Improved the Location Privacy Preserving Method in Location based Services using Modified Bloom Filter

Sandeep Yadav
Samrat Ashok Technological Institute
Department of Information Technology
Vidisha, India

Nirmal Gaud
Samrat Ashok Technological Institute
Department of Information Technology
Vidisha, India

ABSTRACT

The increasing technology of smart device used GPS based service for the positing of location. The location of user and server disclose the actual position of location. The actual location of position faced a problem of threats. The privacy of real position of server and user is major issue in GPS enabled smart devices. In this paper proposed location privacy preservation algorithm using improved bloom filter. Bloom filter is basically data structure and map the single bit information. The proposed method based on two basic processing feature of GPS area of interest (AOI) and position of interest (POI). The proposed algorithm validated the real location of privacy preservation. The proposed algorithm preserves location privacy at low computational and communication cost.

Keywords

LBPS, privacy preserving, bloom filter, Google map

1. INTRODUCTION

The advancement of mobile devices loaded with totally different options of facility such as positioning capability and location primarily based capability will increase the demand of market worth. The placement primarily based services impact the lifestyle of human like looking a nearest ATM machine, hospital, school and lots of a lot of things associated with lifestyle activity. History of locations, or location birthplace, is that the history of locations traveled by a user. The birthplace of location could be a crucial demand in path vital situations [1, 2]. A sound claim of travel path must be valid solely in terms of the placement birthplace of the travel. The integrity of a product is also extremely even by the availability chain and also the inter-mediate locations that a product travels, because it is transported from the manufacturer to the hands of the ultimate client. Location presence and generating proof of presence need the data to be valid and unrestricted at a later time, specified it are often used as a secure token of proof. However, birthplace for location could be a continuous method [8, 9]. The birthplace records need location birthplace to be preserved, because the user travels around assembling location proofs. Moreover, in contrast to the final information things, the sequence, within which the locations are traveled, must be preserved in written record order among the birthplace. As a result, birthplace for location proofs portrays a larger challenge than that for general information things. a standard application state of affairs of location-based services re-quires the service supplier to find out once the user is near some sensitive or attention-grabbing locations. This can be the case, for example, of "around-me" applications or security and military systems [6]. During this case, the placement of the user ought to be unbroken non-public for as long as she is way from one among the areas of interest, and find disclosed to the service supplier only she enters one such space. The same downside, called non-public proximity take look acting has been studied in privacy analysis literature: Alice will test if she is near Bob while not either party revealing the other data concerning their location [26]. Currently a day's numerous authors used numerous organization and data processing approach for the privacy suffusion of location. During this paper changed by the conception of entropy of user question and method value primarily based location manipulation for the process of user request [12]. In section 2 discuss the connected work and in section 3 discuss the bloom filter. In section 4 discuss the projected methodology. In section 5 discuss the experimental result and at last discuss conclusion and future add section 6.

2. RELATED WORK

In this section discuss the related work in the field of location based privacy preservation using different approach for the purpose of security. The location based smart device increases the rehabilitee of interest but not reliability of interest.

Authors [1] introduce Encore, a mobile platform that builds on secure encounters between pairs of devices as a foundation for privacy-preserving communication. An encounter occurs whenever two devices are within Bluetooth radio range of each other, and generates a unique encounter ID and associated shared key. Encore detects nearby users and resources, bootstraps named communication abstractions called events for groups of proximal users, and enables communication and sharing among event participants, while relying on existing network, storage and online social network services. At the same time, Encore puts users in control of their privacy and the confidentiality of the information they share. Using an Android implementation of Encore and an app for event-based communication and sharing, we evaluate Encore's utility using a live tested deployment with 35 users.

[2] Authors discuss present OTIT a model for designing secure location provenance. We formalized the features and characteristics for the domain of secure location provenance schemes, using formal propositional logic and logical proofs. We also present several schemes, which can be used in various modes to provide secure location provenance services. Based on the characteristics defined in OTIT, we have analyzed different schemes to show their adherence to the desired features of secure location provenance. Furthermore, we present experimental results on the performance of the various schemes, in terms of time and storage, to show a comparative applicability analysis.

Authors [3] Based on DHT network, using RSA key agreement with the state, BF combination with B + tree search algorithm, Sync data update algorithm, proposed a cloud storage system for secure file sharing solution, to enhance the security of cloud data storage environments, ensure their privacy, integrity. Among them, the homomorphism key agreement allows authorized users get more control key and in order to achieve the purpose of file sharing. SP in the key negotiation process completely unable to get control of the key information to ensure the privacy of user data. When using DHT network and other errors Shamir secret sharing algorithms such loss or malfunction occurs in the network, you only need to re-select other nodes to obtain data, without the use of retransmission mechanism to improve the resource utilization.

[4] Authors present a survey of this emerging field. Basic concepts of SAN are introduced. We intend to generalize the widely-used social properties in this regard. The state-of-the-art research on SAN is reviewed with focus on three aspects: routing and forwarding, incentive mechanisms and data dissemination. Some important open issues with respect to mobile social sensing and learning, privacy, node selfishness and scalability are discussed. Socially-aware networking is going to be a new hotspot of research on network science and engineering. The close connection between ubiquitous mobile devices and the users' social relationships attracts researchers to explore the potential of introducing social properties into network design.

Authors [5] identify different design dimensions of pervasive computing middleware and investigate their use in providing various system services. In-depth analysis of the system services has been carried out and middleware systems have been carefully studied. With a view to aid future middleware developers, we also identify some challenging open research issues that have received little or no attention in existing middleware solutions. They investigated a large number of disparate Pac middleware solutions and infer that Pac middleware helps the programmer develop applications in several ways.

[6] Authors discuss the aim to provide a clear categorization on safety challenges and a deep exploration over some recent solutions in MSNs. This work narrows the safety challenges and solution techniques down from Opponents and delay-tolerant networks to MSNs with the hope of covering all the work proposed around security, privacy, and trust in MSNs. To conclude, several major open research issues are discussed, and future research directions are outlined. The concept of MSNs is a novel social communication paradigm that exploits opportunistic encounters between human-carried devices and social networks. Like any other emergent archetype of technology, MSNs demand time to be totally safe and immune.

[7] Authors present a survey of security and privacy preserving issues in M2M communications in Cyber-Physical Systems. First, we discuss the security challenges in M2M communications in wireless networks of Cyber-Physical Systems and outline the constraints, attack issues, and a set of challenges that need to be addressed for building secure Cyber-Physical Systems. Then, a secure architecture suitable for Cyber-Physical Systems is proposed to cope with these security issues. Eventually, the corresponding countermeasures to the security issues are discussed from four aspects: access control, intrusion detection, authentication and privacy preserving, respectively. Along the way we highlight the advantages and disadvantages of various existing security schemes and further compare and evaluate these schemes from each of these four aspects.

[8] Authors investigate the research progress in RFID with anti-collision algorithms, authentication and privacy protection protocols, localization and activity sensing, as well as performance tuning in realistic settings. We emphasize the basic principles of RFID data management to understand the state-of-the-art and to address directions of future research in RFID. As a key technology of automatic identification, RFID has attracted increasing attention in recent years. In this article, we have discussed several research challenges and opportunities, and provided an overview of existing solutions, including anti-collision algorithms, authentication and privacy protection protocols, localization and activity sensing, as well as performance tuning in realistic settings.

Authors [9] present security requirements, challenges and existing authentication schemes in WSN. WSN finds applicability in many domains and hence information gathered is sensitive and should be held confidential. To achieve this confidentiality, authentication of node is necessary. Many schemes proposed on authentication and some of the significant ones are discussed in this paper. While most authentication schemes are focus only on the security while other major compelling challenges for authentication is to provide proper scalability, reduced communication and computation overhead.

3. BLOOM FILTER

A Bloom filter (BF) is a data structure that represents a set of elements in a space-efficient manner. A BF generated for a specific set allows membership queries on the originating set without knowledge of the set itself. The BF always determines positively if an element is in the set, while elements outside the set are generally determined negatively, but with a probabilistic false positive error [14].

Definition 1. We define a Bloom alter B(S) representing a set

$$\mathrm{S} = \{a_{1,\dots\dots\dots,}a_1\} \subseteq \{0,1\}^* \quad \text{as the set}$$

$$\mathrm{B(S)} = \bigcup_{a\in S, h\in H} h(a) \qquad (1)$$

Where H = $\{h_1, h_k\}$ is a set of *k* hash functions such that each h_i ∈ H: $\{0,1\}^*$ → {1, m}, that is, the hash functions take binary strings as input and output a number uniformly chosen in {1, m}.

A Bloom alter B(S) can be represented as a binary vector b composed of *m* bits, where the it bit

$$\mathrm{b}[I] = \begin{cases} 1 & if \quad i \in B(S) \\ 0 & if \ i \notin B(S) \end{cases} \qquad (2)\ .$$

The bloom alter is built as follows. Initially all bits are set to 0. Then, for each element a ∈ S and for each h ∈ H we calculate h (a) = *I*, and set the corresponding *i*t bit of b to 1. Thus, m bits are needed in order to store b.

We test an element a_u against b to determine membership in S, that is, we verify whether a_u ∈ S if

$$\forall \mathrm{h} \in \mathrm{H},\ \mathrm{b}\ [\mathrm{h}\ (a_u)] = 1 \qquad (3)$$

If any bit in b that corresponds to a value output by one of the hash functions for a_u is 0, then a_u ∈ S. If, instead, all the hashes map to bits of value 1, then a_u ∈ S minus a false positive probability p determined by the number *n* of elements in S, the number *k* of hash functions in H and the maximum possible value m output by the hash functions (equal to the binary length of b) as follows:

$$p = \left(1 - (1 - \tfrac{1}{m})^{kn}\right)^k \approx (1 - e^{-\frac{kn}{m}})^k \qquad (4)$$

This small false positive probability is due to the potential collision of hashes evaluated on different inputs, resulting into all bits associated to an element outside the originating set having value 1. As such, it is determined largely by k: if k is sufficiently small for given m and n, the resulting b is sufficiently sparse and collisions are infrequent. If we consider the approximation in (4), we can calculate the optimal number of hashes k as

$$opt\ (k) = \frac{m}{n}\ In\ 2, \qquad (5)$$

From which we can infer

$$m\ = \left[-\ \frac{n\ ln\ p}{(\ln 2)^2}\right] \qquad (6)$$

However, the number of hashes also determines the number of bits read for membership queries, the number of bits written for adding elements to the altar, and the computational cost of calculating the hashes themselves. Therefore, in constrained settings, we may choose to use a less than optimal k, according to performance reasons, if the resulting p is considered sufficiently low for the specific application domain.

4. PROPOSED METHOD

In this section discuss the improved bloom filter for the location privacy preservation. Here modified the vector counter of the location the value of M-counter stored in the vector with the index value of an incoming query and server proceeds data. The value of query generated transforms location of same query and send to server for the processing. Transform location is basically a validation point of area of interest and position of interest. The size of LBP vector is subtracted by the size of M*k matrix. it is a maximum limit for accepting query[18]. After getting the value of transform counter check the maximum frequent change value of transform. In this time duration compute the maximum change frequent value of the M-counter and generate the near location according to the query. For the processing of algorithm some notation is used. The used notation describes in table.

Notation	Description
M	The value of counter for the processing of query
E	The frequency of user query
H(x)	Index of processing query
LBP	Location based processing
T	Transformation value of POI
SA	Result Query on user side.
POI	Point of interest in MAP
AOI	Area of interest in MAP
N	Number of user processing

The proposed algorithm describes in two sections, in first section describe the input query transformation process and second process discuss the search space of query according to their point of interest according to their location map.

I. The transformation process map the user selected and search location in coordinate system in terms of geo location (x, y). The value of coordinate map according to the LBP matrix table. The value of matrix changes the value of coordinate according to their location. The algorithm steps given below.

1) Input LBP= (user selected query, AOI, POI)

2) Output SA= H(X), (Xu,Yu) here X and Y u user location coordinate

3) Randomly assigned the coordinate matrix according to the coordinate

4) Transform the coordinate value according to counter value M

T= {Xu, YU→ X1, X2} and forwarded to H(X)

5) Map H(X) into M

6) Count the value of M counter

7) Store the value of M and calculate frequency of query

8) E= {query frequency}

II. The retrieval of query result map the coordinate system and search the result in search space and measure the frequency of query and processing cost.

1) Creates the query frequency counter with location Matrix.

2) Decode the coordinate H(x)

DH=1-H(X) here DH is decoded index

3) Compute the coordinate of MAP location of transform T

4) Get real coordinate of transform location

5) Measure the value of POI

6) Gets query result.

5. EXPERIMENTAL RESULT ANALYSIS

For the validation of proposed method for privacy preservation used Google map and java software for the processing of location and position. Also design the android application for the accessing of query and measure some value of cost in terms of time and processing cost [22].

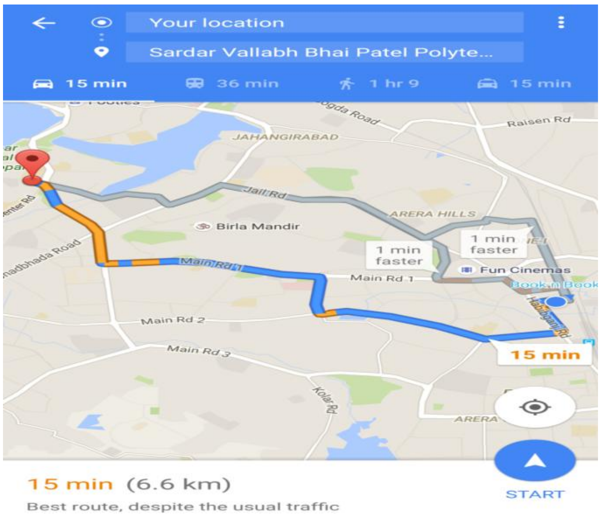

Figure 1 given window represented path from source to destination point SV Polytechnic of User Polytechnic in the program

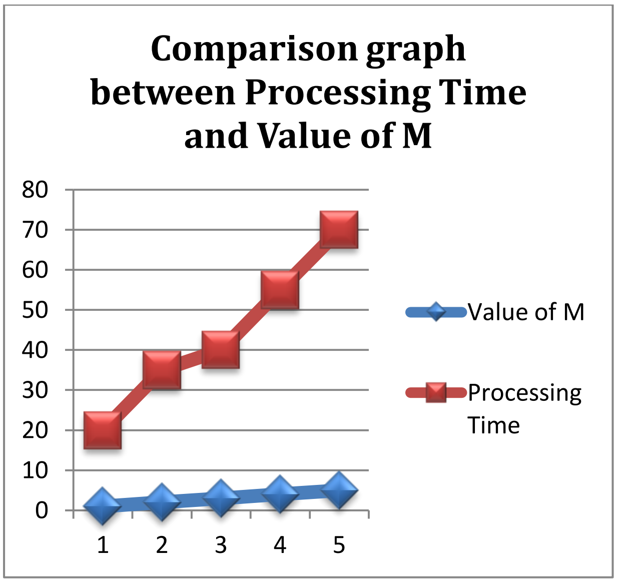

Figure 2 shows that the processing time and value of M with bloom counter according to the query on the Google map form the retrieval of location during server

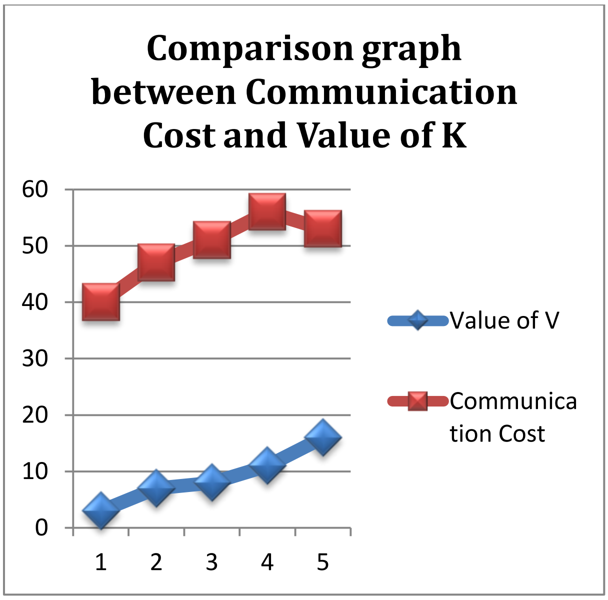

Figure 3 shows that the processing time and value of V with improved bloom counter according to the query on the Google map form the retrieval of location during server

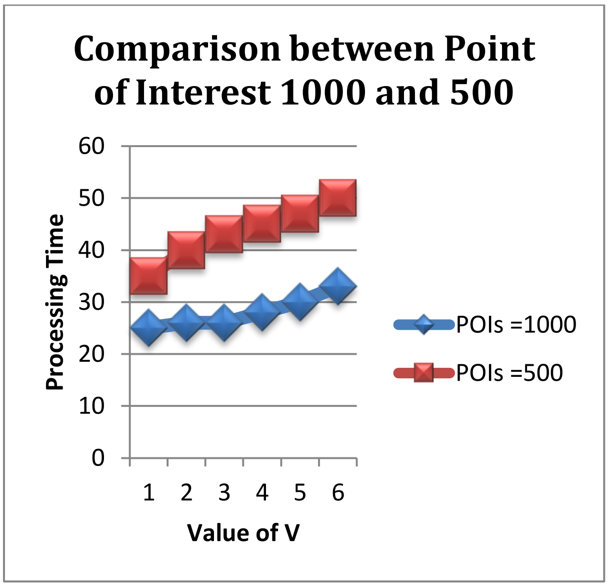

Figure 4 shows that the comparison of 500 POIs and 1000 POIs with parameter of processing time and value of V with bloom counter according to the query on the Google map form the retrieval of location during server

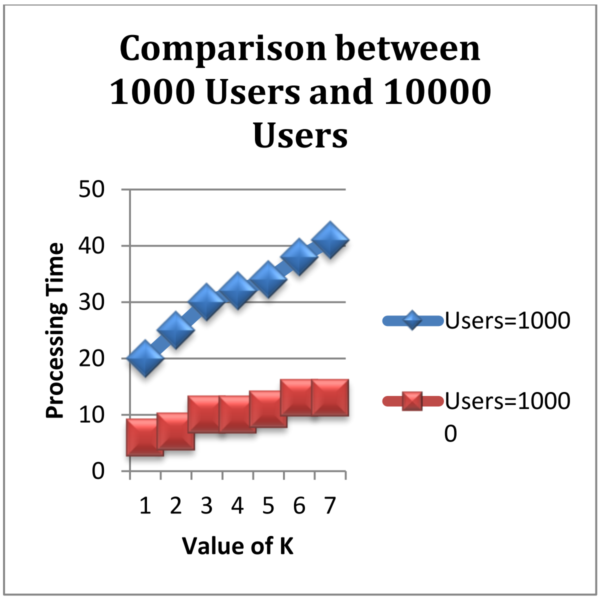

Figure 5 shows that the comparison of 1000 Users and 10000 Users with parameter of processing time and value of V with bloom counter according to the query on the Google map form the retrieval of location during server

6. CONCLUSION & FUTURE SCOPE

In this paper modified the bloom filter for the processing of privacy preservation in location based services. The proposed method is very efficient for the location and position privacy. The proposed algorithm used the value of counter for the process of user location query according. The transform value of query produces the near value of user location and preserves the real location of user. A key feature of the system is that we get rid of the fully trusted entities to provide enhanced security. It is not expected that the stronger privacy guarantee will result in much higher cost. Extensive evaluations suggest that our proposed scheme preserves location privacy at low computational and communication cost. In our future work, we will improve our scheme by deploying multiple counters to avoid the potential bottleneck between the users and the spatial location and ensure the high security of the system.

7. REFERENCES

[1] Paarijaat Adyta, Viktor Redeye, Matthew Lentz, Elaine Shi, Bobby Bhattacharjee and Peter Druschel “Encore: Private, Context-based Communication for Mobile Social Apps”, International conference on Mobile systems, applications, and services, 2014, Pp 135-148.

[2] Rasa Khan, Shams Zeroed, Mad Mineral Hague and Raga Has an “OTIT: Towards Secure Provenance Modeling for Location Proofs”, Information, computer and communications security, 2014, Pp 87-98.

[3] Shunning Lu and Goofing Sheen “A Novel Safe File Sharing Method Based on Cloud Storage Structure in DHT Networks”, International Journal of Security and Its Applications, 2015, Pp 189-200.

[4] Fang Xia, Li Liu, Jibe Li, Xinhua Ma and Athanasius V. Vasilakos “Socially-Aware Networking: A Survey”, IEEE, 2013, Pp 1-18.

[5] Vassar Raychoudhury, Japanning Cao, Mohan Kumar and Daring Zhang “Middleware for pervasive computing: A survey”, journal Pervasive and Mobile Computing, 2013, Pp 1-24.

[6] Asher Najaflou, Beerhouse Javari, Fang Xia, Laurence T. Yang and Mohammad S. Obadiah “Safety Challenges and Solutions in Mobile Social Networks”, IEEE, 2013, Pp 1-21.

[7] Dong Chen and Guerin Chang “A Survey on Security Issues of M2M Communications in Cyber-Physical Systems”, KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, 2012, Pp 24-45.

[8] Lei Xian, Member, Aveng Yin, Athanasius V. Vasilakos and Single Lu “Managing RFID Data: Challenges, Opportunities and Solutions”, IEEE, 2014, Pp 1-18.

[9] Santali Patel, Dr Vijay Kumar B P, Somali Singh and Rashique Jamal “A Survey on Authentication Techniques for Wireless Sensor Networks”, International Journal of Applied Engineering Research, 2012, Pp 1-4.

[10] Yao Zhen, Ming Li, Wending Lou and Y. Thomas Hour “Location Based Handshake and Private Proximity Test with Location Tags”, IEEE, 2015, Pp 1-14.

[11] Xingjian Chen, Kia Make, Kang Yen and Nike Passion “Xingjian Chen, Kia Make, Kang Yen, and Nike Passion”, IEEE, 2009, Pp 52-73.

[12] Paarijaat Adyta, Bobby Bhattacharjee, Peter Druschel, Viktor Redeye and Matthew Lentz “Brave New World: Privacy Risks for Mobile Users”, Security and privacy in mobile environments, 2014, Pp 1-5.

[13] Rasa Khan and Raga Has an “SecP2PSIP: A Distributed Overlay Architecture for Secure P2PSIP”, ASE, 2014, Pp 1-12.

[14] Keen Sung, Brian Neil Levine and Marc Liberator “Location Privacy without Carrier Cooperation”, IEEE, 2014, Pp 1-10.

[15] Ming-Chin Chuang and Jeng-Farn Lee “TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks”, IEEE, 2013, Pp 1-10.

[16] Yao Zhen, Ming Li, Wending Lou and Y.Thomas Hour “SHARP: Private Proximity Test and Secure Handshake with Cheat-Proof Location Tags”, Springer Berlin Heidelberg, 2012, Pp 1-18.

[17] Iris A. Jungles and Richard T. Watson “LOCATION-BASED SERVICES”, COMMUNICATIONS OF THE ACM, 2008, Pp 65-70.

[18] Lenin Ravindranath, Jitendra Paddy, Shared Agawam, Retool Mahakam, Ian Obermiller and Shahn Shayandeh “AppInsight: Mobile App Performance Monitoring in the Wild”, USENIX Symposium on Operating Systems Design and Implementation, 2012, Pp 107-120.

[19] Jibe Liu, F. Richard Yu, Chung-Horn Lung and Helen Tang “Optimal Combined Intrusion Detection and Biometric-Based Continuous Authentication in High Security Mobile Ad Hoc Networks”, IEEE, 2009, Pp 806-815.

[20] L. Garc´es-Erice, P.A. Feebler, E.W. Bier sack, G. Purvey-Keller and K.W. Ross “Data Indexing in Peer-to-Peer DHT Networks”, EURECOM, 2003, Pp 1-12

[21] J.A. Powel’s, P. Garbacki, D.H.J. Edema, H.J. Sips “THE BITTORRENT P2P FILE-SHARING SYSTEM:

MEASUREMENTS AND ANALYSIS", IEEE, 2006, Pp 1-6.

[22] Stephen Void, W. Keith Edwards, Mark W. Newman, Rebecca E. Granter and Nicolas Ducheneaut "Share and Share Alike: Exploring the User Interface Affordances of File Sharing", ACM, 2006, Pp 1-10.

[23] Keith Cheers, Gareth Smith, Keith Mitchell and Nigel Davies "Exploiting Context to Support Social Awareness and Social Navigation", ACM, 2000, Pp 512-518.

[24] Kay Roomer, Oliver Chasten and Friedman Matter "Middleware Challenges for Wireless Sensor Networks∗" NCCR-MICS, 2001, Pp 1-2.

[25] Don Carney, Our Çetintemel, Mitch Cherniack, Christian Convey, Sang Don Lee, Greg Sideman, Michael Stonebreaker, Newsome Tactful and Stan Sonic "Monitoring Streams – A New Class of Data Management Applications", VLDB Conference, 2002, Pp 1-12.

[26] Alastair R. Beresford and Frank Stefano "Location Privacy in Pervasive Computing", IEEE, 2003, Pp 46-55.