ISSN: 0067-2904

Secure Location Privacy Transmitting Information on Cellular Networks

Bashar M. Nema*, Shatha J. Mohammed
Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq

Received: 13/11/2021 Accepted: 9/1/2022 Published: 30/11/2022

Abstract

As smartphones incorporate location data, there is a growing concern about location privacy as smartphone technologies advance. Using a remote server, the mobile applications are able to capture the current location coordinates at any time and store them. The client awards authorization to an outsider. The outsider can gain admittance to area information on the worker by JSON Web Token (JWT). Protection is giving cover to clients, access control, and secure information stockpiling. Encryption guarantees the security of the location area on the remote server using the Rivest Shamir Adleman (RSA) algorithm. This paper introduced two utilizations of cell phones (tokens, and location). The principal application can give area information by means of the geographic position method of these gadgets. Every cell phone can create a token. The token holds secret keys got from versatile fixed identifiers for the most part of the Social Security Number (SSN) for each SIM (Endorser Personality Module) Chronic Number) and IMEI (Global Portable Hardware Character) by RSA calculation. The token is going through the short and informative administration of Short Message Service (SMS) from the client to the outsider. Information is scrambled before being stored on a faraway worker. The actual worker can't comprehend the area's information. The third-party cannot follow the area if the client utilizes distinctive mystery keys. The client's data and area information are saved by the various workers. The proposed application offers a mysterious sharing instrument that uses token verification to grant clients access to scrambled area data and provides encryption data in a remote server with an authentication token, achieving mutual authentication on each mobile device and user concealment.

Keywords: JSON Web Token, Location Privacy, Mobile Device, RSA Algorithm.

تأمين خصوصية الموقع في نقل المعلومات في الشبكات الخلوية

بشار مكي العيساوي*, شذى جاسم محمد
قسم علوم الحاسوب، كلية العلوم، الجامعة المستنصرية، بغداد، العراق

الخلاصة

نظرًا لأن بيانات الموقع مضمنة في الهواتف الذكية، فهناك قلق متزايد بشأن خصوصية الموقع مع تقدم تقنيات الهواتف الذكية. باستعمال خادم بعيد، يمكن لتطبيقات الهاتف المحمول التقاط إحداثيات الموقع الحالي

*Email: bashar_sh77@uomustansiriyah.edu.iq

في أي وقت وتخزينها. يمنح العميل الإذن لشخص خارجي، ويمكن للطرف الخارجي الحصول على إذن بالدخول إلى معلومات المنطقة الخاصة بالعامل عن طريق JSON Web Token (JWT). الحماية هي تغطية العملاء والتحكم في الوصول وتخزين المعلومات بشكل آمن. يضمن التشفير أمان منطقة الموقع في الخادم البعيد، الذي يستعمل خوارزمية RSA (Rivest Shamir Adleman). قدمت هذه الورقة استعمالين للهواتف المحمولة ، ويمكن للتطبيق الرئيسي تقديم معلومات المنطقة عن طريق طريقة الموقع الجغرافي لهذه الأدوات ، ويمكن لكل هاتف محمول إنشاء رمز مميز ، ويحمل الرمز المميز مفاتيح سرية تم الحصول عليها من معرفات ثابتة متعددة الاستعمالات في معظم الأحيان SSN (SIM (وحدة شخصية المصادقة) الرقم المزمن) و IMEI (شخصية الأجهزة المحمولة العالمية) عن طريق حساب RSA ، يمر الرمز المميز عبر إدارة المعلومات القصيرة (SMS) من العميل إلى الخارج ، ويتم خلط معلومات المنطقة قبل التخزين في عامل بعيد والعامل الفعلي لا يستطيع فهم معلومات المنطقة. لا يمكن للطرف الثالث متابعة المنطقة إذا كان العميل يستعمل مفاتيح غامضة مميزة، يتم حفظ بيانات العميل ومعلومات المنطقة في طبقات مختلفة. التطبيق اللاحق الذي يعطي أداة مشاركة غامضة باستعمال التحقق من الرمز الذي يعطي قبولًا لمعلومات المنطقة المشوشة للعملاء.

1. Introduction

Location-based services have gotten popular through cell phones, like utilizing cell networks, GPS, WIFI, and Bluetooth. Finding geographic places for versatile clients that are turning out to be more convenient and precise can be accomplished with low-control and minimal-cost gadgets. Thus, the privacy of the site becomes at all times and at all times more reasonable [1]. When the problem of position share is overcome, the token content depends on the query of content. The JSON Web Token was used to protect the shared location data. Each mobile device has an independent role in determining the token content. To protect user location data [2], an asymmetric key is used. With Android Emulators, the mobile application works. The Android studio and the Android software development kit have created the mobile application (SDK). Position data (latitude, longitude, and current time and date) can be provided in the application, which will later be used in mobile location. The GSM/UMTS and GPS can naturally deliver these geographical coordinates [3].

The user app allows the geographic location of a cell phone to be identified for each specific period in this design concept. A third-party application permits access to the geographical location of the user. The user stores information (user and third party) on server 1, generates a token, and stores the native app with password and user name (PW, UN) and the existing time and date for every specific period of time. The user and third parties exchange their tokens directly through SMS messages. The token analyzes and obtains the modulus, private key, and (PW, UN) in the third-party application. In a mobile device, the HTTP transaction uses a server-side 2 user location encoder, a (PW, UN), and decrypts position information with a private key and a modulus. Figure 1 shows a description of location privacy [4].

In this paper, the contributions can be summarized as follows: confidentiality of stored data is provided in the application by encryption/decryption data using RSA algorithms for the privacy of a location. The location data, which can be received from a third-party authority, is transformed into a remote server. Token creation includes a JWT secret key and sends it to authorized users. The token gives access to encrypted data, which can only be decrypted through a token parser.

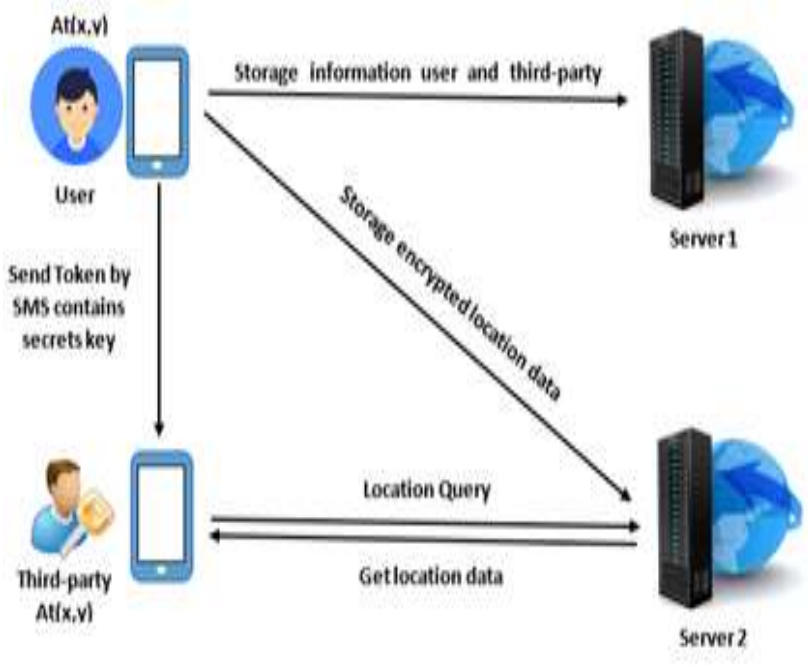


Figure 1: Basic design location privacy [4].

2. Related Works

In [5], privacy location is improved by introducing a dual encryption method by using the LocX technology. Before storage on various servers, location data and user information were encrypted. A third party cannot track a remote server's location, and a remote server cannot recognize the location data itself. Asymmetrical keys were applied in order to encrypt data locations using 2 keys (private key/public key). LocX is used to improve the privacy of a localization. LocX uses low-cost symmetric keys to encrypt/decrypt data so that all mobile phones work efficiently. [6], use of Android location privacy by enabling localization data to be transferred in an encrypted style. This paper presents a number of methods offered in encryption algorithms for the transmission of data in an encrypted way (RSA, Blowfish, Triple DES, AES). The application securely transmits data and third-party servers guess the method of encryption. In [7], the authors propose that information about the location of a user be protected to prevent violation of privacy. In semanticized information, a user's behavior includes space and time data. The space and time factors for semantic information are taken into consideration, and the b-diversity technique is proposed in order to prevent exposure to sensitive user behavior. [8], discusses how the ambiguous server can transform publicly available geographical data into a hidden personal region during user technicians to have a privacy system for user location sharing. [9], offers enhanced security and privacy-preserving location sharing using Bloom Filter to conceal sensitive data exchanges in the communications of location sharing procedures. [10], shows that the new algorithm allows users to accurately locale search services (LSSs) with high privacy protection and reduces quality loss (QL).

3. Theoretical Background

3.1 RSA algorithm

The RSA algorithm is based on equations in which the real public/private key challenge is generated. The secret keys are associated with high numbers and are used to multiply large numbers. When users select small prime numbers, it can penetrate, or it will take a very long time to select a large number. RSA is the most popular cryptography in asymmetric; a public

RSA key is used to encrypt data so that only a private key can decrypt it. RSA can be described briefly as follows [11, 12]:

1. Primes p, q.
2. Moduls = p*q, phi = (p −1) *(q −1).
3. Public key and private key are computed, such that private key = public key^-1 mod(phi).
4. Moduls, e is a public key and the plaintext M is encrypted as C = Me mod modulus.
5. The private key d is required to decrypt the cipher text as M = C^d mod modulus.

3.2 Tokens

The authorization token can be implemented via JWT. Each mobile device generates a token that contains all the information for secret keys derived from a mobile device's fixed identifier such as the SIM Serial Number and IMEI. The JWT claim sends an SMS message [13, 14]. The JWT consists of three structures separated by the dots (.) as in the following [15, 16]:

- **Header**: There are two parts in the header. The first part is the token type, such as HMAC, and the second part is hashing algorithms such as SHA256.
- **Payload:** It is the second part of the token, which consists of a claim that contains the token reserved. The claim is the statement about supplementary metadata and entities (usually users). The JWT defines eight claims that can be included in a token as issuer (iss), subject (sub), audience (aud), expiration time (exp), not before (nbf), issued at (iat), JWT ID (jti), and type (typ).
- **Signature:** Created to take an encoded header that is used to verify if it is trusted or not.

4. Proposed Methods

The proposed model offers privacy and encryption of user location via two mobile applications. The first application described for the user whose location is tracked is registering personal information (name, username, password, email, and phone number) and reading the mobile device's fixed identifiers (IMEI number and SIM Serial Number). All information is stored on an external server (server 1). After the user's information registration process is completed, the user enters the third-party information (name, phone number, and email). The third-party is authorized personnel to access the user's location. The application generates a secret key according to the RSA Algorithm, the token created by JWT, and sends it via SMS to a third-party. The location coordinates are encrypted by an RSA algorithm and then stored on another external server (server 1). As illustrated in Figure 2, the location data, password merged with the username, and current date and time were stored on another server (server 2). The third-party is allowed access to the user's location by token. The application uses a token parser to obtain the user's encrypted location while the user sends the password and username to the server. The third-party can decrypt the location data after receiving it from the server. The results are displayed on the Google map. Figure 3 shows a basic system that can be separated into three parts: Key Generation, Location Encryption/Decryption, and Token Phase.

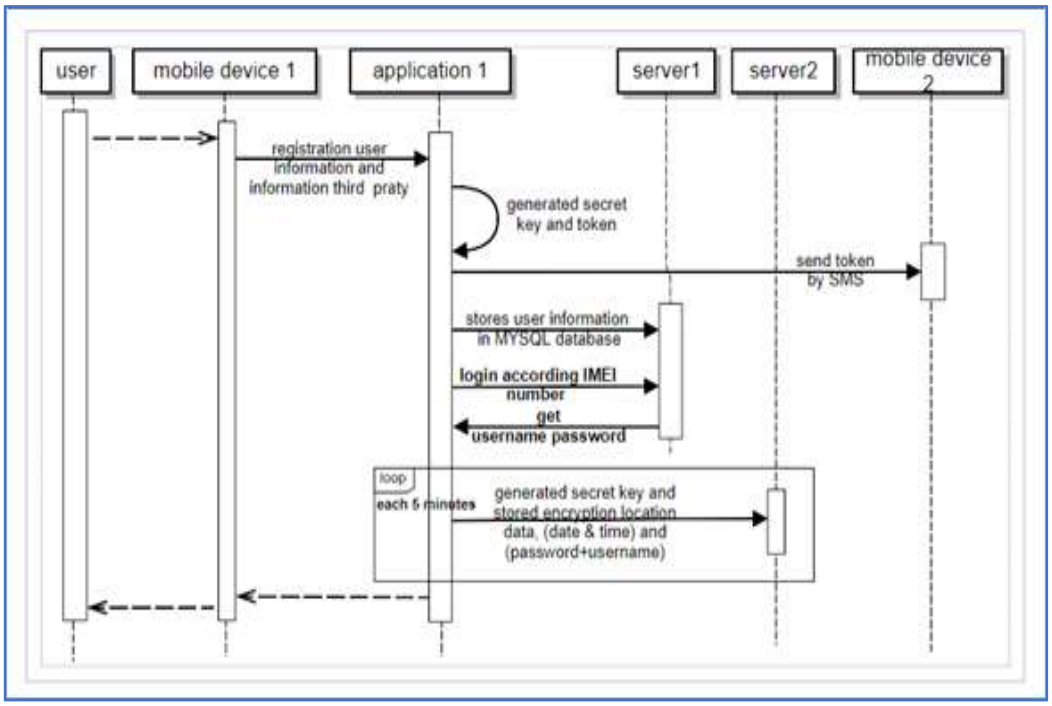


Figure -2 Sequence Diagram that allows the location to be tracked.

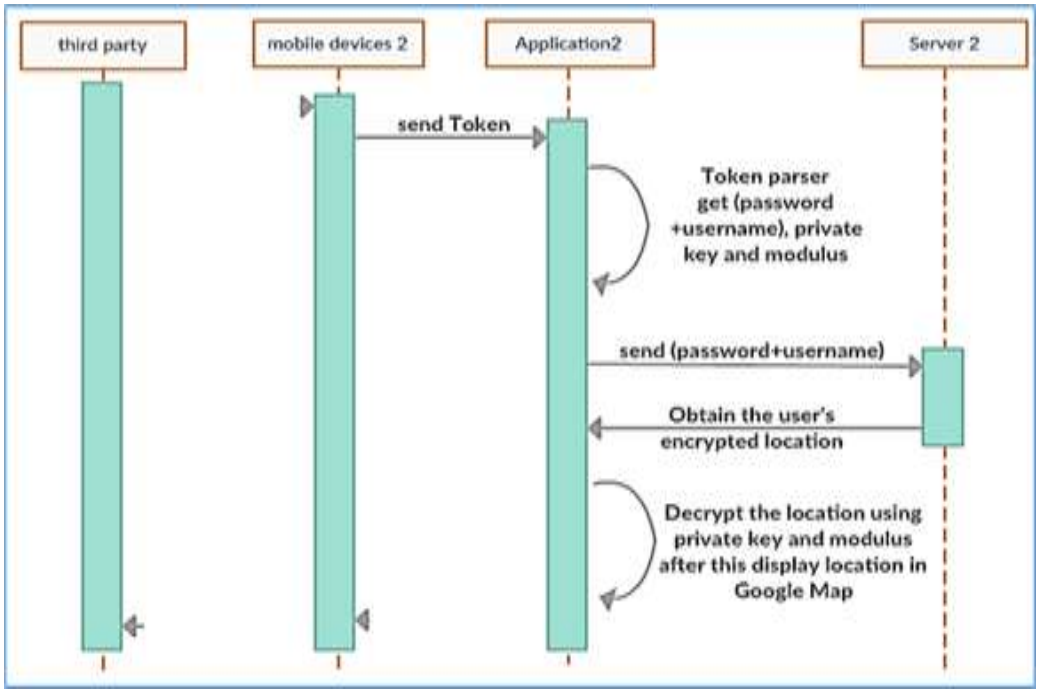


Figure 3: Sequence Diagram of third-party that allows Token parser to obtain user location.

4.1 Key Generation

The mobile device can encrypt (latitude and longitude) since the secret key is available to the device. The device creates the (public and private) keys according to RSA algorithm rules depending on the mobile device's IMEI number and SIM serial number. The encryption and decryption use different keys. The public key is used to encrypt the location data. This key does not need to be kept and is derived from a unique IMEI number. The private key is used to decrypt the location data. For security reasons, this key does not need to be kept. It can get the private key when analyzing the received token from the person tracked. The public key and private key were generated in Algorithm 1.

Algorithm (1): Description of the generated secret key.

Input: IMEI, SSN;
Output: public key, private key, modulus;
Begin
Step 1: Get the IMEI number and SIM serial number for your smartphone.
Step 2: Convert type IMEI and SIM serial number from String into BigInteger.
Step 3: Choose two prime numbers: convert number for the IMEI and SIM serial number into the prime number using the command nextProbablePrime ().
Step 4: Account multiply between subtracting one from IMEI prime (from step3) and subtract one from SIM serial number prime (from step3), the result put in variable type BigInteger name Phi.
Step 5: Account multiply between IMEI prime (from step3) and SIM serial number prime (from step3), the result put in a variable type BigInteger name modulus.
Step 6: Choose public key: public key equal SIM Serial Number prime (from step3).
Step 7: Private key computed by Inverse of Public Key.
End

4.2 Location Encryption/Decryption

The mobile application obtains the current position via a positioning technique such as a GPS network or cellular network. After the application gets the user's location (latitude and longitude), the mobile device encrypts this result and sends it to the remote server. The server cannot compute the encryption and decryption locations for the user's location. This paradigm protects and prevents the exposure of the user location. The user location encryption uses the public key. The mobile device allowed to be tracked generates the public/private key as indicated in the algorithm (1). The private key and modulus are sent to a third party. The third-party uses the private key and modulus for data decryption. The following steps have been taken to encrypt/decrypt at a user location by the RSA algorithm, as described in Algorithm (2).

Algorithm (2): Description of the encryption/decryption.

Input: public key, private key, modulus, m represents user location (latitude or longitude) type Double.
Output: cipher user location (E), plain text user location (D).
Begin
Step 1: Call an algorithm (1) that gets each from (public key, private key, modulus).
Step 2: Convert type m from Double into BigInteger.
Step 3: Encryption m according to the equations m.modPow(publicKey, modulus) or (m ^ public key mod modulus), the result put in a variable name E.
Step 4: Decryption according to the equations E.modPow(priavteKey, modulus) or (E ^ private key mod modulus), the result put in a variable name D.
End

4.3 Location Token phase

The token authentication allows third-parties to use their username, password, private key, and modulus after the token analysis. The token has been created on the user's mobile device; the user can send a token by SMS to a third party; the third party can access the user's location on the remote server. The JWT is a representation of the claim format, which is contained in the password+username, private key, and modulus parameters. That is using the payload structure (setIssuer(password+username), setAudience(modulus) and

setSubject(privateKey)), that will be used for a password with a username as an authentication code with a remote server thus retrieved user location encryption. This code includes Java syntax and consists of instructions which will be executed to create a token authentication:

```
compactJws = Jwts.builder()
. setIssuer (password+username.toString())
. setAudience (modulus.toString())
. setSubject (privateKey.toString())
. compact ();
```

5. Results

The experiment is introduced to provide the location privacy of each mobile device during two applications for a mobile device. The applications are implemented with a written program in the Java language on the Android Studio platform. The first application allows the user to register user and third-party information. The login is a process automatically done by an IMEI number through a technique that connects to a server (1) and identifies the name, username, and password. Figure 4 represents the registration and login process. The user and third-party information are stored on an external server (1); the server database has a MySQL database, illustrated in Figure 5.

(a) **(b)** **(c)**

Figure 4: Application interface **(a)** user information **(b)** third-party information **(c)** login according to IMEI number

Figure 5: MySQL database contains (user and third-party) information**.**

Actually, the user application completes the registration process immediately, generates the secret key by the Algorithm (1), and therefore will get the public key, private key, and modulus according to the RSA algorithm rules. Choose a real phone device that has the IMEI number (359435058919189) and SIM serial number (8996405440003317062), the secret key result illustrated in Table 1.

Table 1: Key generation according to IMEI and SIM Serial Number

Name	Contain number
Prime IMEI	359535058919213
Prime SIM Serial Number	8996405440003317073
Modulus	323362351938872062604791433062354 9
Public key	8996405440003317073
Private key	4861224567549357840805204340840 17

Each mobile device that generates the token has all the information for secret keys; the token is derived from (password + username), modulus, and private key. The token can be distributed by SMS message. A third party was allowed to track a mobile device's location. At any time, the tokens are revoked and newly configured by changing the user account (username and password). The token is used when the third-party wants to access the remote server (2). The token was parsed into components (password + username, private key, and modulus). The application must verify (password + username) authorization for every HTTP

transaction to fetch encrypt location data from the server (2), and the result is presented to create a token according to the following paragraph (Token phase):

eyJhbGciOiJub25lIn0.eyJpc3MiOiJhbGkxMTFhbGkgbmFmYWEiLCJhdWQiOiIzMjMzNjIzNTE5Mzg4NzIwNjI2MDQ3OTE0MzMwNjIzNTQ5Iiwic3ViIjoiNDg2MTIyNDU2NzU0OTM1Nzg0MDgwNTIwNDM0MDg0MDE3In0.

The application is allowed to track the user's location on the mobile device. These application processes are running in a background service using the Android service. Continue to update current location data every 5 minutes and send encrypted location data according to Algorithm (2) on the server (server 2). The application was implemented at 4:19 pm on 13th July, 2018. The user's location (latitude = 33.2474611, longitude = 44.3624758) was obtained. The results were encrypted as follows: Table 2, while Figure 6 indicates encrypted location data on a remote server (server 2).

Table 2: Encryption of Location Data

Location	Encryption
Latitude	**24956121716840661137950085177909 38**
longitude	**12753525282562592125905829054573 69**

The second application of the mobile device, after obtaining the token from the user and allowing him to track the coordinates of his position, performed the token analysis by (Jwts.parser()). The result (jwt.getBody()) was put into the matrix of the string type being split on the basis of the comma. Getting three elements in the matrix, the first of the password+username, the second of the modulus, and the three of the private keys. After the query process for the location data according to the password+username of the server (2), the location data is decrypted according to modulus and private key, after getting latitude and longitude, and then represented in the Google maps as shown in Figure 7.

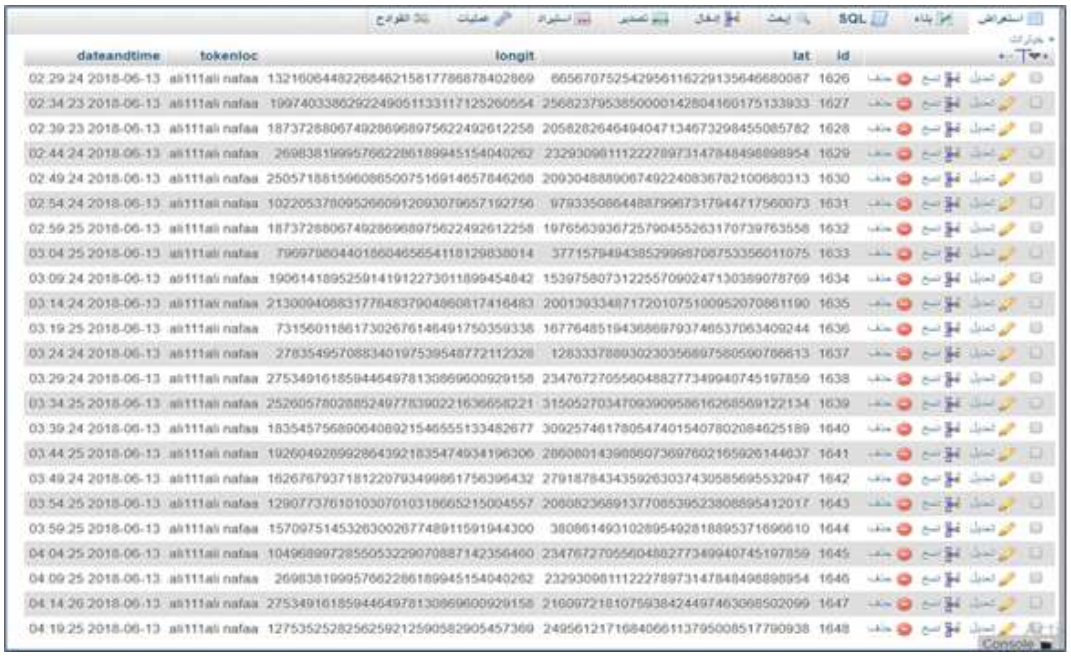
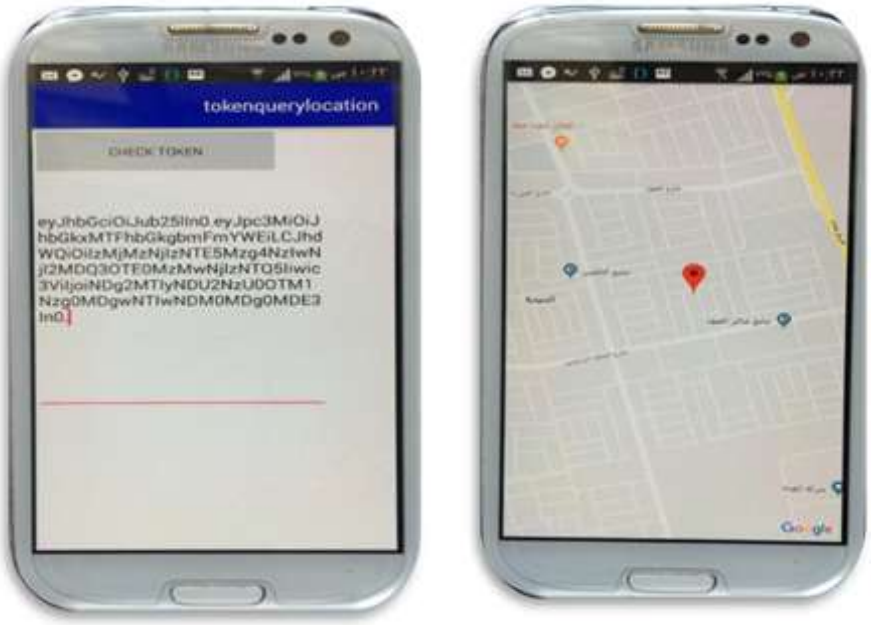


Figure 6: Stored Encryption Location data with date and time.



(a) **(b)**

Figure 7: Second application: **(a)** Interface of entering token and **(b)** Result for location data.

6. Conclusions

The techniques used in this paper attempt to improve location privacy via a mobile application by encrypting data on a remote server with an authentication token, achieving mutual authentication on each mobile device, and enabling user concealment on all the Android mobile phones with two remote servers. The low computational cost and the fact that the user can change his username and password at any time by contacting the remote server means that the application uses inexpensive symmetric keys derived from IMEI and SIM serial numbers to encrypt data. In the future, the token content will be established between the mobile device of the user and the remote server. Privacy can be used by two cryptographic algorithms with a dual asymmetric key. It uses a different kind of server database management system like Oracle/SQL Server to establish the more powerful main central database.

Acknowledgements

I would like to express my gratitude to everyone who assisted me in carrying out this research, particularly Mustansiriyah University, College of Science, and my colleagues in the Department of Computer Science.

References

[1] A. Albelaihy and J. Cazalas, "A Survey of The Current Trends of Privacy Techniques Employed In Protecting The Location Privacy of Users In LBSs" *Anti-Cyber Crimes (ICACC), 2nd International Conference on IEEE*, 2017.

[2] A. Hadi and C. Jonathan, "Improved Recommender for Location Privacy Preferences" *Computer and Information Science*, Vol. 8, No. 4, 2015.

[3] D. Fernández-Pacheco, J. Molina-Martínez, A. Ruiz-Canales and M. Jiménez, "A new mobile application for maintenance tasks in photovoltaic installations by using GPS data" *Energy Conversion and Management*, Vol. 57, pp. 79–85, 2012.

[4] K. Puttaswamy, S. Wang, T. Steinbauer, D. Agrawal, A. El Abbadi, C. Kruegel and B. Zhao, "Preserving Location Privacy in Geosocial Applications" *IEEE Transactions on Mobile Computing*, Vol. 13, pp. 159 – 173, 2014 .

[5] S. Anju and J. Jasmine, "Location Based Service Applications to secure locations with dual encryption" *International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) IEEE,* 2015. DOI: 10.1109/ICIIECS.2015.7193061.

[6] T. Ritu and M. Dilip, "SecTrans: Enhancing user privacy on Android Platform" *International Conference on Nascent Technologies in Engineering (ICNTE) IEEE*, 2017. DOI: 10.1109/ICNTE.2017.7947884

[7] O. Yuna, J. Kangsoo and P. Seog "A privacy preserving technique to prevent sensitive behavior exposure in semantic location-based service" *Procedia Computer Science*, Vol. 35, pp. 318 – 327, 2014. https://doi.org/10.1016/j.procs.2014.08.112.

[8] C. Cherng and A. Masayoshi, "A user sensitive privacy-preserving location sharing system in mobile social networks", *Procedia Computer Science*, Vol. 35, pp. 1692-1701, 2014.

[9] S. Nan, Y. Jun, Y. Ke, F. Chuan and J. Chunfu, "An efficient and privacy-preserving location sharing mechanism", *Computer Standards & Interfaces*, Vol. 44, pp. 102-109, 2016.

[10] H. Yan, C. Zhipeng and B. G. Anu, "Search Locations Safely and Accurately: A Location Privacy Protection Algorithm with Accurate Service" *Network and Computer Applications*, Vol. 103, pp. 146-156, Feb 2018.

[11] S. Balram, S. Ravindar and C. Sanjay, "Dual Modulus RSA based on Jordan-Totient function" *Procedia Technology*, Vol. 24, pp. 1581-1586, 2016.

[12] S. Santanu and M. Subhamoy," Cryptanalysis of RSA with two decryption exponents" *Information Processing Letters*, Vol. 110, pp. 178–181, 2010.

[13] C. Joaquin, J. Eun-Sung, K. Rajkumar, R. Nageswara, F. Ian, C. Russ and O. Henry, "Advance Reservation Access Control Using Software-Defined Networking and Tokens" *Future Generation Computer Systems*, 2017. http://dx.doi.org/10.1016/j.future.2017.03.010 .

[14] P. Mestre, R. Madureira, P. Melo-Pinto, and C. Serodio, "Securing RESTful Web Services using Multiple JSON Web Tokens" *Proceedings of the World Congress on Engineering*, Vol. I, 2017.

[15] S. A. Ahmed, "Retrieving Mobile Phone Information Based on Digital Search Tree", *eijs*, Vol. 62, No. 10, pp. 3733-3743, Oct. 2021.

[16] K. S. Noori and A. A. Fahad, "Monitoring and Enhancement of Mobile System Performance", *eijs*, Vol. 61, No. 9, pp. 2418-2425, Sep. 2020.