

Secure Database Server Handles Spatial Location

Srikanth Kottalanka and D. Arivazhagan

Department of Information Technology, AMET University, Chennai, India

Abstract: Now a days spatial location is upgraded simultaneously to consumers, accessing spatial information from location based service providers. System that processed under this location services, need a trusted server to manage all user location based information securely from third party. People are involved with cabs (taxi) for their day to day life cycle, each time they need to answer their location to the perspective drivers. New database server is designed to keep all their location information securely using Extended Matrix-Attribute Based Encryption (EM-ABE) algorithm which provides security as well as privacy for users. Here, we store user's location on a database and whenever the user needs to share that location with their respective cab running companies. The users permanent location is been hidden without the user they can't access any location related information as well as users sensitive information. RSA algorithm is implemented to encrypt users query and process simultaneous for multi-query mechanism.

Key words: Location based service providers, database server, RSA algorithm, security, simultaneous, implemented

INTRODUCTION

Location based services emerged quickly to the environment, providing user to search location using GPS via, mobile phones (Ghinita *et al.*, 2008). When we come up with spatial query search functions worked perfectly to share and know the location of our neighbors. It all end up with a server and data base which contains of location information that connect to Google map and show the location searched. But these kinds of information need to secured to prevent user location from third parties who follow user's activities.

In cases, the searches come up with some false information on location (Yiu *et al.*, 2009). The database management privacy is an important role in this concept where the location of a user and a query has to be secured and also not reveal that sensitive information to other.

Location services always a data store and retrieve process whenever a query raise by a user or location add in a database should be accurate and could not provide some other location to the user. A new concept is been implemented to secure the information of the user by maintaining a database that add location, user's information and fetch it back to the user when required.

Literature review: Location services related methods and systems provides a valiant process where user query is been processed and response back with proper information. Each process requires a server to monitor

query and search similar information for that query and give it to the user (Ghinita *et al.*, 2010). They provide a system to contribute service among all users whenever they need they can access information from the server as a query. Even in Google maps the spatial information of a random query cannot be right all the time and that lacks in accuracy which tends to wrong for the user. Whenever a location is stored on a database, action of checking the location is right or wrong is necessary to convey trusted location all the time to the user (Ghinita *et al.*, 2010).

Applications process that kind of information as a front end connected with a database to store and retrieve spatial information whenever required. Even that application lacks in privacy issues where information access control standards come on to the location based service providers and access information without the knowledge of the user (Kirubakaramoorthi *et al.*, 2015). Some protocols prevent privacy among third parties but in other ways they try out paillier public key cryptosystem to decrypt information and view the spatial information from the database (Shanthi and Anita, 2016). Secure and Efficient Distance Effect Routing Algorithm for Mobility (SE-DREAM) in MANETs was described by Shanthi and Anita (2016). New cryptography algorithm for effective data communication was proposed and an Inception of DdoS attacks for popular websites-identifying on application-layer was explained (GaneshKumar and Arivazhagan, 2017; Ganeshkumar and Arivazhagan, 2014; Ganeshkumar *et al.*, 2016).

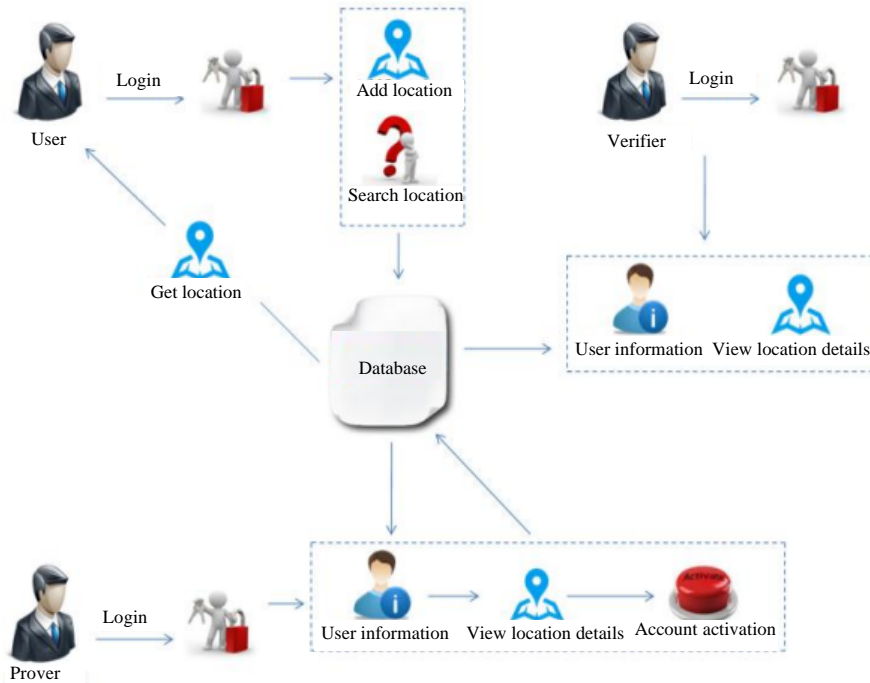


Fig.1: Architecture of proposed system

MATERIALS AND METHODS

An application is implemented to store user information on the database securely using EM-ABE algorithm. In Fig.1, a database is implemented where user will access their account, add location and search location whenever necessary. Then, it moves to prover to check the user is trusted or un-trusted to activate user account to further proceedings. Once the account activation is processed, user can access information on database according to their query. The term verifier is another user, who tries to access user’s information on the database. There we provided privacy where no other person can have the right to access some other user’s information on the database without any knowledge. In proposed research the modules are:

- User
- Prover
- Verifier

User: When the user is come over login process they can add their locations into the database which is been secured and hidid. Where some personal information’s are encrypted when someone access user details, the content cannot be seen by even verifier and prover. User

have to enter the valid query, then location is been connected via. Google API and accuracy of location is increased.

Prover: An authentication is also, created for prover to secure user details and location details in the database. After the verification process, the prover can activate the account of user to further procedures. Here, prover can view the user details and location details that can show some of the details and hides user’s personal information. Each user can have a valid account after the prover activates the account.

Verifier: An authentication is also, created for verifier to secure user details and location details in the database. Each user information has been verified here and providing the valid location to increase the accuracy of the location. Where now days in Google it self showing fake locations and some other location for queries which misleads the user to unknown places. After the verifier process the prover follows.

RESULTS AND DISCUSSION

Spatial location, prover storing, verifier access is discussed in this study. Figure 2-5 are discussed in this study.

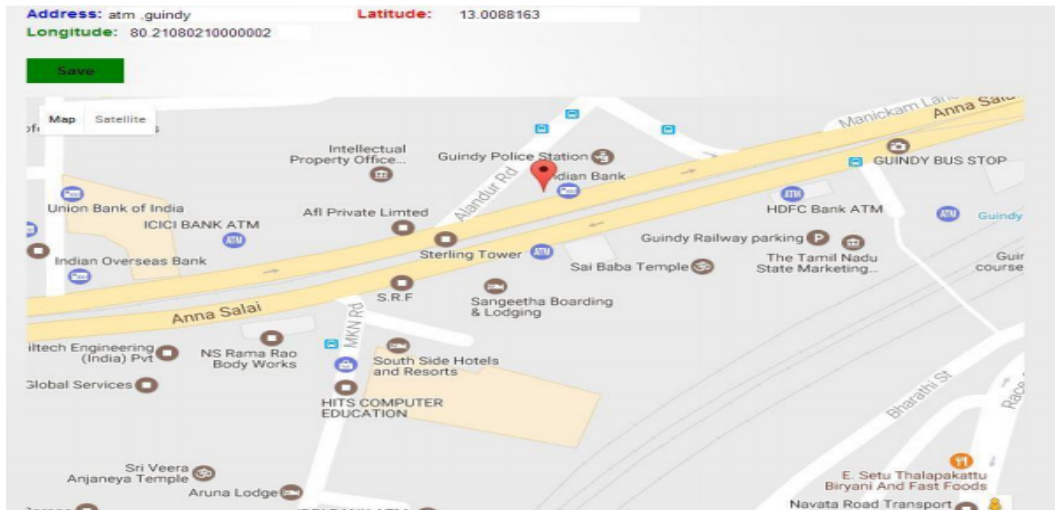


Fig. 2: Spatial location (Store option)

User Details!

NAME	USERID	PASSWORD	MAIL ID	DATE OF BIRTH	LOCATION	GENDER	TIME	ACCEPT	DELETE	STATUS
Arunchalam arunchalam	*****	*****	vetech.software@gmail.com	2010-03-16	Vellore	Male	2017-03-01 17:07:47.0	Accept	Delete	Yes
naveen	naveen	*****	dotnetjava.projects@gmail.com	2017-03-21	villupuram	Male	2017-03-01 17:17:39.0	Accept	Delete	Yes
Arunachalam Arun	*****	*****	arunachalamvs777@gmail.com	2013-05-08	Moulivakkam	Male	2017-03-06 14:44:44.0	Accept	Delete	Yes
Sowparanika Barani	*****	*****	sowparanika55@gmail.com	2017-03-09	Thiruvanamalai	Female	2017-03-09 13:02:35.0	Accept	Delete	Yes
pavithra pavi	*****	*****	pavithrait706@gmail.com	1996-06-26	nallavanpalayam	Female	2017-03-20 10:12:13.0	Accept	Delete	Yes

Fig. 3: Prover activating user accounts

Location Details!

USERID	PURPOSE	LOCATION	DESCRIPTION	LATITUDE	LONGITUDE	ACCEPT	DELETE	STATUS
parthy	Bank	Pondicherry	wowo... ww	11.926467279	64335000000005	Accept	Delete	Yes
parthy	ck college	cuddalore	surpb college	11.749574	79.763822	Accept	Delete	Yes
parthy	INDIAN BANK	PONDICHERRY	GOOD BANK	11.993220279	63792379999995	Accept	Delete	No
gyanu	Work	Mugalivakkam	its a great place for setup industry	13.017226	80.14270039999997	Accept	Delete	Yes
gyanu	School	Moulivakkam	this is good place to open CSBE School	13.017226	80.14270039999997	Accept	Delete	Yes
naveen	Engineering college	kallaikuruchi	best place	11.741705878	98230079999996	Accept	Delete	Yes
Arun	schools	porur	asdf	13.040393880	15551690000007	Accept	Delete	Yes
Arun	School	vadapalani	fgh	13.048658180	21492949999993	Accept	Delete	Yes
Barani	atm	guindy	skdfkls	13.015110480	20349439999995	Accept	Delete	Yes
Barani	temple	tiruvannamalai	nice place to pray	12.231646179	06773989999999	Accept	Delete	Yes
pavi	beach	cuddalore	gyfghkhui	11.739392879	78659390000007	Accept	Delete	Yes

Fig. 4: Prover storing trusted location to database

User Details!

NAME	USERID	PASSWORD	MAIL ID	DATE OF BIRTH	LOCATION	GENDER	TIME
Arunchalam	arunchalam	*****	vetech software@gmail.com	2010-03-16	*****	Male	2017-03-01 17:07:47.0
naveen	naveen	*****	dotnetjava.projects@gmail.com	2017-03-21	*****	Male	2017-03-01 17:17:39.0
Arunachalam	Arun	*****	arunachalamvs777@gmail.com	2013-05-08	*****	Male	2017-03-06 14:44:44.0
Sowparanika	Barani	*****	sowparanika55@gmail.com	2017-03-09	*****	Female	2017-03-09 13:02:35.0
pavithra	pavi	*****	pavithrait706@gmail.com	1996-06-26	*****	Female	2017-03-20 10:12:13.0

Fig. 5: Verifier access (Hiding information)

CONCLUSION

We conclude our proposed implemented a database to securely add location and search queries without revealing it to the third party. An authentication method is used to prevent un-authorized access. Query search, retrieval process are simultaneously done without any time delay. Accuracy is been improved to provide trusted location to the user for comfortable usage while necessary. Administrator cross verify each location as well as user to maintain an efficient data base to store and fetch with a privacy.

REFERENCES

GaneshKumar, K. and D. Arivazhagan, 2017. New cryptography algorithm with fuzzy logic for effective data communication. *Indian J. Sci. Technol.*, Vol. 9, 10.17485/ijst/2016/v9i48/108970

Ganeshkumar, K. and D. Arivazhagan, 2014. Generating a digital signature based on new cryptographic scheme for user authentication and security. *Indian J. Sci. Technol.*, 7: 1-5.

Ganeshkumar, K., D. Arivazhagan and S. Rajkumar, 2016. An inception of DDoS attacks for popular websites-identifying on application-layer. *Indian J. Sci. Technol.*, Vol. 9, 10.17485/ijst/2016/v9i47/108078

Ghinita, G., P. Kalnis, A. Khoshgozaran, C. Shahabi and K.L. Tan, 2008. Private queries in location based services: Anonymizers are not necessary. *Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data*, June 09-12, 2008, ACM, New York, USA., ISBN:978-1-60558-102-6, pp: 121-132.

Ghinita, G., P. Kalnis, M. Kantarcioglu and E. Bertino, 2011. Approximate and exact hybrid algorithms for private nearest-neighbor queries with database protection. *GeoInformatica*, 15: 699-726.

Kirubakaramoorthi, R., D. Arivazhagan and D. Helen, 2015. Survey on encryption techniques used to secure cloud storage system. *Indian J. Sci. Technol.*, Vol. 8, 10.17485/ijst/2015/v8i36/87861

Shanthi, H.J. and E.M. Anita, 2016. Secure and efficient distance effect routing algorithm for mobility (SE_DREAM) in MANETs. *Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC-16')*, March 10-11, 2016, Springer, Cham, Switzerland, ISBN 978-3-319-30347-5, pp: 65-80.

Yiu, M.L., G. Ghinita, C.S. Jensen and P. Kalnis, 2009. Outsourcing search services on private spatial data. *Proceedings of the IEEE 25th International Conference on Data Engineering (ICDE'09)*, March 29-April 2, 2009, IEEE, Shanghai, China, ISBN:978-1-4244-3422-0, pp: 1140-1143.