TECHNIQUE FOR DETECTING SUSPICIOUS ELECTRONIC MESSAGES

Abstract

The disclosure relates to a method of detecting suspicious electronic messages. The method is performed in a messaging server which is in communication with a plurality of message senders and a plurality of message receivers, and comprises the steps of: receiving electronic messages sent from the plurality of message senders to at least one message receiver; extracting from each received message at least one message sender feature and at least one message content feature; recording the extracted message sender features and message content features in a database; determining, on the basis of the message content features recorded in the database, whether a specific content feature that can be associated with a current message has already been recorded in the past; if the specific content feature has already been recorded in the past, determining, on the basis of the message sender features recorded in the database, a number of message senders that can be associated with the specific content feature; and classifying the current message as suspicious if the determined number of message senders that can be associated with the specific content feature exceeds a predetermined threshold value. Also disclosed is a messaging server implementing the above described method.

(Fig. 1)