International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 10 – NOVEMBER 2018.

Privacy Based Protection Mechanism for Location Data with an Accurate Service

K. Spatika[#1]

[#]*Vellore Institute of Technology, India*

***Abstract*— Location based service are suitable for the user based services. Due to some of the malicious attacks the leakage happens on the location privacy. For example the mobile user will report their location with their friends through the picture or by message in the social network by using the tagging; it will tag the friends in their list by their names. Nowadays the modeled algorithm used for these issues are obfuscated location to inquiry service, which are resulted in the imprecise output. In order to get the betterment of the result it must sacrifices the quality of service (QOS). The quality of service is resolved by using the Location Searching Service (LSS) and Location Based Service (LBS). This paper studies the current status of the location privacy issues in the social network application. And developed the four novel modules for the improvement of the privacy leakage of information, the modules are User, Admin, Attacker and Two way authentications. By using these modules the social network websites are not ignored from the protection of social aspects. Thus the experimental results shows, that the privacy risk are been controlled and the system is safe from the attacker. And also the different parameters are been studied in different scenarios.**

***Index Terms*— Social Network, Quality of Service, Location Searching Service, Location Based Service.**

I. INTRODUCTION

Association regarding industry and the business involves the remarkable potential use of the location privacy with the user experiences [1]. In traditional approaches the user used to share their data service and voice to the remote user, now in advantage the co location are been shared [2]. By doing this the cost will be higher in network. So many scholars have discussed about these issues so far but the result does not meet the requirement, and also it is difficult to trace the information in location privacy preservation because the privacy level is too low [3]. The user can get the information from anywhere at anytime which is used to search the distance at the desired location. There are many approaches that are been developed, namely location service, navigation services and tracking the location service [4]. So in order to protect the location data from the attackers there are many protection criteria are been designed [5].

The service provider are been provide with the co location detail; which are lacking in the accuracy level. The user will check the location based service, and then the friend finder and the games are based upon the location which swaps the vast amount of location data [6]. If this data is misused, it leads to the tracking of the user location and the privacy measure will be unauthorized. Authentication is to safeguard the information against the illegitimate user [7]. One of the rising trend, is the co-location with new user on social network that are used for friends to tag there pictures and upload the messages there post and make an interaction on chatting [8]. There are many co location are been used such as automatic face recognition on their pictures and Bluetooth is enabled to the device that are sniffed by the neighboring device as a report [9]. Attacker exploits the location and co-location information; which are very powerful method to unauthorized, so they deployed to improve the performance of the localization attack [10].

The rest of the paper are been organized into Section II is the discussion of the Literature Survey and Section III is designing modules for the Proposed System, Section IV is the Experimental result of the work system and followed by Section V is the Conclusion.

II. LITERATURE SURVEY

C. Vicente, et al, Presented a Geo-social networks (GeoSNs) provide context-aware services that help associate location with users and content. The proliferation of GeoSNs indicates that they're rapidly attracting users. GeoSNs currently offer different types of services, including photo sharing, friend tracking, and "check-ins." However, this ability to reveal users' locations causes new privacy threats, which in turn call for new privacy-protection methods. The authors study four privacy aspects central to these social networks - location, absence, co-location, and identity privacy - and describe possible means of protecting privacy in these circumstances.

A. Narayanan, et al, obtained operators for online social networks that increases sharing potentially sensitive information about users and their relationships with advertisers, application developers, and data-mining researchers. Privacy is typically protected by anonymization, i.e., removing names, addresses, etc. We present a framework for analyzing privacy and anonymity in social networks and develop a new re-identification algorithm targeting anonymzed social-network graphs. To demonstrate its effectiveness on real-world networks, we show that a third of the users who can be verified to have accounts on both Twitter, a popular micro blogging service, and Flickr, an online photo-sharing site, can be re-identified in the anonymous Twitter graph with only a 12% error rate. Our de-anonymization algorithm is based purely on the network topology, does not require creation of a large number of dummy "sybil" nodes, is robust to noise and all existing defenses, and works even when the overlap between the target network and the adversary's auxiliary information is

small.

G. Ghinita, et al, Discussed about the Mobile devices equipped with positioning capabilities (e.g., GPS) can ask location-dependent queries to Location Based Services (*LBS*). To protect privacy, the user location must not be disclosed. Existing solutions utilize a trusted anonymizer between the users and the LBS. This approach has several drawbacks: (*i*) All users must trust the third party anonymizer, which is a single point of attack. (*ii*) A large number of cooperating, trustworthy users is needed. (*iii*) Privacy is guaranteed only for a single snapshot of user locations; users are not protected against correlation attacks (e.g., history of user movement).We propose a novel framework to support private location-dependent queries, based on the theoretical work on Private Information Retrieval (*PIR*). Our framework does not require a trusted third party, since privacy is achieved via cryptographic techniques. Compared to existing work, our approach achieves stronger privacy for snapshots of user locations; moreover, it is the first to provide provable privacy guarantees against correlation attacks. We use our framework to implement approximate and exact algorithms for nearest-neighbor search. We optimize query execution by employing data mining techniques, which identify redundant computations. Contrary to common belief, the experimental results suggest that PIR approaches incur reasonable overhead and are applicable in practice.

K. P. Murphy, et al, presented recent, researchers who have demonstrated that "loopy belief propagation" -- the use of Pearl's poly tree algorithm in a Bayesian network with loops -- can perform well in the context of error-correcting codes. The most dramatic instance of this is the near Shannon-limit performance of "Turbo Codes" -- codes whose decoding algorithm is equivalent to loopy belief propagation in a chain-structured Bayesian network. In this paper we ask: is there something special about the error-correcting code context, or does loopy propagation work as an approximate inference scheme in a more general setting? We compare the marginals computed using loopy propagation to the exact ones in four Bayesian network architectures, including two real-world networks: ALARM and QMR. We find that the loopy beliefs often converge and when they do, they give a good approximation to the correct marginals. However, on the QMR network, the loopy beliefs oscillated and had no obvious relationship to the correct posteriors. We present some initial investigations into the cause of these oscillations, and show that some simple methods of preventing them lead to the wrong results.

P. Ilia, et al, obtained the capabilities of modern devices, coupled with the almost ubiquitous availability of Internet connectivity, have resulted in photos being shared online at an unprecedented scale. This is further amplified by the popularity of social networks and the immediacy they offer in content sharing. Existing access control mechanisms are too coarse-grained to handle cases of conflicting interests between the users associated with a photo; stories of embarrassing or inappropriate photos being widely accessible have become quite common. In this paper, we propose to rethink access control when applied to photos, in a way that allows us to effectively prevent unwanted individuals from recognizing users in a photo. The core concept behind our approach is to change the granularity of access control from the level of the photo to that of a user's personally identifiable information (PII).We implement a proof-of-concept application for Facebook, and demonstrate that the performance overhead of our approach is minimal. We also conduct a user study to evaluate the privacy offered by our approach, and find that it effectively prevents users from identifying their contacts in 87.35% of the restricted photos. Finally, our study reveals the misconceptions about the privacy offered by existing mechanisms, and demonstrates that users are positive towards the adoption of an intuitive, straightforward access control mechanism that allows them to manage the visibility of their face in published photos.

III. PROPOSED SYSTEM

The proposed system composed of four modules, which are used for the security purposes for co location information in location data. The first module is the Users module; initially user must have to register their detail on the cloud server. The registration phase consider of the username and the password validation it must consist of the numerical and the character. After successful registration user can search their friends and the user can able to view the recommended friends in the recommended friend section. User can send friend request to known users and response the request in notification module. User can post a status update and that will appear on newsfeeds section. When the users post a status their geo location will add on the status. Others users comment on the post update by a user. The second phase is the Admin module; he/she can view all the user's details in the database. He/she can view all the status posted by the users and posted location attached on that. Only the authorized person can only see the admin updates if the particular he/she is one of the legitimate user means there can see the update of the admin. Cloud server will able to see the graphical analyze of user details. The primary responsibilities of a cloud server are to configure the Cloud Management service, and to monitor and manage the services. The primary responsibilities of a cloud server are to configure the Cloud Management service, and to monitor and manage the services.

The third module; is the Attacker module, Attacker are been attacked in the login section and find the details of the user. Attacker can view the user's path and last location visited. And the user information are also be modified; and it results on, the user details leakage and they are been misused by the illegitimate user. By tracing the path of the user visited in geographical area thus the communication are unintentionally leaked using their IP address by obtaining where there are, and with whom there are with. Today most of the services still use simple username and password type of knowledge-based authentication, but some exception are financial institutions which are using various forms of secondary authentication (such as shared secret questions, site keys, virtual keyboards, etc.) that make it more difficult

for popular phishing attacks. Some of the authentication attacks are listed as follows:

1) Brute Force Attacks: In this type of attack, all possible combinations of password apply to break the password. The brute force attack is generally applied to crack the encrypted passwords where the passwords are saved in the form of encrypted text.
2) Dictionary Attack: This type of Attack is relatively faster than brute force attack. Unlike checking all possibilities using brute force attack, the dictionary attack tries to match the password with most occurring words or words of daily life usage.
3) Shoulder Surfing: Shoulder Surfing is an alternative name of "spying" in which the attacker spies the user's movements to get his/her password. In this type of attack the attacker observes the user; how he enters the password i.e. what keys of keyboard the user has pressed
4) Replay Attacks: The replay attacks are also known as the reflection attacks. It is a way to attack challenge response user authentication mechanism.
5) Phishing Attacks: It is a web based attack in which the attacker redirects the user to the fake website to get passwords/ Pin Codes of the user.
6) Key Loggers: The key loggers are the software programs which monitors the user activities by recording each and every key pressed by the user.

The final module is the two step verification here, there are two way of authentication is used to safeguard from the attackers there are password or pin verification and other one is the One-time Password verification. Password and PIN based authentication Mostly knowledge-based authentication process is accessed by using password or Personal Identification Number (PIN) and it is compulsory to deliver knowledge of a secret for authentication process. SMS based authentication. It acts as a delivery channel for a one-time password (OTP) produced by an information system. Two types of one-time passwords are available such as a challenge-response password which returns with a challenge value once a user identifier is received. Password list includes list of sequentially used passwords used by a person to contact a system. A password is received by user in email id and process of authentication is completed if the password is entered. This is applied in banking system for authentication process. By using this type of authentication the system are secure and no leakage of the co-location information happens.

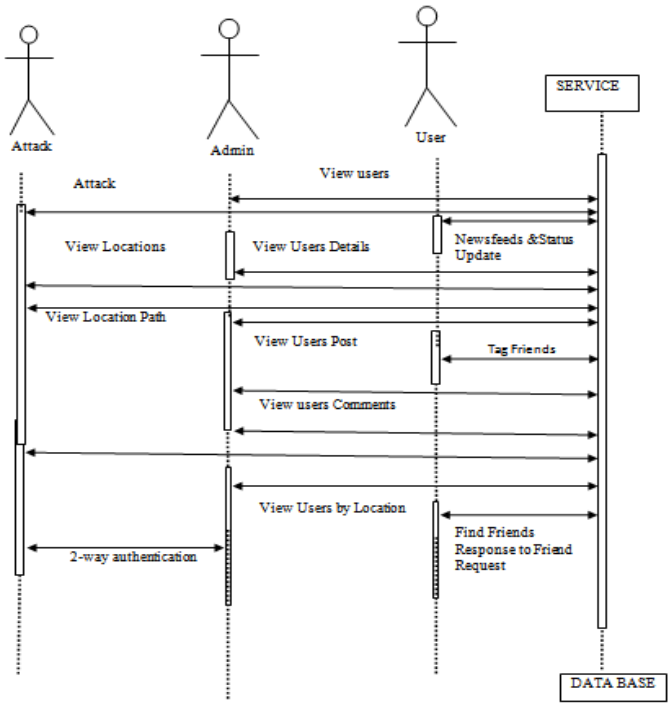


Fig.1. Proposed Architecture

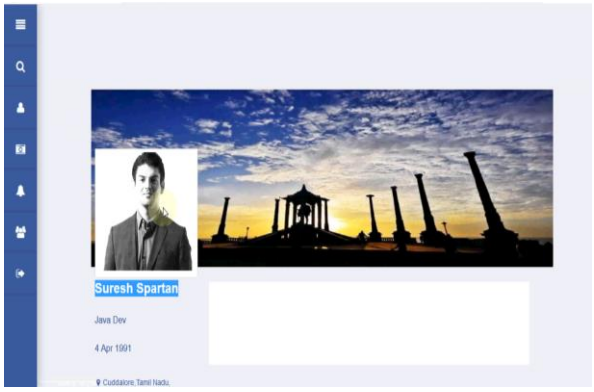
IV. EXPERIMENTAL RESULT

The implementation of this co-location information considers with only a single friend of the targeted user. A paramount finding of our work is that users partially lose control over their location privacy as co-locations and individual location information disclosed by other users substantially affect their own location privacy. Our experimental results also show that a simple countermeasure (i.e., coordinated location disclosure) can reduce the privacy loss. The experimental results have been shown as below

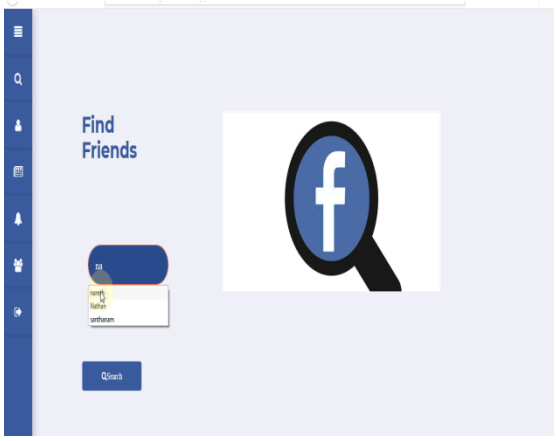
STEP 1: User login phase with the username and the password, the password must be numerical and also character. Here the privacy of the single user is been maintained.

STEP 2: In this step the registered user are interacting with their friends, by tagging their names, messages and also sharing the information with each other.

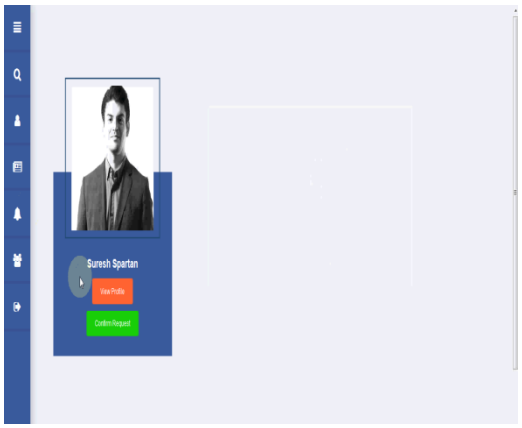
STEP 3: In this image the second module, Admin are responsible for the user details which are been registered in the time of registration. Here the Suresh Spartan is signing this profile and his location is seems that he is in Pondicherry.



STEP 4: In this step the single he/she will find the friends and share their location

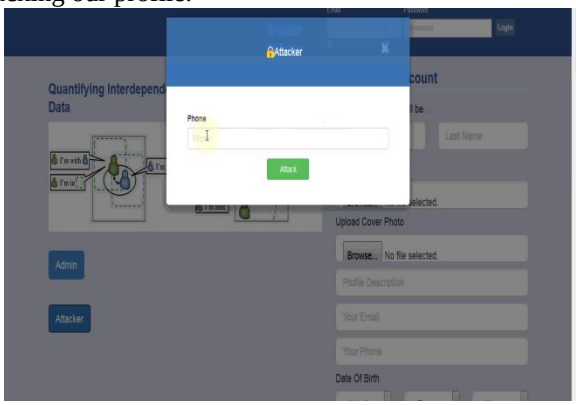


STEP 5: This is the Third module where the attacker will view he/she profile and trace the location and modify their information where the information leakage will happens.

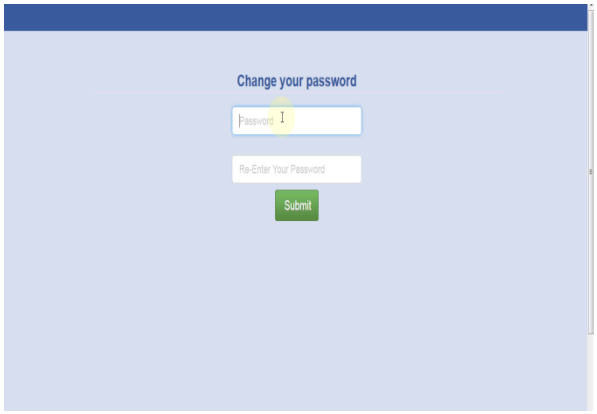


STEP 6: In this step the user status and the location are been traced/viewed.

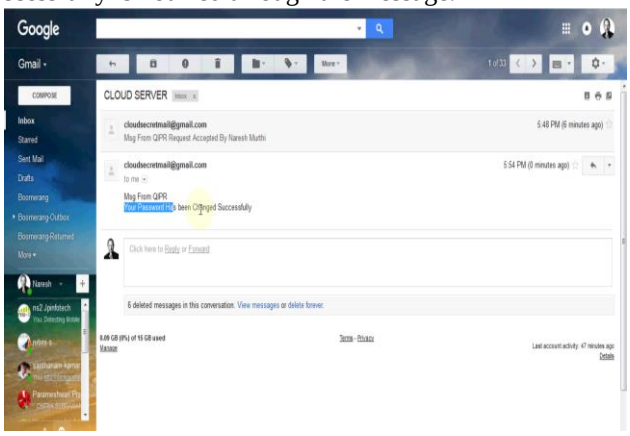
STEP 7: When the attacker attacks and login using your phone number the alert will been shown that someone is tracking our profile.



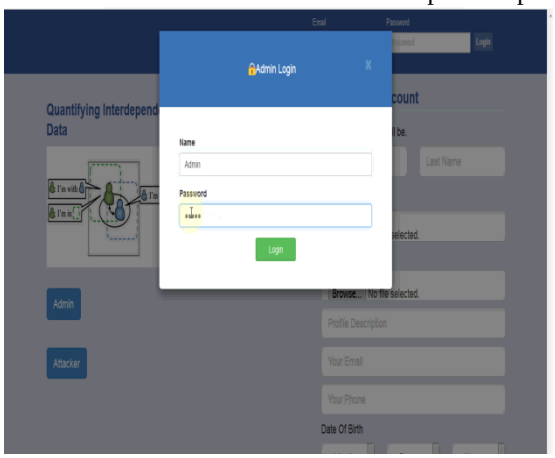
STEP 8: The OTP are been generated and the change of password is required for the recovery of the system.



STEP 9: In this step the change of password is done successfully is notified through the message.



STEP 10: Then to verify that our profile is secured sign in to the admin with the username with the upadated password.



V. CONCLUSION

In this paper, the study is about the co-location identification of the friends who are tagged with their friends list to share their location and messages. And in the existing work there are facing some issues regarding the attacker, who can easily attackers the information of he/she. Here, the designed modules are used to secure the particulars information in two way authentication. In this two way authentication, the attacker login into the admin by using the user he/she phone number. When the phone is been submitted the OTP are generated to the registered email id which is used during the time of registration phase. Then the user aware that the some attackers are accessing our profile then he/she changes the password and it is indicated by the message through the mail. Thus the experimental results show that the constructed modules are efficient against the attackers. Thus the co-location or the information is not leaked and the profile of the user tagging with their friends is secured.

REFERENCES

[1] Zaigham Mahmood, et al, "Data Location and Security Issues in Cloud Computing", International Conference on Emerging Intelligent Data and Web Technologies, 2011.
[2] A. S. Anakath,et al," Privacy preserving multi factor authentication using trust management", Springer, 2017.
[3] Sahana Shivaprasad, et al," Privacy Preservation in Location Based Services", Science Direct 11(5), 2016.
[4] Tao Peng, et al," Multidimensional privacy preservation in location-based services", Science Direct , 93, Pp. 312-326, 2017.
[5] Shaobo Zhang, et al,' Enhancing privacy through uniform grid and caching in location-based services", Science Direct, 86, Pp.881-892, 2018.
[6] Yan Huang, et al," Search locations safely and accurately: A location privacy protection algorithm with accurate service", Science Direct, 103(1), 2018.
[7] Robyn L. Raschke,et al," Understanding the Components of Information Privacy Threats for Location-Based Services", Journal of Information Systems, 28(1), Pp. 227–242, 2015.
[8] Shuo Wang ,et al, "Privacy-protected place of activity mining on big location data", IEEE International Conference on Big Data (Big Data), Pp. 1101 – 1108,2017.
[9] Maria Luisa Damiani, et al," Privacy Challenges in Third-Party Location Service", IEEE 14th International Conference on Mobile Data Management, Pp. 63 – 66, 2013.
[10] Shuo Wang, et al, "Protecting the location privacy of mobile social media users", IEEE International Conference on Big Data (Big Data), Pp. 1143 – 1150, 2016.
[11] Carmen Ruiz Vicente,et al," Location-Related Privacy in Geo-Social Networks", IEEE Internet Computing,15(3),Pp.20-27,2011.
[12] Arvind Narayanan, et al," De-anonymizing Social Networks", IEEE Symposium on Security and Privacy, Pp. 173 – 187,2009.
[13] Gabriel Ghinita et al," Private Queries in Location Based Services: Anonymizers are not Necessary", International Conference on Management of data,2008.
[14] Kevin Murphy, et al," Loopy Belief Propagation for Approximate Inference: An Empirical Study ", Artificial Intelligence, 2013.
[15] Panagiotis Ilia, et al," Face/Off: Preventing Privacy Leakage From Photos in Social Networks", ACM, 2015.