Implementation and Performance Analysis of Attribute-Based Encryption(ABE) in ICN

Project Presentation

Nurefşan Sertbaş and Samet Aytaç

January 6, 2017

Boğaziçi University

Table of contents

1. Introduction

2. Project Work

3. Implementation Details

4. Experimental Results

5. Case Study for Demonstration

6. Conclusion and Future Works

Introduction

ICN in a nutshell

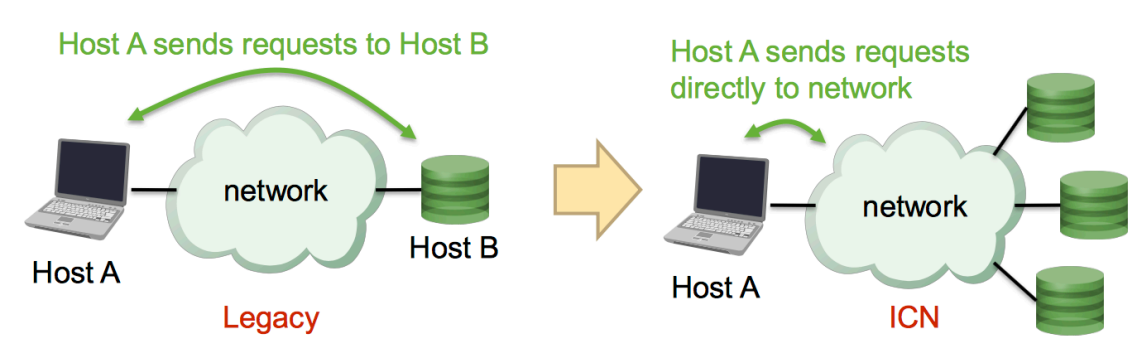


Figure 1: ICN vs traditional networks [4]

What is ICN

- In ICN, request has been done by identifying the content instead of identifying the content owner's address.
- Basic principle: name based routing
  - * User asks for an object by name
  - * Network delivers desired object from a nearby cache
- Network is aware of content
- Multiple copies of the content is cached in network

ABE as a candidate security solution

Potential Problems

- Security of data object
- Access control
- Distributed caches

ABE Solution

- No need to encrypt the data separately for each type of user
- Will be decrypted only by clients that have the correct set of attributes

Project Work

Problem Description

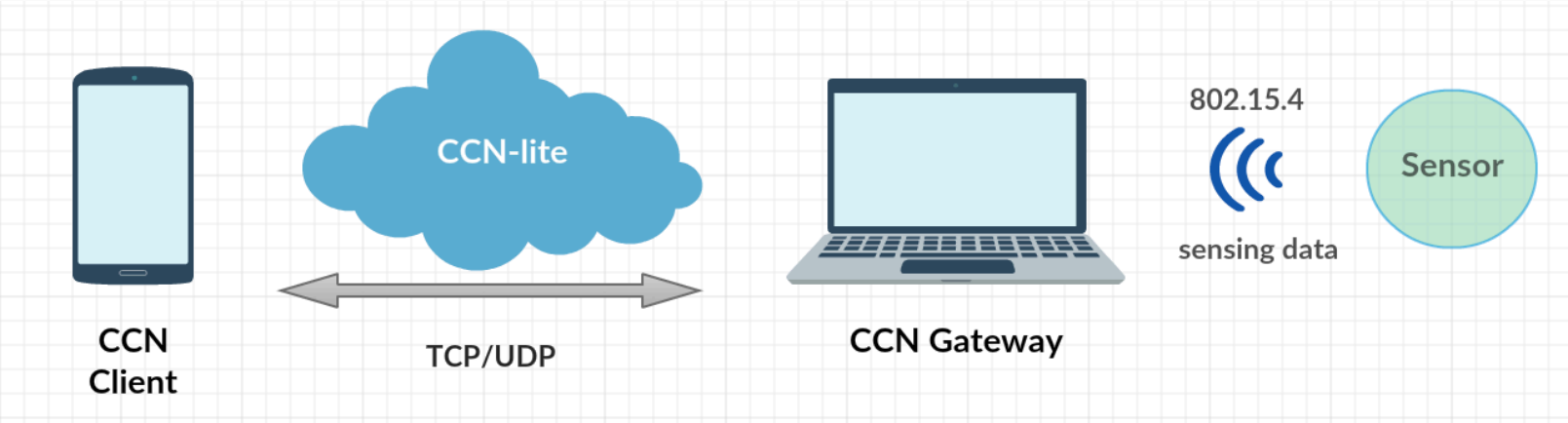


Figure 2: Block diagram for the implementation adapted from [3].

Two main phases:

1. ABE encryption on sensor devices
2. Transport of sensor data over an ICN network

Discussions

Outcomes

- No need to establish a secure end-to-end connection such as TLS
- Enables delay tolerant networking derived from store-and-forward mechanism [3].

Limitations

- Feasibility of ABE on resource constrained devices
  - Memory
  - Energy consumption
  - Processing load

Implementation Details

Simulation Environment

- CCN-lite for ICN environment [2]
- Cpabe Toolkit for ABE implementation [1]

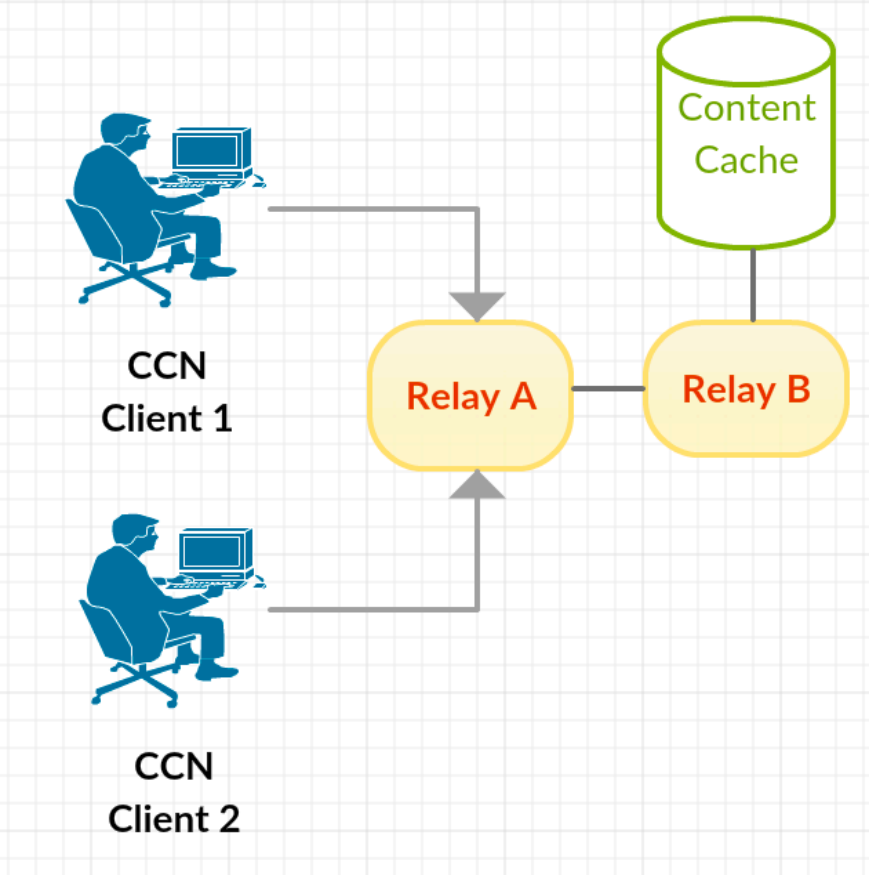


Figure 3: Users with attributes

Experimental Results

Experimental Results-I

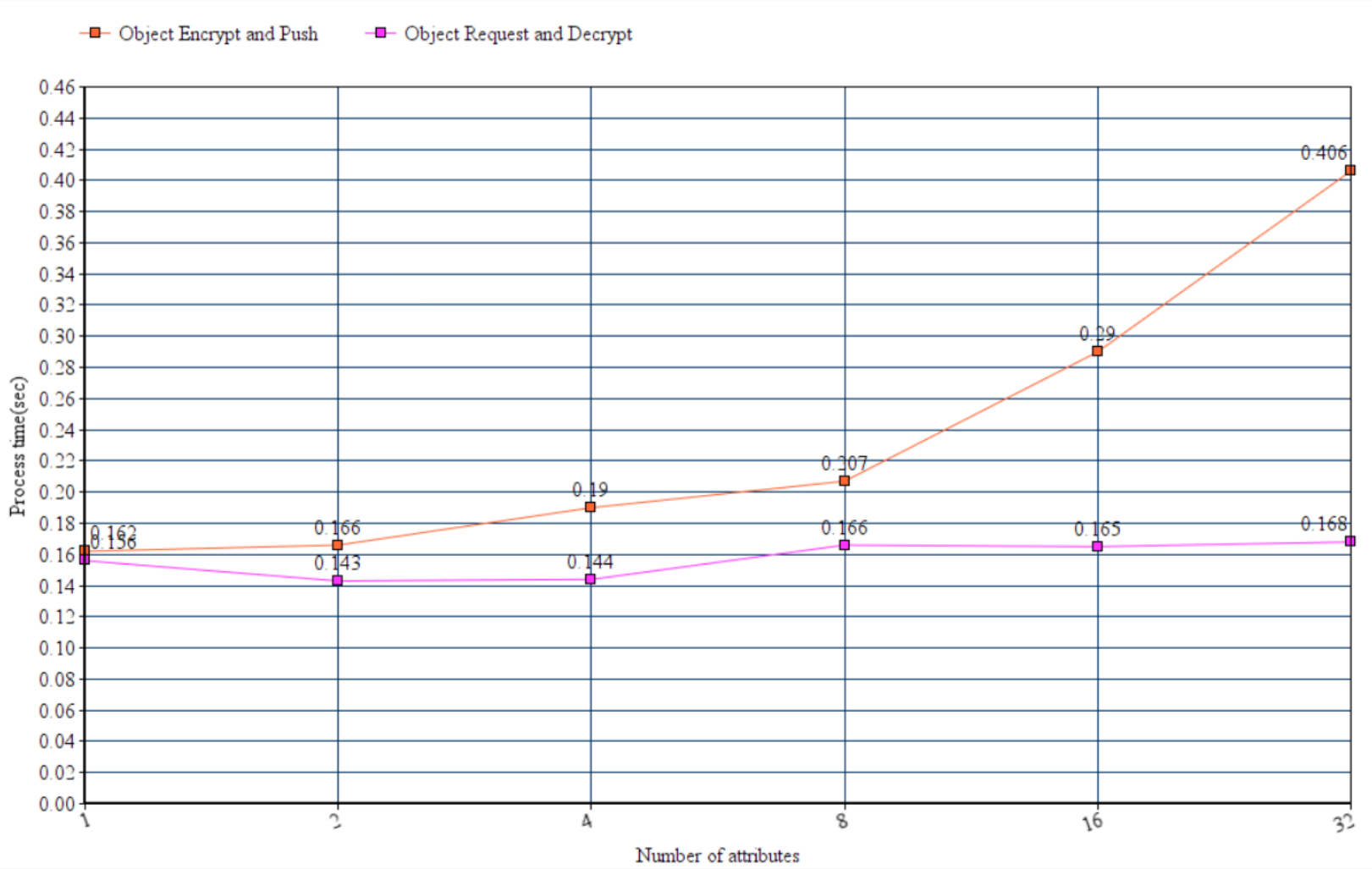


Figure 4: Processing time with various number of attributes

Experimental Results-II

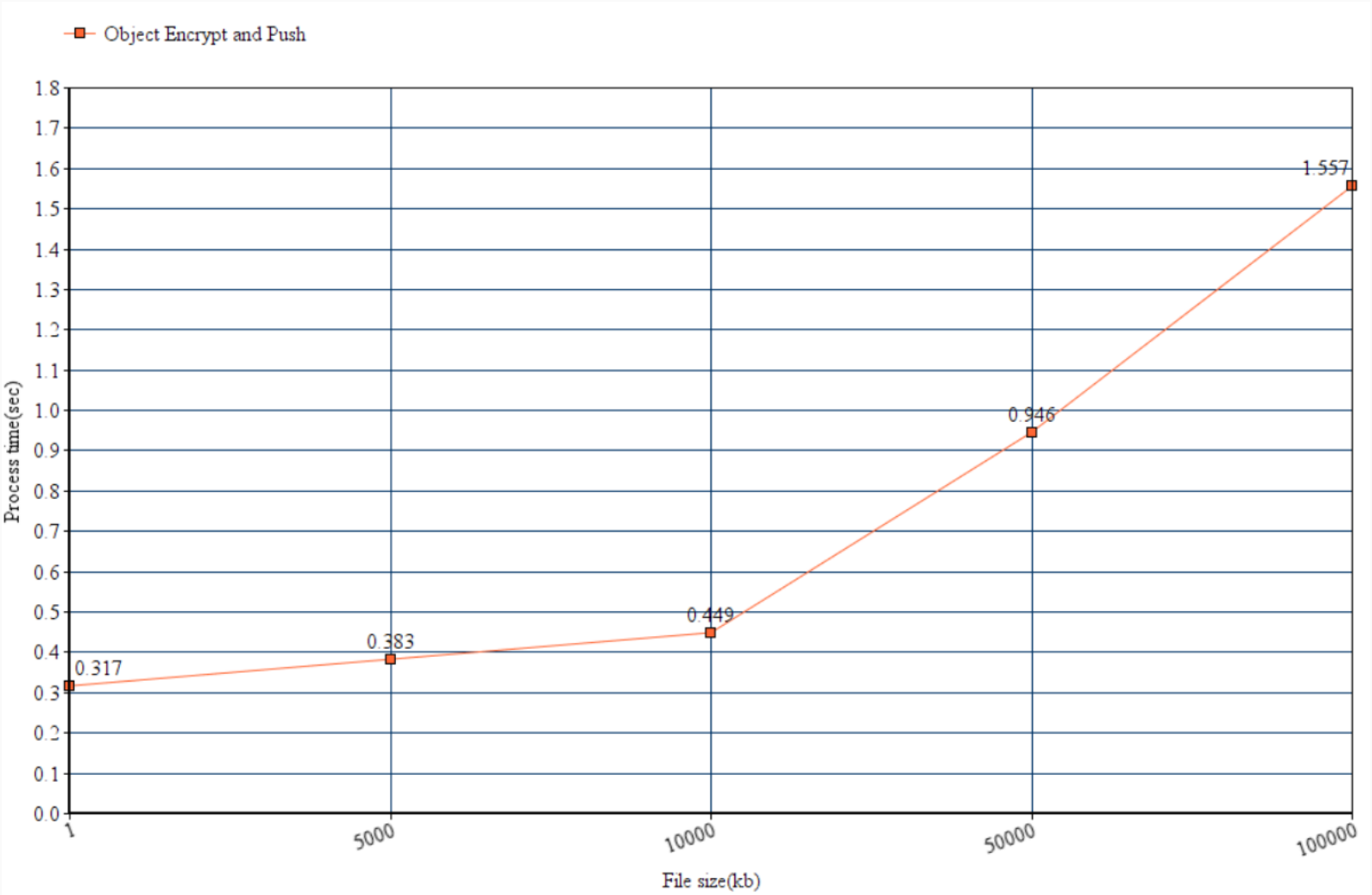


Figure 5: Processing time with various file sizes

Case Study for Demonstration

Case Study for Demonstration

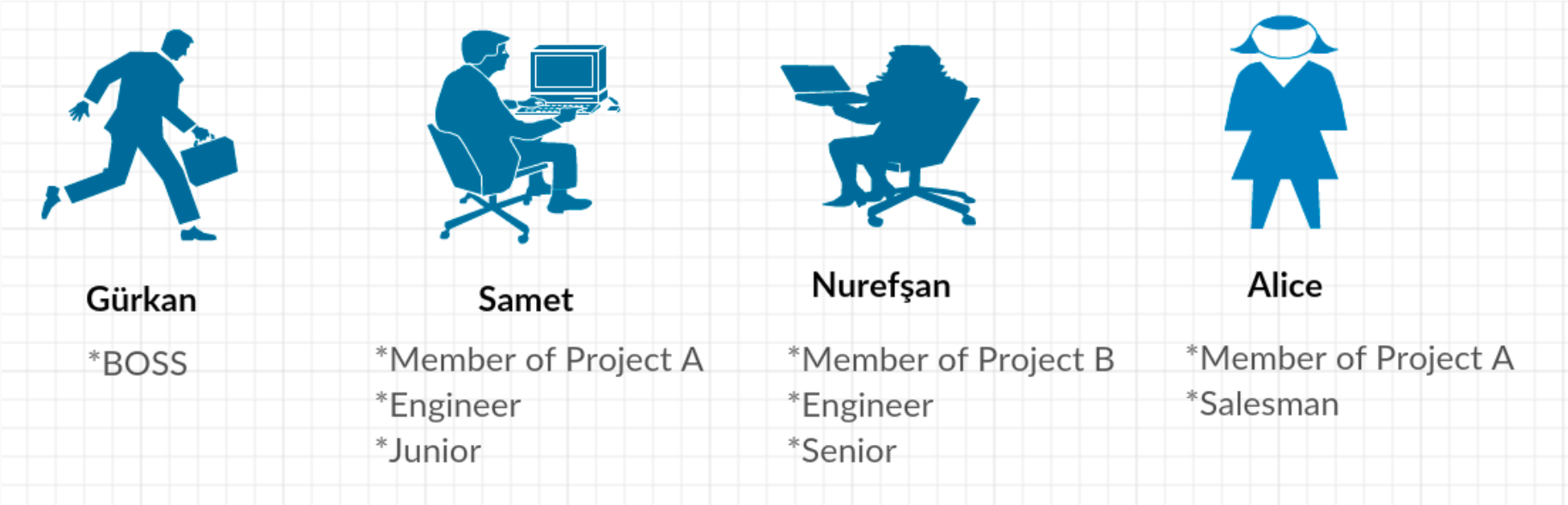
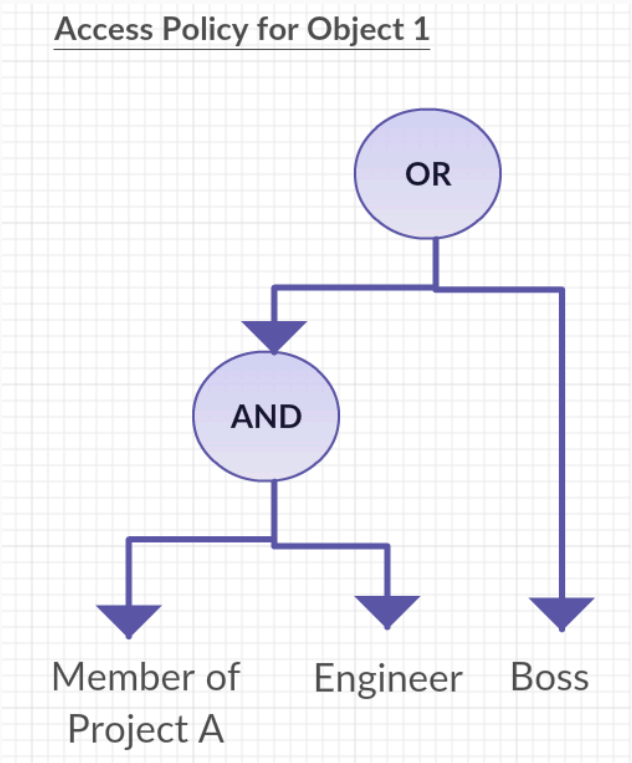
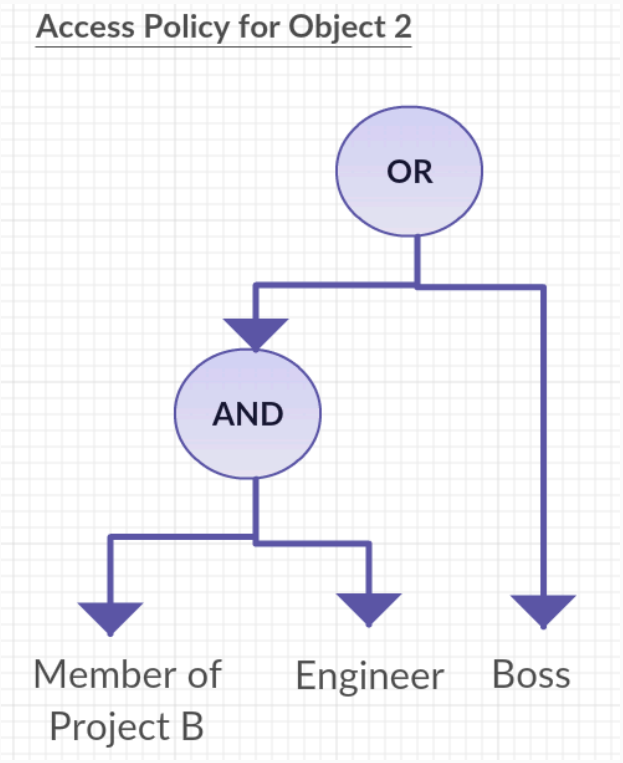


Figure 6: Users with attributes

Access policies for objects





	Content 1	Content 2
Gürkan	•	•
Samet	•	x
Nurefşan	x	•
Alice	x	x

Conclusion and Future Works

Conclusion and Future Works

We implement CP-ABE scheme over ICN to ensure object security

As future work,

- Implementation in real sensor devices
- Therefore, more realistic measurements
- Optimization to decrease the energy consumption of sensors

Source code available at

`https://github.com/sertbasn1/ABE_ICN_Project.git`

Questions?

References I


J. Bethencourt, A. Sahai, and B. Waters.
Ciphertext-policy attribute-based encryption.


Cn-uofbasel.
Cn-uofbasel/ccn-lite.


A. M. Malik, J. Borgh, and B. Ohlman.
Attribute-based encryption on a resource constrained sensor in an information-centric network.
In *Proceedings of the 2016 conference on 3rd ACM Conference on Information-Centric Networking*, pages 217–218. ACM, 2016.


M. Vahlenkamp, F. Schneider, D. Kutscher, and J. Seedorf.
Enabling information centric networking in ip networks using sdn, 2013.