Internet Banking Through Location Based Data Encryption Algorithm

Bharati Sutar[1], Kiran Shirke[2], Rasika Jare[3], Prof. Sonali Tidke[4]
[1, 2, 3, 4] Department of Computer Engineering
[1, 2, 3, 4] Pune UniversitySuman Ramesh Tulsiani Technical Campus, Maharashtra, India.

Abstract*- In the project a Location Based Data-Security System to secure data by applying Encryption-Algorithm and co-ordinate using GPS device. Encryption means of efficient secure integer comparison. The encryption technology cannot restrict the location of data decryption. In order to meet the demand of a Location-dependent approach location-dependent data encryption algorithm is needed. A target latitude/longitude co-ordinate is Determined firstly. The co-ordinate is incorporated with a random key for data encryption. The receiver can only decrypt the cipher Text when the co-ordinate acquired from GPS receiver is matched with the target co-ordinate. GPS-based encryption is an innovative Technique that uses GPS-technology to encode location information into the encryption keys to provide location based security. GPS based encryption adds another layer of security on top of existing encryption methods by restricting the decryption of a message to a Particular location.*

Keywords- GPS, Data Encryption, Ddecryption, LDEA, data privacy, authentication, mobile, location, Tolerance Distance, Security.

I. INTRODUCTION

The popularity of mobile devices increases the frequency of data transmission among mobile users. Nowadays mobile communication has become an important part of our daily life. All the communications need security. Secure communication is possible through encryption of data. The concept of “geoencryption” or “location-based encryption” is developed to restrict the location and time of data decryption. Location-based encryption or geo-encryption refers to an encryption method in which cipher text can be decrypted only at a specified location.

In the project developing banking application using Location Based Encryption Algorithm (LDEA). As compare to current banking application which is location-independent. It means in Cryptography Cipher-text can only be decrypted at a specified location i.e. location-dependent approach. If an attempt to decrypt data at another location, the decryption process fails and reveals no information about the plaintext. This is important in real time application, example in military base application, Cinema Theater. But our system is flexible enough to provide access to customer to his/her account from any location. Our system also provide solution to physical attack using virtualization, in which customer is allowed to perform fake transaction for his/her physical security purpose.

User has username and password. When he/she wants to login in the system then it needs that.

Location Based Encryption: When the user goes to login there is must to input the encryption key. User location changed then the encryption key will also change.[1,2]

Transaction: There is Credit, Debit View Account Details operations. Which simply same as the Bank. In that the each operation is depends on the key and location and also on Tolerance Distance (TD) region.

Physical Attack: Physical Attack also work as same as main transaction. But it launch when the user type wrong credentials.

The mobile client transmits a target latitude/longitude coordinate for data encryption to information server. Then, the server encrypts the message and sends the cipher text back to the mobile client. The client can only decrypt the cipher text when the coordinate acquired form GPS receiver matches with the target coordinate. Traditional encryption technology cannot restrict the location of mobile clients for data decryption. A target latitude/longitude coordinate is determined firstly. The coordinate is incorporated with a random key for data encryption. The receiver can only decrypt the cipher text when the coordinate acquired from GPS receiver is matched with the target coordinate. The purpose of LDEA is mainly to include the latitude/longitude coordinate in the data encryption and thus to restrict the location of data decryption. When the target coordinate and TD (toleration distance) is given by the sender on the left-hand side, an LDEA-key is generated from latitude/longitude coordinate and TD. 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, the result is indiscriminate and meaningless. [4] Explains how location can be used as one of the credentials to give access to data only to legitimate user. This technique is relatively new approach towards information security. Location Based Authentication is a technique that will take into account the geographical location of the user; which is latitude, longitude of the person who is trying to authenticate his identity. Location information is captured at that instance when he is trying to access his mail account.

Cloud:-

Cloud is set of different type of hardware and software which work together to deliver many aspect of computing to end user as an online service.

Cloud is scalable network of server that connected together through grid. [1, 2]. We use service over internet and store data and information at another location doing, we give some privacy [4].Cloud computing allow individual or organization to use software and hardware that manage by remote server and provide the independence access them through network [3, 4]. In this paper, we have discussed about cloud and also explained location based cryptography and geoencryption algorithm.

GPS: -

The Global Positioning System is a space-based satellite navigation system that provides location and time information, anywhere on or near to the Earth where there is unobstructed line of sight to four or more GPS satellites. The United States government has created the system, which maintains it, and makes it freely accessible to anyone with the GPS receiver. In the cryptography, encryption is a process of encoding the messages or information in such a way that only the authorized parties can read it [8]. Encryption does not of itself prevent the interception, but denies the message content to interceptor [9]. In encryption scheme, the message or the information, referred to as plaintext, is encrypted using encryption algorithm, generates cipher text that can only be read if decrypted [10]

GPS Interfacing and Location:

Global Positioning System satellites broadcast signals from Space that are used by GPS receivers to provide current Location by making use of longitude and latitude.[5] location matching is the key process for successful decryption of data. The co-ordinates fetched by GPS must be matched with the co-ordinates which were entered while encrypting the data. As current location retrieved by GPS device will not be exactly same every time due to weather conditions, etc. Tolerance distance (TD) important role in rounding up or down the co-ordinate values at certain extent.

Encryption:

The process of converting the plaintext to human non Understandable form, so that if the data is obtained by third Party person then they will not able to understand or retrieve It.

Decryption:

The location co-ordinates which were used as key while encryption must be matched with co-ordinates values fetched by GPS device at receiver side. If this condition is satisfied then only user can decrypt the data otherwise encrypted file will be discarded from the system automatically. [6]

Geolock mapping function have eight inputs:

i) First, user enters username and passwords.

ii) This username and password collectively called label. This clients label is sent to cloud.

iii) Searching for the similar label and retrieving it is done on cloud.

iv) By using this information and geoencryption algorithm encryption of data takes place. And this encrypted data is send to the user. Users Mobile receives that encrypted data.

v) Anti-spoof GPS is used to measure the users location and delivers the location to the user’s computer.

vi) Then calculate the geolock code by using the mapping table.

vii) Geolock Encrypted key=Session key.

viii) Finally decrypts the data by using this session key.

II. Literature Survey

i) On location models for ubiquitous computing:-

Common queries regarding information processing in ubiquitous computing are based on the location of physical objects

ii) Securing Sensor Networks with Location-Based Keys:-

Based on location based keys, we develop a node-to-node authentication scheme, which is not only able to localize the impact of compromised nodes within their vicinity, but also to facilitate the establishment of pair wise keys between neighboring nodes.

iii) A Survey on Location Based Data Encryption:-

This paper presents a brief survey of Location based services, the technologies deployed to track the mobile user's location, the accuracy and reliability associated with such measurements, the network infrastructure elements deployed by the wireless network operators to enable these kinds of services Algorithms for Mobile Devices.

iv) Taint Droid an Information-Flow Tracking System for Real time Privacy:-

Smart phone operating systems frequently fail to provide users with adequate control over and visibility into how third-party applications use their private data.

v) Location Based Services using Android Mobile Operating System:-

The motivation for every location based information system is to assist with the exact information, at right place in real time with personalized setup and location sensitiveness.

vi) Location Based Services using Android:-

Two such major factors are web browser and GPS services.

vii) Context Sensitive Access Control:-

We response context-sensitive verification methods that allow checking the user's claimed authenticity in various ways and to various degrees.[7]

III. Existing System

This technology which enable individuals, companies and etc. To store their data and information on the cloud and they can access their own data at any time, from any place and using any computer through the internet.

It is even possible to deploy a platform in a cloud and Use it (instead of installing software on a personal computer).

Disadvantages of Existing System

i) Regarding the current structure of cloud computing, this method is considered not fully developed and gradually progresses toward evolution.

ii) The biggest challenge raised about cloud computing and many researchers are working on it, is "security".

iii) Users (people, companies, institutions and etc.) do not know what will happen to their data and information in the cloud and whether other people can gain access to their data and so on.

Comparison SYSTEM

a) Existing System:-A one-time password (OTP) is a password that is valid for only one login session or transaction.

b) Proposed System:-To overcome the drawbacks of the existing system we design our new system. In this system we are concentrating on the security of the confidential data. In our proposed system, it not only checks the authorized log in but also checks the location of the user at the time of log in.

IV. Proposed System

Data security in the cloud is very important. Users (individuals or companies) are concerned about the access to the information by unauthorized users.

Now suppose that data is some critical and confidential information from a bank, or a company. Certainly the necessity of access control in the cloud computing is more than ever and is a very important part of data security in cloud.

In our method we use the user's location and geographical position and we will add a security layer to the existing security measures.

Our solution is more appropriate for banks, big companies, institutions and examples like this. The only thing we need is an Anti-Spoof and accurate GPS that company can afford to buy. Also implementing the Geo- Encryption algorithm on the cloud and the user's computer (which is connected to the GPS) is required.

As we have already mentioned in previous section, data security in the cloud is very important. As we are implementing the bank application, bank data is stored on cloud. This data is critical and confidential. So the access control to such information in cloud is very important part of data security in cloud.

As we know that encryption, decryption etc. are used to secure the data access in cloud. But it is not sufficient to secure the data in cloud. So to provide extra security layer we use user location and geographical position. To provide this, we need Anti-spoof GPS which is very accurate and it can give us the latitude, longitude and altitude accurately. Label can be given to data which is stored on cloud. Index table contains this label and refers to user's geographic location and timeframe. Label and data stored on cloud can be added manually or automatically.

Nowadays we use username and password to provide security to data access stored on cloud in many applications such as banks, big companies, institutions etc. But this security is not sufficient to cloud data access. Because any unauthorized user can access data on cloud easily from any location. So to provide extra security to cloud data access we use location based encryption. By using this method, we can avoid any unauthorized access. is also considered in final key, which provides a range of location coordinates to the client to decrypt the data, it increase the accuracy & inconsistency of coordinates. Time, as constraints could be used on the decryption location.

Advantages

1. Military- In military this technology can be used to keep the data secured from the attackers during wars.
2. Banks- This technology can also be used in banking for the purpose of money transaction.
3. Individual use- It can also be used to store one's confidential data. For e.g.: for business purpose.
4. Multinational Industries-In Industries important data can be secure by using this technology.
5. College-In college's important data can be secure by using this technology. For e.g. Question paper.
6. Data security in cloud.
7. It is more appropriate for banks, big companies, Institutions.
8. Save time and money
9. Instant access from any mobile device.

ALGORITHM USESD FOR PROPOSED SYSTEM

i) LOCATION-BASED DATA ENCRYPTION

Location-based encryption technique is used for encryption wherein the cipher text can be decrypted at a specified location. If someone try to decrypt the data at another location the decryption processes fails and no information about the plain text. The device performing the decryption and determine its location by using.[8,9]

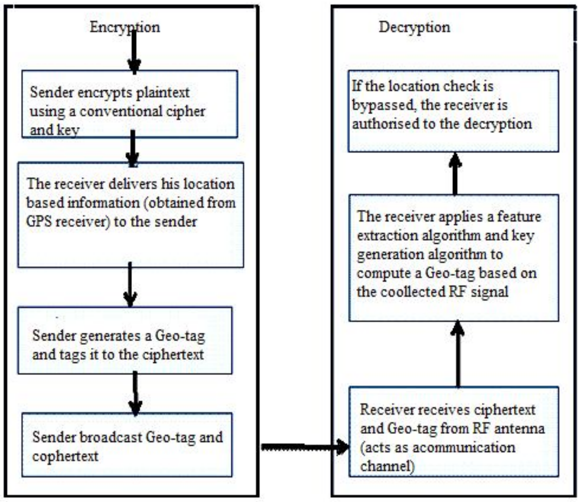
Encryption
Sender encrypts plaintext using a conventional cipher and key
The receiver delivers his location based information (obtained from GPS receiver) to the sender
Sender generates a Geo-tag and tags it to the ciphertext
Sender broadcast Geo-tag and cophertext
Decryption
If the location check is bypassed, the receiver is authorised to the decryption
The receiver applies a feature extraction algorithm and key generation algorithm to compute a Geo-tag based on the coollected RF signal
Receiver receives ciphertext and Geo-tag from RF antenna (acts as acommunication channel)

Figure 1. Basic Geo-encryption Working

V. System Architecture

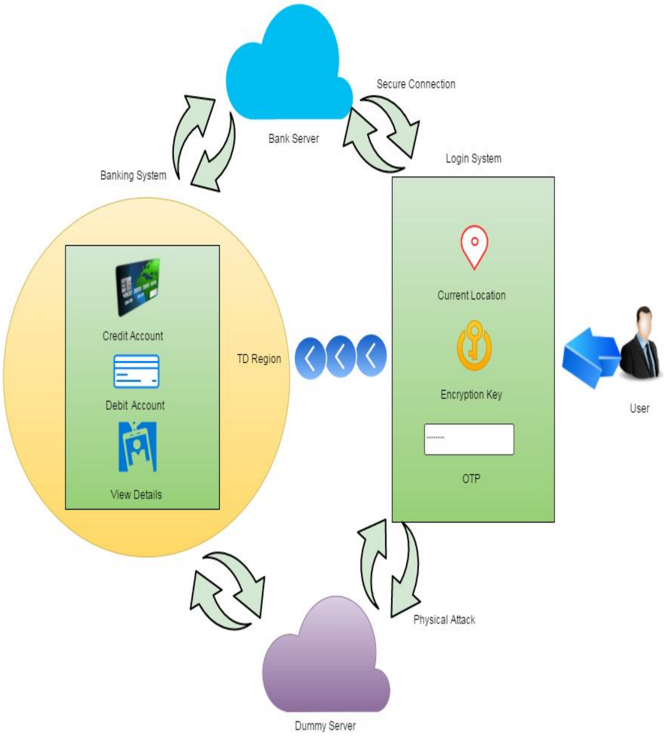

Figure 2. A sample of data flow diagram

In this system architecture user are registered first and then login in to the system from login page after that user's current location will be fetched and encryption key is generated.

While entering the valid OTP user can access the banking system through secure connection in given tolerance distance (TD). If the reverse password entered by user at that time user access banking system through dummy server.

VI. CONCLUSION AND FUTURE WORK

Location based encryption and “Geo- Encryption” algorithm 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.

Data access control is one of the most challenging issue in cloud computing. Also there are some advantage of cloud computing. So many people and company uses cloud computing. But there are some challenges in using cloud computing. So, to provide extra security layer to cloud we are using location based encryption technique. This method can be used for many applications such as banks, big companies, institutions, etc.

REFERENCES

[1] L. Scott, D. Denning, “A Location Based Encryption Technique and Some of Its Applications”, Proceedings of ION NTM 2003.

[2] H.Liao, P.Lee, Y.Chao, C.Chen, “A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security”, In The 9th International Conference on Advanced Communicate Technology, pp. 625-626, Feb. 2007.

[3] CloudHooks: “Security and Privacy Issue in Cloud Computing’’, Proceesing of the 44thHawai International conference on System Sciences-2011.

[4] Weiss, A.(2007) “Computing in the Clouds’’, Networker, Vol 11, No. 4, pp:16-25, December 2007.

[5] Loganscott& Dorothy E. Denning, “Location Based Encryption & Its Role in Digital Cinema distribution’’, Proccedings of ION GPS/GNSS 2003, pp 288-297.

[6] GurudattKulkarni 1 et al, “Cloud Security Challenges’’, 7th International Conference on telecommunication systems, Srevices and Applications(TSSA),IEEE,2012.

[7] Meer SoheilAbolghasemi, Mahdi sefidab, Reza EbrahimiAtani, “Using Location Based Encryption to Improve the Security of Data Access in Cloud Computing’’, international conference on advances in computing2013.

[8] Dax, J. "Publikationen." To appear in Distributed User Interfaces: Collaboration and Usability. Springer 2014 (2013).

[9] Kuseler, Torben, and Ihsan Alshahib Lami. "Using geographical location as an authentication factor to enhance mCommerce applications on smartphones."International Journal of Computer Science and Security (IJCSS) 6.4 (2012): 277-287.

[10] Shamir, Adi. "How to share a secret." Communications of the ACM 22.11 (1979): 612-613