International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Specific Location Based Privacy protecting Access Control System

Ms. M. M. Jadhao[1], Mrs. S. M. Gothe[2], Mrs. S. V. Nimkarde[3]

[1]*Dept. of Computer engineering, G. S. Moze Institute of Technology, Pune, India.*
[2]*Dept. of Computer engineering, G. S. Moze Institute of Technology, Pune, India.*
[3]*Dept. of Computer engineering, Bharati Vidyapeeth I.O.T, Navi Mumbai, India.*

ABSTRACT

T*his paper introducing a unique technique to improve the safety of data access in cloud computing for specific locations using the location-based cryptography. The wide unfold of mobile devices will increase the frequency of data transmission among mobile users. Most of the data encoding technology is location-independent. DEA algorithmic rule by using the GPS coordinate, known as LDEA algorithm, was proposed in previous research. It is mainly to include the latitude/longitude coordinate within the encoding and so to limit the location of data decryption. A toleration distance is designed to beat the quality and inconsistent drawback of GPS receiver. Encrypted information is often decrypted. The technology cannot limit the placement of data decryption. Meet the demand of mobile users in the future. A location-dependent (LD) approach, referred to as location-dependent encoding algorithm, is proposed during this paper. A target latitude/longitude coordinate is set firstly. The coordinate is incorporated with a random key. The receiver will decode the cipher text once the coordinate non-inheritable from GPS receiver is matched with the target coordinate. GPS receiver is inaccuracy and inconsistent. The placement of user is troublesome to precisely match with the target coordinate. A toleration distance (TD) is additionally designed in LDEA to extend. The safety analysis shows that break LDEA is nearly not possible since the length of the random key is adjustable. The results show that the cipher text can only be decrypted under the restriction of TD.*

Keywords: *Data Encryption, GPS, Location-Based Service, Mobile Computing,*

I Introduction

In this paper propose a location-dependent approach for mobile information system. The mobile client transmits a target latitude/longitude coordinate for encoding to info server. The server encrypts the message and sends the cipher text back to the client. The client will only decode the cipher text when the

coordinate acquired form GPS receiver matches with the target coordinate. The approach can meet the confidentiality, authentication, simplicity, and practicability of security problems. If the data encoding algorithm will give such function for increasing the safety of mobile data transmission. A location-dependent algorithm (LDEA) is proposed during this paper. The latitude/longitude coordinate is used for encoding in LDEA. When a target coordinates for encoding, the cipher text will only be decrypted at location. The GPS receiver is inaccurate betting on what number satellite signals received. It's difficult for receiver to decipher the cipher text at the situation matched with the target coordinate. It's impractical by using the inaccurate GPS coordinate as key for encoding. A toleration distance is designed in LDEA. The sender can confirm the TD and the receiver can decode the cipher text at intervals vary of TD. This paper tends to developing banking application using Location based encoding. If an attempt to decode information at another location, the decoding method fails and reveals no info about the plaintext. This is important in real time application [1].

II Literature Survey

1.Location based Encryption-Decryption Approach for data Security

Authors: BorseManoj V, BhandureHarshad D, PatilDhiraj M, Bhad Pratik B

Encryption means that of efficient secure integer comparison. The encryption technology cannot prohibit the location of data decoding. in order to fulfill the demand of a location-dependent approach location-dependent encryption algorithmic program is required. A target latitude/longitude co-ordinate is determined firstly. The co-ordinate is incorporated with a random key for encryption. The receiver will solely decode the cipher text when the co-ordinate acquired from GPS receiver is matched with the target co-ordinate.

2. A Location based encryption Technique and some of Its Applications

Author: Logan Scott, Dorothy E. Denning

Location based cryptography enhances security by integrating position and time into encoding and decoding processes. It's not enough to easily enable or disable decoding based on location and time; these aspects should be integrated into the key construction method. Furthermore, keys or files in transit mustn't reveal something regarding their locations/times of relevance. after reviewing the objectives of location-based encoding, this paper introduces a selected approach known as geo-encryption.

3. Location based encryption & Its Role In Digital Cinema Distribution

Authors: Logan Scott, Dorothy E. Denning

This paper starts by describing a geo-encryption approach that builds on established cryptographic algorithms and protocols in a way that has an extra layer of security beyond that provided by conventional cryptography. It permits information to be encrypted for a selected location(s) or for specific area(s), e.g. a studio's campus area. Constraints in time and velocity as well as location may be enforced. This paper discuss a method of applying successive geo-encryptions at the originating node to enforce specific geographic routings for transmission to the ultimate destination node

4. A Generalized Study on encryption Techniques for Location based Services

Author: Y. lakshmi Prasanna, Prof. E. Madhusudhan Reddy

"location-based encryption" is used to any methodology of encryption whereby the cipher text will solely be decrypted at a specified location. If an attempt is created to decode the info at another location, the decoding method fails and reveals no data regarding the plaintext. The device performing the decoding determines its location using some sort of location device, for example, a GPS receiver or another satellite or radio frequency positioning system

5. Location based encryption using Message Authentication Code in Mobile Networks

Author: Swapna B Sasi, Betsy K abraham, Jinil James, Riya Jose

The popularity of mobile devices will increase the frequency of knowledge transmission among mobile users. A way to give a secure and convenient protocol for information transmission is vital. Secure communication is feasible through cryptography of knowledge. The conception of "geo-encryption" or "location-based encryption" is developed to limit the placement and time of data decoding. Location-based cryptography or geo-encryption refers to an cryptography methodology during which cipher text can be decrypted solely at a specified location. If someone tries to decode the info at another location, the decoding method fails ad reveals no details regarding the first plaintext datal

III Proposed System

For Data security within the cloud is vital. People or firms are involved about the access to the information by unauthorized users. Currently information is a few vital and confidential information from a bank, or an organization and etc. the need of access control in the cloud computing is over ever and may be an important a part of information security in cloud. Traditional encryption is used to provide that only

approved users will the secure content. However, it'd still be helpful to have a further layer of security provides the secure will only be used at approved location and time. Encoding will be wont to guarantee security in order that information cannot be decrypted outside a specific facility, this methodology is tend to use the user's location and geographical position can add a security layer to the prevailing security measures. This paper resolution is more appropriate for banks, huge firms, establishments and examples like this. Correct GPS those firms will afford to buy. Also implementing the location-dependent data encryption algorithm (LDEA), on the cloud and the user's computer in which the GPS is needed and that system will label the data. Label contains name of the company or a person who works within the company (for example the company's boss).

These labels are placed in an index table that refers to the user's geographic location and the timeframe thought-about to access data, during a database.

IV Methodology

Fig 1: Architecture diagram of proposed system

The proposed system contains the Bank server, Dummy server, User.

User:

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

Bank Server:

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

Dummy Server:

It also works same as main server but the transaction made here are fake the dummy server is for providing security from physical attack.

Third-Party Provider Solutions

For last few years, a big range of third-parties providing to deliver alert messages (and different info services) via text electronic messaging services. Whether or not activated through an online interface, directly from a phone, or as software system running on a field administrator's laptop, these services act as SMS aggregators and inject text messages into the network. Within the event of Associate in Nursing emergency message is shipped to the service center from the victim or footer mobile.

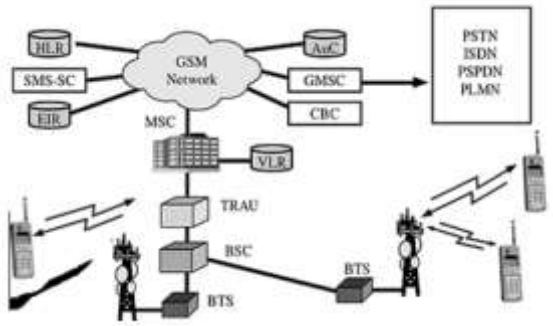
Short Message Service

SMS (Short Message Service) is similar to paging. However SMS messages do not require the mobile phone to be active and within range and will be held for a number of days until the phone is active and within range. SMS messages are transmitted within the same cell or to anyone with roaming service capability. Short Message Service (SMS) may well be a text transmission service part of phone internet or mobile communication systems, exploitation standardized communications protocols that modify the exchange of short text messages between fixed line and itinerant devices. SMS text transmission is that the foremost typically used information application among the planet, with 3.6 billion active users, or seventy eight of all itinerant subscribers. The term SMS is used as a similar word for all styles of short text transmission additionally as a result of the user activity itself in many parts of the world, easy user generated text message services embrace news, sport, financial, language and placement based services, additionally as many early samples of mobile commerce like stocks and share prices, mobile banking facilities and leisure booking services. SMS has used on modern handsets originated from radio telegraphy in radio memoranda pagers exploitation standardized

Phone protocols and Later made public as a vicinity of the planet System for Mobile Communications (GSM) series of standards in 1985 as a technique of inflicting messages of up to at least one hundred sixty characters, to and from GSM mobile handsets. Since then, support for the service has expanded to include various mobile technologies like ANSI CDMA networks and Digital AMPS, additionally as satellite and landline networks. Most SMS (Short Message Service) messages are mobile to mobile text messages though the standard supports various types of broadcast transmission additionally.

GSM Technology

Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan. European mobile cellular radio System operating at 900 MHz. It is estimated that many countries outside of Europe will join the GSM partnership



V Advantages

•Location-based encryption is a standard procedure to get access to a machine, especially a working position with a computer and the functions of this computer.

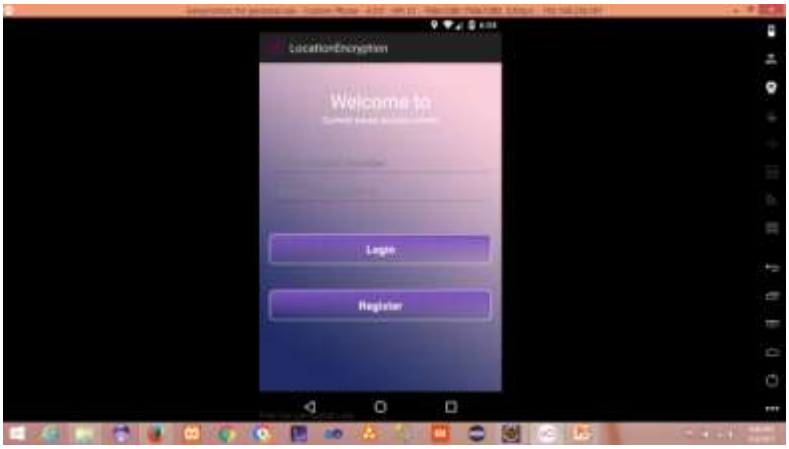
•Location-based encryption is a novel procedure to provide additional information about the authenticity of a user's sphincter circumference

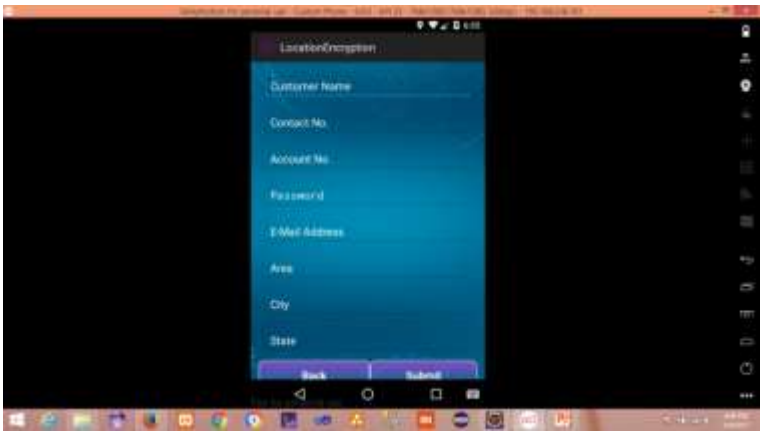
VI Application

- E-wallet
- Banking Applications

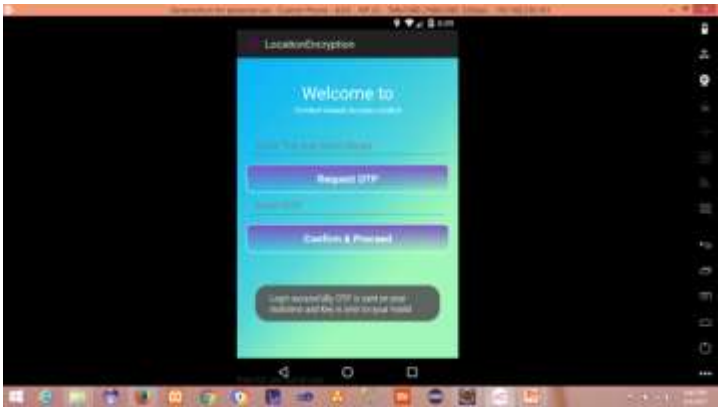
International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

VII Simulation Results

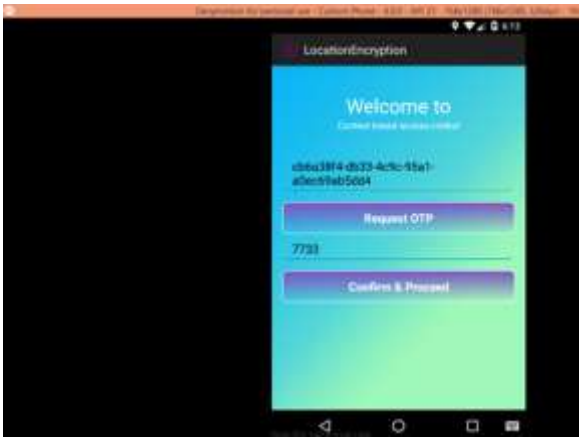


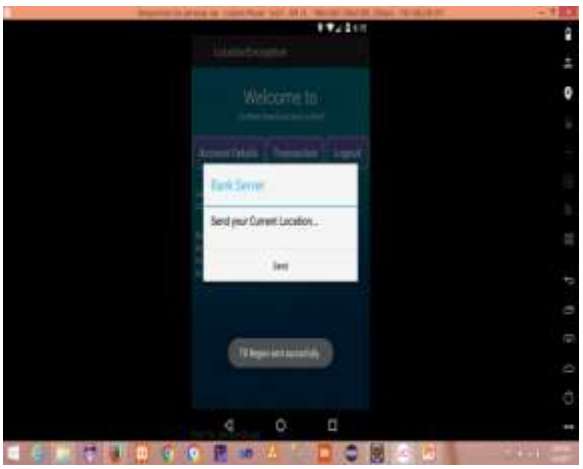



LocationEncryption
Welcome to
Login
Register


LocationEncryption
Welcome to
Request OTP
Confirm & Proceed

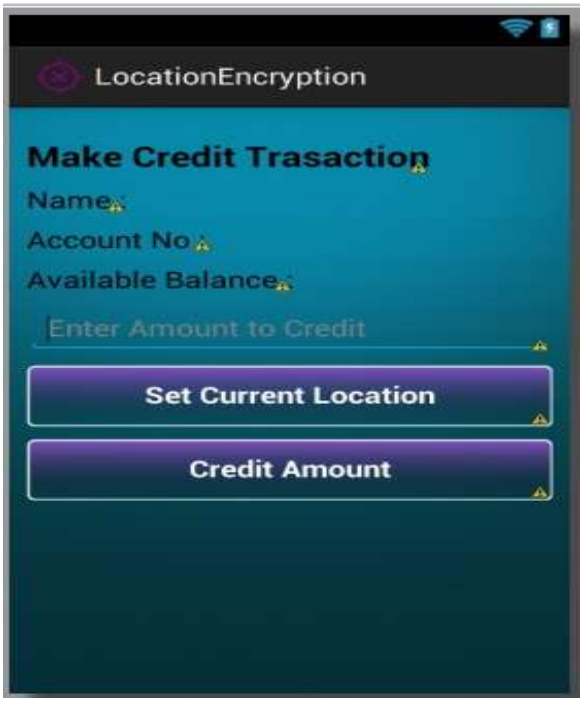

LocationEncryption
Welcome to
Request OTP
Confirm & Proceed


LocationEncryption
Welcome to
Request OTP
7733
Confirm & Proceed


Welcome to
Bank Server
Send your Current Location...
Sent


Welcome to
Account Details
Transaction
Logout


LocationEncryption
Make Debit Trasaction
Name
Account No
Available Balance
Set Current Location
Debit Amount


LocationEncryption
Make Credit Trasaction
Name
Account No
Available Balance
Enter Amount to Credit
Set Current Location
Credit Amount

VIII Conclusions

- LDEA algorithm is based on the DES algorithm.
- Traditional encryption cannot restrict the location of mobile users for data decryption.
- In order to meet the demand of mobile users in the future, LDEA algorithm is proposed in this paper.
- LDEA provide latitude/longitude coordinate as the key of data encryption. A toleration distance is also designed to overcome the inaccuracy and inconsistent of GPS receiver.
- The experimental result of the prototype also shows that the decryption is constrained by the range of TD.
- As a result, LDEA is effective and practical for the data transmission in the mobile environment. The LDEA algorithms can be extended to the other application domains, the authorization of mobile software. If mobile software is authorized within area, software may activate the location check based on the LDEA algorithm.
- It activate when the user is within the authorized area.
- The proposed LDEA algorithm provides for data security.
- Many possible applications will be developed in the future to demonstrate and promote the concept of LDEA algorithm.
- The proposed method can be used in several places such as banks, big companies, institutions to meet the desired performance.

REFERENCES

[1] Aikawa, M., K. Takaragi, S. Furuya and M. Sasamoto, "A Lightweight Encryption Method Suitable for Copyright Protection", *IEEE Trans. on Consumer Electronics*, Vol. 44, No. 3, 1998, pp. 902-910.

[2] Becker, C. and F. Durr, "Location Models for Ubiquitous Computing. Personal and Ubiquitous Computing", *ACM Digital Library*, Vol. 9, Issue 1, January 2005 pp. 20-31.

[3] Eagle, N. and A. Pentland, "Social Serendipity: Mobilizing Social Software" *IEEE Pervasive Computing*, Vol. 4, No. 2 Jan.-March 2005, pp. 28-34.

[4] Gruteser, M. and X. Liu, "Protecting Privacy in Continuous Location-Tracking Applications*" IEEE Security & Privacy Magazine*, Vol 2, Issue 2, March-April 2004, pp. 28-34.

[5] Jamil, T., "The Rijndael Algorithm*", IEEE Potentials*, Vol 23, Issue 2, 2004, pp. 36-38.

[6] Jiang, J., "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.

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

Authors

M. M. Jadhao: Ms. Manisha M. Jadhao, (ME-Computer Engg.) Lecturer, G S Moze Institute of Technology, Pune, Maharashtra, India

S. M. Gothe: Mrs. Sonali M. Gothe, (ME-Computer Engg.) Lecturer, G S Moze Institute of Technology, Pune, Maharashtra, India

S. V. Nimkarde: Mrs. Suwarna Nimkarde, (MTech-Computer Engg.) Lecturer, Bharati Vidyapeeth Institute of Technology, Navi Mumbai, Maharashtra, India