Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.019243
Review

Tech Science Press

A Review on Privacy Preservation of Location-Based Services in Internet of Things

Raniyah Wazirali*

College of Computing and Informatics, Saudi Electronic University, Saudi Arabia, Riyadh
*Corresponding Author: Raniyah Wazirali. Email: r.wazirali@seu.edu.sa

Received: 07 April 2021; Accepted: 12 June 2021

Abstract: Internet of Things (IoT) has become popular with the rapid development of sensing devices, and it offers a large number of services. Location data is one of the most important information required for IoT systems. With the widespread of Location Based Services (LBS) applications, the privacy and security threats are also emerging. Recently, a large number of studies focused on localization and positioning functionalities, however, the risk associated with user privacy has not been sufficiently addressed so far. Therefore, privacy and security of device location in IoT systems is an active area of research. Since LBS is often exposed to attacks, it has privacy concerns, such as the privacy of a user's current location, which could include personal details. If the user's current position is compromised as a result of unauthorized access, it may have serious consequences. As a result, maintaining user privacy while achieving precise location remains a challenge in IoT. In this paper, we survey different challenges related to the privacy and security of user's location in IoT systems. First, we provide in depth analysis of several studies related to this issue. Secondly, we propose potential solutions to address the problem at hand. Finally, we discuss some limitations that still require attention through related case studies.

Keywords: Privacy-preservation; IoT services; location information

1 Introduction

Over the world, increasing development has reshaped our lives with the emerging technology of the Internet of things (IoT) and has become an integral part of our daily activities. IoT has provided various technologies and facilities in every field of life [1]. For instance, safe and smooth driving experience using IoT based cars that interact with other vehicles and traffic rules to be safe, data collection of our body system, health monitoring, and daily activities using wearable tools and gadgets and smart home devices that are capable of enhancing the quality of life [2]. According to the prediction of IoT analytics, it is estimated that 34 billion IoT devices would be connected by 2025 [3]. Moreover, IoT will play a significant role in the growth and development of data generation and the rapid increase in the amount of IoT instruments and devices [4]. In addition, it has been estimated in the International Data Corporation's

2013 report, that in 2013 and 2020, data increases from 4.4 to 44 zettabytes that could lead to 180 zettabytes by 2025 [5].

IoT devices have diversity in privacy protection, but most have disadvantages of power consumption and limited computational. So, many conventional privacy preservation techniques based on IoT did not prove successful [6]. Recently, new practical techniques and methods (Machine learning (ML)) have gained attention to address and enhance the conventional privacy preservation approaches limitations. IoT-based devices interact and generate shared network systems, software, hardware, and application and process data. In new techniques, there is an opportunity to enhance previous operations and guide the automatic procedure. It is predicted that organizations' IoT projects based on approach machine learning were 10% in 2017, increasing to 80% by 2020 [7]. IoT produces many data that provide a platform to advance devices for data collection, monitoring, and processing of services of privacy protection. There are a privacy preservation operations like authentication, access control, regulatory compliance, and data aggregation of organizational data owners, users, and collectors enhanced using machine learning devices. Among various IoT, data components become protected, secured, and minimized contextual raw data sharing using ML-based devices. The risk related with user privacy has not been adequately addressed so far. Therefore, privacy and security of device location in IoT systems is an effective area of research. Since LBS is often exposed to attacks, it has privacy concerns, such as the privacy of a user's current location, which could include personal details. If the user's current location is exposed as a result of unauthorized access, it may have severe concerns. As a result, providing user privacy while attaining accurate location remains a challenge in IoT.

In an IoT environment, privacy must be a significant concern; for instance, privacy issues may arise in different phases of data sharing and interaction due to a large number of location information generation and collection in IoT devices. Location-based information in the IoT includes sensing, detecting, storing, processing, sharing, and using data among devices [8–14]. A GPS sensor gathers information of locations that could be very sensitive for few uses. A consistent and flexible approach of privacy preservation-based services has dominant importance in the field of Information technology. It should be in mind that computational cost and energy resources are considered as a priority while selecting any privacy preservation technique in the IoT ecosystem. The following list highlights the privacy concerns within the IoT ecosystem as given below:

(a) Identification: While using any intelligent device, identification is an essential factor to know whether inventions in the field of the internet and communication devices like computers, mobile devices have become ubiquitous, networking, and some other technologies the Internet of Things (IoT) now have a significant role in the modern lifestyle, which is fundamentally changing science and society. Moreover, the applications based on the users' current location are rapidly expanding. Wireless technologies, RFID, 3G and 4G networks, Bluetooth, GPS systems, and other networking technologies are used to link networks of objects in the Internet of Things. This network allows the objects or "thing" to have unique identification and some backend system pattern of activities to communicate with each other by using cloud computing, web portals, or mobile computing. Keeping in view the pace of innovation in this industry it can be predicted that usage of IoT will exceed that of the Internet 30 times over and market worth will be more than $100 billion. Our day-to-day activities will become uprising as a result of a merger between location-based services (LBSs), communication, and computing technologies. Both technologies play an important role in the world of the Internet of Things. Location-based services are being used in mobile devices more conventionally and become a very important element in developing the Internet of things. Usage of RFID technology and mobile logistic information collection in mobile devices highlights the importance of IoT. In an organization, identifying any user or system could be a serious issue [15]. There is a need to obtain a system that gives the device's identity to all connected authorized party's devices simultaneously. Authorized users should know about connected devices' identity to differentiate them from other instruments [16–18].

(b) Authentication: Authentication is a challenging task in privacy preservation that requires proper authentication servers and frameworks to attain their goal through transmitting appropriates texts to other connected nodes to network devices. IoT-based privacy preservation techniques are lack of exchanging multiple messages to authentication servers like RFID approaches. These approaches do not exchange information to sensor notes as well [15,19].

(c) Data Integrity: While any cyber breach, cybercriminals can be affected by various data control factors as they often face data changes during data transition, server outages, and electromagnetic intrusion. Data integrity is a valuable method to prevent data transmission and reception from external disturbances and cybercriminals' involvement using basic security surveillance methods. Therefore, in this case, without identification of threat system cannot exchange the data among users. Checksums and cyclic redundancy checks (CRC) ensure data accuracy and reliability using the error detection method [15,17].

(d) Trust: Trust is a multifactor term in various disciplines, dimensions, and concepts. It is more complex to establish and identify because of covering broad scope than security concerns in intelligent devices. Moreover, it is related to privacy concepts in which professionals use to identify any user's personal information about whether, when, and to whom he/she could disclose their privacy leaks [20]. In permeating systems or IoT devices, many studies aim to enhance identity trust and attain privacy preservation. Therefore, a user will adopt the policies, beliefs, and Security of manufactured devices before sharing personal data with other instruments [21].

(e) Data Confidentiality: Data confidentiality prevents the users and confirms that sensitive information is trusted through using different mechanisms to secure unauthorized leakage. Security methods of data protection from illegal users are individually identified includes data encryption, biometric verification, and two-stage authentication of two dependent users [22]. For example, in IoT-based intelligent devices, data do not appear to other unauthorized readers, nor can they view sensor nodes or data labels [23].

In this paper, the author explains the location-based services on Section 2 and this include: Location Awareness, Location Information via GPS, Location Information Through Wireless and Location Using Cellular Network. Then, in Section 3 the paper discusses the privacy issues of location-based privacy follow by deliberating the existed works of location-based privacy. In Section 4, the paper analyses some related works and give the weaknesses and the strength of each method. Finally, Section 5 provides the conclusion.

2 Location-Based Services

In the Internet of things (IoT), there is a variety and broad use of LBSs in smartphone applications. Smartphone applications that users use and run on Androids or iPhones like group calendars, digital banking, and social networking (Facebook, WhatsApp, Twitter) often enable users to enhance the availability of devices services and access remote data anytime and anywhere. Consequently, almost every mobile phone, there are some examples of LBSs daily, including searching for a restaurant in the vicinity and searching the nearby area for shopping deals or discount shops. The lifestyle and the way of communication have improved using and sharing location information. The exchange of location data among servers, users, or ordinary people makes socialization easier through mobile location-based services.

A few years ago, studies estimated and found that most youngsters use SMS/text/messages to interact with other friends and organize parties or seminars [24]. After that, mobile applications like WhatsApp, Facebook, Instagram, etc., in the cell phone industry significantly entered through SMS evolution. In addition, all smartphone applications take over the conventional use of messages with the extensive use of iOS, Android cell phones and Windows mobiles, SMS, and VOIP apps functioning on 3G, 4G, 5G, and wireless networks. These applications are considered social location information leakage sources that share location-based services and data to friends and other connected users [25]. Mobile applications like "WhatsApp" and "Viber" with cross-exchange capability offer users to share locations using audio, video texts, text messages, photos to other users without any cost via wireless Internet. Child location services are different location-based services that are also becoming common [26].

2.1 Location Awareness

In traditional methods, only usernames, passwords, digital certificates, and other information are used to identify the user's location using just computer systems or authenticating individuals—IP addresses of users and time of access to the area often recorded in conventional methods. Recently, location awareness has become a common term among smartphone users—this term initiated from location and configuration information of networking. Moreover, network configuration and location information and notification of information changes in application are services provided in Network location awareness (NLA) [26]. This term has been evolved with the emerging technology of GPS and radio-equipped mobile gadgets. In Mobile devices and pervasive computing system providing location data as well as identity authentication becomes more useful. Identity of location information using the combination of these two terms defines the location based services. There are three methods that Hopper describes commonly used to save location data [27]: 1. Coordinates: It is a 2D or 3D trajectory of real values that showing the distance of a specific origin from an entity; 2. Proximity: Showing how much two or more than two entities are close to each other using a real numbers rounded to binary value; and, 3. Containment: a number showing the total of integration of various entities.

2.2 Location Information via GPS

In 1972, the first research was conducted on the Global Positioning System (GPS) when United States Air Force (USAF) used ground-based pseudo-satellites to try development flight assessments of two prototypes of GPS operators on white sands missile range. Therefore, in the 1990's gulf war first time GPS satellites were extensively used [28]. GPS receivers equipped with any device provide calculated precise timing of the signals sent out by GPS satellites. Usually, two dimensional (2D) operational mode required calls from 3 satellites. The 2D operation mode would not provide the elevation reading but calculate the horizontal coordinates. The 3D operation mode required four satellites that provided information on both the horizontal and elevation coordinates. Time is noted when the message is sent through satellite and transmitted from satellites and satellite's point at message sending. So, a minimum of four satellites received the message and a GPS receiver will obtain the time sent and position of satellite by calculating message transmission. The location procedure is as follows: the GPS receiver calculates the distance of four satellites from each satellite to locate these four satellites and their location. A mathematical principle called Trilateration was used to start this process. This principle is based on using geometrical shapes of circle, sphere or triangles to measure the distance points and relative and absolute location of each point as well. Consequently, latitude and longitude information along with altitude information sometimes obtained through a GPS navigation device.

2.3 Location Information Through Wireless

With the development of wireless equipment, wireless devices connected to Wi-Fi signals obtained through wireless local areas networks (WLANs) are attracting more applications worldwide that called as Wi-Fi-based positioning systems (WPS). There are two methods of positioning in Wi-Fi access points using the localization mechanism. The first one is based on calculating the intensity of received signals, while the second one is based on WLAN fingerprinting [29]. A WLAN fingerprinting method is also called scene analysis or pattern matching technology. Its functioning setting is observed, and devices' current location is estimated via those observations [30]. This technique estimates that every physical location contains a rare fingerprint that is similar to human fingerprints and various characteristics in wireless signal space. Fingerprinting technique further has two phases of operating procedure. In the first phase, WLAN scanning and online locations are executed along with the map construction using the offline sampling phase. At the same time, the second phase is based on real-time monitoring of WLAN measurements to locate the WLAN devices [31].

2.4 Location Using Cellular Network

GSM localization is a positioning system of obtaining device location via the cellular network. Radio towers are used to locate any device performed by multilateration of radio signals among two networks of two towers and devices. Multilateration is a navigation method in which the variation of distance of two or more than two locations are measured by recording the signals at known times [32]. Excitingly, an active phone call is not required in this process of location searching. The signals strength of any antennae masts in vicinity area provide location signals to GSM. Following is the working procedure of GSM localization method: GSM enabled devices send calls through base stations that processed these calls to other networks. Then, general location or geographical area of any device determined in a base station. Other base stations likewise connect with the GSM empowered gadget and if data from a few base positions assembled, the area of the gadget can be limited utilizing triangulation. Triangulation is the way toward deciding the area of a location by estimating points from recognized focuses over one or the flip side of a fixed standard [33].

3 LBS Security Problems

In location based services (LBSs) GPS application used to obtain users current location where he/she is living via smart devices like Android and iOS devices. This location information is obtained when the LBS server receives a text question of his location. This query will allow LBS server to locate the user's location via returning points of interest (POIs) near the uses like available vehicles in the vicinity, any restaurant, and obtain just-in-time tickets. Though, the linked possible privacy issues may offset the benefits. For instance, a cybercriminal could collect all queries and sensitive data sent to the LBS server of any particular user about his workplace, attitude, and personal profiles [34,35]. Moreover, in the greed of money and other strategic benefits, the LBS server may disclose the user's sensitive information to a third party. Expectedly, in recent research studies, LBSs are a hot topic of privacy-preservation. The study's objectives are to identify the conventional methods of privacy preservation, location-based services in the IoT ecosystem; and privacy and security challenges and issues related to these data prevention approaches.

4 Related Works

In recent advanced and technological development, many advanced types of research have been studied on the preservation of Privacy for IoT-based services [36,37]. The most focused solution to preserve privacy and handle massive amounts of data is the association of IoT and cloud computing. Location-based services have been gaining attraction among users in a recent era with widespread positioning technologies, wireless communication devices, and mobile wireless-based devices [38–40]. IoT may significantly impact users' data privacy as massive amounts of data are collected and shared with other devices. Furthermore, there are many challenges regarding user's Privacy from authorized parties and the collection of personalized and computational data in IoT [41]. Location information is a primary source of leaking someone's location privacy that further impacts the data handling or processing of the Internet of Things (IoT). Therefore, location data is a massive component of the inefficient portfolio, supply chains, effective transportation systems, mobile applications context-aware, and many other IoT-based services [42]. Moreover, delicate location data is handled or organized without users' permission could cause privacy attacks and threat consequences, leading to severe challenges for the Security and Privacy of IoT services [43–45].

Henze et al. suggested a user-driven privacy enforcement method that studied Privacy-preserving for single end-user for cloud-based services in the IoT [46]. Another research proposed the idea of PAgIoT, a Privacy-preserving Aggregation protocol that allows groups of entities for appropriate IoT settings and allows PAgIoT, a Privacy-preserving Aggregation protocol along with the permission of value correlation for privacy-preserving [47]. In [48], a trust model of inconsequential privacy-preserving had been designed to minimize the privacy losses in the presence of unauthorized service providers. While using this model, the provider could be secured from disclosing information to third parties for illegal use. The authors in [49] conducted research work for roaming service to provide standard roaming capability and multilayered privacy preservation using a conditional privacy-preserving authentication with access linkability (CPAL). In [50], authors presented the idea of available resources and time duration for attackers that showed the trade-off among the handling load for an IoT note in contrast with the desired time limit of privacy preservation and estimated cost of breaking public-key cryptosystem as well. In addition, Jin et al. [51] discussed the architecture of smart cities realization by the Internet of things (IoT) that includes a complete urban localization data system and presents a transformational role of a conventional cyber-physical system. The authors in [52] suggested a privacy-by-design (PbD) technique to design new platforms for IoT devices. They could guide software engineers to analytically access the middleware platforms and IoT application's privacy capabilities.

This paper [53] presented a solution for IoT-based location privacy. Their project approves order securing symmetric encryption (OPSE) and k-anonymity method based on a uniform grid system. So, the anonymizer could only execute superficial similarities and differences of operations because of unawareness of the user's actual location information. In their proposed approach, they used to transform the user-based grid framework into a uniform grid framework by employing an entity of conversion capability. This permit user to avoid repeating queries from various users at the same query location base with a combined caching system that resultantly minimizes the overhead of the LBS server. Using this idea, it was concluded that user's location privacy could preserve by decreasing overheads at LBS server and anonymizers. In [54] research, they presented the collaborative trajectory privacy-preserving (CTPP) scheme for nonstop queries. There is no need for any completely trusted entities to guarantee a trajectory privacy through caching-aware collaboration between users in this scheme. Their scheme's primary aim is to confuse LBS attackers by complicating the actual trajectory and issuing fake requests or queries. Moreover, they used to collect important information from multi-hop peers that was based on combined caching with the help of a multi-hop caching-aware cloaking algorithm. They then introduce a collaborative privacy-preserving fake queries-based algorithm to confuse the location service provider (LSP). The resultant verification of their scheme proved to be effective and efficient in processing time and cost of communication.

The authors of [55] research aimed to study previous or traditional studies to examine the limitation and future opportunities of using machine learning-based (ML) IoT privacy solutions. First, they explored, collected, and categorized various data sources in IoT. Then, they analyze the existing solutions designed, established, and performed to protect IoT privacy concerns. The authors of [56] study ensure location-based privacy by comparing the Enhanced Semantic Obfuscation technique (ESOT) with a simple location obfuscation mechanism. Consequently, they concluded that ESOT has more computational overheads as compared to Simple Obfuscation Techniques. A novel Obfuscation technique is proposed to ensure the location privacy and get rid of Privacy and computational overhead. In [57], researchers aimed to describe and focused on possible location privacy risks of road networks provided and their protection methods in LBSs. They investigated various attacks (co-relation attack, inference, and intellectual merits attack) with possible broader impacts over LBSs for vehicular ad-hoc networks and provided (V ANET) users. Other objectives of the research were to provide effective and prolonged location privacy solutions and approaches.

In [58] paper, they proposed an efficient k-anonymity based Dummy Location and separate Circular Area (k-DLCA) approach to secure the user's location privacy. Compared to previous research, the k-DLCA algorithm attains a greedy method to select locations and showed resistance from adversary attacks with less chance of data exposure. Recently, there has been much research about protecting and preserving Privacy with quick response [59]. Therefore, those researches can be summarized into two main methods: spatial and temporal cloaking and transformation of the user's location. In this paper, a new architecture is proposed by attaching a database to the existing gateway mobile location center (GMLC) in the mobile core network to protect user privacy and reduce response time. The results show that the new architecture protects user privacy well and reduces response time. A research study in [60] conducted privacy preservation of users' mobile phones in location-based Cyber Services (PPCS) by proposing a region-of-interest division-based algorithm. As compared to previous preserving methods, their suggested PPCS method produces dummy location information during specific locations' semantic data. The user's actual location exposure will exclude or minimize by enabling the generated sites of the PPCS algorithm. They analyzed and described that PPCS is prone to both plotting attacks and implication attacks. Moreover, they utilize extensive simulation to demonstrate and evaluate the proposed method effectively.

Authors in [61] first identify the threats to both global navigation satellite systems (GNSS) and non-global navigation satellite system (n-GNSS) and their solutions. They then proposed concrete cryptographic keys for location and positioning-based services in IoT devices' privacy and security threats. Consequently, they describe the state of art of policy rules preventing positioning resolutions and legal instruments to location information privacy. The studies reviewed in this literature provided information on IoT-based positioning system and localization in terms of technical and legal aspects and their security and privacy issues. They also aimed to suggest recommendations and visions for future IoT-based vigorous, secure, and privacy-preserving location-based ideas. In [62] literature study, they presented a privacy preservation method based on radius-constrained dummy trajectory (RcDT) in MSNs. For location information where the client sent LBS query, they propose trajectory (RcDT) in MSNs idea to view a user's reallocation by constraining the generated circular radius R. Additionally, this method leads to a comprehensive study of both risks of the single-location exposure and trajectory exposure threats.

In [63] study, authors proposed an advanced location privacy preservation mobile app, called MoveWithMe. This app hides the actual user's location and behavior by generating decoy queries in the user's app while using location-based mobile devices. MoveWithMe behaves like an actual human who quickly identifies the threats compared to previously studied research on dummy trajectories. Moreover, every decoy has semantical variation from all other real user's traces and specific geographic locations using different moving patterns, daily schemes, and social attitudes. This study [64] proposes a responsible rethought LBS privacy-preserving plan. In the rethinking situation, to cause clients to cooperate with cloud workers to acquire inquiry information, first and foremost, they develop area various leveled list and quality progressive file dependent on Bloom Filter. Furthermore, they partition one locale into nuclear areas utilizing Hilbert Curve, which guarantees the Privacy of questions and improves inquiry efficiency. Finally, they understand the sharing of scrambled information among various clients by responsible intermediary re-encryption (APRE) innovation, which can successfully reduce the intermediary re-encryption key [65].

5 Discussion

Above described techniques for privacy preservation in IoT devices provided opportunities and limitations in their uses as shown in table. For last years, location privacy has been a significant factor in the demanding developmental era. Moreover, most of the devices developed and commercially used because accuracy of devices is limited to few applications along with the availability of specific service providers.

In order to support innovation development effective and efficient location based services (LBSs), used to aware the servers on the basis of location and positioning information of Wi-Fi frameworks. Following is the table presenting the strengths and weakness of existing LBS techniques:

Related work	Strengths	Weaknesses
[53]	The simulation and analysis of the proposed scheme in this paper showed that this method could efficiently preserve the location privacy along with the minimization of overheads at the anonymizer and LBS server.	This idea cannot have proved to be high Security for user's key because, in this method, users always use a similar permit for infrequent queries.
[54]	Based on collaborative caching, it collects valuable information from multi-hop peers. This proposed idea is effective and efficient in terms of less processing time and low communication cost.	A fully trusted third party is not easy to find. Attackers could easily access the user's location and query requests because these are attractive targets for adversaries. So, when attackers attacked their Privacy, user's information will be exposed publically.
[55]	This proposed idea has a robust analytical framework as well as an effective processing scheme.	Chances of less accuracy in analysis results because needed homomorphic encryption during the work to keep products accurate to the original model.
[56]	High-level privacy preservation opportunity in terms of less computational cost and efficient solutions of location privacy preservation.	Less enhanced privacy preservation efficiency due to which users required and prefer to use advanced S-Obfuscation or Enhanced Semantic Obfuscation Technique for privacy preservation in IoT services.
[57]	The proposed model investigated various attacks (co-relation attack, inference, and intellectual merits attack) with possible broader impacts over LBSs for vehicular ad-hoc networks and provided (V ANET) users.	In the road map study of finding location information, this technique did not provide the complete guidelines for mobile users to locate a path for identifying their privacy preferences. Users could get confused due to a lack of proper procedures.
[58]	The proposed *k*-DLCA algorithm could improve entropy for user's location privacy preservation and hide the larger anonymity zone's real-time location.	The proposed *k*-DLCA algorithm has a limitation of less user's mobile device communication range.

(continued).

Related work	Strengths	Weaknesses
	Minimize the chances of exposing the actual location of users.	
[59]	The proposed GMLC technique minimizes location services' response time to protect the user's privacy in the mobile core network.	High maintenance and implementation cost of launching new location services.
[60]	Provides better experimental results of user's anonymity of reallocation as well as improved location privacy preservation opportunity.	Users could not select their own desired privacy preservation levels in devices.
[66]	Effectively apply statistical methods to detect and exclude single satellite faults.	Required sufficient satellite visibility clearance for redundancy.
[67]	Quick response to any satellite faults and enhance accuracy using differential corrections.	Limited service coverage area. Need to receive and proceed satellite signals.
[68,69]	Minimizing multiple errors without any objection of external services.	Multiple faults will need the maximum number of receivers and cause complexity.

Although this paper presents review on privacy preservation of location-based services in Internet of Things, the approach can be generalized and made applicable to many other applications within privacy applications. This IoT location study is urgent and essentially to assist dealing with massive crowds and gatherings which can also produce fast statistical information to be dealt with via visualizations [70–74]. On the other hand, The work confidentially consideration is becoming vital problem affecting all IoT data. Because of high location mobility streaming demand, specific security methods could help solving this issue via light-weight cryptography and proper security [75].

6 Conclusion

Privacy has become the top of the significant suggestions as to the IoT devices. Protection prolonged methods obscurity in the IoT. Reporting and information mining inside any IoT situation could shape expected damage to people because of the programmed interaction of information assortment, their capacity, and how individual information can be effortlessly shared and examined. In addition, the establishments and guidelines for advanced protection were set up specific years before the Internet incorporation. These guidelines manage the assortment of information and access privileges and guarantee right. That is not true anymore today. At its most straightforward definition, protection implies giving clients the alternative to control how their gathered individual data may be utilized, explicitly for auxiliary utilization and outsider access. For instance, in the online climate, security decisions can be practiced by just clicking a container on the program screen that demonstrates a client's choice concerning utilizing the data being gathered. The idea continued as before in the advancement of long-range interpersonal communication, where clients on Facebook show to whom and to which degree their data can be uncovered. These are known as the standards of notice and decision.

The major consequence faced in the development of the Internet of Things is "Privacy". Information collection and reporting within an IoT situation can be harmful to individuals because personal data can be easily shared due to automation in the process of data collection, storage, and assessment. Unfortunately, security and privacy issues have not always gotten the attention they merit when developing IoT devices and systems, resulting in widespread security issues that affect protected localization, location data, and location based services IoT. Context-awareness is a key feature of IoT, and location data and location-based services play critical roles in such systems. The demand will increase for the use of LBS in terms of technology,

One of the upcoming market trends is the rising popularity of cloud-based analytics. Retailers can boost their sales volume and profitability by using big data analytics to improve their understanding of customer market trends. Improve the search experience for customers big data analytics are used by location-as-a-service companies to provide cloud-based and mobile LBS web services that can incorporate real-time location data.

Recently, a number of traditional methods have been proposed to preserve the privacy of IoT systems and the localization data of the users. When transmitting the information between the devices, the traditional methods of obfuscation simply substitute the true location data with a fake location data. Whereas, some methods aim to avoid the disclosure of unnecessary information, while others rely on access control and anonymization strategies like mix zone. Furthermore, there are numerous solutions for improving the robustness, stability, and privacy of LBSs in the IoT. They always come with hefty costs and necessitate advanced knowledge in order to be properly implemented. All of these methods have certain limitations, therefore keeping in view the aspects of the IoT system and its heterogeneity, it is essential to investigate and research reliable solutions.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] R. Agarwal, D. G. Fernandez, T. Elsaleh, A. Gyrard, J. Lanza *et al.,* "Unified IoT ontology to enable interoperability and federation of testbeds," in *2016 IEEE 3rd World Forum on Internet of Things*, Reston, VA, USA, IEEE, pp. 70–77, 2016.

[2] D. A. Audich, R. Dara and B. Nonnecke, "Privacy policy annotation for semi-automated analysis: A cost-effective approach," in *IFIP Int. Conf. on Trust Management*, Cham, Springer, pp. 29–44, 2018.

[3] K. L. Lueth, "State of the IoT 2018: Number of IoT devices now at 7B–market accelerating," *IOT Analytics*. 2018. [Online]. Available: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

[4] I. Lin and T. Liao, "A survey of blockchain security issues and challenges," *IJ Network Security*, vol. 19, no. 5, pp. 63–72, 2017.

[5] M. Kanellos, "152,000 smart devices every minute in 2025: IDC outlines the future of smart things," 2016. [Online]. Available: https://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/#636d2caa4b63.

[6] R. Das, A. Gadre, S. Zhang, S. Kumar and J. K. F. Moura, "A deep learning approach to IoT authentication," in *2018 IEEE Int. Conf. on Communications*, Kansas City, USA, IEEE, pp. 1–6, 2018.

[7] M. P. Papernot, N. McDaniel, S. Patrick and W. Arunesh, "Sok: Security and privacy in machine learning," in *2018 IEEE European Symp. on Security and Privacy*, UK, pp. 399–414, 2018.

[8] R. P. Minch and P. Robert, "Location privacy in the era of the internet of things and big data analytics," in *2015 48th Hawaii Int. Conf. on System Sciences*, (HICSS), USA, IEEE, pp. 1521–1530, 2015.

[9] J. H. Ziegeldorf, O. G. Morchon and K. Wehrle, "Privacy in the internet of things: Threats and challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, 2014.

[10] S. Jain and N. Kesswani, "IoTP an efficient privacy preserving scheme for internet of things environment," *International Journal of Information Security and Privacy*, vol. 14, no. 2, pp. 116–142, 2020.

[11] R. Kaur, K. Verma, S. K. Jain and N. Kesswani, “Efficient routing protocol for location privacy preserving in internet of things,” *International Journal of Information Security and Privacy*, vol. 13, no. 1, pp. 70–85, 2019.

[12] S. Kraijak and P. Tuwanut, “A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends,” in *2015 IEEE 16th Int. Conf. on Communication Technology*, Korea (South), pp. 26–31, 2015.

[13] S. Moganedi and J. Mtsweni, “Beyond the convenience of the internet of things: Security and privacy concerns,” in *IST-Africa 2017 Conference, 02 June 2017*, Windhoek, Namibia, pp. 1–10, 2017.

[14] S. K. Jain, N. Kesswani and B. Agarwal, “Security, privacy and trust: Privacy preserving model for internet of things,” *International Journal of Intelligent Information and Database Systems*, vol. 13, no. 2–4, pp. 249–277, 2020.

[15] S. Sicari, A. Rizzardi and L. A. Grieco, “Security, privacy and trust in internet of things: The road ahead,” *Computer Networks*, vol. 76, no. 15, pp. 146–164, 2015.

[16] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, “Internet of things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[17] L. Atzori, I. Antonio and M. Giacomo, “The internet of things: A survey,” *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[18] A. Riahi Sfar, E. Natalizio, Y. Challal and Z. Chtourou, “A roadmap for security challenges in the Internet of Things,” *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, 2018.

[19] M. Farooq, M. Waseem, A. Khairi and S. Mazhar, “A critical analysis on the security concerns of internet of things (IoT),” *International Journal of Computer Applications*, vol. 111, no. 7, pp. 1–6, 2015.

[20] M. Abdur, S. Habib, M. Ali and S. Ullah, “Security issues in the internet of things (IoT): A comprehensive study,” *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, pp. 383–388, 2017.

[21] D. Miorandi, S. Sicari, F. De Pellegrini and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[22] E. Leloglu, “A review of security concerns in internet of things,” *Journal of Computer and Communications*, vol. 5, no. 1, pp. 121–136, 2016.

[23] H. Sundmaeker, P. Guillemin, P. Friess and S. Woelfflé, “Vision and challenges for realizing the internet of things,” *Cluster of European Research Projects on the Internet of Things, European Commission*, vol. 3, no. 3, pp. 34–36, 2010.

[24] R. Ling, “The sociolinguistics of SMS: An analysis of SMS use by a random sample of Norwegians,” in *Mobile Communications*. London: Springer, pp. 335–349, 2015.

[25] I. Smith, C. Sunny, L. Anthony, H. Jeffrey, S. James *et al.,* “Social disclosure of place: From location technology to communication practices,” in *Int. Conf. on Pervasive Computing and Communications*, (PerCom 2022) March 21–25, 2021 in Pisa, pp. 134–151, 2015.

[26] A. Leonhardi and K. Rothermel, “Architecture of a large-scale location service,” in *Proc. 22nd Int. Conf. on Distributed Computing Systems*, Vienna, Austria, IEEE, pp. 465–466, 2016.

[27] A. Hopper, “The Clifford Paterson lecture 1999, Sentient computing,” *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 358, no. 1773, pp. 2349–2358, 2017.

[28] K. Elgethun, M. G. Yost, C. T. E. Fitzpatrick, T. L. Nyerges and R. A. Fenske, “Comparison of global positioning system (GPS) tracking and parent-report diaries to characterize children’s time-location patterns,” *Journal of Exposure Science & Environmental Epidemiology*, vol. 17, no. 2, pp. 196–206, 2006.

[29] K. Kaemarungsi and P. Krishnamurthy, “Properties of indoor received signal strength for WLAN location fingerprinting,” in *The First Annual Int. Conf. on Mobile and Ubiquitous Systems: Networking and Services*, Boston, Massachusetts, USA, IEEE, pp. 14–23, 2014.

[30] V. Honkavirta, T. Perala, S. Ali-Loytty and R. Piché, “A comparative survey of WLAN location fingerprinting methods,” in *2009 6th Workshop on Positioning, Navigation and Communication*, IEEE, pp. 243–251, 2019.

[31] H. Liu, H. Darabi, P. Banerjee and J. Liu, “Survey of wireless indoor positioning techniques and systems,” *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 6, pp. 1067–1080, 2017.

[32] M. Rahnema, “Overview of the GSM system and protocol architecture,” *IEEE Communications Magazine*, vol. 31, no. 4, pp. 92–100, 2011.

[33] Y. Liu, Z. Yang, X. Wang and L. Jian, “Location, localization, and localizability,” *Journal of Computer Science and Technology*, vol. 25, no. 2, pp. 274–297, 2014.

[34] V. Memos, K. E. Psannis, B. G. Kim and B. B. Gupta, “An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework,” *Future Generation Computer Systems*, vol. 83, no. 7, pp. 619–628, 2018.

[35] R. Schlegel, C. Y. Chow, Q. Huang and D. S. Wong, “User-defined privacy grid system for continuous location-based services,” *IEEE Transactions on Mobile Computing*, vol. 14, no. 10, pp. 2158–2172, 2015.

[36] M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe *et al.,* “A comprehensive approach to privacy in the cloud-based Internet of Things,” *Future Generation Computer Systems*, vol. 56, pp. 701–718, 2016.

[37] A. Sadeghi, C. Wachsmann and M. Waidner, “Security and privacy challenges in industrial internet of things,” in *52nd ACM/EDAC/IEEE Design Automation Conf.*, San Francisco, CA, USA, IEEE, pp. 1–6, 2015.

[38] C. Chow, M. Mokbel and W. Aref, “Casper: Query processing for location services without compromising privacy,” *ACM Transactions on Database Systems*, vol. 34, no. 4, pp. 1–48, 2011.

[39] D. Liao, H. Li, G. Sun, V. Anand, B. Niu *et al.,* “Protecting user trajectory in location-based services, enhancing privacy through caching in location-based services,” in *2015 IEEE Global Communications Conf.*, USA, IEEE, pp. 1–6, 2015.

[40] A. Ye, Y. Li and L. Xu, “A novel location privacy-preserving scheme based on l-queries for continuous LBS,” *Computer Communications*, vol. 98, no. 10, pp. 1–10, 2017.

[41] X. Caron, R. Bosua, S. Maynard and A. Ahmad, “The internet of things (IoT) and its impact on individual privacy: An Australian perspective,” *Computer Law & Security Review*, vol. 32, no. 1, pp. 4–15, 2016.

[42] R. Minch, “Location privacy in the era of the internet of things and big data analytics,” in *IEEE Hawaii 48th Int. Conf. on System Sciences*, USA, pp. 521–530, 2015.

[43] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov *et al.,* “The quest for privacy in the internet of things,” *IEEE Cloud Computing*, vol. 3, no. 2, pp. 36–45, 2016.

[44] S. Sicari, A. Rizzardi, L. Grieco and A. Coen-Porisini, “Security, privacy and trust in internet of things: The road ahead,” *Computer Networks*, vol. 76, no. 15, pp. 146–164, 2015.

[45] B. Weinberg, G. Milne, Y. Andonova and F. M. Hajjat, “Internet of things: Convenience *vs*. privacy and secrecy,” *Business Horizons*, vol. 58, no. 6, pp. 615–624, 2015.

[46] M. Henze, L. Hermerschmidt and D. Kerpen, “A comprehensive approach to privacy in the cloud-based internet of things,” *Future Generation Computer Systems*, vol. 56, no. 15, pp. 701–718, 2016.

[47] L. González-Manzano, J. de Fuentes and S. Pastrana, “PAgIoT privacy-preserving aggregation protocol for internet of things,” *Journal of Network and Computer Applications*, vol. 71, no. 1, pp. 59–71, 2016.

[48] P. Appavoo, M. Chan and A. Bhojan, “Efficient and privacy preserving access to sensor data for internet of things (IoT) based services,” in *14th Int. Conf. on Communication Systems and Networks*, India, pp. 1–8, 2016.

[49] C. Lai, H. Li and X. Liang, “CPAL: A conditional privacy preserving authentication with access linkability for roaming service,” *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 46–57, 2014.

[50] S. Premnath and Z. Haas, “Security and privacy in the internet-of-things under time-and-budget-limited adversary mode,” *IEEE Wireless Communications Letters*, vol. 4, no. 3, pp. 277–280, 2015.

[51] J. Jin, J. Gubbi and S. Marusic, “An information framework for creating a smart city through internet of things,” *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 112–121, 2014.

[52] C. Perera, C. McCormick and A. Bandara, “Privacy-by-design framework for assessing internet of things applications and platforms,” in *IoT’16: The 6th International Conference on the Internet of Things*, Stuttgart Germany, pp. 83–92, 2016.

[53] S. Zhang, K. K. R. Choo, Q. Liu and G. Wang, “Enhancing privacy through uniform grid and caching in location-based services,” *Future Generation Computer Systems*, vol. 86, no. 2, pp. 881–892, 2018.

[54] T. Peng, Q. Liu, D. Meng and G. Wang, "Collaborative trajectory privacy preserving scheme in location-based services," *Information Sciences*, vol. 387, no. 1, pp. 165–179, 2017.

[55] A. Zarandi, Mohammad, R. A. Dara and E. Fraser, "A survey of machine learning-based solutions to protect privacy in the internet of things," *Computers & Security*, vol. 96, pp. 101921, 2020.

[56] S. K. Jain and N. Kesswani, "A comparative study of location privacy preservation in the internet of things," *Procedia Computer Science*, vol. 171, no. 12, pp. 1760–1769, 2020.

[57] Tyagi, A. Kumar and N. Sreenath, "Location privacy preserving techniques for location based services over road networks," in *2015 2nd Int. Conf. on Communications and Signal Processing-ICCSP*, China, pp. 1319–1326, 2015.

[58] D. Dan, X. Huang, V. Anand, G. Sun and H. Yu, "k-DLCA: An efficient approach for location privacy preservation in location-based services," in *2016 IEEE Int. Conf. on Communications*, 23–27 May 2016, Kuala Lumpur, Malaysia, pp. 1–6, 2016.

[59] M. Aal-Nouman, O. H. Salman, H. Takruri-Rizk and M. Hope, "A new architecture for location-based services core network to preserve user privacy," in *2017 Annual Conf. on New Trends in Information & Communications Technology Applications (NTICT)*, Iraq, pp. 286–291, 2017.

[60] G. Sun, S. Cai, H. Yu, S. Maharjan, V. Chang *et al.,* "Location privacy preservation for mobile users in location-based services," *IEEE Access*, vol. 7, pp. 87425–87438, 2019.

[61] L. Chen, S. Thombre, K. Järvinen, E. S. Lohan, A. Alén-Savikko *et al.,* "Robustness, security and privacy in location-based services for future IoT: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.

[62] J. Zhang, X. Wang, Y. Yuan and L. Ni, "RcDT: Privacy preservation based on R-constrained dummy trajectory in mobile social networks," *IEEE Access*, vol. 7, pp. 90476–90486, 2019.

[63] J. Kang, D. Steiert, D. Lin and Y. Fu, "MoveWithMe: Location privacy preservation for smartphone users," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 711–724, 2019.

[64] Z. Liu, L. Wu, J. Ke, W. Qu, W. Wang *et al.,* "Accountable outsourcing location-based services with privacy preservation," *IEEE Access*, vol. 7, pp. 117258–117273, 2019.

[65] A. Mujunen, J. Aatrokoski, M. Tornikoski and J. Tammi, "GPS time disruptions on 26-Jan-2016," Feb. 2016, [online] Available: https://aaltodoc.aalto.fi:443/handle/123456789/19833.

[66] European GNSS Agency, *EGNOS Safety of Life (SoL) Service Definition Document, Eur.* Prague, Czech Republic: GNSS Agency, 2015.

[67] M. H. Maras, "Tomorrow's privacy internet of things: Security and privacy implication," *International Data Privacy Law*, vol. 5, no. 2, pp. 99–104, 2015.

[68] T. Walter, J. Blanch, M. Joerger and B. Pervan, "Determination of fault probabilities for ARAIM," in *Proceedings of the IEEE/ION Position, Location and Navigation Symposium*, USA, vol. 55, pp. 451–461, 2016.

[69] E. Borgia, "The internet of things vision: Key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1–31, 2014.

[70] S. A. Aly, T. A. AlGhamdi, M. Salim, H. H. Amin and A. Gutub, "Information gathering schemes for collaborative sensor devices," *Procedia Computer Science*, vol. 32, pp. 1141–1146, 2014.

[71] S. Kim, S. Guy, K. Hillesland, B. Zafer, A. Gutub *et al.,* "Velocity-based modeling of physical interactions in dense crowds," *Vis Comput.*, vol. 31, pp. 541–555, 2015.

[72] S. Aly, T. Alghamdi, M. Salim and A. Gutub, "Data dissemination and collection algorithms for collaborative sensor devices using dynamic cluster heads," *Trends in Applied Sciences Research*, vol. 8, no. 2, pp. 55, 2013.

[73] N. Alharthi and A. Gutub, "Data visualization to explore improving decision-making within Hajj services," *Scientific Modelling and Research*, vol. 2, no. 1, pp. 9–18, 2017.

[74] A. Gutub and A. S. Aly, "Trialing a smart face-recognition computer system to recognize lost people visiting the two holy mosques," *Arab Journal of Forensic Sciences and Forensic Medicine*, vol. 1, no. 8, pp. 1120–1132, 2018.

[75] N. Farooqi, A. Gutub and M. O. Khozium, "Smart community challenges: Enabling IoT/M2M technology case study," *Life Science Journal*, vol. 16, no. 7, pp. 11–17, 2019.