Access Control for Secure Distributed Data Structures in Distributed Hash Tables

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Research Project's Objective

Develop a security architecture for access control for securely distributed data structures in P2P networks without depending on trusted third parties.



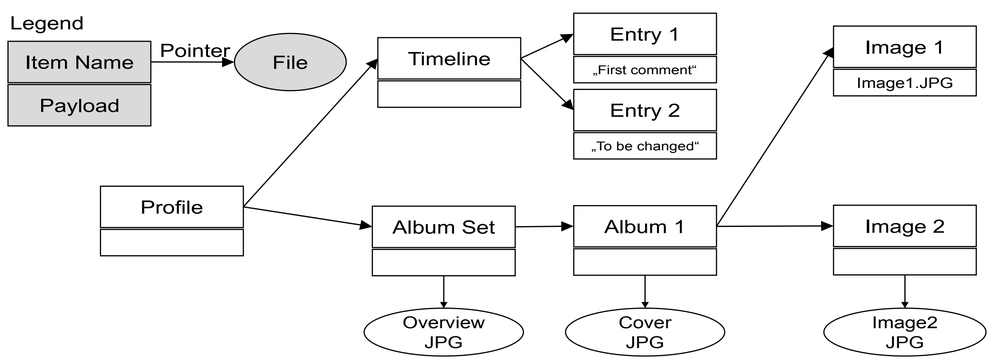
Example use case: LIBRESOCIAL

Distributed Data Structures in P2P Networks

Problem: P2P networks (only) offer storage/retrieve operations based on only single data items. P2P-based online social networks require distributed data structures such as lists, sets or trees.

Approach: Distributed Data Structures (DDS) Project

- Middleware for distributed storage in DHTs
- Offers known data structures in distributed form
  - Such as: Distributed Data Tree, List, Set, ...
- Data fragments stored in a distributed manner
  → Load balancing
- Replication Protocol ensures availability of data



Example of a distributed profile with photo album

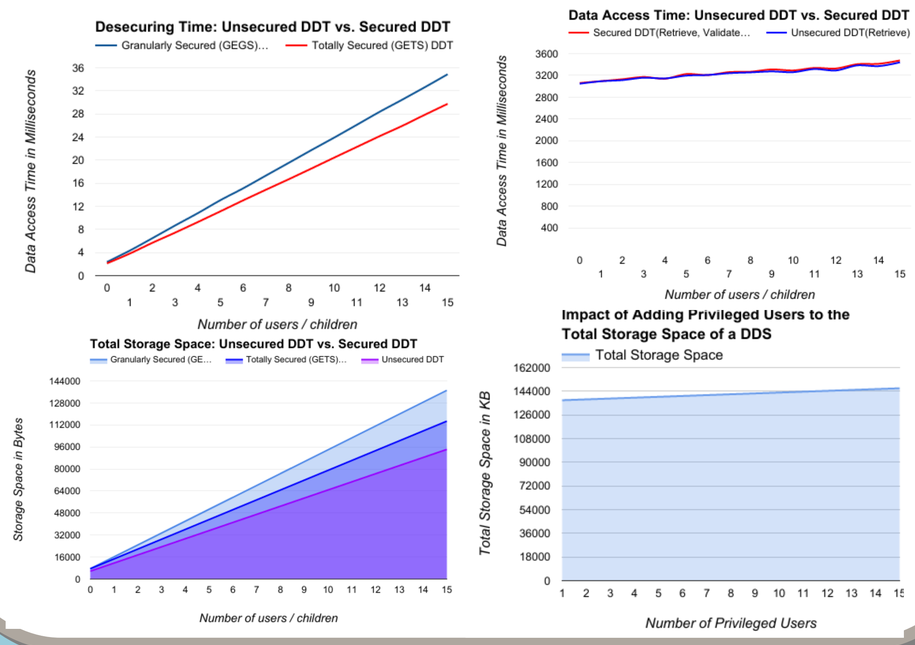
Protecting Identities (Anonymous identities)

Problem: How to protect the identities of users which have privileged access to the data.

Approach: Anonymous identity

→ A public-private key pair specially created for having anonymous access to a certain Distributed Data

Experiments with a list of 15 elements



Security and Access Contol Model

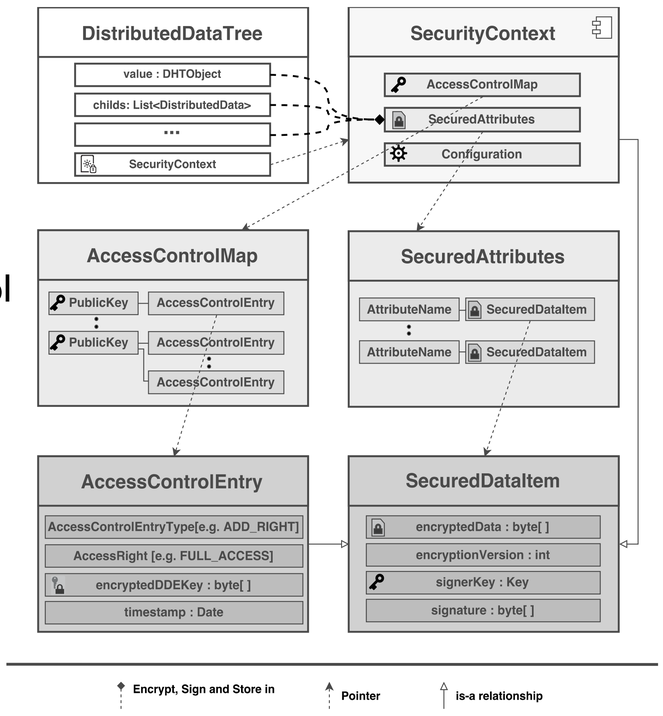
Problem: Difficult to guarantee the security of data stored in P2P networks

A Security Context is a module of a Distributed Data responsible for a complete security and access control

→ Access Control Map

→ Secured Data Items

→ Configuration



SubjectKey	ACE-Type	AccessRight	Enc_DDEKey	EV	TimeStamp	Signer	Signature
Bob							
	ADD_RIGHT	FULL_ACCESS	[1ca484505b..]	0	03.07.2096	Bob	[a835e46358..]
Alice							
	ADD_RIGHT	FULL_ACCESS	[956d345a90..]	0	04.07.2096	Bob	[78342bbac3..]
Carol							
	ADD_RIGHT	READ_ONLY	[bb3573582a..]	0	07.07.2096	Alice	[a4667934cd..]

can Bob give full access?

can Alice give read access?

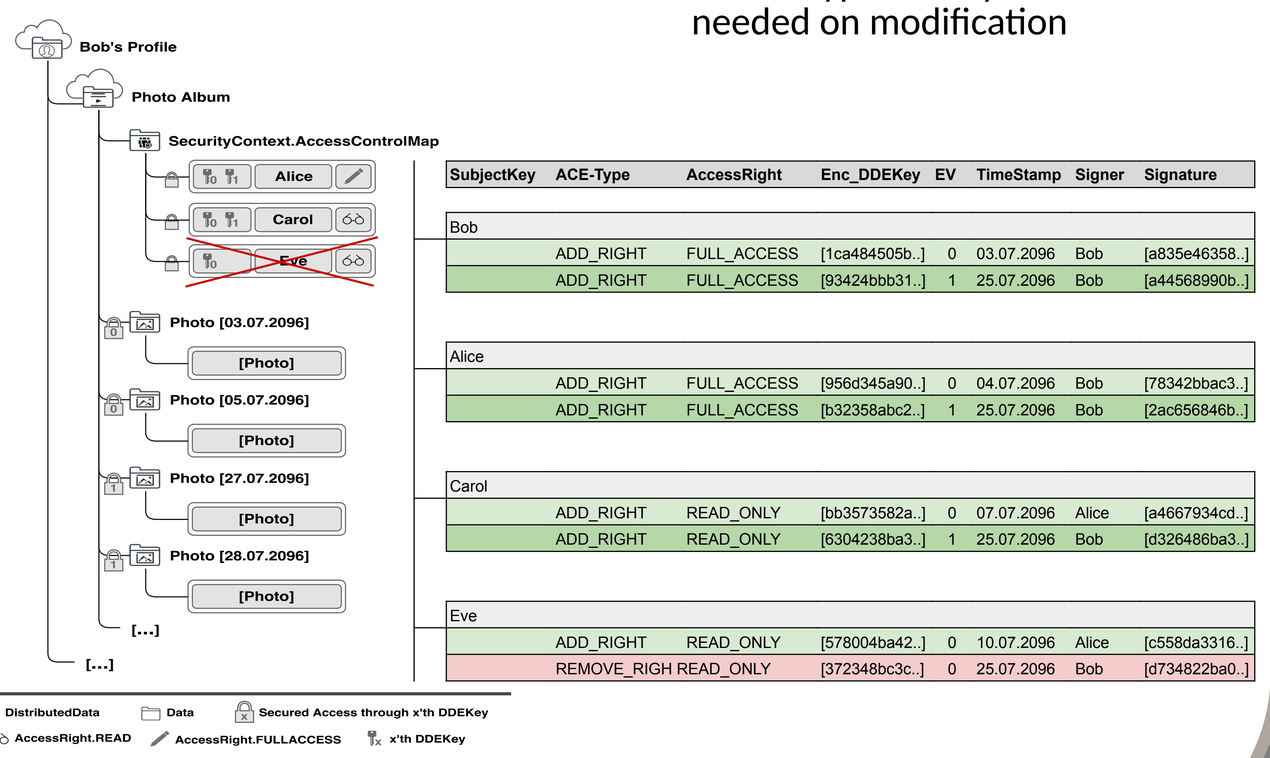
SubjectKey = the public key of the user the access right has been shared with
ACE-Type = AccessControlEntryType
Enc_DDEKey = DDEKey encrypted With the SubjectKey
EV = EncryptionVersion

Access Revocation

Problem: Hard to encrypt all the data with new encypted key in order to revocate the access for one user while he has the ecrypted key

Approach: Lazy Revocation
→ ignore the older versions of the data which the user could have read anyways

→ Re-encryption only needed on modification



SubjectKey	ACE-Type	AccessRight	Enc_DDEKey	EV	TimeStamp	Signer	Signature
Bob							
	ADD_RIGHT	FULL_ACCESS	[1ca484505b..]	0	03.07.2096	Bob	[a835e46358..]
	ADD_RIGHT	FULL_ACCESS	[93424bbb31..]	1	25.07.2096	Bob	[a44568990b..]
Alice							
	ADD_RIGHT	FULL_ACCESS	[956d345a90..]	0	04.07.2096	Bob	[78342bbac3..]
	ADD_RIGHT	FULL_ACCESS	[b32358abc2..]	1	25.07.2096	Bob	[2ac656846b..]
Carol							
	ADD_RIGHT	READ_ONLY	[bb3573582a..]	0	07.07.2096	Alice	[a4667934cd..]
	ADD_RIGHT	READ_ONLY	[6304238ba3..]	1	25.07.2096	Bob	[d326486ba3..]
Eve							
	ADD_RIGHT	READ_ONLY	[578004ba42..]	0	10.07.2096	Alice	[c558da3316..]
	REMOVE_RIGH	READ_ONLY	[372348bc3c..]	0	25.07.2096	Bob	[d734822ba0..]

IEEE LANMAN 2017:
IEEE International Symposium on Local and Metropolitan Area Networks
Osaka, Japan, June 2017

PEER FACT SIM .KOM

Technology of Social Networks

LIBRESOCIAL

HEINRICH HEINE UNIVERSITÄT DÜSSELDORF

Contact:

Raed Al-Aaridhi
Technology of Social Networks
Institute of Computer Science
Heinrich Heine University Düsseldorf
alaaridhi@cs.uni-duesseldorf.de
http://tsn.hhu.de

