BVRIT HYDERABAD
College of Engineering for Women
Department of Information Technology
Mini Project - Academic Year 2019-20

TEAM 20

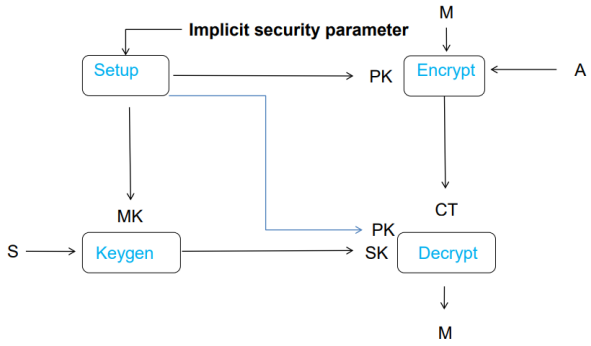
Cipher Text Policy Attribute Based Encryption

Abstract

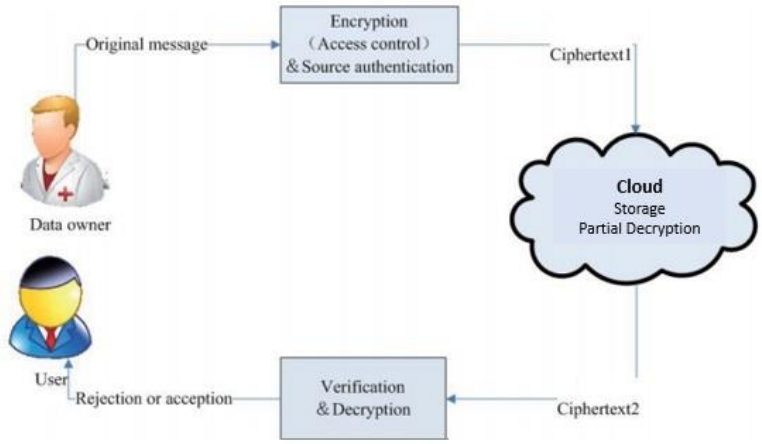
In cloud, for achieving access control and keeping data confidential, data owners could adopt attribute-based encryption to encrypt the stored data. Users with limited computing power are however more likely to delegate the mask of the decryption task to the cloud servers to reduce the computing cost. As a result, attribute-based encryption with delegation emerges. It enables to achieve strongest form of access control, a construction for realizing circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation has been considered in the project. In such a system, combined with verifiable computation and encrypt-then-mac mechanism, the data confidentiality, the fine-grained access control and the correctness of the delegated computing results are well guaranteed at same time.

Modules

Data Owner
Data Consumer
Admin
Cloud Server



Architecture



Tools and Technologies

- **NetBeans 8.02**
- **Advanced Java (Servlets, JSP)**
- **MySQL 5.0**
- **Apache Tomcat 8.0.15**
- **HTML, CSS**

Conclusion and Future Scope

In this project, Cipher Text Policy Attribute Based Encryption is used where attribute policies are associated with data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data. It will be suitable for the application that needs high level security and accessed time is being reduced which indeed cost is reduced comparatively. Thus, we could apply it to ensure the data confidentiality, the fine-grained access control and the verifiable delegation in cloud.

Guide

Ms. S. Rama Devi
Associate Professor of IT
ramadevi.s@bvrithyderabad.edu.in

Team

12WH1A1217
D. N. V. Kiranmai