A Survey on Privacy Preservation in Location-Based Mobile Business:
Research Directions

Ahmed Aloui, Intelligent Computer Science Laboratory LINFI, University of Biskra, Algeria

Okba Kazar, Intelligent Computer Science Laboratory LINFI, University of Biskra, Algeria

iD https://orcid.org/0000-0003-0522-4954

ABSTRACT

In mobile business (m-business), a client sends its exact locations to service providers. This data may involve sensitive and private personal information. As a result, misuse of location information by the third party location servers creating privacy issues for clients. This paper provides an overview of the privacy protection techniques currently applied by location-based mobile business. The authors first identify different system architectures and different protection goals. Second, this article provides an overview of the basic principles and mechanisms that exist to protect these privacy goals. In a third step, the authors provide existing privacy protection measures.

1. INTRODUCTION

Nowadays, people are becoming more and busier and therefore prefer online mobile business portals to the markets or offline stores. In this way, websites based on mobile business are the best solution for many entrepreneurs. To be able to sell their products to a large number of users all over the world. The mobile devices with enhanced positioning technology (as GPS) have significantly increased the use of m-business. M-business is a general category of information services available to mobile users that uses information about the geographic locations of mobile clients based on mobile communication technologies (for example GPS). As a result, new types of m-business applications providing location-based services (LBS) have become popular in recent years.

In m-business, a customer sends its exact locations to service providers. This data may involve sensitive and private personal information. As a result, misuse of location information by service providers creating privacy issues for customers. Therefore, location-based mobile business can also pose a serious threat to the privacy of users (Shklovski, Mainwaring et al., 2014). For example, revealing specific user location may allow an adversary to derive sensitive information when a user

visits, such as a hospital. In addition, revealed user data could be used for criminal harassment, armed robbery or search for empty houses for burglary. As a result, mechanisms for protecting location privacy are mandatory when using m-business providing LBS. A mechanism most commonly used to protect users' locations is the obfuscation of the location, which deliberately reduces the accuracy of a location, so that attackers can only retrieve coarse-grained location information (Ardagna et al., 2007).

Mechanisms implementing the concept of k-anonymity (Kalnis et al., 2007) to protect the identity of the user (examples of different privacy goals). In general, these mechanisms attempt to find a set of k users that cannot be distinguished from each other, so that an attacker cannot identify a single user outside of this set.

Location information has three aspects: identity, location, and time. If an attacker is able to make the connection between them, the privacy of the location is broken. Historical location data are also important because they enable behavior models to be established and possibly identify the user's home, place of work and generally frequented places.

In the 19th century, Louis Brandeis defines the term of privacy and is actually quite simple: "The right to be left alone" (Wightman et al., 2013), that is why privacy itself is a complex subject. There are different approaches to meeting the privacy requirements of m-business providing LBS. Some are designed to protect the user's identity when sending queries; others focus on protecting specifically the user's location. Some have also proposed protocols for the query privacy specifically as well. In (Micciancio et al., 2010) the authors have presented a framework providing specifics to obfuscate queries. An ideal approach to ensure the privacy of the location would provide statistics on the behavior of m-business users while protecting each individual identity and location information. Statistics are important to ensure service improvements that enable Ambient Intelligence techniques.

This paper will provide information on available Location Privacy Protection Mechanisms (MPPPs), identify their ease of use and provide a measure for comparing methods. In addition, in this article, we present the key concept of location privacy metric. A location privacy metric is used to estimate the level of protection offered to users.

The rest of the paper is organized as follows. The relation between m-business and web portals are discussed in Section 2. The privacy model is discussed in Section 3. The different system architectures for the customer privacy protection are presented in section 4. In section 5, we define the different protection objectives. The technological measures for the protection of privacy are presented in section 6. In section 7, we provide an overview of existing mechanisms for user privacy protection to achieve the different protection objectives. In section 8, we propose a qualitative comparison of the mechanisms based on a simple comparison table. Discussion and analysis are presented in section 9. Finally, existing privacy protection measures, conclusions and future works are drawn in section 10 and 11.

2. M-BUSINESS AND WEB PORTALS

The Web has had a significant impact on the role of the mobile business: selling goods and services, electronic data interchange (EDI) network, mail or other online system. A standard corporate m-business web portal used for much of an organization's online business presence can encompass internal enterprise systems, corporate communication and collaboration, and the mobile business for remittances, of goods, services and / or data between companies (B2B) or between the company and its customers (B2C). The new m-business portal model includes web-based communities and hosted services such as social networking capabilities and social savings to facilitate creativity, collaboration, and user-to-user sharing.

Web Portal Solution is a web site designed to provide customized functionality for its visitors. Additionally, business web portals are created to share workplace communication.

Related Content

Facet of Modeling Web Information Systems from a Document-Centric View
Bálint Molnárand András Benczúr (2013). *International Journal of Web Portals (pp. 57-70).*
www.irma-international.org/article/facet-of-modeling-web-information-systems-from-a-document-centric-view/103983

The IFIP Portal
Arthur Tatnalland J. Barrie Thompson (2007). *Encyclopedia of Portal Technologies and Applications (pp. 469-475).*
www.irma-international.org/chapter/ifip-portal/17914

Delivering Deep Health Information Using Clinical Eye
Olga Nabuco (2013). *International Journal of Web Portals (pp. 28-40).*
www.irma-international.org/article/delivering-deep-health-information-using/78351

Economical Aspects when Deploying Enterprise Portals
Shota Okujavaand Ulrich Remus (2007). *Encyclopedia of Portal Technologies and Applications (pp. 282-289).*
www.irma-international.org/chapter/economical-aspects-when-deploying-enterprise/17883

Evaluating Students' Perceptions of Interactive Response System (IRS): Extending Technology Acceptance Model
Ying Chieh Liu (2011). *New Generation of Portal Software and Engineering: Emerging Technologies (pp. 233-245).*
www.irma-international.org/chapter/evaluating-students-perceptions-interactive-response/53742