**INTRODUCTION**

Recently the number of security incidents reported all over the world has increased. The national CERTs (e.g. CERT Poland [1]) report that the number of attacks has increased significantly when compared to the previous years. According to the report [1] in 2012 there were 1082 incidents, which is an increase of nearly 80% in comparison to the previous year, mainly due to malware and phishing. The increased number of incidents is strongly related to the increased number of mobile device users who form the population of connect-from-anywhere terminals and regularly test the traditional boundaries of the network security. Also the so-called BYOD (bring your own device [4]) trend exposes the traditional security of many enterprises to novel and emerging threats. Many of nowadays malwares like ZITMO (Zeus In The Mobile) do not aim at mobile device itself but rather on gathering the information about the users, their private data and gaining the access to remote services like banks and web services. There is also a significant number of reported incidents that are connected with a huge widespread adoption of the social media. This trend has an impact on accelerated spread of different kinds of malwares and viruses. As reported by SophosLabs [2] in 2013, botnets have become more widespread, resilient and camouflaged and they are finding some dangerous new targets. Moreover, since cloud services and SaaS have been adapted by small and medium enterprises, a big challenge for network security arises. Such companies store, maintain and transport crucial data using third party infrastructure where traditional points of inspection cannot be deployed. This trend is connected with the criminals that see the potential to get more return on their investment with cloud attacks, since they only need to ‘hack one to hack them all’. Other well-known problems like attacks on the web applications to extract data or to distribute malicious code still remain unsolved. Cybercriminals continuously steal data and distribute their malicious code via legitimate web servers they have compromised. Moreover, as it is shown in the Figure 1, the attacks on web applications constitute more than a half of all incidents identified by Kaspersky Lab [13]. The list of top 10 most critical risks related to web applications security, provided by OWASP (Open Web Application Security Project) indicates ‘Injection’ (including Structured Query Language (SQL), Operating System (OS) and Lightweight Directory Access Protocol (LDAP) injections) as a major vulnerability [5]. Factors, such as easy exploitability and severe impact of potential attacks are mentioned as the most crucial. To perform an injection attack, the attacker sends a simple text that exploits the syntax of the targeted interpreter, and therefore almost any source of data can be an injection attack vector. A successful injection can cause serious consequences including data loss, corruption, lack of accountability or the denial of access. Additionally, the level of prevalence is described as common, while level of detectability is identified as average [5]. Therefore, in this article we focus on detecting emerging application layer attacks. The major contribution of this article is the proposition of a machine learning technique to model normal behaviour of application and detect cyber attacks. The article is structured as follows: in Section 2, the overview of cyber attack detection techniques based on machine learning is provided. In Section 3, the proposed method is described in detail. In Section 4, the benchmark database used in our experiments is discussed. The experimental set-up and results are presented in Section 5. Conclusions are given thereafter.