any information of the user's location to the attacker. Using symmetric keys the user can transform all their locations and data shared with the server. Thus, defending the data stored on the server against attacker. The indices stored on the index server are encrypted. Hence only the user having the decryption keys can decrypt the indices. Hence the attacker cannot link transformed locations with data stored in data server. In [1] they see that in future information about our surrounding will be through social recommendation; therefore it will provide a pivotal role as a primary source of information.

The architecture in [1], describes the fact that location coordinate are sent to the server in plain text. This hampers the user's location privacy. So they proposed *coordinate transformation* which handles the privacy issue. Every user chooses some secrets which they reveal to their friends through their physical meetings or through other secure channel. The secret contains a symmetric key, a rotation angle and a shift. Users when sharing the location coordinates with the server use the secret angle and shift to transform all their location coordinates. Users encrypt all the location data they share with the server using the symmetric key. As these secrets are only known to the friends, therefore only they can encrypt and decrypt the data as depicted below in Fig 1. The paper [1] illustrates the design and implementation of *LocX* to create a system for building Location Based Applications (LBAs) ensuring user location privacy.

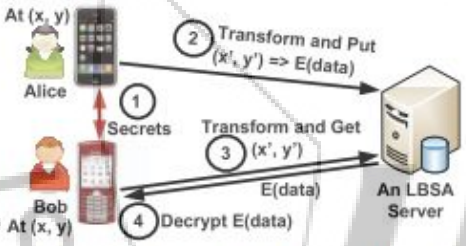

Fig. 1. A basic design. In this design, (1) Alice and Bob exchange their secrets, (2) Alice stores her review of the restaurant (at (x, y)) on the server under transformed coordinates, (3) Bob later visits the restaurant and queries for the reviews on transformed coordinates, and (4) decrypts the reviews obtained.

Zhichao Zhu and Guohong Cao [2], put forward an architecture called *A Privacy-Preserving LocAtion proof Updating System (APPLAUS)*. The bluetooth enabled mobile devices colocated at a location generate location proofs for updating the location proof server. The architecture contains following entities: Location Proof Server, Prover, Witness, Certificate Authority and Verifier. The mobile devices use the randomly changed pseudonyms to protect the source location privacy from each other. The locations proofs can be queried to the server by an authorized verifier. The location proof requests are broadcasts by the Prover node using Bluetooth. The Witness node is the node which provides the location proof to the Prover. The locations proofs send by the Prover node are stored as pseudonyms on the location proof server. The Certificate Authority generates the public/private keys and works as a bridge between the location proof server and the verifier. It does the mapping between the real entities and the pseudonyms. The Verifier can be a user or an application which verifies the Prover's location within a given time limit as shown in Fig. 2. In paper [2] the most important facet is users can dynamically change their location privacy preferences in real time and can also check whether and when to accept a query related to location proof.

Figure 2: Location proof updating architecture and message flow

Sebastein Gambs, Marc-Olivier Killijian, Matthieu Roy and Moussa Traore [3], defined *Location Based Services (LBS)* as a service whose input is the current location of a user (found through the GPS of his mobile device) and whose output depend on the given input i.e. the current acquired location of the user. They proposed *locanym*, which is a pseudonym linked to a particular location and can be used for creating privacy preserving LBS. This locanym can be used for privacy-preserving location based services. They proposed the framework for solving the Secure Positioning Verification problem by a technique which contains two entities the Prover (the User) and the group of Verifiers. The Prover proves his location position by interacting with the group of verifiers. For this it uses the *Distance-bounding Protocol (DBP)* and the *Received Signal Strength Indicator* (RSSI).

The architecture in [3] of *Distance-bounding Protocol (DBP)* contains a verifier which sends a challenge to the prover and starts its timer. After receiving the challenge, the prover does a set of computations which creates a response to the given challenge, which is then sent to the verifier, who stops the timer when the response is received by it. Then the elapsed time is multiplied with the propagation speed of signal (e.g. ultrasound, electromagnetic signals) using which the verifier produces an upper bound on his distance with the prover. Also an authentication mechanism layer can be created upon DBP using which the prover can be authenticated by the verifier using a secret which is shared between them.

The *Received Signal Strength Indicator (RSSI)* mechanism in [3] deals with the following two observations. The signal strength of RF decreases 1) when the transmitter and receiver are far apart from each other and 2) Due to obstacles between them. Using these observations, different reading of the signal strength are measured at different locations of the given location site and are stored in the database. Upon receiving a location query from the user, the system compares the values of the user's current signal strength with that of the stored values in the database. Hence, the system can accurately find the location of the user and can sent it.

Thus using the above two mechanism (*DBP and RSSI*) the authors in [3] ensure unlikability, accountability and sovereignty with privacy for creating *Location Based Services (LBS)*.

Bogdan Carbunar, Mahmudur Rahman, Jamie Ballesteros, Naphtali Rishe [4], introduced the *Location Centric Profile (LCP)* aggregates which are created using the user profiles present at a given location. The GSN hosts a system with a client application wherein both the users and the venue owners or businesses (restaurants, yoga classes, cafeteria etc) register themselves with unique user id. The system stores information of both the registered venues and the registered subscribers with an associated geographic location. When a user visits a registered venue, they are encouraged to write their reviews about the venue, specify their location which is done by check-in at the specified venue. There is a new paradigm of business between the GSN providers and the venue owners which provide targeted advertisement to the users when they visit a specified venue or location. Profitability is based upon the collection of more user profiles. User profiles are created based upon the information provided by the user. Therefore more detailed the user profile, more the targeted advertisement and better business. But this personal information collected from the user's movement or travel is at a risk and can be leaked to third party. So user information privacy becomes jeopardy. Hence there is urgent need for addressing the security concerns related to user data i.e. user profiles. In [4] concept of *Location Centric Profiles (LCPs)* was put forward. These are created using two methods: 1) based upon the users visit to a certain location or 2) through a collection of co-located users.

The proposed framework creates profiles of users who are present at a venue while maintaining privacy with ability to prove correctness whether the said user or users are actually present at the specified venue. Correctness can be proved in two ways: 1) *Location Correctness* and 2) *LCP Correctness*. Using Location Correctness, users who are present at a specified venue can only add the LCPs. LCP Correctness provided a predefined way for users to update their LCPs. The proposed framework in [4] creates and stores venue centric profiles. For this, the venue owners who participate in this venture install an affordable device like any Android smartphone, Raspberry PI or a Beagleboard at the venue location which does the functions of activities related to LCPs and also checks the participating user's physical presence at the specified venue. [4] Introduced the concept of *snapshot LCPs*. The snapshot LCPs are created using user devices by using the profiles of co-located users. The user devices communicate with each other using wireless adhoc network. These snapshot LCPs are not attached to venues, the user devices create LCPs of neighbors at the given location of interest. It uses Benaloh's homomorphic cryptosystem and zero knowledge proofs for computing correct LCP.

The architecture for creating snapshot LCPs in [4] is shown in the Fig. 3. The algorithm is deduced in the following way. Let *K* denote the level of privacy which needs to be provided to the user at any location. We define a private LCP solution to be a set of functions. P P(*k*) = {*Setup, Spotter, CheckIn, PubStats*}. At each venue *Setup* is run to collect statistics about user's check-ins. User runs *Spotter* so as to prove his physical presence at the venue. If *Spotter* generates error then verification is failed otherwise user verification is proved. Between the user and the venue *Check-In* is run, only after Spotter is successful, so that user's profile information can be collected. PubStats publishes the collected user's profiles.

During a check-in by a user *U* at venue *V*, the Spoter protocol with *SPOTRv* is executed. During this the Venue *V* verifies *U*'s physical presence using a challenge/response protocol between *SPOTRv* and the user device. Is successful the Spoter sends a secret key created by the Benaloh cryptosystem to *U*.

Figure 3: System Architecture.

During each venue visit by user *U*, his profile is updated with the set *Sh* of shares of secret key send to him so far. User *U* executes *CheckIn* in conjunction with *SPOTRv* and sends his secret key and receives the encrypted counter sets. During *CheckIn*, user *U* increments the counter according to his range and re-encrypts all the counters and gives the resulting set to *SPOTRv*. Now *U* and *SPOTRv* execute the zero knowledge protocol to verify that exactly one counter has been incremented by user *U*. The latest encrypted counter set sent by user *U* is stored by *SPOTRv*. Now all the *K* users complete their *CheckIn* procedure, *SPOTRv* executes *PubStats* to generate private key to decrypt all the encrypted counters and publish the tally.

B. Krishnamurthy and C. E. Wills and Craig E. Wills [5], study clearly shows that there is no awareness about privacy between the users of online social networking sites regarding their social information data stored in the OSNs. In their study consistently demonstrate leak age of user identifier information to one or more third-parties via Request- URIs, Referrer headers and cookies. The users are outraged because they cannot delete their data regarding social information about their friends and family members from these sites. The results in [5] show that a user cannot access his friend's private content stored on OSN. It can be accessed by two methods. 1) A user should register with all the other OSN sites with whom their friends use. 2) Until he receives secret URLs using which he can view the content, he has to wait. Thus both these methods raise the alarm of security issues. Firstly, there is need for duplicating the user's social data due to multiple registrations which he has

to perform. Finally, the secret URLs which users sent through emails expose the risk to privacy.

R. Dingledine, N. Mathewson and P. F. Syverson [6] shows Tor's emphasis on deploy ability and design simplicity has led us to adopt a clique topology, semi centralized directories, and a full-network-visibility model for client knowledge. These properties will not scale past a few hundred servers. The results in [6] show that Tor omits cover traffic - its costs in performance and bandwidth are clear but its security benefits are not well understood.

A user's social networking information is provided least amount of privacy by the current online social networking sites [7]. Security to a user's information stored by these sites should be paramount. In [7] Amin Tootoonchian, Stefan Saroiu, Yashar Ganjali and Alec Wolman proposed system architecture for designing *Lockr* which ensure privacy to both centralized and decentralized online content sharing system. It can be done in following three steps. Firstly, there is a clear separation between the services the OSNs provide and the social networking content. This helps the user to decide or control which OSN can store their social information, which third party can be given access to it and most important they can manage it by themselves. Here user is given the total control of his social information. Secondly, the proposed system Lockr provides access to the social data only through digitally signed social relationships and this data can't be reused by OSN for any other purpose. Finally, using a social relationship key the messages are encrypted. The relationship between two strangers is verified by a common friend using this key. The result in [7] clearly shows the advantages of *Lockr* for simplifying the sharing of content on the Internet through decoupling of management of social information from the clutches of online social networks and letting the user control or decide which OSN to allow storage of their social information.

Using [8] Jaime Ballesteros, Bogdan Carbunar, Mahmudur Rahman, Naphtali Rishe and S.S. Iyengar proposed a novel framework that defined public safety. Their investigation use datasets that are a combination of space and time index, which provide personalized safety recommendations to social network and mobile users through the use of mobile and OSN technologies. The reviews of geographic locations given by the users of OSN sites like Yelp and the crime index of the location (venue) are used. *Mobile traces* using mobiles and geosocial networks of users are stored which help to provide the users with personalized safety recommendation about a geographic location. In [8] they put forward a distribution algorithm named isafe that answers the privacy alarms ringing due to the use of crime and safety index values and user's collected trajectory traces.

Their architectural framework consists of three components i.e. a) geosocial networks, b) service provider and c) mobile device user. The geosocial networks like Foursquare, Yelp contains collection of ratings about a given venue or geographic location given by its registered users. The service provider collects census about crime related to venue are can be collected using a request. The users have mobile devices which provide facilities like GPS for finding geographic location about a user and an adhoc wireless network providing internet connectivity, using which the users get safety recommendations about a venue or location through a mobile application client installed in their mobile device. The architecture in [8] is efficient in terms of communication overheads and computation.

In [9] it is observed by Dario Freni, Carmen Ruiz Vicente, Sergio Mascetti, Claudio Bettini and Christian S. Jensen is there is increased proliferation of geo-tagging content using geo-spatial and temporal coordinates by users leading to the advent of geo-aware social networks (GeoSNs) which increase privacy concerns. This tagged content (ex. a photos taken at a location or region) which is accessible to numerous users and cannot be controlled by the user who uploaded it to GeoSNs. *Location privacy* and *Absence privacy* are the two privacy challenges that affect the GeoSNs. Location privacy deals with the issues concerned to the information of *presence* of a user at a given location at a specified time. Absence privacy deals with the issues related to the information of *absence* of a user at a given location at a specified time. Hence a lot of sensitive information regarding the presence or absence of a user at a location exposes them to privacy vulnerability threats that may lead to assault or stalking is observed in [9].

The algorithm analyses the changing constraints on inter dependency between resources; combine together meta-data generalization with spatio-granularities and constraints related to the user's speed of movement. By publishing resources at appropriate temporal delay absence privacy is achieved. User privacy preferences are taken into account while publishing information related to the user. The paper [9] is the first to address the security threats related to location privacy and absence privacy and providing a solution for defining the privacy preferences according to the user's wish.

The Online Social Network (OSN) services like Facebook, MySpace and LinkedIn etc provide a centralized architecture for storing a user's online social information. In [10] it has been observed that this centralized architecture is not suitable for providing security to the user's social data as it is prone to network attacks as well as user's information can be sold to third parties. Leucio Antonio, Cutillo Refik Molva and Thorsten Strufe in [10] proposed a new decentralized mechanism called *Safebook*. The two important pillars in the design architecture of *Safebook* are: 1) instead of having a centralized storage provider, the architecture uses peer-to-peer system thus there is no centralized entity control over the users data and 2) provides trust management and privacy for communication of user with OSN services.

The architecture of Safebook provides following facilities like: a) *Privacy* which guarantees anonymous, untraceable and unlikable user communication and secured protect to user information, b) *End-to-end Confidentiality* measures are brought to force that resists eavesdropping and man in middle attacks and c) *Authentication* by providing appropriate access control to user profiles and data. The architectural benefits of [10] clearly indicate the advantages of using a decentralized system for hosting the user's online social information through the use of peer-to-peer substrate.

The vulnerabilities found in the existing centralized OSN architecture are nullified through the use of decentralized approach.

3. Conclusion

In this way we have studied the existing approaches for preserving privacy in geosocial network. The coordinate transformation technique is simple but involves revealing the secrets to the friends which adds another privacy concerns. The locanym approach is very complex and computation intensive due to the calculation of RF signal strength at different location points in a given geographic site. The novel approach of *Location Centric Profiles (LCPs)* construction using the profiles of users check-in at venues is the best mechanism for providing strong user location privacy and correctness assurances. Its decentralized solution with venue centric approach computes real time LCP snapshots.

References

[1] "Preserving Location Privacy in Geosocial Applications", by Krishna P.N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, Amr El Abbadi, Christopher Kruegel and Ben Y. Zhao.
[2] "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System", by Zhichao Zhu and Guohong Cao.
[3] "Locanyms: Towards Privacy-Preserving Location-Based Services", by Sebastien Gambs, Marc-Olivier Killijian, Matthieu Roy, Moussa Traore.
[4] "Eat the Cake and Have It Too: Privacy Preserving Location Aggregates in Geosocial Networks", by Bogdan Carbunar, Mahmudur Rahman, Jaime Ballesteros and Naphtali Rishe.
[5] "On the leakage of personally identifiable information via online social networks", By B. Krishnamurthy and C. E. Wills and Craig E. Wills Worcester Polytechnic Institute Worcester, MA USA.
[6] "Tor: The second generation onion router" by R. Dingledine, N. Mathewson, and P. F. Syverson, in *Proc. USENIX Security Symp.*, 2004.
[7] A. Tootoonchian, S. Saroiu, Y. Ganjali, and A. Wolman, "Lockr: Better privacy for social networks," in *Proc. ACM CoNEXT*, 2009, pp. 1-12.
[8] J. Ballesteros, B. Carbunar, M. Rahman, N. Rishe, and S. S. Iyengar, "Towards safe cities: A mobile and social networking approach," *IEEE Trans. Parallel Distrib. Syst.*, vol. 3, no. 6, pp. 1-14, Nov. 2013.
[9] D. Freni, C. Ruiz Vicente, S. Mascetti, C. Bettini, and C. S. Jensen, "Preserving location and absence privacy in geo-social networks," in *Proc. 19th ACM CIKM*, New York, NY, USA, 2010, pp. 309-318.
[10] A. Cutillo, R. Molva, and T. Strufe, "Safebook: Feasibility of transitive cooperation for privacy on a decentralized social network," in *Proc. IEEE* WOWMOM, Jun. 2009, pp. 1-6.
[11] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SLAM J. Comput.*, vol. 18, no. 1, pp. 186-208, 1989.
[12] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, and S. Barocas, "Adnostic: Privacy preserving targeted advertising," in *Proc. Network Distrib. Syst. Security (NDSS) Symp.*, 2010, pp. 1-3.
[13] S. Mascetti, D. Freni, C. Bettini, X. Sean Wang, and S. Jajodia, "Privacy in geo-social networks: Proximity notification with untrusted service providers and curious buddies," *VLDB J.*, vol. 20, no. 4, pp. 541-566, Aug. 2011.
[14] K. P. N. Puttaswamy and B. Y. Zhao, "Preserving privacy in location - based mobile social applications," in *Proc. 11th Workshop Mobile Comput. Syst. Appl.*, New York, NY, USA, 2010, pp. 1-6.
[15] M. Wernke, F. Durr, and K. Rothermel, "PShare: Position sharing for location privacy based on multi-secret sharing," in *Proc. PerCom*, 2012, pp. 153-161.

Author Profile

Miss. Kiran Suresh Nagale, Research Scholar, G. H. Raisoni Collage of Engineering and Management Ahmednagar, University of Pune, India. She received B.E. in Information Technology from Pravara Rural Engineering College, Loni.

Prof. Amruta Amune received the B.E. and ME degrees in Computer Science and Engineering. Currently she is working as Assistant Professor at Computer Engineering Department in G. H. Raisoni Collage of Engineering and Management, Ahmednagar, India.