MULTI PARTY GEO ACCESS CONTROL

Pranshu Aggarwal[1], Himshikha Suhag[2] Rahul Bansal[3],
Purnank Jain[5], Dharmender Saini[5]
Department of Computer Science Engineering, GGSIP University, Delhi, India

ABSTRACT

Geo-encryption provides users with location based encryption and subsequent decryption of data. However, a single party access to data is less secure than encrypting the data and distributing it to multiple parties. With multiple party access data becomes more secure due to its distribution amongst multiple parties. This paper combines the concept of geo-encryption and multi-party control to provide an integrated system bridging the gap between the shortcomings of the two. Geo-fencing and a newly, self- designed data encryption algorithm (Trans Modulo Substitution Algorithm) has been used for geo- encryption of the data. The encrypted data is then distributed to multiple parties through a sequencing mechanism.

KEYWORDS: *Geo-encryption, multi-party access, geo-fencing, encryption algorithm, Trans Modulo Substitution Algorithm*

I. INTRODUCTION

With the increasing popularity of the mobile devices, location based service (LBS) is becoming vital. Systems use LBS to provide aid to users according to their location. LBS is an information service which finds its use in vehicle tracking, social networking, mobile commerce, etc. LBS in the field of data encryption has particularly been useful and thus, has given rise to Geo-encryption**.** Geo-encryption is the use of a geographical location to encrypt the data. The overall idea is to fetch the location where the user wishes to encrypt the data. Location is usually obtained in the form of location coordinates (latitude, longitude pair). Upon the retrieval of the location coordinates, an encryption scheme is employed to encrypt the data. Subsequently, when the user returns to the same location, the data is then decrypted. However, the work that has yet been done in this field involves only a single person. Multi-party concept has found no applicability in geo-encryption. Multi-party control is referred to a scenario wherein multiple users agree to form a group, in which the tasks/functions are distributed such that each person is allocated a subtask which individually, cannot be performed. Later, when all the people forming the group re-assemble, they combine their individual subtasks to facilitate the execution of the overall complete task.

Through this paper, we integrate the services of multi-party control and geo-encryption. This paper walks through the existing work being done in this field and how this system will reduce the shortcomings of them. We then describe the entire system (architecturally) and illustrate its working.

Subsequently, the algorithm for geo-encryption (which will take place through self-designed encryption scheme-Trans Modulo Substitution Algorithm (TMSA)) has been explained and illustrated, followed by a cryptanalysis.

II. RELATED WORK

Exhaustive research has been done on location based data encryption, for example, Logan Scott and Dorothy E. Denning(2003) proposed a geo encryption technique [1] where data is encrypted using the asymmetric algorithm. Algorithm is modified to include the GeoLock. Geo-lock is evaluated using the recipient's position, velocity and time (PVT) block.

Thomas Mundt(2005) proposed Location Dependent Digital Rights Management system [2]. It was implemented using a precise clock. Trusted computing platform architecture (TCPA) device were responsible for decryption which took satellite signal, encrypted data and shape of the accessible area as input.

Hsien-Chou and Yun-Hsiang(2008), proposed a location based data encryption algorithm LDEA [3], wherein latitude/longitude coordinate is used as the key for data encryption in LDEA. Subsequently, Hatem Hamad and Souhir Elkourd(2009) suggested data encryption using dynamic location and speed of mobile node [4]. Unlike LDEA, they used dynamic tolerance distance. Some of the researches mentioned above make precise use of the user location.

In the field of multi-party, individual work in different domains such as multi-party in data mining (2010) [5], Online Social Networks (OSNs) (2013) [6] has been done. Taken together, however, the combined field of Multi party control geo-encryption has not seen much progress.

The aforementioned researches on geo-encryption have not been able to overcome the difficulties in decryption due to the precision that is required in the user's location. Due to their dependence on a single user location, the encryption at times tends to fail. Although the concept of toleration distance [3] has proven to be effective; the boundary conditions are still not covered in those implementations (when the user hovers around the toleration distance boundary area). Through this paper, we aim to bridge the gap between the shortcomings of precise user location and variations due to boundary level location pattern exhibited by the user respectively by the following ways:

- Creating a geo-fence (Virtual perimeter around the user's location with a specified radius)
- Creating two separate geo-fence (inner and outer)

Integrated with the use of multi-party control to add another layer of security, the encryption algorithm (TMSA) encrypts the user data, to complete the multi-party geo access control system.

III. WORKING

The system works in two stages; initial stage (when the system is run for the first time) and later stage (subsequent operation of the system). The entire system is comprised of three main components:

- Server(S) (AZURE)
- Central controlling device(CCD) (ANDROID DEVICE)
- Other devices(OD) (ANDROID DEVICES)

INITIAL STAGE: All the devices, including the Central Controlling Device (CCD) and the Other Devices (OD) are registered in the server through their IMEI number for the purposes of authentication. Geo-fence is set by the users through CCD every time a user requests for the

encryption of the message. Once all the OD enters the geo-fence, they notify the server of their presence in it, by using the mobile services of Azure [7]. They use asynchronous calls from the device to notify the server. Additionally, either the OD or the CCD sets the data (plaintext) which is to be encrypted. Once the server gets the notification from all the devices forming the multi-party, it intimates the CCD about the simultaneous presence of all the parties in the geo-fence, by issuing a push notification to the CCD via Google Cloud Messaging (GCM). Further the plaintext is kept at the CCD for Encryption.

Upon receiving the push notification from the server, the CCD uses the aforementioned encryption scheme to encrypt the plaintext to obtain the encrypted text and store it. Subsequently, the CCD generates a Sequence Number (SN) for each OD. The Key is stored on the CCD in its MD5 hash form (provides security so that any security breach at CCD may not be able to obtain the key) and split into Subkeys equal to the number of OD. Subkey and SN is then sent to the Server where it is mapped with IMEI number of each OD and server issues a notification to each OD to fetch their Subkey. Upon fetching, Subkey along with SN is forwarded to the OD, which, upon the retrieval may/may not leave the geo-fence. SN is not stored on the device; it is only delivered in the form of a notification. Later, when the devices enter the geo-fence (already mentioned earlier) for decryption of data, they send the Subkey in the same order that they are designated to, which is then forwarded to CCD. Upon the verification of the MD5 hash of supplied key with the MD5 hash of original key, the CCD decrypts the data and sends it to the server, which then broadcasts the message to all the OD.

LATER STAGE: Once the initial stage of the project is over, the next time when the users want to encrypt the data they just need to supply the plain text and the geo-fence area where message can be decrypted. For decrypting the data all the devices (OD) must be present in the geo-fence specified by them, the same set of steps takes place as mentioned above.

Note: There exists 2 geo-fences:

Inner Geo-fence: The data will be decrypted (encrypted for the first time) when all the authorized users (OD) are in the inner geo-fence.

Outer Geo-fence: The data will be encrypted when any of the OD moves out of this outer geo-fence.

The above methodology has been adopted so as to reduce the processing needed at the server and consequently reducing the amount of data that is required on the server. This reduces the load on the server. It may so happen that a user may wander on the boundary of the inner geo-fence. In such a case, constant location reporting of that particular user will need huge processing. By creation of separate and concentric geo-fences, such scenario can be avoided.

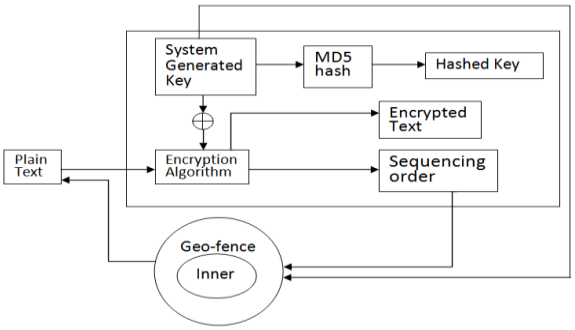

Figure 1 Initial Stage

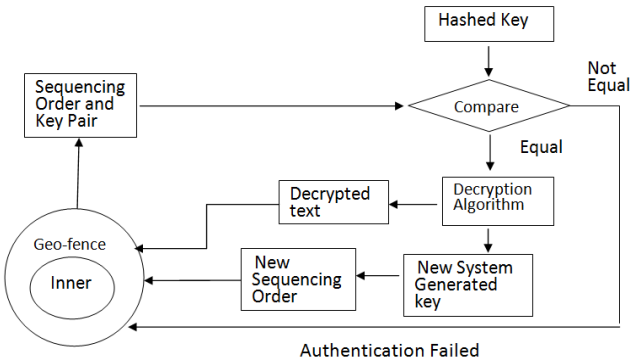

Figure 2 Later Stage

TSMA has the following features:

- It is a symmetric key cipher algorithm.
- Poly Alphabetic Substitution Concept is followed.
- Matrix Transposition Technique [8] is used.
- A variable size key is generated using multiplicative inverse in modular arithmetic [9] technique.
- Multilayer Encryption.

3.1 Algorithm

1. Characters are assigned with numerical values according to their codes mentioned in the hash table. In this algorithm, position of each character in the alphabets is used for substitution. (1 for a, 2 for b and so on)

2. Given the plain text, a key K (K1K2) is generated subject to the following constraints:

- K1 and K2 will be multiplicative inverse.
  In modular arithmetic, the modular multiplicative inverse of an integer K1 modulo N is an integer K2 such that K1*K2 mod N=1
- N>K1>K2
- Length of N should be even

3. The plain text is partitioned to form groups of two adjacent characters. Each letter in the plain text is assigned the numerical value according to the aforementioned rule.

For a plain text (M) of length Z (including whitespace), Z/2 groups (G) will be generated

4. For each group $G_1, G_2 \ldots G_{Z/2,}$ Ciphered Group (CG) is obtained as follows

   a. $CG_Z = (K1 * G_Z) \bmod N$ for odd Z

   b. $CG_Z = (K2 * G_Z) \bmod N$ for even Z

   Length of each Ciphered Group should be equal to N. If it's not equal, zero is added in the beginning to make length equal to N.

5. Having obtained the Ciphered groups, each group is split into pairs to obtain an equivalent message (E) of original length Z.

6. Equivalent message E is arranged in a matrix ($T_{i \times j}$), where 'i' depends on the size of plain text and 'j' is equal to the length of the key (K), in the row major order. Each column is assigned a separate digit from key (K) sequentially. Empty entries of matrix after arranging in row major order are filled with a period (.)

7. Every column in matrix T is given the same number of circular-up shift as the corresponding key value assigned to that column, to obtain a new matrix $T^{RM}{}_{i\ x\ j}$.The content of this new matrix T^{RM} read in row major order is the Encrypted Message Layer1(EML_1)

8. In a new matrix ($T^{P}{}_{i\ x\ j}$), ELM_1 is input in row major order with

number of columns: = length of key

Right most column of the matrix is comprised of the key such that for each row i, a separate digit from key (K) is assigned in the sequential reverse order. If number of rows in the matrix is less than the length of the key then only required number of digits are used from the key. If number of rows is more than the length of key then the key is repeated.

9. Every row in matrix T^{P} is given the same number of circular-left shift as the corresponding key value assigned to that column, to obtain a new matrix $T^{CM}{}_{i\ x\ j}$. The content of this new matrix T^{CM} read in row major order is the Final Encrypted Message (FEM).

3.2 Illustration

Message (M): **ENCRYPTION IS COOL**

STEP 1:

For explanation we shall use:

N = 3000

K1 = 017 K2 = 353

Thus K = 017353

Length (K) = 6 (Even)

STEP 2:

EN CR YP TI ON .I S. CO OL

STEP 3:

G1	G2	G3	G4	G5	G6	G7	G8	G9
0514	0318	2516	2009	1514	2709	1927	0315	1512

STEP 4:

CG1	CG2	CG3	CG4	CG5	CG6	CG7	CG8	CG9
2738	1254	0772	1177	1738	2277	2759	0195	1704

STEP 5:

Equivalent message (E): 27 38 12 54 07 72 11 77 17 38 22 77 27 59 01 95 17 04

STEP 6, 7, 8:

0	1	7	3	5	3
27	38	12	54	07	72
11	77	17	38	22	77
27	59	01	95	17	04

After shifting is done.

0	1	7	3	5	3
27	77	17	54	17	72
11	59	01	38	07	77
27	38	12	95	22	04

Encrypted Message Layer 1(EML_1):

27 77 17 54 17 72 11 59 01 38 07 77 27 38 12 95 22 04

STEP 9, 10:

27	77	17	54	17	72	**3**
11	59	01	38	07	77	**5**
27	38	12	95	22	04	**3**

After shifting is done

54	17	72	27	77	17	**3**
59	01	38	07	77	11	**5**
95	22	04	27	38	12	**3**

Final Encrypted Message:

54 17 72 27 77 17 59 01 38 07 77 11 95 22 04 27 38 12

IV. RESULT AND DISCUSSION

In this paper we introduced a new system for multi-party geo access control and proposed a new encryption algorithm (TMSA). An attempt to incorporate multi-party concept with geo encryption has been made to increase the security. The designed encryption algorithm TMSA provides multi-level encryption. Additionally, the cryptanalysis of the algorithm yields positive result against various attacks such as cipher-text only, known plain text, chosen plain text, adaptive chosen plaintext and brute force. The concept and the system described in the paper provides a strong and secure means for data transmission and data sharing in mobile environment among multiple members.

Table 1 Cryptanalysis

	Type of cryptography	Cipher Text Only	Known Plain Text	Chosen Plain Text	Adaptive Chosen Plain Text
AES	Symmetric	X	X	X	X
RSA	Asymmetric	√			√
DES	Symmetric			X	√
3DES	Symmetric		√	√	√
BlowFish	Symmetric	Depends	Upon the	Size of	Key
TMSA	Symmetric	X	X	X	X

V. FUTURE WORK

The system currently encrypts only text (numbers, alphabets etc). However, data encryption is not limited to encrypting the text only. Hence, in the future, we aim to target the field of encryption in multimedia. This will include the study and implementation of encrypting schemes on images and voice, through a new encryption scheme or an incremental scheme based on TMSA. Additionally, we wish to refine the security and effectiveness of our algorithm by implementing a bit level encoding-decoding scheme rather than one based on values. Scalability remains an area of concern.

Consequently, we aim to increase the number of people involved in the multi-party without having to trade-off with speed and efficiency.

VI. CONCLUSION

With the advent of multi-party and geo-encryption schemes, multi party geo access control is most likely to be a field of research in the future. Since this is a relatively untouched field, various innovations and efficient methodologies can be devised to facilitate a system more effective than the one explained in this paper. However, this system is an attempt to conglomerate the existing technologies with meticulous procedures to yield the maximum output from the available resources.

REFERENCES

[1]. Scott, Logan, and Dorothy E. Denning, (2003) "Geo-Encryption Using GPS to Enhance Data Security." *GPS WORLD* 14.4, pp. 40-49.

[2]. Mundt, Thomas. "Location dependent digital rights management, (2005)" *2012 IEEE Symposium on Computers and Communications (ISCC)*. IEEE Computer Society

[3]. Liao, Hsien-Chou, and Yun-Hsiang Chao, (2008) "A new data encryption algorithm based on the location of mobile users." *Information Technology Journal* 7, pp. 63-69.

[4]. Hamad, Hatem, and Souhir Elkourd, (2010) "Data encryption using the dynamic location and speed of mobile node." *Journal Media and Communication Studies*2, pp. 67-75.

[5]. Lindell, Yehuda, and Benny Pinkas, (2009) "Secure multiparty computation for privacy-preserving data mining." *Journal of Privacy and Confidentiality* 1.1, pp. 5.

[6]. Hu, Hongxin et al., (2013) "Multiparty access control for online social networks: model and mechanisms." *Knowledge and Data Engineering, IEEE Transactions on* 25.7, pp. 1614-1627

[7]. "Get Started With Mobile Services", December 2, 2014. [Online].Available:http://azure.microsoft.com/en-us/documentation/articles/mobile-services-android-get-started/

[8]. "Transposition Ciphers", March 25, 2004. [Online]. Available: http://libguides.murdoch.edu.au/content.php?pid=144623&sid=1229947

[9]. W.Stallings, "Basic Concepts in Number Theory and Finite Fields" in *Cryptography and Network Security: Principles and Practices*, 5th ed., Prentice Hall,2005,ch.4, sec. 4.3, pp. 108-110

AUTHORS

Pranshu Aggarwal is final year Computer Science undergraduate form Bharati Vidyapeeth's College of engineering, New Delhi.

Himshikha Suhag is final year Computer Science undergraduate form Bharati Vidyapeeth's College of engineering, New Delhi.

Rahul Bansal is final year Computer Science undergraduate form Bharati Vidyapeeth's College of engineering, New Delhi.

Purnank Jain is final year Computer Science undergraduate form Bharati Vidyapeeth's College of engineering, New Delhi.

Dharmender Saini is B.Tech, M.Tech and PhD in Computer Science. Currently, he is the principal of Bharati Vidyapeeth's College of Engineering. His area of interest includes cryptography.