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

# Smart Technology:A Mobile Device using Context Management System

[1]Rohit Pardeshi, [2]Dipak Rathod, [3]Unati Salunke, [4]Sushma Ugale, [5]Prof.Minal Nerkar,

[1,2,3,4,]Department of Computer Engineering, AISSMS IOIT
[5] Asst Professor, Department of Computer Engineering, AISSMS IOIT

**Abstract –** *We investigate the sensible practicability of exploitation context data for dominant access to services. Based entirely on situational context, we show that users will be transparently provided anonymous access to services which service suppliers will still impose numerous security levels. Thereto, we propose context-sensitive verification strategies that permit checking the user's claimed legitimacy in numerous ways that and to numerous degrees. Additional exactly, standard data management approaches are wont to compare historic discourse (service usage) information of a personal user or cluster. The result's a comparatively robust, less intrusive and additional versatile access management method that mimics our natural means of authentication and authorization within the physical world.*

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

## I. INTRODUCTION

Cloud computing is a new approach within the field of information technology and development of computer technologies supported the World Wide Web. One among the foremost necessary challenges during this area is that the security of cloud computing. On the opposite hand the protection of access to important and steer in banks, establishments and etc. is very essential. Generally even with the large prices, it's not absolutely secured and it's compromised by the attackers. By providing a completely unique technique, we have a tendency to improve the protection of knowledge access in cloud computing for an organization or the other specific locations victimization the location-based secret writing. The wide unfold of local area network and also the quality of mobile devices will increase the frequency of knowledge transmission among mobile users. However, most of the information secret writing technology is location-independent. An encrypted knowledge are often decrypted anyplace. The encryption technology cannot limit the placement of knowledge decoding. In order to fulfill the demand of mobile users within the future, a location-dependent approach, referred to as location-dependent data encryption algorithm (LDEA), is projected during this paper. A target latitude/longitude coordinate is decided foremost. The coordinate is incorporated with a random key for data encryption. The receiver will solely rewrite the cipher text once the coordinate acquired from GPS receiver is matched with the target coordinate. However, current GPS receiver is quality and inconsistent. The placement 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 utility. The protection analysis shows that the chance to interrupt LDEA is almost not possible since the length of the random secret is 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 knowledge transmission in mobile surroundings.

This is 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 victimization virtualization, within which client is allowed to perform fake transaction for his/her physical security purpose.

## 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 neighbor 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, Vineet Kushwaha
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 programmer 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 within the cloud is therefore vital. Users (individuals or companies) are involved concerning the access to the data by unauthorized users. Currently suppose that information is a few vital and counseling from a bank, or an organization and etc. definitely the need of access management within the cloud computing is quite ever and could be a important part of information security in cloud. Several ways are planned for the safety of knowledge transmission. However, these ways are location-independent. The sender cannot limit the placement of the receiver for information decryption. If the information encoding algorithmic program will offer such operate, it's helpful for increasing the safety of mobile information transmission within the future. Therefore, a location-dependent data encryption algorithm (LDEA) is proposed during this paper. The latitude/longitude coordinate is employed because 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 depending on how many satellite signals received. It's difficult for receiver to decrypt the cipher text at constant location exactly matched with the target coordinate. It is impractical by victimization 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 therefore the receiver can decipher the cipher text inside the region of TD.
In our technique 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 answer is a lot of acceptable for banks, massive corporations, establishments and examples like this. The sole factor we'd like is associate degree Anti-Spoof and correct GPS those corporations will afford to shop for. Conjointly implementing the location-dependent encoding algorithmic program (LDEA), on the cloud and therefore the user's pc (which is connected to the GPS) is needed. We will 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-about to access information, in a very info. These labels and values of the info is additional manually or mechanically. As an example, suppose that a bank stores some info within the cloud and solely the accountant will have access to that. The accountant's area 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 offered solely inside the accountant's space and his operating hours (in addition to the existing security measures). As mentioned the new generation "Anti-Spoof" GPS is extremely correct and may offer us the latitude, meridian and altitude accurately. As a result we will limit the information access to the space placed on a selected floor of a building and a fixed timeframe. Another example: the data which will be offered solely within the chief's space of various branches of a bank or an organization. Within the usual technique, once users commit to access the information, they use commonplace security measures and so get access to the cloud.

## IV. METHODOLOGY

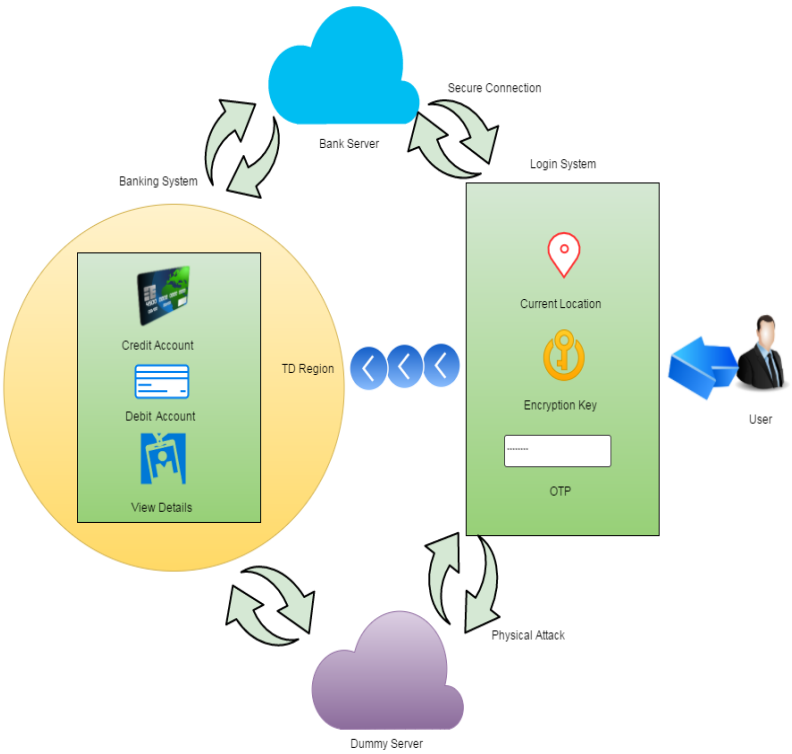


**Fig 1: Architecture diagram of proposed system**

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

#### 4.1.1. Bank Server:

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

#### 4.1.2. 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 any transaction else the dealings are going to be closed.

#### 4.1.3. 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.

.

### 4.2. 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.

**4.2.1. 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 ar mobile-to-mobile text messages although the quality supports alternative styles of broadcast electronic communication in addition.

**4.2.2. 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.

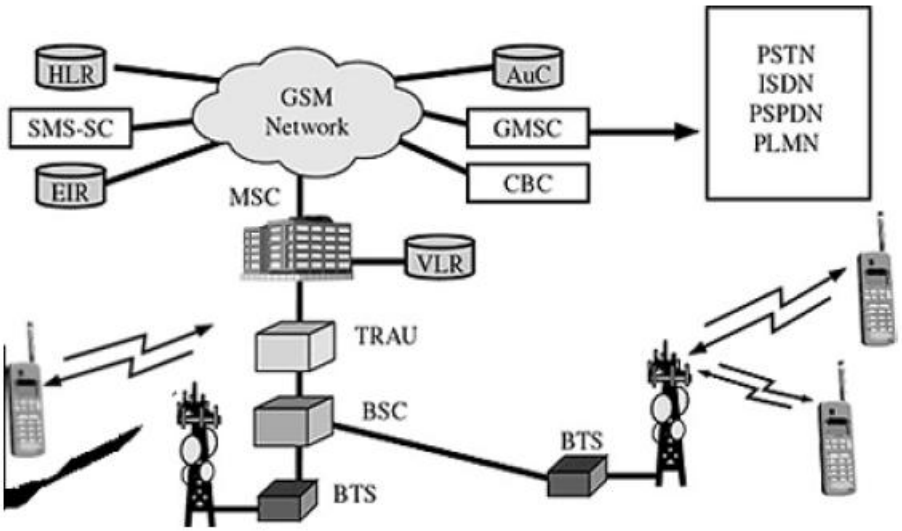


**Fig 2: GSM Network along with SMSC**

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.

**4.2.3. 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).

## V. CONCLUSION

Security in context aware environments would force solutions terribly different from those of today's systems that are predicated on comparatively stable, well-defined, consistent configurations, static contexts, and participants of security arrangements. For example, historically a user authentication mechanism is taken into account secure if it's a mixture of one thing the user has, one thing the user is aware of, or one thing the user is. what's required will be characterized by the term 'conformable security', within which the degree and nature of security related to any specific sort of action can amendment over time, with dynamical circumstances and with changing obtainable information therefore on suit the context .

We have additional context awareness as a fourth dimension to security. Context sensitive security exploits the power to sense and use discourse information to enhance or replace ancient user attributes like username/password for the aim of authentication and access management by creating security less intrusive and adaptable to situational or discourse changes. We've got incontestable this by concerning the access management method as a context aware service, whose objective is to grant or deny the access of a supplicant to a resource (e.g., a service) supported context information. The code will be executed only if the user is at intervals the approved area. Besides, the distribution of multimedia system content is also utilized the LDEA algorithm for advanced access management except the username/password. The planned LDEA algorithm provides a brand new means for information security. It's additionally meet the trend of mobile computing. Several doable applications are developed within the future to demonstrate and promote the thought of LDEA algorithmic program. The planned methodology will be employed in many places like banks, huge companies, and institutions to fulfill the required performance.

## REFERENCES

[1] 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.

[2] Becker, C. and F. Durr, 2005. On Location Models for Ubiquitous Computing. Personal and Ubiquitous 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.

[6] 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.

[7] 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.

[8] 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.

 