User Define Grid System

Akshay Gudhate[1], Ashraf Ansari[2], Nikhil Kakade[3], Suhail Shaikh[4], Prof. Tanuja Lonhari[5]
[1, 2, 3, 4, 5] Computer Department
[1, 2, 3, 4, 5] DYPIEMR,Akurdi,Pune

Abstract- *Cloud computing is a new approach in the field of information technology and development of computer technologies based on the World Wide Web. One of the most important challenges in this area is the security of cloud computing. On the other hand the security of access to critical and confidential information in banks, institutions and etc. is extremely essential. Sometimes even with the enormous costs, it is not fully guaranteed and it is compromised by the attackers. By providing a novel method, we improve the security of data access in cloud computing for a company or any other specific locations using the location-based encryption. The wide spread of WLAN and the popularity of mobile devices increases the frequency of data transmission among mobile users. However, most of the data encryption technology is location-independent. An encrypted data can be decrypted anywhere. The encryption technology cannot restrict the location of data decryption. In order to meet the demand of mobile users in the future, a location-dependent approach, called location-dependent data encryption algorithm (LDEA), is proposed in this paper. 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. However, current GPS receiver is inaccuracy and inconsistent. The location of a mobile user is difficult to exactly match with the target coordinate. A toleration distance (TD) is also designed in LDEA to increase its practicality. The security analysis shows that the probability to break LDEA is almost impossible since the length of the random key is adjustable. A prototype is also implemented for experimental study. The results show that the cipher text can only be decrypted under the restriction of TD. It illustrates that LDEA is effective and practical for data transmission in mobile environment.*

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

I. INTRODUCTION

The banking application utilizing Location Based cryptography, as contrast with current managing associate account application that square measure space autonomous, we square measure making banking application that is space subordinate. It implies in Cryptography Cipher-content must be decoded at a predefined space i.e. area subordinate approach. On the off chance that associate endeavor to decipher info at another space, the unscrambling procedure fizzles and uncovers no data concerning the plaintext. This is critical unendingly application, case in army installation application, Cinema Theater. However, our framework is sufficiently adaptable to offer access to consumer to his/her record from any space. Our framework additionally offer answer for physical assault utilizing virtualization, in which consumer is permissible to perform pretend exchange for his/her physical security reason.

Numerous techniques square measure planned for the security of knowledge transmission. Notwithstanding, these techniques are space free. The sender can't confine the space of the collector for info secret writing. In the event that the knowledge encryption calculation will offer such capability, it is valuable for expanding the safety of moveable info transmission presently. Subsequently, an space subordinate info cryptography calculation (LDEA) is planned during this paper. The scope/longitude facilitate is utilized because the key for info cryptography in LDEA. At the point once associate objective organize is resolved for info cryptography, the figure content must be unscrambled at the traditional space. Since the GPS recipient is off base and conflicting relying upon what number of satellite signs got. It is troublesome for beneficiary to unscramble the figure content at an analogous space exactly coordinated with the target facilitate. It is unfeasible by utilizing the off base GPS organize as key for info cryptography. Subsequently, a toleration remove (TD) is made public in LDEA. The sender will likewise decide the TD and the recipient can decipher the figure message within the scope of TD. We square measure making managing associate account application utilizing Location based mostly cryptography. As contrast with current managing associate account application that is space autonomous, we square measure making saving cash application that is space subordinate. It implies in Cryptography Cipher-content must be decoded at a planned space i.e. area subordinate approach. In the event that an attempt to decode info at another space, the unscrambling procedure fizzles and uncovers no data concerning the plaintext. This is critical unendingly application, case in army installation application, Cinema Theater. However, our

framework is sufficiently adaptable to offer access to consumer to his/her record from any space. Our framework additionally offer answer for physical assault utilizing virtualization, in which consumer is permissible to perform pretend exchange for his/her physical security reason.

II. LITERATURE SURVEY

1. Supporting Anonymous Location Queries in Mobile Environments with Privacy Grid.

AUTHORS: Bhuvan Bamba, Ling Liu, Peter Pesti, Ting Wang

The PrivacyGrid framework offers three distinctive capabilities. First, it provides a location privacy protection preference profile model, called location P3P, which permits mobile users to expressly outline their most popular location privacy needs in terms of each location concealing measures (e.g., location k-anonymity and placement l-diversity) and location service quality measures (e.g., most abstraction resolution and maximum temporal resolution). Second, it provides fast and effective location cloaking algorithms for location k-anonymity and location l-diversity in an exceedingly mobile atmosphere. We develop dynamic bottom up and top-down grid cloaking algorithms with the goal of achieving high anonymization success rate and potency in terms of each time quality and maintenance price. A hybrid approach that carefully combines the strengths of each bottom-up and top-down cloaking approaches to additional scale back the average anonymization time is additionally developed. Last but not the least, PrivacyGrid incorporates temporal cloaking into the location cloaking process to additional increase the success rate of location anonymization.

2. Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking

AUTHORS: Marco Gruteser and Dirk Grunwald

This paper presents a middleware architecture and algorithms that will be utilized by a centralized location broker service. The adaptive algorithms regulate the resolution of location info on abstraction or temporal dimensions to meet such as obscurity constraints supported the entities United Nations agency is also victimisation location services among a given space. Using a model supported automotive traffic counts and devising material, we estimate the realistically expected abstraction resolution for totally different obscurity constraints. The median resolution generated by our algorithms is 125 mts. Thus, anonymous location-based requests for urban space would have the same accuracy presently required for E-911 services; this may give enough resolution for method finding, automated bus routing services and similar location-dependent services.

3. Preventing Location-Based Identity Inference in Anonymous Spatial Queries

AUTHORS: Panos Kalnis, Gabriel Ghinita, Kyriakos Mouratidis, and Dimitris Papadias

The expanding pattern of implanting situating capacities (for instance, GPS) in cell phones encourages the boundless utilization of Location-Based Services. For such applications to succeed, security and secrecy are basic. Existing security improving procedures depend on encryption to defend correspondence channels, and on pen names ensure client characters. By the by, the question substance may uncover the physical area of the client. In this paper, we display a system for anticipating area based personality surmising of clients who issue spatial questions to Location-Based Services. We propose changes in view of the settled K-namelessness idea to register correct responses for range and closest neighbor seek, without uncovering the question source. Our techniques advance the whole procedure of anonymizing the solicitations and preparing the changed spatial questions. Broad trial thinks about recommend that the proposed strategies are pertinent to genuine situations with various portable clients.

4. A Two-level Protocol to Answer Private Location-based Queries.

AUTHORS: Roopa Vishwanathan, Yan Huang.

A critical security issue in Location Based Services (LBS) is to conceal a client's character and area while as yet giving quality area based administrations. A client's character can be effortlessly covered up through mysterious web perusing administrations. In any case, a client's area can uncover a client's character. For instance, a client at home might need to ask questions, for example, "Discover the closest healing center around me" through a GPS empowered cell phone however he may not will to unveil his own area. A typical approach to accomplish area protection is through shrouding, e.g. the customer sends a shrouded district to the server and channels the outcomes to locate the correct answer. As of late, Private Information Retrieval has been received to answer private area based inquiries. Be that as it may, we contend that guaranteeing the server does not uncover a larger number of information than what is questioned is vital in the meantime. In this paper, we propose an effective two-level arrangement in light of two cryptographic conventions: PIR

and Oblivious Transfer. Our answer is a broadly useful one and can utilize either a two-level PIR [2] or it can utilize a blend of PIR and Oblivious Transfer [11]. Our approach gives security to the client/customer, does not utilize a confided in gathering or anonymizer, is provably protection safeguarding, and when contrasted with past methodologies guarantees that the server uncovers as least information as is required, and the information that is discharged by the server is as fine-grained or exact as could be expected under the circumstances.

III. EXISTING SYSTEM

Area Based Services (LBSs) offer significant open entryways for a broad extent of business areas; they demonstrate customer's significant security perils. A prominent one is organization lack of clarity hazard i.e., the potential introduction of organization businesses. Much the same as expected Internet get to, a customer won't not want to be identified as the endorser of a couple of LBS, especially when the organization is sensitive. Another risk, which is more certified, is region security. A customer's region revealed in her organization request may uncover sensitive private information, for instance, prosperity conditions, lifestyles, and so on. In particular, it can allow a foe to locate the subject and result in physical naughtiness.

Disadvantages:

- Data can be effortlessly gotten to if third individual know the points of interest of client.
- Your account data may get hacked by unapproved individuals over the web.

IV. GET PEER REVIEWED

Information security in the cloud is so critical. Clients (people or organizations) are worried about the entrance to the data by unapproved clients. Presently assume that information is some basic and secret data from a bank, or an establishment and so forth. Absolutely the need of get to control in the distributed computing is like never before and is an essential piece of information security in cloud. In our strategy we utilize the client's area and geological position and we tend to add a security layer to the current safety efforts. Our answer is more suitable for banks, enormous organizations, foundations and illustrations like this. The main thing we need is an Anti-Spoof and exact GPS those organizations can stand to purchase. Likewise executing the area subordinate information encryption calculation (LDEA), on the cloud and the client's PC (which is associated with the GPS) is required. We can name the information. Name contains name of the organization or a man who works in the organization (for instance the organization's manager).

In this framework we make client to make enlist with the client qualifications, Mobile number, area, Account points of interest and this subtle elements additionally put away in the cloud database. At the point when client login with the username and secret key, first we will check whether the present area of client and the area at the season of enrollment are coordinating so that to give area protection. In the event that the area doesn't matches then we ask client some protection address with respect to client's last exchange points of interest in the event that he gives the right subtle elements of his record points of interest then the OTP (One Time Password) is sent to his enrolled portable number if client enter remedy OTP sent to his versatile number then client can make exchange.

Advantages:

- Account points of interest will be gotten to in view of the client area confirmation.
- The information will be secured.
- Unauthorized individuals can't get to in light of the fact that its area based get to where client gives the area amid enrollment

V. METHODOLOGY

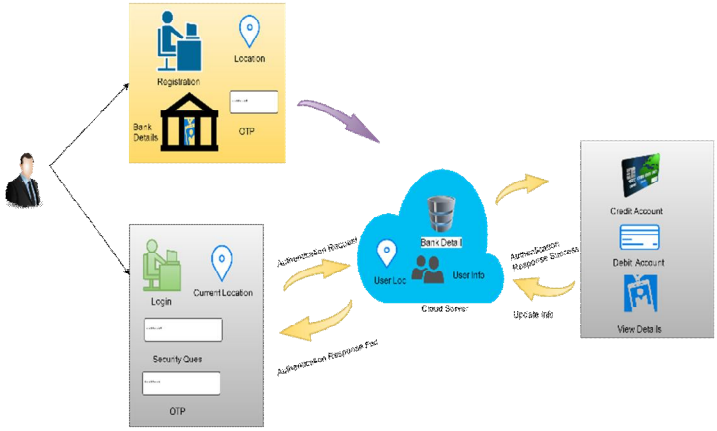

Figure 1. Architecture diagram of proposed system

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

User:

The client needs to login to his/her record with the qualifications gave amid the enlistment procedure. Client current area is gotten and interviewed with the enlisted area if its comparable then client can continue with further exchange else the exchange will be shut.

Bank Server:

It is fundamental server implied for sparing the information of client amid exchange. Client can credit, charge and enquiry about his/her record points of interest.

Dummy Server:

The dummy server is for giving security from physical assault. It additionally works same as principle server yet the exchange made here are fake i.e. the exchange doesn't influence the clients principle account.

2. Third-Party Provider Solutions

For latest couple of years, a noteworthy extent of pariahs providing for pass on prepared messages (and differing information organizations) by method for substance electronic illuminating organizations. The diagram of those systems is likewise immediate. Despite whether ordered through an online interface, clearly from a phone, or as programming structure running on a field chief's versatile PC, these organizations go about as SMS aggregators and imbue texts into the framework. Inside the event of an emergency message is transported to the organization center from the loss or footer compact.

Short Message Service

Short Message Service (SMS) could be a substance electronic correspondence advantage part of phone, web, or compact correspondence systems, mishandle regulated exchanges traditions that enable the exchanging of short texts between secured line and vagrant contraptions. SMS content electronic correspondence is that the most overall used data application inside the world, with 3.6 billion element customers, or seventy eight of each wanderer endorser. The term SMS is used as an equivalent word for an extensive variety of short substance electronic correspondence in addition in light of the way that the customer activity itself in a couple parts of the globe. Coordinate customer made text organizations - get a handle on news, wear, cash related, tongue and position basically based organizations, likewise as a couple of early cases of adaptable systematic stocks and share costs, convenient sparing cash workplaces and unwinding booking organizations. SMS has used on chic handsets started from radio media transmission in radio memoranda pagers abuse systematized phone traditions and later plot as a part of the world System for Mobile Communications (GSM) course of action of benchmarks in 1985] as a methodology for making messages of up to one hundred sixty characters, and from GSM compact handsets. Starting now and into the foreseeable future, bolster for the organization has enlarged to breaker elective versatile developments like ANSI CDMA frameworks and Digital AMPS, in addition as satellite and land line frameworks. Most SMS messages are convenient to-flexible texts notwithstanding the way that the quality support elective styles of impart electronic correspondence furthermore.

GSM Technology

GSM could be a cell framework, which proposes that cellphones interface with it by taking a gander at cells inside the incite neighborhood. There square measure five absolutely uncommon cell sizes in an exceedingly GSM compose. The extension space of every cell changes per the execution air. Indoor extension is in addition maintained by GSM. GSM uses various crypto authentic counts for security. An accommodating office of the GSM framework is that the short message advantage. The Short Message Service – indicate point (SMS-PP) was at first plot in GSM recommendation that is at this moment kept up in 3GPP as TS twenty three.040. GSM 03.41 (now 3GPP TS twenty three.041) describes the Short Message Service – Cell Broadcast (SMS-CB), that stipends messages (publicizing, open data, et cetera.) to be convey to any or each and every convenient customer in an exceedingly apparent geographic locale. Messages square measure sent to a concise message advantage center (SMSC) that gives a "store and forward" segment. It makes an attempt to send messages to the SMSC's recipients. In case the supporter's flexible unit is power-driven off or has left the extension space, the message is hold tight and offered back to the endorser once the compact is power-driven on or has given back the degree space of the framework. This work ensures that the message will be gotten.

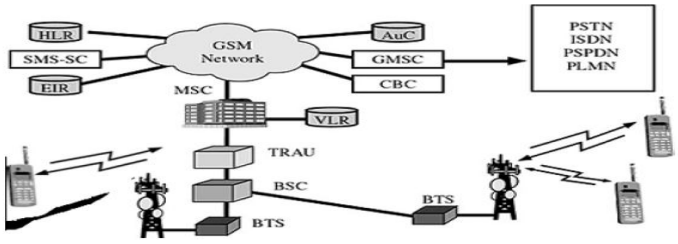

Figure 2. GSM Network along with SMSC

Both versatile ended (MT, for messages sent to a portable handset) and portable beginning (MO, for those sent from the versatile handset) operations are upheld. In Message conveyance, delay or finish loss of a message is phenomenal, ordinarily influencing under 5% of messages.

GPS Technology

The Global Positioning System (GPS), in addition suggested as Navstar, could be a world course satellite structure (GNSS) that has region and time data all things considered climatic conditions, wherever on or close to the planet wherever there's accomplice degree unhindered distinguishable pathway to four or a lot of GPS satellites. The GPS structure works severally of any media transmission or web gathering, notwithstanding' these advances will enhance the utility of the GPS arranging data. The GPS system gives fundamental arranging capacities to military, normal, and mechanical customers round the world. The US government made the structure, cares for it, and makes it straightforwardly accessible to anyone with a GPS recipient. The GPS beginning is predicated on time besides the lauded position of specific satellites. The satellites pass on dreadfully stable atomic timekeepers that square measure synchronized with each other and to ground tickers. Any buoy from honest to goodness time kept up on the base is balanced each day. In addition, the satellite ranges square measure celebrated with lovely accuracy. GPS recipients have tickers additionally; in any case, they're consistently not synchronized with certifiable time, and square measure less unfaltering. GPS satellites unendingly transmit their present time and position. A GPS beneficiary screens diverse satellites and lights up conditions to see the correct position of the recipient and its deviation from bona fide time. No less than, four satellites should be clear of the recipient for it to work out four loud sums (three position composes and clock deviation from satellite time).

VI. RESULT

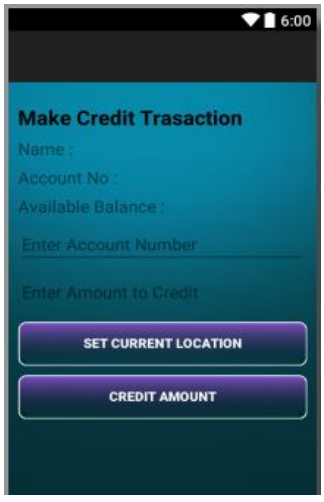

Figure 3.

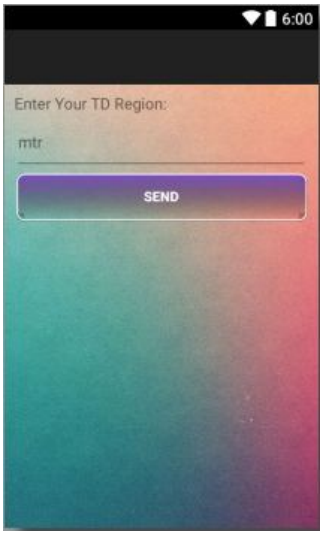

Figure 4.

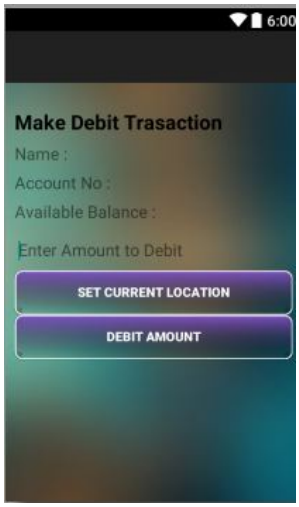

Figure 5.

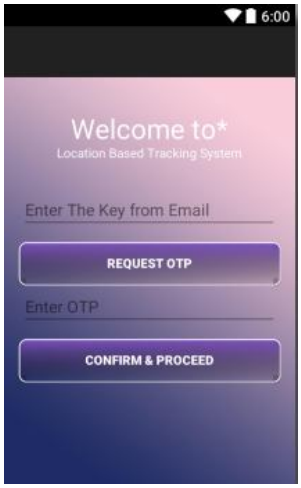

Figure 6.

Figure 7.

Figure 8.

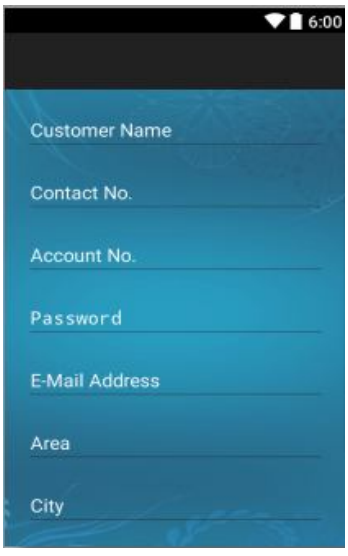

Figure 9.

Figure 10.

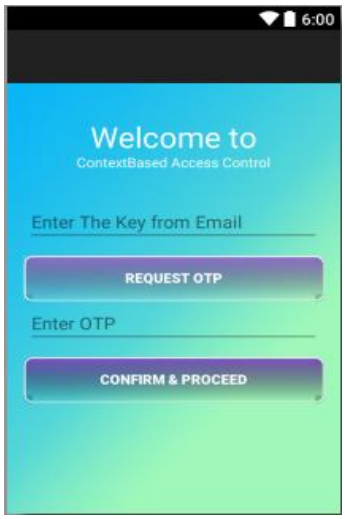

Figure 11.

VII. CONCLUSION

Conventional encryption innovation can't limit the area of versatile clients for information unscrambling. Keeping in mind the end goal to take care of the demand of portable clients later on, LDEA calculation is proposed in this paper. LDEA give another capacity by utilizing the scope/longitude facilitate as the key of information encryption. A toleration separate (TD) is additionally intended to conquer the incorrectness and conflicting of GPS beneficiary. The security quality of LDEA is customizable when important. The exploratory aftereffect of the model likewise demonstrates that the unscrambling is compelled by the scope of TD. Accordingly, LDEA is powerful and pragmatic for the information transmission in the versatile environment. The LDEA calculations can be reached out to the next application spaces, e.g., the approval of versatile programming. On the off

chance that portable programming is approved inside a pre-characterized range, for example, a city, the execution of the product may enact the area check in light of the LDEA calculation. The product can be executed just when the client is inside the approved region. Also, the circulation of media substance might be used the LDEA calculation for cutting edge get to control with the exception of the username/watchword. The proposed LDEA calculation gives another approach to information security. It is likewise meet the pattern of portable registering. Numerous conceivable applications will be produced later on to exhibit and advance the idea of LDEA calculation. The proposed technique can be utilized as a part of a few places, for example, banks, huge organizations, foundations to meet the craved execution.

REFERENCES

[1] B. Bamba and L. Liu. PrivacyGrid: Supporting Anonymous Location Queries in Mobile Environments. Technical report, Georgia Tech., 2007.

[2] R. Bayardo and R. Agrawal. Data Privacy through Optimal k-Anonymization. In ICDE, 2005.

[3] A. Beresford and F. Stajano. Location Privacy in Pervasive Computing. Pervasive Computing, IEEE, 2003.

[4] C. Aggarwal. On k-Anonymity and the Curse of Dimensionality. In VLDB, 2005.

[5] N.R. Adam and J.C. Wortmann, "Security-Control Methods for Statistical Databases: A Comparative Study," ACM Computing Surveys, vol. 21, no. 4, pp. 515-556, 1989.

[6] C.C. Aggarwal, "On K-Anonymity and the Curse of Dimensionality," Proc. 31st Int'l Conf. Very Large Data Bases (VLDB '05), pp. 901-909, 2005.

[7] R. Agrawal and R. Srikant, "Privacy-Preserving Data Mining," Proc. 19th ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '00), pp. 439-450, 2000.

[8] R. Bayardo and R. Agrawal, "Data Privacy through Optimal KAnonymization," Proc. 21st IEEE Int'l Conf. Data Eng. (ICDE '00), pp. 217-228, 2005.

[9] N. Beckmann, H.-P. Kriegel, R. Schneider, and B. Seeger, "The R_-Tree: An Efficient and Robust Access Method for Points and Rectangles," Proc. Ninth ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '90), pp. 322-331, 1990.

[10] A.R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," IEEE Pervasive Computing, vol. 2, no. 1, pp. 46-55, 2003.

[11] N. Li, T. Li, and S. Venkatasubramanian. T-Closeness: Privacy beyond k-Anonymity and l-Diversity. In ICDE, 2007.

[12] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam. l-Diversity: Privacy Beyond k-Anonymity. In ICDE, 2006.

[13] M. Mokbel, C. Chow, and W. Aref. The New Casper: Query Processing for Location Services without mpromising Privacy. In VLDB, 2006.

[14] L. Sweeney. Achieving k-Anonymity Privacy Protection Using Generalization and Suppression. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002.

[15] X. Xiao and Y. Tao. Personalized Privacy Preservation. In SIGMOD, 2006.

[16] X. Xiao and Y. Tao. m-Invariance: Towards Privacy Preserving Re-publication of Dynamic Datasets. In SIGMOD, 2007.