RSA algorithm

- Choose a prime number p=5 and q=11, p≠q terms.
- Calculating the value of n=(5x11=55)
- Calculate the value of m=(5-1)x(11-1)=40
- Choose the integer e=3 condition 1 <e <m
- Compute d to satisfy the congruence relationship 3×27=1 mod 40; so that the value of d=27, make it a private key
- Determination of the public key, namely e, n=(3, 55) and the private key, namely n, d=(55, 27).

The results of the encryption key application using the RSA algorithm are shown in Table 5.

Table 5. Results of the RSA encryption algorithm

Chipertext Symmetric Key	Integer (P)	C= P^3mod 55	Chipertext
K	11	$(11)^3$ mod 55	11
M	13	$(13)^3$ mod 55	52
0	27	$(27)^3$ mod 55	48
S	19	$(19)^3$ mod 55	39
E	5	$(5)^3$ mod 55	15
9	36	$(36)^3$ mod 55	16

3.5. Encryption using the RSA algorithm

RSA algorithm encryption process based on the key that has been created, namely: C=P ᵉmod n, based on the previous stages is known the value of e=3, and n=55. The message is used for encryption using symmetric key encryption results in Table 4. Results of the RSA encryption algorithm, shown in Table 5.

3.6. Hybrid algorithm decryption

The decryption process using a hybrid algorithm is carried out by translating a sample message, namely "KM0SE9", by combining the RSA and symmetric algorithms, so that a plaintext message can be obtained that can be accessed by the recipient. The working steps of the hybrid algorithm to carry out the decryption process are described as follows;

3.6.1. Decryption using RSA

Encryption results of the message sample "KM0SE9" in Table 5, are used for the description process by applying the RSA algorithm. The steps taken to produce the translation of the decrypted message

are using the equation $P=C^d$ mod n. Results of message decryption using RSA are shown in Table 6, assuming the values of d=27 and n=55.

Table 6. Results of the RSA decryption algorithm

Chipertext RSA Algorithm (C)	$P = C^{27}$ mod 55.	Integer (decryption)	Plaintext RSA Algorithm
11	$(11)^{27}$ mod 55	11	K
52	$(52)^{27}$ mod 55	13	M
48	$(48)^{27}$ mod 55	27	0
39	$(39)^{27}$ mod 55	19	S
15	$(15)^{27}$ mod 55	5	E
16	$(16)^{27}$ mod 55	36	9

3.6.2. Symmetric algorithm decryption

The final stage for translating the message is done by a decryption process using a symmetric key algorithm. In the previous process, it was known that the values of k=15 and k_1=12, so that to translate the ciphertext into the original message "plaintext" P=(I*k*k1) mod 37, I is the decrypted plaintext using the RSA algorith. Results of the description process using the symmetric algorithm shown in Table 7, is the last stage of the application of a hybrid algorithm that combines the RSA and symmetric algorithms, so that the original or original plaintext message is obtained.

Table 7. Symmetric key algorithm encryption results

Chipertext RSA	Integer (I)	$P = (I*k*k_1)$ mod 37	P	Plaintext
K	11	(11*15*12) mod 37	19	S
M	13	(13*15*12) mod 37	9	I
0	27	(27*15*12) mod 37	13	M
S	19	(19*15*12) mod 37	16	P
E	5	(5*15*12) mod 37	12	L
9	36	(36*15*12) mod 37	5	E

3.7. Analysis of experiment results

Testing the results of the encryption using an example of the message "SIMPLE", by performing a simulation using Matlab, shows that the message security technique using cryptography uses a hybrid algorithm. Based on the experiment, it shows that the time needed to encrypt and decrypt messages is longer for a hybrid algorithm, compared to implementing one algorithm. In the implementation of cryptography, an important issue of concern is the file size or the number of strings and the time it takes to complete the encryption and decryption process which affects system performance and directly shows the complexity of each algorithm that has different work steps [35]. The hybrid algorithm has a stronger level of security because to translate messages or information one must perform a decryption process using two types of keys at once. Table 8 shows the comparison of the test results based on time (millisecond).

Table 8. Comparison of algorithmic performance based on time

Algorithm	Number of Strings	Encryption Time (millisecond)	Decryption Time (millisecond)
Simple Symmetric Key	300	1501	1550
	600	2050	2136
	900	3751	3970
	1200	4089	4172
	1500	4870	4997
RSA	300	2087	2245
	600	2506	2897
	900	3998	4184
	1200	4561	4830
	1500	5072	5239
Hybrid (Simple Symmetric & RSA)	300	2456	3053
	600	4654	5410
	900	6342	7521
	1200	8569	9064
	1500	9350	10043

Experiments in Table 8, using samples of different numbers of strings, show that the running time required for the decryption process is longer than the encryption process. The application of the hybrid

algorithm requires high running time, due to the weaknesses of the RSA algorithm which has a working concept of finding the multiplication factor of two large prime numbers [36]. Another factor is the application of two types of keys simultaneously for both the encryption and decryption processes, resulting in the greater complexity of the hybrid algorithm. The problem of running time can be overcome, by combining the symmetric key with other suitable algorithms, including the encryption technique using the advanced encryption standard (AES) method which can be considered in terms of saving the time needed for the decryption process [37].

4. CONCLUSION

The convenience of transacting and exchanging information in an e-business system can be supported by information security guarantees that apply cryptographic techniques. The application of the proposed hybrid method can improve the security of messages or information through the encryption process by combining two types of keys, namely symmetric and asymmetric keys, but in implementation, the time for the decryption process is longer than encryption. The main cause of the high running time during the decryption process is due to factors in the multiplication of two large prime numbers, the work step of the RSA algorithm.

ACKNOWLEDGEMENTS

Acknowledgments author to convey to Ministry of Research and Technology/National Research and Innovation Agency (RISTEK/BRIN) Republic of Indonesia who has supported financially the implementation of the study under the SP DIPA-042.06.1.401516/2020 and research grant contract 119.11/UN52.8/LT/2020.

REFERENCES

[1] L. Sumaryanti, L. Lamalewa, and T. Istanto, "Implementation of Fuzzy Multiple Criteria Decision Making for Recommendation Paddy Fertilizer," *Int. J. Mech. Eng. Technol.*, vol. 10, no. 3, pp. 236-243, 2019.

[2] L. Sumaryanti, T. K. Rahayu, A. Prayitno, and Salju, "Comparison Study of SMART and AHP Method for Paddy Fertilizer Recommendation in Decision Support System," in *IOP Conference Series: Earth and Environmental Science*, 2019, pp. 1-5, doi: 10.1088/1755-1315/343/1/012207.

[3] C. T. Sheung, "E-Business; The New Strategies Ande-Business Ethics, that Leads Organizations to Success," *Glob. J. Manag. Bus. Res. A Adm. Manag.*, vol. 14, no. 8, pp. 8-14, 2014.

[4] R. Čiarnienė and G. Stankevičiūtė, "Theoretical Framework of E-Business Competitiveness," *Procedia Soc. Behav. Sci.*, vol. 213, pp. 734-739, 2015, doi: 10.1016/j.sbspro.2015.11.528.

[5] B. Rondović, T. Djuričković, and L. Kašćelan, "Drivers of e-business diffusion in tourism: A decision tree approach," *J. Theor. Appl. Electron. Commer. Res.*, vol. 14, no. 1, pp. 30-50, 2019, doi: 10.4067/S0718-18762019000100104.

[6] S. M. Sheikh and M. Basti, "Customer Satisfaction in Business to Consumer (B2C) E-commerce: A Comparative Study of Turkey and Pakistan," *Eurasian J. Bus. Econ.*, vol. 8, no. 16, pp. 73-100, 2015, doi: 10.17015/ejbe.2015.016.05.

[7] R. Tamilarasi and N. Elamathi, "E-Commerce Business Technology Society," *Int. J. Eng. Technol. Manag. Res.*, vol. 4, pp. 33-41, 2017, doi : 10.5281/zenodo.1042456.

[8] D. P., S. S. Babu, and Y. Vijayalakshmi, "Enhancement of e-commerce security through asymmetric key algorithm," *Comput. Commun.*, vol. 153, no. May 2019, pp. 125-134, 2020, doi: 10.1016/j.comcom.2020.01.033.

[9] A. H. M. Sobihah, A. M. B. M. Salleh Embat, W. A. A. B. W. Mohd Amin, and M. S. Muda, "The Relationship between E-Commerce Adoption and Organization Performance," *Int. J. Bus. Manag.*, vol. 9, no. 1, pp. 56-62, 2013, doi: 10.5539/ijbm.v9n1p56.

[10] Z. H. A. Almtiri and S. J. Miah, "Impact of E-Commence Technology Adoption in Dubai SMEs," *Conference: IEEE CSDE ConferenceAt: Melbourne, Australia*, 2020, pp. 1-8, doi: 10.1109/CSDE48274.2019.9162358.

[11] M. I. Setiawan *et al.*, "E-Business, Airport Development and Its Impact on the Increasing of Information of Communication Development in Indonesia," *J. Phys. Conf. Ser.*, vol. 1007, no. 1, 2018, doi: 10.1088/1742-6596/1007/1/012046.

[12] Y. Li and J. Li, "Risk Management of E-commerce Security in Cloud Computing Environment," *Proc. - 2020 12th Int. Conf. Meas. Technol. Mechatronics Autom. ICMTMA 2020*, 2020, pp. 787-790, doi: 10.1109/ICMTMA50254.2020.00172.

[13] R. Suwandi, S. M. Nasution, and F. Azmi, "Secure E-voting sSystem by Utilizing Homomorphic Properties of The Encryption Algorithm," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 16, no. 2, pp. 862-867, 2018, doi: 10.12928/TELKOMNIKA.v16i2.8420.

[14] N. Argyropoulos, H. Mouratidis, and A. Fish, "Attribute-based security verification of business process models," *Proc. - 2017 IEEE 19th Conf. Bus. Informatics, CBI 2017*, vol. 1, 2017, pp. 43-52, doi: 10.1109/CBI.2017.37.

[15] R. I. Fady, "Evaluate the e-business maturity of the port of Alexandria," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 2013, pp. 3888-3899, doi: 10.1109/HICSS.2013.207.
[16] H. Liao, L. Li, J. Xuan and H. Wang, "Application of Cryptographic Technology Based on Certificateless System in Electricity Internet of Things," in *International Conference on Advanced Electronic Materials, Computer and Software Engineering (AEMCSE)*, 2020, pp. 417-423, doi: 10.1109/AEMCSE50948.2020.00097.
[17] Z. Ming, H. Lv, A. Xu, and H. Yang, "Exploring Computer Information Security Technology and Protection Methods," in *Proceedings-2019 International Conference on Communications, Information System, and Computer Engineering, CISCE 2019*, 2019, pp. 425-427, doi: 10.1109/CISCE.2019.00100.
[18] H. Teymourlouei and V. Harris, "Effective Methods to Monitor IT Infrastructure Security for Small Business," in *Conference on Computational Science and Computational Intelligence, CSCI 2019*, 2019, pp. 7-13, doi: 10.1109/CSCI49370.2019.00009.
[19] C. A. Sari, G. Ardiansyah, D. R. I. Moses Setiadi, and E. H. Rachmawanto, "An Improved Security and Message Capacity using AES and Huffman Coding on Image Steganography," *TELKOMNIKA Telecommunication, Computing, Electronics and Control,* vol. 17, no. 5, pp. 2400-2409, 2019, doi: 10.12928/TELKOMNIKA.v17i5.9570.
[20] S. D. Putra, M. Yudhiprawira, S. Sutikno, Y. Kurniawan, and A. S. Ahmad, "Power Analysis Attack Against Encryption devices: A Comprehensive Analysis of AES, DES, and BC3," *TELKOMNIKA Telecommunication, Computing, Electronics and Control,* vol. 17, no. 3, pp. 1282-1289, 2019, doi: 10.12928/TELKOMNIKA.V17I3.9384.
[21] A. Abid, M. Alabaichi, A. Abbas and S., "Dual Method Cryptography Image by 2FS and Steganography Secret Message in Internet of Things (IoT)," *TELKOMNIKA Telecommunication, Computing, Electronics and Control,* vol. 18, no. 1, pp. 2928-2938, 2020, doi: 10.12928/TELKOMNIKA.v18i6.15847.
[22] S. Zaineldeen and A. Ate, "Improve the Security of Transfer Data File on the Cloud by Executing Hybrid Encryption Algorithms," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 20, no. 1, pp. 521-527, 2020, doi: 10.11591/ijeecs.v20.i1.pp521-527.
[23] K. Vasavi and Y. M. Latha, "RSA cryptography based multi-modal biometric identification system for high-security application," *Int. J. Intell. Eng. Syst.*, vol. 12, no. 1, pp. 10-21, 2019, doi: 10.22266/IJIES2019.0228.02.
[24] I. Jahan, M. Asif, and L. Jude Rozario, "Improved RSA Cryptosystem Based on The Study of Number Theory and Public Key Cryptosystems," *Am. J. Eng. Res.*, vol. 4, no. 1, pp. 2320-847, 2015.
[25] N. Tahat, A. A. Tahat, M. Abu-dalu, and R. B. Albadarneh, "A New RSA Public Key Encryption Scheme With Chaotic Maps," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 2, pp. 1430-1437, 2020, doi: 10.11591/ijece.v10i2.pp1430-1437.
[26] J. Mazarire and C. Kwenda, "Hybrid Algorithm for E-commerce Applications," *Int. J. Res. IT Manag.*, vol. 6, no. 1, pp. 40-48, 2016.
[27] N. A. Kako, H. T. Sadeeq, and A. R. Abrahim, "New Symmetric Key Cipher Capable of Digraph to Single Letter Conversion Utilizing Binary System," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 18, no. 2, pp. 1028-1034, 2020, doi: 10.11591/ijeecs.v18.i2.pp1028-1034.
[28] C. Science, A. Info, S. R. M. Zeebaree, and I. Technology, "DES Encryption and Decryption Algorithm Implementation Based on FPGA," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 18, no. 2, pp. 774-781, 2020, doi: 10.11591/ijeecs.v18.i2.pp774-781.
[29] H. V. Gamido, A. M. Sison, and R. P. Medina, "Modified AES for Text and Image Encryption," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 11, no. 3, pp. 942-948, 2018, doi: 10.11591/ ijeecs.v11.i3.pp942-948.
[30] P. S. Sankaran and V. B. Kirubanand, "Hybrid cryptography security in public cloud using TwoFish and ECC algorithm," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 4, pp. 2578-2584, 2019, doi: 10.11591/ijece.v9i4.pp2578-2584.
[31] B. Muruganantham, P. Shamili, S. G. Kumar, and A. Murugan, "Quantum Cryptography for Secured Communication Networks," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, pp. 407-414, 2020, doi: 10.11591/ijece.v10i1.pp407-414.
[32] K. Suresh, P. P. Reddy, and P. Preethi, "A Novel Key Exchange Algorithm for Security in Internet of Things," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 16, no. 3, pp. 1515-1520, 2019, doi: 10.11591/ijeecs.v16.i3.pp1515-1520.
[33] J. I. Ahmad, R. Din, M. Ahmad, and J. I. Ahmad, "Analysis Review on Public Key Cryptography Algorithms," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 12, no. 2, pp. 447-454, 2018, doi: 10.11591/ijeecs.v12.i2.pp447-454.
[34] A. E. Omolara and A. Jantan, "Modified Honey Encryption Scheme for Encoding Natural Language Message," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 3, pp. 1871-1878, 2019, doi: 10.11591/ijece.v9i3.pp1871-1878.
[35] B. T. Hammad, A. M. Sagheer, I. T. Ahmed, and N. Jamil, "A Comparative Review on Symmetric and Asymmetric DNA-Based Cryptography," *Bull. Electr. Eng. Informatics*, vol. 9, no. 6, pp. 2484-2491, 2020, doi: 10.11591/eei.v9i6.2470.
[36] F. Q. A. Al-yousuf and R. Din, "Review on Secured Data Capabilities of Cryptography, Steganography and Watermarking Domain," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 17, no. 2, pp. 1053-1059, 2020, doi: 10.11591/ijeecs.v17.i2.pp1053-1059.
[37] A. Y. U. Pyrkova and Z. H. E. Temirbekova, "Compare Encryption Performance Across Devices to Ensure The Security of The IoT," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 20, no. 2, pp. 894-902, 2020, doi: 10.11591/ijeecs.v20.i2.pp 894-902.

BIOGRAPHIES OF AUTHORS

Lilik Sumaryanti, S. Kom., M.Cs obtained her M.Cs in 2015 from the department Computer Science Gadjah Mada University. Her M.Cs research in image processing and neural network. Currently, she is a senior lecturer in the department of informatics at Musamus University. Her research interest includes artificial intelligence, expert system, digital image processing, decision support system, cryptography, and stenography.

Dedy Hidayat Kusuma, S.T., M.Cs , obtained his Master of computer science in 2015 from Universitas Gadjah Mada. Curently he assistant professor in departement of information technology Politeknik Negeri Banyuwangi. His research interest are in, machine learning, and expert system.

Rosmala Widijastuti, S.P., MP, obtained her M.P in 2015 from Hasanudin University. Currently, she is a lecturer in the department of agrotechnology at Musamus University and a reviewer in the Agricola journal. Her research interest includes agricultural systems technology, rice cultivation, agricultural product development.

Muhammad Najibulloh Muzaki, S.Kom., M.Cs. obtained his M.Cs. in 2017 from Gadjah Mada University in Intelligence System. Currently, he is a lecture in the Department of Information System at Nusantara PGRI Kediri University. His research interest include data mining, machine learning, information system