

Secure payment on Internet?

March 31 2015

Now that it has become a common feature on the news to hear about cyber attacks on an international scale, cybersecurity is seen as a first priority by Internet users. There can be no doubt that the web has become a battleground without borders on which to defend political, financial and ideological interests. We are all affected by this struggle, since it is almost impossible to avoid operating through Internet, but, at what price?

Cybersecurity, or [data security](#), in other words the practice of defending information systems against external attacks, comprises both the actual data systems themselves and the area of communications. Cybersecurity, therefore, covers both the processes and mechanisms associated with our hardware equipment (for example, servers or cell phones), and the information that flows or is stored through them, and also the services that they enable, protecting them from unauthorized and malicious access as well as from alteration or destruction of the data.

It is common knowledge that there is much more information in data than the data themselves. For instance, it is possible to classify neighborhoods in a city just by observing cell phone use patterns. Cybersecurity should not be limited, therefore, to the data and the user's [information system](#), but must extend its analysis considerably further afield. To do so, it must incorporate studies of the structures and patterns underlying the data, and combine the internal data of a given entity with other external data sources.

In this context, IMDEA Networks Institute has recently concluded a

pioneering research project, led by the private company Zed Worldwide S.A. and financed by the CDTI (the Spanish Centre for the Development of Industrial Technology), for the analysis and evaluation of secure payment systems on Internet with the aim of detecting fraudulent users and transactions. This project, called iPAY, has applied [data mining techniques](#) on Big Data to create a technology platform for financial intermediation in a mobile cloud computing environment. The Madrid based institute has focused its research in networks on developing techniques and algorithms that will identify security threats or breaches in secure payment systems. To conduct this study millions of data have been analyzed, originating from different Internet sources (websites, blogs, social networks, etc.).

The result of this project consists of two modules that combine to form a powerful [cybersecurity](#) technology platform. First of all, graph algorithms have been designed and developed for analyzing and detecting fraud patterns, in conjunction with data mining techniques applied to payment transactions. In this module, algorithms have been designed to analyze payments made by users. Payment data are modeled in graphs to identify patterns of behavior that enable fraudulent actions to be detected in organized networks for money laundering, arbitration of exchange, etc. Secondly, a prediction system was developed based on payment transaction history. In this module algorithms have been designed and developed to predict user behavior and identify future purchases of interest, as well as operations outside the usual casuistry which are likely to be fraudulent.

With this study, IMDEA Networks has shown that it is possible to prevent and identify potential malicious behavior online. On Internet, as in real life, the unusual ways of relating with others and behavior that we associate with fraud and dishonesty allow us to find mechanisms for staying alert and prepared against cybercriminals.

More information: "Empirical Comparison of Graph-based Recommendation Engines for an Apps Ecosystem." *International Journal of Interactive Multimedia and Artificial Intelligence*, 3 (2). pp. 33-39. ISSN 1989-1660

Provided by IMDEA Networks Institute

Citation: Secure payment on Internet? (2015, March 31) retrieved 28 April 2024 from <https://phys.org/news/2015-03-payment-internet.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.