ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152

www.ijmece .com

Vol 9, Issue.2 May 2021

PRIVACY PRESERVING THE GENERAL AREA OF REGION OF THE ENTITY USING SPATIOTEMPORAL MOBILITY

Shyam Prasad Teegala

Assistant Professor Department of IT

shyam.tprasad@gmail.com

B V Raju Institute of Technology Narsapur

Abstract

In the paper, the main focus is on privacy-aware systems, and a new architecture is proposed to address privacy concerns, specifically regarding location privacy. The proposed architecture incorporates two methods: spatiotemporally-based anonymization and location information disturbing. The spatiotemporally-based anonymization method involves dividing space and time into smaller units or pieces. When an entity transitions from one domain to another, its identification (ID) is refreshed. This approach helps in preserving the person's location privacy by ensuring that there is no direct association or continuity between the entity's ID in different domains. This technique makes it difficult for an observer to track or link the entity's movements across different locations and times. The location information disturbing method aims to introduce variability or obfuscation into coordinate data to further protect privacy. Two specific approaches are mentioned: transferring coordinates to random data and transferring coordinates to fixed data. This method involves replacing the original coordinate data with random values. By doing so, the exact location of the entity is obscured, making it challenging to discern the entity's actual whereabouts. In this method, the original coordinate data is transformed into fixed values. It is unclear from the provided information how the fixed values are determined, but this approach may involve mapping coordinates to predetermined or predefined locations. The purpose is to obfuscate the precise location information while still preserving the general area or region of the entity.

Keywords: 1. Spatiotemporally 2. Anonymization 3. Identification 4. Privacy aware systems

1.0 Introduction

Privacy-preserving techniques in ubiquitous computing aim to protect users' sensitive information and maintain their privacy in a pervasive computing environment where computing devices are seamlessly integrated into everyday life. Privacy has been a significant concern in

the context of ubiquitous computing. The seamless integration of computing and communication technologies in a ubiquitous computing environment can potentially lead to extensive data collection, tracking, and surveillance, raising privacy risks for individuals. As a result, privacy concerns have been identified as one of the primary barriers to the success and adoption of context aware computing. The pervasive nature of computing devices and the constant collection of personal data can erode individuals' privacy and give rise to various privacy-related challenges. Ubiquitous computing environments generate vast amounts of data, often collected without individuals' explicit consent or awareness. This raises concerns about the collection and retention of personal information, including location data, behavioral patterns, and preferences. Ubiquitous computing systems may involve sharing and aggregating personal data among multiple entities. The potential for data sharing without individuals' knowledge or control raises concerns about secondary uses of data and the creation of comprehensive user profiles. The continuous monitoring and tracking capabilities of ubiquitous computing systems can intrude upon individuals' privacy and result in the collection of sensitive information about their activities, movements, and behaviors. This can lead to concerns about constant surveillance and potential misuse of collected data. The integration of diverse data sources in a ubiquitous computing environment may increase the risk of re-identifying individuals even if their personal information is anonymized or pseudonymized. This poses challenges to maintaining true anonymity and protecting individuals' identities.

1.1 Privacy in Ubiquitous computing environments

Ubiquitous computing environments often involve collecting and analyzing contextual information, such as health data, personal preferences, or social interactions. Preserving privacy in such contexts requires considering the sensitivity of different types of data and implementing privacy safeguards accordingly. Addressing these privacy concerns in ubiquitous computing requires a multidimensional approach that combines technical, legal, and user-centric considerations. Transparent data practices, and user empowerment through informed consent and privacy settings are some of the strategies employed to mitigate privacy risks.

Privacy in a ubiquitous computing environment refers to the protection of individuals' personal information and their ability to control how their data is collected, used, and shared within the context of pervasive computing. Retention and processing of personal data to what is necessary for the intended purpose. Avoid collecting excessive or unnecessary information to minimize privacy risks. Clearly communicate the scope, and duration of data collection, as well as any sharing or processing practices, to ensure individuals are aware of and can make informed decisions regarding their privacy.

Empower users to exercise control over their personal data. Provide options for users to specify their privacy preferences, including the ability to opt-in or opt-out of data collection, choose data

sharing settings, and manage data retention periods. Apply techniques such as anonymization or pseudonymization to protect individual identities when collecting and analyzing data. Ensure the use of secure communication protocols (e.g., encryption) when transmitting and storing personal data. This protects the confidentiality and integrity of the information and prevents unauthorized access. Integrate privacy considerations into the design and development of ubiquitous computing systems from the outset. Adopt privacy-preserving technologies, follow privacy best practices.

Be transparent about data practices, including data collection, usage, sharing, and retention policies. Provide clear and easily accessible privacy policies that explain how personal data is handled, and regularly update users on any changes to those policies. Conduct regular audits to ensure compliance with privacy regulations and internal privacy policies. Promote user education and awareness regarding privacy risks and best practices. Educate users about the importance of privacy, how their data is used in ubiquitous computing environments, and provide guidance on safeguarding their privacy. It's essential to note that privacy in ubiquitous computing is an ongoing challenge, and there are often trade-offs between privacy and functionality..

2.0 Ubiquitous Security Architecture

A ubiquitous security architecture refers to a comprehensive framework that aims to provide security across all aspects of a ubiquitous computing environment. It involves the integration of various security mechanisms and protocols to protect the confidentiality, integrity, and availability of data and services in a pervasive computing ecosystem.

Authentication and Access Control: This component focuses on verifying the identities of users and devices in the system and granting appropriate access rights. Secure communication protocols, such as Transport Layer Security (TLS) or IPsec, are employed to encrypt data transmission and protect it from eavesdropping, tampering, or unauthorized interception. This component ensures the confidentiality and integrity of data exchanged between devices or over networks.Data protection mechanisms involve techniques such as encryption, data masking, and tokenization to safeguard the confidentiality of sensitive information stored on devices or transmitted across the ubiquitous computing environment.

Trust management encompasses mechanisms for establishing and managing trust relationships among devices and entities in the system. It involves evaluating the trustworthiness of devices, verifying the authenticity of communications, and managing trust levels to make informed decisions about granting access or sharing resources.

Security Monitoring and Intrusion Detection: Continuous monitoring of the ubiquitous computing environment is essential to detect and respond to security incidents promptly. Intrusion detection systems (IDS) and security monitoring tools help identify unauthorized activities, anomalies, or potential attacks, enabling timely mitigation measures. Establishing and enforcing security policies is crucial to maintain a secure ubiquitous computing environment. Policies define rules and guidelines for data access, sharing, usage, and behavior of entities within the system. Enforcement mechanisms ensure compliance with these policies, detecting and addressing violations.

Physical Security: Physical security measures protect the physical infrastructure of the ubiquitous computing environment, including devices, sensors, networks, and data centers. It involves measures such as secure hardware design, tamper-resistant devices, surveillance systems, and access controls to prevent unauthorized physical access or tampering. Privacy-preserving mechanisms and techniques, as discussed earlier, are integrated into the security architecture to protect individuals' personal information and ensure compliance with privacy regulations. This includes anonymization, consent management, data minimization, and user-centric privacy controls.

Incident Response and Recovery: This includes processes for incident detection, containment, eradication, and system restoration to minimize the damage caused by security breaches. Promoting security education and awareness among users and stakeholders is essential to foster a security-conscious culture. Training programs, guidelines, and best practices help users understand their roles and responsibilities in maintaining a secure ubiquitous computing environment. It's important to note that a ubiquitous security architecture should be adaptable and scalable to accommodate evolving security threats and technologies.

2.1 Spatiotemporal Mobility

Researchers have put a lot of effort into developing analogous solutions for protecting trajectory privacy in response to the aforementioned necessity.

Anonymity is a significant aspect of the scheme. Users remain anonymous during querying, applying, and utilizing services, with only RSNs (presumably Random Serial Numbers) used to represent users. Additionally, a spatiotemporally-based anonymous matching strategy allows for changing RSNs. The scheme also replaces users' actual coordinates with fake ones during service matching, further enhancing anonymity.

The scheme ensures protection of user preferences by requiring user preference input only during the authentication step. It assumes that the authentication center is trustworthy, suggesting that user preferences are securely handled and not compromised.

While these properties highlight the potential security benefits of the proposed scheme, it is important to subject it to a thorough security and privacy analysis to ensure its effectiveness and robustness. Such an analysis should consider potential vulnerabilities, threats, and attacks that could compromise the system's security and privacy objectives. Additionally, an evaluation of the scheme's compliance with relevant privacy regulations and standards should be performed.

The spatiotemporally-based anonymous matching strategy described in the proposed scheme aims to enhance privacy by periodically updating an individual's random data stream and distributing a new data stream to represent the person. This strategy involves dividing time into intervals and carving the entire domain into specific areas. This process invalidates the old random data stream and ensures that there is no direct connection between the previous and new data streams. The intention behind this strategy is to mitigate long-term attacks targeting a specific individual. By regularly updating the random data stream and introducing a new representation, it becomes inefficient for an attacker to persistently track or identify an individual over an extended period.

It's important to note that achieving spatiotemporally-based anonymity is a challenging task, and the level of anonymity achieved may depend on the specific techniques and parameters used. The balance between privacy and data utility needs to be carefully considered, as excessive anonymization may result in reduced data usefulness for analysis or services. Additionally, the legal and ethical aspects of data anonymization should also be taken into account, ensuring compliance with relevant regulations and guidelines.

The focus is on protecting user trajectory privacy in the context of Location-Based Services (LBSs). While LBSs offer convenience, the collection of location data raises concerns about privacy. Trajectory k-anonymity is identified as an important technology to protect user trajectory privacy, but it is observed that user attributes are often not adequately, rendering user trajectories vulnerable. Spatiotemporal Mobility (SM) measurement is to assess user characteristics. This improvement in privacy preservation is achieved while maintaining the same quality of services. The importance of considering user attributes and their relationship with trajectories when aiming to protect trajectory privacy. The proposed MTPPA algorithm offers a potential solution by leveraging the SM measurement and trajectory graph modeling. However, it is crucial to critically evaluate the algorithm's effectiveness, efficiency, and potential limitations, as well as assess its robustness against privacy attacks or inference techniques. Additionally, the compliance of the proposed algorithm with privacy regulations and ethical considerations should be thoroughly examined.

The development of 5G technology has made location-based services (LBSs) more common in our daily lives. The user's trajectory data has, however, been stored by these service providers. A significant quantity of the user's private information, such shopping preferences, home address,

ISSN2321-2152

www.ijmece .com

Vol 9, Issue.2 May 2021

place of employment, or regularly frequented locations, is contained in the trajectory data. It would expose the user's private information as a result. Therefore, a method to safeguard user trajectory data is required for greater privacy. One of the crucial methods lately employed to shield a user's trajectory is k-anonymity. Similar trajectories combine to create the k-anonymity set, which is then given to the service providers, where k stands for the level of anonymity. However, creating an effective k-anonymity set is difficult since the attacker might take into account. The majority of the methods now in use for creating the k-anonymity set take the direction similarity between trajectories into account [6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]. These approaches, however, disregard the fact that various users have unique characteristics and movement patterns. The trajectories produced by various user attributes are highly dissimilar

The user may visit the grocery, the park, the neighbourhood, or any other places as stopovers. Even with the anonymity provided by the SM, the attacker can still identify the trajectory. Figure 1 depicts the daily movement patterns of two users. Alice and Bob's respective trajectories are those with the red and green colouring, respectively. Alice makes a number of stops at different places throughout the area. She moves relatively quickly on average. It is simple to assume that her daily movement pattern is erratic and unpredictable. Bob, on the other hand, only makes stops in two different places. He travels less frequently than Alice. He moves slower on the whole. His daily movement pattern is thought to be more predictable and predictable, and fixed. It is determined that Alice has greater mobility than Bob. Once the attacker discovers Bob is an employee of a company using data mining techniques, the attacker will readily filter out this trajectory with high mobility in the anonymity set if the trajectory k-anonymity set given by Bob contains a trajectory created by Alice.

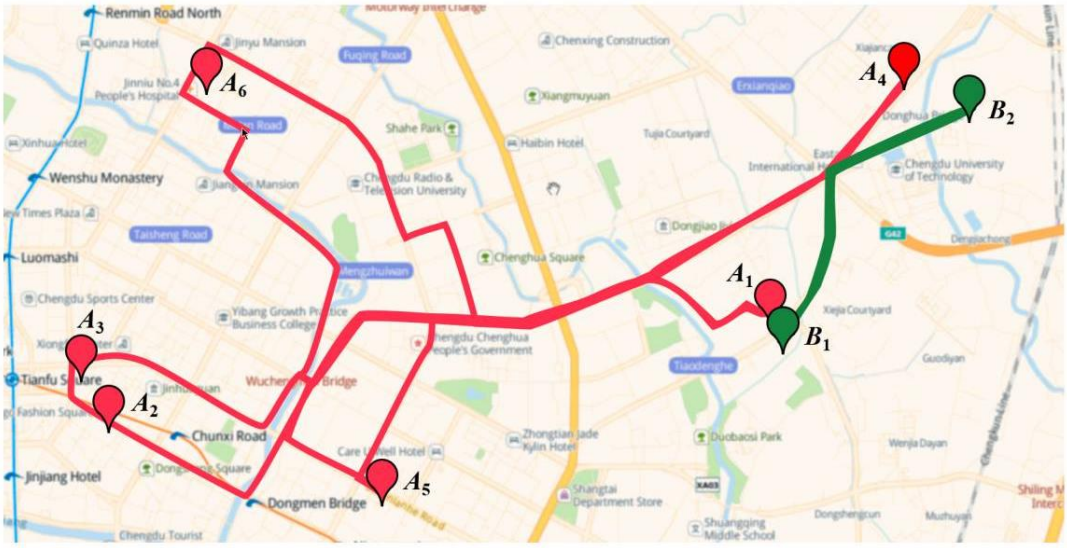

Fig 1. spatiotemporally-based anonymity

ISSN2321-2152

www.ijmece .com

Vol 9, Issue.2 May 2021

The majority of the methods now in use for creating the k-anonymity set take the direction similarity between trajectories into account [6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]. These approaches, however, disregard the fact that various users have unique characteristics and movement patterns. The trajectories produced by various user attributes are highly dissimilar.

3.0 Spatiotemporally-based Trajectory

Definition 1.

A user's trajectory, denoted as T, is represented as a polyline in three-dimensional space. It consists of a sequence of sampling points accessed over time. Each sampling point (xi, yi, ti) represents the user's coordinates (xi, yi) at a specific sampling time ti.

Equivalence Class: Given a starting timestamp ts and an ending timestamp te, trajectories Ti and Tj are considered part of the same equivalence class if all their sampling points fall within the time interval [ts, te]. In other words, if the sampling points of Ti and Tj exist within the same time range, they are grouped together as an equivalence class.

Synchronized Trajectories: If trajectories Ti and Tj from an equivalence class have the same number of sampling points and cover the same sampling time length, they are referred to as synchronized trajectories. Essentially, synchronized trajectories have identical lengths and contain sampling points that correspond to the same time instances.

Synchronized Trajectory Set: A synchronized trajectory set refers to a collection of trajectories in which any two trajectories from the set are synchronized. This set consists of trajectories that exhibit the same time duration and have the same number of sampling points.

Definition 2

The stopover S of a user denotes a particular site or location where the location is functional, beneficial, or relevant to the user (for example, a bus station, a market, or even the user's homesite).

Definition 3

The total number of stopovers N and the average movement speed v of a user's trajectory are used to calculate their spatiotemporal mobility M. The ratio of the trajectory's entire length to its total moving time, given in Equation (1), determines the average moving speed v in the time range [t1, tn]:

$$\bar{v} = \frac{\sum_{i=1}^{n-1} \sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2}}{t_n - t_1}. \quad (1)$$

After applying the normalization process the SM

ISSN2321-2152

www.ijmece .com

Vol 9, Issue.2 May 2021

$$M = \alpha \frac{N}{n} + \beta \frac{\bar{v}}{v_{max}}, \tag{2}$$

Definition 4

Kinematic Similarity. The similarity of two synchronised trajectories is assessed using their SM differences. Allow the SM of the two users' synchronised trajectories, Mi and Mj. The absolute value of the difference between Mi and Mj is defined as the mobility difference between Ti and Tj and is as follows:

$$\Delta M\left(T_i, T_j\right) = |M_i - M_j| \tag{3}$$

where, ΔM(Ti,Tj)∈[0,1].

Definition 5

Graph of Trajectories. A series of synchronous trajectories are combined to create a trajectory graph, which is represented by the weighted undirected graph TG=(V,E,W), in which each vertex represents a trajectory Ti. When Ti and Tj are comparable, then E is the set of edges where an edge ei,j occurs between vertexes vi and vj. Wi,j is the SM difference between Ti and Tj, and W is the set of the weight of edge E.

Definition 6

Assume the location services provider receives the anonymity set Ss. The level of attack similarity required for the attacker to recognise the false trajectory in the anonymity set is a. Any two of the set's trajectories when sa are comparable to the attacker's. Any phoney trajectory in the set is indistinguishable to the attacker. The two trajectories are not similar to the attacker when s>a, let's say the mobility difference M(Ti,Tj) between Ti and Tj in the set is bigger than a. Less comparable trajectories make it simpler for the attacker to discern one trajectory from another.

Suppose a collection of synchronous trajectories is used to build the trajectory graph TG=(V,E,W). Let s determine the trajectory graph TGs=(V,Es,W). ask(k1)2 is used to determine the value of Es in accordance with Definition 5. Let a, the degree of vertex vi in TG ais di, determine the trajectory graph TGa=(V,Ea,W). When the attacker is small, the trajectory is immediately identifiable. Let |Ea| be the total degree of all the vertices of TGa. The attacker is more likely to recognize the bogus trajectories when |Ea|is small. Thus, there is a higher likelihood of privacy disclosure throughout the route. As a result, the chance of privacy disclosure along a route is defined as follows:

$$P = 1 - \frac{|E_a|}{|E_s|} \tag{4}$$

4.0 Spatiotemporal Mobility (SM) based Trajectory Privacy-Preserving Algorithm (MTPPA)

In this part provides an overview of the suggested MTPPA algorithm. In MTPPA, there are three phases. The trajectory pre-processing is created in stage I. The stopovers are identified, and the equivalence classes are created. Stage II is where the initial trajectory candidate selection and trajectory graph construction are designed. In stage III, the simulated annealing algorithm chooses an ideal trajectory k-anonymity set. After completing all three steps, the created ideal anonymity set can safeguard the user's trajectory privacy while complying with service-level

standards. When there is an edge connecting every pair of the graph's vertices, the graph is referred to as a clique. A k-clique is a clique with k vertices.

4.1 Service Matching Process

The service matching process described in the proposed scheme involves the privacy system checking whether the available services meet the entity's requirements. It considers the spatial and temporal preferences of both the services and the entity. The matching process ensures that the services being considered have spatial and temporal preferences that strictly align with the entity's requirements. This implies that the services should fall within the defined spatial limits and be available during the required time period specified by the entity.

By performing this matching, the scheme aims to provide the entity with services that are suitable in terms of their spatial and temporal characteristics. This ensures that the entity receives relevant and applicable services that meet their specific requirements. However, it is crucial to consider the practical implementation and effectiveness of the service matching process. The analysis should assess how well the matching algorithm performs in accurately identifying suitable services while considering any potential privacy or security implications. Additionally, the scheme should handle cases where no services strictly match the entity's requirements and provide appropriate alternatives or recommendations.

4.2 Random Coordinates

The use of random coordinates instead of the entity's precise spatiotemporal information can enhance privacy in the proposed scheme. The system avoids revealing the exact location of the entity, providing an additional layer of protection. This approach helps in mitigating the risk of unauthorized tracking or identification based on the individual's real-time or historical location data. By using random coordinates, it becomes difficult for service providers or adversaries to associate specific activities or actions with a particular location or individual. It is important to consider the potential limitations and implications of using random coordinates. For example, the chosen coordinates should still fall within the valid area and should not introduce biases or skew the overall distribution of service requests. The selection process should also ensure that the randomly chosen coordinates are plausible and align with the geographical context of the service being accessed. Furthermore, the security and privacy analysis of the scheme should also evaluate the robustness of the random coordinate selection process against potential attacks or inference techniques that could exploit patterns or statistical properties of the chosen coordinates.

4.3 Service Matching

The service matching process occurs after the entity has been authenticated and applies for services within a ubiquitous computing environment. It is noted that all services in pervasive environment have spatial and temporal limits, indicating that they are bounded by specific geographical areas and time durations. To determine the validity of a service for an entity, the privacy system performs a check based on the spatial and temporal preferences of both the

service and the entity. This implies that the service must fall within the desired spatial boundaries and be available during the required time period specified by the entity. By enforcing this strict matching criterion, the privacy system ensures that only services that precisely align with the entity's spatial and temporal preferences are considered valid. This helps tailor the services to the specific needs and constraints of the entity, enhancing the relevance and usefulness of the provided services. It is important to note that the specifics of how the service matching process is conducted and the mechanisms employed by the privacy system are not explicitly mentioned in the given statement. Further details and analysis would be required to fully understand the implementation and effectiveness of the service matching process within the privacy system.

5.0 Conclusion

The importance of user acceptance in the success of ubiquitous computing (UCE) and emphasizes the need for managing privacy risks associated with exposing personal information. The study aims to propose an architecture for privacy protection in ubiquitous computing by integrating privacy protection technologies into the access control architecture. This study defines spatiotemporal mobility (SM) as a metric for comparing trajectory similarity. The MTPPA algorithm is suggested based on SM and trajectory graph modelling. This implies that privacy-preserving features and technologies are essential to make UCE appealing to users. By integrating privacy protection technologies into the access control architecture, the goal is to ensure that different technologies work together, avoid conflicts, and provide multi-level privacy protection. The study also mentions the design of a ubiquitous software system based on a service-oriented approach. This design likely focuses on leveraging services to provide functionality while incorporating privacy protection mechanisms.

References

1. Wang S., Hu Q., Sun Y., Huang J. Privacy Preservation in Location-Based Services. *IEEE Commun. Mag.* 2018;**56**:134–140. doi: 10.1109/MCOM.2018.1701051. [CrossRef] [Google Scholar]

2. Kang J., Steiert D., Lin D., Fu Y. MoveWithMe: Location Privacy Preservation for Smartphone Users. *IEEE Trans. Inf. Forensics Secur.* 2020;**15**:711–724. doi: 10.1109/TIFS.2019.2928205. [CrossRef] [Google Scholar]

3. Majeed A., Lee S. Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey. *IEEE Access.* 2021;**9**:8512–8545. doi: 10.1109/ACCESS.2020.3045700. [CrossRef] [Google Scholar]

4. Huo Z., Meng X.F. A Survey of Trajectory Privacy Preserving Techniques. *Chin. J. Comput.* 2011;**34**:1820–1830.

5. Zhang S.B., Wang G.J., Liu Q., Abawajy J.H. A trajectory privacy-preserving scheme based on query exchange in mobile social networks. *Soft Comput.* 2018;**22**:6121–6133.

6. Zheng Y., Xie X., Ma W.Y. GeoLife: A Collaborative Social Networking Service among User, location, and trajectory. *IEEE Data Eng. Bull.* 2010;**33**:32–40. [Google Scholar]

7. Gruteser M., Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking; Proceedings of the 1st International Conference on Mobile Systems, Applications and Services; San Francisco, CA, USA. 5–8 May 2003; pp. 31–42. [Google Scholar]

8. Liu H., Li X.H., Li H., Ma J.F., Ma X.D. Spatiotemporal Correlation-Aware Dummy-Based Privacy Protection Scheme for Location-Based Services; Proceedings of the IEEE INFOCOM 2017—IEEE Conference on Computer Communications; Atlanta, GA, USA. 1–4 May 2017; pp. 1–9. [Google Scholar]

9. Wang T., Zeng J.D., Bhuiyan M.Z.A., Tian H., Cai Y.Q., Chen Y.H., Zhong B.N. Trajectory privacy preservation is based on a fog structure for cloud location services. *IEEE Access.* 2017;**5**:7692–7701. doi: 10.1109/ACCESS.2017.2698078. [CrossRef] [Google Scholar]

10. Shaham S., Ding M., Liu B., Dang S., Lin Z., Li J. Privacy Preservation in Location-Based Services: A Novel Metric and Attack Model. *IEEE Trans. Mob. Comput.* 2020;**99**:1. doi: 10.1109/TMC.2020.2993599. [CrossRef] [Google Scholar]

11. Zhao J., Zhang Y., Li X.H., Ma J.F. A Trajectory Privacy Protection Approach via Trajectory Frequency Suppression. *Chin. J. Comput.* 2014;**37**:2096–2106. [Google Scholar]

12. Privacy-preserving Microdata On A Tabular Data Publishing Using Additive Noise Approach Page No: 311-316- **DOI:20.18001.GSJ.2022.V9I1.22.38503**

13. Li J., Bai Z.H., Yu R.Y., Cui Y.M., Wang X.W. Mobile Location Privacy Protection Algorithm Based on PSO Optimization. *Chin. J. Comput.* 2018;**41**:71–85. [Google Scholar]

14. Xu H.J., Wu Q.H., Hu X.M. Privacy Protection Algorithm Based on Multi-characteristics of Trajectory. *Comput. Sci.* 2019;**46**:190–195. [Google Scholar]

15. Data Security and Sensitive data protection using Privacy by Design technique – BDCC – 2019 – Suresh Babu et.al.

16. Zhang J., Xu L., Tsai P.W. Community structure-based trilateral Stackelberg game model for privacy protection. *Appl. Math. Model.* 2020;**86**:20–35.