Therefore, adopting both the location k-anonymity and cloaking granularity as privacy metrics, they have proposed a new incremental clique-based cloaking algorithm, called I Clique Cloak, to defend against location-dependent attacks [10]. The main idea is to incrementally maintain maximal cliques needed for location cloaking in an undirected graph that takes into consideration the effect of continuous location updates. Thus, a qualified clique can be quickly identified and used to generate the cloaked region when a new request arrives. The efficiency and effectiveness of the proposed I Clique Cloak algorithm are validated by a series of carefully designed experiments.

The results of implemented system have shown that the price paid for defending against location-dependent attacks is small.

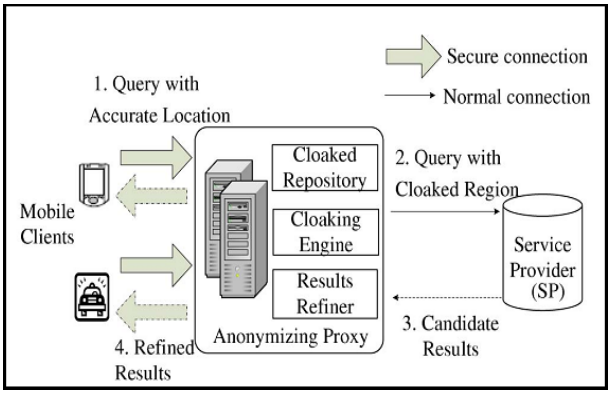

Figure 5: System architecture for clocking region [13]

Algorithm 1: ICliqueCloak Algorithm
Input: A set of requests awaiting for anonymization, a new query requestu.
Output: A set of cloaked requests.

Step 1: Incrementally update the max-clique set for the new request u.
Step 2: Find the cloaking set CS_{ti} satisfying location k anonymity from the max-clique set.
Step 3: Generate the cloaked region for CS_{ti}.
Step 4: Update the max-clique set upon request Cloaking or expiration.

8. Comparison

Table 1: Comparison between different approaches

No	*Approach*	*Advantages*	*Disadvantages*
1	Location obfuscation	Allow users to express their privacy preferences	Degraded quality of service to user
2	APPLAUS	Provides location proofs effectively also preserves the source privacy	Computation time is costly and colliding attacks detection ratio is low
3	LocaWard	Resilient to various attacks such as multi token request attack	Do not provide security to general LBS
4	Oblivious Transfer and PIR	Computationally and also in communication more efficient	The overhead of the primality test is larger
5	IClique Cloak	Effectively prevent location-dependent attacks when locations are updated	The cost for location dependent attacks is small

9. Conclusion

A detailed survey of Privacy approaches for Location based services in particular is done giving their major advantages and limitations. Also inclusive study of each approach individually is completed. The study gives a baseline for additional research in privacy of user's personal location data and a user can decide the impact of location inaccuracy on the service accuracy before giving away his actual location.

References

[1] Matt Duckham and Lars Kulik, A Formal Model of Obfuscation and Negotiation for Location Privacy, Germany: Springer-Verlag, 2001.
[2] Ming Li, Sergio Salinas and Pan Li, LocaWard: A Security and Privacy Aware Location-Based Rewarding System, IEEE Transaction On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014

[3] Zhichao Zhu and Guohong Cao, "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System," IEEE Transaction On Mobile Computing, Vol. 12, No. 1, January 2013.
[4] Russell Paulet, Md. GolamKaosar, Xun Yi, and Elisa Bertino, "Privacy-Preserving and Content-Protecting Location Based Queries," IEEE transaction on knowledge and data engineering.
[5] Reza Shokri, George Theodorakopoulos, PanosPapadimitratos, Ehsan Kazemi, and Jean-Pierre Hubaux, "Hiding in the Mobile Crowd: Location Privacy through Collaboration," IEEE transaction on Dependable And Secure Computing, Vol. 11, No. 3, May-June 2014.
[6] Zhichao Zhu and Guohong Cao, "APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-based Services", IEEE INFOCOM 2011.
[7] Hui Zang and Jean Bolot, "Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study", MobiCom'11, September 19–23, 2011, Las Vegas, Nevada, USA.
[8] Rinku Dewri, Member and Ramakrisha Thurimella," Exploiting Service Similarity for Privacy in Location-Based Search Queries", IEEE Transaction on Parallel and Distributed Systems, Vol. 25, No. 2, February 2014.
[9] Hidetoshi Kido, Yutaka Yanagisawa and Tetsuji Satoh, "An Anonymous Communication Technique using Dummies for Location-based Services".
[10] Xion Pan, Jianliang Xu and XiafengMeng,"Protecting Location Privacy against Location-Dependent Attacks in Mobile Services", IEEE transaction on Knowledge and data engineering, Vol. 24, No. 8, August 2012.
[11] M.L. Yiu, C.S. Jensen, X. Huang and H. Lu, "Space Twits: Managing the Trade-offs Among Location Privacy, Query Performance and Query Accuracy in Mobile Services", Proc., 24th Int'l Conf. Data Eng., pp. 366-375,2008.
[12] M. Gruteser and D. Grunwald, "Anonymous Usage of Location Based Services through Spatial and Temporal Cloaking,"Proc. First Int'l Conf. Mobile Systems, Applications and Services, pp. 31-42, 2003.
[13] B. Gedik and L. Liu, "Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms," IEEE Trans.Mobile Computing,vol. 7, no. 1, pp. 1-18, Jan. 2008.

Author Profile

Sneha Sonwane received the B.E. degree in Computer Engineering from Bharati Vidyapeeth College of Engineering for Women, Dhankawdi, Katraj, Pune in 2012. And she is now pursuing her M.E. degree from D.Y. Patil College of Engineering, Akurdi, Pune.