IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 23, Issue 2, Ser. I (Mar. – Apr. 2021), PP 47-51
www.iosrjournals.org

Location Based Services with Data Examination and Restoration

R.Ranjith[1], E.shalini[2]
[1](Assistant Professor/Computer Science Department, St.Joseph's college of engineering, Chennai)
[2](PG student/Computer Science Department, St.Joseph's college of engineering, Chennai)

Abstract: *The main motivation to provide location-based services(LBS) that include identifying the user locations and Storing large amounts of data with cloud service providers (CSPs) concern about data protection .The purpose of the work is provide a implementation methodology for location based services ,examine the data and restoration which is stored in cloud. To solve the particular areas problems like water problem, electricity problem, transport problem and sewage problems in a particular area. User files the complaint along with location in the website that will be moved to the particular department. Then admin will view the user complaints and then based on station the respective admin will respond to user regarding the complaints. Once the problem solved that information send to the user. Verification of data in cloud is performed by third-party Examiner (TPE). TPE are also appropriate for public data examining, in public examiner a third-party Examiner (TPE) is designated to check the correctness of cloud data without retrieving the entire data from the cloud service provider CSP and also examine the loss of data that stored in cloud. Advanced Encryption Algorithms (AES) for cloud data Examine, the integrity and privacy issues that these algorithms face and generate report to user*

Date of Submission: 07-03-2021 Date of Acceptance: 20-03-2021

I. Introduction

The development of Location Based Services (LBS) and management system that's easy, effective and efficient to perform the report and management of problems within city. Since the people don't find convenient to travel recommended office to register a compliant because of several reasons like power supply or water scarcity etc. Also some problems don't seem to be investigated thanks to lack of proper details. This method allows the individuals within a city to register the complaints and helpful to the officer and section in identifying problems. This application can improve the efficiency of system in an exceedingly city and problem solving procedures may be enhanced to attain better results. The main scope is to develop an internet problem solving report and managing system which is well easily accessible to the people. This method provides proper security and reduces the manual work .In proposed system tries to eliminate or reduce difficulties up to some extent. This method will help the user to scale back the workload and mental conflict. It helps the user to figure user friendly and user can easily do their jobs without time lagging. Storing large amounts of knowledge with cloud service providers (CSPs) raise concerns about data protection. Data integrity and privacy are often lost thanks to the physical movement of information from one place to a different by the cloud administrator, malware, dishonest cloud providers, or other malicious users who might distort the information. Verification of information in cloud is performed by third-party Examiner (TPE). TPE are appropriate for public data examining, publicly examiner a third-party Examiner (TPE) is designated to test the correctness of cloud data without retrieving the whole dataset from the cloud service provider (CSP) and also examine the loss of knowledge that stored in cloud. Advanced Encryption algorithms for cloud data Examine, the integrity and privacy issues. The development of Location Based Services (LBS) and management system that's easy, effective and efficient to perform the report and management of problems within city.

II. Related Work

Several techniques were used for Location based services with data examination and restoration. Few related works are as follow:

Gang sun ,Shuai cai, Hongfang yu , sabita Maharjan, Victor chang, Xiaojiang du and Mohsen Guizani[1] Propoesd PPCS algorithm.PPCS approach can generate dummy locations that don't contain the important location of a user location-based cyber services are increasingly found in mobile applications (e.g., social networking and maps), user location privacy preservation is crucial and remains one altogether the several on-going research challenges. Author proposed a region-of-interest division-based algorithm to preserve the position Privacy of mobile device users in location-based Cyber Services (PPCS).existing methods author proposed PPCS approach generates dummy locations while considering the semantic information of those locations. The Privacy of mobile device users in location-based Cyber Services (PPCS) algorithm enables

the generated locations to exclude. Author demonstrates that PPCS is resilient to both colluding attacks and inference attacks. Efficiency is evaluated and demonstrates the simulations.

Walid i. Khedr, Hebam. Khater, and Ehab r. Mohan[2] proposed Rivest-Shamir-Aldeman(RSA) algorithm. A PDP scheme allow athorized user to efficient verify that a cloud storage provider possesses the outsourced data. Most of the currently available data possession check schemes make selective (i.e., probabilistic) rather than checking the complete dataset checks using random data blocks to verify data integrity. Therefore, these schemes are considered inadequate by critical infrastructure sectors that involve sensitive data (critical data). During this paper, a very efficient data integrity check scheme called cryptographic-accumulator provable The underlying scheme of the CAPDP relies on a modified RSA-based cryptographic accumulator that has the next advantages: 1) it allows the data owner to perform an infinite number of knowledge integrity checks; 2) it supports data dynamics; 3) it's efficient in terms of communication, computation and storage costs for both the knowledge owner and also the cloud storage provider; 4) the verification operation within the proposed scheme is independent of the number of blocks being verified; 5) it minimizes the burden of the verification process on the information authorised , enabling verification to be performed even on low-power devices.6) it prevent forgery, data deletion, replacement, and data leakage

Shuo Yang, Hao Yu and Wei Deng Solvang[3] proposed Mobility is significant to non-public freedom. With the increasing availability of mobile devices, many providers begin to provide location-based services. The services enrich mobility experiences, with user and also come the privacy concerns, as a location-based service provider now can continuously track the position of a user.Although some solutions are proposed to handle the privacy concerns in various aspects, there has not been any comprehensive study of the problem; furthermore, most of the prevailing solutions require that a user trust a 3rdparty type of a location server.

R. Shahid, N. Pissinou, S. S. Iyengar, J. Miller, Z. Ding and T. Lemus[4] proposed In Location-Based Services (LBS), users are required to disclose their precise location information to question a service provider. Unauthorized service provider can overwrite the queries to infer sensitive information on a user through spatiotemporal and historical data analyses. Disadvantage of existing privacy-preserving approaches in Location Based Services, author proposed a user-centric obfuscation approach, called KLAP, supported the three fundamental obfuscation requirements: k number of locations, l-diversity, privacy area preservation. Considering user's sensitivity to different locations and utilizing Real Time Traffic Information (RTTI), KLAP generates a convex Concealing Region (CR) to hide user's location specified the locations, forming the CR, resembles similarsensitivity and are resilient against an outsized range of inferences in spatio-temporal domain. For the first time, a totally unique CR pruning technique is proposed to significantly improve the delay between successive CR submissions

III. Proposed System

The motivation is to provide easy, fast and accurate online systems that help the people to register their complaints at any time by getting the API key in the website Google map will be enabled in the website. User can file complaints in online along with location and user can also check the status of the complaint .once the problem was solved user can check the status of the complaint. It is an easy way get the information from the department. Public verifier is able to audit shared data integrity without retrieving the entire data, to improve the efficiency verifying multiple auditing tasks, further extend our mechanism to support batch auditing. Advantage of proposed system the proposed system can perform multiple auditing tasks simultaneously. For multiple auditing task efficiency is improved. High security provide for file sharing. It reduces the man power and time. Maintain all the complaint records. By using hashing technique to find corruption of data .Hashing technique generate hash key and Advanced Encryption Algorithm is used for authorization purpose whether authorized user registered the complaint.

SYSTEM ARCHITECTURE

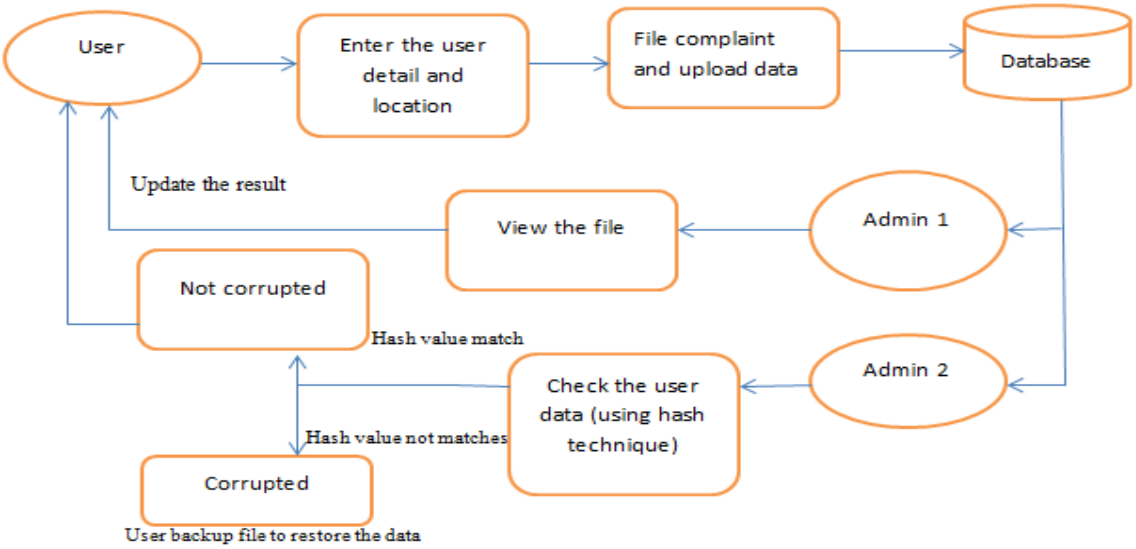

Figure 1.1: Proposed architecture

IV. Methodology

Procedure methodology: The main motivation to provide location-based services(LBS) that include identifying the user locations and Storing large amounts of data with cloud service providers (CSPs) concern about data protection. The purpose of the work is providing a implementation methodology for location based services to examine the data and restoration which is stored in cloud. To solve the particular areas problems like water problem, electricity problem and sewage problems in a particular area. The project consists of about four modules by which it satisfies its above-mentioned aim. The modules are for various actions such as User Register the complaint, Server Access the complaint, analyzing the data about corruption and Intimate the result about complaint. The modules are hereby explained below

1. User Register the complaint
2. Server Access the complaint
3. Analyzing the data about corruption
4. Intimate the result about complaint

1. User Register the complaint

User register with Name, email ID, password, age, gender and product key. After registration user automatically proceed to map the location of the user. Java database connectivity used for storing the data and all the data are stored in database. Complaints uploaded by the user automatically proceed to the respective Department. User registered information are stored in database by using Java database connector. User will mention their location based on the compliant like sewage, transport, water, Food and garbage. It will move to the respective domain. User can view the status of the compliant. Google map is used for location based service for that to generate the API key.

A) Step to generate API key

Step1: To generate the API key user must Sign-in with Google account in Google cloud platform.
Step2: Select the project and then enter the name of the project, select country and agree the Terms &condition.
Step3: Created API is displayed in dashboard.
Step4: Select credential API and created project will be displayed.
Step5: Click the Google map project to create a credential.
Step6: The API key ID is created.

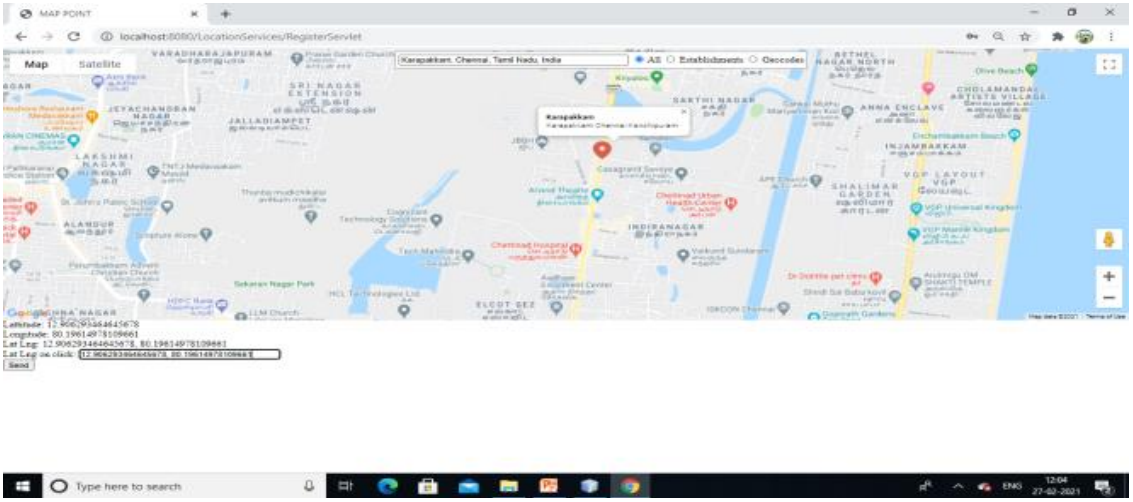

Figure 1.2: Map the user location

2. Server Access the complaint

All the station have separate admin .It is a back-end process in this module admin manage user details and complaint. Admin login using username and password. Each station admin have a separate username and password which is stored in database. Admin login into system by user name and password, admin can view all the compliant which is registered by users. Enter the ID of the user and update the status of complaint whether the problem solved or not. Compliant was solved the information will be posted on the site so user can easily view the status of the complaint. Once admin logout then admin cannot go back must login again. Java database connectivity is used to update the status.

Server access API key

Server access the API key based on the location the respective station admin will view the complaint. Each station admin have separate email and password all the mail ID and password of the admin is stored in database and type of the complaints is stored in the Database

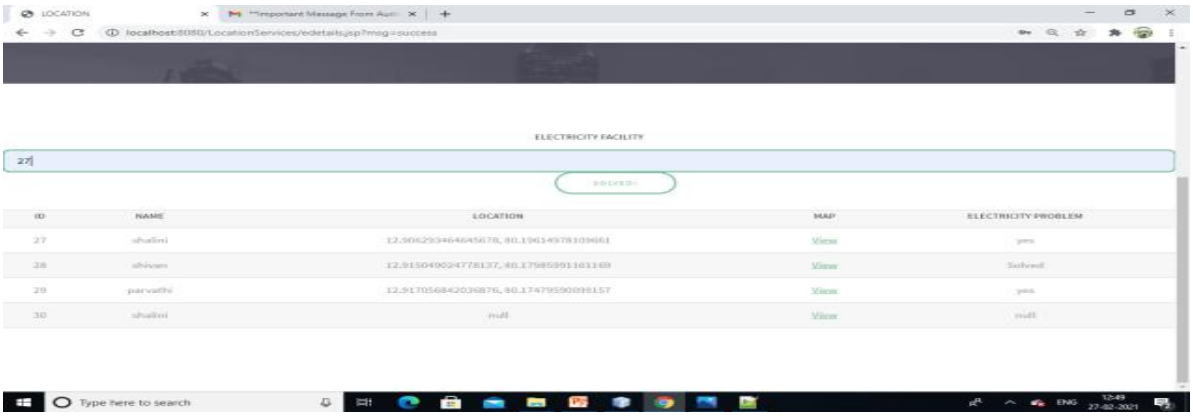

Figure 1.5: Update the status

3. Analyzing the data about corruption

The users file the complaint and then uploaded file going to be encrypted for encryption AES (Advanced Encryption Standard) algorithm is used. Admin view the complaint and check the corruption of data by using hashing technique for generating hash value. If hash value doesn't match perfectly it shows data has been corrupted, when corruption occur in the file containing the data will produce unexpected result. Corrupted data may be overwritten or it may be disabled. If the data is corrupted backup the file and restore the data. If hash value perfectly matches data stored in the database is not corrupted.

4. Intimate the result about complaint

Admin want to view the user uploaded complaint. Admin should have a secret key. For getting secret key admin want to register the key, select the user name and email ID for receiving the secret key Admin enter

the user name and password to download the user uploaded complaint. Admin received the user private key by registered email ID. If private key matches perfectly admin can download the user uploaded complaint

If private key doesn't matches perfectly admin cannot download user uploaded complaint .It will check unauthorized user uploaded the complaint by using Advanced Encryption algorithm, and it will compare to the stored data with hash value.

If systems find the uploaded complaint is fake it will inform the admin to remove the fake complaint from the website. This process will be done at the Back End by java coding. At the complaint page fake complaint will not be displayed, it will be removed by the admin who maintain the database.

A) AES Algorithm

Step1: User upload a file at that time user receive the secret key stored in database.
Step2: Using the secret key file encrypted.
Step3: MD5 for hashing it is used for data checking purpose
Step4: Hash value generated is compared with previously stored hash value.
Step5: If both value same file is not encrypted.
Step6: If both value not same regenerate the file.

V. Conclusion

Thus the work brought a clear view of User will register with proper data (where username and password must be unique for everyone).Once User registered then user can login in the system and register their complaint. User will mention their location based on the location the compliant will move on to the respected domain. The main motivation to provide location-based services(LBS) that include identifying the user locations and Storing large amounts of data with cloud service providers (CSPs) concern about data protection .The purpose of the work is provide a implementation methodology for location based services a ,examine the data and restoration which is stored in cloud.. The future classification can give more update to the user uploading the file like user can register the requirement what user needed for the time of natural disaster. Requirement directly moved to the corporation.

References

[1]. G. Sun et al., "Location Privacy Preservation for Mobile Users in Location-Based Services", IEEE Access, Vol. 7, 2019
[2]. W. I. Khedr, H. M. Khater and E. R. Mohamed, "Cryptographic Accumulator-Based Scheme for Critical Data Integrity Verification in Cloud Storage", IEEE Access, Vol. 7, 2019.
[3]. R. Moreno-Vozmediano, R.S. Montero and I.M. Llorente, "Key Challenges in Cloud Computing to Enable the Future Internet of Services", IEEE Internet Computing, vol. 17, no .4, July/Aug.2013.
[4]. B. Wang, B. Li, and H. Li, "Certificate less Public Auditing for Data Integrity in the Cloud", Proc. IEEE Conf. Comm. and Network Security (CNS'13), pp. 276-284, 2013.
[5]. C. Wang, S.S. Chow, Q. Wang, K. Ren , and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.
[6]. B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud", Proc. IEEE INFOCOM,pp. 2904- 2912, 2013.
[7]. A. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication Challenges", IEEE Comm. Magazine,vol. 50, no. 9, pp. 24-25, Sept. 2012.
[8]. X. Liu and X. Li, "Privacy Preserving Techniques for Location Based Services in Mobile Networks", 2012 IEEE 26th International Parallel And Distributed Processing Symposium Workshops & PhD Forum, Shanghaip, 2474-2477,2012.
[9]. K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring", IEEE Internet Computing, vol. 14, no. 5, pp. 14-22, Sept.-Oct. 2010.
[10]. Damiani, M.L., Bertino, E., Silvestri, c.," The PROBE Framework for the Personalized Cloaking of Private Locations", Transactions on Data Privacy, 123-148, August 2010.
[11]. Mascetti, S., Freni, D., Bettini, C., Wang, X.S., Jajodia, S.," Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies", The VLDB Journal 20, pp 541-566, December 2010.
[12]. P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing", Nat'l Inst. of Standards and Technology, 2009.
[13]. [13]. Poolsappasit, Nayot Ray, Indrakshi , "Towards Achieving Personalized Privacy for Location-Based Services", Transactions on data privacy, 2009.
[14]. Ardagna, C.A., Cremonini, M., Gianini, G.," Landscapeaware location-privacy protection in location-based services", Journal of Systems Architecture - Embedded Systems Design 55, 243-254, April 2009.
[15]. Ghinita, G., Kalnis et al.," Private queries in location based services: anonymizers are not necessary", In: Proceedings of the 2008 ACM SIGMOD international conference on Management of data, New York, NY, USA, ACM , 121-132, 2008.
[16]. T. Jiang, H.J. Wang, and Y.c. Hu," Preserving location privacy in wireless LANs", In Proceedings of the 5th International Conference on Mobile Systems, Applications and Services, pages 246--257, 2007.

R.Ranjith, et. al. "Location Based Services with Data Examination and Restoration." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 23(2), 2021, pp. 47-51.