ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Security Using Locations Based Encryption for Online Transaction

Priyanka Walunj[1], Shital Zaware[2], Manjushri Tambe[3], Shubhangi Shruti Patil[4]

Department of Computer Engineering, SKN Sinhgad Institute of Technology and Science, Lonavala, India

ABSTRACT: Cloud computing may be a new approach within the field of information technology and development of computer technologies supported the globe Wide internet. One in all 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 confidential information in banks, institutions and etc. is very essential. Generally even with the large prices, it's not absolutely secure and it's compromised by the attackers. By providing a completely unique technique, we tend to improve the protection of information access in cloud computing for a corporation or the other specific locations mistreatment the location-based cryptography. 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 information cryptography technology is location-independent. Associate encrypted information will be decrypted anyplace. The cryptography technology cannot limit the situation of information secret writing. So as to fulfil the demand of mobile users within the future, a location-dependent approach, known as location-dependent encoding algorithm (LDEA), is projected during this paper. A target latitude/longitude coordinate is set foremost. The coordinate is incorporated with a random key for encoding. The receiver will solely decipher the cipher text once the coordinate acquired from GPS receiver is matched with the target coordinate. However, current GPS receiver is inaccuracy and inconsistent. The situation of a mobile user is tough 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 likelihood to interrupt LDEA is nearly not possible since the length of the random secret's adjustable. An example is additionally enforced for experimental study. The results show that the cipher text will solely be decrypted under the restriction of TD. It illustrates that LDEA is effective and sensible for information transmission in mobile setting.

KEYWORDS: Data encryption, GPS, mobile computing, location-based service, LDEA.

I. Introduction

Many strategies are planned for the protection of information transmission. However, these strategies are location-independent. The sender cannot limit the location of the receiver for information decoding. If the data encryption algorithm will offer such operate, it's helpful for increasing the protection of mobile information transmission within the future. Therefore, a location-dependent encryption algorithm (LDEA) is planned in this paper. The latitude/longitude coordinate is employed as the key for encryption in LDEA. Once a target coordinate is set for encryption, the cipher text will only be decrypted at the expected location. Since the GPS receiver is inaccurate and inconsistent counting on what percentage satellite signals received. It's troublesome for receiver to rewrite the cipher text at constant location specifically matched with the target coordinate. It's impractical by mistreatment the wrong GPS coordinate as key for encryption. Consequently, a toleration distance (TD) is intended in LDEA. The sender can also verify the TD and also the receiver can rewrite the cipher text inside the region of TD. We are developing banking application using Location based encoding. As compare to current banking application that is location-independent, we are developing banking application that is location dependent. It means that in Cryptography Cipher-text will solely be decrypted at a specific location i.e. location-dependent approach. If a trial to rewrite information at another location, the decoding method fails and divulges no data regarding the plaintext. This is often vital in real time application, example in military base application, Cinema Theatre. However our system is versatile enough to produce access to client to his/her account from any location. Our system additionally offer answer to physical attack using virtualization, within which customer is allowed to perform pretend dealings for his/her physical security purpose.

DOI: 10.15680/IJIRCCE.2016. 0410141

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

II. LITRATURE SURVEY

1] On location models for ubiquitous computing
Published Year: 2014
AUTHORS:Christian Becker Æ Frank Du rr
Common queries relating to information processing in present computing are supported the location of physical objects. Regardless of whether or not it's the next printer, next eating place, or a friend is looked for, a notion of distances between objects is needed. A pursuit for all objects in a very bound geographic region needs the chance to outline spatial ranges and spatial inclusion of locations. In this paper, they tend to discuss general properties of symbolic and geometric coordinates. They gift a summary of existing location models letting position, range, and nearest neighbour queries. The location models are classified consistent with their quality with relevance the question process and also the concerned modelling effort alongside different needs. Besides summary of existing location models and approaches, the classification of location models with relevance application needs will assist developers in their style choices.
.

2]Location Based Services using Android Mobile Operating System
Published Year: 2011
AUTHORS: Amit Kushwaha1, VineetKushwaha
The motivation for each location primarily based system is: “To assist with the precise data, at right place in real time with customized setup and placement sensitiveness”. In this era we are managing palmtops and iPhones that are attending to replace the large desktops even for machine functions. We’ve got huge variety of applications and usage wherever an individual sitting in a very roadside café has to get relevant information and data. Such wants will solely be catered with the assistance of LBS. These applications embrace security connected jobs, general survey relating to traffic patterns, call supported transport data for validity of registration and license numbers etc. a really appealing application includes police work wherever instant data is required to determine if the individuals being monitored are any real threat or an incorrect target. We’ve got been ready to produce variety of various applications wherever we offer the user with data relating to an area he or she needs to go to. However these applications are restricted to desktops solely. We want to import them on mobile devices. We should make sure that individual once visiting places needn't carry the travel guides with him. All the knowledge should be out there in his mobile device and additionally in user custom format.

3]Location Based Services using Android
Published Year: 2009
AUTHORS: Sandeep Kumar, Mohammed Abdul Qadeer, Archana Gupta
Initially mobile phones were developed just for spoken language however currently days the situation has modified, spoken language is simply one facet of a mobile phone. There are alternative aspects that are major focus of interest. Two such major factors are applications programme and GPS services. Each of those functionalities is already enforced however are solely within the hands of makers not within the hands of users thanks to proprietary problems, the system doesn't enable the user to access the mobile hardware directly. But now, once the discharge of android based open supply mobile a user will access the hardware directly and design custom-built native applications to develop web and GPS enabled services and might program the other hardware elements like camera etc. during this paper we are going to discuss the facilities accessible in mechanical man platform for implementing LBS services (geo-services).

4]Context Sensitive Access Control
Published Year: 2005
AUTHORS**:** R.J. Hulsebosch†, A.H. Salden, M.S. Bargh, P.W.G. Ebben, J. Reitsma
We investigate the sensible feasibleness of using context data for controlling access to services. Primarily based solely on situational context, we have a tendency to show that users will be transparently provided anonymous access to services which service suppliers will still impose varied security levels. Thereto, we have a tendency to propose context-sensitive verification strategies that enable checking the user’s claimed believability in varied ways that and to numerous degrees. A lot of exactly, typical data management approaches are accustomed compare historic discourse (service usage) knowledge of a personal user or cluster. The result's a comparatively robust, less intrusive and a lot of

versatile access management method that mimics our natural manner of authentication and authorization within the physical world.

III.PROPOSED SYSTEM

Data security in the cloud is so vital. Users (individuals or companies) are involved concerning the access to the information by unauthorized users. Currently suppose that information is a few essential and counselling from a bank, or an organization and etc. actually the requirement of access management within the cloud computing is over ever and could be a vital a part of information security in cloud. In our methodology we use the user's location and geographical position and that we can add a security layer to the present security measures. Our answer is a lot of applicable for banks, massive companies, institutions and examples like this. The sole issue we'd like is an Anti-Spoof and correct GPS those companies will afford to shop for. Additionally implementing the location-dependent encryption rule (LDEA), on the cloud and therefore the user's pc (which is connected to the GPS) is needed. We are able to label the information. 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 an index table that refers to the user's geographic location and therefore the timeframe thought of to access information, in a database. These labels and values of the info are often further manually or mechanically. For instance, suppose that a bank stores some data within the cloud and solely the controller will have access to that. The accountant's space is on the third floor of the bank's building and accountant's operating hours are from eight am to three pm. we are able to create the knowledge within the cloud on the market solely inside the accountant's space and his operating hours (in addition to the present security measures). As mentioned the new generation “Anti-Spoof” GPS is extremely correct and might provide us the latitude, meridian and altitude accurately. As a result we are able to limit the information access to the space placed on a selected floor of a building and a fixed timeframe. Another example: the knowledge that may be on the market solely within the chief's space of various branches of a bank or an organization. Within the usual technique, once users plan to access the information, they use customary security measures and so get access to the cloud.

A. SYSTEM MODEL

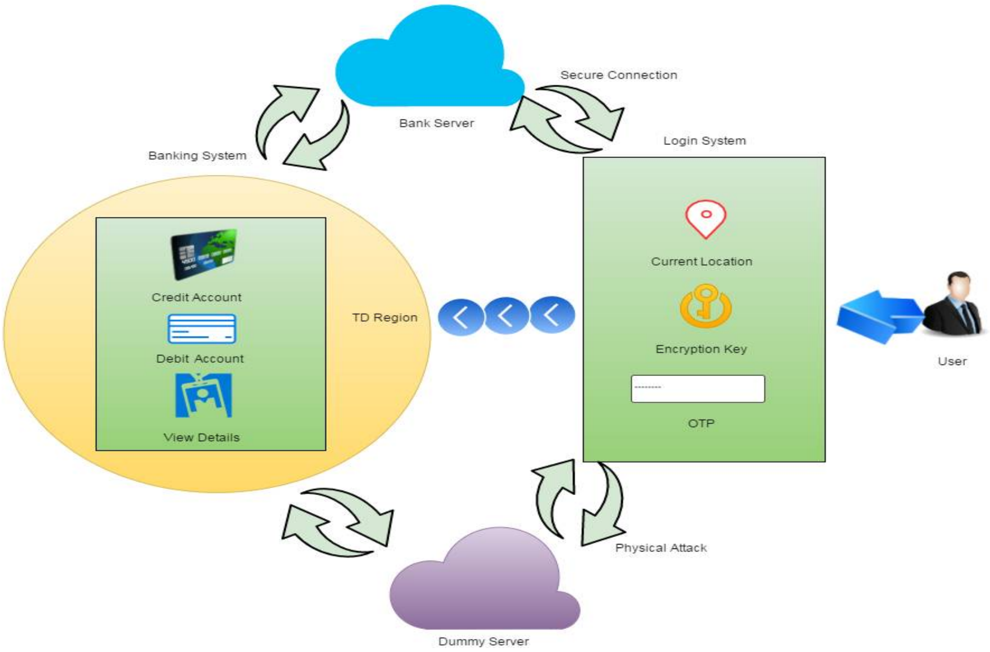

Fig 1: Architecture diagram of proposed system

B. THE PROPOSED SYSTEM CONSISTS OF THE BANK SERVER, DUMMY SERVER, USER.

i. 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.

ii. ***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.

iii**.** ***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.

iv. ***THIRD-PARTY PROVIDER SOLUTIONS***

For previous few years, an enormous varies of third-parties providing to deliver alert messages (and totally different information services) via text electronic communication services. The planning of these systems is relatively simple. Whether or not activated through an internet interface, directly from a phone, or as software running on a field administrator's portable computer, these services act as SMS aggregators and inject text messages into the network. Among the event of Associate in Nursing emergency message is shipped to the service centre from the victim or footer mobile.

iii. a. ***SHORT MESSAGE SERVICE***

Short Message Service (SMS) can be a text transmission service component of phone, web, or mobile communication systems, exploitation standardized communications protocols that change the exchange of short text messages between fixed line and itinerant devices. SMS text transmission is that the foremost usually used data application inside the planet, with 3.6 billion active users, or seventy eight of all itinerant subscribers. The term SMS is used as identical word for all types of short text transmission additionally as a result of the user activity itself in many parts of the world. simple user generated text message services - embrace news, sport, financial, language and placement based totally 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 printed 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 land line networks. Most SMS messages are mobile-to-mobile text messages though the standard supports various sorts of broadcast transmission additionally.

iii. b. ***GSM TECHNOLOGY***

GSM might be a cellular network, which means that cell phones connect with it by searching for cells among the immediate neighbourhood. There unit five completely totally different cell sizes in an extremely GSM network. The coverage house of each cell varies per the implementation atmosphere. Indoor coverage is in addition supported by GSM. GSM uses several 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 printed in GSM recommendation that's presently maintained in 3GPP as TS twenty 3.040. GSM 03.41 (now 3GPP TS twenty 3.041) defines the Short Message Service – Cell Broadcast (SMS-CB), that allows messages (advertising, public information, etc.) to be broadcast to any or all mobile users in an extremely nominal region. Messages unit sent to a quick message service centre (SMSC) that gives a "store and forward" mechanism. It makes a shot to send messages to the SMSC's recipients. If the subscriber's mobile unit is powered off or has left the coverage house, the message is hold on and offered back to the subscriber once the mobile is powered on or has re-entered the coverage house of the network. This operate ensures that the message are getting to be received. 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 unusual, generally poignant but five-hitter of messages.

iii. c. ***GPS TECHNOLOGY***

The Global Positioning System (GPS), in addition said as Navstar, may well be a world navigation satellite system (GNSS) that has location and time knowledge altogether weather conditions, anywhere on or near the earth where there is academic degree clear line of sight to four or plenty of GPS satellites. The GPS system operates severally of any telecommunication or net reception, though' these technologies can enhance the utility of the GPS positioning knowledge. The GPS system provides essential positioning capabilities to military, civil, and industrial users around 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 based on time and additionally the celebrated position of specialized satellites. The satellites carry very stable atomic clocks that square measure synchronous with one another and to ground clocks. Any drift from true time maintained on very cheap is corrected daily. Likewise, the satellite locations unit of measurement celebrated with nice accuracy. GPS receivers have clocks as well; however, they are generally not synchronous with true time, and unit of measurement less stable. GPS satellites incessantly transmit their current time and position. A GPS receiver monitors multiple satellites and solves equations to check the precise position of the receiver and its deviation from true time. At a minimum, four satellites ought to be visible of the receiver for it to figure out four unknown quantities (three position coordinates and clock deviation from satellite time).

IV. CONCLUSION

Traditional coding technology cannot limit the situation of mobile users for information decoding. So as to fulfil the demand of mobile users in the future, LDEA algorithmic rule is projected in this paper. LDEA offer a brand new performs by exploitation the latitude/longitude coordinate as the key of data encryption. 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 image conjointly show that the decoding is forced by the region of TD. As a result, LDEA is effective and sensible for the info 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 among a pre-defined space, like a town, the execution of the software could activate the location check based on the LDEA algorithmic rule. The software will be executed only if the user is among the authorized space. Besides, the distribution of multimedia system content is also utilised the LDEA algorithm for advanced access management except the username/password. The projected LDEA algorithm provides a brand new manner for information security. It’s conjointly meeting the trend of mobile computing. Several potential applications are developed within the future to demonstrate and promote the construct of LDEA algorithm.

V. ACKNOWLEDGMENT

We might need to convey the analysts and additionally distributers for creating their assets accessible. We additionally appreciative to commentator for their important recommendations furthermore thank the college powers for giving the obliged base and backing.

REFRENCES

[1] Wikipedia, (May 2013). Samsung galaxy s4 specifications. [Online]. Available: http://en.wikipedia.org/wiki/Samsung_ Galaxy_S4
[2] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, “Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones,” in Proc. 9th USENIX Conf. Oper. Syst. Des. Implementation, 2010, pp. 1–6.
[3] J. Leyden, (Apr. 2013). Your phone may not be spying on you now—but it soon will be. [Online]. Available: http://www.theregister.co.uk/2013/04/24/kaspersky_mobile_malware_infosec/

[4] R. Templeman, Z. Rahman, D. J. Crandall, and A. Kapadia, “Placeraider: Virtual theft in physical spaces with smartphones,” in Proc. 20th Annual Netw. Distrib. Syst. Security Symp. (NDSS), Feb. 2013.
[5] R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang, “Soundcomber: A stealthy and context-aware sound trojan for smartphones,” in Proc. 18th Annu. Netw. Distrib. Syst. Security Symp., Feb. 2011, pp. 17–33.[6] L. L. N. Laboratory, Controlled items that are prohibited on llnlproporty. (2013). [Online]. Available: https://www.llnl.gov/ about/controlleditems.html
[7] M. Conti, V. T. N. Nguyen, and B. Crispo, “Crepe: Context-related policy enforcement for android,” in Proc. 13th Int. Conf. Inf. Security, 2011, pp. 331–345.
[8] A. Kushwaha and V. Kushwaha, “Location based services using android mobile operating system,” Int. J. Adv. Eng. Technol., vol. 1, no. 1, pp. 14–20, 2011.
[9] S. Kumar, M. A. Qadeer, and A. Gupta, “Location based services using android,” in Proc. 3rd IEEE Int. Conf. Internet Multimedia Serv. Archit. Appl., pp. 335–339.
[10] M. S. Kirkpatrick and E. Bertino, “Enforcing spatial constraints for mobile RBAC systems,” in Proc. 15th ACM Symp. Access Control Models Technol., 2010, pp. 99–108.
[11] A. Gupta, M. Miettinen, N. Asokan, and M. Nagy, “Intuitive security policy configuration in mobile devices using context profiling,” in Proc. IEEE Int. Conf. Soc. Comput., 2012, pp. 471–480.
[12] W. Enck, M. Ongtang, and P. McDaniel, “Understanding android security,” IEEE Security Privacy, vol. 7, no. 1, pp. 50–57, Jan. 2009.
[13] E. Trevisani and A. Vitaletti, “Cell-id location technique, limits and benefits: An experimental study,” in Proc. 6th IEEE Workshop Mobile Comput. Syst. Appl., 2004, pp. 51–60.
[14] J. LaMance, J. DeSalas, and J. Jarvinen, AGPS: A low-infrastructure approach. (2002). [Online]. Available: http://www.gpsworld. com/innovation-assisted-gps-a-low-infrastructure-approach/.
[15] Sky hook. (2003). [Online]. Available: http://www.skyhookwireless.com/.
[16] O. G. CONSORTIUM, “Open gis simple features specification for sql. revision 1.1,” 1999.
[17] M. Shehab, G. Cheek, H. Touati, A. Squicciarini, and P.-C. Cheng, “User centric policy management in online social networks,” in Proc. IEEE Int. Symp. Policies Distrib. Syst. Netw., 2010, pp. 9–13.
[18] R. W. Reeder, L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vaniea, “More than skin deep: Measuring effects of the underlying model on access-control system usability,” in Proc. ACM SIGCHI Conf. Human Factors Comput. Syst., 2011, pp. 2065–2074. [Online]. Available: http://doi.acm.org/10.1145/1978942.1979243.
[19] L. Cranor and S. Garfinkel, Security and Usability. Cambridge, MA, USA: O’Reilly Media, Inc., 2005.
[20] K. Fisler and S. Krishnamurthi, “A model of triangulating environments for policy authoring,” in Proc. 15th ACM Symp. Access Control Models Technol., 2010, pp. 3–12 [Online]. Available: http:// doi.acm.org/10.1145/1809842.1809847.