Advanced Security System For Banking Transactions

Prathmesh Patil[1], Rajesh Bhosle[2], Suyog Meher[3], Swapnil Mulay[4], K.D.Bamane[5]
[1, 2, 3, 4, 5] Department of Information Technology
[1, 2, 3, 4, 5] D.Y.Patil College of Engineering, Akurdi, Pune.

Abstract-*The omnipresence of WLAN and the rise in use of mobile devices increases the frequency of data transmission among mobile users. However, most of the data encryption technology is location-independent. An encoded data can be decoded anywhere. The encryption technology cannot forbid the location of data decryption. To fulfill the needs of mobile users in the future, a location-based method, called location-dependent data encryption algorithm (LDEA),is put forth in this paper. A desired latitude/longitude coordinate is determined firstly. The coordinate is attached with a random key for data encryption. The receiver can only decode the cipher text when the coordinate acquired from GPS receiver is matched with the desired coordinate. However, current GPS receiver is inaccurate and inconsistent. The location of a mobile user is difficult to exactly match with the target coordinate. A phenomenon of toleration distance (TD) is also introduced in LDEA to increase its practicality. The security analysis shows that the possibility to break LDEA is almost impossible since the length of the random key is adjustable. A prototype is also implemented for experimental study & research study. The results show that the cipher text can only be converted to plaintext under the restriction of TD only. It illustrates that LDEA is effective, secured and practical for data transmission in mobile environment.*

Keywords-data encryption, GPS, mobile computing, location-based service

I. INTRODUCTION

Cloud computing is a new emerging domain of information technology and development of computer technologies based on the World Wide Web. One of the most important drawback in this field is the security of cloud computing. On the other hand the security of access to critical, sensitive and confidential information in banks, institutions, organizations etc. is extremely essential. Sometimes even with the enormous costs, it is not fully guaranteed and it is not completed secured from the attackers. By providing a naive method, we emphasize on the improvement of the security of data access & transmission in cloud computing for a firm or any other specific locations using the location-based encoding approach.

II. LITERATURE SURVEY

1) On location models for ubiquitous computing
Published Year: 2014
AUTHORS: Christian Becker Æ Frank Du rr

Common queries regarding data processing in ubiquitous computing environment are based on the location of physical objects. No matter whether it is the next printer, next restaurant, nearby friend or next theatre is searched for, a concept of distances between objects is required. A search for all objects in a certain physical area requires the possibility to determine spatial ranges and spatial inclusion of locations. In this paper, we discuss general attributes of symbolic and geometric coordinates. Based on that, we present an overview of existing location models allowing for position, range,tolerate distance and nearest neighbor queries. The various location models are differentiated based on their suitable nature in accordance with query processing along with other requirements. Besides an overview of present location models and approaches, the classification of location models with respect to application requirements can assist developers in their design decision making process.

2. **Location Based Services using Android Mobile Operating System**
Published Year: 2011
AUTHORS: Amit Kushwaha1, Vineet Kushwaha

The reason for developing such type of system is to provide the users with exact information at right time in proper format. In today’s world we are making use of smart phones which are proofing an option for the desktops even for computational purposes.Such needs can only be catered with the help of LBS.A very appealing application includes surveillance where instant information is needed to decide if the people being monitored are any real threat or an erroneous target. We have been able to create a number of different applications where we provide the user with information regarding a place he or she wants to visit. But these applications are limited to desktops only. We need to import them on mobile devices. We must ensure that a person when visiting places need not carry the travel guides with him. All the information must be available in his mobile device and also in user customized format.

3. Securing Sensor Networks with Location-Based Keys

Published Year: 2005
Authors: Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang

This paper proposes the naive concept of location-based keys for designing zero compromise-tolerant security mechanisms for sensor networks. Based on location based keys, we designed a node-to-node authentication scheme, which is not only able to nullify the impact of compromised nodes within their closeness, but also to provide the formation of pair keys between neighboring nodes. Compared with previous methods, our scheme has perfectly robust against node compromise, low storage overhead and good network coverage. We also demonstrate the use of location-based keys in combating a few notorious cyber actions against sensor network routing protocols.

4. Location Based Services using Android
Published Year: 2009
AUTHORS: Sandeep Kumar, Mohammed Abdul Qadeer, Archana Gupta

In the beginning mobile phones were developed only for voice communication but today’s scenario has changed, voice communication is just one aspect of a mobile phone. There are other factors which are major point of interest. Two such major aspects are web browser and GPS services. Both of these functions are already implemented but are only in the hands of manufacturers not in the hands of end users because of proprietary & commercial issues, the system restricts the user to access the mobile hardware directly. But now, after the emergence of android based open source mobile device a user can access the hardware directly and design customized user-friendly applications to develop Web and GPS enabled services and can program the other hardware components like camera,sensors etc. In this paper we will discuss the facilities available in android platform for implementing LBS(Location Based Services) geo-services.

III. PROPOSED SYSTEM

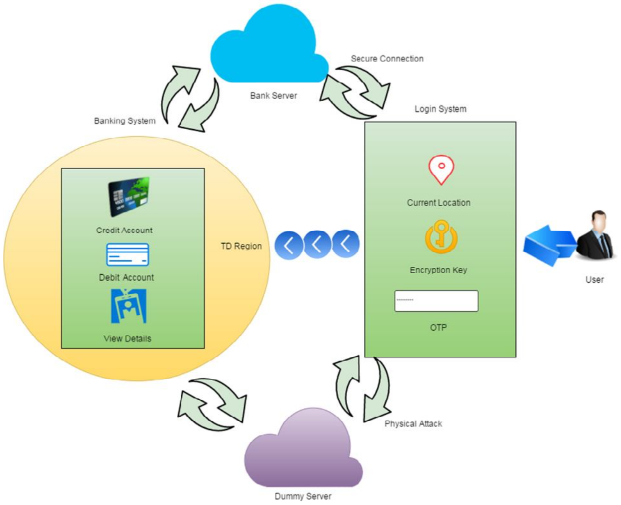

Fig.1 System Architecture

The proposed system consists of the Bank server, Dummy server and User.

- User:

The user needs to login to his/her account with the credentials provided during the registration process. User current location is acquired and verified with the registered location if its similar then user can proceed with further transaction else the transaction will be closed.

- Bank Server:

It is main server meant for saving the data of user during transaction. User can credit, debit and enquiry about his/her account details.

- Dummy Server:

The dummy server is for providing security from physical attack. It also works same as main server but the transaction made here are fake i.e. the transaction doesn’t affect the users main account.

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’ is the system

S = {…………

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- Geo encryption algorithm.
DD- Deterministic Data
Customer information
NDD- Non Deterministic Data: Location of customer

IV. TECHNIQUES USED

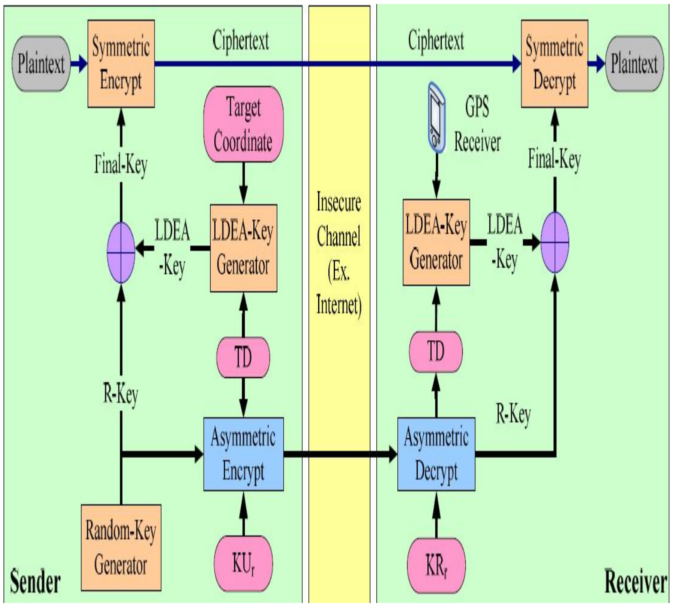

Fig.5.2 LDEA Algorithm

Steps of Algorithm

LDEA-key is generated from EX-OR of latitude/longitude coordinate and TD.

1. The random-key generator issues a session key, called R-key.
2. The final-key for encrypting the plaintext is generated by exclusive-or R-key with LDEA-key.
3. KUr and KRr is the public and private keys generated on the receiver side. KUr is transmitted to the sender side firstly.
4. TD and R-key is transmitted via asymmetric encryption algorithm.
5. The receiver gets the TD and R-key, the LDEA-key can be generated from TD and the coordinate acquired from GPS receiver
6. The final-key is generated by exclusive-or R-key with LDEA-key
7. If the acquired coordinate is matched with the target coordinate within the range of TD, the cipher text can be decrypted back to the original plaintext otherwise, indiscriminate and meaningless.

V. RESULT ANALYSIS

Methodologies Of Problem Solving And Efficiency Issues

We are proposing system in which when the user is under attack he/she can login to his /her account by entering the password with extra key, that is identified at server side and hence access will be prohibited. We are using “Geo-Encryption” algorithm, location based cryptography, positioning tools (Anti-spoof GPS).That means our system provide solution to physical attack using virtualization, in which customer is allowed to perform fake transaction for his/her physical security purpose.

Outcome

Using this system one can able to do the secure transaction from mobile with the help of Geo-encryption algorithm and anti-spoof GPS. In case of physical attack, our system creates a virtual environment (Dummy server) with extra key in password and allows fake transactions.

VI. CONCLUSION

Location based encryption and location-dependent data encryption algorithm (LDEA), were also reviewed. Finally a new security level was added to the existing security measures using location-based encryption. This method can be used in several places such as banks, big companies, institutions and have the desired performance.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the college powers for giving the obliged base and backing.

REFERENCES

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

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

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

[4] Gruteser, M. and X. Liu, 2004. Protecting Privacy in Continuous Location-Tracking Applications. IEEE Security & Privacy Magazine, 2 (2): 28-34, March-April 2004.

[5] Jamil, T., 2004. The Rijndael Algorithm. IEEE Potentials, 23 (2): 36-38.Jiang, J., 1996. Pipeline Algorithms of RSA Data Encryption and Data Compression, In: Proc. IEEE International Conference on Communication Technology (ICCT'96), 2:1088-1091, 5-7 May 1996.

[6] 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.

[7] 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: Pro Advanced Communication Technology (ICACT 2007), 1: 625-628, Feb. c. the 9th International Conference on 2007.