ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

Enabling Privacy Protection and Content Assurance in Geo-Social Networks

[1] M.S.Vivekanandan, [2]Dr.C.Rajabhusanam
[1] Asst. professor, Dept. of CSE, Bharath Institute of Higher Education and Research, Chennai
[2] P.G Student, Dept. of CSE, Bharath Institute of Higher Education and Research. Chennai

Abstract: ***Analyzing the conflict on privacy preserving mechanisms and functionality in geo social networks, PROFILR-A framework is proposed for constructing location centric profiles (LCPs), aggregates built over the profiles of users that have visited discrete locations thereby preserving users from unwanted issues. PROFIL Rendows users with strong privacy guarantees and providers with correctness assurances. Steps are taken toward addressing this conflict. The approach is based on the concept of location centric profiles (LCPs). LCPs are statistics built from the profiles of users that have visited a certain location or a set of co-located users. A novel approach is proposed to define the location and user based safety metrics. Our key insight is to apply secure user-specific, distance-preserving coordinate transformations to all location data shared with the server. In addition to a venue centric approach, a decentralized solution is proposed for computing LCP snapshots over the profiles of co-located users is presented for private information retrieval that allows a user to retrieve information. In future, cryptographic techniques are further applied to enhance the security such that a technique 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 see or infer the actual location data from the transformed data or from the data access.***

Keywords—ProfilR; Location Centric Profiles; Geo-aware social networks.

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 social networks are popular because of informative nature. People know what others are doing and how they feel about it. It also allows the users to meet others who are geographically closer and who have similar interests. Geosocial networking allows users to interact relative to their current locations. Web mapping services with geocoding data for places (streets, buildings, and parks) can be used with geotagged information (meetups, concert events, nightclubs or restaurant reviews) to match users with a place, event or local group to socialize in or enable a group of users to decide on a meeting activity.

Geo-aware social networks (GeoSNs) are enabled by the availability of social network services, mobile devices with Internet connectivity, and geo-location capabilities. GeoSN users generate and share very large volumes of content, or resources, tagged with the geo-location request and responses. 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, Popular geosocial applications likeYelp, 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. Thus social networks can be expanded by real world contact and recruiting new members.

Benefits of Geosocial networks

- Geosocial networking allows users to interact relative to their current locations.
- Can find out what others think about a certain restaurant or location.
- Allows the users to know where their friends are.
- Increases knowledge of others people's likes and habits.

Geosocial Network Applications

Geosocial Applications Are The Applications That Use A Geosocial Networking Which Is A Type Of Social Networking In Which Geographic Services And Capabilities Are Used To Enable Additional Social Dynamics. Geo-Social Networks Such As Yelp, Foursquare And Facebook Places Are Very Famous.

II. LITERATURE REVIEW

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. GeoSN resources are easily spread among users in real time; additional threats such as stalking or assault are possible [1]. This paper presents 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 [2].

Personally identifiable information" (PII) an individual's identity either alone or when combined with other public information that is linkable to a specific individual. The growth in identity theft has increased concerns regarding unauthorized disclosure of PII [3]. 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 [4].

III. EXISTING SYSTEM

Overtly, personal information allows GSN providers to offer a variety of applications, including personalized recommendations and targeted advertising, and venue owners to promote their businesses through spatio-temporal incentives, e.g., rewarding frequent customers through accumulated badges. There exists therefore a conflict. Existing systems have not taken the approaches to improving user privacy in geo-social systems such as, introducing uncertainty or error into location data, relying on trusted servers or intermediaries. More specifically, they target geo-social applications, and assume that servers (and any intermediaries) can be compromised and, therefore, are untrusted [5].

DISADVANTAGES OF EXISITNG SYTEM:

- Providing personal information exposes however users to significant risks, as social networks have been shown to leak and even sell user data to third parties.
- Without privacy people may be reluctant to use geosocial networks.
- without user information the provider and venues cannot support applications and have no incentive to participate.

The disadvantages of the traditional approach outlined above can be overcome by the implementation of a framework named PROFILR.

IV. PROPOSED METHODOLOGY

Online social networks have become a significant source of personal information. Their users voluntarily reveal a wealth of personal data, including age, gender, contact information, preferences and status updates. A recent addition to this space, geosocial networks (GSNs) such as Yelp and Foursquare further collect fine grained location information, through check-ins performed by users at visited venues.

Overtly, personal information allows GSN providers to offer a variety of applications, including personalized recommendations and targeted advertising, and venue owners to promote their businesses through spatio-temporal incentives, e.g., rewarding frequent customers through accumulated badges. Providing personal information exposes however users to significant risks, as social networks have been shown to leak and even sell user data to third parties. There exists therefore a conflict. Without privacy people may be reluctant to use geosocial networks, without user information the provider and venues cannot support applications and have no incentive to participate [6]

First steps are taken towards addressing this conflict. The main approach is based on the concept of location centric profiles (LCPs). LCPs are statistics built from the profiles of (i) users that have visited a certain location or (ii) a set of co-located users.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

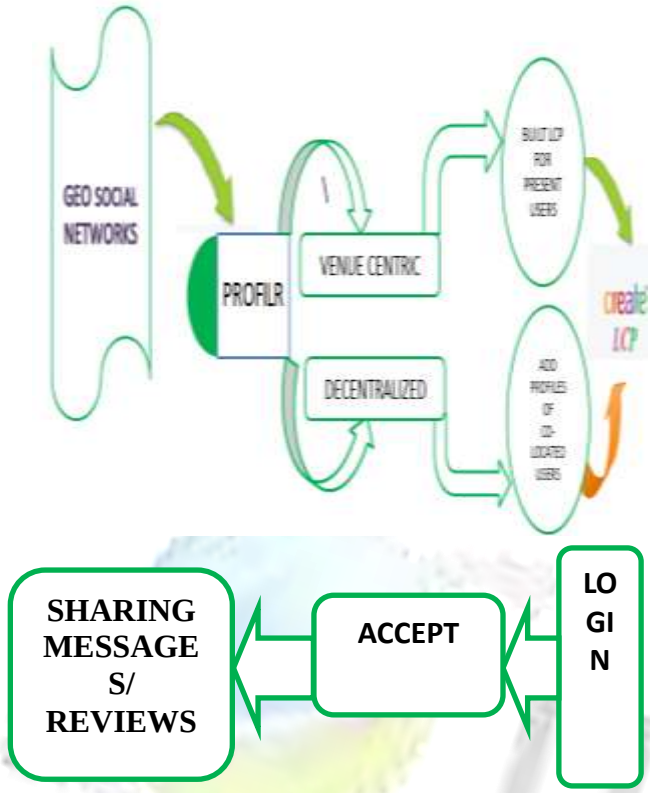

Figure 1. Proposed Methodology

PROFILR, a framework that allows the construction of LCPs based on the profiles of the present users is introduced, while ensuring the privacy and correctness of the participants. Informally, privacy is defined as the inability of venues and the GSN provider to accurately learn user information, including even anonymized location trace profiles. Verifying the correctness of user data is necessary to compensate for this privacy constraint: users may cheat and bias LCPs anonymously. Two user correctness components are considered. First, location correctness, where users should only contribute to LCPs of venues where they are located. This requirement is imposed by the recent surge of fake check- ins, motivated by their use of financial incentives. Second, LCP correctness, where users should be able to modify LCPs only in a predefined manner [7].

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, 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, without assistance from a venue device. •Introduce the problem of computing location centric profiles (LCPs) while simultaneously ensuring the privacy and correctness of participants [8].

The Steps are:

- ✓ Propose PROFILR, a framework for computing LCPs. Devise both a venue centric and a decentralized solution. Prove that PROFILR satisfies the proposed privacy and correctness properties.
- ✓ Provide two applications for PROFILR :
  1. Privacy preserving.
  2. Personalized public safety recommendations
- ✓ Evaluate PROFILR framework.

ADVANTAGES OF PROPOSED SYSTEM:

- PROFIL*R* satisfies the proposed privacy and correctness properties.
- Provide two applications for PROFIL*R*: (i) privacy preserving, personalized public safety recommendations and (ii) privately building real time statistics over the profiles of venue patrons with user accounts.
- Introduce the problem of computing location centric profiles (LCPs) while simultaneously ensuring the privacy and correctness of participants.

V. ALGORITHM AND TECHNIQUES USED

ADVANCED ENCRYPTION STANDARD (AES)

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 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 [9].

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 are 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.

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 key.

High-level description of the algorithm

1. 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.
2. InitialRound
    1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds
    1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
    3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
    4. AddRoundKey
4. Final Round (no MixColumns)
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey.

VI. RESULT AND DISCUSSION

In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.In the SubBytes step, each byte aij in the state matrix is replaced with a SubByte S(aij) using an 8-bit substitution box, the Rijndael S-box. This operation provides the non-linearity in the cipher.While performing the decryption, Inverse

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

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 [10].

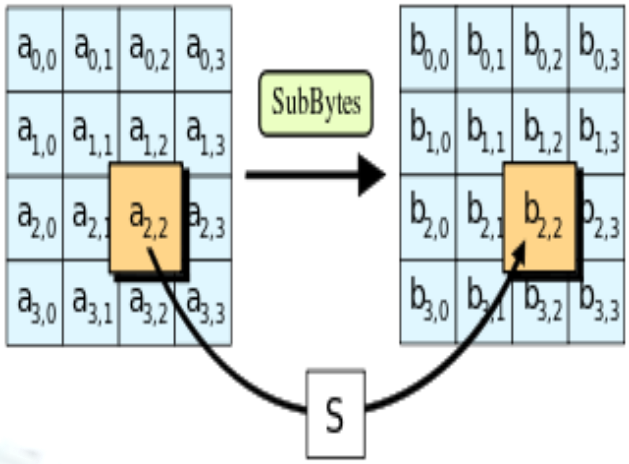

Figure 2. Sub Bytes

THE SHIFTROWS STEP

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.

THE MIXCOLUMNS STEP

In the MixColumns step, the four bytes of each column of the state are combined using an invertible linear transformation. The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes.

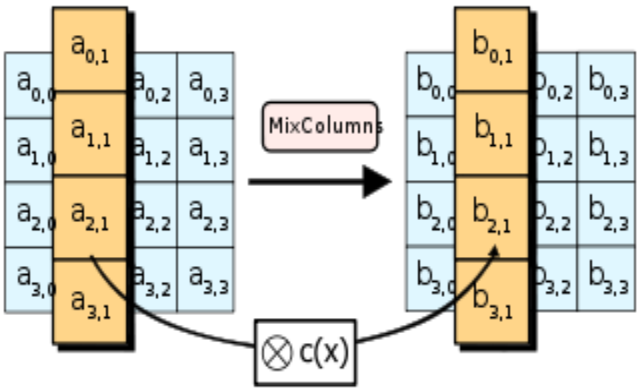

Figure 3. Mix Column

In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XORoperation (⊕).In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main keyusing Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

AES has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. By 2006, the best known attacks were on 7 rounds for 128-bit keys, 8 rounds for 192-bit keys, and 9 rounds for 256-bit key.

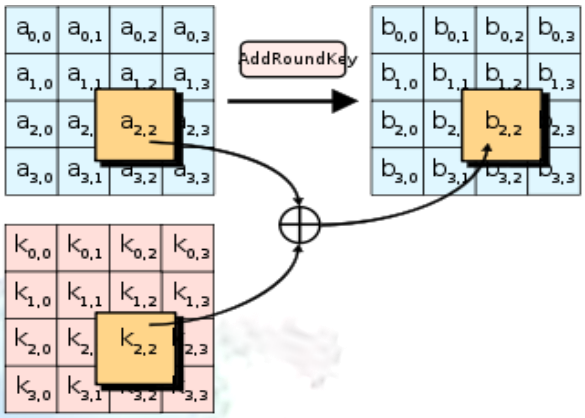

Figure 4. Add Round Key Strp

VII. CONCLUSION

PROFILR-A framework is proposed for constructing location centric profiles (LCPs), aggregates has been built over the profiles of users that have visited discrete locations thereby preserving users from unwanted issues which endows users with strong privacy guarantees and providers with correctness assurances. The concept of Location Centric Profiles (LCPs) is applied for addressing the conflict. LCPs are statistics built from the profiles of users that have visited a certain location. A decentralized solution for computing LCP snapshots over the profiles of co-located users has been framed. In future, cryptographic techniques are further applied to enhance the security such that a technique 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 see or infer the actual location data from the transformed data or from the data access.

REFERENCES

[1] Dario Freni, Carmen Ruiz Vicente, Sergio Mascetti, Claudio Bettini, and Christian S. Jense. “Preserving Location and Absence Privacy in Geo-Social Networks”. Proceedings of the 19th international conference on Information and knowledge management. ACM, 2010, pp. 309-318.

[2] Tootoonchian, Amin Saroiu, S. Ganjali, Y. and Wolman, A. "Lockr: better privacy for social networks." Proceedings of the 5th international conference on Emerging networking experiments and technologies. ACM, 2009, pp. 169-180.

[3] Krishnamurthy, Balachander, and Craig E. Wills. "On the leakage of personally identifiable information via online social networks." Proceedings of the 2nd ACM workshop on Online social networks. ACM, 2009,, pp. 7-12.

[4] Olumofin, Femi, K.Tysowski, I.Goldberg and U.Hengatnar “Achieving efficient query privacy for location based services” International Symposium on Privacy Enhancing Technologies Symposium. Springer, Berlin, Heidelberg, 2010, pp. 93-110.

[5] Ballesteros, Jaime, Ballesteros, L., Carbunar, B., Rahman, M., Rishe, N., & Iyengar, S. S. “Towards safe cities: A mobile and social networking approach”, IEEE Transactions on Parallel and Distributed Systems, 2014, pp. 2451-2462.

[6] Carbunar, Bogdan, Carbunar, B., Rahman, M., Ballesteros, J., & Rishe, N. , "Eat the cake and have it too: Privacy preserving location aggregates in geosocial networks."arXiv preprint arXiv:1304.3513, 2013.

[7] De Cristofaro, Emiliano, Clau

[8] dio Soriente, Gene Tsudik, and Andrew Williams, "Hummingbird: Privacy at the time of twitter." In Security and Privacy (SP) Symposium on IEEE, 2012, pp. 285-299.

[9] Dey R., Jelveh, Z. and Ross, K "Facebook users have become much more private: A large-scale study", In Pervasive Computing and Communications Workshops (PERCOM Workshops), International Conference on IEEE, 2012, pp. 346-352.

[10] Han, S., Ng, W. K., and Philip, S. Y. "Privacy-preserving singular value decomposition" In Data Engineering, ICDE'09, 25th International Conference on IEEE, pp. 1267-1270.

Jernigan, C, and Mistree, B. F, "Gaydar: Facebook friendships expose sexual orientation", 2009.