**ABSTRACT**

The increased usage of cloud services, growing number of web applications users, changes in network infrastructure that connects devices running mobile operating systems and constantly evolving network technology cause novel challenges for cyber security. As a result, to counter arising threats, network security mechanisms, sensors and protection schemes also have to evolve, to address the needs and problems of the users. In this article, we focus on countering emerging application layer cyber-attacks since those are listed as top threats and the main challenge for network and cyber security. The major contribution of the article is the proposition of machine learning approach to model normal behaviour of application and to detect cyber-attacks. The model consists of patterns (in form of Perl Compatible Regular Expressions (PCRE) regular expressions) that are obtained using graph-based segmentation technique and dynamic programming. The model is based on information obtained from HTTP requests generated by client to a web server. We have evaluated our method on CSIC 2010 HTTP Dataset achieving satisfactory results