End-to-End Privacy Protection for Facebook Mobile Chat based on AES with Multi-Layered MD5

https://doi.org/10.3991/ijim.v12i1.7472

Wibisono Sukmo Wardhono(✉), Nurizal Dwi Priandani, Mahardeka Tri Ananta, Komang Candra Brata, Herman Tolle
Brawijaya University, Malang, Indonesia
wibiwardhono@ub.ac.id

Abstract—As social media environments become more interactive and amount of users grown tremendously, privacy is a matter of increasing concern. When personal data become a commodity, social media company can share users data to another party such as government. Facebook, inc is one of the social media company that frequently asked for user's data. Although this private data request mechanism through a formal and valid legal process, it still undermine the fundamental right to information privacy. In This Case, social media users need protection against privacy violation from social media platform provider itself. Private chat is the most favorite feature of a social media. Inside a chat room, user can share their private information contents. Cryptography is one of data protection methods that can be used to hides private communication data from unauthorized parties. In our study, we proposed a system that can encrypt chatting content based on AES and multi-layered MD5 to ensure social media users have privacy protection against social media company that use user informations as a commodity. In addition, this system can make users convenience to share their private information through social media platform.

Keywords—AES, MD5, Social media, Chatting, End-to-End Security.

1 Introduction

User's information privacy has been recognized as an important issue in social media era, and its impact will continue to increase as the value of information continues to grow in social media [1]. Understanding and protecting personal privacy in social media is becoming increasingly critical with widespread use of social media and the Internet. A fundamental problem at this point is while companies are thirsty for ever more information about user data, they undermine the fundamental right to information privacy by buy some social media users data from social media company like Facebook [2][3].

In defining a private situation, it is necessary to define who has access to what under which circumstances. The privacy of private chatting in Facebook represents a good example of the complexity of the restrictions that must be placed on a privacy situation. As of the third quarter of 2016, Facebook had 1.79 billion monthly active

users [4]. Chatting is one of the most favorite feature of Facebook because in a chat room, user can share their private content of information. With this massive amount of users, the demand about Facebook user data will increase linearly with the value of information itself. For many reasons and purposes, worldwide governments requested Facebook users' data up to 60,000 times in first half of 2016 [5]. By giving private users information to another parties without permission, Facebook, Inc. as a social media platform provider will be a serious threat to the Facebook user privacy.

In this paper, we present an implementation of Advanced Encryption Standard (AES) cryptography in Facebook private chatting. Encryption is a basic concept of this proposed method to obtain secure communications between Facebook end users. The chat history between end to end users will be encrypted with randomly generated key which secured with multi-layered MD5 that only corresponding users can decrypt the chat content. For next step, this encrypted content will be sent to Facebook's database.

The objective of this study is to propose a system that have privacy protection mechanism so user will be never worried about privacy violation although Facebook, inc give their users history data to another parties.

2 Related AES 128, MD5 And Mobile Chat

This section discussed related AES 128 and the relationship to our Facebook mobile chat work and also briefly summarizes related mobile chat work that our facebook mobile chat takes advantage of. Due to space limitations and the depth of the field, this is not a comprehensive survey of related work but rather it concentrates on the specifics of adapting AES 128 and analyzing our Facebook mobile chat.

2.1 AES 128

The Advanced Encryption Standard (AES) [6] specifies a cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. The implementation of AES to secure communication was proposed by Ahmad et.al [7].

2.2 MD5

The MD5 algorithm is intended for applications that serve to preserve the integrity of digital information, in which information files of a certain size must be safely compressed before being encrypted with a private key (secret) under a public key cryptosystem such as RSA [11]. In this research the algorithm was developed into Multilayer MD5 to secure the manipulation key used by AES algorithm. With the combined AES and multi-layer MD5 mechanisms implemented in this application make the decryption process only possible by users who already use the Facebook chat app.

2.3 Mobile Chat

The work in this paper is built on the idea that the facebook chat leaving a privacy concern for users. The previous work [8] built a prototype of system providing convenient, secure instant messaging within Facebook Chat, but it has focused on the usability evaluation.

To support the experimental scenarios in this paper, we takes advantage of the XO: XMPP overlay service for distributed chat [9] to utilize extensible Messaging and Presence Protocol (XMPP) standards for developing facebook mobile chat. Furthermore we complete our work to achieve the privacy protection by taking advantage of Announcing the Advanced Encryption Standart (AES) [6] work.

3 System Design

In this section, the main design and task of AES Based End-to-End Privacy Protection for Facebook Mobile Chat are explained. Chat history between end-users was encrypted with a random generated key which resulted from this manipulation key would be secured with MD5 before being sent to the Facebook server. Multi-layer MD5 was to secure the key manipulation used by the AES algorithm, since this manipulation key was the key to unlock encryption. If someone can discover the manipulation key then automatically he will be able to disassemble the AES encryption process. The multi-layer MD5 implementation of the chat apps proposed in this study had two private keys that were only owned by this application so that the chipertext can only be decrypted by the recipient's chat app. After the encryption process, the data was sent by the program to the Facebook account of the recipient user. To summarize, the major tasks of this work were: Key Generation, Encryption and Key distribution.

3.1 Key Generation

The key generation was conducted to obtain the Manipulation Key which would be distributed and the Real Keyfor encryption process purpose. The key generation process which shown in Figure 1 have these process:

a) Integer number randomization with range 10 to 99 for 16 times. In this stage, it has been obtained 16 pairs of integer which combined later and used as the Manipulation Key.
b) Splitting for every 2 digit in the Manipulation Key asan early initialization conversion each pair of integers to ASCII.
c) Summation to each pair of integer with number 27. The result of this process was converted into ASCII table.
d) The result of the process in the point C was combined into a sequence. This sequence was used as the Real Key for encryption purpose.

The randomize key generation aimed to increase the security of the encrypted message. The utilization of random number with range 10 to 99 made the key possibility became 90^{16}. It make the chat more safely and give highly protection of user privacy.

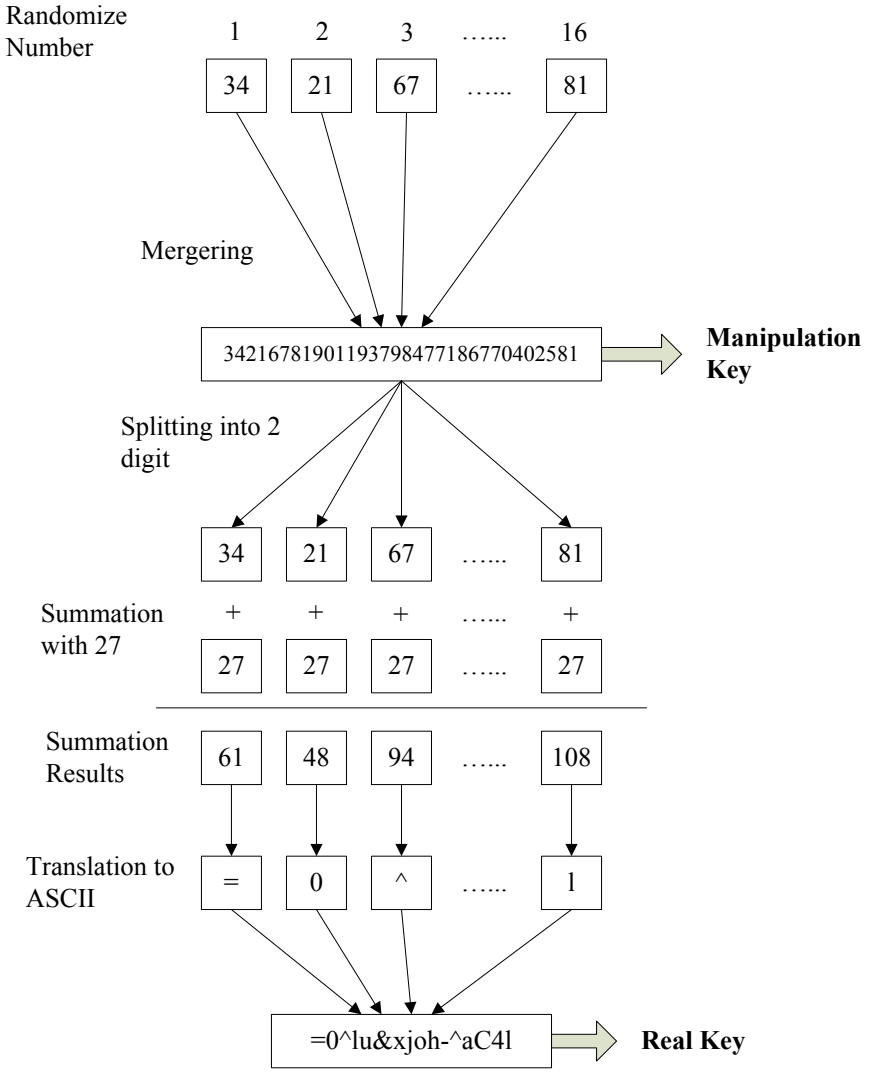


Fig. 1. Key Generation Process

3.2 Key Encryption and Distribution

Plaintext encryption process was conducted when the key generation process has been conducted. The encryption and distribution process is shown in figure 2.

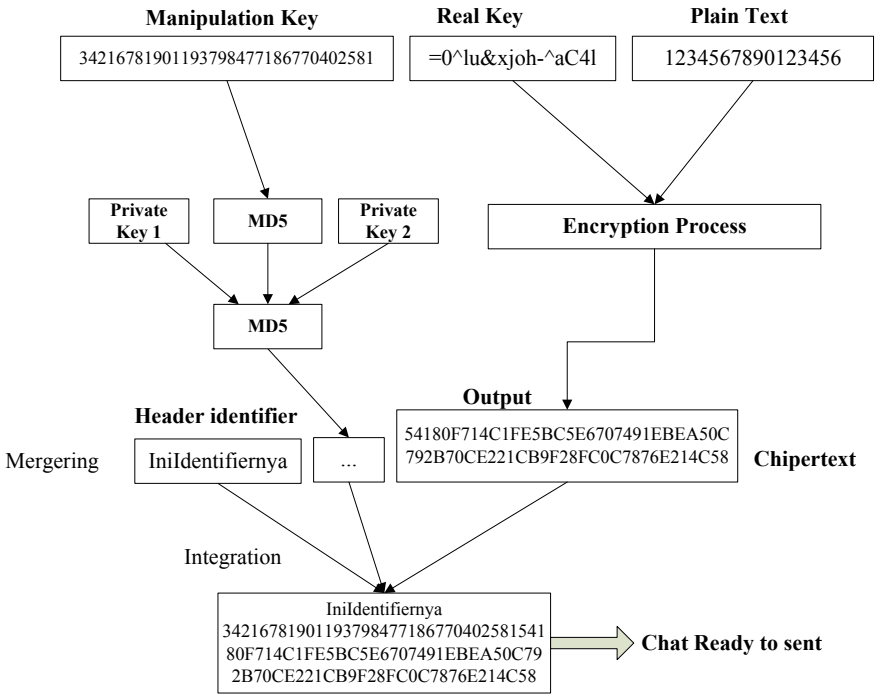


Fig. 2. Encryption and Key Distribution Process

On the receiving end, it was assumed that the user has been sent a chipertext message by the user's friend, then the user could see incoming and unread message notification. Because the message was still in the form of chipertext, the user was required to see the details of the message to read it. The Manipulation Key was encrypted with multi-layer MD5 which also included in messages required for AES decryption process. The application translated the hash results from multi-layer MD5 to get the value of manipulation key. This value was processed into the real key which then the application ran the next process, the AES decryption. The decryption process was the process which the chat received with the chipertext form was converted to plaintext with a key in order to be able read by the recipient user. With the combined AES and multi-layer MD5 mechanisms implemented in this application made the decryption process only possible by users who already use the Facebook chat application developed in this research.

4 Experiment And Discussion

In this section, we present the setup and results from experimentation. The main experimental objective was to determine the performance of our proposed method. For this task, an Android-based end-to-end privacy protection Facebook chat application prototype was created which shown in Figure 3.

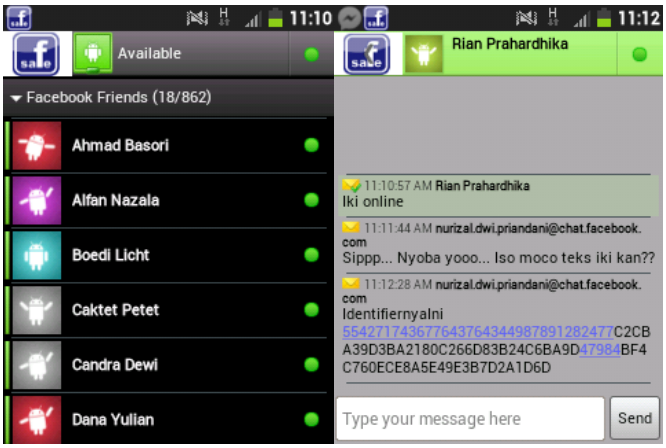


Fig. 3. Facebook chat application prototype

4.1 Experiment Setup

The testing process was performance test. The performance test was a test which aimed to understand the speed of the application to serve the user on encryption and distribution features. The application was tested by measuring the time needed to conducted the encryption and decryption process with the expansion of the character amount as the parameter. Smartphone Samsung Galaxy Young GT S5360 was used as the device for the performance test. We assumed that the device was a low specification device to made the worst case performance measurement.

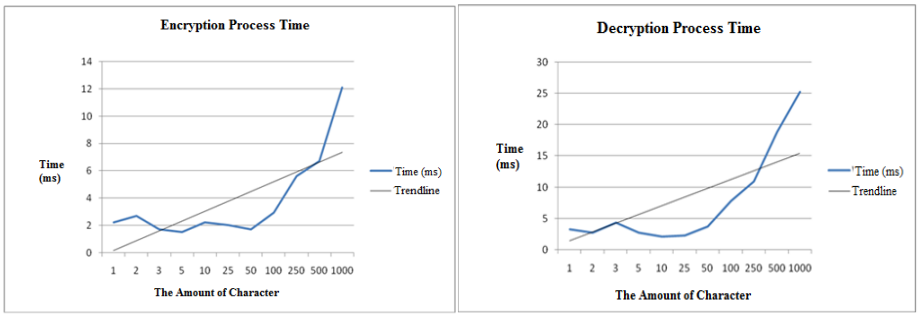
4.2 Experiment Results

The performance test was conducted with character expansion started with 1 to 1000 characters. The result of the performance test is shown in Table 1.

Table 1. Performance Test Result

Test Case Number	Character Amount	Encryption Time (ms)	Decryption Time (ms)
Perf_01	1	2.2	3.3
Perf_02	2	2.7	2.7
Perf_03	3	1.7	4.3
Perf_04	5	1.5	2.7
Perf_05	10	2.2	2.1
Perf_06	25	2	2.3
Perf_07	50	1.7	3.7
Perf_08	100	2.9	7.8
Perf_09	250	5.6	10.9
Perf_10	500	6.7	18.9
Perf_11	1000	12.1	25.3

The effect of character amount to encryption and decryption process graph below which based on the performance test result is shown in Figure 4.



(a) (b)

Fig. 4. Encryption (a) and Decryption (b) Process Time Graph

Based on the trendline in the encryption or decryption process time graph, the effect of the character amount was obtained. The more the amount of the character, the process would take a longer process. It affected the application respond which took a longer time to the user. Although there was an increase on the process time, all average times on each data were less than allowed deadline, which was 1 second or even less than 0,1 second (100 ms). Based on the user's experience on Human-Computer Interaction, 0,1 second (100 ms) deadline was a limit which user felt the action that was given to the application was responded immediately by the application [10]. Based on the performance test result, we concluded that our proposed method was able to serve the user on encryption and decryption process in a swift manner.

5 Conclusion

Based on the experiment which has been conducted, there were some results. Based on the performance experiment, there was time increase on the average time of the encryption and decryption process. The maximum time process of encryption and decryption process were 12,1 millisecond and 25,3 millisecond respectively. It can be stated that the our proposed method was able to conduct the encryption and decryption process in a swift manner which the user felt the action that given was responded quickly and immediately by the application. Based on the our randomize key generation method, the probability of key generation is 90^{16}. It make the chat more safely and give highly protection of user privacy. Security scheme on key distribution, multi-layer MD5 design has been used. It makes it easier for users to secure keys and at the same time improve security in key distributions.

6 References

[1] Earp, Julia Brande, et al. "Examining Internet privacy policies within the context of user privacy values." *IEEE Transactions on Engineering Management* 52.2 (2005): 227-237. https://doi.org/10.1109/TEM.2005.844927

[2] Raul, Alan Charles. *Privacy And The Digital State: Balancing Public Information And Personal Privacy*. Springer Science & Business Media, 2002. https://doi.org/10.1007/978-1-4615-0889-2

[3] Hachman, Mark. "The price of free: how Apple, Facebook, Microsoft and Google sell you to advertisers." (2015).

[4] Statista. 2016. *Number Of Monthly Active Facebook Users Worldwide As Of 3rd Quarter 2016 (In Millions)*. [online] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/. Last accessed on 2017 January

[5] Tom Brant. *Government Requests For Facebook Data Up 27 Percent*. Foxnews. 2016

[6] Federal Information Processing (FIPS). "*Announcing the ADVANCED ENCRYPTION STANDARD (AES)*". 2001

[7] Ahmad, Rafidah, Asrulnizam Abd Manaf, and Widad Ismail. "Implementation of a High-Performance Blowfish for Secure Wireless Communication." *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)* 8.6 (2016): 147-151.

[8] Robison, Chris, et al. "Private Facebook Chat." *International Conference on Privacy, Security, Risk and Trust (PASSAT), and 2012 International Confernece on Social Computing (SocialCom)*. IEEE, 2012. https://doi.org/10.1109/SocialCom-PASSAT.2012.58

[9] Robert, N. Lass, et al. "XO: XMPP overlay service for distributed chat." *MILITARY COMMUNICATIONS CONFERENCE 2010*. IEEE, 2010.

[10] Nielsen, Jakob. 2009. *Powers of 10: Time Scales in User Experience*. [online] http://www.nngroup.com/articles/powers-of-10-time-scales-in-ux/, Last accessed on 2017 January

[11] Samsudin A., et. al., 2015. J S Teh, A Samsudin, A. Akhavan, "Parallel chaotic hash function based on the shuffle-exchange network[J]", Nonlinear Dynamics, vol. 81, no. 3, pp. 1067-1079, 2015. https://doi.org/10.1007/s11071-015-2049-6

7 Authors

Wibisono Sukmo Wardhono is with the Multimedia, Game and Mobile Technology Research Group, Department of Computer Science, Faculty of Computer Science, Brawijaya University, Malang – East Java, Indonesia.

Nurizal Dwi Priandani is with the Multimedia, Game and Mobile Technology Research Group, Department of Computer Science, Faculty of Computer Science, Brawijaya University, Malang – East Java, Indonesia.

Herman Tolle is with the Multimedia, Game and Mobile Technology Research Group, Department of Computer Science, Faculty of Computer Science, Brawijaya University, Malang – East Java, Indonesia.

Mahardeka Tri Ananta is with the Multimedia, Game and Mobile Technology Research Group, Department of Computer Science, Faculty of Computer Science, Brawijaya University, Malang – East Java, Indonesia.

Komang Candra Brata is with the Multimedia, Game and Mobile Technology Research Group, Department of Computer Science, Faculty of Computer Science, Brawijaya University, Malang – East Java, Indonesia.

Article submitted 25 July 2017. Published as resubmitted by the authors 13 September 2017.