An EPLQ Approach for Preserving Privacy over Outsource Encrypted Data

C. Shyamala kumari, Florence S

Abstract— Location based services is a combination of network computing and wireless telecommunication, which offers services based on the geographical information of the user. The user's location privacy is considered to be a threat nowadays .Keeping that in mind, point of interest is developed which is used for a short range. This further goes on as how well the privacy issues are taken care. So they come up with an approach for protecting the privacy policy which is EPLQ.In this schema they consider the spatial data queries for their particular range and design a inner structure tree for preserving their privacy. As LBS finds much application in real words nowadays the privacy must be preserved well. Because of this approach they find themselves in a considerable position.

1. INTRODUCTION

The advent of big data and cloud in the services aspects makes, location based services to find a considerable place in the blooming technological world. Clouds acts as a data pool and acts as a key to computing purpose. Such aspect finds application here in terms of privacy. The big clients are outsourcing a large amount of data only because of this emergence of spatial computing and big data. The EPLQ approach is studied extensively and it proves that they are much secured when it comes to the privacy of the user. In order to lessen the fault tolerance they use a primary tree like structure with inner circle in their design. Nowadays social networks acts as a powerful medium in communication and spreading news all round the globe. They immensely used location as a primary basis for their access,LBS finds a place in all these applications and maintain their privacy significantly according to the user's needs. As data is being outsourced it remains as a biggest challenge to preserve the privacy. The growing trend of outsourcing is mainly because of its less financial investments and the operation benefits at various levels of data warehouse. They face challenges to design a protocol for maintaining the privacy of location by integrating the cloud and mobile computing in the spatial query range. The cost would be much high to design such a thing, which includes the cost to be paid for the storage and the computation. If the privacy is maintained then there would be an increase in the latency too.

A scheme called as IPRE is used to test to the privacy by taking in to account of the vectors. They do not disclose the vectors. They consider the product of them within a particular distance. Second, EPLQ is used which accounts for the preservation of the privacy .This technique can be even applied for the outsourced data, as they are the challenging task nowadays. They use the Euclidean distant method as the convention having the spatial data analysis. The main advantage is that they can be less cost and more reliable and secured. They can be stored archived and can be discarded anytime.

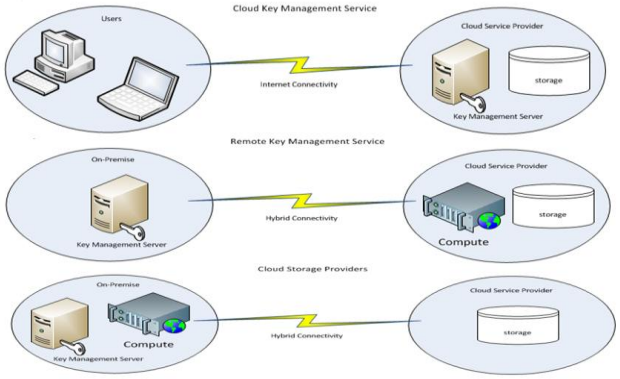


Figure 1. Management Services and Storage providers

2. PROCESS DESCRIPTION

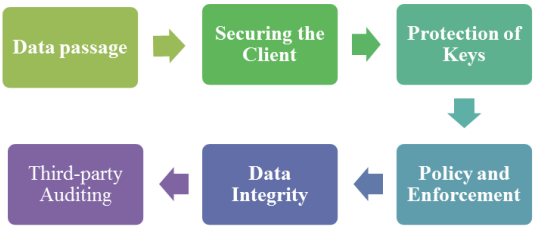


Figure 2. Process Diagram

2.1 Data Passage:

Data passage means the information is broadcasted from one archive to the other one. All sensitive information during the transmission is secured while sending through wired, air and other sorts of medium in consideration. This is mainly done by the encryption before they get to travel from one node to the other.

2.2 Securing the Client:

In today's world everyone need to be under their private space. In accordance with that ,the services which are provided by the computing servers needs to consider the

Revised Version Manuscript Received on 30 May, 2018.

C. Shyamala kumari, Assistant Professor, Department of Computer Science and Engineering, Veltech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamilnadu, India.(E-mail: shyamala.c1@gmail.com)

Florence S, Assistant Professor, Department of Computer Science and Engineering, Veltech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamilnadu, India.

policy of privacy while sending the encoded information through channels. The service providers should consider them too and provide necessary services in order to curb any kind of faults in the devices which provides geographical location. They should monitor them accordingly and provide necessary services based on their utility to the client.

2.3 Protection of Keys

In this encoding the role of key is considered to be in top priority. They should produce keys and store them before sending and archive them after transit and de-provisioning them. The key generated here plays a major role as it is encrypted along with the location it needs special attention while get encoded.

2.4 Policy And Enforcement

Policy breach is something which makes negative impact nowadays, so one must enact policy in such a way that it must be safe and secure. The cloud provider should value the clients and enact the services and policy which would meet their privacy needs and it should be strictly enforced based on the applications they are used for.

2.5 Data Integrity

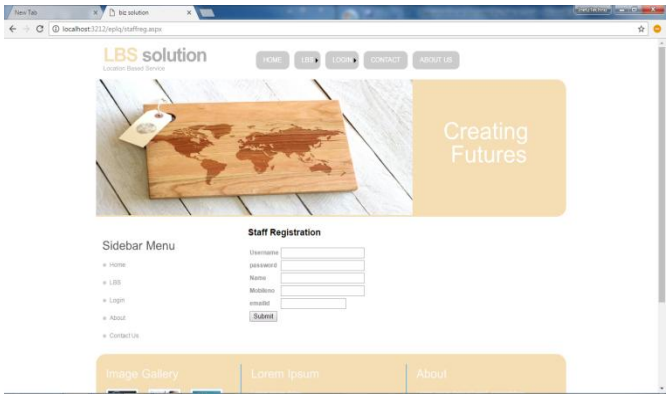
If an information is send in a channel it must be properly encrypted so that it will be secured. The encoded data and the location using the device GPS are integrated in to a single unit and get transmitted. so that it is wrapped and can't be decoded that easy.

2.6 Third-Party Auditing

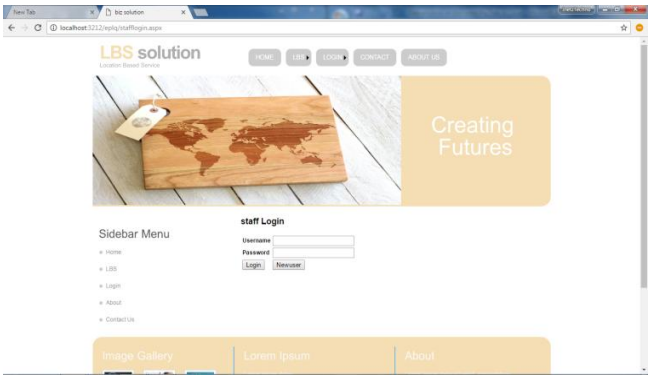
Here cloud service providers acts as a third party ,they should hope with the on presumption policy. This also depends not only on the end users but also on the third party clients and require them to monitor them on monthly basis and check any flaws present while they transmit the data through their dedicated servers.

3. EXPERIMENT RESULTS

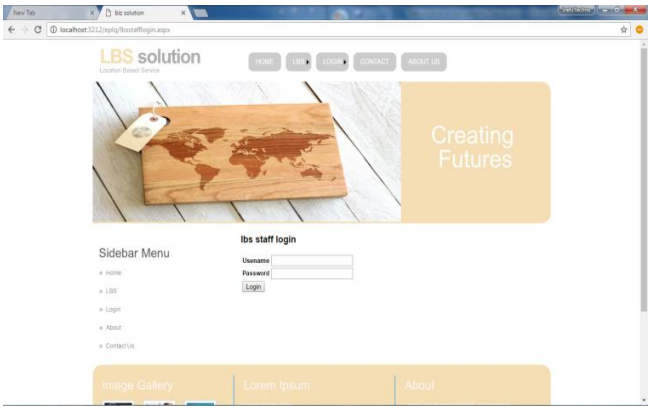
3.1 Register Page:



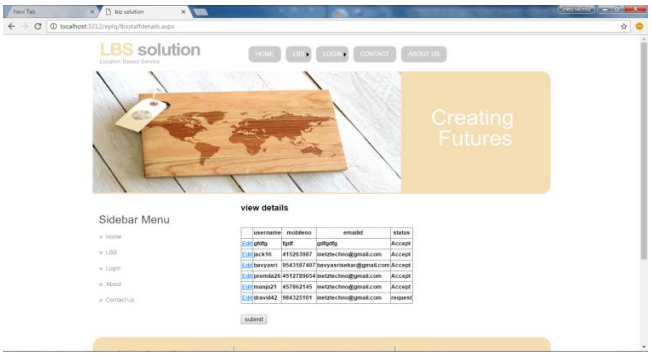
3.2 Login Page:



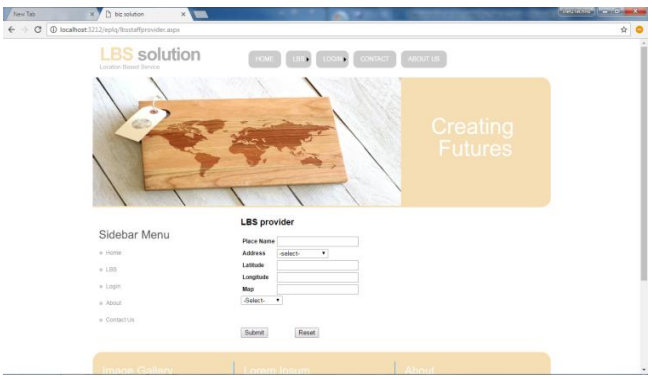
3.3 LBS Provider Login:



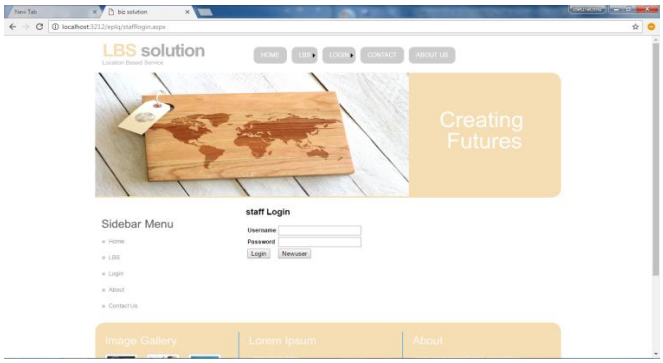
3.4 LBS View Details:



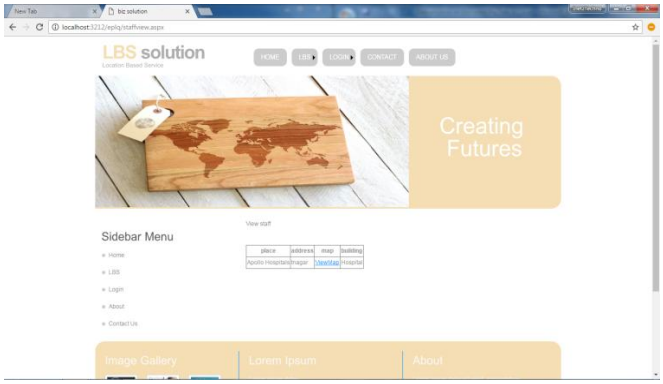
3.5 LBS Provider:



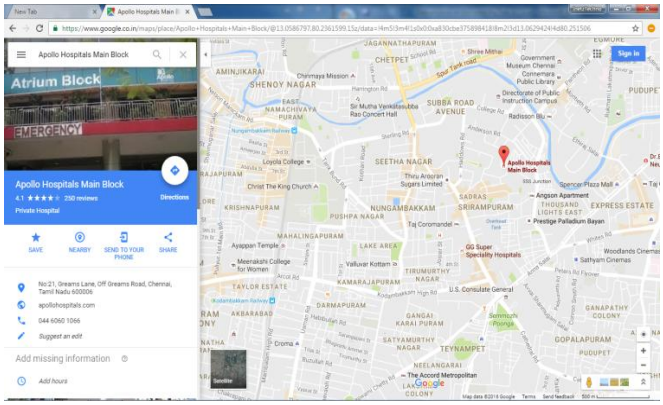
3.6 User Login:



3.7 Place View:



3.8 Access the Location:



4. CONCLUSION

With this above mentioned approach, the information or data can be integrated in a third party cloud storage other than the clients. It has a huge potential along with personal navigation It can be retrieved whenever they are requested on demand. Moreover they can be achieved and even discarded after their need. The security tier is maximized even better before. They show us the traffic n sending and receiving is much less when compared to the conventional methods. A proposal is kept forwarded for setting this approach under multiserver setting which gives less fault tolerance. The running time is calculated using test beds and it very much less. When it comes to security it is much secured and hard to decode for the crackers.

5. FUTURE ENHANCEMENT

Future work embraces optimizing our plan and achievement for convenient exploitation and learning certifiable estimation to guarantee that CSP perform as predictable in de duplication organization.

REFERENCES

1. Chen R., 2005. Navigation Methods and Wireless Locations, Finnish Geodetic Institute, Department of Navigation and Positioning, http://users.tkk.fi/~rchen/Wireless_Location.pdf, (accessed 10 Feb. 2006).
2. Prasad M., 2005. Location based services, http://www.gisdevelopment.net/technology/lbs/techlbs003.htm (accessed 24 Nov. 2005).
3. Roth, J., Context-aware Web Applications Using the PinPoint Infrastructure, in IADIS International Conference WWW/Internet. 2002, IADIS Press: Lisbon, Portugal.
4. Marmasse, N. and C. Schmandt, Safe & sound - a wireless leash, in Proceedings of CHI 2003, extended abstracts. 2003.
5. Y. Wang et al., “A Fast Privacy-Preserving Framework for Continuous Location-Based Queries in Road Networks,” J. Network and Comp. Applications, vol. 53, 2015.
6. F. Olumofin et al., “Achieving Efficient Query Privacy for Location Based Services,” Proc. Int’l. Symp, Privacy Enhancing Technologies, Springer, 2010.
7. A. Pingley et al., “Protection of Query Privacy for Continuous Location Based Services,” Proc. IEEE INFOCOM 2011.