CLOUD SERVICE ACCESS PERMISSION SETTING METHOD FOR ENCLAVE INSTANCE AND CLOUD MANAGEMENT PLATFORM

ABSTRACT

A cloud service access permission setting method for an enclave instance and a cloud management platform are provided. The cloud management platform provides an IAM service and an STS. The IAM service is used to confirm an enclave enclave instance type input or selected by a first tenant and a conversion rule input or selected by the first tenant. The conversion rule is used to convert, into a tenant-customized attribute, an enclave instance attestation document provided by an enclave instance corresponding to the enclave enclave instance type. The STS is used to receive a token obtaining request sent by an application program in the enclave instance. The token obtaining request carries the enclave instance attestation document. The STS is further used to: convert the attestation document into the tenant-customized attribute according to the conversion rule, and return, to the application program, a token carrying the tenant-customized attribute. The token indicates that the application program in the enclave instance has permission to access a target cloud service.

FIG. 4