PRIVACY IN QUERY PROCESSING WITH ANONYMISER IN ROAD NETWORKS

B.Jyothi*[1] ,Prof V. Anandam*[2] ,V.Sridhar Reddy*[3]

*[1]Assistant Professor in GITAM University,Hyderabad,AndhraPradesh, INDIA.
*[2]Professor of CSE & IT in CMR college Of Engineering, Hyderabad,AndhraPradesh, INDIA.
*[3]Assistant Professor in Vignana Bharathi Institute of Technology, Hyderabad,AndhraPradesh, INDIA.

ABSTRACT

The rapid growth of location aware devices along with wireless communications and mobile databases results in realizing location-based applications that gives particular information to the users depending upon their current locations. Location-based store finder, location-based traffic reports, and location-based advertisements are the examples of location –based service applications. The main problem with location based services is revealing user locations which threaten the privacy and security of users and such services may also share private location information with other services. If a user wants to hide their location information then they has to turn off location aware device and also has to unsubscribe from the location based services. In regard with this issue, we in this paper introduce a frame work for query processing with an Anonymizer in road networks. We design the frame work in such a way to provide anonymous LBS access to the users and allow efficient query processing at the location based services side. The techniques discussed in this paper make use of the existing network database infrastructure without requiring specialized schemes or functionalities. The effectiveness of the frame work introduced in this paper can be demonstrated by comparing the experimental results with other alternative designs.

1. INTRODUCTION

The LBS makes the users to get the spatial data available through one or more location servers that index and answer user queries on them. The LS has to be able to answer to all the questions what ever the user asks, so it could be able to know the know the position of the querying user. There are so many algorithms that are able to process the spatial query processing but still LBS could make some difference, specifically user's identity can be revealed even though they try to access information with their fake ids. Hence user privacy may be threatened due to the sensitive nature of accessed data. So we introduce a frame work which forwards Anonymizer.

An **anonymizer** or an **anonymous proxy** is a tool that attempts to make activity on the Internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information. There are many purposes for using anonymizers. It helps minimize risk. They can be used to expose human rights abuses without retribution, to speak about a taboo without loss of reputation, to receive information within a repressive regime, to prevent identity theft, or to protect search histories from public disclosure. However, anonymizers can also be used by individuals wishing to avoid the consequences of engaging in criminal, disruptive, or socially unacceptable behaviour online. For example much of the child pornography distributed through the internet is accessed through anonymizers. Also, they are used to bypass web technologies that limit online content access to a certain number of minutes or quantity of data.

Anonymizers are not entirely secure. If an anonymizer keeps logs of incoming and outgoing connections and the anonymizer is physically located in a country where it is subjected to warrant searches then there is a potential risk that government officials can reverse engineer and identify all users who used the anonymizer and how they used it. Most anonymizers state they do not keep logs but there is currently no way to confirm that. However, if the user used another anonymizer to connect to the exposed anonymizer, that user is still anonymous. This is sometimes called daisy-chaining. Further, an untrustworthy web based anonymizer is capable of man in the middle attacks. The anonymizer can read, inject, and modify content into the message that the user is sending as well as receiving. The anonymizer can intercept and record private unencrypted information such as username and password credentials, credit card numbers, e-mails, etc. that have been transported using the anonymizer. To avoid this, content should be encrypted and credentials should be exchanged outside of the anonymizer. For even trustworthy anonymizers, anonymizers cannot filter out any malicious code that may reveal the identity of the user who wishes to remain anonymous. See malware. Care should be taken to prevent information leaks. For example, anonymizing an HTTP connection but not a DNS lookup can reveal the location of the viewer. Anonymizers also present a high value target. Groups opposite the people who want to remain anonymous target public anonymizers, especially as they are often misused. Free anonymizers, mainly open socks and http proxies, are usually operated against the knowledge of the server owner; bionetworks and other malware are known to install such services. They are used to log passwords or place advertisements/malware into the (http/email) traffic and cause high damages to the server owner because of the high bandwidth consumed and the security breach. "Bad" HTTP proxies almost always anonymize the connection by hiding the real identity of the client user to be more attractive, this can be detected through a free proxy analyzer.

2. USE OF ANONYMIZERS

Protocol specific anonymizers: Sometimes anonymizers are implemented to work only with one particular protocol. The advantage is that no extra software is needed. The operation occurs in this manner: A connection is made by the user to the anonymizer. Commands to the anonymizer are included inside a typical message. The anonymizer then makes a connection to the resource specified by the in-band command and relays the message with the command stripped out. An example of a protocol specific anonymizer is an anonymous remailer for e-mail. Also of note are web proxies and bouncers for FTP and IRC.

Protocol independent anonymizers: Protocol independence can be achieved by creating a tunnel to an anonymizer. The technology to do so varies. Protocols used by anonymizer services may include SOCKS, PPTP, or OpenVPN. In this case either the desired application must support the tunneling protocol, or a piece of software must be installed to force all connections through the tunnel. Web browsers, FTP and IRC clients often support SOCKS for example, unlike telnet.

Use of multiple relays: One example of "daisy-chained" anonymizing proxies is the "Tor network". Tor does not encrypt your traffic from end to end; rather it builds up a series of encrypted connections through the relays in the Tor network. An additional layer of encryption should be used with Tor if end-to-end encryption is required. See risks of using anonymous proxy servers. Another example is I2P - the Anonymous Network. It works similar to Tor, yet with some crucial differences: I2P is an internal network. It is totally decentralized and does not rely on central lists servers and unlike Tor it uses no bidirectional tunnels, which makes timing attacks far more difficult, and it is end-to-end encrypted. As you never know if a given mix logs all connections or not, the only way to be really sure there is no logging is to run your own anonymizing mix node and blend your traffic with those of other users, who in turn need not trust you, as they blend their traffic with yours and other users' traffic in their own mix nodes. This is the philosophy behind i2p - each nodes routes traffic for others and blends its own traffic in, whereas one's own traffic will be relayed by other peers through so-called tunnels made-up of various other peers. The network is highly dynamic and totally decentralized. It takes care of other nodes learning about the node existing, for without peers using your node, there would be no traffic to blend yours with. As all traffic always stay within the i2p network, a routing user's i2p will never show on public websites' logs. Another example of multiple relays is sending an e-mail to an anonymizing remailer, which relays it to another remailer, which eventually relays it to its destination.

3. EXISTING SYSTEM

Existing method a current location-based services where users have to report their exact locations to the database server in order to obtain their desired services. For example, a mobile user asking about her nearest restaurant has to report her exact location. With untrusted service providers, reporting private location information may lead to several privacy threats. LS make spatial data available to the users through one or more location servers (LS) that index and answer user queries on them. Examples of spatial queries could be “Where is the closest hospital to my current location?” or “Which pharmacies are open within a 1 km radius?” In order for the LS to be able to answer such questions, it needs to know the position of the querying user. Existing peer-to-peer (P2P) spatial cloaking algorithm in which mobile and stationary users can entertain location-based services without revealing their exact location information. The main idea is that before requesting any location-based service, the mobile user will form a group from her peers via single-hop communication and/or multi-hop routing. Then the spatial cloaked area is computed as the region that covers the entire group of peers.

4. PROPOSED SYSTEM

The proposed system designs a frame work that uses an anonymiser for the purpose of providing security to the user’s data which has sent for the query processing. The frame work introduces some Query processing techniques by network expansion. Starting from the user location u, it discovers objects on encountered edges while traversing the network like Dijkstra’s algorithm, until the query results are found.

The proposed system also uses alternative location privacy approaches other than spatial anonymity. It uses cryptographic techniques, to guarantee that an adversary cannot effect the user’s location.

5. SYSTEM DESIGN

Anonymizer: When a user wishes to pose a query, she sends her location to a trusted server, the anonymizer (AZ), through a secure connection (e.g., SSL). The latter obfuscates her location, replacing it with an anonymizing spatial region (ASR) that encloses u. The ASR is then forwarded to the LS. Ignoring where exactly u is, the LS retrieves (and reports to the AZ) a candidate set (CS) that is guaranteed to contain the query results for any possible user location inside the ASR. The AZ receives the CS and reports to u the subset of candidates that corresponds to her original query. In order for the AZ to produce valid ASRs, the users send location updates whenever they move (through their secure connection)

Location Server: The ASR construction at the AZ abides by the user's privacy requirements. Particularly, specified an anonymity degree K by user, the ASR satisfies two properties: 1) it contains user and at least another K _ 1 users and 2) even if the LS knew the exact locations of all users in the system, it would not be able to infer with a probability higher than 1=K who among those included in the ASR is the querying one.

Add Location information inside the location server: LBS make spatial data available to the users through one or more location servers (LSs) that index and answer user queries on them. Examples of spatial queries could be "Where is the closest hospital to my current location?" or "Which pharmacies are open within a 1 km radius?" In order for the LS to be able to answer such questions, it needs to know the position of the querying user.

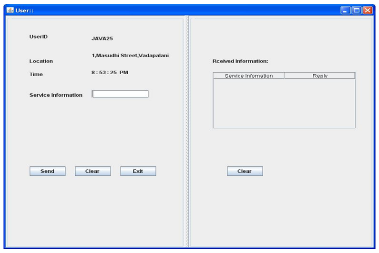
Category: Users are reluctant to use LBSs, since revealing their position may link to their identity. Even though a user may create a fake ID to access the service, her location alone may disclose her actual identity. Linking a position to an individual is possible by various means, such as publicly available information (e.g., city maps and telephone directories), physical observation, cell phone signal triangulation, etc. User privacy may be threatened because of the sensitive nature of accessed data, e.g., inquiring for pharmacies that offer medicines for diseases associated with a social stigma, or asking for nearby addiction recovery groups.

Receiver information at the destination: While the above ASR properties guarantee spatial K-anonymity to u, imposes requirements on CS computation. In particular, given an ASR, the LS must produce an inclusive and minimal CS. Inclusiveness demands that CS is a superset of us query results; this property ensures that u receives accurate and complete answers. Minimality, on the other hand, requires that the CS contains the minimum number of data objects, without violating inclusiveness. Minimality ensures that CS transmission (from the LS to the AZ) and its filtering at the AZ do not incur unnecessary communication and processing overheads.

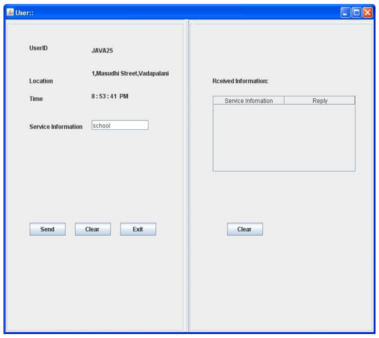
6. IMPLEMANTATION

We adopt the trusted anonymizer model (i.e., the use of the AZ as a mediator between users and the LS),
1. the proliferation of this model in existing anonymous services provide anonymous use of the Internet/e-mail-based services without revealing the user's real e-mail, the Anonymizer provides anonymous Web surfing,etc
2. Its suitability for time-critical applications
3. The existence of information security techniques and system architectures that support trusted third-party services.
4. The availability of methods to ensure that a third party (i.e., the AZ) will honor the user privacy requirements.

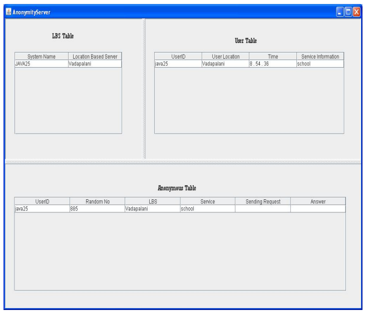
7. RESULTS



UserID JAVA25
Location 1,Masudhi Street,Vadapalani
Time 8 : 53 : 25 PM
Service Information



UserID JAVA25
Location 1,Masudhi Street,Vadapalani
Time 8 : 53 : 41 PM
Service Information school



LBS Table

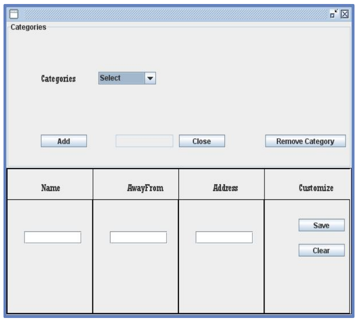
System Name	Location Based Server
JAVA25	Vadapalani

User Table

UserID	User Location	Time	Service Information
java25	Vadapalani	8 . 54 . 36	school

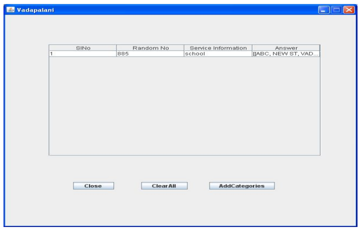
Anonymous Table

UserID	Random No	LBS	Service	Sending Request	Answer
java25	885	Vadapalani	school		

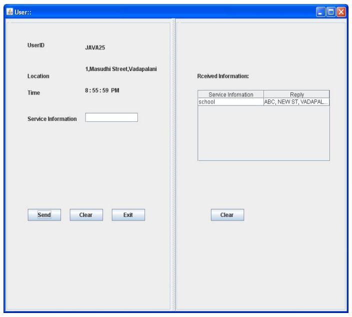


Categories Select

Name	AwayFrom	Address	Customize



SINo	Random No	Service Information	Answer
1	885	school	[[ABC, NEW ST, VAD...



UserID JAVA25

Location 1,Masudhi Street,Vadapalani

Time 8 : 55 : 59 PM

Service Information

Rceived Information:

Service Infomation	Reply
school	ABC, NEW ST, VADAPAL...

8. CONCLUSION

In this paper the network-based anonymization and processing (NAP) frame work has been proposed. This frame work mainly relies on global user ordering satisfies reciprocity and guarantees k-anonymity. The subsequent processing can be identified and compared with the alternatives. We also proposed some techniques that are used for query evaluation. Network based anonymization and processing achieves user privacy and economically feasible costs and quick responses all over. This framework is ready to deploy as it requires only basic network operations.In the location based service the data available uses a location server. When the data sent to the third party, the challenge is how to encrypt the owners' data so that the data can not be revealed to location server. So we propose anonymiser which could verify that the location server could not get access for the data of the owner and it could not reveal the users identity.

REFERENCES

[1.] Anonymous Query Processing in Road Networks Kyriakos Mouratidis and Man Lung Yiu

[2.] G. Aggarwal, M. Bawa, P. Ganesan, H. Garcia-Molina, K. Kenthapadi, N. Mishra, R. Motwani, U. Srivastava, D. Thomas, J. Widom, and Y. Xu, "Vision Paper: Enabling Privacy for the Paranoids," Proc. Int'l Conf. Very Large Data Bases (VLDB), 2004.

[3.] http://www.spamgourmet.com/, 2009.

[4.] http://www.mailshell.com, 2009.

[5.] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Hippocratic Databases,” Proc. Int’l Conf. Very Large Data Bases (VLDB), 2002.

[6.] A.R. Butz, “Alternative Algorithm for Hilbert’s Space-Filling Curve,” IEEE Trans. Computers, vol. 20, no. 4, pp. 424-426, Apr. 1971.

[7.] T. Brinkhoff, “A Framework for Generating Network-Based Moving Objects,” GeoInformatica, vol. 6, no. 2, pp. 153-180, 2002.

[8.] A.R. Beresford, “Location Privacy in Ubiquitous Computing,” PhD thesis, Computer Laboratory, Univ. of Cambridge, 2005.

[9.] C.-Y. Chow and M.F. Mokbel, “Enabling Private Continuous Queries for Revealed User Locations,” Proc. Int’l Symp. Spatial and Temporal Databases (SSTD), 2007.

[10.]C.-Y. Chow, M.F. Mokbel, and X. Liu, “A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location-Based Service,” Proc. Ann. ACM Int’l Symp. Advances in Geographic Information Systems (GIS), 2006.