TELKOMNIKA, Vol.16, No.3, June 2018, pp. 1426~1434
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v16i3.4045

Efficient Data Security for Mobile Instant Messenger

Putra Wanda*[1], Huang J. Jie[2]
[1]School of Computer Science, Harbin University of Science and Technology, China
[1,2]University of Respati Yogyakarta, Indonesia
*Corresponding author, e-mail: wpwawan@gmail.com[1], huangjinjie163@163.com[2]

Abstract

Instant Messenger (IM) becomes one of the most popular applications in mobile technology and communication. A lot of users around the world installed it for daily activities. Current IM found security lacks both in authentication and encryption matters. Various IM growing today still not apply an efficient method in authentication and encryption process, conventional security methods and client-server architecture system have to risk too many users for attacking server such as compromising, cracking password or PINs by Unauthorized people. Common IM services lack native encryption to protect information being transmitted over the public network and still used high computation in the mobile environment, this problem needs efficient security methods. Then, in public IM also found various messages with fake users, it occurs because public IM carry out the separate system in authentication and encryption process, strong authentication need to solve this issue in messenger environment. The tremendous growth of mobile IM user needs efficient and secure communication way. This paper proposes a new efficient method for securing message both in encryption and authentication within the end-to-end model. In this research, security method proposes new algorithms based on Elliptic Curve (EC) works in Peer to Peer (P2P) architecture than a conventional client-server model. The result shows this method produces efficient time in authentication and encryption process while applying in a mobile environment. Besides, it is compatible with the mobile phone which has a limitation of computation capabilities and resources.

Keywords*: efficient, authentication, security, mobile instant messenger*

1. Introduction

Mobile internet is becoming more popular and is a revolutionary advance in digital technology. Mobile internet terminals have features of mobility and personalization different to internet terminals. With the rapid development of mobile broadband technology and services, as well as the increasing of the user, the global mobile Internet market is developing with each passing day [1]. In next-generation mobile internet (5G), communication model dubbed Device-to-device (D2D) communication is a promising technology. D2D will enhance the capacity and perform traditional cellular networks. Security issues must be considered in all types of communications, especially when it comes to wireless communication between devices [2].

The large growing of IM becomes risk target of attacking while users build communication over a public network. A lot of text-based messages transmitted on the internet with various IM applications still in plaintext mode, weakness of security concern is one of a basic problem in IM today. IM applications are being more widely used among users that created by various developers. A major concern in these applications is privacy and security. Several applications like WhatsApp, Viber, Facebook, Telegram, Line, WeChat, and Beetalk.

The services of these websites divided into two groups: subscription services in which a unique number is assigned to the user by charging him/her and free services in which user can see the received messages of some online numbers without any registration [3]. The problem of malicious activities in social networks, such as Sybil attacks and fake identities, can severely affect the social activities in which users engage while online [4] Moreover, Telegram IM is so-called the most encrypted messenger may able to reconstruct the log of the data made or received by the user [5]. Most of IM has the ability to find the online user and running text message transaction. Most IM application is easy installing on a computer or smartphone. Nowadays, the user of mobile phone prefers social presence, flow, and self-disclosure than security aspect. It will be a serious problem for their data privacy [6].

Received May 25, 2016; Revised April 20, 2018; Accepted May 8, 2018

Various IM growing today still not apply the efficient method in authentication and encryption process, conventional security methods and client-server architecture system have a risk to many users for attacking server such as compromising, cracking password or leakage of PINs. Unauthorized people may able to crack the simple passwords and build attack on it, PINs leakage issue not only in mobile devices but in wearable devices [7]. several studies have tried to solve the problems with conventional public-key cryptography (PKC) implemented to give user authentication [18], model of the ranking algorithm using a transitional Bayesian inference model [8]

But solving that issue with PKC architecture is not strong enough while implemented in a client-server model with vast users. As we know, public-key computations need large memory and long time enough, for this problem algorithm choice become a solution to alleviate computation overhead. Computational overhead is one of the main concerns for the public key model. So that in this paper we propose a method to solve the problem of computational overhead. Currently, most of IM doesn't implement an efficient method for securing data while transmitting via a public network. Therefore a novel approach needed in data security by digital signature and encryption method which have good security level, low computational, fastly encryption.

Therefore, this paper proposes a novel approach focused on the efficient method in securing message both in encryption and authentication within the end-to-end model. In this research, security method proposes new algorithms based on Elliptic Curve (EC) scheme with the specific curve. This model computed within the specific curve, with prime selected p-256 for achieving efficient computation. This model is Peer to Peer (P2P) architecture than using conventional client-server model. In this method, end-to-end authentication phase will make each of data become validated among users. Then, encryption process uses to achieve data privacy simultaneously. This is a novel approach with Curve computing concept in securing mobile communication environment

2. Related Work

Several ways to secure instant messaging based on A research in 2011, a paper proposed a secure module for the instant messaging which adds other "secure module" and apply a hash algorithm to secure the path in transceiver and routing modules. On the paper, the hash algorithm is helping secure network conversation and it will result in a private environment data transmitting along sender and receiver in IM message. While sending, the application disguises the text in the network that a process it protected toward the attackers. It will secure the system.

In this approach, a secure architecture divided into four modules; chat module, transceiver module, secure module, and a routing module. In this research, secure module applied the hash algorithm. The main function of the hash algorithm is to convert into a hash value. Purpose of encryption is to make sure unauthorized person cannot view the original data or information through the network. IM application in securing IM has developed and tested [9].

Another authentication for security method called group authentication, which authenticates all users on a line. It is particular design to support applications with group oriented. Propose a special type of authentication, called group authentication which designed for group-oriented applications. The proposed method is no longer a one-to-one type of authentication but in this approach, it is a many-to-many type of authentication. Group authentication can authenticate multiple users [10].

Besides, authentication agent needs to secure data on the internet, it like the system designed for e-Shopping. In its model, an agent creates connectivity anytime, anywhere, any-device-basis in providing the customer the specific goods. But Internet being heterogeneous and nonsecure medium; privacy, authenticity, integrity, and non-repudiation are the key requirements to addressed by such systems where face to face interaction is impossible. Most of the systems don't provide the required level of security service so that many problems exist in the systems like denying, losing, misusing, stealing double spending etc. This approach address all the security service problems to an e-shopping system using Elliptic Curve Cryptosystem (ECC) [11].

3. Mobile Security Overview

Nowadays, various methods have proposed for securing mobile internet from threats, such as by Business Diversification, Platform Diverse, Terminal Security etc. [12]. Terminal security is a problem that solved in mobile Internet and is also the most concerned by users. Mobile internet terminal securities mean includes the traditional terminal protection, mobile terminal security management, terminal access control and other [13].

IM is one of the most important applications in Mobile Internet. Based on a review of several papers, the most popular IM products: Skype Messenger, Facebook Instant Messenger, Yahoo Messenger, Google Talk Instant Messenger, eBuddy, Whatsapps instant messaging and SimpPro are still vulnerable to security violations. They allow users to transfer clear text in chat sessions that risk in IM communication, it will give an opportunity eavesdropper for changing a message. Some IM application still sends the message to sender and receiver over the internet in a plaintext. The following table will show format of the text while transmitting.

Table 1. List of Instant Message Encryption Web Based

Messenger	Text conversation over the internet	Text conversation android browser
Skype App	Encrypted Message	-
WhatsApp	Encrypted Message	-
Yahoo App	Plaintext	-
Gmail Messenger	Encrypted Message	Encrypted Message
Facebook Messenger	Plaintext	-
Google Talk	Plaintext	-

The table shows how to risk the message that sends over the internet [14]. Based on the paper, vulnerable aspect can cause a program to sniff and change the packet that sends via public networks. As we know, the main concept of security defined that s Confidentiality: How an information still in secrecy while transmitting over a network. Authentication will ensure that the people using the application which sending a message are the authorized users of that system. Then, Non-Repudiation systems able to ensures that neither sender nor the receiver can deny communication while they exchange a message [15].

4. Our Approach

There are possibilities of making the algorithm more efficient and secure in a public-key cryptosystem. Elliptic Curve Cryptography has become one of the latest trends in the field of public-key cryptography. EC Cryptography promises a faster and more secure method of encryption compared to any other standard public-key cryptosystem. Elliptic curve widely used in security, various aspect successfully applied this algorithm for achieving high-level security such as internet protocol, image processing until securing service for Session Initiation Protocol [16].

One of the methods which used to authenticate message while transmitting via the public internet is Digital Signature. It can use to help authenticate the HTML script, message text etc. Digital signatures can help build secure and efficient internet application. Wider adoption of digital signatures would be possible to make the method for securing IM message while running a chat in a session efficiently [17].

4.1. Security model

While many methods have proposed in client-server communication architecture, in this paper, we use two schemas for securing IM data in Peer to Peer architecture, authentication, and cryptography process. Authentication ensures that the people using the application which sent a message to authorized people [15]. Cryptography use to create a random text for avoiding unauthorized people compromise data while transmitting over the internet.

This study will use Elliptic Curve concept for designing authentication and cryptography algorithm efficiently. This model, each user generates a key pair with specific algorithms before initiating a communication between them. Generating process produces private key and public key, the key is a key air which used along with a communication session. The key pair will be erased after communicating finished completely.

4.1.1. Authentic process

Each of user will own a key pair consists of a private key and public key. The private key will be saved for signing and decrypting message while public key used for verifying and encrypting the message. In the authentication process, each user sent a public key by peer to peer communication, this model may able to fasten keys transaction between them.

Authentication process will use a key pair. The key pair own private key and public key, the private key will sign the message (M) while sending a message over the internet and the public key will verify the message. In this process, generating key pair session will apply Elliptic Curve concept in that algorithm.

4.1.2. Crypto process

Crypto process is an encryption and decryption process which will use to change plaintext into ciphertext, this process will get the key pair that generated. Key pair includes a private key and public key, receiver's public key will encrypt the message (M) and receiver's private key will decrypt a ciphertext.

At the sender, for instance, Alice, the private key will sign M message and M has to add a hash function as a message digest. Combination of hash value and sign will produce Message signature (S). S as a secure message will be exchanged via the public internet. An example, Bob is M receiver. When the receiver gets M in the application, Alice's Public key will verify M message. It will use a hash function for comparing the M value. If the value is compatible, so S is a valid Message from Alice and vice-versa. This cryptography will result in communication of IM be fastly and fulfill the level of security. The proposed model illustrated in Figure 1.

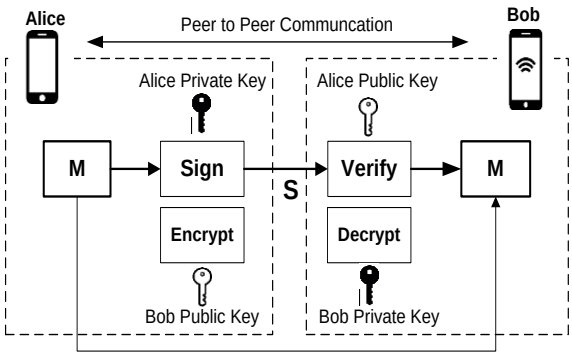

Figure 1. Efficient security model in IM communication

When Alice wants to make a chat with Bob, Alice will send a message (M). While M message sends to Bob, ECC schema will encrypt it become ciphertext and generate its signature. Bob will decrypt the ciphertext with his private key and verify the signature with the public key of Alice. Since the Bob knows Alice's public key, it can verify whether Alice sends the message indeed.

In this paper, each data exchange use key pair per session used for a session data transaction in mobile IM system. Key pair will guard user along a session information transaction after a session is finished, the system will automatically delete the key pair so that other session cannot use to sign or encrypt a message when they start another session.

4.2. Designed algorithms

In this paper, we make several algorithms to reach efficient security for data transaction in mobile IM. Two types algorithms in our model, encryption-decryption algorithm and signature algorithm. Then, when the receiver wants to read the original message, he will use decryption process. Decryption process will use the following algorithm. While sending a message, a user will sign it with ECC algorithm to give authentication. Signing process will use the following algorithm. After receiving a signature message, the receiver will verify it with public key based on ECC algorithm to check the validation of signature. Verifying process will use the following algorithm.

Algorithm 1. Encryption
Input: Message (M)
Output: Ciphertext (M')
S1: Choose public key $Q=dP$ based Elliptic Curve
S2: Choose a point of P (in Elliptic Curve)
S3: Choose a prime number p
S4: Choose a random $k \in \{2,\ldots,p-1\}$ and compute kQ dan kP.
Ciphertext: M'=[kP, M $\oplus$ X(kQ)]

Algorithm 2. Decryption
Input: Message ciphertext (M')
Output: Message plaintext (M)(r,s)
S1: Read a private key d for Elliptic Curve E
S2: Read the value of kP and compute $d(kP)$.
S3: read binary number of M_2
Decryption: M=[$M_2 \oplus$ X(d(kP))]

Algorithm 3. Signing Message
Input: Message (M)
Output: Message Signature (S)(r,s)
S1: Choose random integer k for Elliptic Curve E
S2: Choose base point P for Elliptic Curve E
S3: Compute kP
S4 : Compute $r=x_1 \bmod n$
S5 : Compute $s=k^{-1}\{h(m)+dr\} \bmod n$
Signature of M=(r,s)

Algorithm 4. Verifying signature of Message
Input: Message Signature (S)
Output: Valid or Invalid(r,s)
S1: Choose the public key Q
S2: r and s is in [1, n-1] interval
S3 : Compute $w=s^{-1} \bmod n$ dan $h(m)$.
S4: Apply a Hash (SHA-256) for M
S5 : Compute $u_1=h(m)w \bmod n$ and $u_2=rw \bmod$
S6 : Compute $u_1P+u_2Q=(x_1, y_1)$ and $v=x_1 \bmod n$.
If $v=r$ then Signature is Valid

Each of user will always run two processes when exchange messages each other. The process includes Authentic process and crypto process. The authentic process steps to sign or verify the message and crypto process is a step when user will encrypt or decrypt the message in a data exchange. To reach efficient message security in mobile IM, we use several parameters in ECC algorithm. The mobile device hasn't a good resource for running heavy computation for all security. So that, in this paper we make ECC algorithm to give good level security aspect and low-level computation overhead in a mobile device.

4. Result

This paper will show the efficient level of above algorithm to give security in mobile IM. there are three indicators that will use to test efficient level include computation time, ciphertext length and signature length. To measure the efficient levels, testing uses more specification in the android emulator with different resources. Encryption time is period for converting a plaintext into ciphertext and Decryption time is vice versa. Encryption process uses a various length of key based ECC parameters. The result of encryption and decryption show in Figure 2.

Figure 2 shows the difference of time which uses to encryption and decryption with various os key length. In this research, as more little time in running the process, as more efficient the key length. The result of this testing shows that key lengths which 224 and 256-bit size is the most effective than another size of key length.

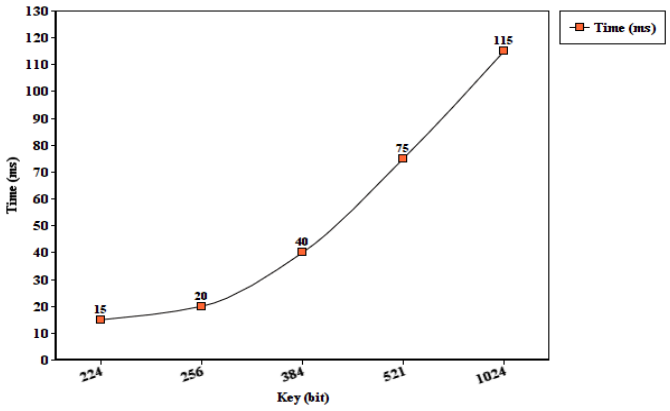

Figure 2. Encryption-decryption time based on key length

On the other hand, time of signing process uses to give a signature and verification of a message. In the testing report, this study produced different time with various of key length. Using of Elliptic Curve in this process has produced efficient time and resource computation, Elliptic Curve concept with key length 224 and 256 bit own good level of signing and verifying process. Therefore, these key size is preferable for implementing in mobile IM. Another aspect of the testing part is the signature length of the message. It is the random character of a message after hash processing finished. Signature length will affect the use of internal memory in the mobile device. The result of signature length shown in Figure 3.

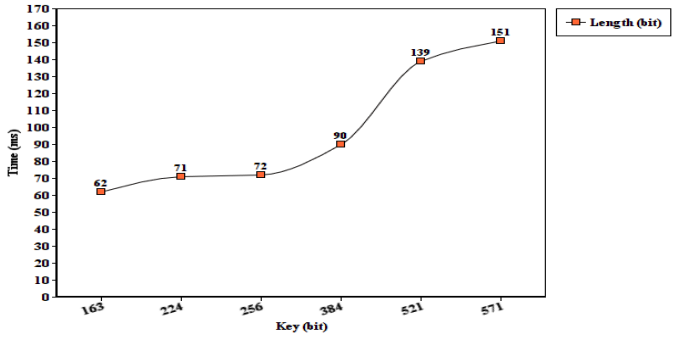

Figure 3. Length of message signature with Elliptic Curve

Figure 3 describes that the length of digital signature affected by key length used in the signing of the message. Testing result show as more key length used to sign the message, as more length of a digital signature of that message. Based on above testing, key length with 256 bit which produces 72 bit of digital signature is the most preferable in mobile IM to reach both efficient security and good strength.

6. Analysis

In this research, we propose a secure communication model with Elliptic Curve concept with both authentication message and encryption-decryption process while exchange data over the public internet. In the first step, one of the most important aspects of security called authentication where an entity should be identified before or during the communication. This avoids any type of attack or malicious activity by which a malicious user and identifies himself as the real user while communication occurs. This study use designed algorithm based on Elliptic Curve basic within formula $y^2 = x^3 + ax + b \; mod \; q$

Algorithm build based on various parameter in NIST recommendation prime curves includes p-256, $a = q - 3$ and value of $a = 3$ while q is the size of the underlying field, therefore new equation for designing algorithm with new curve (y^2):

$$y^2 = x^3 + 3x + mod \; q$$

This model computed within the above curve, with prime selected p-256 based on NIST recommendation curve [24]. This curve is used to achieve fast and secure implementations of Digital Signature for the curve P-256, providing 128-bits of security, on low-cost and low-power when testing in available hardware. The curve used to compute key generation and encryption process, generation is an important phase that generates a key pair in a communication session. The sender will be encrypting the message with receiver's public key and the receiver will decrypt the message with the private key in the same curve. This is a novel approach to securing mobile communication environment. This application runs in peer-to-peer architecture chat so that the message will be more private than client-server architecture. Then, this method will update key pair (public key and private key) of each user when they want to build a session chat in the IM environment.

6.1. Peer to peer secure chat

Security in mobile IM message will be held between sender and receiver using the designed algorithm. Peer to Peer architecture more precise and fast in IM environment, then it may able to elevate the level of data privacy for users.

In this architecture, each of session generate a key pair consist of public key and private key that used by sender and receiver, environment will delete the key pair when a communication session finished completely, the key pair will only valid for one session, when sender or receiver isn't active, the key pair will be deleted so that unauthorized people can't use the key pair. The schema avoids unauthorized people to compromise the data.

6.2. Efficient security with curve computing

In this research, using of Elliptic Curve concept for designing new algorithm in mobile IM has more advantage such as shorter key size, less computational overhead, less memory space. Based on the study, mobile devices consumed less power in running security process both in authentication and encryption process. In another hand, Elliptic Curve is known as for high-security level. it is easy to implement both in hardware and software. Since EC has enormous feature for providing security and high-efficiency application. Designing specific algorithms for mobile IM have achieved efficient computation and good security level.

This study uses a curve computing in building the security algorithm and this is a novel approach in mobile IM security. Based on our result, implementation of Elliptic Curve in mobile IM produced efficient time with using little resources in running the security process like to run encryption-decryption and to generate a digital signature. In another hand, this research uses designed algorithms that show the effective result in generating and confirm the sign so that it can cut the power in computation and it is very compatible when applying in a current mobile device that owns limit hardware resources. Many researchers put his effort to develop cryptographic algorithm and protocol based on Elliptic Curve. This feature makes ECC very popular among the many cryptographic systems.

7. Comparison Result

Various research conducted in IM security and algorithms before, those papers proposed securing data or communication architecture in IM environment. Yusof et al. proposed a secure architecture divided into four modules; chat module, transceiver module, secure module, and a routing module. In this research, secure module applied the hash algorithm. The main function of the hash algorithm is to convert into a hash value. Purpose of encryption is to make sure unauthorized person cannot view the original data or information through the network. IM application for securing IM has developed and tested for security analysis [19].

Marc et al proposed a simple security mechanism to protect Peer to Peer applications against various of vulnerabilities when transmitting over the public network. The protocol overhead tested to assess its impact on device performance, an important requisite on limited devices. This method implemented the modifications of the JXME protocols to solve the most glaring vulnerabilities, providing basic protection against simple spoofing and replay attacks in the network [20-21].

A model of work proposed a security framework based on JXTA architecture The main features of the in this work include a modular approach which may cater to set of scenarios, an effective secure key distribution and a hybrid authenticity scheme which balances the need for important information at end-user level and simplicity at the lower middleware layers. This model designed in Peer to Peer application, design focused on scalability or overall performance issues [22]. Each of study produced different overhead in computing process, overhead consist of cryptography time and overall time used in computation process. Overhead in this research formulated by:

$$Overhead = 100 \times \frac{Cryptography\ time}{Total\ Time}\%$$

Various research in securing Peer to Peer communication especially in IM environment has been conducted. Based on above formula, more different overhead in computing process shown in Table 2:

Table 2. Comparison Result in Computing Overhead

Research	Activity	Interval time (s)	Hash Size (byte)	Overhead (%)
Yusof et al.	Generate Hash	1	50	56.4 %
	(SHA)	5	250	44.5 %
Marc et al.	Generate Hash	1	50	47 %
	(JXME Protocol)	5	250	44.3 %
Joan et al.	Secure Login	1	-	51 %
	(JXTA Overlay)	5	-	46 %
This approach	Generate Hash	1	50	42.1 %
	(Elliptic Curve Computing)	5	250	38 %

Our study with designed algorithms based on Elliptic Curve concept produced more efficient result both in authentication and cryptography process. Curve Computing are possibilities of making the algorithm more efficient and secure in public-key cryptosystem and promises a faster and more secure method of encryption.

In another hand, an experiment conducted in Windows and Linux environment for analyzing Elliptic Curve Cryptosystem (ECC) as an asymmetric block cipher algorithm and a set of symmetric block cipher algorithms namely Triple-Data Encryption Standard (T-DES), Advanced Encryption Standard (AES), and Blowfish. Performance evaluation based on CPU execution time is shown in Figure 4

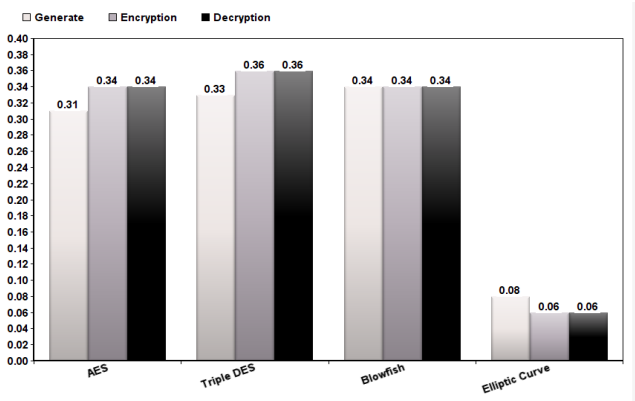

Figure 4. Performance Comparison of symmetric and asymmetric block ciphe algorithms

In this study, Elliptic Curve Cryptosystem (ECC) as an asymmetric block cipher algorithm and three symmetric block ciphers: Triple-DES, AES, and Blowfish were presented. This experiment runs in Java environment with Cryptography Architecture (JCA) and Java Cryptography Extension (JCE). Based on CPU execution time, ECC outperform the other three algorithms in all tests and under the computing environment [23].

8. Conclusion and Future Work

Common mobile IM services lack native encryption to protect information being transmitted over the public network and still used high computation, this problem should be addressed with efficient security methods. In this study, we propose an efficient method with Elliptic Curve concept. It has designed new algorithm with designed Curve for building security model in mobile IM environment. Security model based on Elliptic Curve (EC) works in Peer to Peer (P2P) architecture rather than a conventional client-server model. In this method, end-to-end authentication phase will make each of data become validated among users. Then, encryption process uses to achieve data privacy between them.

The result shows this method produces efficient time in authentication and encryption process while applying in a mobile environment. This paper recommends Elliptic Curve for using

in mobile IM security with key length 256 bit within curve $y^2 = x^3 + 3x + mod\ q$. It has produced efficient in time to each of security process include generating key, signing, verifying, encryption and decryption. Therefore, this security method suitable to mobile IM environment. Besides, EC algorithm outperform others cryptography algorithms both symmetric and asymmetric block cipher algorithms. Besides, it is compatible with a mobile phone which has the limitation of computation capabilities and resources. This research still testing in text format, so that it next time probably will use other data format. Then, to increase authentication level, it needs to add SHA-3 (Keccak) algorithm in Elliptic Curve Cryptography.

References

[1] T Sutikno, D Stiawan, IMI Subroto. Fortifying Big Data infrastructures to Face Security and Privacy Issues. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2014; 12(4): 751-752.

[2] O Nait Hamoud, T Kenaza, Y Challal. Security in device-to-device communications: a survey. in *IET Networks*, 2018; 7(1):14-22.

[3] Mehdi Dadkhah, Tole Sutikno, Shahaboddin Shamshirband, Social Network Applications and Free Online Mobile Numbers: Real Risk, *International Journal of Electrical and Computer Engineering (IJECE)*, 2015: 5(2):175-176

[4] M Al-Qurishi, M Al-Rakhami, A Alamri, M Alrubaian, SMM Rahman, MS Hossain. Sybil Defense Techniques in Online Social Networks: A Survey. in *IEEE Access*; 2017; 5:1200-1219.

[5] C. Anglano, M. Canonico, M. Guazzone, Forensic analysis of Telegram Messenger on Android smartphones, Digital Investigation, *Elsevier*; 2017; 23: 31-49,

[6] S Park, K Cho, BG Lee. What makes smartphone users satisfied with the mobile instant messenger?: Social presence, flow, and self-disclosure. *Int. J. Multimed. Ubiquitous Eng.* 2014; 9(11) :315–324.

[7] C Wang, X Guo, Y Chen, Y Wang, B Liu. Personal PIN Leakage from Wearable Devices. In *IEEE Transactions on Mobile Computing;* 2018; 17(3): 646-660.

[8] B Rashidi, C Fung, A Nguyen, T Vu, E Bertino. Android User Privacy Preserving Through Crowdsourcing. in *IEEE Transactions on Information Forensics and Security*, 2018; 13(3): 773-787.

[9] M Yusof, A Abidin. A secure private instant messenger. in Proc. 17th Ascia-Pacific Conference on Communications, 2011; 821-825.

[10] L Ham. Group Authentication. *IEEE Trans. Vehicular Technology*; 2013; 62(9).

[11] L Ham. Agent Based Secured e-Shopping Using Elliptic Curve Cryptography. International Journal of Advanced Science and Technology; 2012; 38.

[12] Y Zhu, L Yan, J Li. Mobile Internet Information Security Analysis and Countermeasures. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2016: 14(3A): 333~337

[13] Dadkhah M, Sutikno T. Phishing or hijacking? Forgers hijacked DU journal by copying content of another authenticate journal. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*. 2015; 3(3): 119-120.

[14] NB Al Barghuthi, H Said. Social networks IM forensics: Encryption analysis. *J. Commun*. 2013; 8(11): 708–715.

[15] Forouzan, A Behrouz. Cryptography and Network Security. Singapore. *Mc Graw-Hill Education (Asia)*, 2008

[16] M Azrour, M Ouanan, Y Farhaou, SIP Authentication Protocols Based on Elliptic Curve Cryptography: Survey and comparison. *Indonesian Journal of Electrical Engineering and Computer Science* 2016: 4(1): 231-239

[17] N Harigopal KB Ponnapalli, A Saxena. A Digital Signature Architecture for Web Apps. *J. ComSoc*. 2013; 13.

[18] L Harn, J Ren. Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications. *IEEE Trans. Wireless Comm*. 2011; 10(7): 2372-2379.

[19] M Yusof, A Abidin. *A secure private instant messenger*. in Proc. 17th Ascia-Pacific Conference on Communications, 2011; 821-825.

[20] M Domingo-Prieto, J. Arnedo-Moreno*. Lightweight Security for JXME-Proxied Relay Authentication*. 2011 14th International Conference on Network-Based Information Systems*,* Tirana, 2011: 104-111.

[21] M Domingo-Prieto, J Arnedo-Moreno, J Herrera-Joancomart´, J Prieto-Bl´ azquez. Towards secure mobile P2P applications using JXME. *Journal of Internet Services and Information Security (JISIS)*, 2012; 2(1):1-21

[22] J Arnedo-Moreno, K Matsuo, L Barolli, F Xhafa. Secure Communication Setup for a P2P-Based JXTA-Overlay Platform. in *IEEE Transactions on Industrial Electronics*; 2011; 58(6): 2086-2096

[23] NA Kofahim. An Empirical Study to Compare the Performance of some Symmetric and Asymmetric Ciphers. *International Journal of Security and Its Applications*. 2013;7(5):1-16.

[24] M Adalier. Efficient and Secure Elliptic Curve Cryptography Implementation of Curve P-256, National Institute of Standards and Technology (NIST) Article, 2017.