ISSN:2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

An Optimal Framework for Preserving Location Privacy in Geosocial Networks

[1]Ramya J, [2]S.subbiah, [3]Hemalatha J

[1]Communication and Networking, [2]Computer science and engineering, [3]electronics and communication engineering,
[1,2]Trichy Engineering College, Trichy, India
[3]k.ramakrishnan College of Technology, Trichy,India

Abstract - Analysing the conflict of privacy in geo social networks, steps are taken towards addressing the conflict. A novel approach is proposed to define the location and user based safety metrics. Secret Key cryptography is used for private information retrieval that allows a user to retrieve information. The approach is based on the construction of the framework which relies on the concept of LCPs, the profiles which are built from the profiles of users that have visited a certain location and DCPs a set of co-located users. The key insight is to apply secure user-specific, distance-preserving coordinate transformations to all location data shared with the server. An Encryption technique, AES is further applied to enhance the security such that a technique which the users are allowed to communicate from a database server without revealing what is actually being retrieved from the server. This allows all location queries to be evaluated correctly by the server, but our privacy mechanisms guarantee that servers are unable to infer the actual location data from the transformed data

Keywords: geosocial networks, security, privacy, secure computing, location based service

I. Introduction

Geo-Social Networking is networking dealing with geographic locations. These are social networks that require sharing a specific location in order to better communicate with others. Using geosocial network applications, others can know the whereabouts through various mobile and online resources. Geo-aware social networks (GeoSNs) are enabled by the availability of social network services, mobile devices with Internet connectivity, and geo-location capabilities Geosocial networking allows users to interact relative to their current locations. A variety of services exists and can be envisioned that exploit GeoSN resources. Privacy in social network services has become a hot topic, and reports indicate that users are leaving social network services due to privacy concerns. Social network users voluntarily reveal a wealth of personal data, including age, gender, contact information, preferences and status updates. In GeoSNs, it is possible for exact locations of users to be exposed to untrusted entities that may in turn utilize these to infer sensitive information about the users. For example, the presence of a user in certain locations, e.g., a hospital or a night club, may reveal sensitive information about the user. Privacy risks are the management headaches users face when interacting with their Online Social Networks (OSNs)[2].Profit is the main participation incentive for social network providers. It relies on user profiles, built from a wealth of voluntarily revealed personal information [1], exposes users to a variety of Privacy vulnerabilities. There exists a conflict between the needs of users and those of providers and participating businesses. Without privacy people may be reluctant to use geosocial networks.

In this paper, steps towards breaking this deadlock is taken, by introducing the concept of cryptographic techniques [3] over the location centric profiles (LCPs) and Decentralized profiles[1].

Contributions. Bodgan[1] et.al has proposed a framework named PROFILR. It has been analyzed and then the construction of Location centric profiles are created by means of the profiles of the user visited in that particular location. Decentralized profiles are created based on the profiles of the co-located users[12].

A framework is proposed by the following steps

First, secret key cryptography is applied on venue centric PROFILR is proposed, that relieves the GSN provider from a costly involvement in venue specific activities. To achieve this, PROFILR stores and builds LCPs at venues.

Second, for the secured information sharing a completely decentralized PROFILR extension is proposed built around the notion of snapshot LCPs. The distributed PROFILR enables user devices to aggregate the profiles of co-located users. Furthermore, an encryption technique-AES is applied over the location data thereby providing user side security such that the server is unable to infer the actual data from the transformed data.

II. LITERATURE SURVEY

Bodgan[1] et al. has proposed a framework named PROFILR for the construction of location centric profiles which are built over the profiles of the user who visited the discrete locations. First, a venue centric PROFILR to relieve the GSN provider from a costly involvement in venue specific activities, PROFILR stores and builds LCPs at venues. Participating venue owners need to deploy an inexpensive device inside their business, allowing them to perform LCP related activities and verify the physical presence of participating users. They have taken steps to address the conflict between the profit and privacy in geosocial networks. It relies on Benaloh's homomorphic cryptosystem and zero knowledge proofs to enable oblivious and provable correct LCP computations.

B.Krishnamoorthy[2] et al. have proposed a method to prevent the leakage of Personally Identifiable Information (PII) through the online social networks(OSNs) making agreements between aggregators and OSNs that forbid aggregators from using any information they may receive as a result of user's interaction with an OSN.OSNs are in the best position to prevent such leakage by eliminating OSN identifiers from the Request-URI and consequently the Referrer header. This elimination can be done directly or by mapping an OSN identifier to a session-specific value. Users have some means for limiting PII leakage via what information they provide to the OSN or browser/proxy techniques to control use of the Referrer header and cookies. However, these controls may break accesses to other sites or not completely eliminate PII leakage via OSNs.

In GeoSNs, it is possible for exact locations of users to be exposed to untrusted entities. Privacy in social network services has become a hot topic, and reports indicate that users are leaving social network services due to privacy concerns. As it is possible for exact locations of users to be exposed to untrusted entities that may in turn utilize these to infer sensitive information about the users. Dario Freni[4] et al has mainly addresses two threats. Location privacy, Availability of the information about the presence of user in specific location. Absence privacy, Availability of the information about the absence of the individual from specific location during given periods of time. This arrangement is undesirable for two main reasons. First, GeoSN service providers are generally interested in as much content as possible being available, as this attracts users and thus increases advertising revenue. Second, in most GeoSN services, users can reference other users in resources; and it is generally not possible for a user to control the resources published by another user. Privacy is preserved by making use of a centralized trusted entity which involves in processing the resource and publish it to geoSN.

With the aim to enable the vision of smart and safe cities, J.Ballesteros[5] et al. have proposed by exploiting mobile and social networking technologies to securely and privately extract, model and embed real-time public safety information into quotidian user experiences. First, the novel approaches to defining location and user based safety metrics. The ability of existing forecasting techniques to predict future safety values is evaluated.iSafe, a privacy preserving algorithm is devised for computing safety snapshots of co-located mobile devices as well as geosocial network users.

B.Carbunar[6] et al. have provided an input to targeted advertising, profiling social network users becomes an important source of revenue. Its natural reliance on personal information introduces a trade-off between user privacy and incentives of participation for businesses and geosocial network providers. Location centric profiles (LCPs), aggregates built over the profiles of users present at a given location. PROFILR is introduced, a suite of mechanisms that construct LCPs in a private and correct manner. It has been combined with iSafe, a novel approach for context aware public safety application. Participating venue owners need to deploy an inexpensive device inside their business, allowing them to perform LCP related activities and verify the physical presence of participating users. PROFILR with the notion of snapshot LCPs is extended and communicated over ad hoc wireless connections. They don't concentrate on geo-social networks. A large number of fake, Sybil accounts cannot be controlled.

F.G.Olumofin[7] et al. have proposed a method for Achieving efficient query privacy for Location Based Service Users of mobile devices tend to frequently have a need to find Points Of Interest (POIs), such as restaurants, hotels, or gas stations, in close proximity to their current locations. Collections of these POIs are typically stored in databases administered by Location Based Service (LBS) providers such as Google, Yahoo!, and Microsoft, and are accessed by the company's own mobile client applications or are licensed to third party independent software vendors. A user first establishes his or her current position on a smartphone through a positioning technology[13] such as GPS (Global Positioning System) or cell tower triangulation, and uses it as the origin for the search. The problem is that if the user's actual location is provided as the origin to the LBS, which performs the lookup of the POIs, then the LBS will learn that location. In addition, a history of locations visited may be recorded and could potentially be used to target the user with unexpected content such as local advertisements, or worse, used to track him or her. Mobile smartphone users frequently need to search for nearby points of interest from a location based service, but in a way that preserves the privacy of the users' locations.

A.Tootoonchian[8] et al. have proposed a framework called Lockr, the Better Privacy for Social Networks . Lockr, a system that improves the privacy of centralized and decentralized online content sharing systems. Lockr offers three significant privacy benefits to OSN users. First, it separates social networking content from all other functionality that OSNs provide. Second, Lockr ensures that digitally signed social relationships needed to access the social data cannot be reused by the OSN for unintended purposes. This feature drastically reduces the value to others of social content that users entrust to OSN providers. Finally, Lockr enables message encryption using a social relationship key. This key lets two strangers with a common friend verify their relationship without exposing it to others, a common privacy threat when sharing data in a decentralized scenario.

III. Proposed Work

A. Overall Architecture Diagram

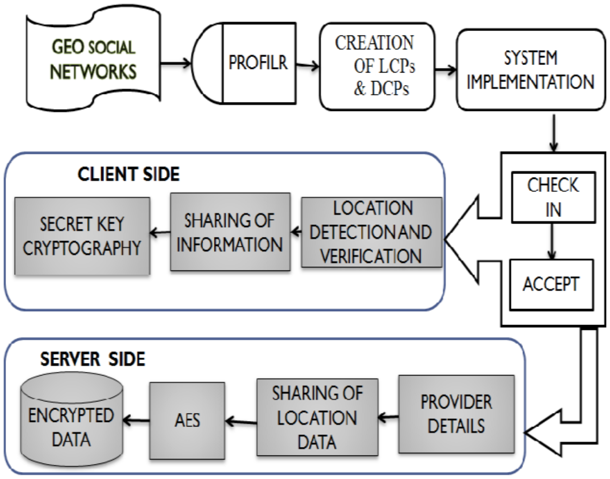


Fig1. Overall Architecture Diagram

We consider a core functionality that is supported by the Most influential geosocial network (GSN) providers, Yelp [9] and Foursquare [10]. This functionality is simple and general enough to be applicable to most other GSNs (e.g., Facebook Places, Google Latitude).

B. Concepts Involved

1) Geosocial Networks:

Geo-Social Networking is networking dealing with geographic locations. They have the Greater capacity for service requests such as geocoding. Thus, resources such as status messages, photos, and "check-ins" are tagged with the location in which they were generated. Further, some of the Popular geosocial applications which involves in GSNs like Google Map,Yelp, Gowalla, Facebook Places
and foursquare allow users to share their locations as well as recommendations for a locations or 'venues'. Geosocial network has the combined potential of bringing a Social Network or Social Graph to a location, and having people at a location form in to a Social Network or Social Graph.

2) Framework :

PROFILR, a framework is used that allows the construction of LCPs based on the profiles of present users, while ensuring the privacy and correctness of participants. First, a venue centric PROFILR is proposed, that relieves the GSN provider from a costly involvement in venue specific activities. To achieve this, PROFILR stores and builds LCPs at venues. Second, completely decentralized PROFILR extension is proposed, which is built around the notion of snapshot LCPs. The distributed PROFILR is designed which enables user devices to aggregate the profiles of co-located users, without assistance from a venue device. PROFILR, a novel alternative that provides significantly improved location privacy without adding uncertainty into query results or relying on strong assumptions about server security. The key insight is designed to apply secure user-specific, distance-preserving coordinate transformations to all location data shared with the server. The friends of a user share this user's secrets so they can apply the same transformation.

3) System Implementation:

In this model, a provider hosts the system, along with information about registered venues, and serving a number of users. To use the provider's services, a client application, the "client", needs to be downloaded and installed.

4) Check-in:

Users register and receive initial service credentials, including a unique user id.User and provider has to log on to the application to access those services. Each and every time check-in has been performed

5) Accept:

Users are encouraged to report their location, through *check-ins* at venues where they are present. During a check-in operation, performed upon an explicit user action, the user's device retrieves its GPS coordinates, reports them to the server, who then returns a list of nearby venues.

C. Client/user Side Security

1) Location Detection and Verification:

After a valid Login, the Google maps API tool has been activated such that the corresponding location has been detected and a map has been displayed showing the exact location of the corresponding input provided. The user's device retrieves its GPS coordinates, along with the latitude and longitude information and reports them to the server, who then returns a list of nearby venues. The device displays the venues and the user needs to choose one as her current check-in location. This is achieved by means of Google maps API.

2) *Sharing of Information:*

The user can share or send reviews to other users only after a valid authentication. This endows the user with location privacy and correctness assurances.

3) *Secret Key Cryptography:*

The sender and receiver needs to know about the secret key though which they are going to share the location data. It is of 16-bit secret key which is known both to sender and receiver to share the information. Secret key Cryptographic technique is applied for secured transformation of location data.

D. *Server Side Security*

1) *Provider Details:*

The provider has to register the personal and professional details to the server and also their services along with the geo-tagged location information. The provider has the option to view the location data based on access controls. Updation of the profiles can be made if correction is needed.

2) *Sharing of Location data:*

User1 and User2 exchange their secrets,User1 generates an Location to an Encrypted Index (L2I) and index to the encrypted location data (I2D) from her review of the restaurant (at (x, y)), and stores the L2I on the index server via a proxy.User1then stores the I2D on the data server directly.User2 later visits the restaurant and fetches for L2Is from his friends by sending the transformed coordinates via a proxy[15].User2 decrypts the L2I obtained and then queries for the corresponding I2D, finally User2 decrypts User1's review.

3) *AES:*

Advanced Encryption Standard (AES) is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a networkers is a variant of Irondale which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael [3]specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state.

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. The number of cycles of repetition is as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

4) *High-level description of the algorithm:*

a) Key Expansion: round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

b) Initial Round:

AddRoundKey: each byte of the state is combined with a block of the round key using bitwise xor

c) Rounds

SubBytes: a non-linear substitution step where each byte is replaced with another according to a lookup table. In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, In the SubBytes step, each byte is replaced with a SubByte using an 8-bit substitution box and the Rijndael S-box. This operation provides the non-linearity in the cipher. While performing the decryption, Inverse SubBytes step is used, which requires first taking the affine transformation and then finding the multiplicative inverse (just reversing the steps used in SubBytes step)

ShiftRows: a transposition step where the last three rows of the state are shifted cyclically a certain number of steps. The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES,the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. Row n is shifted left circular by n-1 bytes.

MixColumns: a mixing operation which operates on the columns of the state, combining the four bytes in each column.

AddRoundKey- each byte of the state is combined with a block of the round key using bitwise xor

D) *Final Round (no MixColumns)*

SubBytes: a non-linear substitution step where each byte is replaced with another according to a lookup table. In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, In the SubBytes step, each byte is replaced with a SubByte using an 8-bit substitution box and the Rijndael S-box. This operation provides the non-linearity in the cipher. While performing the decryption, Inverse SubBytes step is used

ShiftRows: a transposition step where the last three rows of the state are shifted cyclically a certain number of steps. The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES,the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. Row n is shifted left circular by n-1 bytes.

AddRoundKey: each byte of the state is combined with a block of the round key using bitwise xor

5) Encrypted Data:

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption

IV. Results and Findings

In the Location centric profiles, we focused on a single profile dimension, *D*.

A. We assume *D* takes values over a range *R* that can be discretized into a finite set of sub-intervals continuous disjoint intervals or discrete values.

B. Then, given an integer *b*, chosen to be dimension specific, we divide *R* into *b* intervals/sets, *R*1, .., *Rb*.

C. For instance, gender maps naturally to discrete values (*b* = 2), while age can be divided into disjoint sub-intervals, with a higher *b* value.

D. We define the aggregate statistics *S* for dimension *D* of *LCP(L)* to consist of *b* counters *c*1, .., *cb*; *ci* records the number of users from *U* whose profile value on dimension *D* falls within range *Ri* , *i* = 1..*b*.

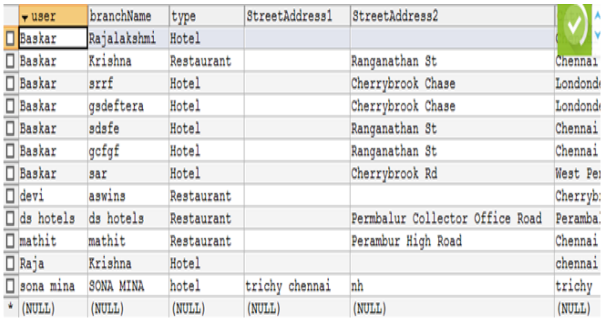
A. Results

Client side

I) To use the provider's services, a client application, the "client", needs to be downloaded and installed.

II) User has to register their self to access the services. Updating of profiles can be done

III) The key insight is designed to apply secure user-specific, distance-preserving coordinate transformations to all location data shared with the server.



	user	branchName	type	StreetAddress1	StreetAddress2	
□	Baskar	Rajalakshmi	Hotel			[illegible]
□	Baskar	Krishna	Restaurant		Ranganathan St	Chennai
□	Baskar	srrf	Hotel		Cherrybrook Chase	Londond
□	Baskar	gsdeftera	Hotel		Cherrybrook Chase	Londond
□	Baskar	sdsfe	Hotel		Ranganathan St	Chennai
□	Baskar	gcfgf	Hotel		Ranganathan St	Chennai
□	Baskar	sar	Hotel		Cherrybrook Rd	West Pe
□	devi	aswins	Restaurant			Cherryb
□	ds hotels	ds hotels	Restaurant		Permbalur Collector Office Road	Peramba
□	mathit	mathit	Restaurant		Perambur High Road	Chennai
□	Raja	Krishna	Hotel			chennai
□	sona mina	SONA MINA	hotel	trichy chennai	nh	trichy
*	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)

Fig2. *Construction of LCPs and DCPs*

IV) User and provider have to log on to the application to access those services. Each and every time check-in has been performed

V) Users are encouraged to report their location, through *check-ins* at venues where they are present.

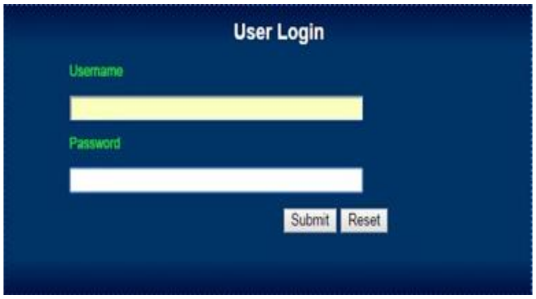
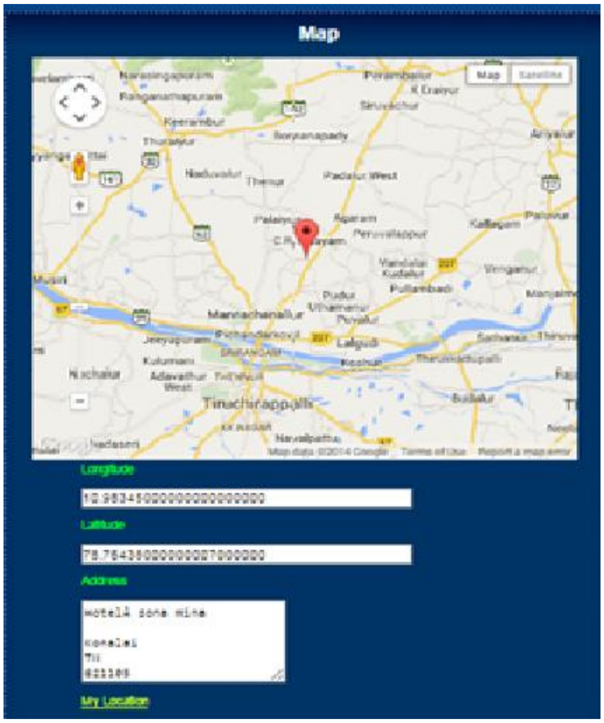


Fig3. *Check-ins*

VI) After a valid Login, the Google maps API tool has been activated such that the corresponding location has been detected and a map has been displayed showing the exact location of the corresponding input provided. The user's device retrieves its GPS coordinates, along with the latitude and longitude information and reports them to the server



Longitude

10.98345000000000000000

Latitude

78.76438000000000700000

Address

hotel4 sona mina

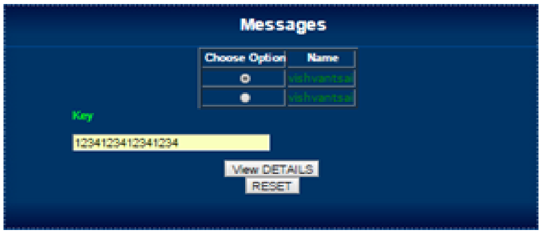
[illegible]

TN

[illegible]

Fig4. *Location detection and verification*

VII) The user can share or send reviews to other users only after a valid authentication.



Choose Option	Name
◉	vishvantsai
●	vishvantsai

Key

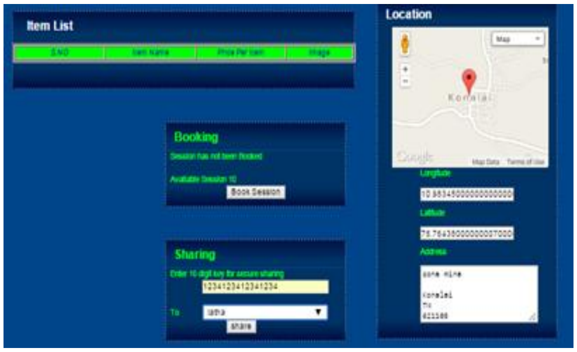
1234123412341234

Fig5. *Sharing of secret messages*

VIII) The sender and receiver needs to know about the secret key though which they are going to share the location data. It is of 16-bit secret key which is known both to sender and receiver to share the information.

Server side

I) The provider has to register the personal and professional details to the server and also their services along with the geo-tagged location information.



Session has not been Booked

Available Session 10

Enter 16 digit key for secure sharing 1234123412341234

To latha

Longitude 10.983450000000000

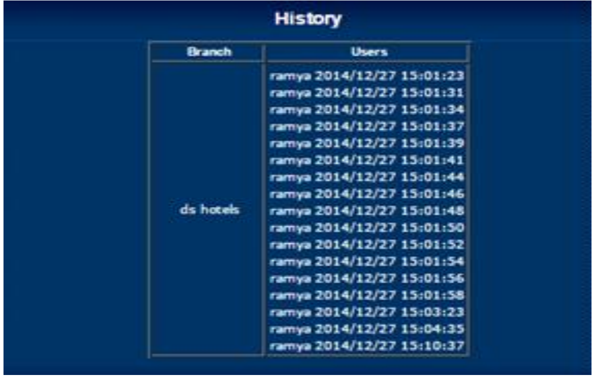
Latitude 78.7643800000007000

Address

Fig6.Sharing secret information

II) User1 and User2 exchange their secrets, User1 generates Location to an Encrypted Index (L2I) and index to the encrypted location data (I2D) from her review of the restaurant (at (x, y)), and stores the L2I on the index server via a proxy. She then stores the I2D on the data server

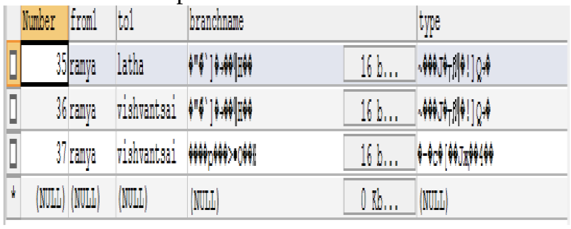
III) Encryption is performed for sharing the location data and messages



Branch	Users
ds hotels	ramya 2014/12/27 15:01:23 ramya 2014/12/27 15:01:31 ramya 2014/12/27 15:01:34 ramya 2014/12/27 15:01:37 ramya 2014/12/27 15:01:39 ramya 2014/12/27 15:01:41 ramya 2014/12/27 15:01:44 ramya 2014/12/27 15:01:46 ramya 2014/12/27 15:01:48 ramya 2014/12/27 15:01:50 ramya 2014/12/27 15:01:52 ramya 2014/12/27 15:01:54 ramya 2014/12/27 15:01:56 ramya 2014/12/27 15:01:58 ramya 2014/12/27 15:03:23 ramya 2014/12/27 15:04:35 ramya 2014/12/27 15:10:37

Fig7. *History of sessions recorded*

IV) Advanced Encryption Standard (AES) is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation



	Number	from1	to1	branchname		type
▯	35	ramya	latha	[illegible]	16 b...	[illegible]
▯	36	ramya	vishvantsai	[illegible]	16 b...	[illegible]
▯	37	ramya	vishvantsai	[illegible]	16 b...	[illegible]
*	(NULL)	(NULL)	(NULL)	(NULL)	0 Kb...	(NULL)

Fig8. Encrypted (secured) location data

B. Advantages

- Introduces location centric profiles (LCPs) while simultaneously ensuring the privacy and correctness of participants.
- Designing both a venue centric and a decentralized solution satisfies the proposed privacy and correctness properties.
- Integration of Google MAPs API provides the location correctness and assurances
- Implementation of Cryptographic technique enforces security

C. Applications

- Privacy preserving, personalized safety recommendations
- Secure Information sharing
- Defense communication system

V. Conclusion

This paper talks about the state – of – the art, a conceptual framework for LCPs and DCPs are designed and the mechanisms for privately and correctly building location-centric profiles are efficiently built. The integration of Google maps API provides the correctness assurances. Furthermore, the Implementation of Cryptographic technique and the encryption technique contribute to the concrete implementation of the framework for providing security Privacy and correctness requirements are achieved and thereby security is enhanced. It is the future of networking which allows us to build the cost effective and agile networks.

Acknowledgement

I would like to express my deep gratitude to my research supervisor Mr.S.Subaiah, Head, CSE for enthusiastic encouragement and continuous support. I extend my thanks to my research co-coordinator Mrs. K. Priyadharshini, Head, ECE for his patient guidance and useful critiques of this work. My grateful thanks are also extended to the Management,Trichy Engineering College for their continuous encouragement. Finally I wish to thank my Parents and my husband for their support and encouragement throughout my study.

REFERENCES

[1] Bogdan Carbunar, Mahmudur Rahman, Jaime Ballesteros, Naphtali Rishe, and Athanasios V. Vasilakos," PROFIL*R*: Toward Preserving Privacy and Functionality in Geosocial Networks" IEEE Transactions on Information Forensics and Security, Vol. 9, No. 4, April 2014

[2] Krishnamoorthy.B, Y.Ginjali and C.E.Wills "On the Leakage of Personally Identifiable Information via Geosocial Networks" Comput.Comn Rev Vol 40 No 1pp 112-117, 2010

[3] Josh Benaloh. Dense probabilistic encryption. InProceedings of the Workshop on Selected Areas of Cryptography, pages 120–128, 2009.

[4] Dario Freni1, Carmen Ruiz Vicente, Sergio Mascetti, Claudio Bettini, Christian S. Jensen,"Preserving Location and Absence Privacy in Geo-Social Networks", CIKM'10, October 26–302010, Toronto, Ontario, Canada.

[5] B.Carbunar, M.Rahman, J.Ballestros, N.Rishe "Towards Safe Cities a Mobile and Social Networking Approach"-IEEE Trans Parallel Distributed Systems Vol3 Pp1-14 Nov2013

[6] B.Carbunar, M.Rahman, J, N.Rishe "Eat the Cake And Have It Too: Towards Privacy Preserving Location Aggregate Functionalites in Social Networking Approach"-IntConf Mob Sec Approach 2013 Pp1-3

[7] Tootoonchian.A, S.SaroiouY.Ginjali and A.Wolman "Lockr-the Better Privacy for Social Networks"ieee-2009 PP 1-12

[8] F.G.Olumofin, P.Tysowski, I.Goldberg, and U.Hengartner, "Achieving efficient query privacy for location based services," in Proc.Privacy Enhancing Tech., 2010, pp93–110.

[9] B.Carbunar, M.Rahman, J.Ballestros,"Private Location Centric Profiles for GeoSocial Networks" " Inproc.19th Newyork, USA

[10] Bogdan Carbunar, Radu Sion, Rahul Potharaju, and Moussa Ehsan. The shy mayor: Private badges in geosocial networks. In *Proceedings of the 10th International Conference Applied Cryptography and Network security (ACNS)*, pages 436–454, 2012

[11] Amirreza Masoumzadeh, James Joshi, "Top Location Anonymization for Geosocial Network Datasets" TRANSACTIONS ON DATA PRIVACY 6 (2013) 107–126

[12] K.P.N. Puttaswamy and B.Y.Zhao, "Preserving privacy in location based mobile social applications," in Proc. Mobile Comput. Syst. Appl., New York, USA, 2010, pp. 1–6.

[13] B.Carbunar, M.Rahman, J.Ballestros, N.Rishe "Towards Privacy Preserving Functionalities in Social Networking Approach"-intConf Mob Sec Approach 2013 Pp1-3

[14] A. M. Kakhki, C. Kliman-Silver, and A. Mislove, "Iolaus: Securing online content rating systems," in *Proc. 22nd Int. World Wide Web Conf.(WWW)*, Rio de Janeiro, May 2013, pp. 1–5.

[15] G. Coley, *Beagleboard System Reference Manual*. Dallas, TX, USA, BeagleBoard. Org., Dec. 2009.

[16] B. Carbunar and R. Potharaju, "You unlocked the Mt. Everest badge on foursquare! countering location fraud in geosocial networks," in *Proc. 9th IEEE Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Feb. 2012, pp. 182–190.

[17] S. Goldwasser and S. Micali, "Probabilistic encryption & how to play mental poker keeping secret all partial information," in *Proc. 14th Annu.ACM Symp. Theory Comput.*, New York, NY, USA, 1982, pp.365–377.

[18] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981.