International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 03 - Issue 10 || October 2018 || PP. 30-34

Proximity-Aware Location Based Collaborative Sensing for Energy-Efficient Mobile Devices

Pranav Nair[1], Hitesh Patil[2], Tukaram Gore[3], Yogesh Jadhav[4]
[1](Computer Engineering, P.K. Technical Campus, India)
[2](Computer Engineering, P.K. Technical Campus, India)
[3](Computer Engineering, P.K. Technical Campus, India)
[4](Computer Engineering, P.K. Technical Campus, India)

Abstract: Bank are providing mobile application to their customer. We are developing banking application using Location Based Encryption. As compare to current banking application which are location independent, we are developing banking application which is location dependent. User can perform transaction only if he/she is with in TD region. TD region is area of Toleration Distance (TD) where user can perform transaction. If user go out of TD region then transaction will terminate automatically. We are providing extra security by OTP and secret key.

Keywords: banking application, encryption, location, mobile, location-based data encryption, data security.

1. INTRODUCTION

Security has always been an integral part of human life. People have been looking for physical and financial security. With the advancement of human knowledge and getting into the new era, the need for information security was added to human security concerns. We are developing a banking application using Location Based Encryption. As compared to current banking application which is location-independent, we are developing banking application which is location dependent. It means User can perform transaction only if he/she is within TD region. TD region is the area of Toleration Distance (TD) where a user can perform a transaction. If the user goes out of the TD region then the transaction will terminate automatically.

Now adays handheld devices like mobile phones and PDA's are more used by people as their daily driver instead of carrying laptops around. This is because computation power and speed of the mobile are increasing day by day. Moreover, one main advantage of using mobile phones and PDA's are that they can transmit their exact/precise location through GPS which is rather difficult when working on laptops or computers.

In our system user register himself/ herself in our application. He/she provide the personal details like name, mobile number, email id, secret bit, etc. then the system will send the encrypted password to email. Encrypted password means "Secret bit" is added into the password, this is done to protect password from visualization. After entering correct username and password user will login to the system and get the secret key on registered email id. If the user entered key is correct then OTP will receive on mobile by SMS. If entered OTP is correct then generate TD region. This TD region specifies the range in meters. After generation TD region successfully user can view account details and User can perform money transaction operation. Our system is flexible enough to provide access to the customer to his/her bank account from any location. Our system also provides a solution to physical attack using virtualization, password send on email is encrypted by secret bit.

2. LITERATURE SURVEY

An encrypted data can be decrypted anywhere. Therefore, a location-dependent data encryption algorithm (LDEA) is proposed. The latitude/longitude coordinate is used as the key for data encryption in LDEA. Using GPS, it is impractical to get accurate coordinate as key for data encryption. Therefore, a toleration distance (TD) is designed in LDEA. A toleration distance (TD) is designed to overcome the inaccuracy and inconsistent problem of GPS receiver. The target coordinate can be determined by the sender or receiver. [1]

Now-a-days most of the data encryption techniques are location-independent. They forward and implements a simple and secured method of data transmission between client and server. Due to massive changes in technology related to security, so many advancements were introduced in the field of data transmission. The method implemented aims at increasing the security, reliability, scalability of the model and help in more secure, location-based data transmission. They propose a system where the client transmits its location for data encryption to the server. The server then encrypts the data and sends the cipher text back to client. But, the real trick in the system is that, the client can only decrypt the data when co- ordinate acquired from GPS receiver matches the target location. [2]

A disclosure control algorithm to hide user position in sensitive areas. They analyze algorithm that suppress location updates and thus hide visit to sensitive areas. For this service provider offers some default policies. For Eg: location tracking should be enabled on public street but not in buildings and private properties. In urban areas user is surrounded by sensitive areas. So to determine if user is about to enter or just passing by is difficult. They suggest 3 algorithm- base, bounded-rate, k-area. Base algorithm only releases location updates in areas classified as insensitive in sensitivity map. Bounded-rate ensures updates are not sent with frequency higher than predefined threshold. K-area algorithm restricts location updates only when an individual enters sensitive areas. [3]

They propose an encryption algorithm called MX. MX is a block cipher that processes a plain text of 64 bits and has secret key from 40 bit to 64 bit. MX algorithm provides high performance in case of data encryption. Suggested system also proves that even MX with a short key length, such as 40 bits, can deal sufficiently with the requirement of copyright protection systems. [4]

They suggests a few ideas of improving data compression performance when various data compression and encryption algorithms are pipelined together as different mapping of input files. With the pipeline of compression and encryption, it is realized from the first pipeline, that the encryption mapping cannot improve the original data file in terms of compression. They suggest that compression prior to encryption which could improve the encryption performance since the redundancy has been removed. [5]

With the popular development of smart phones and social networks, a large quantity of location-embedded data is collected in mobile cloud. By utilizing these data, the service providers of mobile cloud (MCSP) can provide users with great convenience by location based queries. Thus the mobile cloud service system (MCSS) comes into being. However, the MCSP are untrustworthy, and the location itself contains much privacy information. Hence, the data publishers always encrypt the location information before publishing it. But it brings a great challenge, that how to utilize the encrypted information efficiently. To solve this problem, this paper designs an efficient privacy-preserving processing scheme for location-based queries in mobile cloud. They adapt the RSA algorithm, and combine it with cipher text policy attribute-based encryption (CP-ABE) approach. The proposed scheme achieves fine-grained access control over location information, efficient and privacy- preserving location distance computation and comparison. The performance evaluation shows that their scheme is efficient enough to be applied into MCSS. [6]

3. MATHEMATICAL MODEL

Let `S' be the system
Where,
S= {I, O, P} Where,
I = Set of input sensors
O = Set of output applications
P = Set of technical processes
Let `S' be the system
S= {s, e, X, Y, Fma, DD, NDD}
s- Initial State: no user login
e- End state: Allow access to authenticated user
X- Input Login id, password, user's personal info.
Y- Secure Transaction.
Fma- Haversine -Distance calculation algorithm.
DD- Deterministic Data: Customer information
NDD- Non Deterministic Data: Location of customer
I={user location, user information}
User location: GPS is used to get users current location
User information: it contain the login id, password, account details.
O={transaction}
Transaction= if users within TD region and provide correct details then transaction willcomplete. If user out of TD region or provide incorrect details then transaction will
P={UL, secret key, OTP, TD region}
UL= Fetch User Current Location
Secret key= generate secrete key and send to email
OTP= generate OTP and send to mobile
TD region= generate TD region and perform transaction with in TD region.

4. ALGORITHM AND PROPOSED WORK

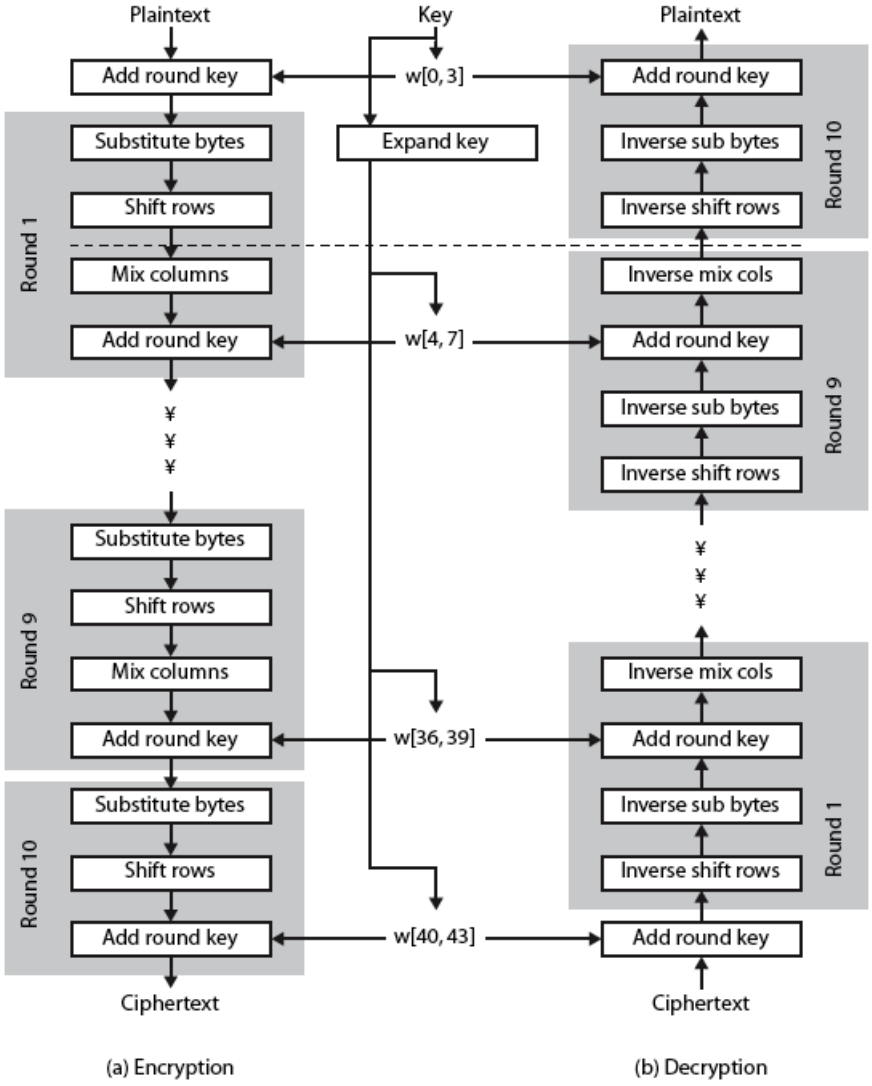

Figure 1. AES Structure

Steps:

1. an **iterative** rather than **Feistel** cipher
2. key expanded into array of 32-bit words
   2.1: four words form round key in each round
3. 4 different stages are used as shown
4. has a simple structure
5. only AddRoundKey uses key
6. AddRoundKey a form of Vernam cipher
7. each stage is easily reversible
8. decryption uses keys in reverse order
9. decryption does recover plaintext
10. final round has only 3 stages

4.1 Proposed work

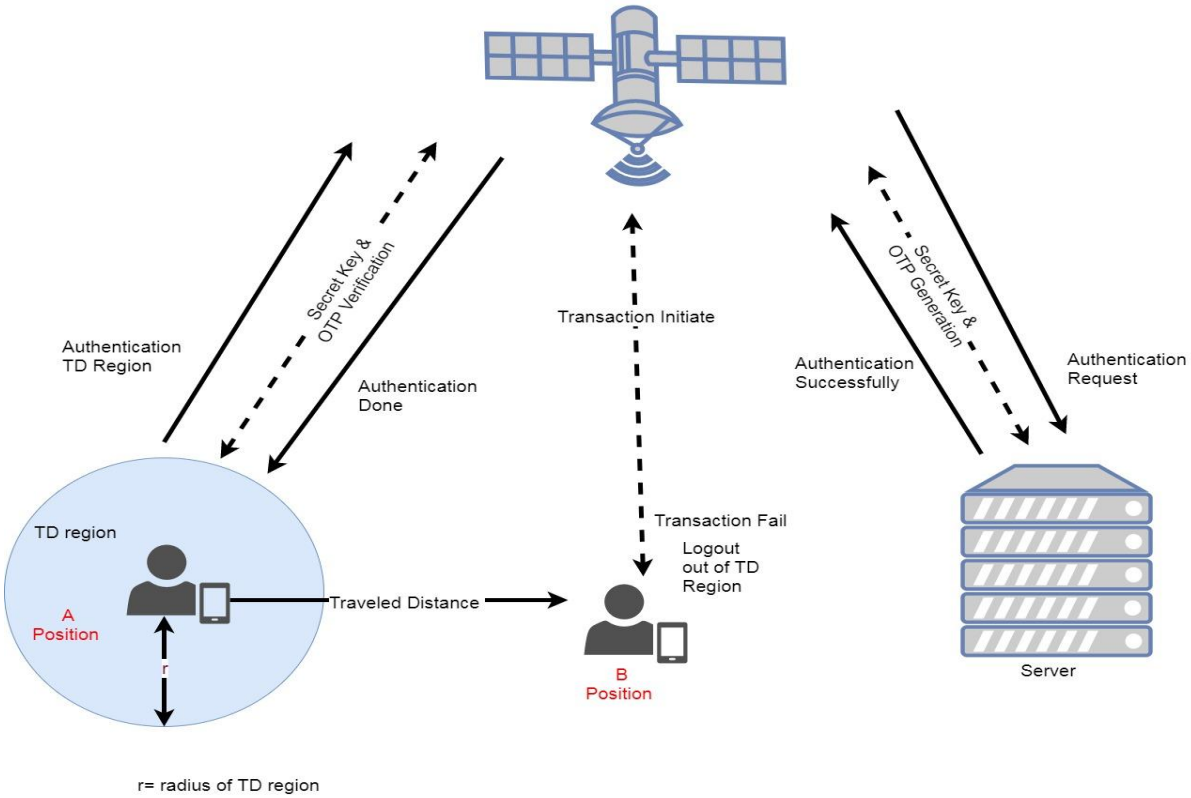

Figure 2. Architecture of Transaction Process

In above architecture, user register himself/ herself in our application. He/she provide the personal details like name, mobile number, email id, secret bit, etc. the system will send the encrypted password to email. Encrypted password means the Secret bit is added into the password, this is done to protect password from visualization.

After entering the correct username and password user will log in to the system and get the secret key on registered email id. If the user entered key is correct then OTP will receive on mobile by SMS. If entered OTP is correct then generate TD region. This TD region specifies the range in meters. After generation TD region successfully user can view account details and User can perform money transaction operation.

5. CONCLUSION AND FUTURE WORK

We are developing a banking application using Location Based Encryption. As compared to current banking application which is location-independent, we are developing banking application which is location dependent. It means User can perform transaction only if he/she is within TD region. TD region is the area of Toleration Distance (TD) where the user can perform the transaction. If the user goes out of the TD region then the transaction will terminate automatically. We providing extra security by using the secret key and OTP. The study shows that location could increase the security of the banking application.

5.1 FUTURE WORK

1. For further security we can provide more authentication using fingerprint or iris verification of the user as now-a-days these sensors are inbuilt in most android phones.
2. The LDEA algorithms can be extended to the other domains, e.g., authorization of mobile software. If mobile software is authorized within a predefined area, such as a city or a country, the execution of the software may activate the location check based on the LDEA algorithm. The software can be executed only when the user is within the authorized area. Besides, the distribution of multimedia content may be utilized the LDEA algorithm for advanced access control except the username/password.

3. Some factors can be incorporated into AES, such as time, moving speed, or moving path, etc., to increase the security strength and usability of AES.

REFERENCES

[1]. H. C. Liao, Y H. Chao, and C. Y Hsu, *"A Novel Approach for Data Encryption Depending on User Location," The Tenth Pacific Asia Conference on Information Systems (PACIS 2006)*, 5-9 July 2006.

[2]. Liao, H.C., P.C. Lee, Y.H. Chao and C.L. Chen, 2007. *A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security. In: Proc. the 9th International Conference on Advanced Communication Technology (ICACT 2007), 1: 625-628*, Feb. 2007.

[3]. Gruteser, M. and X. Liu, 2004. *Protecting Privacy in Continuous Location-Tracking Applications. IEEE Security Privacy Magazine, 2 (2): 28-34*, March-April 2004. Jamil, T., 2004. *The Rijndael Algorithm. IEEE Potentials, 23 (2): 36-38.*

[4]. Aikawa, M., K. Takaragi, S. Furuya and M. Sasamoto, 1998. *A Lightweight Encryption Method Suitable for Copyright Protection. IEEE Trans. on Consumer Electronics, 44 (3): 902-910.*

[5]. Jiang, J., 1996. *Pipeline Algorithms of RSA Data Encryption and Data Compression, In: Proc. IEEE International Conference on Communication Technology (ICCT96), 2:1088-1091*, 5-7 May 1996.

[6]. Becker, C. and F. Durr, 2005. *On Location Models for Ubiquitous Computing. Personal and Ubiquitous Computing, 9 (1): 20-31*, Jan. 2005.

[7]. Eagle, N. and A. Pentland, 2005. *Social Serendipity: Mobilizing Social Software. IEEE Pervasive Computing, 4 (2)*, Jan.-March 2005.

[8]. Lian, S., J. Sun, Z. Wang and Y. Dai, 2004. *A Fast Video Encryption Scheme Based-on Chaos. In: Proc. the 8th IEEE International Conference on Control, Automation, Robotics, and Vision (ICARCV 2004), 1: 126-131*, 6-9 Dec. 2004.

[9]. Y Zhang, W. Liu, W. Lou, and Y Fang, *Securing Sensor Networks with Location- Based Keys, Proc. of IEEE Wireless Comm. and Networking Conf: on Comm. Society (WCNC 2005), Vol. 4, 13-17* March 2005, *pp. 1909-1914.*

[10]. L. Barkhuus and A. Dey, *Location-based Services for Mobile Telephony: A Study of Users Privacy Concerns, Proc. 9th Int^al Conf. Human-Computer Interaction (INTERACT),* ACM Press, 2003, *pp. 709-712*.

[11]. Toye, E., Sharp, R., Madhayapeddy, *A., and Scott, D., Using Smart Phones to Access Site-Specific Services, IEEE Pervasive Computing (4:2*), Jan.-March 2005,*pp. 60-66.*

[12]. Scott, L. and Denning, D. E., *Using GPS to Enhance Data Security: Geo-Encryption, GPS World (14),* April 2003, *pp. 40-49.*