Exploiting Blockchain Technology to Design an Attribute based Access Control System

Paolo Mori
Istituto di Informatica e Telematica
Consiglio Nazionale delle Ricerche

Damiano Di Francesco Maesa
Department of Computer Science and Technology
University of Cambridge, UK

Laura Ricci
Dipartimento di Informatica
Università di Pisa
Agenda

● Background
  – Attribute Based Access Control
  – XACML

● Our Proposal
  – Implementation of the XACML based Access Control Service exploiting the Blockchain technology
  – Examples of Application Scenarios
  – Experimental Results
Background:

Access Control and XACML
Access Control

Technique to decide whether a Subject requesting to perform an Action on a Resource in a given Context holds the right to perform it.
Attribute Based Access Control (ABAC)

An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.

Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publication 800-162
Attributes

- Attributes represent characteristics of the
  - Subjects
  - Resources
  - Actions
  - Environment

- Examples:
  - Subject
    - Role (e.g., in a company: Worker, Employee, Executive, CEO...)
    - Projects assigned to the subject
    - Physical location
  - Resources
    - Owner/producer
    - Number of copies of a document
    - Project of a document
    - Security classification
Extensible Access Control Markup Language 3.0 (XACML)

XACML defines:

- A XML-based Language to express Attribute based Access Control Policies
- A reference architecture for the Access Control Framework
XACML: Policy Example

<Condition>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and"> 
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal"> 
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only"> 
<AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-location" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/> 
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">EUROPA</AttributeValue> 
</Apply>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal"> 
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only"> 
<AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/> 
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Executive</AttributeValue> 
</Apply>
</Apply>
</Apply></Apply>
</Condition>
</Rule>
XACML: Reference Architecture

Subject

Service Requester

Policy Enforcement Point

1. Define policy

2. Request resource

3. Forward request

4. Notify request

5. Query attribute

6. Inquire attribute

7. Collect attributes from Subject, Resource, Environment

8. Return attribute from PIP

9. Include resource in context

10. Return attributes

11. Send response context

12. Respond to resource request

13. Execute obligations

Resource Owner

Policy Administration Point

Obligations Service

Context Handler

Policy Information Point

Attribute Manager Resources

Attribute Manager Subjects

Attribute Manager Environment
Blockchain based Access Control
Main Idea

Implement a XACML based Access Control Framework exploiting the Blockchain technology
Advantages

- Outsource the access control decision process
- No need of a Trusted third party to perform the access control decision process
- Auditability

Drawbacks

- Cost
- Performance
- Privacy
Blockchain based Access Control System
Examples of Application Scenarios
Application Scenario 1: Smart Contracts
Application Scenario 2: Cloud Services
Experimental Results
# Testbeds

- **International Educational Blockchain Academic Testnet** ([http://blockchain.open.ac.uk/](http://blockchain.open.ac.uk/))
  - Ethereum based

- **Ropsten testnet**
  - Good reproduction of the Ethereum main network for testing
Experimental Results: Gas Cost

Deployment and Evaluation Experimental Gas cost

- Block gas limit
- Deployment
- Evaluation

Gas cost (millions of units) vs. Number of policy rules
Experimental Results: Policy Deployment Time on Academic Testnet

Number of policy rules
Confirmation Times Mean & StDev

Deployment Confirmation Time

Number of policy rules
Confirmation Times Mean & StDev

Shaded variance region
Experimental Results: Policy Deployment Time on Ropsten

![Graph showing deployment confirmation time vs number of policy rules. The graph has two y-axes: one for confirmation time (seconds) and another for block height difference. The x-axis represents the number of policy rules. The shaded variance region indicates the confirmation times mean & standard deviation.](image-url)
Experimental Results: Policy Evaluation

Time on Ropsten

Execution Time

Number of Evaluation Requests

Confirmation Time (block height difference)

- 20 policy rules
- 40 policy rules
- 60 policy rules
- 80 policy rules
Ongoing and Future Work

- Performance evaluation on other testbeds
  - Optimization
- Other access control models
thank you
paolo.mori@iit.cnr.it