Secure Location and Content Sharing in OSN

[1]Appidi Haritha, [2]Dr B.V.Seshu kumari
[1]M-Tech, [2]Associate professor
Dept of IT (CNIS), VNRVJIET, Hyderabad

Abstract: *In social networking sites it is very a common task that shares the user locations to other friends. In this process there are two types of the situations involved, one is share the location to another user and another is share the location to the group of people in social groups. Location sharing feature in the groups in current systems is not much useful to the users, because of the sharing location in the in group just like a normal micro blog. This is the reason in our location sharing system when user shares location into the groups it won't share like micro blog, it will available to the others all the time. User will get the remaining user's locations within the group by the query request. In other part this paper is security of user location. For this we are proposing AORE notation(Advance Order Retrievable Encryption) which will secure the user co-ordinates and the content information using two different encryption algorithms. For Co-ordinates data we use AES encryption and for content information we use DES encryption.*

Keywords: *Location Share, AORE, location query, and location security*

1. Introduction

In chat oriented social networking sites like whatsapp and facebook messengers etc kind of application provide chat communication between the users and media sharing services. In these social networking sites also have a common task that shares the user locations to other friends using Google Map service or IOS map services etc. When user share location in the chat it has the co-ordinate information, means latitude and longitude data which is very important to the track our location and another optional services [1] [2] like write something about that location like *this is my home,my office* etc. So when user sharing location in chats we note that there is two types of the data we need to process, one is location co-ordinate and another one is content information. In social network sites sharing service process there are two types of the situations involved, one is share the location to another user and another is share the location to the group of people in social groups. Location sharing feature in the groups in latest apps [3][4][5] is not much useful to the users, because of the when we share location in the groups about an event or something the location sharing data will post like a normal message, if group members did any chat that location sharing post will not visible to the users easily. So the process of the location sharing in the current apps are not much useful to the user. For this in our paper we are enhancing this concept to the server client architecture model.In this model when user share any location to the users in the groups it will save permanent in the server machine and when the user raise any query Q, here Q means query which requesting the locations of the group members in particular distance. And we are providing the security service to the location data ant content of the location with two different security services.

The rest of this paper organized with AORE architecture, implementation, results conclusion, future work and references .

2. AORE Architecture

In proposed work, we develop a sharing location based in online social network which can share the location securely in the social chat groups. Our database server honest but curious. So we need to focus the security issues in the server side. In the Fig 1.user can be any online social network user who share the location in the groups to the group members through the server. Server will collect the user location co-ordinates and content information. Server will encrypt the location data with AES algorithm with (d+1) x (d+1) matrix key. Content information will encrypt by the DES encryption Separately.

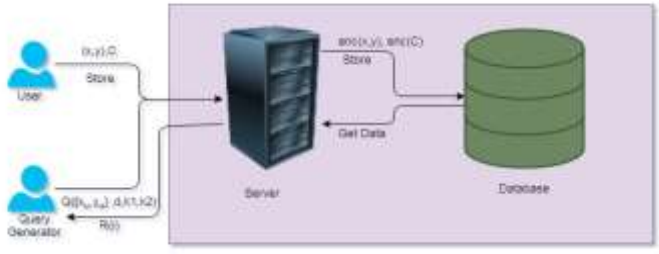


Fig 1:AORE Architecture

When user raise query for user locations then query generation process will execute. In this module system will collect the current location of the user for distance calculation, and collect the distance that how much user can be travel and visit.

3.CONTRIBUTION

3.1. AES:

In the existing work, the security is lacking. So, to enhance the security we have implemented AES algorithm. AES comes under the category of Symmetric cryptography algorithms. It uses only one key i.e., secret key for both the encryption and decryption. Here, in this context, 128 bit AES is used. AES consists of another bits – 192,256. 128 bit AES consists of 10 rounds. Most common key used is 128 bits. We have implemented AES because, it is very fast and it can easily be implemented in Java.Working of AES is based on the principle of ‘Substitution – Permutation network’. AES executes its operations on bytes rather than bits. 128 bits of data are treated as 16 bytes (1 byte = 8 bits). In general, the encryption process consists of four phases - Byte Substitution, Shift rows, Mix columns and Add round key process. Decryption process is the reverse process of encryption. Decryption possesses Add round key, Mix columns, Shift rows and Byte substitution.

3.2.DES:

The DES algorithm is very popular security algorithm. It's a symmetric algorithm, that meansthe same keys are used for both encrypt/decrypt sensitive data. Here the key length is 8 byte (64 bit). So, to encrypt/decrypt data, the DES algorithm uses an 8-byte key, but 1 byte (8 bit) for parity checking. This is a block cipher algorithm — So, the data block size of DES algorithm is 64 bit.For encryption/decryption of data, the DES algorithm uses the Feistel structure. Hence it uses some rounds to encrypt/decrypt data. Despite data block size is 64 bit, the number of rounds will be 16 rounds. So, it will use different subkeys for each round and the number of subkeys will be 16 subkeys.

4. Implementation

In the implementation there is two parts. One part the data collection, encryption and storage and another part is data retrieval. In the storage part we collect the group G member’s *m* location sharing the data in to the database with content and after the encryption. Here we are collecting two important data, first one location co-ordinates like latitude and longitude values *(x,y)* and another one is content information. If we have location co-ordinates of user, we can’t judge the this information properly without content because of co-ordinates may be home address or office address or visited mall address. So here we need to take some importance to the content information also not only for co-ordinates. Co-ordinates data here we are encrypt [6] this information using AES encryption notation. And content information not encrypting same algorithm using separate DES algorithm we are using for encrypting the data.In our implementation another important module is query generation. When user raise query for user locations then query generation process will execute. In this module system will collect the current location of the user for distance calculation, and collect the distance that how much user can be travel and visit.

Query Generation = Q([x_u, y_u], d, k1, k2)

Where,

- Q is query of the user
- x_u , y_u current location of the query generator.
- d is the distance which user wants to travel.
- k1 symmetric key 1 for location data
- k2 symmetric key 2 for content data

Server will encrypt the location data with AES algorithm with (d+1) x (d+1) matrix key. Here d is nothing but dimensions. We are using 2 dimension data so key should be 3x3 matrix for location data encryption. Content information will encrypt by the DES encryption Separately.

Algorithm 1: AORE w.r.to location retrieval

In algorithm 1, we assume m members are present in the group G, collect the all locations of m and decrypt the locations with symmetric key SKG, and calculated the distance between query generator location and the m locations. For distance calculation we are using Euclidian distance algorithm

Algorithm 1:

```
Input : User location(x,y),Query location( )

Output: User's Query data Q.

Initialization :

i. Let G => G(u), where u is users in group.

ii. User set location, defined current  location x,y

iii. SKG <= Symmetric key(d+1) (d+1) invertible matrix.(Secret sharing to Group members).

Let   $x_q$,$y_q$ Є G, distance d (nearby results)

   Q=($x_q$,$y_q$ );

    C<=Q Gen(SKG,Q,dist); // Encrypted Query

Compute distance,

    For each m:G

$cmp_0$=m(x,y);

 $cmp_1$=mi($x_i$,$y_i$ ); //Decrypt with SKG

            $Dist_i$= cmp( $cmp_0$, $cmp_1$);

            If dist>$dist_i$

 $Cmp_1$=>R;

            end if;

end for;

Sort(R);
```

Algorithm 2: Euclidean distance

5. Results

```
Input: x,y, $x^1$, $y^1$

Output: Distance d

Initialization:

I. theta=y- $y_p$ ;

II. x,y - User Location id’d

III. $x_p$, $y_p$ – POI co-ordinates

Distance d= sin(deg_to_rad (x))*sindeg_to_rad ( $x_p$))+cos(deg_to_rad (y))*cos

(deg_to_rad( $y_p$))*cos(deg_to_rad(theta))

d=arc cosine(d);

d=rad_to_deg(d);

Calculate deg_to_rad(deg)

      return(deg*Π/180.0);

Calculate rad_to_deg(double rad)

      return(rad*180/Π);

return d;
```

We develop our application in the java based web application. We use windows operating system having 8 GB Ram, 500 GB HDD and i5 processor. We compare the results in terms of the computation cost between the AES and DES algorithm. We got best performance to the AES comparing with DES.

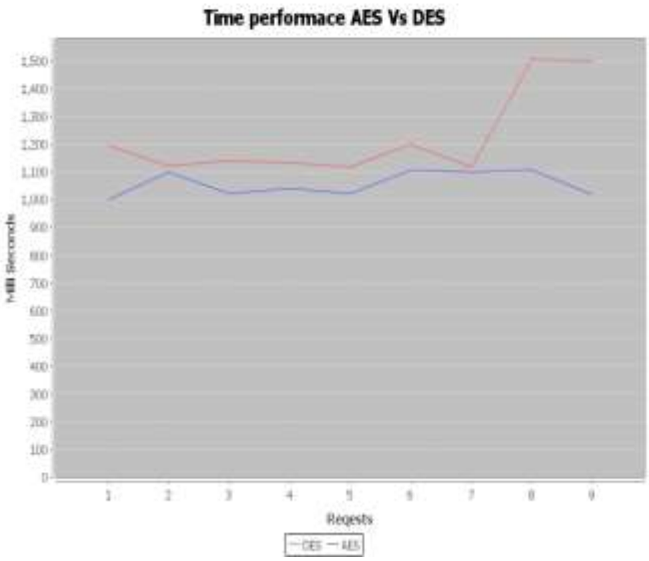
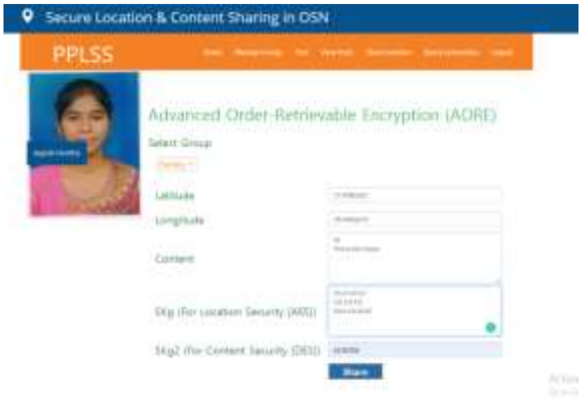


Fig 2: Performance Evaluation

Generation of the security keys in our application.



Advanced Order-Retrievable Encryption (AORE)

Select Group

Latitude

Longitude

Content

Skg (For Location Security (AES))

Skg2 (For Content Security (DES))

Share

6. Literature Survey

Location sharing to the users with privacy preserving concept is achieved by proposing concept of Identity based broadcast encryption (IBBE) by the Michael et al [7]. This is a three tier architecture. Here mainly service provider will maintain the users location data, user location information will store in the SP in the form of the encryption. Mokbel et al. proposed concept a new framework called Casper [5] for secure location sharing service, in this they have taken traditional topic in anonymization topic. Anonymization topic will helps to hide or blur the information in a certain useful level.Puttaswamy et al. proposed a concept called LocX [8], in this survey also they proposed three layer architecture but in the different way. Users, Proxy server, and Data Server. Here there is no middle server, it is like hierarchical model. User should get the data from the both servers simultaneously. In this survey they noticed importance of the location data and content data. In this data will store after the Identity based encryption.

7. Conclusion

Location sharing feature in the groups in latest apps is not much useful to the users, because of the when we share location in the groups about an event or something the location sharing data will post like a normal message, if group members did any chat that location sharing post will not visible to the users easily. We proposed a location sharing service with AORE notation. And we achieved prosperous results in terms of the security.

8. Future Work

In the future work,

- While requesting the query generation of query generator, she/he needs to share the current location to the server. So we need to focus of the secure the location of query generator.
- In our paper we are only focus about the location sharing concept in the social network groups, we need to survey on the security issues in the location sharing personally.

9. References

[1] L. Siksnys, J. R. Thomsen, S. Saltenis, and M. L. Yiu, “Private and flexible proximity detection in mobile social networks,” in Proceedings of the International Conference on Mobile Data Management, 2010.

[2] L. Siksnys, J. R. Thomsen, S. Saltenis, M. L. Yiu, and O. Andersen, “A location privacy aware friend locator,” in Proceedings of the International Symposium on Spatial and Temporal Databases, 2009.

[3] C.-Y. Chow, M. F. Mokbel, and W. G. Aref, “Casper*: Query processing for location services without compromising privacy,” ACM Transactions on Database Systems, vol. 34, no. 4, pp. 1–48, 2009.

[4] M. Gruteser and D. Grunwald, “Anonymous usage of location-based services through spatial and temporal cloaking,” in Proceedings of the ACM International Conference on Mobile Systems, Applications, and Services, 2003.

[5] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, “The new casper: Query processing for location services withoutcompromising privacy,” in Proceedings of the International Conference on Very Large Data Bases, 2006.

[6] W. K. Wong, D. W.-L. Cheung, B. Kao, and N. Mamoulis, “Secure kNN computation on encrypted databases,” in Proceedings of the ACM International Conference on Management of Data, 2009.

[7] M. Herrmann, A. Rial, C. Diaz, and B. Preneel, “Practical privacypreserving location-sharing based services with aggregate statistics,” in Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks, 2014, pp. 87–98.

[8] [8] K. P. N. Puttaswamy et al., "Preserving Location Privacy in Geosocial Applications," in IEEE Transactions on Mobile Computing, vol. 13, no. 1, pp. 159-173, Jan. 2014. doi: 10.1109/TMC.2012.247