

Abstract

Hypervisor-based attestation of data provenance for mobile device applications is disclosed. A hypervisor in a mobile device blocks write permission
5 of software on a buffer so that only a hardware device can write to the buffer. Raw data inputted via hardware are intercepted by the hypervisor. The intercepted raw data are signed with security information at least including the hypervisor signature and a current timestamp, for generating an attestation message to be transmitted to a remote server for verification. At a remote server, an incoming current
10 attestation message is verified at least for a valid hypervisor signature, and an identical precedent for a current timestamp included in the current attestation message from any previous attestation message for a user identity of the current attestation message. Based on the verification criteria, a determination is made as to whether data provenance is from authenticated human user or software user.

15

(Figure 3)