Currently, many information systems interact through XML files. These interactions may fall victim to one or more adversary attacks, including: information leakage, dictionary and buffer overflow attacks, cross-site scripting, SQL injection, parameter tampering and more.

The goal of this research is to study a new automated context learning method for producing a list of rules, which describes precisely the usable values ranges of the XML elements within the XML transactions. The studied algorithm allows to (1) decrease the XML attack-surface, and (2) classify XML transactions as abnormal or normal (i.e. attacked or not).

The studied algorithm for automated context-learning XML can be used as an XML firewall to defend against most of the known XML attacks. The XML-firewall framework is divided into separate logical units: the outlier detection model trainer, and the XML-firewall prototype. The model trainer is responsible for inducing value-range rules for XML elements, and to train an XML classification model. It is an off-line program in the sense that it processes historical data only. The XML firewall prototype unit is an on-line program which uses the classification model, trained by the model trainer, to detect and block abnormal XML transactions.