# Protecting Privacy of User Data in Intelligent Transportation Systems

**Yazed Alsaawy, Ahmad Alkhodre, Adnan Abi Sen**
aalkhodre@gmail.com
Department of Computer Science
Faculty of Computer and Information Systems
Islamic University of Madinah
Madinah 42351, SAUDI ARABIA

**Abstract**
The intelligent transportation system has made a huge leap in the level of human services, which has had a positive impact on the quality of life of users. On the other hand, these services are becoming a new source of risk due to the use of data collected from vehicles, on which intelligent systems rely to create automatic contextual adaptation. Most of the popular privacy protection methods, such as Dummy and obfuscation, cannot be used with many services because of their impact on the accuracy of the service provided itself, they depend on changing the number of vehicles or their physical locations. This research presents a new approach based on the shuffling Nicknames of vehicles. It fully maintains the quality of the service and prevents tracking users permanently, penetrating their privacy, revealing their whereabouts, or discovering additional details about the nature of their behavior and movements. Our approach is based on creating a central Nicknames Pool in the cloud as well as distributed sub-pools in fog nodes to avoid intelligent delays and overloading of the central architecture. Finally, we will prove by simulation and discussion by examples the superiority of the proposed approach and its ability to adapt to new services and provide an effective level of protection. In the comparison, we will rely on the well-known privacy criteria: Entropy, Ubiquity, and Performance.

***Keywords:***
*privacy, intelligent transport systems, multi-layered comprehensive approach*

## 1. Introduction

The problem of traffic congestion is one of the problems most concerned with governments because of its impact on all aspects of life in cities and the performance of businesses [1, 2]. In addition, it is closely related to the high rate of accidents and deaths, as well as the issue of environmental pollution and waste of fuel and time [3, 4]. With the advent of the Internet of Things and related technologies [5] such as cloud computing [6], fog computing [7], wireless sensor networks (WSNs) [8], radio frequency identifiers (RFID) [9], and other smart things that can be communicated and controlled from anywhere over the network. Many solutions [10] to this problem have emerged that are different from traditional solutions, which may be very expensive or not possible in some places [11], such as building bridges and tunnels [12], or those that are not as effective as traditional traffic lights, which may cause more congestion at peak times [13].

Through our previous work [14], we proposed a multi-layered comprehensive approach (MLCA) to solving the traffic problem in the Kingdom of Saudi Arabia - Medina. The MLCA is articulated on a set of layers that are integrated with each other to give a comprehensive, homogeneous, and uninterrupted solution. This solution is not affected by weather and ambient conditions. It can work in all contexts to provide an outstanding service. This solution was based on a range of services starting from smart vehicles [15, 16], smart traffic lights [17], smart roads [18], and a large number of smart applications such as the smart parking application and the emergency application [19, 20]. All of these solutions were based in a simplified way on processing images captured by sensors, drones, and cameras implanted in smart signals. On the other hand, information collected from social media and historical information about road conditions, people, and vehicles [21]. All these with each other to reach an adaptive optimal solution.

On the other hand, vehicle pioneers have many applications on their mobile phones, such as Google and its family, navigation applications [22], shopping and tracking applications [23], social networking applications, school applications [24], and other applications that pertain to different daily user segments. As a result, for all previous smart solutions and applications, a huge amount of data is generated and flows between users and services providers [25, 26]. Unfortunately, this data has caused big problems regarding the security and privacy of users [27, 28] including the two types of attacks Active attack such as the denial of service, and the Passive attack that is eavesdropping, obtaining, and exploiting users' information to reveal their personal and private data [29, 30]. For that, most people and governments became aware of the importance of the privacy and security of data [31], where the attackers can know everything about users and their movements, jobs, homes, hopes, tastes, trends, diseases, and financial incomes, etc.[32]. This has led many to refrain from using smart applications and avoiding

Manuscript received May 5, 2023
Manuscript revised May 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.5.18

dealing with smart objects to prevent infringement of their privacy [33].

Government and researchers considered privacy and security as the most challenging for new technologies like IoT. So, many of country put a new laws to enforce companies to preserve the privacy and security of their customers [34]. General Data Protection Regulation (GDPR) [35] is a European law for preserving privacy, it is announced in 2016, and started applying in 2018. Actually, the law solution is not enough to ensure privacy and security [36]. Also, the several protection solutions to the problem of Location-based privacy that have been proposed by researchers, including [37]: Dummy, obfuscation, peers cooperation, etc. are not suitable or compatible with new smart services like the traffic management. Where most of these methods affect adversely the quality of the main service and the accuracy of its functionality, (more detail will be in the previous works section, where we will discuss these methods and their negatives).

Therefore, the contributions of this research are:

- Review previous approaches to privacy and mentions the disadvantages of these approaches
- Propose a new approach for preserving the privacy of users in the location-based services called the "Nicknames Pool Approach".
- Present a new approach that solves all the cons in the previous methods with highly compatible with the nature of location-based services.
- Proof by simulation of the superiority of the proposed approach according to privacy and performance metrics.

## 2. Previous works

The problem, of data privacy and data security, has become a sensitive issue and many countries have begun to regulate special laws and policies that companies and service providers must adhere to ensure the security and privacy of users [37, 38]. Unfortunately, the governmental laws, despite their importance, are insufficient and do not guarantee the service provider's commitment, and on another side, they are insufficient to deal with malicious actors or external attackers on the other [36 - 38].

Privacy [39] is the right of each person to have full access to their data and the ability to decide who, when, why, how, and whether their data will be used by the service provider. To protect privacy, anonymity must be ensured in applications or public services. In addition, it is not enabling the attacker to create a profiling file for each user through which queries are linked to their users. Finally, preventing the user from being tracked and knowing his real location at a specific time. Thus, since data security [40] is concerned with protecting the confidentiality, integrity, and availability of data, we find that privacy faces a greater challenge because the user sends his data to the service provider, who can himself be a source of threat to the user, such as being malicious or being hacked by an attacker or a repairer of servers. For more details about the difference between security and privacy, see [41].

Therefore, during the past years, many techniques for protecting privacy have appeared, and the table 1 shows the most common techniques:

TABLE 1: THE MOST COMMON TECHNIQUES FOR PROTECTING PRIVACY

| PRIVACY TECH | WORKING MECHANISM | DRAWBACKS |
|---|---|---|
| Processing Data [42] | Deleting or collecting private data before sending it to the service provider. | Only valid with some services, not sensitive to time or delays |
| Anonymity [43] | Use a pseudonym or hash code to hide the real name | Simple and does not provide enough protection, it is easy to detect by the attacker |
| Mix-zone [44] | Improving the previous technique by changing the pseudonym every period of time | Easy to be tracked by malicious providers and therefore easy to crack |
| Third Trusted Party (TTP) [45] | Anonymizing the user by relying on a trusted third party | The need to trust a third party that may itself be a danger to the user |
| Obfuscation [46] | Add obfuscation to the data in order to protect the original data | An additional Load on the user as it affects the main service objective as well |
| Peers Cooperation [47] | Collaboration among the users themselves misleads the service provider | Collaboration between Peers is difficult to manage, and ineffective in dynamic and moving environments |
| Cloak Area [48] | It relies on a distributed TTP in cells so that each TTP is responsible for hiding the identity of users within its own cell | Difficulty in publishing plus the need to trust a TTP node that's called Anonymizer |

| | | |
|---|---|---|
| Private Information Retrieval (PIR) [49] | Pulling a large amount of data from the service provider and storing it locally for later use | It consumes very large user resources and causes a large load on the network |
| Dummy [50] | Sending a mixed package of fake and real inquiries to the service provider | Extra load on the user, network, and system. And also dummy is easy to detect and it affects the goal of the main service (e.g. calculating the percentage of congestion in a particular area) |

Anonymity-based methods are best suited to location-based applications and services [51]. Thus, it is better for most of the applications and services of the intelligent transportation sector. This is because other methods affect the accuracy of the basic service (for example the calculation of congestion rates in a specific area, the accuracy of a shipment receipt for a specific location, or reaching a specified target). That is meant it affects the accuracy of the main service and its results. However, the traditional methods in the previous table that use the concept of anonymity (Anonymity, Mix-zone, and TTP) have many drawbacks, such as ineffectiveness in protection, ease of detection, or the need to trust a third party [51, 52].

To deal with the previous problems, researchers at [51] have relied on fog nodes in smart cities to play the role of managing cooperation between two vehicles by switching alias between them in order to mislead the service provider and prevent it from drawing a correct tracking path for each. However, the disadvantage of this method is that it only works in the case of intersections in addition to the presence of detection of part of its data (its exact location) during the swap. This is due to the two exchanged vehicles being in the same location as the protection service provider. Therefore, if there are several malicious fog nodes, the user will be at risk of attack tracking the areas.

The Centralized pseudonym-changing scheme [52] is similar to the previous method but it is centralized rather than distributed. This method requires the user to send their exact location to the central protector, which then replaces their nickname with that of another nearby user. The problem of this approach is that it depends on absolute centralization, which is lead to a server bottleneck problem. In addition, this approach requires the user to send his accurate and trusted location, and therefore the server itself may be a source of danger to the user, whether it is malicious or hacked. Finally, when exchanging with a user in the same location, this leads to the disclosure of accurate information to the protector service provider (such as the exact geographical location of both users).

Our proposed alternative solution is a mixture between central and distributed. We relied on the fog node to relieve the load on the central server while keeping the option of direct contact with the central protection provider available in case the user did not trust the fog node, in order to break the fog-mix-zone tracking attack. The proposed approach does not require the user to send their query or their exact location to the security provider (whether the fog node or the central server). Therefore, the proposed approach will not pose any threat to the user's privacy. The user only sends him the area he is in, and he sends him a nickname that has been used by others in the same area or a neighboring area. Finally, the algorithm of the proposed approach uses the same name for K number of users and not just swapping between two users only, which means hiding the identity between K users. This means a higher rate of privacy and more difficulty for attackers to jailbreak, all without a noticeable impact on performance. Moreover, most importantly, it should not have any impact on the main service based on the location.

## 3. The proposed Solution

The idea of this approach is to mislead the attacker even if it is the service provider himself, by using the same aliases between different users and in different places. Thus, the formation of a misleading database of the service provider that it cannot use to analyze a particular user's queries in order to disclose additional information about it and to penetrate its privacy.

To achieve this, it was suggested that relying on a third party responsible only for tracking the nicknames used by users in different regions without knowing any details about users' data, queries, or destinations. We create a central database of nicknames used in each area during an earlier period, and the user is given a specific, not random, nickname based on his current area without disclosing his real location or destination.

The suggested nickname is a nickname used in an early period and one of the adjacent areas to the current user's area. Therefore, the service provider will consider that the user of that nickname still uses the same nickname and that he has moved to a closed area. It will therefore store fake information about both users. The complexity and distortion of the service provider will be increased as the number of users of the proposed approach increases. The nicknames are exchanged periodically between each other without the need for cooperation directly.

To solve the bottleneck problem and prevent overloading the cloud that contains the central database or Pool-of-Nicknames, we suggest benefiting from the fog infrastructure distributed at the edge of the end-user network. The cloud distributes a part of data to each fog node (containing nicknames used during the previous period within the nodes adjacent to the node itself).

The fog node has two caches (primary with big size and secondary with small size). The fog stores these nicknames within the primary cache, and once a new request from a user is raised within the area, one of the nicknames is given and that nickname is stored in the secondary cache. At each synchronization period (X), each fog node will send its second cache content (its nicknames used within the X period) to the Central Pool cloud. At the same time, the fog node receives a list of nicknames used within the neighbor nodes to store in the primary cache.

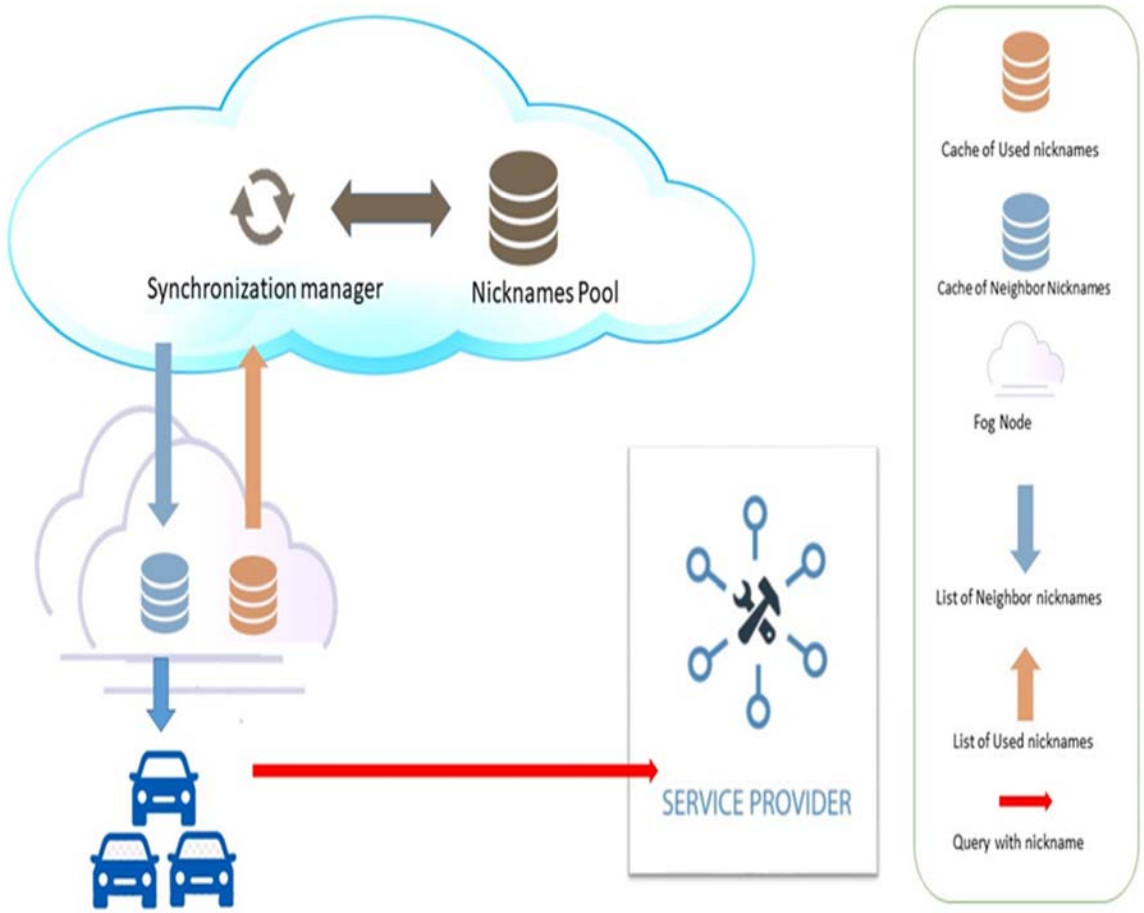


**Figure 1**. NIPA: NICKNAMES POOL APPROACH FOR PROTECTING PRIVACY,

Fig 1: represents the proposed approach. The approach consists of the users, fog nodes, and the cloud containing and managing the nicknames pool. Operationally at the beginning of the command and before the service request process begins with the service provider, the Nickname is obtained from the fog node and then the request is sent. On the other hand, the system develops and updates Nicknames, as shown in Fig 1, so that the used nicknames are sent to the cloud, which in turn sends the nicknames used in the neighboring nodes. The synchronizer in the cloud manages the exchange of Nicknames between fog nodes.

### 3.1 Suggested policy features:

1. The user does not need to trust any third party. This means that the user does not provide the fog or the cloud any information about his exact location, the direction of movement, or query.
2. The user does not need to cooperate with other users.
3. Great misinformation to service providers in such a way that it is difficult for them to form a true profile of each user or link each Nickname to their real user. Thus, the level of privacy has been significantly improved compared to previous methods that have used the principle of anonymity by Nicknames.
4. Improve system performance by employing the huge number of fog nodes in smart city environments
5. Relieve load for a user who will only have to use a Nickname without having to generate a jamming area or generate a dummy.
6. The proposed approach does not affect the performance of smart traffic systems that rely on the information on the number of vehicles in a particular area. Obfuscation or Dummy are not used.

## 4. Result and discussion

### 4.1 PRELIMINARIES

This section provides proof of the effectiveness of the proposed NiPA approach compared to previous methods (FM-ZA, Mix-Zone, and Anonymity) that have also relied on Nickname as its own protection principle. A simulation of the working mechanism of each of the previous methods was implemented based on the visual environment Studio.Net according to the following assumptions [51]:

1. Divide the study area into 100 * 100 cells, equal in size
2. 10,000 users randomly distributed over cells
3. 100 different points of interest
4. 4G as a network between users and Anonymizer or Fog
5. Internet Connection with the Service Provider
6. The service provider is a malicious attacker that seeks to collect information about users to breach their privacy

To compare all methods the following criteria have also been used [53, 54, 55, and 56]:

**Entropy [53]**, which is the main method for measuring the level of privacy, as it represents the amount of correct information collected by the service provider, which can be associated with the user. In other words, the privacy entropy represents the uncertainty rate of the service provider. The entropy is given by the following equation:

$$E = -\sum_{i=0}^{k} Pi * Log2(Pi) \quad (1)$$

Where Pi is the probability of that query belongs to submitted Peer ➔ Pi=1 ➔ E=0

Therefore, the best value for the **Entropy** is E equals to one, i.e. absolute uncertainty for the attacker.

**Estimate Error [54]**: it is the error rate on the attacker's side, which means the ratio of linking information by a specific user, and it represents the privacy violation rate:

$$EstError = E * 100\% \quad (2)$$

**K-Anonymity [55]:** A simple measurement represents the percentage of collected user queries by the service provider or attacker.

$$K - anonymity = \frac{Q_y}{Q_x} \quad (3)$$

Where $Q_y$ : is the number of queries related to a user and $Q_x$ is the number of queries, which is not related to a user.

Manuscript received May 5, 2023
Manuscript revised May 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.5.18

**Cost & Performance [56]**: The volume of data or the number of queries sent to the service provider against the number and size of the real query, as well as the response time of the query.

There are also other non-quantitative criteria, the most important of which is the immunity of approaches against certain attacks and the need to trust a particular party or not.

In the following, we present simulation results according to the above-mentioned hypotheses and based on the criteria for comparison:

### 4.2 Performance analysis

Fig 2 shows that both NiPA and FM-ZA approaches achieve the highest entropy rate due to the number of times the nickname is used. On the other hand, since the nickname is already used, this further misleads the service provider, thus collecting false data and continuing to protect privacy.

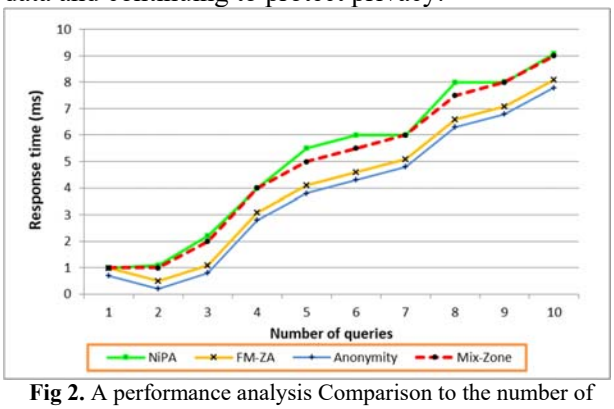


**Fig 2.** A performance analysis Comparison to the number of queries sent by the NiPA, FM-ZA, Anonymity and Mix-Zone

In the traditional Anonymity approach that has the lowest level of protection, we notice that with the time and increase in the number of queries that use the same nickname, the service provider can collect the queries and relate them to one user. After analysing those queries, there will be a breach of the user's privacy. The Mix-Zone approach has improved the protection of the Anonymity approach by changing the nickname when entering each new region. Nevertheless, according to the time tracking, the service provider can also hack it and record information about the real user. Similarly, NiPA and FM-ZA will achieve a maximum listen rate of 100%, and K-Anonymity is always equal to zero.

In Fig 3, it is clear that both approaches NiPA and FM-ZA are worse than Mix-Zone, while the Anonymity is better. It is rational because anonymity only needs the user to generate a nickname once for the first time. While in the Mix-Zone, the user needs to regenerate at each entry to a new cell, adversely affecting the level of protection achieved.

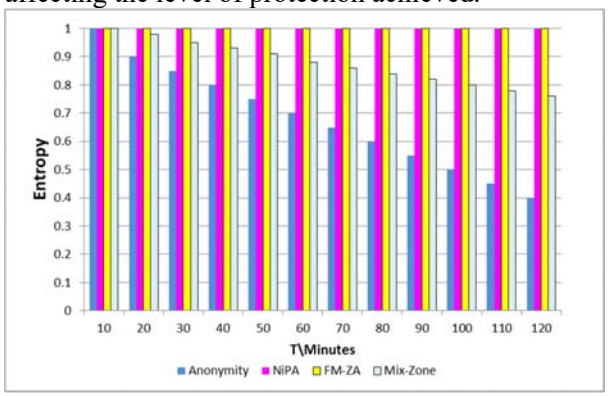


**Fig 3.** An entropy Comparison by the NiPA, FM-ZA, Anonymity and Mix-Zone.

In the FM-ZA and NiPA approaches, the user connects to the fog node or nickname pool server (in the cloud) to get a nickname at each query. However, it can be noted that the delay effect is very simple, as the nickname's selection process is not compared with other methods such as generating a wide range of fake queries as in Dummy, or Query obfuscation and creating a locked area as in Obfuscation [3] or Cloak Area [13], which is one of the famous protection methods used. NiPA and FM-ZA do not affect the size of the query or the number of queries sent, which means effective protection with a neglected effect on the response time.

More, NiPA and FM-ZA can outperform Mix-Zone or Anonymity in response time if they relied upon a cache in the fog nodes. However, this means the need to trust the fog node itself and the user should send his query also to the fog node and not only its direction or area.

### 4.3 The superiority of NiPA over FM-ZA

We have noticed through the previous results the convergence in the results between both approaches, but what the reason for the superiority of NiPA is. The NiPA approach is superior to the other approaches in three important points:

1- Applicability and service availability: In the NiPA approach, protection can be applied

anywhere by simply contacting the pool, while in FM-ZA it is intended to work when there are intersections to change directions between users when changing names among them.

2- The second and most dangerous point is that the FM-ZA approach indirectly exposes the user's area since all the cooperative users are at the same point (at the intersection), which means that the user's site is not well protected as well as not immune to a path tracing attack, or a tracing attack User's area. As for the NiPA approach, it exchanges nicknames with other users in neighboring regions, that is, the region is completely changed, thus protecting the exact location of all users.

Finally, fog nodes pose a danger to users of the FM-ZA approach if they are malicious because of the necessity of contacting them. Nevertheless, in the NiPA approach, users, in some cells, can communicate with Nickname Pool Server directly. This could completely prevent the zone tracking attack this is a suffering point for the FM-ZA approach.

## 5. Conclusion

In this paper, we presented a new approach based on the use of smart nicknames. This approach maintains the quality of service and prevents users from permanently tracking them, compromising their privacy, revealing their whereabouts, or discovering additional details about their behaviour and movements. Our new approach relied on creating a central pool of aliases in the cloud as well as distributed sub-pools in fog nodes to avoid intelligent delays and overload of the central architecture. Finally, through simulation and discussion on actual examples, the proposed approach excels and adapts to new services and provides an effective level of protection. For the comparison, we relied on well-known privacy criteria: Entropy, Ubiquity, and Performance.

## Acknowledgment

The Deanship of Scientific Research, Islamic University of Madinah, Saudi Arabia, funded this research under Tamayuz research grant number 2/710.

## References:

[1] Mahmud, K., Gope, K., & Chowdhury, S. M. R. (2012). Possible causes & solutions of traffic jam and their impact on the economy of Dhaka City. J. Mgmt. & Sustainability, 2, 112.

[2] Petrovska, N., & Stevanovic, A. (2015, September). Traffic congestion analysis visualization tool. In 2015 IEEE 18th International Conference on Intelligent Transportation Systems (pp. 1489-1494). IEEE.

[3] Isa, M. N., & Siyan, P. (2016). Analyzing factors responsible for road traffic accidents along Kano-Kaduna-Abuja Dual Carriageway Nigeria. Journal of Economics and Sustainable Development, 7(12).

[4] Farda, M., & Balijepalli, C. (2018). Exploring the effectiveness of demand management policy in reducing traffic congestion and environmental pollution: Car-free day and odd-even plate measures for Bandung city in Indonesia. Case Studies on Transport Policy, 6(4), 577-590.

[5] Patel, P., Narmawala, Z., & Thakkar, A. (2019). A survey on intelligent transportation system using internet of things. Emerging Research in Computing, Information, Communication and Applications, 231-240.

[6] Alam, T. (2020). Cloud Computing and its role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1(2), 108-115.

[7] Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Fog computing and the internet of things: A review. Big data and cognitive computing, 2(2), 10.

[8] Kandris, D., Nakas, C., Vomvas, D., & Koulouras, G. (2020). Applications of wireless sensor networks: an up-to-date survey. Applied System Innovation, 3(1), 14.

[9] Ibrahim, A. A. A., Nisar, K., Hzou, Y. K., & Welch, I. (2019, October). Review and analyzing RFID technology tags and applications. In 2019 IEEE 13th International Conference on Application of Information and Communication Technologies (AICT) (pp. 1-4). IEEE.

[10] Mandhare, P. A., Kharat, V., & Patil, C. Y. (2018). Intelligent road traffic control system for traffic congestion a perspective. International Journal of Computer Sciences and Engineering, 6(07), 2018.

[11] Jabbarpour, M. R., Zarrabi, H., Khokhar, R. H., Shamshirband, S., & Choo, K. K. R. (2018). Applications of computational intelligence in vehicle traffic congestion problem: a survey. Soft Computing, 22(7), 2299-2320.

[12] Nguyen, M. Q., Pham, T. T. X., & Phan, T. T. H. (2019). Traffic Congestion-A Prominent Problem in Vietnam Current Situation and Solutions.

[13] Pop, M. D. (2018). Traffic lights management using optimization tool. Procedia-social and behavioral sciences, 238, 323-330.

[14] Alsaawy, Y., Alkhodre, A., Abi Sen, A., Alshanqiti, A., Bhat, W. A., & Bahbouh, N. M. (2022). A Comprehensive and Effective Framework for Traffic Congestion Problem Based on the Integration of IoT and Data Analytics. Applied Sciences, 12(4), 2043.

[15] Cao, Z., Ceder, A. A., & Zhang, S. (2019). Real-time schedule adjustments for autonomous public transport

vehicles. Transportation Research Part C: Emerging Technologies, 109, 60-78.
[16] Tokody, D., Mezei, I. J., & Schuster, G. (2017). An overview of autonomous intelligent vehicle systems. Vehicle and Automotive Engineering, 287-307.
[17] Elsagheer Mohamed, S. A., & AlShalfan, K. A. (2021). Intelligent traffic management system based on the internet of vehicles (IoV). Journal of advanced transportation, 2021.
[18] Alharbi, A., Halikias, G., Sen, A. A. A., & Yamin, M. (2021). A framework for dynamic smart traffic light management system. International Journal of Information Technology, 13(5), 1769-1776.
[19] Lin, T., Rivano, H., & Le Mouël, F. (2017). A survey of smart parking solutions. IEEE Transactions on Intelligent Transportation Systems, 18(12), 3229-3253.
[20] Alharbi, A., Halikias, G., Yamin, M., Sen, A., & Ahmed, A. (2021). Web-based framework for smart parking system. International Journal of Information Technology, 13(4), 1495-1502.
[21] Lv, Y., Chen, Y., Zhang, X., Duan, Y., & Li, N. L. (2017). Social media based transportation research: The state of the work and the networking. IEEE/CAA Journal of Automatica Sinica, 4(1), 19-26.
[22] Dayu, S., Huaiyu, X., Ruidan, S., & Zhiqiang, Y. (2010, November). A GEO-related IOT applications platform based on Google Map. In 2010 IEEE 7th International Conference on E-Business Engineering (pp. 380-384). IEEE Computer Society.
[23] SUCIU, G., BALANEAN, C., PASAT, A., ISTRATE, C., Hussain, I. J. A. Z., & MATEI, R. (2020, June). A new concept of smart shopping platform based on IoT solutions. In 2020 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. 1-4). IEEE.
[24] Ghareeb, M., Bazzi, A., Abdul-Nabi, S., & Ibrahim, Z. A. A. (2018). Towards smarter city: clever school transportation system. Analog Integrated Circuits and Signal Processing, 96(2), 261-268.
[25] Jan, B., Farman, H., Khan, M., Talha, M., & Din, I. U. (2019). Designing a smart transportation system: an internet of things and big data approach. IEEE Wireless Communications, 26(4), 73-79.
[26] Liu, M. (2021, July). Urban smart transportation based on big data. In Journal of Physics: Conference Series (Vol. 1972, No. 1, p. 012092). IOP Publishing.
[27] Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies, 33(3), e3677.
[28] Hahn, D., Munir, A., & Behzadan, V. (2019). Security and privacy issues in intelligent transportation systems: Classification and challenges. IEEE Intelligent Transportation Systems Magazine, 13(1), 181-196.
[29] Wernke, M., Skvortsov, P., Dürr, F., & Rothermel, K. (2014). A classification of location privacy attacks and approaches. Personal and ubiquitous computing, 18(1), 163-175.
[30] Eian, I. C., Lim, K. Y., Yeap, M. X. L., Yeo, H. Q., & Fatima, Z. (2020). Wireless Networks: Active and Passive Attack Vulnerabilities and Privacy Challenges.
[31] Gerber, N., Reinheimer, B., & Volkamer, M. (2019). Investigating People's Privacy Risk Perception. Proc. Priv. Enhancing Technol., 2019(3), 267-288.
[32] Seliem, M., Elgazzar, K., & Khalil, K. (2018). Towards privacy preserving iot environments: a survey. Wireless Communications and Mobile Computing, 2018.
[33] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.
[34] Barrett, L. (2018). Confiding in Con Men: US privacy law, the GDPR, and information fiduciaries. Seattle UL Rev., 42, 1057.
[35] Zaeem, R. N., & Barber, K. S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. ACM Transactions on Management Information Systems (TMIS), 12(1), 1-20.
[36] Bruschi, D. M. (2019). Information privacy: Not just gdpr. In Computer Ethics Philosiphical Enquiry (pp. 1-10). ODU Digital Commons.
[37] Sen, A., Ahmed, A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things: a survey. International Journal of Information Technology, 10(2), 189-200.
[38] Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety and ethics. In Digital twin technologies and smart cities (pp. 123-149). Springer, Cham.
[39] Solove, D. J. (2005). A taxonomy of privacy. U. Pa. l. Rev., 154, 477.
[40] Denning, D. E., & Denning, P. J. (1979). Data security. ACM Computing Surveys (CSUR), 11(3), 227-249.
[41] Abi Sen, A. A., & Basahel, A. M. (2019, March). A comparative study between security and privacy. In 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 1282-1286). IEEE.
[42] Malik, M. B., Ghazi, M. A., & Ali, R. (2012, November). Privacy preserving data mining techniques: current scenario and future prospects. In 2012 third international conference on computer and communication technology (pp. 26-32). IEEE.
[43] Daubert, J., Wiesmaier, A., & Kikiras, P. (2015, June). A view on privacy & trust in IoT. In 2015 IEEE International Conference on Communication Workshop (ICCW) (pp. 2665-2670). IEEE.
[44] Liu, X., Zhao, H., Pan, M., Yue, H., Li, X., & Fang, Y. (2012, March). Traffic-aware multiple mix zone placement for protecting location privacy. In 2012 Proceedings IEEE INFOCOM (pp. 972-980). IEEE.
[45] Gupta, A., & Bhartiya, R. (2017, August). A result evaluation on anonymiser and active object based TTP location privacy framework. In 2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC) (pp. 1-6). IEEE.
[46] Ardagna, C. A., Cremonini, M., di Vimercati, S. D. C., & Samarati, P. (2009). An obfuscation-based approach for protecting location privacy. IEEE Transactions on Dependable and Secure Computing, 8(1), 13-27.
[47] Fawaz, A., Hojaij, A., Kobeissi, H., & Artail, H. (2011, August). Using cooperation among peers and interest mixing to protect privacy in targeted mobile

advertisement. In 2011 11th International Conference on ITS Telecommunications (pp. 474-479). IEEE.

[48] Zhangwei, H., & Mingjun, X. (2010, April). A distributed spatial cloaking protocol for location privacy. In 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing (Vol. 2, pp. 468-471). IEEE.

[49] Grissa, M., Yavuz, A. A., & Hamdaoui, B. (2019). Location privacy in cognitive radios with multi-server private information retrieval. IEEE Transactions on Cognitive Communications and Networking, 5(4), 949-962.

[50] Siddiqie, S., Mondal, A., & Reddy, P. K. (2021, April). An Improved Dummy Generation Approach for Enhancing User Location Privacy. In International Conference on Database Systems for Advanced Applications (pp. 487-495). Springer, Cham.

[51] Abi Sen, A. A., Alnsour, A., Aljwair, S. A., Aljwair, S. S., Alnafisah, H. I., & Altamimi, B. A. (2021, March). Fog mix-zone approach for preserving privacy in iot. In 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 405-408). IEEE.

[52] Didouh, A., El Hillali, Y., Rivenq, A., & Labiod, H. (2022). Novel Centralized Pseudonym Changing Scheme for Location Privacy in V2X Communication. Energies, 15(3), 692.

[53] Wagner, I., & Eckhoff, D. (2018). Technical privacy metrics: a systematic survey. ACM Computing Surveys (CSUR), 51(3), 1-38.

[54] Yamin, M., Alsaawy, Y., B Alkhodre, A., Sen, A., & Ahmed, A. (2019). An innovative method for preserving privacy in Internet of Things. Sensors, 19(15), 3355.

[55] Jiang, H., Li, J., Zhao, P., Zeng, F., Xiao, Z., & Iyengar, A. (2021). Location privacy-preserving mechanisms in location-based services: A comprehensive survey. ACM Computing Surveys (CSUR), 54(1), 1-36.

[56] Wang, J., Cai, Z., & Yu, J. (2019). Achieving personalized $ k $-anonymity-based content privacy for autonomous vehicles in CPS. IEEE Transactions on Industrial Informatics, 16(6), 4242-4251.Author, Title of the Book, Publishing House, 200X.