ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

CONTINUOUS SERVICE PROVISION TO REDUCE COMMUNICATION OVERHEAD IN NETS

G. Naga Archana*, Rajesh Banala
M.Tech. Student, Computer Science Engineering, SVS Group of Institutions, JNTU, India
Assistant Professor, Computer Science Engineering, SVS Group of Institutions, JNTU, India

DOI: 10.5281/zenodo.167233

ABSTRACT

Regrettably, existing privacy-protecting approaches for LBS have a lot of restrictions, for example needing a completely-reliable 3rd party, offering limited privacy guarantees and incurring high communication overhead. Location-based services2 (LBS) require customers to continuously report their whereabouts to some potentially untrusted server to acquire services according to their whereabouts, which could expose these to privacy risks. Within this paper, we advise a person-defined privacy grid system known as dynamic grid system (DGS) the very first holistic system that satisfies four essential needs for privacy-protecting snapshot and continuous LBS. (1) The machine only needs a semi-reliable 3rd party, accountable for transporting out simple matching procedures properly. This semi-reliable 3rd party doesn't have any details about a user's location. (2) Secure snapshot and continuous location privacy is guaranteed under our defined foe models. (3) Experimental results reveal that our DGS is much more efficient compared to condition-of-the-art privacy-protecting way of continuous LBS. The communication cost for that user doesn't rely on the user's preferred privacy level, it just is dependent on the amount of relevant sights near the consumer. (4) Although we simply concentrate on range and k-nearest-neighbor queries within this work, our bodies can be simply extended to aid other spatial queries without altering the calculations operated by the semi-reliable 3rd party and also the database server, provided the needed search section of a spatial query could be abstracted into spatial regions.

KEYWORDS: Dynamic grid systems, location privacy, location-based services, spatial-temporal query processing, cryptography.

INTRODUCTION

This is actually look for nearby sights (POIs), location aware advertising by companies, traffic information tailored towards the highway and direction a person travels and so on. Currently of mobility and ever-present Internet connectivity, an growing number of individuals use location-based services (LBS) to request information highly relevant to their current locations from a number of providers [1]. Using LBS, however, can reveal a little more about someone to potentially untrustworthy providers than lots of people could be prepared to disclose. By monitoring the demands of the person you'll be able to develop a movement profile which could reveal details about a user's work, medical records, political sights, etc. Nonetheless, LBS can be quite valuable and therefore customers should have the ability to utilize them without getting to stop their whereabouts privacy. Numerous approaches have lately been suggested for protecting the consumer location privacy in LBS [2][3]. Generally, these approaches could be classified into two primary groups. (1) Fully-reliable 3rd party (TTP). Typically, the most popular privacy-protecting techniques need a TTP to become placed between your user and also the company to cover the user's location information in the company. The primary task from the 3rd party is monitoring the precise location of customers and blurring a querying user's location right into a cloaked area which includes k - 1 other customers to attain k-anonymity. This TTP model has three drawbacks. (a) All customers need to continuously report their exact place towards the 3rd party, while they don't sign up for any LBS. (b) Because the 3rd party knows the precise location of each and every user, it is really an attractive target for attackers. (c) The k-anonymity-based techniques only achieve low regional location privacy because cloaking an area to incorporate k customers used usually leads to small cloaking areas. (2) Personal data retrieval (PIR) or oblivious transfer (OT). Although PIR or OT techniques don't require a 3rd party, they get in a much greater communication overhead

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

between your user and also the company, needing the transmission of great importance and more details compared to user really needs. Within this paper, we advise a person-defined privacy grid system known as dynamic grid system (DGS) to supply privacy-protecting snapshot and continuous LBS [3] [4]. The primary idea is to put a semi trusted 3rd party, called query server (QS), between your user and also the company (SP). QS only must be semi-reliable because it won't collect/store or perhaps get access to any user location information. Semi-reliable within this context implies that while QS will attempt to look for the location of the user, still it properly performs the straightforward matching procedures needed within the protocol, i.e., it doesn't modify or drop messages or create new messages. An untrusted QS would randomly modify and drop messages in addition to inject fake messages, and that's why our bodies are dependent on the semi-reliable QS [5].

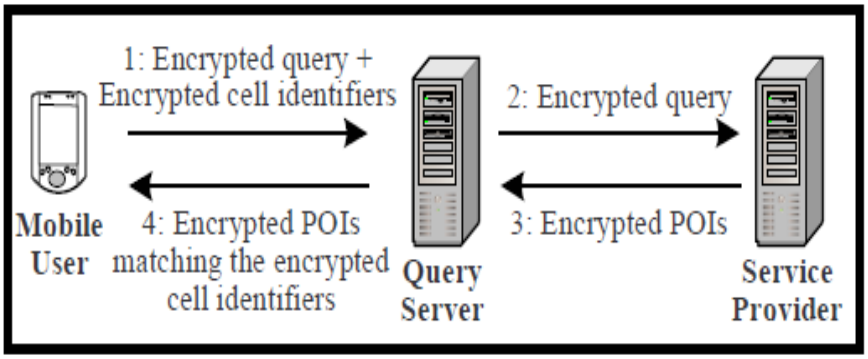

Figure 1: Framework of DGS

THE PRIMARY CONCEPT OF OUR DGS

In DGS, a querying user first determines a question area, in which the user feels safe to show the truth that she's anywhere between this question area. The query area is split into equal-sized grid cells in line with the dynamic grid structure per the consumer. Then, the consumer encrypts a question which includes the data from the query area and also the dynamic grid structure, and encrypts the identity of every grid cell intersecting the needed search part of the spatial query to make a group of encoded identifiers. QS stores the encoded identifiers and forwards the encoded query to SP per the consumer [6]. SP decrypts the query and chooses the POIs inside the query area from the database. For every selected POI, SP encrypts its information, while using dynamic grid structure per the consumer to locate a grid cell since the POI, and encrypts the cell identity to create the encoded identifier for your POI. The encoded POIs using their corresponding encoded identifiers are came back to QS. QS stores the group of encoded POIs and just returns towards the user a subset of encoded POIs whose corresponding identifiers match any of the encoded identifiers initially sent through the user.

SYSTEM IMPLEMENTATION

This is actually look for nearby sights (POIs), location aware advertising by companies, traffic information tailored towards the highway and direction a person travels and so on. Currently of mobility and ever-present Internet connectivity, an growing number of individuals use location-based services (LBS) to request information highly relevant to their current locations from a number of providers. Using LBS, however, can reveal a little more about someone to potentially untrustworthy providers than lots of people could be prepared to disclose. By monitoring the demands of the person you'll be able to develop a movement profile which could reveal details about a user's work, medical records, political sights, etc. Nonetheless, LBS can be quite valuable and therefore customers should have the ability to utilize them without getting to stop their whereabouts privacy. Numerous approaches have lately been suggested for protecting the consumer location privacy in LBS. Generally, these approaches could be classified into two primary groups. (1) Fully-reliable 3rd party (TTP). Typically, the most popular privacy-protecting techniques need a TTP to become placed between your user and also the company to cover the user's location information in the company. The primary task from the 3rd party is monitoring the precise location of customers and blurring a querying user's location right into a cloaked area which includes k - 1 other customers to attain k-anonymity. This TTP model has three drawbacks. (a) All customers need to continuously report their exact place towards the 3rd party, while they don't sign up for any LBS. (b) Because the 3rd party knows the precise location of each and every user, it is really an attractive target for attackers. (c) The k-anonymity-based techniques only achieve low regional location privacy because cloaking an area to incorporate k customers used usually leads to small cloaking areas. (2) Personal data retrieval (PIR) or oblivious transfer (OT). Although PIR or OT techniques don't require a 3rd party, they get in a much greater communication overhead between your user and also the company, needing the transmission of great

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

importance and more details compared to user really needs. Within this paper, we advise a person-defined privacy grid system known as dynamic grid system (DGS) to supply privacy-protecting snapshot and continuous LBS. The primary idea is to put a semi trusted 3rd party, called query server (QS), between your user and also the company (SP). QS only must be semi-reliable because it won't collect/store or perhaps get access to any user location information [7]. Semi-reliable within this context implies that while QS will attempt to look for the location of the user, still it properly performs the straightforward matching procedures needed within the protocol, i.e., it doesn't modify or drop messages or create new messages. An untrusted QS would randomly modify and drop messages in addition to inject fake messages, and that's why our bodies are dependent on the semi-reliable QS. The primary concept of our DGS. In DGS, a querying user first determines a question area, in which the user feels safe to show the truth that she's anywhere between this question area. The query area is split into equal-sized grid cells in line with the dynamic grid structure per the consumer. Then, the consumer encrypts a question which includes the

Figure 2: System Implementation execution pages.

data from the query area and also the dynamic grid structure, and encrypts the identity of every grid cell intersecting the needed search part of the spatial query to make a group of encoded identifiers. QS stores the encoded identifiers and forwards the encoded query to SP per the consumer [5]. SP decrypts the query and chooses the POIs inside the query area from the database. For every selected POI, SP encrypts its information, while using dynamic grid structure per the consumer to locate a grid cell since the POI, and encrypts the cell identity to create the encoded identifier for your POI. The encoded POIs using their corresponding encoded identifiers are came back to QS. QS stores the group of encoded POIs and just returns towards the user a subset of encoded POIs whose corresponding identifiers match any of the encoded identifiers initially sent through the user. The execution of system implementation steps are shown in fig.2.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

EXPERIMENT TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, subassemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. five are various types of test. Each test type addresses a specific testing requirement.

a) *Unit testing*

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results. Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases. The test have mainly three objectives they are, all field entries must work properly, pages must be activated from the identified link, the entry screen, messages and responses must not be delayed. The tested features are verified the entries are of the correct format, no duplicate entries should be allowed, all links should take the user to the correct page.

b) ***Integration testing***

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components. Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects. The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error. The test Result is found all the test cases mentioned above passed successfully. No defects encountered.

c) *System Test*

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

d) *White Box Testing*

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

e) *Black Box Testing*

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box you cannot "see" into it. The test provides inputs and responds to outputs without considering how the software works.

CONCLUSION

DGS doesn't need any fully-reliable 3rd party (TTP) rather, we must have just the much less strong assumption of no collusion between QS and SP. Our DGS includes the query server (QS) and also the company (SP), and cryptographic operates to divide the entire query processing task into a double edged sword which are carried out individually by QS and SP. Within this paper, we suggested an engaged grid system (DGS) for supplying privacy-protecting continuous LBS. This separation also moves the information transfer load from the user towards the affordable and-bandwidth outcomes of QS and SP. DGS provides better privacy guarantees compared to TTP plan, and also the experimental results reveal that DGS is definitely an order of magnitude more effective compared to TTP plan, when it comes to communication cost. When it comes to computation cost, DGS also always outperforms the TTP plan for NN queries its comparable or a little costlier compared to TTP plan for range queries. We designed efficient methods for the DGS to aid both continuous k-nearest-neighbor (NN) and range queries. To judge the performance of DGS, we compare it towards the condition-of-the-art technique needing a TTP.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

REFERENCES

[1] M. Kohlweiss, S. Faust, L. Fritsch, B. Gedrojc, and B. Preneel, "Efficient oblivious augmented maps: Location-based services with a payment broker," in *PET*, 2007.
[2] C.-Y. Chow and M. F. Mokbel, "Enabling private continuous queries for revealed user locations," in *SSTD, 2007*.
[3] T. Xu and Y. Cai, "Location anonymity in continuous location-based services," in *ACM GIS, 2007*
[4] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," in *ACM MobiSys*, 2003.
[5] Gkoulalas-Divanis, P. Kalnis, and V. S. Verykios, "Providing kanonymity in location based services," *SIGKDD Explor. Newsl., vol. 12, 2010, 3–10*.
[6] S. Yau and H. An, "Anonymous service usage and payment in servicebased systems," in *IEEE HPCC*, 2011, 714–720.
[7] M. Balakrishnan, I. Mohomed, and V. Ramasubramanian, "Where's that phone?: Geolocating ip addresses on 3G networks," in *ACM SIGCOMM IMC*, 2009.