Accepted Manuscript

PrivBox: Verifiable decentralized reputation system for the on-line marketplaces

Muhammad Ajmal Azad, Samiran Bag, Feng Hao

PII: S0167-739X(17)33031-5
DOI: https://doi.org/10.1016/j.future.2018.05.069
Reference: FUTURE 4244

To appear in: *Future Generation Computer Systems*

Received date : 31 December 2017
Revised date : 4 April 2018
Accepted date : 27 May 2018

Please cite this article as: M.A. Azad, S. Bag, F. Hao, PrivBox: Verifiable decentralized reputation system for the on-line marketplaces, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.05.069

PrivBox: Verifiable Decentralized Reputation System for the On-line Marketplaces

Muhammad Ajmal Azad, Samiran Bag, Feng Hao

School of Computing Science, Newcastle University, Newcastle Upon Tyne, United Kingdom

Abstract

In online marketplaces (e-commerce, cloud marketplaces), potential buyers/consumers do not have direct access to inspect the quality of products and services offered by service providers or retailers of the marketplace. Therefore, consumers have to trust the reputation system of the online marketplace for deciding whether or not to interact with the particular service provider. Consumer's feedback about the service provider plays an important role to evaluate the trustworthiness of the service provider, but it brings the challenge of security and privacy of the feedback providers. Existing centralized reputation systems collect feedback from consumers about their service providers but they leak sensitive information about consumers transactions (such as buying history, likes and dislikes). To ensure the privacy of consumers, this paper presents a privacy-preserving decentralized reputation system named PrivBox that protects consumer's feedback values using homomorphic cryptographic methods and zero-knowledge proof primitives in a decentralized way. The design of PrivBox ensures the following characteristics. 1) It ensures the privacy of consumers without the use of any trusted setup or trusted third party, 2) it ensures that consumer's provided feedback value remains within the prescribed range, and 3) it enables consumers and service providers to verify the aggregated reputation without relying on any trusted third party. PrivBox achieves privacy-preservation properties using an encrypted exchange of feedback values and ensures well-formedness of encrypted values using zero-knowledge proof of knowledge. To evaluate the performance, we implement a prototype of the proposed system. The results demonstrate that our solution preserves privacy of participants while incurring only small computation and bandwidth overheads.

Keywords: Online Marketplaces, Privacy Preservation, Decentralized Reputation Aggregation, E-commerce, Cloud Marketplaces

1. Introduction

It is estimated that around 1.61 billion people around the world have purchased products and services over the Internet (online) marketplaces (for example Amazon, eBay, Taobao, Rakuten, Alibaba etc.) in the year 2017 [1]. These transactions result in an aggregate revenue of around 1.9 trillion US dollars [2]. Recent statistical forecast for the online marketplaces shows that sales over the online marketplaces will be increasing rapidly and would earn a revenue of more than 4 trillion US dollars by the year 2020 [3]. Other online systems such as Airbnb, Uber etc. have also attracted a large number of users for the services other than purchasing products (for example room sharing, room, and car booking etc.). Recently, cloud marketplaces operated by the cloud service providers (for example, AWS Marketplace, Oracle Marketplace, salesforce, Azure Marketplace) have also attracted a large number of customers by providing consumers an access to the software applications and hardware platforms to perform their computationally expensive tasks. Gartner predicted that cloud marketplaces are expected to reach $71.55 billion by the year 2021 [4].

The online marketplaces have also attracted a large number of fraud retailers who misuse the platform for financial benefits by committing frauds with the consumers. Some of the most common frauds happening today over the online marketplaces are: buyers not receiving goods that they have ordered, receiving products that have inferior value or are significantly different from the original description [5, 6]. The statistics by Experian revealed that e-commerce frauds (online auctions, buying products etc.) have increased by 33% since 2015 [7]. Frauds over the online marketplaces have resulted in an annual loss that cost users billions of dollars all over the world [8, 9, 10].

In the electronic marketplace, a consumer[1] does not have access to physically inspect the products or services before purchasing them, thus has to rely on some third-party information to learn the trustworthiness of retailers or service providers on the marketplace. Similarly, in a cloud-based edge computing, the consumer may wish to know the trustworthiness of nearby mobile edge before outsourcing the sensitive information to the edge nodes.

Email addresses: muhammad.azad@ncl.ac.uk (Muhammad Ajmal Azad), samiran.bag@ncl.ac.uk (Samiran Bag), feng.hao@ncl.ac.uk (Feng Hao)

[1]The terms consumer and buyer are used interchangeably in this paper and refer to the same entity.