

Selective and Authentic Third-Party distribution of XML Documents

- Yashaswini Harsha Kumar
- Netaji Mandava

(Oct 16th 2006)

Contents

- ◆ Terminology
- ◆ Security Properties
- ◆ XML Overview
- ◆ Merkle Hash function
- ◆ Access Control Model
- ◆ Architecture
- ◆ Actor Interactions
- ◆ References

Terminology

- ◆ Owner : Producer of information
- ◆ Publisher : Manages the owner information and answers subject queries.
- ◆ Subject : A person who produces queries for documents.
- ◆ Merkle Hash Trees : A Merkle hash tree is a tree of hashes in which the leaves are hashes of data blocks in, for instance, a file or set of files. Nodes further up in the tree are the hashes of their respective children. For example, in the picture to the right *hash 0* is the result of hashing *hash 0-0* and then *hash 0-1*. That is, $hash\ 0 = hash(hash\ 0-0 | hash\ 0-1)$.