EMITTER International Journal of Engineering Technology
ISSN: 2443-1168, Vol. 8, No. 1, June 2020, pp. 102~125
DOI : 10.24003/emitter.v8i1.486

Secure Data Travelling User using Hybrid Cryptosystem with User Privacy Protection

Anindya Dwi Putri Islamidina, Amang Sudarsono, Titon Dutono

Electrical Engineering Department, Politeknik Elektronika Negeri Surabaya
E-mail: anindyaislamidina@gmail.com, {amang, titon}@pens.ac.id

Received March 23, 2020; Revised April 16, 2020; Accepted May 9, 2020

Abstract

Nowadays traveling is the activity that everyone likes the most, but sometimes there is one traveling member who is lost and confused looking for the location of the other members. When traveling, they must bring a smartphone because of its small size and easy to carry anywhere. For this reason, an Android-based smartphone application that is able to send GPS data to all travelling members is proposed. In order to secure data transmission, cryptography and group signature to ensure that only traveling members could find out the location are applied. We use hybrid cryptography, which is a combination of symmetric cryptography using AES and asymmetric cryptography using IB-mRSA. We also add group signature as verification that members are in the same traveling group. The test result showed that the proposed method is safer than the comparison method because the symmetric key is encrypted before the key is distributed, so the attacker can not know the key. The total processing time needed to send data until member get data is 2.01 s.

Keywords: GPS, AES, IB-mRSA, Group Signature

1. INTRODUCTION

Nowadays, traveling is one of the activities carried out by many people from young to old. Usually traveling is done in group both from group of friends who are already known and from other group who will meet at their destination. When traveling in an outdoor area with a large area sometime there is one of the members is separated from the group. When other members realize there is member who are left behind, they will be hard to find the location of these member and member who are left behind also difficult to find the location of the group. In outdoor condition, location search can be done using GPS (Global Positioning System) technology. At present, this technology can be used mobile using smartphone, while many smartphones are now equipped with GPS technology. GPS can provide position through intersections of latitude and longitude throughout the world using satellite signals [1][2]. The technology that utilizes GPS on smartphone has previously been done by

Uddin et al [3]. The research conducted is to track location using GPS on user's smartphone who are sent to the admin for data retrieval. Data sent from the user to the admin is not equipped with security, so this data is most likely to be tapped by eavesdroppers.

Data security when sending via internet media is very important so that the data is not known by eavesdroppers because nowadays data can be accessed legally or illegally. Data security can be said to be successful if it includes confidential, availability, authentication and integrity [4]-[7]. One of the methods that can be used to secure data on a network is cryptography [8] and group signature [9]. Cryptography consists of two types, namely symmetric cryptography and asymmetric cryptography. Symmetric cryptography is a data security technique where the keys used to do encryption and decryption are the same. While asymmetric cryptography is a data security technique where the key used to encrypt is different from the key used for decryption [10]. One of the asymmetric cryptography is Identity Based Mediated RSA (IB-mRSA) which was first designed by Boneh et al [11]. IB-mRSA is a combination of RSA (Rivest-Shamir-Adleman) and mediated RSA. The public key used for encryption is generated from a unique user ID such as an e-mail address or username and then encryption is done the same as encryption in the RSA algorithm. Whereas the private key for decryption is divided into two parts, one for the user and the other for Security Mediated (SEM). The decryption process uses the mRSA algorithm where this process is done in user and SEM [12]-[14]. Both parties cannot cheat each other because the decryption process involves one another. Symmetric cryptography used by Sarbpreet [15] is AES that is implemented to secure communication when tracking ambulance's position that are delivering or picking up patients. While others using symmetric cryptographic are [16]-[18].

Group signature algorithm is a digital signature carried out by one member in a group and the identity of the member is unknown to other members [19]-[23]. This algoritma involves a third trusted party authorized to add new members and can see the identity of the members who signed the information. The function of group signature is to limit data access so that only members of the same group as the signer can find out the data. Secure group signature must include properties of correctness, unforgeability, anonymity.

In this research, we propose an android-based location tracking application using GPS technology to determine member's position. In order to secure data transmission between members, we propose data encryption using hybrid cryptography, namely AES and IB-mRSA and group signature to limit data access. The AES algorithm is used for GPS data encryption while the IB-mRSA algorithm is used for AES key encryption. Key generation at AES is carried out randomly with a 256-bit key length while key generation at IB-mRSA is done based on the email address of the member after registration. In this case, the email address between members at registration must not be the same so that the key generated varies by each member. In the group signature, the key generation is carried out by the Group Manager (GM), which is a

trusted third party. GM is not only responsible for generating keys, but also as a server on our system. The server acts as a verifier of the signature sent by the member, if and only if verification is valid then the processes is continued by decrypting the encrypted data. Our research showed that the use of hybrid cryptography combined with group signature only takes 2.1 second since the member-*i* first started GPS to get the GPS location of all members. The total processing time is fast enough to be used for tracking application on walking people with the assumption that the walking speed is around 5 km/h.

This paper consists of section II explains the previous paper discussing cryptography and group signature. Section III explains the originality of this study. Section IV explains the review of security requirement, AES, IB-mRSA, group signature and the proposed method used in this study. Section V shows the research results of the proposed method with the previous paper. Finally section VI is the conclusion of this study.

2. RELATED WORKS

There are some research related to data security using algorithms in symmetric and asymmetric cryptography

A research [8] conducted a GPS location tracking study for post-stroke sufferers for the rehabilitation process that was secured using AES and QR Code. The authors use a GPS sensor that is integrated with Arduino and placed in the footwear of post-stroke sufferers. The sensor is integrated with an android application that is used for sending data by scanning a QR Code on a walking stick sufferer. After a successful QR Code scan, the data from the sensor is secured and sent to the web service to be seen by families of sufferers.

A.D.P. Islamidina et al. [14] has proposed research to secure GPS location data using asymmetric cryptography and group signatures. The asymmetric algorithm used is the RSA and the IBE scheme which is integrated with the RSA called IB-mRSA. The algorithm is different in the generation of keys, where the RSA key is generated from two random prime numbers while the IB-mRSA key can be generated from e-mail, username, telephone number or unique data from the user and the private key is divided into two that are used for that user and Security Mediated as Third Trusted Party. The advantages of the IBE scheme are the security of the private key when there is an attacker, because the private key is the key pair of user and Security Mediated

Sarbpreet et al. [15] has proposed research to secure data on ambulance tracking service in real time with IoT using the AES-CCM algorithm. The authors use a hybrid security protocol between AES and CCM or Counter with Cipher Block Chaining Message Authentication Code (CBC-MAC). The result of the study show that the security protocol can work well on devices with limited power and consumes less energy and memory and can work quickly

A research about group signature by modifying the basic group signature named ACJT was proposed by G. Ateniese et al. [22]. This scheme was obtained from the Fiat-Shamir heuristic identity escrow scheme. The results of the study show that the ACJT scheme is safer and efficient with lower computing time.

J. Camenisch et al. [23] has proposed a group signature by modifying the ACJT scheme in the join process section by reducing the join cycle and adding the revocation process. The results of the study show that CG schemes are more efficient, computational time in the join process is faster and there is full revocation.

3. ORIGINALITY

In this section, we develop a security system for GPS location data using a hybrid scheme that combines symmetric cryptography and asymmetry. The method used is the AES method for symmetric cryptography and IB-mRSA for asymmetric cryptography. In addition to using cryptography, group signature are also used to secure the user's personal data as well as user authentication. The advantage of this system is that the hybrid scheme can make GPS location data safer because the AES key is encrypted using the IB-mRSA method, so it difficult for the attacker to identify the key used. Merging cryptography with group signature also make the data more valid because of the authentication that the GPS location data that is sent is data from user in the same group. But because of the merging of this system, the computation time used become longer when compared with the use of one cryptographic technique or the use of group signature only. This method will be compared with research [15] that uses the AES-CCM algorithm to encrypt GPS location data in ambulance tracking. We also refined the research [15] by adding group signatures. We also compare with research [22] [23] which uses group signature so that signature transmissions are in the same group.

4. SYSTEM DESIGN

In this section, we discuss the security requirements, AES algorithm, the IB-mRSA algorithm and the Camenisch-Groth method for group signature and explain the proposed security system.

4.1 Security Requirements

Oracevic et al. [5] identify security requirements in sending data through internet media. Data communication through internet media has very dangerous threats such as data theft, hacking attempts, malware etc. To minimize the danger in data transmission, data security is carried out such as cryptography and group signature. Based on the consideration, we set the security requirements in the proposed system through the internet as follows:

a. Condifentiality: only authorized users can retrieve original data from encrypted data
b. Data integrity: data is not changed from the original by unauthorized persons, so that the consistency, accuracy and validity of the data is maintained.
c. Authentication: the information sent is truly original, the sender and recipient are truly persons who are authorized to access the information
d. Privacy: user traveling data is anonymous and unknown to other users.

e. Correctness : Signatures made by members using the sign procedure must be received by verifier
f. Unforgeability : Only group members can sign messages on behalf of their groups

If we compare with the method [15], on their system they only fulfill confidentiality, data integrity and authentication. But because of the use of cryptographic simetric, the distribution of symmetric key becomes unsafe because there may be the possibility of the simetric key being captured by the attacker when sending data. Whereas methods [22] and [23] that use group signature only meet the privacy, correctness and unforgeability security requirements because there is no cryptographic process. Because it only uses group signature, the data sent is not safe because the data can be seen by the attacker. In the system that we propose, with the hybrid cryptography, the distribution of the symmetric key is safer because the symmetric key is encrypted first by the IB-mRSA before sending. The addition of group signature also add to the security requirements of privacy, correctness and unforgeability.

4.2 Advanced Encryption Standard (AES)

AES is a cryptographic technique that uses the same key for the encryption and decryption process. The key length of AES consists of 128 bits, 192 bits, and 256 bits. The difference in key length will affect the number of rounds in this AES algorithm. The number of rounds used on AES-128 is 10 round, AES-192 is 12 round and AES-256 is 14 round. The encryption process requires input in the form of message and key while the decryption process requires input in the form of ciphertext and key as in equation 1 and 2 respectively

$$C = Enc\ (m, k) \tag{1}$$

$$M = Dec\ (C, k) \tag{2}$$

AES has 5 operating modes namely Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR) operating modes. Each mode of operation has its advantages and disadvantages. In this study, the authors used the CBC operating mode for the proposed method and CTR for the comparison method

4.2.1 Cipher Block Chaining (CBC) Operation Mode

CBC operation mode breaks the plaintext into several blocks and the ciphertext results in the first block affect the next block as illustrated in Figure 1

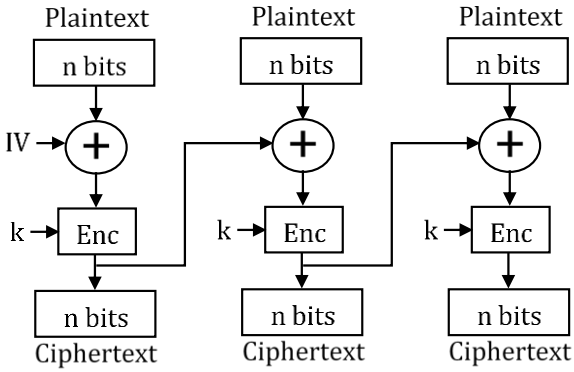


Figure 1. CBC operation mode

The first plaintext data block is XORed with Initial Vector (IV) where the value of IV is a random number. Then the result of the XOR operation is encrypted to produce the first ciphertext. The result of the ciphertext in the first block becomes input for a replacement IV in the second block. With CBC mode, if the previous block changes then the next block will also change due to dependency between the blocks

4.2.2 Counter (CTR) Operation Mode

The CTR operation mode requires a counter for the encryption process. Each block requires IV (nonce) combined with up counter (0,1, ..., n) as shown in Figure 2

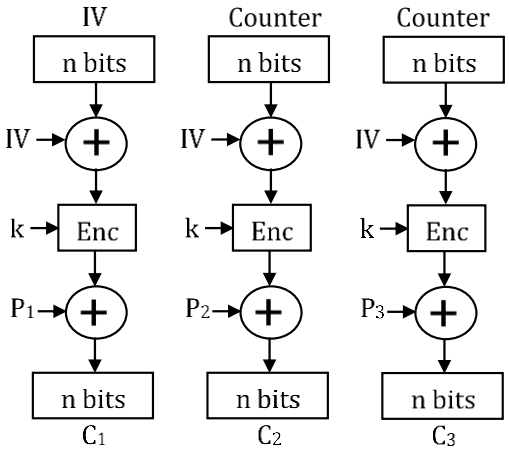


Figure 2. CTR operation mode

Each block will be encrypted with a key, nonce and counter, then the result of the encryption are performed XOR operations with plaintext data to produce ciphertext data. The advantage of this mode of operation, unlike CBC, encryption can be done in parallel and each block does not depend on the previous block

4.3 Identity Based Mediated RSA (IB-mRSA)

IB-mRSA is asymmetric cryptography or called public key cryptography where the key used for the encryption process is different from the decryption process. Identity-based public key encryption makes it easy to recognize public key cryptography by creating public keys based on a person's identity such as email or name. One algorithm that can be used is RSA with the addition of Security Mediator (SEM). Mediated RSA (mRSA) [11] involves a special entity, called SEM, which is a trusted server. A user will get a private key based on his identity generated by the Certifying Authority (CA). The private key is divided into two parts, one part is given to the user and the other is given to SEM. A user must get identity-based data from SEM. Without this data, the user cannot uses the key to decrypt the message. The KeyGen process, encryption and decryption can be seen in Algorithm 1

Algorithm 1 IB-mRSA Cryptography

1. Key Generator :
   a. Select random bit primes p' and q' such that $p = 2p' + 1$ and $q = 2q' + 1$. Set $n = p.q$, $\emptyset(n) = (p-1)(q-1)$, $e \, \epsilon_R Z^*_{\emptyset}(n)$, $d = e^{-1} \, mod(n)$
   b. For each user (y)
      1) $s = k - F(IDy) - 1$
      2) $e_y = 0^s || F(IDy) || 1$
      3) $d_y = \frac{1}{e_y} mod \, \emptyset(n)$
      4) $d_{y,u} \in_R Z_n - \{0\}$
      5) $d_{y,SEM} = (d_y - d_{y,u}) mod \, \emptyset(n)$
2. Encryption : In the encryption section (i.e. message sent from Alice to Bob), message (m) is encrypted using a standard RSA algorithm with Bob public key pair (e_B,n) with the encryption equation $m' = m^{e_B} \, mod \, n$
3. Decryption :
   a. Bob gets m' from Alice
   b. Bob sends m' to SEM
   c. SEM calculates $PDsem = m'^{d_{B,SEM}} \, mod \, n$ and send $PDsem$ to Bob
   d. Bob calculates $PDu = m'^{d_{B,u}} \, mod \, n$
   e. Bob decrypts $m = (PDsem * PDu) \, mod \, n$

4.4 Group Signature

A group signature is a mechanism for signing electronic messages by group members on behalf of the group and the member who signs the message is unknown (anonymity). In group signature, there is a Group Manager (GM) whose job is to manage the group members and carry out group signature procedures. The management of GM is in the form of makes secret key for each member and makes public key to be shared with all members. Therefore, GM must be assumed to be fully trusted (trusted party), and communication between GM and group members must be carried out securely.

In this study, we use the Camenisch-Groth (CG) algorithm developed by Jan Camenisch and Jens Groth [23]. CG algorithm has 6 processes, namely key generator, join, sign, verify, open and revoke. Key generator is used by GM to generate group manager secret key (*gmsk*) that are used by GM to perform open and revoke procedures and group public key (*gpk*) which are key that is shared with all members who are members of the group as shown in Algorithm 2. Algorithm 3 shows the join process, the process for generating a member secret key (*msk*) key when a new member joins. The sign process is the signing of an electronic message by one of the members using *msk* as shown in Algorithm 4. Algorithm 5 shows the verify process that is used to verify the signature whether the signature is from the same group as the member who conducted the verification process. Algorithm 6 shows the open and revoke process. The open process is used to open member's identity if members commit fraud or things that are not in accordance with group rules. While the revoke process is used to revoke membership from members.

Algorithm 2 Key Generator Process

Note that : $\ell_n = \ell_P = 2048$, $\ell_E = 504$, $\ell_Q = 282$, $\ell_c = 160$, $\ell_e = \ell_s = 60$

1. Choose ℓ_n-bit modulus $n = p.q$ from two bit primes $p = 2p' + 1$ and $q = 2q' + 1$ where p' and q' are random primes.
2. Choose random $a, g, h \in QR_n$ and random ℓ_Q-bit and ℓ_P-bit primes Q and P such that $Q|P-1$. Let F of the order element Q in $\mathbb{Z}_P^*$
3. Choose random components $X_G, X_H \in \mathbb{Z}_Q$, calculate $G = F^{X_G} mod\, P$, $H = F^{X_H} mod\, P$ and select random w, $f \in QR(n)$
4. Set group public key, *gpk* = (n, a, g, h, Q, P, F, G, H, w, f)
5. Set group manager secret key, *gmsk* = (*gpk*, p, q, X_G).

Algorithm 3 Join Process

Assume, there is member-i who wants to join the group. GM and member-i together do a join process to get msk

1. Member-i generates random integer $x_i \in \mathbb{Z}Q$, calculates $Y_i = G^{x_i} \bmod P$, sets $g^{x_i}h^{r'i} \bmod n$ to x_i and sends Y_i and $g^{x_i}h^{r'i} \bmod n$ to GM
2. GM chooses $e_i \in \{0,1\}^{le}$ such that $E_i = 2^{lE} + e_i$ is prime, then calculates $w_i = w^{E_i^{-1}} \bmod n$, selects random $r'' \in \mathbb{Z}_e$ and set $y_i = (ag^{x_i}h^{r_i'+r_i''})^{E_i^{-1}} \bmod n$. Then GM sends w_i, y_i, E_i and r'' back to member-i
3. Member-i sets member secret key, $msk_i = (gpk, w_i, x_i, r_i = r_i' + r_i'', y_i, e_i)$

Algorithm 4 Sign Process

Given msk_i and message (m), member-i of a group can sign message on behalf of the group to get a valid signature (signature)

1. Select random number $r \in \{0,1\}^{\ell n/2}$ and $R \in \mathbb{Z}_Q$, sets $u = h^r y_i w_i \bmod n$ and computes $U_1 = F^R \bmod P$, $U_2 = G^{R+x_i}$, $U_3 = H^{R+e_i} \bmod P$
2. Choose $r_x \in \{0,1\}^{l_Q+l_c+l_s}$, $r_r \in \{0,1\}^{\frac{l_n}{2}+l_c+l_s}$, $r_e \in \{0,1\}^{l_e+l_c+l_s}$, $R_R \in \mathbb{Z}_Q$
3. Computes :
   a. $v = u^{r_e}g^{-r_x}h^{r_r} \bmod n$, $V_1 = F^{R_R} \bmod P$, $V_2 = G^{R_R+r_x} \bmod P$, $V_3 = H^{R_R+r_e} \bmod P$
   b. $z_x = r_x + cx_i$, $z_r = r_r + c(-r_i - rE_i)$, $z_e = r_e + ce_i$, $Z_R = R_R + cR \bmod Q$
   c. $c = hash(gpk, u, v, U_1, U_2, U_3, V_1, V_2, V_3, m)$
4. The output signature $\sigma = (c, u, U_1, U_2, U_3, z_x, z_r, z_e, Z_R)$

Algorithm 5 Verify Process

This process is used to verify the signature using gpk. The output of this process is true if the signature is valid and false if the signature is invalid

1. Checks if $z_e \in \{0,1\}^{l_e+l_c+l_s}$ and $z_x \in \{0,1\}^{l_Q+l_c+l_s}$
2. Computes $v = (aw)^{-c}g^{-z_x}h^{z_r}u^{c2^{\ell_E}+z_e} \bmod n$, $\bar{V}_1 = U_1^{-c}F^{Z_R} \bmod P$, $\bar{V}_2 = U_2^{-c}G^{Z_R+z_x} \bmod P$, $\bar{V}_3 = U_3^{-c}H^{Z_R+z_e} \bmod P$, $c' = hash(gpk, u, v, U_1, U_2, U_3, \bar{V}_1, \bar{V}_2, \bar{V}_3, m)$
3. If and only if $c' = c$, the signature is valid

Algorithm 6 Open and Revoke Process

Open process is used by GM to open the user's identity if the user is cheating or things that are not in accordance with group rules. The process is GM uses X_G decrypt $U_1^{\frac{P-1}{Q}} \bmod P$, $U_2^{\frac{P-1}{Q}} \bmod P$ to get $G^{\frac{P-1}{Q}x_i} \bmod P$ and return i so it can be seen which member is doing the signature Then, revoke process is used to revoke membership so that members are no longer joined in the group. The process is publish E_i and changes w element in gpk to w_j

4.5 Proposed Secure Data Travelling User

The proposed security method is a hybrid cryptographic algorithm using symmetric and asymmetric cryptography and group signature algorithm to secure personal data and verification. The system design used for this proposed method is shown in the figure 3.

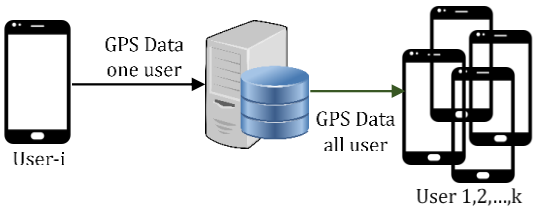


Figure 3. Proposed system design

In the proposed system, GPS data on a smartphone is sent to the server via the internet media which will later be processed. GPS and sensor data is retrieved using the android application on a user-*i* smartphone. Then the server will spread the information to other users through internet media. For example user-1 wants to share the location of its coordinates to his friends (users 2 and 3) then user-1 will send the coordinates to the server, which later the server will share the information to members of the user group A. Data processing and sending data from sender to recipient are shown in Figure 4

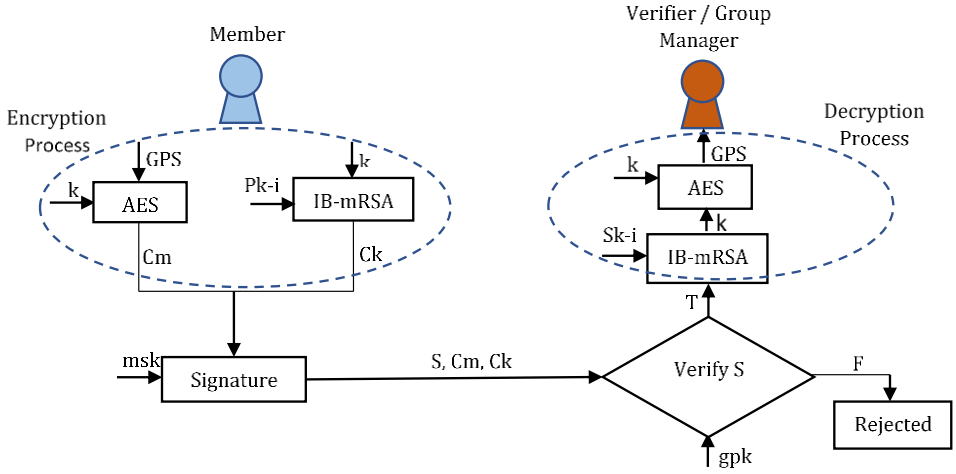


Figure 4. Processing and sending data

In the proposed system there are 3 main points of the data security process, namely the encryption, decryption and group signature process. In the encryption section, we use 2 algorithms namely AES and IB-mRSA algorithms. AES algorithm is used for encrypting GPS data using symmetric key (*k*), while the IB-mRSA algorithm is used for encryption of symmetric key (*k*) from AES. Both of the encryption results are signed using the member secret key (*msk*). The results of the signature are verified to prove that the sender is in the same group as the recipient. If the sender is not in the same group as the recipient, the data is rejected, but if the sender is in the same group as the recipient, the data encryption continues into the decryption process. AES-256 with CBC operating mode is used for AES algorithm. AES-256 uses a 256-bit key length with 14 rounds. Each AES cycle consists of 4 types of transformation byte, namely SubByte, ShiftRow, MixColumn and AddRoundKey.

Algorithm 7 Proposed Secure Data Travelling Method

1. Input : GPS data (m), member's email (IDm), recipient's email (IDr)
2. Key Generator :
   a. Calculates e_m, e_r = public key member and recipient from member's email (IDm) and recipient's email (IDr) of Algorithm 1 line 1b
   b. Calculates $d_{m,u}$, $d_{m,sem}$, $d_{r,u}$, $d_{r,sem}$ = private key member, SEM and recipient, SEM of Algorithm 1 line 1c-d
   c. Calculates gpk and msk_i = group public key for verify signature and member secret key for signing
3. Encryption :

a. $C_{AES} = Enc_{AES-CBC}(m, k)$ % GPS data is encrypted using AES
b. $C_{IB-mRSA} = k^{e_r} \bmod n$ % symmetric key AES is encrypted using IB-mRSA

4. Signing process :
Given message $m \in \{0,1\}^*$ which is merging of C_{AES} and $C_{IB-mRSA}$. From Algorithm 4 in lines 1 to 3b, we can get the result $c = hash(gpk, u, v, U_1, U_2, U_3, V_1, V_2, V_3, m)$ and output signature $\sigma = (c, u, U_1, U_2, U_3, z_x, z_r, z_e, Z_R)$
5. Verifying process :
From Algorithm 5, we can get the result $c' = hash(gpk, u, v, U_1, U_2, U_3, \bar{V}_1, \bar{V}_2, \bar{V}_3, m)$ and verify signature by checking $c = c'$. If and only if true, the signature is valid and verifier decrypts the encrypted message
6. Decryption :
a. SEM calculates $PDsem = {C_{IB-mRSA}}^{d_{r,SEM}} \bmod n$, receiver calculates $PDu = {C_{IB-mRSA}}^{d_{r,u}} \bmod n$
b. Receiver decrypts $k = (PDsem * PDu) \bmod n$ % receiver gets symmetric key (k)
c. Receiver decrypts $m = Dec_{AES-CBC}(C_{AES}, k)$ % receiver gets GPS data

The method used in this proposed method combines hybrid cryptography with group signature as in Algorithm 7. The input used is GPS data as location data to be encrypted, email member and email receiver that are used to generate IB-mRSA keys as in line 2a-b. In this method, we encrypt GPS data using AES cryptography and encrypt symmetric key using IB-mRSA cryptography as in line 3a-b. In line 4 the privacy and unforgeability security requirements are carried out through the signature process of combining the results of AES and IB-mRSA encryption. Valid group signatures contain encryption on the user's identity, namely the calculation of U1, U2 and U3 so that the user's identity becomes anonymous. The hidden user identity is made into a message block then the message block is converted to an ASCII value for calculation. The results of these calculations are combined and become a signature. In line 5 the security requirements for correctness are carried out through the signature verification process by the receiver after the sender sends the encryption and signature results to the receiver. To perform the decryption process, the receiver decrypts the IB-mRSA to get the symmetric key first as in lines 6a-b. After the receiver has received the AES symmetric key, the receiver can decrypt the AES to get GPS data as in line 6c.

5. EXPERIMENT AND ANALYSIS

The purpose of this study are to provide location and personal data security and limit the access of non-members to find out the position of members in a group. Experiment carried out produce computational time proposed method, comparison total processing time, security discussion and attack experiment on the system.

5.1 Implementation System

Test conducted in the implementation involves servers and five users where the user is a smartphone device used to access the traveling application. The specifications of the hardware and software used in the experiment describe in Table 1

Table 1. Hardware and software specification

Entity	Hardware and Software Specification
Server	Windows 10 Education 64 bit, CPU @ 1.70 GHz, ~2.4 GHz, RAM 8 GB, libs/cg.jar, firebase-auth:17.0.0, firebase-database:17.0.0
Member 1	Android 6.0.1, Octa-core 1.6 GHz Cortex-A53, RAM 2 GB
Member 2	Android 9.0, Octa-core (2x2.2 GHz Kryo 360 Gold), RAM 4 GB
Member 3	Android 9.0, Octa-core (4x2.0 GHz Kryo 260 Gold), RAM 3 GB
Member 4	Android 8.1, Octa-core (2x1.95 GHz Cortex-A53), RAM 2 GB
Member 5	Android 4.4.2, Quad-core 2.5 GHz Krait 400, RAM 3 GB

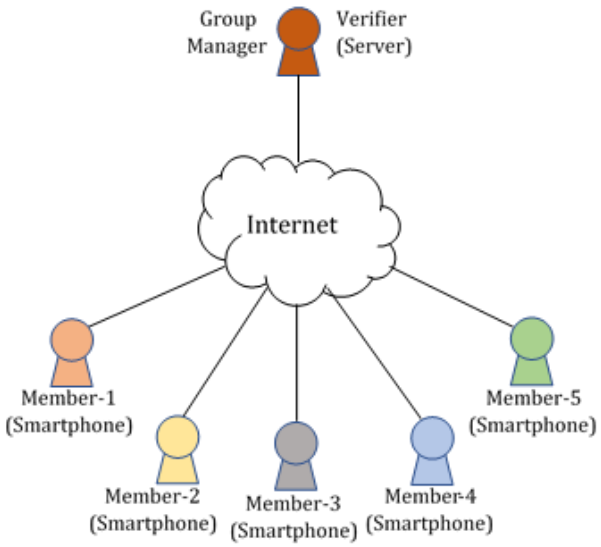


Figure 5. system scenario

Our test took place at Kenjeran Park Surabaya where the place is an outdoor playground that can be accessed by GPS with an area of approximately

100m^2. In our scenario there are 2 players namely Group Manager who also acts as a verifier and five smartphones as legitimate members. Figure 5 shows an implementation scenario where GM is responsible for setting up the system, generate a public key group (*gpk*), group manager secret key (*gmsk*) and member secret key (*msk*) when a member joins. In this experiment, we combine GM and verifier into 1 player. Verifier represented as server has the authority to verify the signature of all members using gpk and decrypts encrypt GPS data from members. Members are assigned as a signer who are responsible for encrypting GPS data, signing it using msk and sending the results of encryption and signature through the network (i.e. Internet).

We made a scenario by spreading 5 members with a distance between 50 meters to 500 meters, the difference in the distance is far enough so that no member is in the same position. We use a tool from Google, named Firebase. Google firebase is used for authentication when members login to the application and as a realtime database so that when members move the GPS data will be updated and synchronized. In this case, each member sends GPS data in realtime, if the member is offline then the stored GPS data is the latest GPS data. Therefore, when the member-*i* sends he/her location and the verification process is successful, then automatically other members who are in the same group will get the latest location. GPS location that has been successfully verified is displayed through the map service application as shown in Figure 6.

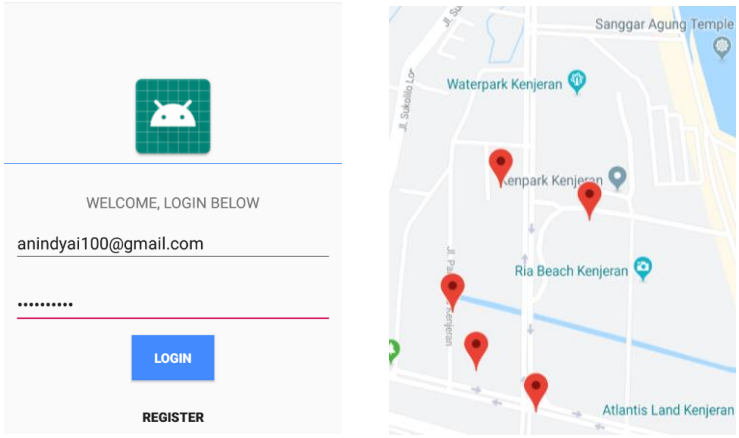


Figure 6. GPS location display if verification is successful

When member-*i* is not in the same group as the other members, then the signature verification done by the verifier is not successful and the location of other members cannot be detected. Figure 7 is the result when the member-*i* are not in the same group as the other members, so that the only locations that are detected is member-*i* location.

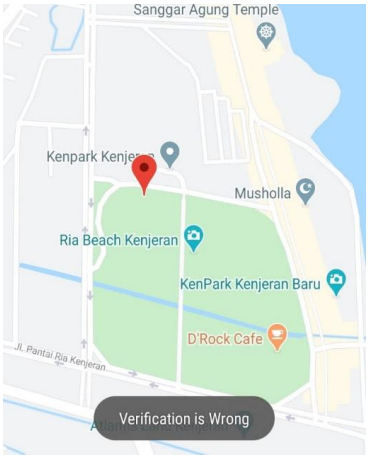


Figure 7. GPS location display if verification is unsuccessful

5.2 Experimental Result

This section explains the results of our proposed experimental method and we compare the results of those experiment with the existing method in terms of total processing time.

5.2.1 Computational Time Proposed Method

The computation time of the key generation performed by GM includes the Setup and Join process where the setup process produces gpk and gmsk while the join process produces msk. Table 2 shows the computational time during the setup, join, IB-mRSA and AES key generation processes. The setup process is done once when a group is created, the join process, IB-mRSA and AES are carried out 5 times each member joins the group. The setup process takes 17,663.8 ms while the join process requires 119.3 ms. Meanwhile, the generation of IB-mRSA key takes 1,425 ms, while the generation of AES key takes 907.6 ms.

Table 2. Measurement key generator process

Setup Process	Join Process	Key Generator AES	Key Generator IB-mRSA
17,663.8 ms	119.3 ms	907.6 ms	1,425 ms

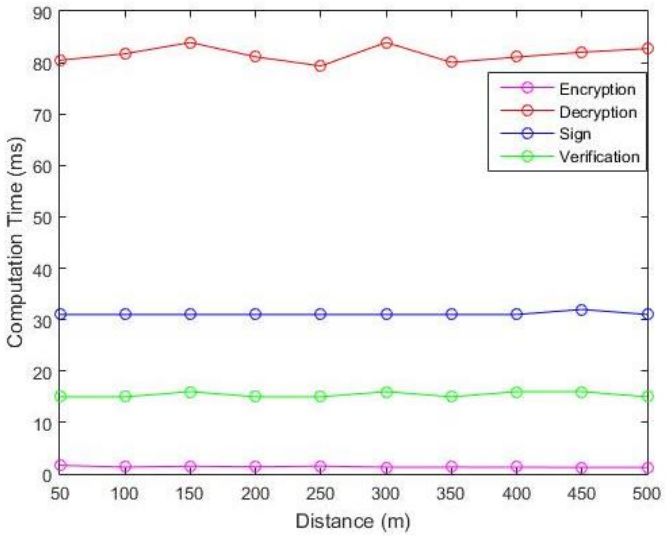


Figure 8. Computation time in encryption, decryption, signing and verification process

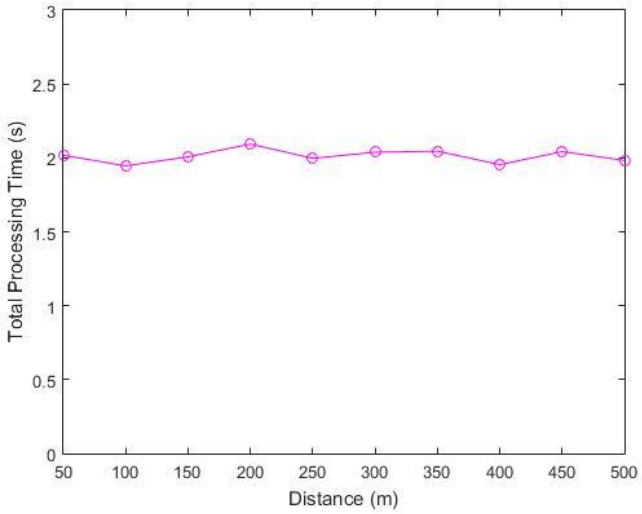


Figure 9. Total processing time with distance 50 to 500 meters

The use of hybrid cryptography, signing process and verification process are the most important mechanism in this experiment. Figure 8 shows the computing time of the encryption, decryption, signing and verification process. Because of the use of hybrid cryptography, the encryption and decryption time is a compilation of computational time from AES and IB-mRSA cryptography. Encryption and decryption time require 1.4 ms and 81,6 ms, respectively. The decryption process requires a longer time because it requires 2 players namely member and SEM to do the decryption. Whereas the sign and verification time require 31.1 ms and 15.4 ms respectively.

Figure 9 shows the total processing time in our experiment with the distance between members 50 to 500 meters. We start the measurement when the member-*i* starts running their GPS, encrypts hybrid cryptography and runs

the sign up process until the member-*i* gets the GPS location of the other four members. Calculation of the total processing time can be seen in equation 3.

$$t = t_1 + t_2 + t_3 + t_4 + t_5 \quad (3)$$

t_1 is the measurement time when member-*i* encrypts GPS data and runs the *Sign* process. t_2 is the transmission time when member-*i* sends encryption and signature data to the server. t_3 is the measurement time when the server verifies the signature using the *Verify* process and decrypts the data encryption. t_4 is the transmission time when the server sends all member's GPS data to member-*i*. The last t_5 is the measurement time when member-*i* gets all member's GPS data and display it in the service application map

5.2.2 Comparison Total Processing Time

The comparison method [15] only uses AES-CCM cryptography to secure GPS data. In this experiment, we made improvement to the comparison method by adding group signature that are used to verify members and protect member's personal data. From the addition of group signature to the comparison method, we compared the total processing time with the proposed method. Figure 10 shows the difference in total processing time between the proposed method and the comparison method.

Calculation of total processing time is the same as in equation 3, it appears that the total processing time of the proposed method is longer than the comparison method [15]. This is because the proposed method uses hybrid cryptography, AES and IB-mRSA, so there are two processes of encryption and decryption. The results of this process make the data sent become longer. Because of the long data, the total processing time between member-*i* to receiver is longer. The total transmission time in the proposed method is 2.01 seconds. Whereas the comparison method is 1.93 seconds. From the data, the percentage of error from the proposed method is 0.04 %

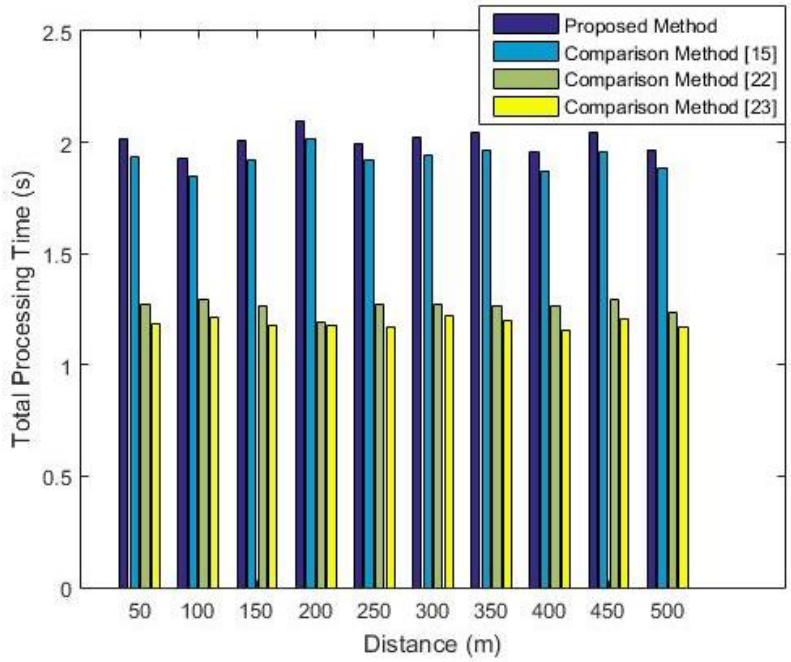


Figure 10. Comparison of total processing time between proposed method and comparison method [15], [22], [23]

We also compared processing time with the methods [22] and [23] that used group signatures. It can be seen that the processing time in the proposed method is better than the comparison method. This is because the methods [22] and [23] do not use cryptography, but only group signatures, whereas the proposed method uses cryptographic and group signature combinations. The total transmission time for method [22] is 1.27 seconds, while for method [23] it is 1.18 seconds. From this data, the percentage of error from the proposed method is 0.6% compared to method [22] and 0.7% compared to method [23]. From the calculation of error less than 1%, it can be said that the proposed method does not spend too long with the advantage of secure data.

5.2.3 Security Discussion

Here, we discuss the security requirements of the proposed method in Section IV. Member-*i* who wants to join the group need to register by inputting their name, age, gender, telephone number, email and password. After the member-*i* successfully joins, GM generates a msk_i which is then given to the member-*i*. To start sending GPS data, member-*i* logged in with the email and password that was entered earlier. When the login process is successful, at that time the member-*i* also generates symmetric key (k), public key user (pk_u), secret key user (sk_u) and secret key SEM (sk_{SEM}). The k is encrypted using IB-mRSA where the k is the key for encrypting GPS data (m). So when k is distributed to the receiver, the data sent is the ciphertext of key and ciphertext of m. These processes meet the data integrity and authentication security requirements.

Ciphertext of key and m are signed, then the signature and ciphertext results are sent to the receiver. This *Sign* process can only be done by a legitimate members because it requires msk to sign messages on behalf of the group without knowing which member is signing, which in this process meets the requirements of unforgeability and privacy. At the receiver, the *Verify* process is carried out to verify that the signature was sent by a legitimate memberss. If the data is actually sent from a legitimate members, the receiver can decrypt the symmetric key (k) and GPS data (m). Therefore, the confidentiality and correctness of data are hold.

5.2.4 Attacking Test

In a data communication, an attack is most likely to occur. We created an attack scenario by MITM where the attacker placed himself in the middle of two devices that communicate with each other. In this test, we carried out active and passive attack scenarios.

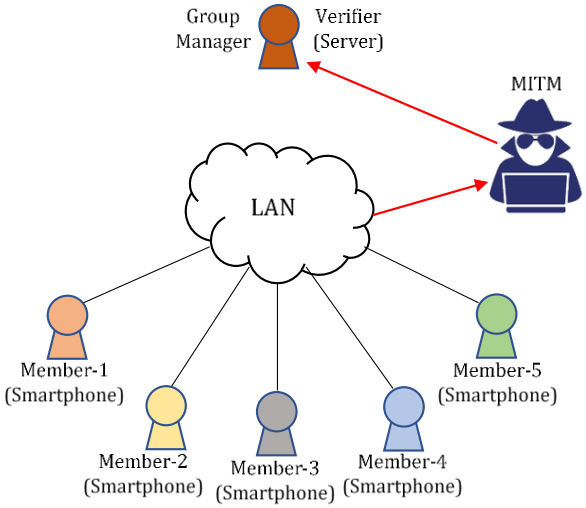


Figure 11. ARP spoofing mechanism

The active attack that we use in this scenario is arp spoofing. ARP spoofing is a type of attack where the attacker changes and sends message that is falsified through the local area network as shown in Figure 11. ARP spoofing will send fake ARP messages to the local network ethernet with the aim of matching the MAC address with other computers such as the gateway computer. So any data traffic to the IP gateway will first lead to the attacker's computer as a fake gateway that will eventually be forwarded to the legitimate gateway and allow it to modify data. In this case, because of an attacker in the middle of data communication, the message from the member-*i* is not sent directly to the server but through the attacker first. As a result the server will gets a fake message so that the fake message cannot be decrypted.

Time	Source	Destination	Protocol	Length	Info
259.197467800	LiteonTe_31:16:70	Vmware_d0:50:82	ARP	60	192.168.43.246 is at ac:b5:7d:31:16:70
259.200663168	da:ce:3a:63:f6:31	Vmware_d0:50:82	ARP	60	192.168.43.1 is at da:ce:3a:63:f6:31
259.315915760	SamsungE_d7:81:32	Vmware_d0:50:82	ARP	60	192.168.43.106 is at 20:5e:f7:d7:81:32
259.817895976	Vmware_d0:50:82	LiteonTe_31:16:70	ARP	42	192.168.43.1 is at 00:0c:29:d0:50:82
259.818316696	Vmware_d0:50:82	da:ce:3a:63:f6:31	ARP	42	192.168.43.246 is at 00:0c:29:d0:50:82

```
Address Resolution Protocol (reply)
   Hardware type: Ethernet (1)
   Protocol type: IPv4 (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: reply (2)
   Sender MAC address: Vmware_d0:50:82 (00:0c:29:d0:50:82)
   Sender IP address: 192.168.43.1
   Target MAC address: LiteonTe_31:16:70 (ac:b5:7d:31:16:70)
   Target IP address: 192.168.43.246
```

Figure 12. Arp spoofing analysis using wireshark

Figure 12 shows arp spoofing analysis using wireshark where the attacker sends an arp reply to the recipient. In the blue box, the attacker's computer sends an ARP-reply to the IP server 192.168.43.246 assuming the sender is from the IP gateway 192.168.43.1. It appears that the MAC address used on the IP gateway is 00: 0c: 29: d0: 50: 82 where the MAC address is the attacker's MAC address. while the original MAC address of the gateway is da: ce: 3a: 63: f6: 31 as in the red box. Because of the intrusion of this MAC address, the IP server assumes that the attacker's computer is a legitimate computer.

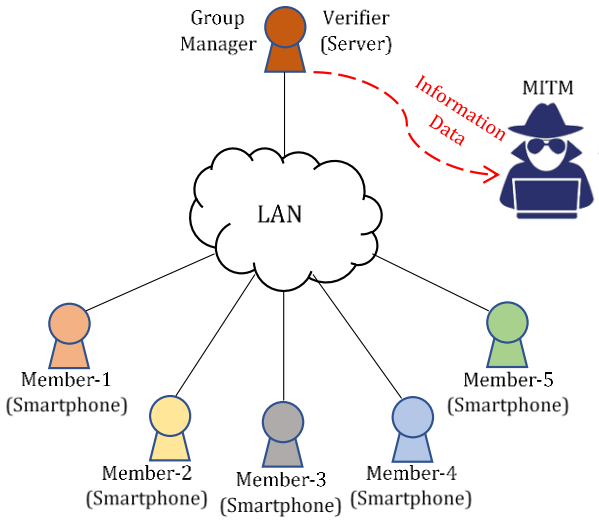
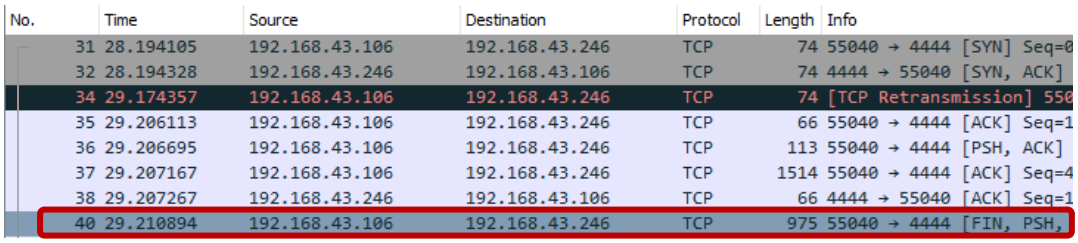


Figure 13. Sniffing mechanism

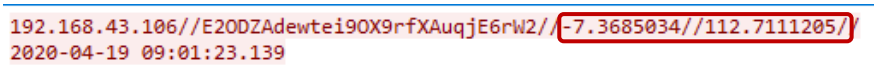
The passive attack we use is a sniffing test. Sniffing test is one of the hacking techniques carried out to obtain important information by capturing packets that run in the network between the sender and receiver as shown in Figure 13. Because hacker is in the middle of communication, hacker can read packets that will be sent / received from both devices. To view information when there is data communication, Wireshark software is used. All types of information packages in various protocol formats will be easily captured and

analyzed. Based on Figure 14 the TCP protocol is used as the communication between sender with IP address 192.168.43.106 to recipient with IP address 192.168.43.246. MITM marks data packets that are considered to have information and view data contents using the follow tcp stream option.



No.	Time	Source	Destination	Protocol	Length	Info
31	28.194105	192.168.43.106	192.168.43.246	TCP	74	55040 → 4444 [SYN] Seq=0
32	28.194328	192.168.43.246	192.168.43.106	TCP	74	4444 → 55040 [SYN, ACK]
34	29.174357	192.168.43.106	192.168.43.246	TCP	74	[TCP Retransmission] 550
35	29.206113	192.168.43.106	192.168.43.246	TCP	66	55040 → 4444 [ACK] Seq=1
36	29.206695	192.168.43.106	192.168.43.246	TCP	113	55040 → 4444 [PSH, ACK]
37	29.207167	192.168.43.106	192.168.43.246	TCP	1514	55040 → 4444 [ACK] Seq=4
38	29.207267	192.168.43.246	192.168.43.106	TCP	66	4444 → 55040 [ACK] Seq=1
40	29.210894	192.168.43.106	192.168.43.246	TCP	975	55040 → 4444 [FIN, PSH,

Figure 14. TCP data packet display



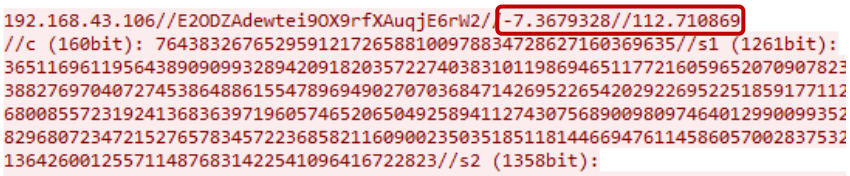
```
192.168.43.106//E2ODZAdewtei9OX9rfXAuqjE6rW2//-7.3685034//112.7111205//
2020-04-19 09:01:23.139
```

Figure 15. Unsecured data seen by MITM

In this sniffing attack we also conducted an experiment where the data sent was not secured so that MITM could immediately see the data sent via Wireshark as shown in Figure 15. The red box is a location data in the form of longitude and latitude that is not secured so that it can be seen clearly. Then we do security using the method [15] and sniffing results recorded by Wireshark as shown in Figure 16. The data display seen by MITM is not original data but information that has been encrypted, the results of signature and symmetric key. In the method [15] the symmetric key on the red box looks very clear so that MITM can decrypt the message sent.

```
192.168.43.106//xDEO81MLVCaSkOOxKREPbJB1jJa2//EJfU1wi4Uh6mzS6j//
... .B....(U....w....]....Q.Lw..O."....OT@.y.N.........B..d..
=..b.y........j...&.~VT.u..N.0.w...'..M.J
<..To.G....Dr}//c (155bit): 425542845835214504274491034322283602058808223 71//u
(1023bit):
72781227216191298534011775742996257243909052335037338627928240058454467542694379
80237112043342637246652085991347846869123400049953322332288977245675921129550939
03228937956392592293086574325425171085119215018063693654800003388425654871585457
08605664054717947759630788016838390906594163616793997//U1 (1020bit):
75441066436686567378073130331922663491932834500537217040559696744446812475217308
74756698459323789048990745799950647924113391300591418002684785780402523669050256
77424645931255043803178574062385365058122379058949243306799633474157657289222069
79429412564956662893336761882503389485955140512517 80//U2 (1024bit):
```

Figure 16. Information seen by MITM using method [15]



```
192.168.43.106//E2ODZAdewtei9OX9rfXAuqjE6rW2//-7.3679328//112.710869
//c (160bit): 764383267652959121726588100978834728627160369635//s1 (1261bit):
365116961195643890909932894209182035722740383101198694651177216059652070907823
388276970407274538648861554789694902707036847142695226542029226952251859177112
68008557231924136836397196057465206504925894112743075689009809746401299009935 2
82968072347215276578345722368582116090023503518511814466947611458605700283753 2
13642600125571148768314225410964167228 23//s2 (1358bit):
```

Figure 17. Information seen by MITM using method [22]

Then using the methods [22] and [23]. sniffing results obtained are seen in Figure 17-18. MITM can see the location data in the red box clearly and the results of the signature. From the methods [15], [22] and [23], we compared them with the proposed method and the results can be seen as shown in Figure 19. The symmetric key sent to the receiver is not visible because it has been encrypted using IB-mRSA cryptography and location data is also not visible because it has been encrypted using AES cryptography. With the group signature, the data sent can be received by members in the same group so members from different groups can not find out the location data of other groups. With the improvement of methods [15], [22] and [23], it can be proven that the proposed method is safer because it can maintain the confidentiality of the symmetric key when distributing key, maintain data security when sending data and the data sent is only obtained by member in the same group.

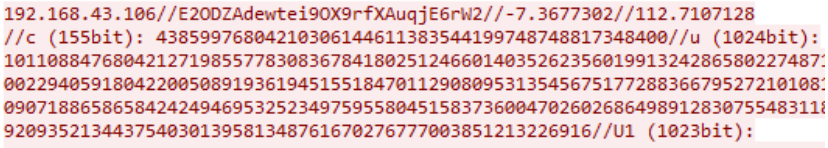


Figure 18. Information seen by MITM using method [23]

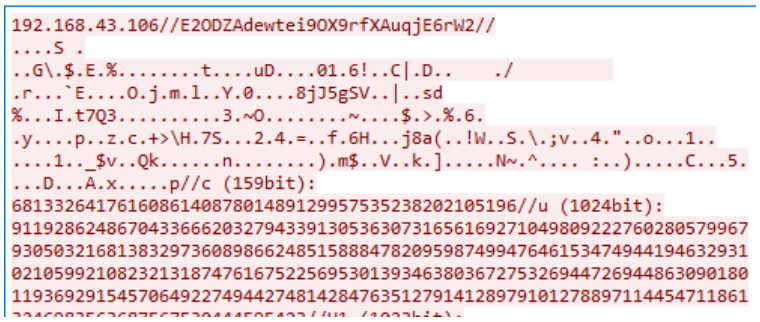


Figure 19. Information seen by MITM in proposed method

6. CONCLUSION

In this study, a data security system has been proposed using hybrid cryptography and group signature. The merging of our system make the data safer because of the verification of the signature which aims to make the data only accessible by members in the same group without expose member identity. Our research showed that the use of hybrid cryptography and group signature can make the distribution of symmetric key safer and protect the personal data of members in a group. But because of the incorporation of this method, the total processing time needed is a little longer when compared to the comparison method [15], [22] and [23] which is 2.01 seconds with a percentage error of 0.04 %, 0.5 % and 0.7 %, respectively. If seen from the percentage of error that are not too large and better data security, the proposed method can improve the previous method. Our future works include the improvement of map service with increasing the number of members up

to hundred members and the implementation of group signature with much faster total processing time.

Acknowledgements

The author would like to return thanks to Zulmi Zakariyah, Postgraduate student in Politeknik Elektronika Negeri Surabaya (PENS) who has helped to retrieve data at Kenjeran Park

REFERENCES

[1] X. Li and Q. Xu, **A Reliable Fusion Positioning Strategy for Land Vehicles in GPS-Denied Environments Based on Low-Cost Sensors**, *IEEE Trans. Ind. Electron.*, vol. 64, no. 4, pp. 3205–3215, 2017.

[2] A. A. Bin Ariffin, N. H. A. Aziz, and K. A. Othman, **Implementation of GPS for location tracking,** *Proc. - 2011 IEEE Control Syst. Grad. Res. Colloquium, ICSGRC 2011*, no. November 2015, pp. 77–81, 2011.

[3] M. P. Uddin, M. Z. Islam, M. Nadim, and M. I. Afjal, **GPS-based Location Tracking System via Android Device,** *Int. J. Res. Comput. Eng. Electron.*, 2013.

[4] M. N. S. Perera and T. Koshiba, **Fully dynamic group signature scheme with member registration and verifier-local revocation,** vol. 253. Springer Singapore, 2018.

[5] A. Oracevic, S. Dilek, and S. Ozdemir, **Security in internet of things: A survey,** *Int. Symp. Networks, Comput. Commun. ISNCC 2017*, no. i, 2017.

[6] S. Eom and J. H. Huh, **Group signature with restrictive linkability: minimizing privacy exposure in ubiquitous environment,** *J. Ambient Intell. Humaniz. Comput.*, vol. 0, no. 0, pp. 1–11, 2018.

[7] L. Zhang, C. Li, Y. Li, Q. Luo, and R. Zhu, **Group signature based privacy protection algorithm for mobile ad hoc network,** *IEEE Int. Conf. Inf. Autom. ICIA 2017*, no. July, pp. 947–952, 2017.

[8] R. M. Awangga, N. S. Fathonah, and T. I. Hasanudin, **Colenak: GPS tracking model for post-stroke rehabilitation program using AES-CBC URL encryption and QR-Code,** *Proc. - 2017 2nd Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. ICITISEE 2017*, vol. 2018-January, pp. 255–260, 2018.

[9] C. Shi, C. Xiangguo, and W. C. Choong, **Practical group signatures from RSA,** *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, vol. 1, pp. 211–215, 2006.

[10] W. Stallings, **Cryptography and Network Security: Principles amd Practices,** Ed. 4, 2011.

[11] D. Boneh, X. Ding, G. Tsudik, and C. M. Wong, **A Method for Fast Revocation of Public Key Certificates and Security Capabilities,** *USENIX Secur. Symp.*, 2001.

[12] M. Jain and M. Singh, **Identity Based Secure RSA Enryption System,** *Proceedings of International Conference on Communication and Networks.*, vol. 508, 2017.

[13] P. Satapathy, N. Pandey, and S. K. Khatri, **NFC Car Keys by Using RSA**

Cryptography in WSN Security, *Proc. 3rd Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2019*, pp. 143–147, 2019.

[14] A. D. Putri Islamidina, A. Sudarsono, and T. Dutono, **Security System for Data Location of Travelling User using RSA based on Group Signature,** *IES 2019 - Int. Electron. Symp. Role Techno-Intelligence Creat. an Open Energy Syst. Towar. Energy Democr. Proc.*, pp. 88–93, 2019.

[15] Sarbpreet, S. Tripathy, and J. Mathew, **Design and evaluation of an IoT enabled secure multi-service Ambulance Tracking System,** *IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON*, pp. 2209–2214, 2017.

[16] S. Banik, A. Bogdanov, and F. Regazzoni, **Compact circuits for combined AES encryption/decryption,** *J. Cryptogr. Eng.*, vol. 9, no. 1, pp. 69–83, 2019.

[17] M. P. Babitha and K. R. R. Babu, **Secure cloud storage using AES encryption,** *Int. Conf. Autom. Control Dyn. Optim. Tech. ICACDOT 2016*, pp. 859–864, 2017.

[18] M. Vaidehi and B. J. Rabi, **Design and analysis of AES-CBC mode for high security applications,** *2nd Int. Conf. Curr. Trends Eng. Technol. ICCTET 2014*, pp. 499–502, 2014.

[19] D. Chaum and E. van Heyst, **Group Signature,** *Advances in Cryptology - EUROCRYPT 1991 of LEcture Notes in Computer Science, Springer-Verlag,* vol. 547, pp. 257-265, 1991.

[20] H. Zheng, Q. Wu, B. Qin, L. Zhong, S. He and J. Liu, **Linkable Group Signature for Auditing Anonymous Communication,** *Australasian Conference on Information Security and Privacy*, pp. 304–321, 2018.

[21] A. Ishida, Y. Sakai, K. Emura, G. Hanaoka and K. Tanaka, **Fully Anonymous Group Signature with Verifier-Local Revocation,** *International Conference on Security and Cryptography for Networks.*, pp. 23–42, 2018.

[22] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, **A Practical and Provably Secure Coalition-Resistant Group Signature Scheme,** Advances in Cryptography - *Crypto 2000,* pp. 255–270, 2000.

[23] J. Camenisch and J. Groth, **Group Signatures: Better Efficiency and New Theoretical Aspects,** *Security and Communication Networks* pp. 120–133, 2005.