International Journal for Rapid Research in Engineering Technology & Applied Science
ISSN (Online): 2455-4723
Vol 2 Issue 7 August 2016

Data Encryption Model using Geo-Location for Mobile Devices

Shailesh Raut *[1], Megha Singh[2] , Dr. Rekha Rathore[3]
*[1]Research Scholar, CIIT College Indore, M.P, India.
[2]Assistant Professor, CIIT College Indore, M.P, India.
*Department of Computer Science & Engineering
*[1]shaileshr124@gmail.com

Abstract

Secure communication and authentication is possible through encryption of data and verification . Most of the existing data encryption techniques are location-independent. Data encrypted with such techniques cannot restrict the location and time of data decryption. The concept of "Geoencryption and Authentication " or " geo location-based encryption and authentication " is being developed for such a purpose. This paper proposes a survey between different technique to which is related to Geo location based Networks. The purpose of Geo location based network is to secure system from disparate user, so that the right user can take the right decision for the security of the items which are relevant for them. In this paper we are comparing different techniques on different aspects of systems which is used in Geo Location based network.

Keywords: Geo encryption, Location Based Encryption, Data Encryption, , location based services (LBS), GPS, AES

1. INTRODUCTION

It is an enhancement to traditional encryption that makes use of physical location or time as a mean to produce additional security and security features. It allows data to be encrypted for a specific place or broad geographic area, and supports constraints in time as well as space. It provides full protection against attempts to bypass the location feature. Depending on the Implementation, it can also provide strong protection against location spoofing. The Geoencryption algorithm does not replace any of the conventional cryptographic algorithms, but instead adds an additional layer of security. The capability has tremendous potential benefits to applications such as location-based services, managing secure data and digital movie distribution where controlling access is main concern [2].

Location information has many properties good for encryption and authentication. Logan Scott, Dorothy Denning [1] developed the idea of Geoencryption and its use in digital film distribution. In order to meet the demand of mobile users, Hsien-Chou Liao and Yun-Hsiang Chao introduced a location dependent approach called Location Dependent data Encryption Algorithm (LDEA) [2]. This protocol is not strong enough because they are using the static location which is latitude/longitude coordinates of mobile node and they are using the static tolerance distance to overcome the inaccuracy and inconsistent of GPS receiver.

Here are a few best practices when handling geolocation services. Not only do they increase the confidence of your users, but they prevent future loss of reputation, revenue, and other hassles that might befall you, the service provider:

Use the least precise measurement necessary. If your application merely needs to know the city in which the user is currently located, only request this degree of accuracy from the location API. Where “coarse” permissions are available, use these.

Discard data after use. Unless data is explicitly needed over an extended period of time, this data should be discarded. This means that either logging subsystems should not receive the data in the first place or they should be immediately expunged. Some companies take the approach of overwriting past positional data immediately when an update is received

Keep data anonymous. If data does need to be retained, ensure that it cannot be associated with other personal data. This includes ensuring that cookies are not used for tracking mechanisms and that requests for location data go over secure channels.

Indicate when tracking is enabled. Users should be visually notified that their whereabouts are being recorded. Systems such as the iPhone and Android have dialogs to inform users about this explicitly, either on use or on install. On platforms that don't have this capability, be sure to notify the user yourself.

Use an opt-in model. All software using Geo Location data should have this functionality disabled until explicit confirmation from the user. Provide an interface to disable this at any time. Wherever possible, give the user the ability to specify their location manually, as with a ZIP code.

Have a privacy policy. Be able to provide guarantees to your users about how you use their positional data, and what you'll do with it if it's requested in a civil or criminal case. It's important to have this ready before a request like this arrives.

Do not share geolocation data with other users or services. Allowing users to access other users' positional data is very risky territory. Avoid this technique if at all possible.

Familiarize yourself with local laws. Different countries and states have different restrictions and requirements involving tracking information. Ensure that you're aware of the ones that apply to your target regions.

2. RELATED WORK

D. E. Denning and P.F. MacDoran[1] providing how location based authentication has so many benefits. By applying geodetic location in grounding cyberspace provide a well authentic environment. Where, geodetic location (latitude, longitude) has to decide whether a person is login from approved given location, as it calculated by location signature.

Hatem Hamad and Souhir Elkourd [3] proposed a protocol, which makes the use of dynamic location of mobile node, and dynamic tolerance distance which makes it very strong to attack. However most of them are not strong enough against tampering. If the device is vulnerable to tampering, it may be possible to an advisory to modify it and bypass the location check[5]. To protect against tampering and spoofing, a signal authentication protocol, Timed Efficient Stream Loss-tolerant Authentication (TESLA) is designed [4].Since then many efforts have been done to complete the above idea and fix its defects [5,6,7]. To Overcome these defects, Rohollahkarimi and Mohammad Kalantari[9] present a modified Geo protocol and improve its efficiency and applicability. Although it is possible to provide security features such as authentication, integrity and confidentiality. So security measures need to be upgraded continuously. What is secure today may not be secure tomorrow. There will always be malicious users trying to exploit and find new holes in a network. Therefore, we need to look into the future so that we are able to face these security issues before they cause damage. This paper revives contemporary location based algorithms and protocols of mobile users.

Geodetic location authentication can be continuously performs, so that connection cannot be hijacked. It also has function of electronic notary. As location signature cannot be stolen. Geodetic location provides how user performs sensitive operation, only in authorized location. It traces the exact location of intruder/attacker from where it done those malicious activities. To accomplish all of these it represent a technique called Cyberlocator, a GPS based technology.

D. Jaros et al. [2], generalize that there are great challenges to provide location authentication especially for those area where GPS signal are unavailable.

So here, this paper introduces a technology background called active infrastructure that has further two location based authentication techniques first is remote authentication and second is local authentication. Here IQRF, Bluetooth as wireless technologies.

S. D. Ghogare et al. [3] introduces a new concept called location based authentication in information security. As traditional method to provide authentication is

. Something you know : password

. Something you have: token

. Something you are: biometric

But all of them has so many drawbacks that how a password get easily guessable, how cards may be stolen, and also sometimes biometric devices get corrupted to identify someone's identity.

So here to apply a new concept Geo-location based authentication by taking multiple authentication techniques and merge into a one single model. Which provide a high level of security so that data can be access only in defined premises. And those multiple techniques are location, biometric, encryption where using AES algorithm does encryption.

N. Gholap et al.[4] represent a location based authentication encryption scheme through a company can securely transfer its data whose branches at two location and centre office where server is located. Thus only legitimate user access or transfer the data from approved location.

AES(Advanced Encryption Standard) is used to implement the encryption scheme and GPS technique is used to track the recipient so that decryption is to be done in right location.

W. Jansen and V. Korolev [5] provide location based authentication on the basis of new concept called policy beacon for mobile handheld devices. As here location treated on proximity basis. As in mobile handheld devices like cell phones, PDA there is so many risks.

3. EXISTING WORK:

3.1 Basic Geo encryption Model

The term "location based encryption" of "Geo encryption" is used to refer any method of encryption wherein the cipher text can only be decrypted at a specified location. If an attempt to decrypt data at another location, the decryption process fails and reveals no information about the plaintext. Making key depended on target geographic position is an applicable way to strengthen its safety in real time applications.

Figure 1 depicts the basic Geoencryption model [1]. Geo-encryption was based on the traditional encryption system and communication protocol. For the sender, the data was encrypted according to the expected PVT (position, velocity and time) of the receiver. A PVT-to-GeoLock mapping function was used to get the GeoLock key. GeoLock key was performed bitwise exclusive-OR with a generated random key to get a GeoLock session key. This GeoLock session key was then transmitted to the receiver by using asymmetric encryption.

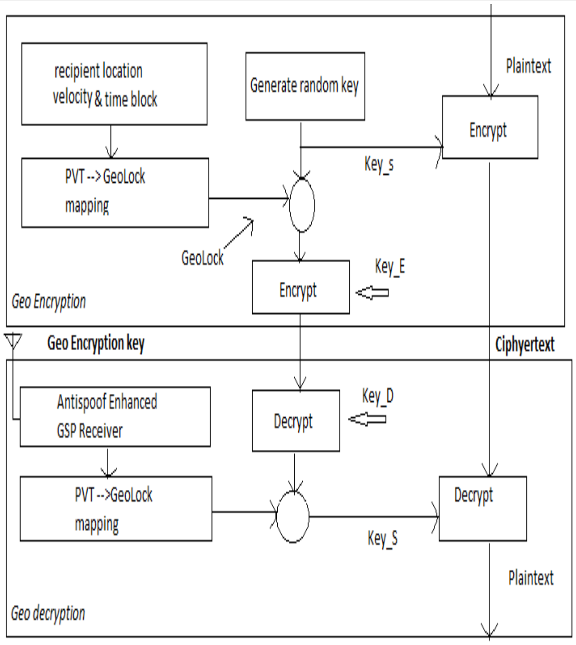


Figure 1: Existing System for Geo Location Encryption

For the receiver, an anti-proof GPS receiver was used to acquire the PVT data. Then the same PVT-to-Geo Lock mapping function was used to get the Geo Lock key. The key was performing exclusive –OR operation with received Geo Lock session key to get the final session. The final session was used to decrypt the cipher text.

3.2 Basic Geo-location based authentication:

Traditional GPS receivers are not appropriate for intruder because the coordinate generated by them sometime knows location authentication. And there a no way of knowing is really calculated by GPS receiver or by someone. But cyber locator sensor removes this problem by implemented differential GPS(DGPS) technique that has access for both clients as well as of its own GPS signal. The location based authentication in building which operates separate facilities.

4. PROPOSED WORK:

Along with the Symmetric keys involved in Encryption algorithm. We are implementing two more keys.

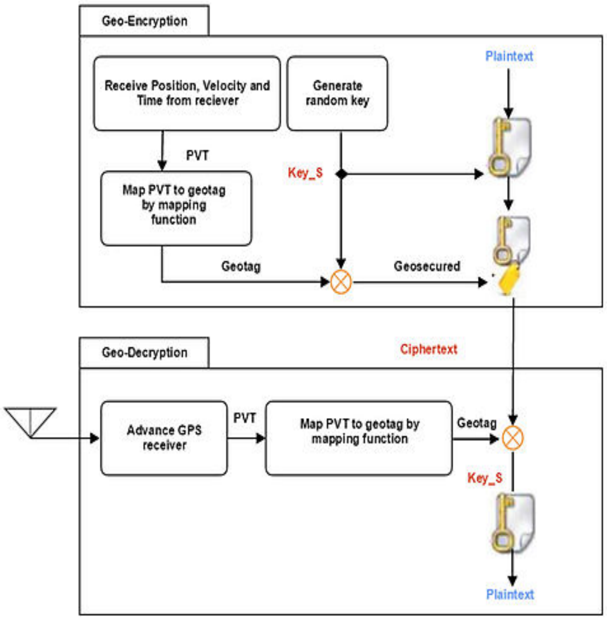


Figure 4: Proposed System for Geo Location Encryption and Authentication

Geo location key: It will check the location of the sender and the receiver i.e the latitude and the longitude positions of both and then only the message will be decrypted. For eg. If the sender is at (x,y) location and the receiver is at (a,b) location then we will use a hash function to convert the values of (x,y) and (a,b) into an integer and multiply it with the formula for encryption

Suppose hash [(x,y)] = p And hash [(a,b)] = q Then, c = [me (mod n)] × (p / q) And at the receiver side we will implement

$$c = [me \ (\text{mod } n)] \times (q / p)$$

Time Key: This key will be optional. This will check the time barrier. For eg, if it takes 30 mins for the data to travel from dest1 to dest2 then the message cannot be decrypted before 30 mins. Due to network delay involved in real time systems, un-synchronized clocks and data traffic, this key is kept optional

Each platform treats GeoLocation services differently, with different methods of requesting user permission, ranging from asking every launch of the application to leaving notification up to the developer.

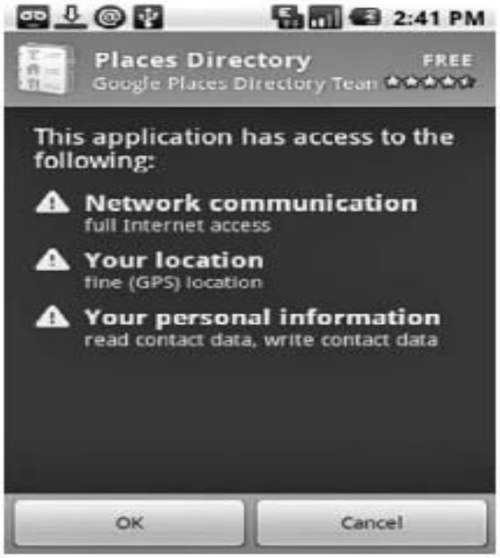
As with most services on Android, permission to use the GeoLocation features is requested via the program manifest and is granted by the user at install time. Either coarse or fine precision can be requested, using the ACCESS_COARSE_LOCATION (for cell triangulation or Wi-Fi) or ACCESS_FINE_LOCATION (GPS) permission. These permissions are requested and controlled separately.

Find Location in Android Using the Location Manager

In Android Location package provides the Location Manager service, which can be called to return both geographic location and current bearing, using the internal compass. In Figure 4 provides an example of using the Location Manager Service in Android.

- locationManager=(LocationManager)
- getSystemService(Context.LOCATION_SERVICE);
- Criteria mycriteria=new Criteria();
- mycriteria.setAccuracy(Criteria.ACCURACY_FINE);
- mycriteria.setBearingRequired(true);
- String myprovider=
- locationManager.getBestProvider(mycriteria, true);
- Location mylocation=locationManager.

  getLastKnownLocation(myprovider);



This application has access to the following:

Network communication
full Internet access

Your location
fine (GPS) location

Your personal information
read contact data, write contact data

Figure 4: Location Manager in Android

5. CONCLUSION:

Geo-location is a secured and full proof way to authenticate users or devices.. There is a need of more robust techniques that can be used to find the location efficiently. The survey provided a brief insight to the existing location based authentication techniques. Finally, the survey will be helpful to researchers to build up a startup platform in the field of geo-location based authentication. This paper explains the importance of location based system, corresponding security and Authentication.

REFERENCES

[1] S U Nimbhorkar, Smruti P patil, "A Survey on Location Based Authentication Protocols for Mobile Devices", IJCSN, pp. 44-48, 2013.

[2] Ku, We Shinn, "Geo-Store: A Framework for Supporting Semantics-Enabled Location-Based Services", IEEE Conference, pp. 35-43, 2013.

[3] Xinxin Zhao, Lingjun Li, Guoliang Xue, "Checking in without Worries: Location Privacy in Location Based Social Networks", IEEE Conference, pp. 3003-3011, 2013.

[4] Asif Hasan and Neeraj Sharma, "A new Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)", IEEE international Conference, pp. 310-313,

[5] Ayesha Khan, "Geolocation Based RSA encryption Techniques", ISSN, 2013, pp. 17-20.

[6] Rohollah karimi and Mohammad kalantari, "Enhancing security and confidentiality in location based data encryption algiritms", IEEE Conference, pp. 30-35, 2011.

[7] V Rajeswari, V Murali and A.V.S. Anil, "A naval approach to identify Geo-Encryption with GPS and Diffrent Parameteers (Location and Time)", IJCSIT, pp. 4917-4919, 2012.

[8] Yan Zhu, Di Ma, Dijiang Huang, Changjun, "Enabling Secure Location- Based Sevices in Mobile Cloud Computing", ACM, pp. 27-32, 2013.

[9] Rohollah karimi and Mohammad kalantari, "Enhancing security and confidentiality on mobile devices by location-based data encryption", IEEE international Conference, pp. 241-245, 2011.

[10] Guojun Wang, Tao Peng,, QinLiu,, "Privacy Preserving for Location-Based Services Using Location Transformation", Springer International Publisher, pp. 14-28.

[11] Ganasan S P "An asymmetric authentication protocol for mobile devices using elliptic curve cryptography :, IEEE Conference, pp. 107-109, 2010.

[12]D. Jaros, R. Kuchta and R. Vrba, “The Location-based Authentication with The Active Infrastructure”, In The Sixth International Conference on Internet and Web Applications and Services (ICIW 2011), Mar. 20- 25, 2011, St. Maarten, The Netherlands Antilles, pp. 228–230.

[13] Shraddha D. Ghogare, Swati P. Jadhav, Ankita R. Chadha and Hima C. Patil, “location based authentication: A new approach towards providing security” , International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012 ISSN 2250-3153.

[14] Nisha Gholap, Prof S. S. Das, and Prof Londhe D, “Location And Authentication Based Encryption Scheme Application Design For Mobile Device”, International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 4, ISSN: 2278-0181, April - 2013

[15] W. Jansen and V. Korolev, “A Location-Based Mechanism for Mobile Device Security”, In Proceedings of the 2009 WRI World Congress on Computer Science and Information Engineering (CSIE '09), vol. 1, pp. 99–104.

[16] W. Jansen, V. Korolev, S. Gavrila, T. Heute, C. Séveillac, “A Framework for Multimode Authentication: Overview and Implementation Guide,” NISTIR 7046, The National Institute of Standards and Technology, August 2003.

[17] Hsien-Chou Liao and Yun-Hsiang Chao, “A New Data Encryption Algorithm Based on the Location of Mobile Users” Department of Computer Science and Information Engineering, Chaoyang University of Technology, 168 Jifong E. Rd., Wufeng Township Taichung County, 41349, Taiwan (R.O.C.)Information Technology Journal 7 (1): 63-69, 2008 ISSN 1812, 2008.