CERIAS

the center for education and research in information assurance and security

A Selective Encryption Approach to Fine-Grained Access control for P2P File Sharing

Aditi Gupta, Salmin Sultana, Michael Kirkpatrick and Dr. Elisa Bertino
(Purdue University)

Access Control Policies (ACPs)

- ACPs specify which users can access which byte ranges
- ACPs are specified by file owner
- File owner can access entire file

Acp1 • Range:[2301-9999], Users: {Eve}

Acp2 • Range:[5001-17500], Users: {Bob}

Acp3 • Range:[0-1000], Users: All (Public policy)

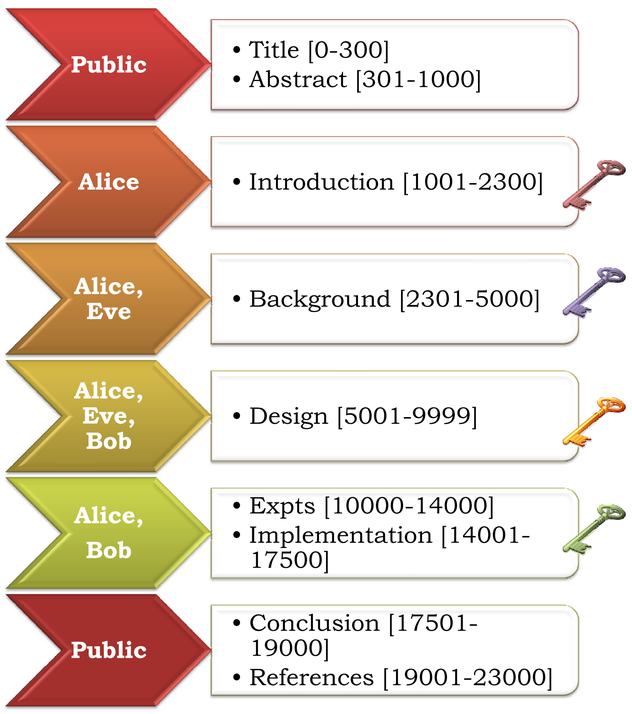
Acp4 • Range:[17501-23000], Users: All (Public policy)

File: ResearchPaper.txt
File owner: Alice

- **Title [0-300]**
- **Abstract[301-1000]**
- **Introduction [1001-23000]**
- **Background [2301-5000]**
- **Design [5001-9999]**
- **Experiments [10000-14000]**
- **Implementation [14001-17500]**
- **Conclusion [17501-19000]**
- **References [19001-23000]**

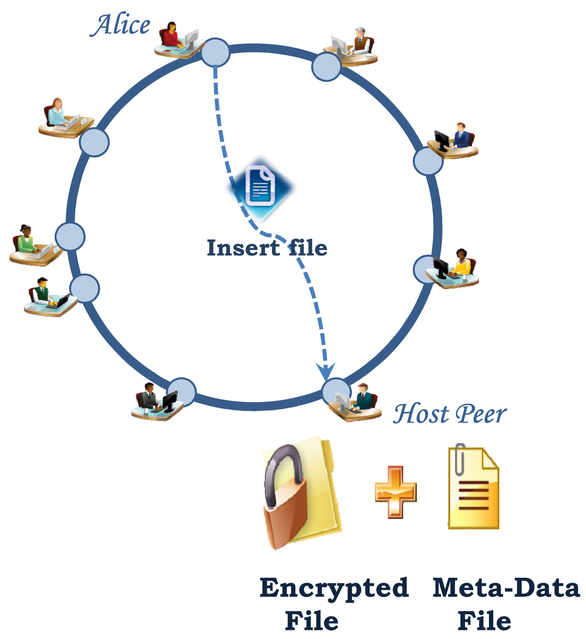
File Partition and Minimal key Generation

- Generate file partitions based on ACPs
- Assign a unique key to each user group
- Encrypt file portions with user group key

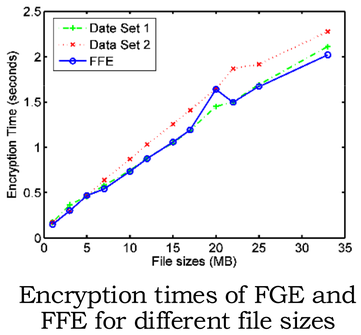


Integration with Chord Peer-to-Peer system

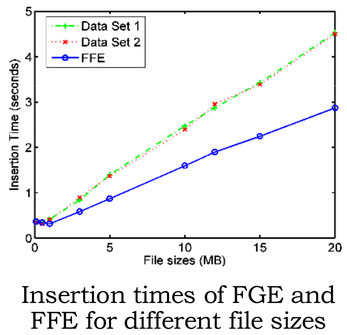
- Owner inserts selectively encrypted file and meta-data into Chord P2P
- Both files are inserted into same node
- Meta-data file contains information to derive decryption keys



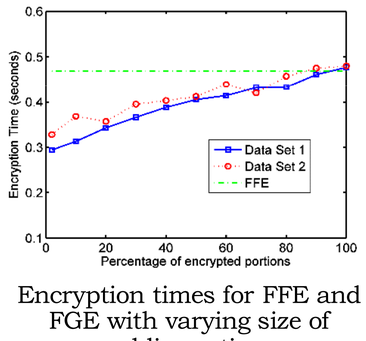
Experiments and Results



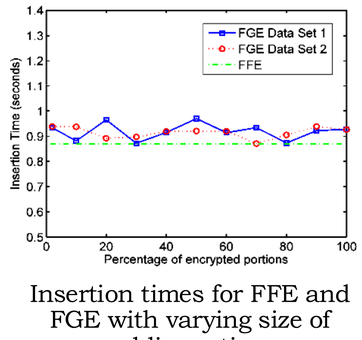
Encryption times of FGE and FFE for different file sizes



Insertion times of FGE and FFE for different file sizes



Encryption times for FFE and FGE with varying size of public portions



Insertion times for FFE and FGE with varying size of public portions

FFE: Full File Encryption, FGE: Fine Grained Encryption

Main Contributions

1. **FGAC mechanism** that allows policies over **arbitrary byte ranges** with no assumptions regarding the file structure.
2. **Low-level architecture** that can be extended to implement previous block- and file-level access control schemes.
3. **Integration with Chord** and experimental results about the performance of our prototype.

Future Work

- Develop key recovery mechanisms.
- Support delegation of authorization.
- Minimize total number of keys per user.
- Increase availability of meta-data files using replication schemes.

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center