ABSTRACT

TRACKING CHANGING STATE DATA TO ASSIST IN COMPUTER NETWORK SECURITY

A session table includes one or more records, where each record represents a session. Session record information is stored in various fields, such as key fields, value fields, and timestamp fields. Session information is described as keys and values in order to support query/lookup operations. A session table is associated with a filter, which describes a set of keys that can be used for records in that table. A session table is populated using data contained in security information/events. Rules are created to identify events related to session information, extract the session information, and use the session information to modify a session table. A session table is partitioned so that the number of records in each session table partition is decreased. A session table is processed periodically so that active sessions are moved to the current partition.

Fig. 1