LOCATION SHARING SYSTEM WITH ENHANCED PRIVACY IN MOBILE ONLINE SOCIAL NETWORK

K.Laxmi Deepthi
PG Scholar, Department of IT
G.Narayamma Institute of Technology and science
JNTUH, Hyderabad, Telengana, India.

Dr.I.Ravi Prakash Reddy
Professor, Department of IT
G.Narayamma Institute of Technology and Science
JNTUH, Hyderabad, Telengana, India.

Abstract—Area sharing is one of the basic segments in versatile online informal organizations, which has pulled in much consideration as of late. With the appearance of mobile networking, an ever increasing number of clients' area data will be gathered by the specialist co-ops in location sharing. Notwithstanding, the clients' security, including area protection and informal organization security, can't be ensured in the past work without the trust supposition on the specialist co-ops. In this paper, going for accomplishing improved protection against the insider assault propelled by the specialist organizations, we present another engineering with numerous area servers out of the blue and propose a safe arrangement supporting area sharing among companions and outsiders in area based applications. In our development, the client's companion set in every companion's inquiry submitted to the area servers is separated into numerous subsets by the informal community server arbitrarily. Every area server can just get a subset of companions, rather than the entire companions' arrangement of the client as the past work. Also, out of the blue, we propose an area sharing development which gives check capacity of the looking outcomes came back from area servers in a proficient manner. We additionally demonstrate that the new development is secure under the more grounded security model with upgraded protection. At last, we give broad exploratory outcomes to show the effectiveness of our proposed development.

Keywords—sharing the location, encryption,privacy of location.

I. INTRODUCTION

With the approach of portable registering, customary social systems have progressively turned out to be new standards called portable online informal organizations (mOSNs). Much like the conventional Web-based informal community, mOSNs likewise happen in virtual network for spreading substance, expanding availability, furthermore, associating clients from any place they are. mOSNs carry enormous changes to customary interpersonal organizations and render versatile interpersonal organizations as a piece of day by day life on the grounds that of its portability of cell phones. This new kind of interpersonal organizations gives more extravagant client experience and advantageous correspondences [1].

Area based administrations (LBSs) are a standout amongst the most significant parts in mOSNs, which gives data and amusement administration dependent on the geological position ofthe cell phone [2]. LBS has encountered touchy development as of late, especially utilizing the quick advancement of portable innovation and the distributed computing. In LBS, the area of a gadget, speaking to a standout amongst the most significant logical data about the gadget and its proprietor, is misused to create imaginative and esteem added administrations to the clients' close to home setting. Numerous individual, business, and undertaking focused LBSs are as of now accessible and have picked up notoriety. Different LBS applications have been proposed, such as area based portable publicizing to cell phone clients. In E-wellbeing frameworks, LBS can likewise be connected to enable access to patient records outside the emergency clinics by specialists with

locationbasedget to innovation. There are likewise numerous instances of LBS counting versatile registration diversions like Foursquare [3], socialsystems like Loopt [4], and area empowered applications likeGoogle Maps. Examiners venture the incomes for LBS to develop from 2.8 billion of every 2010 to hit 10.3 billion by 2015.

With the expanding prominence of LBS, the security concerns on clients' areas have been raised. Since the locationtracking capacity of cell phones has been improved incredibly, client's close to home data, for example, the position and inclination will be spilled and powerless against inappropriate use. As an outcome, it abuses client's security and blocks the improvement of different LBS applications. An ongoing MIT study demonstrated that, with a piece of data gathered from cell phones, they can particularly recognize 95% of 1.5 M individuals in a portability database [5]. This risk turns out to be significantly progressively genuine when it comes to mOSNs, in which clients' physical areas are being corresponded with their profiles [6]. Without an assurance of security, clients might be reluctant to share areas throughmOSNs [7]. Thusly, how to secure the area protection is one of the fundamental difficulties in mOSNs.

Be that as it may, none of these strategies thought about the security necessity of interpersonal organization protection. We call attention to that the past works can't avoid the area specialist organization from learning client's touchy data of his informal organization by connecting inquiries from a similar client. There are two stages which may conceivably release the client's personality data to the area server. One is the stage amid creating/refreshing client's data in the area server. The essential security necessity in LBS is to accomplish namelessness of client's character against the area server in a solitary inquiry. The greater part of the past work can just accomplish the security concerning this prerequisite. Notwithstanding, another significant stage is the inquiry stage. There are two sorts of area questions, including the close-by companions' question and outsiders' inquiry. For companions' area question, a client can present an inquiry to get the majority of his/her close-by companions' areas. Notwithstanding, the informal community server needs to send the client's companion rundown to the area server so as to think about the separation between the client and the majority of his companions. Regardless of whether the interpersonal organization server sends the phony character list to the area server, despite everything it will be connected to a similar client by the area server. All the more explicitly, the shortcoming that two companions' inquiries from a similar client will be connected exists on the whole of the past works.

II. RELATED WORKS

An overview of portable distributed computing: Architecture, applications, and methodologies Creators: H. T. Dinh, C. Lee, D. Niyato, and P. Wang Driven by advancements, for example, versatile registering, distributed computing framework, DevOps and flexible figuring, the micro service structural style has risen as another option in contrast to the solid style for planning enormous programming frameworks. Solid heritage applications in industry experience relocation to micro service-arranged models. A key test in this setting is the extraction of micro services from existing solid code bases. While casual relocation examples and strategies exist, there is an absence of formal models and robotized bolster devices here. This paper handles that challenge by exhibiting a formal micro service extraction model to permit algorithmic suggestion of micro service competitors in a refactoring and movement situation. The formal model is actualized in an online model. An exhibition assessment shows that the displayed methodology gives sufficient execution. The proposal quality is assessed quantitatively by custom micro service-explicit measurements. The outcomes demonstrate that the delivered micro service competitors bring down the normal advancement group size down to half of the first size or lower. Moreover, the span of suggested micro service adjusts with micro service estimating revealed by experimental reviews and the area explicit excess among various micro services is kept at a low rate.

Unique in the group: The security limits of human portability Creators: Y.- A. Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel We present a childish directing model to upgrade the distribution of undertakings in a portable crowd sensing (MCS) framework. The players of our game are detecting administration requesters that desire to course their interest along ways that are comprised of assets having a place with the group members. Asset use includes load-subordinate expenses and one asset may serve a few demands in the meantime. Because of human contribution and portability there exists vulnerability, which we address by presenting conviction parameters. For the

Nash equilibrium of our game, we can exchange productivity ensures, i.e., the most pessimistic scenario proportion between the welfare of a balance and the welfare of a social ideal is provably limited by a little steady when cost capacities are polynomials. An epsilon-estimation of a Nash balance arrangement can be processed in polynomial time for relative cost capacities. In light of our model, we build up a component for the mechanization of effective assignment allotments in MCS frameworks and we present a proof for the honesty of this system.

Adaptable security protecting area partaking in portable online interpersonal organizations AUTHORS: W. Wei, F. Xu, and Q. Li, "Mobishare Area sharing is a principal segment of portable online interpersonal organizations (mOSNs), which additionally raises noteworthy protection concerns. The mOSNs gather a lot of area data after some time, and the clients' area protection is undermined if their area data is mishandled by enemies controlling the mOSNs. In this paper, we present Mobi Share, a framework that gives adaptable security protecting area partaking in mOSNs. Mobi Share is adaptable to help an assortment of area based applications, in that it empowers area sharing between both confided in social relations and untreated outsiders, and it supports range question and client characterized access control. In Mobi Share, neither the interpersonal organization server nor the area server has total information of the clients' personalities and areas. The clients' area security is ensured regardless of whether both of the substances intrigues with noxious clients.

Ensuring area security of clients in mOSNs has gotten a colossal consideration as of late. There are a few different ways to accomplish the area security, for example, concealing the relations between client character and area [17], area secrecy, etc. Area secrecy is a successful strategy for area security assurance. In this strategy, cell phones or the confided in third server first procedures area data through down to earth techniques, for example, encryption, to conceal clients' character and afterward sends the outcomes to the server supplier to perform inquiry. These strategies of accomplishing area obscurity can be ordered into three sorts:

1) K-obscurity. The primary thought of this K-namelessness, which was proposed by Sweeney [18], is to muddle the real area by developing shrouding districts that contain the areas of K mysterious clients.

2) Dummy areas. The primary thought of the fake area technique, which was proposed in [19], is to give clients a chance to create enough sham areas and exchange them to the specialist co-op. The genuine area is incorporated into the fake areas, and the administration supplier can't recognize which is the genuine area from the phony areas.

3) Location encryption. Khoshgozaran [20] proposed an encryption strategy for the client's area based on Hilbert bends, which uses Hilbert bends to change the unique area to an encoded area. There are additionally numerous different works proposed to comprehend the area protection issues by consolidating the previously mentioned three strategies. Duckham and Kulik [21] proposed a formal model for area jumbling methods, for example, including incorrectness, imprecision, and ambiguity.

Krumm [22] demonstrated that the impacts of spatial shrouding calculations and including Gaussian commotion or undermining the area (i.e., lessening granularity) can debase the ID accomplishment of the enemy. There are additionally some other related chips away at different applications. The paper [23] exhibited an arrangement of MobiMix, which is a street network based blend zone structure to secure area protection of portable clients going on street systems. As opposed to spatial cloaking-based area security assurance, the methodology in MobiMix is to break the progression of area presentation by utilizing blend zones, where no applications can follow the client development. In informal communities, security controls must be adaptable enough to permit sharing between both confided in social relations what's more, untrusted outsiders. To address this issue, [24] proposed a framework called SmokeScreen, which talked about sharing nearness with the two companions and outsiders while saving client protection. As demonstrated in a past research [25], area and nearness are two wellsprings of protection spillage presented by mOSNs. SmokeScreen [24] takes care of the issue of how to adaptably share nearness with the two companions and outsiders while saving client protection. Past work [26], [27] talked about sharing areas between built up relations in a protection safeguarding way. Afterward, considering adaptable security protecting area sharing in mOSNs, Wei et al. [6] proposed Mobishare, which is an augmentation of SmokeScreen. In Mobishare, clients can share their area data with outsider applications furthermore, different clients, however either the OSN

supplier or the area server has total learning of the clients' character and area.

This is accomplished by part area requesters into two gatherings, to be specific, outsiders and companions. At that point, utilizing an encryption plan to ensure the area information, this data is transmitted to the area server or the online social arrange. In any case, this instrument can't anticipate the area server from connecting the questions from a similar client and concentrate delicate data.

III. SYSTEM ANALYSIS

Existing Method:

We see that the personality of the equivalent questioning client is linkable by the area specialist organization in the companions' area inquiry of past works. Albeit various counterfeit personalities have been embedded for every client in these frameworks, companions' inquiries from a similar client will be connected in light of a similar companion set. Thus, this security defenselessness will possibly support the area specialist co-op recognize which record is valid in the area database and make area fakers futile. In expansion, with the genuine phony personality, the area administration supplier can get the companion relations and areas regardless of whether some of them are fakers. All the more truly, if we consider various questions without area refreshes, the area specialist organization can at long last get the topological structure of the informal organization and dispatch various assaults.

Going for fixing this security issue, we propose another framework by presenting another design with various area servers. All the more explicitly, all area data will be put away in every area server. At the point when a solicitation of companions' areas is submitted from a client, this set will be separated into various subsets, and every subset will be sent to an area server, individually. Along these lines, companions' area inquiries from a similar client will be not quite the same as the point perspective on every area server with enough high likelihood. Therefore, these questions can't be connected to a similar client, and improved security has been accomplished in this new framework.

Disadvantages:

1. It can be make an increasingly number of versatile assaults must consideration as of late.

2. The protection of the security was less dimension of the portable online informal community.

3. Occurrence of failure in single point.

Proposed method:

In this undertaking, going for accomplishing upgraded protection against the insider assault propelled by the specialist organizations in mOSNs, we present another engineering with various area servers out of the blue and propose a safe arrangement supporting area sharing among companions and outsiders in area based applications. In our development, the client's companion set in every companion question submitted to the area servers is isolated into various subsets by the informal organization server arbitrarily. Every area server can just get a subset of companions, rather than the entire companions set of the client as the past work.

These methods of accomplishing area obscurity can be arranged into three kinds

1. Geo location API which was proposed to muddle the genuine area by developing shrouding locales that contain the areas of mysterious clients.

2. DES Encryption strategy is utilized here for the security reason.

3. In expansion, out of the blue, we propose a Location based administrations method which gives check capacity of the looking outcomes came back from area servers in a proficient manner.

ADVANTAGES:

1. The secure arrangement supporting area sharing among companions and outsiders in area based applications.

2. Location sharing development which gives check capacity of the looking outcomes came back from area servers in a productive manner.

IV. ALGORITHM DETAILS

This venture has following modules,

- Geo location API.
- Location based services technique
- AES Algorithm.

ADMINISTRATOR MODULE DESCRIPTION

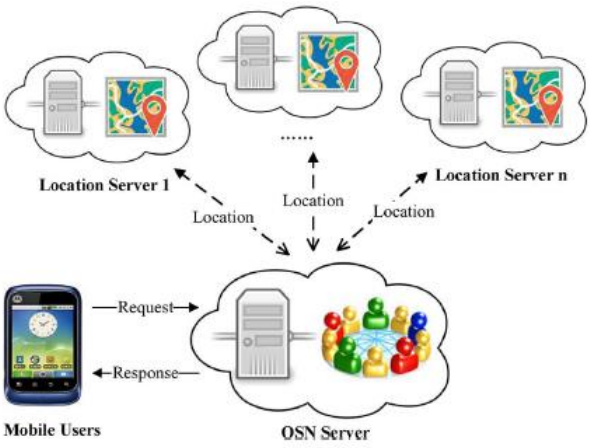
Administrator needs to login by giving username and secret phrases. On the off chance that the username and secret word matches, at that point administrator will see all clients. Administrator used to include area with spot name, unique of that spot and depiction of the spot.

CLIENT MODULE DESCRIPTION

Client right off the bat registers by giving his/her subtleties and after that login with username and secret key. Client can share his/her present area to their companions, with the goal that his/her companion can see his area in encoded group (Inbox). To decode the mutual area, client will send key solicitation to the next client. Client can look through any area by giving the watchword.

In the above two different algorithm are considered. In the first method every node receives traffic with equal intensity for other network also. The part of the total load happens the number nodes and sum of loads in the network along with network when interpreting the results. In the second method, each node obtains the incoming traffic to only two adjacent nodes, thus maintain, the constant total incoming load for each node in various overlays.\

V. ARCHITECTURE



The area protection is in danger by SOSN conniving with unscrupulous clients. The shot of getting to clients' areas is when accepting the reaction from LS in companions what's more, outsiders' area question. Note that, in these answers amid the two phases, the genuine areas are secured by the symmetric/halter kilter encryption plot, which won't release any data to SOSN.

Interpersonal organization Privacy the security of the interpersonal organization is kept from LS by including sham clients into every companion's area inquiry. Along these lines, the interpersonal organization data for each autonomous area question is shielded from LS. Moreover, for every client, distinctive pseudo-IDs will be appointed when the client refreshes his area. Subsequently, for various area inquiries from a similar client U, the pseudoidentity of U as well as the phony personalities of his companions will be unique if every one of them have refreshed their areas. Along these lines, it will be outlandish for LS to get the data from the social organize server. The area servers even don't know which client is presenting the area question since we apply sham area updates and questions to keep LS from knowing which client's genuine phony personality is. In light of the investigation on the previously mentioned two, the relations between client's phony personality and his companions' phony characters are covered up also. At last, we can reason that the protection of the informal organization is safeguarded.

Approved Access in our security model, the area servers and informal organization server are thought to be "honest but inquisitive." Each client characterizes two limit separations for companion's area question and more abnormal's area inquiry. In this manner, on the off chance that the area servers and informal organization server play out the questions in a legitimate manner, the area data and character data of the clients will be ensured with the end goal that lone fulfilled clients' data will be returned as the question result.

EVALUATION:

1) Evaluation on Mobile Device: For the client with versatile gadget, the tasks including Location Updates and Area Query have been tried dependent on the previously

mentioned picked parameters and cryptographic instruments. Area Updates. In this stage, a symmetric key encryption is requested. On the off chance that any client is erased from his companion list, a BE is likewise required. The collectors in the BE are the majority of the client's companions demonstrate the execution times of the AES what's more, BE conspire:

a) Two AES usage are analyzed in, and the end is that the local usage called JNI has preferred productivity over android API, while both fulfill pragmatic necessities.

b) The execution time of BE is appeared in, and we can see that the normal time of encryption is about 1.6 s and that of decoding is about 1.2 s. Since the BE plan is utilized in the key dissemination between companions, it can likewise fulfill the commonsense application. The computational expense for the division of companions' set is immaterial contrasted and the other computational time and in this way is excluded here. As appeared in Fig. 4, we can see that the encryption what's more, decoding times are direct with the quantity of companions. Indeed, even the quantity of companions is greater than 100, the execution time is just 200 ms, and therefore, it is effective and down to earth. Outsiders' Location Query. To present a question for outsiders' areas, the client just needs to present a question moving forward without any more.

2) Evaluation of Location Server: The location server must Work under multithread mode to improve concurrent ability. For LS, the operations include Location updates, Friends' Location Query, and Strangers' Location Query, which are tested. Location Updates. In this phase, the location server decrypts the position encrypted using the BE scheme. The average time of decryption is about 33 ms. Friends' Location Query. The location server encrypts the data containing records of nearby friends. We can see that the execution time is linear with the number of records, for the reason that the user's ID with length less than 10 will be contacted and encrypted by AES-CBC. Strangers' Location Query. Similar to the friends' location query, the location server encrypts all of the ID strings using the AES-CBC model. Therefore, the execution time is linear with the number of records. However, even the number of records is 1000, and the average encryption time is only 30 ms, so that the system is very efficient and practical.

3) Comparison With Other Systems: Until now, there are three normal area sharing frameworks for mOSN: Mobishare in 2012 and our proposed framework. Table II records the examinations of exhibitions among them.

a) About the cell towers. The Mobishare framework employments

cell towers to go about as a confided in focus, and some cryptographic calculation will be kept running in them. Be that as it may, the different frameworks needn't bother with them and make the framework progressively adaptable.

b) About the presentation in a cell phone. Three frameworks have comparable exhibitions. At the point when a client needs to refresh his sharing key, N-Mobi share and our framework will execute when the BE plot, however the Mobi share expects client to execute n-times symmetric encryptions. For this situation, the previous will be progressively adaptable and proficient.

c) About the presentation in the OSN server. To give better security, our framework requires the OSN server to store client's area to multi location servers. Looked at with two different frameworks, our framework must scramble more area data for these servers.

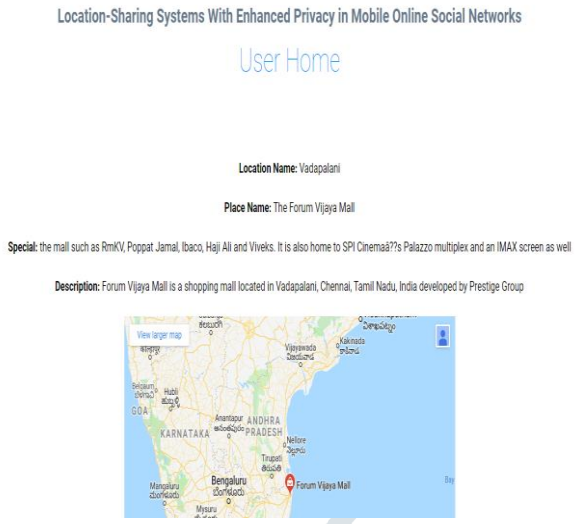
d) About the exhibition in the area server. In our framework, every area server will have a superior execution since it inquiries among the littler informational indexes after separating the areas to multi servers. In actuality, the different frameworks require putting away the majority of the areas into the single server, which is anything but difficult to shape the bottleneck.

VI. RESULTS

1. Security of User's Identity:

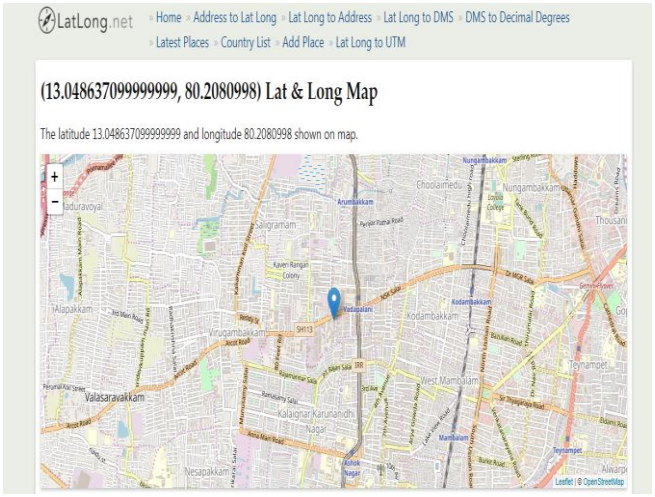
The client's close to home data, counting the client's character and explicit companions' data, ought to be shielded from the area servers. Note that such data does not have to shield from the informal organization server. In this way, we just need to think about what the area servers can get from the collaborations and other put away data. The client's personality has been anonymized by the interpersonal organization server with a pseudo identity each time when the client performs the area update or sends

the adjacent companions' area demand. Along these lines, the area server can't get the genuine character of the client.



2. Protection of User's Friends' Information:

When a client submits companions' area inquiry, the interpersonal organization server will initially include sham client data in the client's genuine companion's set. Moreover, the companion's set with sham clients is additionally partitioned into arbitrary subsets and sent to various area servers. The prerequisite of the quantity of sham clients included into the genuine companions' set ought to be bigger than some predefined number, which may rely upon the quantity of genuine companions and area servers. On the off chance that the number is sufficiently enormous, at that point the complete number of subsets will be sufficiently enormous. Subsequently, every area server can just get some portion of the companion list with sham clients, who can't separate companions from outsiders with no other data. Albeit different solicitations will be sent by the same client, the area server still can't connect them precisely to a similar client on the grounds that the subset allocated to it will be unique with a high likelihood.



CONCLUSION AND FUTURE WORKS

We have tended to the issue of clients' protection against insider assault propelled by the specialist organizations in mOSNs. Two sorts of protection have been considered, including the area protection and informal community security. We have presented another design with different area servers out of the blue and proposed a safe arrangement supporting area sharing among companions and outsiders in area based applications. In our development, the client's companion set in every companion's question submitted to the area servers is separated into different subsets by the informal organization server arbitrarily. Besides, every area server can just get a subset of companions, rather than the entire companions' set. Along these lines, an improved interpersonal organization security against the insider assault can be accomplished. To further secure namelessness, the personality of every client in the inquiry set will be supplanted with a pseudoidentity before sending the inquiry to the area servers.

We have additionally demonstrated that the new development is secure under the more grounded security model with improved protection. At long last, we have given broad trial results to show the effectiveness of our proposed development.

REFERENCES

[1] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud
computing: Architecture, applications, and approaches," *Wireless Commun.*
Mobile Comput., vol. 13, no. 8, pp. 1587–1611, Dec. 2011.

[2] (2010, Apr.) Top Benefits of Location-Based Services. [Online].
Available: http://www.pingmobile.com/blog/top-benefits-of-locationbased-
services/

[3] [Online]. Available: https://foursquare.com

[4] [Online]. Available: https://www.loopt.com

[5] Y.-A. Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique
in the crowd: The privacy bounds of human mobility," in *Nature Sci. Rep.*,
vol. 3, 2013, Art. ID. 1376.

[6] W. Wei, F. Xu, and Q. Li, "Mobishare: Flexible privacy-preserving location
sharing in mobile online social networks," in *Proc. INFOCOM*, 2012,
pp. 2616–2620.

[7] L. Barkhuus and A. K. Dey, "Location-based services for mobile telephony:
A study of users' privacy concerns," in *Proc. INTERACT*, 2003,
vol. 3, pp. 702–712.

[8] J. Li, J. Li, X. Chen, Z. Liu, and C. Jia, "Mobishare+: Security improved
system for location sharing in mobile online social networks," in *Proc.*
5th Int. Workshop MIST, 2013.

[9] Z. Liu, J. Li, X. Chen, J. Li, and C. Jia, "New privacy-preserving location
sharing system for mobile online social networks," in *Proc. 3PGCIC*,
2013, pp. 214–218.

[10] Z. Liu, D. Luo, J. Li, X. Chen, and C. Jia, "N-Mobishare: New privacypreserving
location-sharing system for mobile online social networks,"
Int. J. Comput. Math., 2014.

[11] D. H. Phan, D. Pointcheval, and S. F. Shahandashti, "Adaptive CCA
broadcast encryption with constant-size secret keys and ciphertexts," in
Proc. Inf. Security Privacy, 2012, pp. 308–321.

[12] U. Feige and J. Kilian, "Making games short (extended abstract)," in *Proc.*
29th Annu. ACM STOC, New York, NY, USA, 1997, pp. 506–516.

[13] R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegation of
computation," in *Information Theoretic Security*, ser. ser. Lecture Notes
in Computer Science, A. Smith, Ed. Berlin Germany: Springer-Verlag,
2012, vol. 7412, pp. 37–61.

[14] P. Golle and I.Mironov, "Uncheatable distributed computations," in *Proc.*
Conf. Topics Cryptology—CT-RSA, 2001, pp. 425–440.

[15] M. Bellare and P. Rogaway, "The exact security of digital
signatures—How to sign with RSA and Rabin," in *Proc. EUROCRYPT*,
1996, pp. 399–416.

[16] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil
pairing," in *Proc. ASIACRYPT*, 2001, pp. 514– 532.

[17] Y. Lei, A. Quintero, and S. Pierre, "Mobile services access and payment
through reusable tickets," in *Computer Communications*, vol. 32, no. 4,
pp. 602–610, Mar. 2009.

[18] L. Sweeney, "*K*-anonymity: A model for protecting privacy," *Int. J.*
Uncertainty, Fuzziness Knowl.-Based Syst., vol. 10, no. 5, pp. 557–570,
Oct. 2002.

[19] H. Kido, Y. Yanagisawa, and T. Satoh, "Protection of location privacy
using dummies for location-based services," in *Proc. 21st Int. Conf. Data*
Eng. Workshops, 2005, p. 1248.

[20] A. Khoshgozaran and C. Shahabi, "Blind evaluation of nearest neighbor
queries using space transformation to preserve location privacy," in *Proc.*
SSTD, 2007, pp. 239–257.

[21] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation
for location privacy," in *Proc. PERVASIVE*, 2005, pp. 152–170.
[22] J. Krumm, "Inference attacks on location tracks," in *Proc. 5th Int. Conf.*
PERVASIVE, vol. 4480, LNCS, Berlin, Germany: Springer-Verlag, 2007,
pp. 127–143.
[23] B. Palanisamy and L. Liu, "MobiMix: Protecting location privacy with
mix-zones over road networks," 2011, pp. 494–505.
[24] L. P. Cox, A. Dalton, and V. Marupadi, "SmokeScreen: Flexible privacy
controls for presence-sharing," in *Proc. MOBISYS*, 2007, pp. 233–245.
[25] B. Krishnamurthy and C. E. Wills, "Privacy leakage in mobile online
social networks," in *Proc. WOSN*, 2010, p. 4.

BIBLIOGRAPHY

K. Laxmi Deepthi was born in Telengana, India in 1991.She has received the Diploma in computer Science from TRR Polytechnic college, Hyderabad, India in 2009 and B.Tech degree in Computer Science from Bhoj Reddy College Engineering and Technology for Women. Now, she presently was perusing M.Tech in Computer Networks and Information Security from G.Narayamma Institute of Technology and Science for Women.

Dr. I. Ravi Prakash Reddy pursued his B.Tech from Vasavi College of Engineering, Hyderabad in 1994 and M.Tech from Andhra University, Vizag in 1997. He obtained his Ph.D from JNTU Hyderabad in 2011. He has over 20 years of teaching experience and has 20 research publications to his credit in both National and International Journals. Currently 5 research scholars are pursuing Ph.D under his guidance. He joined GNITS in 2001 and took charge as Head of the department IT in 2011. He is a member of **Editorial Board of Journal of Current Trends in Information Technology**, and also a member of professional bodies such as CSI, ISTE. He is the incharge of computer purchases, maintaence, Internet & Wi-Fi in the Institution.