Scientific Journal of Impact Factor (SJIF): 4.72

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

International Journal of Advance Engineering and Research Development

Volume 4, Issue 2, February -2017

Survey on Security Oriented Location Based Transaction System

Mr. Sumeet Nathe[1], Mr. Sandeep Ghogare[2], Miss. Priyanka Shelke[3], Mrs. Deepali Gothawal

[1,2,3] *BE Scholar, Department of Computer Engineering, D Y Patil College of Engineering, Akurdi, Pune, MH, India*

[4]*Asst. Professor, Department of Computer Engineering, D Y Patil College of Engineering, Akurdi, Pune, MH, India*

Abstract - *Cloud computing is another approach in the field of data innovation and improvement of PC advancements in light of the World Wide Web. A standout amongst the most imperative difficulties here is the security of distributed computing. Then again the security of access to basic and classified data in banks, organizations and so on is amazingly fundamental. Some of the time even with the colossal costs, it is not completely ensured and it is traded off by the aggressors. By giving a novel technique, we enhance the security of information access in distributed computing for an organization or some other particular areas utilizing the area based encryption. Across the board of WLAN and the ubiquity of cell phones builds the recurrence of information transmission among portable clients. In any case, a large portion of the information encryption innovation is area free. A scrambled information can be decoded anyplace. The encryption innovation can't limit the area of information unscrambling. Security threats have been a major concern. To solve this issue effective mechanism of "cryptography" is used to ensure integrity, privacy, availability, authentication, and accuracy. Cryptology methods like PKC and SKC are used of data recovery. In this project we describe exploration private key architecture that is efficient symmetric AES Algorithm on the basis of attributes like encipherment and Decipherment and degree of security issues. It's essential for wired and wireless communication. The work explores private key algorithm based on security of system and to improve encipherment and Decipherment time with encipherment/Decipherment performance. The work opens a new direction over cloud security and internet of things.It represents that AES is successful and down to earth for information transmission in versatile environment.*

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

I. INTRODUCTION

Information security means protective data and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Maintaining privacy in our personal communication are a few things everybody needs. Encryption is a means to attain that privacy. It absolutely was invented for the exact same purpose. The security has become a serious concern for business and customers. There's a necessity for an end to end encryption so as to produce a secure medium for communication.

The banking application utilizing Location Based Encryption, as contrast with current managing an account application which are area autonomous, we are creating banking application which is area subordinate. It implies in Cryptography Cipher-content must be decoded at a predefined area i.e. area subordinate approach. On the off chance that an endeavor to decode information at another area, the unscrambling procedure fizzles and uncovers no data about the plaintext. This is critical continuously application, case in army installation application, Cinema Theater. However, our framework is sufficiently adaptable to give access to client to his/her record from any area. Our framework additionally give answer for physical assault utilizing virtualization, in which client is permitted to perform fake exchange for his/her physical security reason.

Privacy Grid is a widely distributed automated energy delivery network. The backbone of smart grid is the communication network. The reliability of the grid depends on the data received from various distributed domains of the over network. Because it is multifaceted nature of the network. The smart grid is highly prone to attacks and the generation of vast amount of data. Grid makes the system unable to use the existing cryptographic algorithms. So, there is a need for a security algorithm that provides high security. In this paper, we propose security algorithm that can

encrypt large amount of data in short time. The algorithm we propose uses two keys k1 and k2. The keys are distributed by the third party through secure channel. It provides NP-hard complexity and will not be able to disclose without knowing both keys. The security and performance of the algorithm are analyzed by AES algorithm. Simulation results demonstrate the suitability of the proposed scheme for the vast data generating systems.

We are creating managing an account application utilizing Location Based Encryption. As contrast with current managing an account application which is area autonomous, we are creating saving money application which is area subordinate. It implies in Cryptography Cipher-content must be decoded at a predetermined area i.e. area subordinate approach. In the event that an endeavor to decode information at another area, the unscrambling procedure fizzles and uncovers no data about the plaintext.

II. LITERATURE SURVEY

In this subsection we give the brief literature review of security oriented location system as follows:

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

This paper presents Privacy-Grid − a framework for supporting anonymous location-based queries in mobile info delivery systems. The Privacy-Grid framework offers two distinctive capabilities. First, it provides a location privacy protection preference profile model, referred to as location P3P, that permits mobile users to expressly outline their most well-liked location privacy necessities in terms of each location concealing measures (e.g., location k-anonymity and placement l-diversity) and placement service quality measures (e.g., most spatial resolution and most temporal resolution). Second, it provides quick and effective location cloaking algorithms for location k-anonymity and placement l-diversity during a mobile surroundings.

Location cloaking algorithms for location k-anonymity and location l-diversity in a mobile surroundings. They 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 complexness and maintenance value. A hybrid approach that fastidiously combines the strengths of each bottom-up and top-down cloaking approaches to more scale back the common anonymization time is additionally developed. Last however not the smallest amount, PrivacyGrid incorporates temporal cloaking into the situation cloaking method to more increase the success rate of location anonymization.

2] Preventing Location-Based Identity Inference in Anonymous Spatial Queries.[2]

The increasing trend of an embedding positioning capabilities (for example, GPS) in mobile devices facilitates the widespread use of Location-Based Services. For such applications to succeed, privacy and confidentiality square measure essential. Existing privacy enhancing techniques think about coding to safeguard communication channels, and on pseudonyms to guard user identities. Nonetheless, the question contents might disclose the physical location of the user.

In this paper, they aim at determination these issues through a comprehensive set of techniques. Specifically, they propose 2 cloaking algorithms: Nearest Neighbor Cloak (NNC) that considerably outperforms the prevailing techniques in terms of potency however has similar namelessness issues for a few distributions, and mathematician Cloak (HC), that never reveals the question supply, freelance of the user location distribution. Moreover, they address the difficulty of anonymized question process at the LBS. Specifically, they adopt an existing formula for computing the k nearest neighbors (kNN) of rectangular regions, as opposition points, and develop a unique formula for computing the kNN of circular regions, that reduces the amount of redundant results, hence, the communication price between the anonymizer and therefore the LBS.

3] A Two-level Protocol to Answer Private Location-based Queries.[3]

An important privacy issue in Location primarily {based} Services (LBS) is to cover a user's identity and placement whereas still providing quality location based services. A user's identity is simply hidden through anonymous internet browsing services. However, a user's location will reveal a user's identity. As an example, a user reception might want to raise queries like "Find the closest hospital around me" through a GPS enabled movable however he might not be willing to disclose his own location. A typical thanks to reach location privacy is thru cloaking, e.g. the consumer sends a cloaked region to the server and filters the results to seek out the precise answer.

In this paper, they propose an efficient 2-level arrangement in sight of two crypto logical conventions: PIR and Oblivious Transfer. Their answer could be a universally helpful one will utilize either a two-level PIR or it can utilize a mix of PIR and Oblivious Transfer. Their approach provides protection to the client/customer, doesn't utilize a place stock in gathering or anonymizer, is incontrovertibly security saving, and once contrasted with past methodologies guarantees that the server uncovers as least data as is needed, and therefore the data that's discharged by the server is as fine-grained or precise as would be prudent.

4] Feeling-based Location Privacy Protection for Location-based Services.[4]

Anonymous location info is also correlative with restricted spaces like home and workplace for subject re-identification. This makes it a good challenge to produce location privacy protection for users of location-based services. Existing work adopts ancient K-anonymity model and ensures that every location disclosed in commission requests could be an abstraction region that has been visited by a minimum of K users. This strategy needs a user to specify an applicable price of K so as to attain a desired level of privacy protection. This can be problematic as a result of privacy is regarding feeling, and it's awkward for one to scale her feeling employing a variety. During this paper, we propose a feeling-based privacy model.

When a user requests an LBS, she also informs the LBDs a travel bound B, a rectangular abstraction region that bounds her travel throughout the service session. In response, the LDS arbitrarily generates a service session ID and contacts the service supplier. Once establishing a service session, the service user sporadically reports her current location to the LDS. For every location update, the LDS computes a cloaking box that contains the service user's current location, and exports this box at the side of the session ID to the corresponding LBS supplier. The data received from the supplier is then forwarded back to the service user. As mentioned early, to stop restricted area identification, the flight created by the sequence of cloaking boxes should be a PPT that satisfies the user's privacy demand. The key issue is the way to realize a typical set of users for cloaking in order that the flight, that is undetermined, will have a resolution that's as fine as potential. Within the following subsections, they 1st describe the most arrangement used for classification the placement samples keep within the footprint information, so gift a heuristic rule for flight cloaking.

5] Efficient Cloud Computing with Secure Data Storage using AES.[5]

Most of the safety schemes in cloud surroundings had not self-addressed the privacy conserving between third party auditor and also the information within the cloud. Cryptography techniques used antecedently are RSA based mostly, that have totally different loopholes which might be overcome by mistreatment the foremost outstanding cryptography techniques that uses advanced cryptography standards (AES) cryptography algorithm.

AES is most often used secret writing algorithm nowadays this algorithm is based on many substitutions, permutations and linear transformations, every dead on information blocks of 16 byte. As of nowadays, no practicable attack against AES exists. Therefore, AES remains the well-liked secret writing normal for governments, banks and high security systems round the world. For economical auditing the formation of batch of task and are executed in batch wise fashion conjointly increase potency of TPA, the batch auditing protocol. In cloud the within the cloud isn't solely accessed by the user however conjointly update information often.

6] Survey on Secure Cloud Data Sharing Using Trusted Third Party.[6]

Data sharing and maintaining its security is apply challenge. Information owner within the information sharing system transfer their files with Cryptography. If any user mistakenly leaks the key data, then it'll be tough for the data owner to keep up security of the shared information. Unauthorized user might attempt few tries and find access if partial password is understood. However, it's terribly vital to handle key shared by the information owner. During this paper we offer a concrete and economical mental representation of theme to prove its security exploitation 2 layers of secret writing and bar from unauthorized user by distinguishing them

TTP is one of the module to authenticate user people who have access to the information on cloud. SHA algorithm is employed by TTP to get the key, this key share to user likewise as owner. TTP module get encrypted file using AES algorithm from information owner and computes hash worth using MD-5. Our system can lie between finish users and cloud suppliers.

7] Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model.[7]

Cloud computing having variety of advantages however the foremost organizations are disquieted for acceptive it as a result of security problems and challenges having with cloud. Security needs needed at the enterprise level forces to style models that solves the structure and distributed aspects of knowledge usage. Such models ought to gift the protection policies supposed to safeguard data against unauthorized access and modification keep in an exceedingly cloud. The projected work describes the approach for modeling the protection needs from the attitude of job functions and tasks performed in a company by applying the cryptography ideas to store knowledge on cloud with the littlest quantity of your time and price for encoding and coding processes.

There ar types of security algorithms which might be enforced to the cloud. There are two forms of algorithms cruciform key and uneven key. DES, Triple-DES, AES, and Blowfish etc are some symmetric algorithms are often accustomed implement cloud security. RSA and Diffie-Hellman Key Exchange are the uneven algorithms these are often used to generate encryption and decipherment key for symmetric algorithms. In cloud computing, cruciform key and uneven key algorithms is employed to inscribe and decode the information. In presented work, RSA algorithmic program is employed to get encryption and decipherment keys for AES symmetric algorithm.

8] Efficient Implementation of AES.[8]

With the quick progression of digital knowledge exchange in electronic approach, info security is changing into rather more vital in knowledge storage and transmission. Cryptography has come back up as an answer that plays an important role in info security system against varied attacks. This security mechanism uses some algorithms to scramble knowledge into unclear text which might be solely being decoded or decrypted by party those possesses the associated key

Symmetric cryptography, like within the data encryption standard (DES), 3DES, and Advanced encryption normal (AES), uses an even key for the sender and receiver, each to encipher the message text and decrypt the cipher text. Asymmetric cryptography, like within the Rivest-Shamir-Adleman (RSA) uses totally different keys for encryption and decryption, eliminating the key exchange problem. Bilateral cryptography is a lot of appropriate for the encoding of an oversized quantity of information. The AES algorithm outlined by the National Institute of Standards and Technology (NIST)

9] Enhanced Amalgam Encryption Approach for Grid Security: A Review.[9]

Grid computing is concerning many processors distributed globally and sharing the machine resources to unravel varied issues. Grid computing has become a more and more vital analysis topic inside computing as in tutorial instructional purpose and industrial analysis to government sector. Grid computing cares a way to share and coordinated use numerous resources in distributed environments. The dynamic and multi-institutional nature of those environments introduces difficult security problems that embrace integration with existing systems and technologies, ability with completely different “hosting environments” and “trust relationships” among interacting hosting environments. The foremost problems related to grid computing are coordinative resource sharing and security measures.

A New technical approaches to handle those security issues. Security solution consist of ARC4 (Rivest Cipher 4) rule combined with Advance encryption standard (AES) that provides answer for security with whitener (Whitening is employed to enhance the safety of the cipher). In related study hybrid answer has been projected however has some overhead whereas process security for big distributed networks. In current technology with development of sensible grid design, we want less overhead to use best resources in grid computing. They projected a enhance amalgam encoding answer victimization AES and RC4 which might overcome overhead and security limitations. Grid computing is bothered the way to share and coordinated use various resources in distributed environments. The dynamic and multi-institutional nature of those environments introduces difficult security problems, that embody integration with existing systems and technologies, ability with completely different “hosting environments” and “trust relationships” among interacting hosting environments. The main problems related to grid computing square measure coordinating resource sharing and security measures.

10] Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking.[10]

Advances in sensing and pursuit technology enable location-based applications however they conjointly produce important privacy risks. Obscurity will offer a high degree of privacy, save service users from handling service providers’ privacy policies, and scale back the service providers’ needs for safeguarding non-public info. However, guaranteeing anonymous usage of location-based services needs that the precise location info transmitted by a user cannot be simply

accustomed re-identify the topic. This paper presents a middleware design and algorithms which will be utilized by a centralized location broker service.

The key plan mistreatment Adaptive-Interval Cloaking Algorithms is that a given degree of obscurity are often maintained in any location regardless of population density by decreasing the accuracy of the disclosed spatial information. To the current finish, the rule chooses a sufficiently massive space, in order that enough alternative subjects inhabit the realm to satisfy the obscurity constraint.

SL. No	Name	Technological Demerits
1.	Preventing Location-Based Identity Inference in Anonymous Spatial Queries.	If a client obtains the items of interest (for example, the closest restaurant), it's unlikely to raise the same question from constant location once more within the future. They additionally assume that the offender doesn't have a priori information of the user question frequencies (that is, a question might originate in any user with equal probability). Moreover, the worth of K isn't subject to attacks, since it's transferred from the shopper to the anonymizer through a secure channel.
2.	Feeling-based Location Privacy Protection for Location-based Services.	Other styles of attack are likely actually. One is observation implication attack. If an adversary has direct observation over the region wherever a user locates, the user doesn't have location privacy at that point. However, the discovered location is also connected to the user's future movement. Orthogonal to the observation implication is that the exclusiveness attack. If the adversary is aware of that a user has never visited a definite region, then any flight that traverses through this region cannot belong to the user.
3.	Survey on Secure Cloud Data Sharing Using Trusted Third Party	A mechanism to secure the key cloud can be an area of research and hardware security support on password matching scheme. To reduce the overhead of network traffic can be another area of research. R
4.	Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model	To achieve efficient user revocation, the private cloud is assumed to be honest-but-curious so as to use the planned theme during this design. That is, the cloud can reliably execute the theme and cannot collaborate with revoked users.
5.	Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking	They assume that clients communicate position information to a location server with very high precision; in different words, the network client really provides a correct location to the placement server. Position determination will be enforced either on the client itself. The total system contains a location info supply, a wireless network, location servers, and LBS servers. In a very typical system, location info is set by a location info supply like a GPS receiver in a very vehicle. It's then periodically transmitted through a cellular or wireless network to the placement server. Once a vehicle sends a message or request to an LBS, the service accesses the vehicle's current location info from the placement server that acts as a proxy or middle ware agent.

III. EXISTING SYSTEM

Existing privacy-preserving techniques for LBS have several limitations, such as requiring a fully-trusted third party, offering limited privacy guarantees and incurring high communication overhead.

Location Based Services (LBSs) offer significant open doors for an expansive scope of business sectors; they show clients significant security dangers. A conspicuous one is administration obscurity risk i.e., the potential presentation of administration employments. Much the same as normal Internet get to, a client might not have any desire to be identified as the endorser of a few LBS, particularly when the administration is delicate. Another danger, which is more genuine, is area security. A client's area uncovered in her administration demand may uncover touchy private data, for example,

wellbeing conditions, ways of life, et cetera. Specifically, it can possibly permit an enemy to find the subject and result in physical mischief.

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. PROPOSED SYSTEM

Data security in the cloud is so 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 an institute and etc. 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 tend to add a security layer to the existing security measures. Our solution is more appropriate for banks, big institutes, institutions and examples like this. The only thing we need is an Anti-Spoof and accurate GPS those companies can afford to buy. Also implementing the Advanced Encryption Standard algorithm (AES), on the cloud and the user's computer (which is connected to the GPS) is required. We can label the data. Label contains name of the company or a person who works in the company (for example the company's boss).

In this system we make user to make register with the user credentials, Mobile number, location, Account details and this details further stored in the cloud database. When user login with the username and password, first we will check whether the current location of user and the location at the time of registration are matching so that to provide location privacy. If the location doesn't matches then we ask user some privacy question regarding user's last transaction details if he provides the correct details of his account details then the OTP (One Time Password) is sent to his registered mobile number if user enter correct OTP sent to his mobile number then user can make transaction.

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
- The grid makes responsive easy
- It is smart System for rapid deployment

V. METHODOLOGY

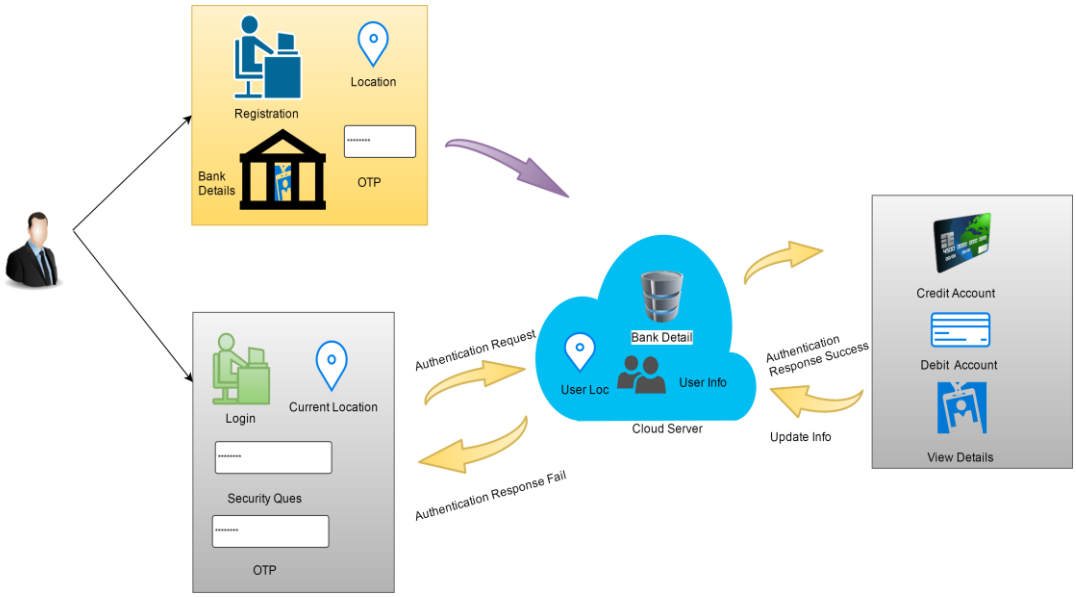

Fig 1: Architecture diagram of proposed system

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

5.1.1. User:

The client needs to login to his/her record with the accreditations gave amid the enrollment procedure. Client current area is gotten and interviewed with the enlisted area if its comparative then client can continue with further exchange else security question in regards to client last transaction will be asked, if client gives the right reply about last transaction then client can make transaction else transaction will be shut.

5.1.2. Bank Server:

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

5.1.3. Dummy Server:

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

.

5.2. Third-Party Provider Solutions

For most recent couple of years, a major scope of outsiders giving to convey ready messages (and diverse data administrations) by means of content electronic informing administrations. The outline of those frameworks is similarly direct. Regardless of whether enacted through an online interface, straightforwardly from a telephone, or as programming framework running on a field director's portable PC, these administrations go about as SMS aggregators and infuse instant messages into the system. Inside the occasion of a crisis message is transported to the administration focus from the casualty or footer portable.

5.2.1. Short Message Service

Short Message Service (SMS) could be a content electronic correspondence benefit component of telephone, web, or portable correspondence frameworks, abuse institutionalized interchanges conventions that empower the trading of short instant messages between secured line and vagrant gadgets. SMS content electronic correspondence is that the most by and large utilized information application inside the world, with 3.6 billion dynamic clients, or seventy eight of every nomad endorser. The term SMS is utilized as a comparable word for a wide range of short content electronic correspondence what's more in light of the fact that the client action itself in a few parts of the globe. Direct client created instant message administrations - grasp news, wear, money related, dialect and position essentially based administrations, what's more as a few early examples of versatile business like stocks and share costs, portable saving money offices and relaxation booking administrations. SMS has utilized on chic handsets began from radio telecommunication in radio memoranda pagers misuse institutionalized telephone conventions and later plot as a part of the world System for Mobile Communications (GSM) arrangement of benchmarks in 1985] as a strategy for making messages of up to one hundred sixty characters, and from GSM portable handsets. From that point forward, support for the administration has widened to fuse elective portable innovations like ANSI CDMA systems and Digital AMPS, what's more as satellite and land line systems. Most SMS messages are portable to-versatile instant messages in spite of the fact that the quality backings elective styles of communicate electronic correspondence what's more.

5.2.2. GSM Technology

GSM could be a cell system, which suggests that cellphones interface with it by looking at cells inside the prompt neighborhood. There square measure five totally extraordinary cell sizes in an exceedingly GSM organize. The scope space of each cell changes per the execution air. Indoor scope is moreover upheld by GSM. GSM utilizes numerous crypto legitimate calculations for security. A helpful office of the GSM system is that the short message benefit. The Short Message Service – point to point (SMS-PP) was initially plot in GSM proposal that is right now kept up in 3GPP as TS twenty three.040. GSM 03.41 (now 3GPP TS twenty three.041) characterizes the Short Message Service – Cell Broadcast (SMS-CB), that grants messages (publicizing, open information, and so forth.) to be communicate to any or every single portable client in an exceedingly ostensible geographic district. Messages square measure sent to a brief message benefit focus (SMSC) that gives a "store and forward" component. It makes an endeavor to send messages to the SMSC's beneficiaries. On the off chance that the supporter's versatile unit is power-driven off or has left the scope space,

the message is hang on and offered back to the endorser once the portable is power-driven on or has returned the scope space of the system. This work guarantees that the message will be gotten.

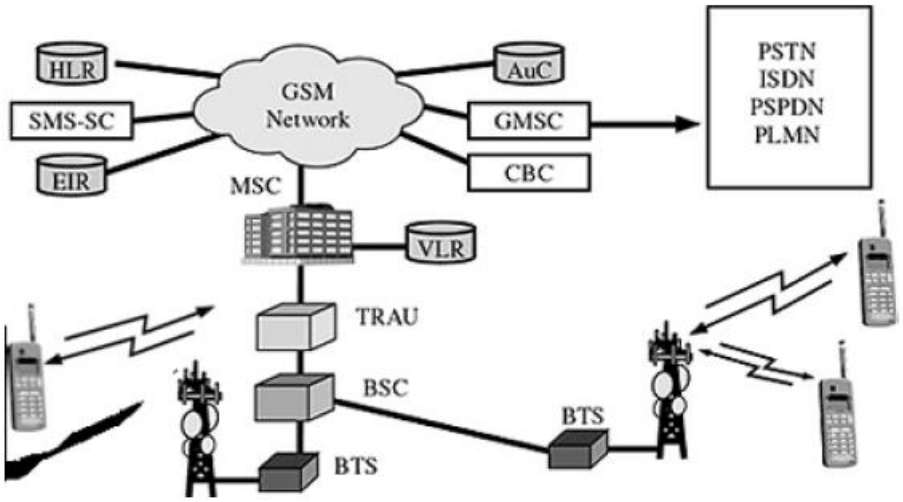

Fig 2: GSM Network along with SMSC

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.

5.2.3. GPS Technology

The Global Positioning System (GPS), moreover alluded to as Navstar, could be a world route satellite framework (GNSS) that has area and time information by and large climatic conditions, wherever on or near the planet wherever there's partner degree unhindered viewable pathway to four or a great deal of GPS satellites. The GPS framework works severally of any media transmission or web gathering, however' these advances will improve the utility of the GPS situating information. The GPS framework gives basic situating abilities to military, common, and mechanical clients round the world. The US government made the framework, looks after it, and makes it openly available to anybody with a GPS beneficiary. The GPS origination is predicated on time furthermore the commended position of particular satellites. The satellites convey awfully stable nuclear timekeepers that square measure synchronized with each other and to ground tickers. Any float from genuine time kept up on the base is adjusted every day. Moreover, the satellite areas square measure celebrated with pleasant precision. GPS beneficiaries have tickers also; be that as it may, they're regularly not synchronized with genuine time, and square measure less steady. GPS satellites endlessly transmit their present time and position. A GPS recipient screens different satellites and illuminates conditions to see the exact position of the beneficiary and its deviation from genuine time. At least, four satellites ought to be obvious of the beneficiary for it to work out four obscure amounts (three positions organizes and clock deviation from satellite time).

VI. CONCLUSION

Conventional encryption innovation can't confine the area of portable clients for information unscrambling. So as to take care of the demand of versatile clients later on, Privacy Grid System calculation is proposed in this paper, Privacy Grid System give another capacity by utilizing the scope/longitude organize as the key of information encryption. A toleration remove (TD) is additionally intended to conquer the incorrectness and conflicting of GPS recipient. The security quality of , Privacy Grid System is customizable when essential. The exploratory consequence of the model likewise demonstrates that the decoding is obliged by the scope of TD. Accordingly, , Privacy Grid System is successful and reasonable for the information transmission in the versatile environment. The , Privacy Grid System calculations can be stretched out to the next application spaces, e.g., the approval of portable programming. In the event that versatile programming is approved inside a pre-characterized zone, for example, a city, the execution of the product may actuate the area check in view of the , Privacy Grid System calculation. The product can be executed just when the client is inside the approved territory. Also, the dissemination of interactive media substance might be used the Privacy Grid System calculation for cutting edge get to control aside from the username/secret key. The proposed Privacy Grid System

calculation gives another approach to information security. It is additionally meet the pattern of versatile processing. Numerous conceivable applications will be created later on to show and advance the idea of , Privacy Grid System calculation. The proposed strategy 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] Panos Kalnis, Gabriel Ghinita, Kyriakos Mouratidis, Dimitris Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial Queries", VOL. 19, NO. 12, DECEMBER 2007

[3] Roopa Vishwanathan, Yan Huang, "A Two-level Protocol to Answer Private Location-based Queries", ISI 2009, June 8-11, 2009

[4] Toby Xu, Ying Cai, "Feeling-based Location Privacy Protection for Location-based Services", *CCS'09,* November 9–13, 2009

[5] Mr. Santosh P. Jadhav, Prof. B. R. Nandwalkar, "Efficient Cloud Computing with Secure Data Storage using AES", Vol. 4, Issue 6, June 2015

[6] Triveni A. Bhalerao, Prof. N. P. Kulkarni , "Survey on Secure Cloud Data Sharing Using Trusted Third Party", Vol. 4, Issue 10, October 2016

[7]Bokefode Jayant, Ubale Swapnaja, Pingale Subhash, "Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model", Volume 118– No.12, May 2015

[8] Ritu Pahal,Vikas kumar "Efficient Implementation of AES", Volume 3, Issue 7, July 2013

[9] Kamal Jyoti, " Enhanced Amalgam Encryption Approach for Grid Security: A Review", Volume 3, Issue 4, April 2013

[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.

