Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 12, December -2016

Overview of Data Security by Location Based Encryption for Banking Application

Waykar Rasika V[1], Naikodi Ravina J[2], Kadam Snehal M[3] And Prof. N.S.Jadhav[4]

Department of Computer Engineering, Jaihind College of Engineering,Kuran

Abstract - *Cloud computing may be a new approach within the field of data technology and development of mobile technologies supported the globe Wide internet. One among the foremost vital challenges during this space is that the security of cloud computing. On the opposite hand the protection of access to crucial and counselling in banks, establishments and etc. is extraordinarily essential. Typically even with the large prices, it's not totally secured and it's compromised by the attackers. By providing a unique technique, we tend to improve the protection of information access in cloud computing for an organization or the other specific locations mistreatment the location-based encoding. The wide unfold of wireless local area network and therefore the quality of mobile devices will increase the frequency of information transmission among mobile users. However, most of the info encoding technology is location-independent. Associate degree encrypted knowledge is decrypted anyplace. The encoding technology cannot prohibit the situation of information cryptography. So as to satisfy the demand of mobile users within the future, a location-dependent approach, known as location-dependent encryption formula (LDEA), is planned during this paper. A target latitude/longitude coordinate is decided first off. The coordinate is incorporated with a random key for encryption. The receiver will solely decode the cipher text once the coordinate inheritable from GPS receiver is matched with the target coordinate. However, current GPS receiver is quality and inconsistent. The situation of a mobile user is troublesome to precisely match with the target coordinate. A toleration distance (TD) is additionally designed in LDEA to extend its usefulness. The protection analysis shows that the chance to interrupt LDEA is sort of not possible since the length of the random secret is adjustable. An image is additionally enforced for experimental study. The results show that the cipher text will solely be decrypted beneath the restriction of TD. It illustrates that LDEA is effective and sensible for knowledge transmission in mobile setting.*

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

I. INTRODUCTION

Many ways are projected for the safety of information transmission. However, these ways are location-independent. The sender cannot prohibit the placement of the receiver for information cryptography. If the information secret writing formula will offer such operate, it's helpful for increasing the safety of mobile information transmission within the future. Therefore, a location-dependent encoding formula (LDEA) is projected in this paper. The latitude/longitude coordinate is employed as the key for encoding in LDEA. Once a target coordinate is set for encoding, the cipher text will solely be decrypted at the expected location. Since the GPS receiver is inaccurate and inconsistent looking on what percentage satellite signals received. It's tough for receiver to decode the cipher text at a similar location precisely matched with the target coordinate. It's impractical by exploitation the wrong GPS coordinate as key for encoding. Consequently, a toleration distance (TD) is intended in LDEA. The sender can also confirm the TD and also the receiver can decode the cipher text inside the region of TD. We are developing banking application exploitation Location primarily based secret writing, as compare to current banking application that is location-independent. It suggests that in Cryptography Cipher-text will solely be decrypted at a location i.e. location-dependent approach. If a shot to decode information at another location, the cryptography method fails and divulges no info regarding the plaintext. This is often necessary in real time application, example in military base application, Cinema Theater. However our system is versatile enough to supply access to client to his/her account from any location. Our system conjointly offer answer to physical attack exploitation virtualization, during which client is allowed to perform faux dealings for his/her physical security purpose.

II. PROPOSED SYSTEM

Data security within the cloud is thus necessary. Users (individuals or companies) are concerned regarding the access to the data by unauthorized users. Currently suppose that information is some crucial and confidential information from a bank, or a corporation and etc. actually the requirement of access management within the cloud computing is quite ever and is a very important a part of information security in cloud. In our methodology we have a tendency to use the user's location and geographical position and that we can add a security layer to the present security measures. Our resolution is additional acceptable for banks, big companies, establishments and examples like this. The sole factor we want is associate degree Anti-Spoof and correct GPS those companies will afford to shop for. Additionally implementing the location-dependent data encryption algorithm (LDEA), on the cloud and also the user's mobile (which is connected to the

GPS) is needed. We will label the info. Label contains name of the corporate or an individual who works within the company (for example the company's boss).
These labels are placed in associate degree index table that refers to the user's geographic location and also the timeframe thought of to access information, in a database. These labels and values of the database are often supplemental manually or automatically. For instance, suppose that a bank stores some information within the cloud and solely the controller will have access to that. The accountant's room is on the third floor of the bank's building and accountant's operating hours are from eight am to three pm. we will create the data within the cloud accessible solely among the accountant's room and his operating hours (in addition to the present security measures). As mentioned the new generation "Anti-Spoof" GPS is incredibly correct and might offer us the latitude, longitude and altitude accurately. As a result we will limit the info access to the room situated on a specific floor of a building and a specified timeframe. Another example: the information that may be accessible solely within the chief's room of various branches of a bank or a company. Within the usual technique, once users attempt to access the information, they use standard security measures and thus get access to the cloud.

III. METHODOLOGY

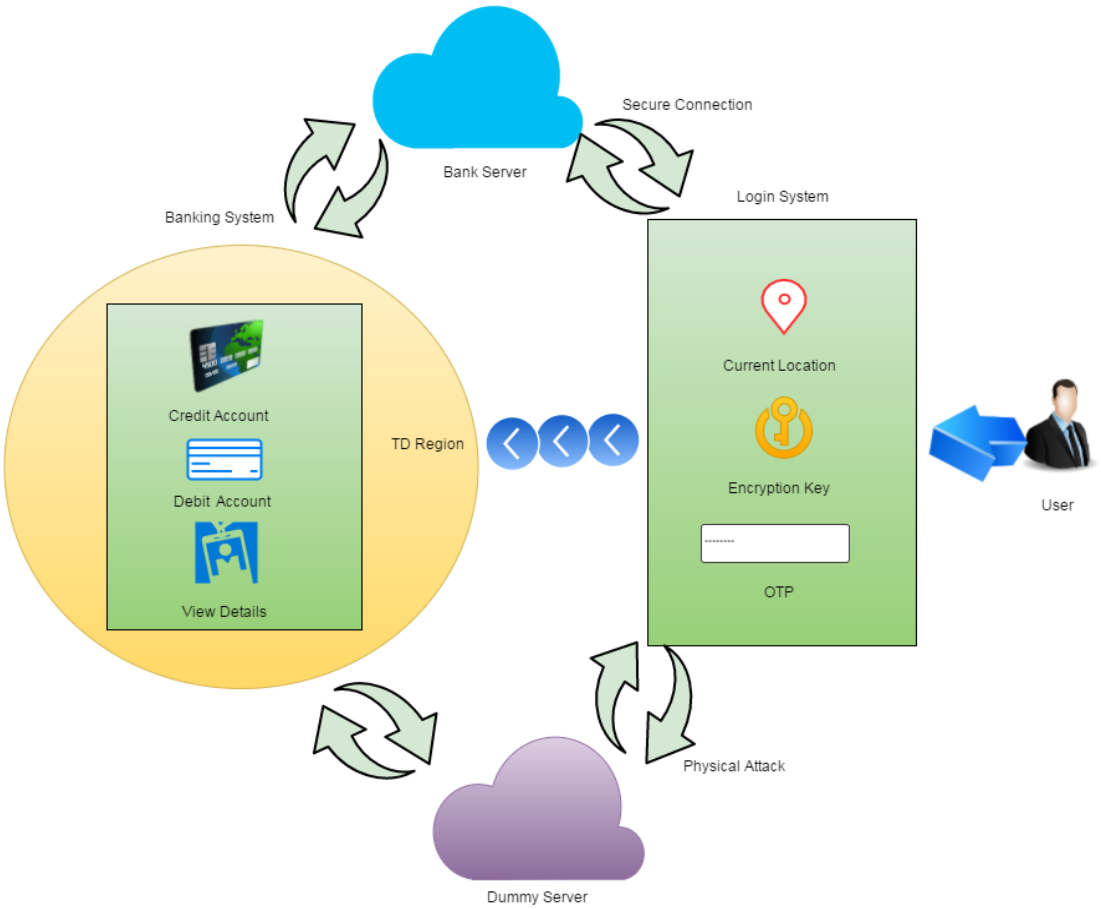


Fig 1: Architecture diagram of proposed system

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

3.1.1. User:
The user must login to his/her account with the credentials provided throughout the registration method. User current location is fetched and cross examined with the registered location if its similar then user will proceed with additional transaction else the transaction are going to be closed.

3.1.2. Bank Server:

It is main server meant for saving the information of user throughout transaction. User will credit, debit and enquiry regarding his/her account details.

3.1.3. Dummy Server:

The dummy server is for providing security from physical attack. It additionally works same as main server however the transaction created here are pretend i.e. the transaction doesn't have an effect on the users main account.

3.2. 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. The design of those systems is comparatively straightforward. 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.

3.2.1. Short Message Service

Short Message Service (SMS) could be a text electronic communication service element of phone, web, or mobile communication systems, exploitation standardized communications protocols that enable the exchange of short text messages between fastened line and itinerant devices. SMS text electronic communication is that the most generally used knowledge application within the world, with 3.6 billion active users, or seventy eight of all itinerant subscribers. The term SMS is employed as an equivalent word for all sorts of short text electronic communication in addition because the user activity itself in several components of the globe. Straightforward user generated text message services - embrace news, sport, financial, language and placement primarily based services, in addition as several early samples of mobile commerce like stocks and share costs, mobile banking facilities and leisure booking services. SMS has used on fashionable handsets originated from radio telegraphy in radio memoranda pagers exploitation standardized phone protocols and later outlined as a part of the world System for Mobile Communications (GSM) series of standards in 1985] as a method of causing messages of up to one hundred sixty characters, to and from GSM mobile handsets. Since then, support for the service has dilated to incorporate alternative mobile technologies like ANSI CDMA networks and Digital AMPS, in addition as satellite and land line networks. Most SMS messages are mobile-to-mobile text messages although the quality supports alternative styles of broadcast electronic communication in addition.

3.2.2. GSM Technology

GSM could be a cellular network, which implies that cellphones connect with it by checking out cells within the immediate neighborhood. There square measure five completely different cell sizes in an exceedingly GSM network. The coverage space of every cell varies per the implementation atmosphere. Indoor coverage is additionally supported by GSM. GSM uses many crypto logical algorithms for security. A convenient facility of the GSM network is that the short message service. The Short Message Service – purpose to purpose (SMS-PP) was originally outlined in GSM recommendation that is currently maintained in 3GPP as TS twenty three.040. GSM 03.41 (now 3GPP TS twenty three.041) defines the Short Message Service – Cell Broadcast (SMS-CB), that permits messages (advertising, public data, etc.) to be broadcast to any or all mobile users in an exceedingly nominal geographic region. Messages square measure sent to a brief message service center (SMSC) that provides a "store and forward" mechanism. It makes an attempt to send messages to the SMSC's recipients. If the subscriber's mobile unit is power-driven off or has left the coverage space, the message is hold on and offered back to the subscriber once the mobile is power-driven on or has reentered the coverage space of the network. This operate ensures that the message are going to be received.

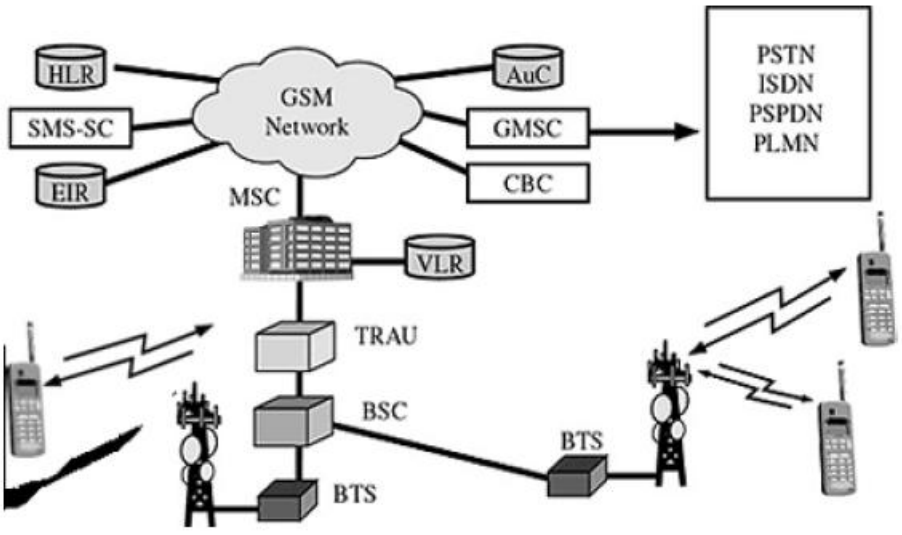


Fig 2: GSM Network along with SMSC

Both mobile terminated (MT, for messages sent to a mobile handset) and mobile originating (MO, for those sent from the mobile handset) operations are supported. In Message delivery, delay or complete loss of a message is uncommon, typically affecting less than 5% of messages.

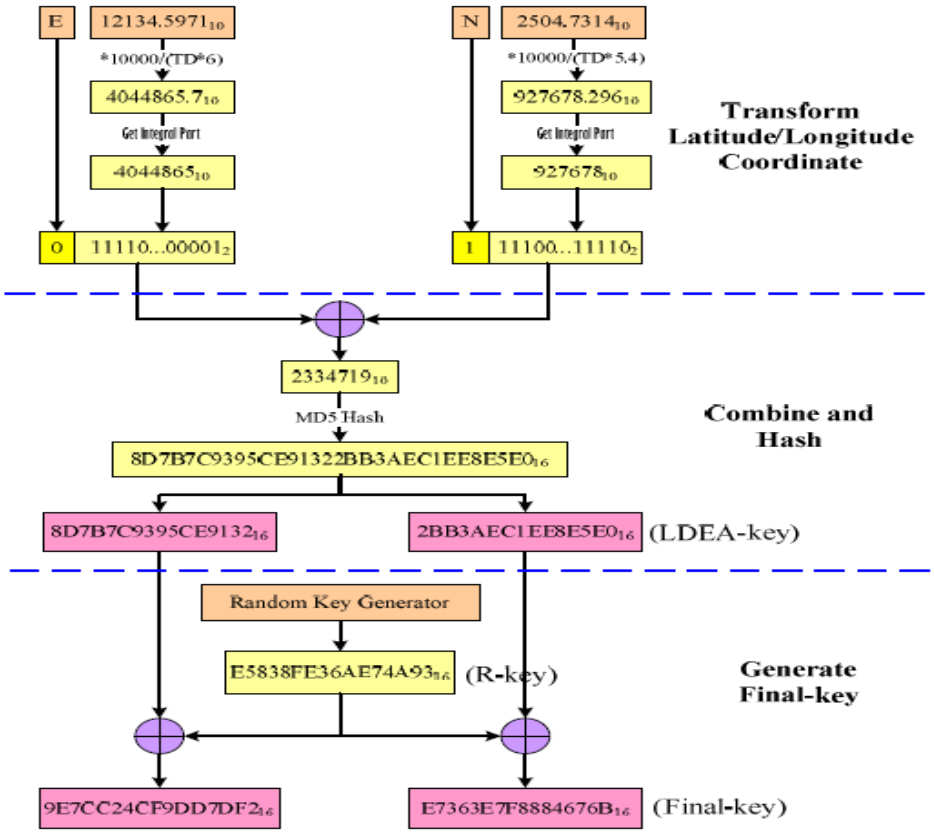
3.2.3. GPS Technology

The Global Positioning System (GPS), additionally referred to as Navstar, could be a world navigation satellite system (GNSS) that has location and time data altogether climatic conditions, anyplace on or close to the planet wherever there's associate degree unobstructed line of sight to four or a lot of GPS satellites. The GPS system operates severally of any

telecommunication or web reception, though' these technologies will enhance the utility of the GPS positioning data. The GPS system provides essential positioning capabilities to military, civil, and industrial users round the world. The US government created the system, maintains it, and makes it freely accessible to anyone with a GPS receiver. The GPS conception is predicated on time and also the celebrated position of specialized satellites. The satellites carry terribly stable atomic clocks that square measure synchronized with each other and to ground clocks. Any drift from true time maintained on the bottom is corrected daily. Likewise, the satellite locations square measure celebrated with nice exactness. GPS receivers have clocks as well; but, they're typically not synchronized with true time, and square measure less stable. GPS satellites ceaselessly transmit their current time and position. A GPS receiver monitors multiple satellites and solves equations to see the precise position of the receiver and its deviation from true time. At a minimum, four satellites should be visible of the receiver for it to work out four unknown quantities (three position coordinates and clock deviation from satellite time).

3.3.Algorithm

LDEA(Location dependant Data Encryption Algorithm) Algorithm:



IV. CONCLUSION

Traditional encryption technology cannot prohibit the location of mobile users for information decoding. So as to satisfy the demand of mobile users in the future, LDEA algorithmic rule is projected in this paper. LDEA give a brand new operate by exploitation the latitude/longitude coordinate as the key of information encoding. A toleration distance (TD) is additionally designed to beat the quality and inconsistent of GPS receiver. The protection strength of LDEA is adjustable once necessary. The experimental results of the prototype additionally show that the decoding is forced by the range of TD. As a result, LDEA is effective and sensible for the information transmission within the mobile surroundings. The LDEA algorithms will be extended to the other application domains, e.g., the authorization of mobile software. If mobile software is permitted at intervals a pre-defined area, such as a town, the execution of the code might activate the placement check supported the LDEA rule. The code will be dead only the user is at intervals the approved area. Besides, the distribution of transmission content could also be utilized the LDEA algorithm for advanced access management except the username/password. The projected LDEA algorithm provides a brand new method for information security. It's additionally meeting the trend of mobile computing. Several potential applications are going to be developed within the future to demonstrate and promote the thought of LDEA algorithm. The projected technique will be utilized in many places like banks, big companies, and institutions to satisfy the specified performance.

REFERENCES

1. Bilal Shebaro, Oyindamola Oluwatimi, and Elisa Bertino, Fellow, Context-Based Access Control System for Mobile Devices IEEE,2015.

2. Hsien-Chou Liao and Yun-Hsiang Chao, LDEA : Data Encryption Algorithm Based on Location of Mobile Users IEEE Transaction on Cyber Security

3. 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.

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

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

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

7. Jamil, T., 2004. The Rijndael Algorithm. IEEE Potentials, 23 (2): 36-38.

8. 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.

9. 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.

10. 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.

