Panayiotis Charalambous

Thesis Proposal

The thesis project will aim to provide a solution for Cloud Based Services (CSPs) that wish to protect their clients' data in a secure but also efficient way. With Attribute Based Encryption (ABE) combined with Symmetric Searchable Encryption (SSE) and Functional Encryption (FE) clients can store their data on the cloud with keys that the provider does not have access to while also being able to search or run functions on the data, without downloading them back to the client devices. Strict but flexible access control can be enforced to the data and with the use of Trusted Execution Environments (TEEs) to protect the sensitive parts of the system, CSPs can offer security guarantees that could not be given in the past.

This thesis project will focus on the different parts that comprise a system running ABE such as the Master or Revocation Authorities, key creation, storage and more. The authorities are the backbone and need to be secured using the best practices which we aim to achieve using TEEs. Security and performance evaluation will be done to compare this solution with different implementations and approaches in the research community.

In ABE, the creation of a key is a procedure that requires the cooperation of various components. First, a registration authority needs to provide a model of attributes. These attributes will describe each user depending on location, physical or technical characteristics etc. The selection of the attributes that will be available is something that needs to be examined thoroughly. After the assignment of the attributes, a request will be made to the master authority which is responsible for the creation of the symmetric keys. After acquiring the key, a user can perform encryption on data. The encryption functions will be executed in a trusted environment which is a challenge that has not been tackled yet.

There are a few factors that need to be taken into consideration in the creation of such system.

Firstly, it is important to separate which components are required to run in a trusted environment such as an enclave. The master authority which will be responsible for the creation of the keys, is a single point of failure for the system. A compromised master authority means that all data can be decrypted as any key can be created to satisfy any attribute policy. In addition, a remote attestation protocol that will be implemented, will provide integrity assurance to all parts of the system that run in enclaves. Before any communication, these tests will be conducted to ensure that no part of the system has been compromised.

The work that will be done is novel and the implementation specifics will stem out of deep research into the existing ABE schemes, trusted execution environment options and remote attestation protocols that in the end, will provide a service that offers ABE functionalities in a secure and trusted way.

Student Signature	Supervisor Signature	Supervisor Signature
Panayiotis Charalambous	Prof. Paola Grosso	Prof. Antonios Michalas