

METHOD AND SYSTEM WITH MULTIPLE HETEROGENEOUS TEE IMPLEMENTATIONS

Abstract

A TEE system that includes a first platform that runs a first TEE, a second platform that runs a second TEE, and a merging unit that is adapted to merge a first output from the first TEE of the first platform, with a second output from the second TEE of the second platform, so as to form an output of the TEE system. The first TEE and the second TEE are based on different implementations. In this way, the security of the system is improved, as a malicious actor even be able to access “t” machines, still would not be able to retrieve the secret unless there are multiple exploitable TEE vulnerabilities on all executing TEE platforms at the same time.

Fig. 1