A New Fuzzy-Based Approach for Anonymity Quantification in E-Services

Wiem Hammami, Higher Institute of Management of Tunis, University of Tunis, Tunis, Tunisia
Ilhem Souissi, National School of Computer Science, Tunis, Tunisia
Lamjed Ben Said, Higher Institute of Management of Tunis, University of Tunis, Tunis, Tunisia

ABSTRACT

In online services, making anonymous transactions is a crucial need in order to ensure the user’s trust towards a particular service. In this context, anonymity quantification is required to provide at which level the e-service respects the user privacy regarding the link between his/her identity and actions. Most of the existing researches are limited to the anonymity quantification in a static way and based, mainly, on the user’s set size. In this paper, the authors propose a new multi-agent based approach for anonymity quantification in e-services considering dynamic and mobile environment’s characteristics. The authors’ quantification is based on the fuzzy logic. It is based not only on the anonymity set size, which is always known in advance, but also on a set of other criteria such as the number of users and the priori and posteriori knowledge about internal and external attackers of an e-service. The carried out experimentations show competitive and better results when compared to other recently proposed anonymity quantification.

Keywords: Anonymity Quantification, Anonymity, Degree of Anonymity, E-services, Fuzzy Logic, Multi-agent Systems

INTRODUCTION

The Internet user’s data become easier to be collected, used, and stored either legally or illegally. The improvement of data storage tools and traceability mechanisms has a great influence on the “invasion of privacy”. According to ISO (2005), Traceability is an ability to trace the history, application or location of an entity or activity using a recorded identification. In other words, traceability helps to control and track the user’s behavior (purchases, participation in discussion forums, download, cookies, etc.). Thereby, users’ personal data is spread freely in a world without borders either on a voluntary (e.g. data filled in a form) or involuntary way (e.g. hacked data). Despite the implementation of many tools to protect privacy, there is practically no system that can be considered as intangible and completely reliable.

DOI: 10.4018/IJISP.2014070102
An electronic service provides Internet users with a set of interactions in different sectors through the Information and Communication Technologies (ICT) (Goblet, 2009). Examples of e-services include e-commerce, e-business, e-sourcing, e-mall, e-learning, e-government, e-democracy, e-health, e-banking, etc. It is thus the users’ intention to make online transactions using a kind of masks (i.e. pseudonyms) to hide their true identity in order to surf anonymously and without being identified. The anonymity is one of the fundamental properties for the users’ privacy protection in online services. The e-service users need to know about their level of privacy protection and particularly their level of anonymity, which makes the anonymity quantification in the context of e-services a crucial issue. The studies related to the anonymity have been initiated at the beginning of the 80s with David Chaum (1981) in his paper entitled: The non-traceability of electronic mail. The studies carried out at that time were not comprehensive enough. However in 2000, this property (anonymity) has drawn the attention of many researchers. In (Pfitzmann and Hansen, 2000), the authors have proposed the following definition: Anonymity is the state of being not identifiable within a set of subjects, the anonymity set (senders and receivers represent the subjects). In other words, if a sender is seen as an anonymous entity, then, the whole of the anonymity senders cannot identify this sender (the same in the case of a receiver). Therefore, the more the anonymity set is large, the more the subject is anonymous. Anonymity isn’t related only to the subject identity but also to all information that can identify the subject. Thus, the purpose of the anonymity property is to ensure that the link between the user and his real identity is hidden. In some specific e-services, the anonymity becomes a fundamental requirement where the identity of the user cannot be revealed in any cases. For example, in e-voting, it should be impossible to discover the real identity of the voter. The major problem in this case, is that e-service entities must ensure that a voter has the right to vote and it should be impossible to reveal and prove the relationship between a voter and his cast vote (Diaz, Claessens, & Preneel, 2003). A service that provides a secure and confidential use of data does not necessarily guarantee the user anonymity. The entities that use this service need to know at which level, it respects their anonymity.

In open environments with dynamic and mobile characteristics, anonymity quantification can no longer be based on certain and precise data. Most existing studies are limited to handle only the case where the number of service users is fixed in advance without considering any kind of knowledge about the attackers. In this context, we propose a new approach to quantify anonymity that considers the following criteria:

- The number of users is not fixed in advance.
- The service may learn some priori knowledge about the internal and external attackers.
- The service may learn some posteriori knowledge about the internal and external attackers.

In this paper, we propose a multi-agent model based on the fuzzy logic to measure the anonymity level for a specific e-service user while considering the above-mentioned criteria. This model is based on the fuzzy logic in order to quantify anonymity in dynamic environments (e.g. pervasive, mobile, etc.). We choose the fuzzy logic because it can handle uncertain data such as the varying number of the uncertain knowledge that an attacker may gain. Our model allows users to control and track their anonymity level. It helps administrators to detect the system vulnerabilities and to control the influence of attackers’ knowledge on the anonymity level. A multi-agent based simulation is performed to illustrate the applicability of our model and to study the system performances. The rest of this paper is structured as follows. In the next section, we present a summarized view of existing works on anonymity and anonymity quantification. In section 3, we describe and discuss our new anonymity quantification model.
24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage: [www.igi-global.com/article/a-new-fuzzy-based-approach-for-anonymity-quantification-in-e-services/136364?camid=4v1](www.igi-global.com/article/a-new-fuzzy-based-approach-for-anonymity-quantification-in-e-services/136364?camid=4v1)


Related Content

Observations on Genderwise Differences among University Students in Information Security Awareness

Impact of Technology Innovation: A Study on Cloud Risk Mitigation
Niranjali Suresh and Manish Gupta (2018). *Information Technology Risk Management and Compliance in Modern Organizations* (pp. 229-267). [www.igi-global.com/chapter/impact-of-technology-innovation/183242?camid=4v1a](www.igi-global.com/chapter/impact-of-technology-innovation/183242?camid=4v1a)
Creating a Policy-Aware Web: Discretionary, Rule-Based Access for the World Wide Web
www.igi-global.com/chapter/creating-policy-aware-web/31080?camid=4v1a

Integrating Security in the Development Process with UML
www.igi-global.com/chapter/integrating-security-development-process-uml/23123?camid=4v1a