ENDORSE
Legal Technical Framework for Privacy Preserving Data Management

ENDORSE is funded by the EC under FP7

Enforcing Security Policies in Outsourced Environments

Muhammad **Rizwan** Asghar

CREATE-NET

PhD Supervisor:
Bruno Crispo

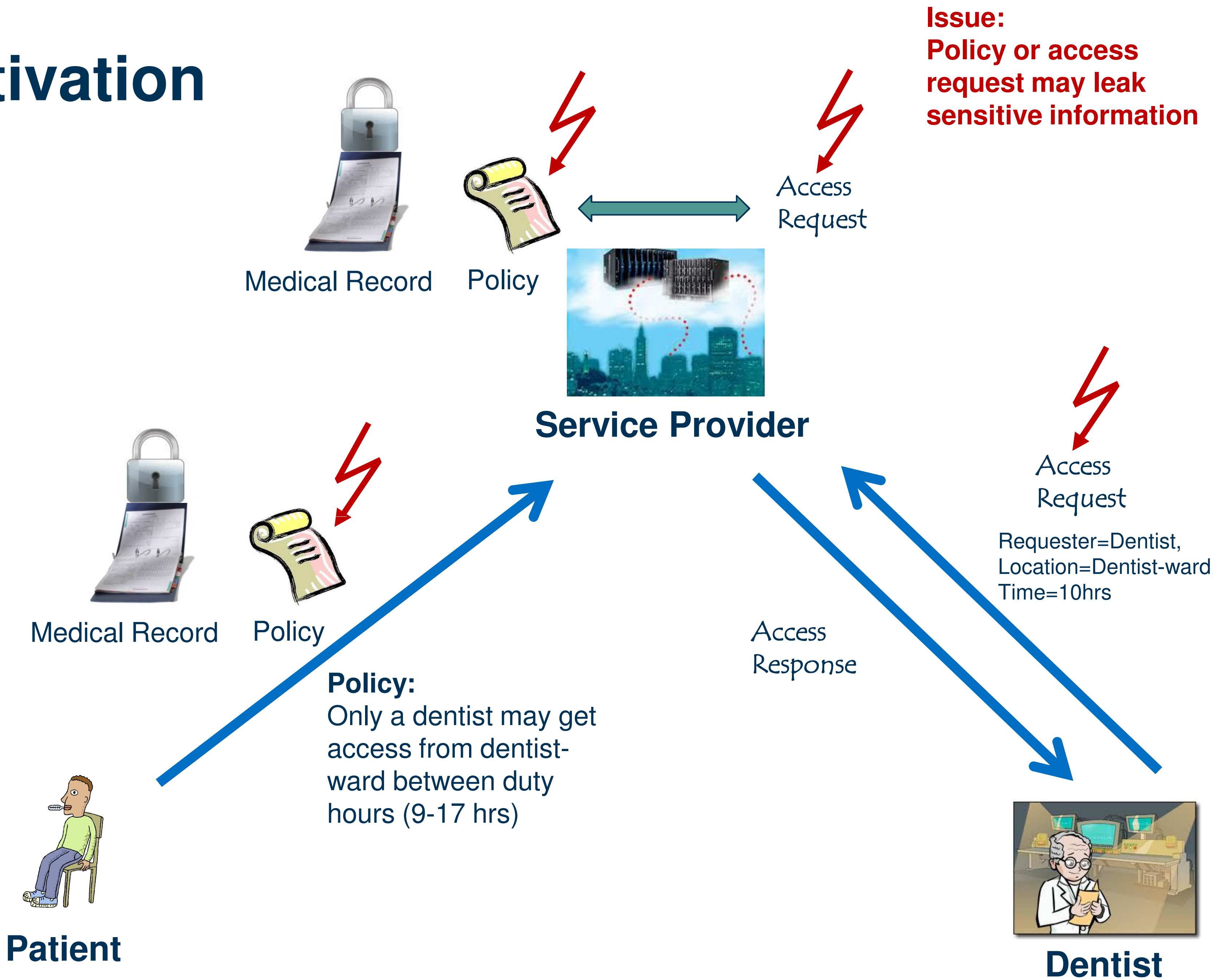
UNIVERSITY OF TRENTO - Italy

BunnyTN3
Trento, Italy
March 12, 2012

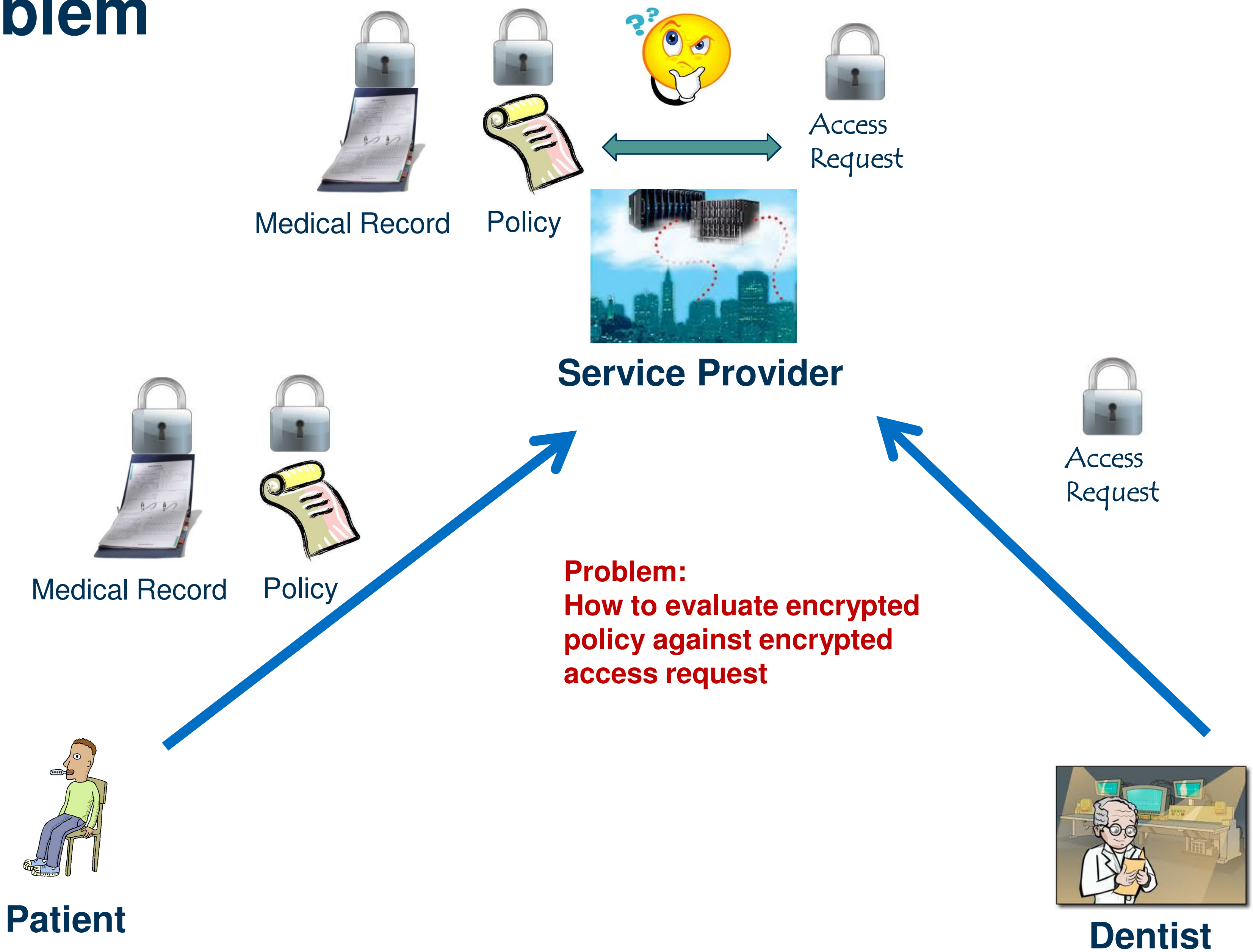
Why Outsourcing

- Cost saving
- Scalability
- Efficiency
- Reliability
- Availability

Motivation


Issue:
Policy or access request may leak sensitive information
Medical Record
Policy
Access Request
Service Provider
Medical Record
Policy
Access Request
Requester=Dentist, Location=Dentist-ward, Time=10hrs
Access Response
Policy:
Only a dentist may get access from dentist-ward between duty hours (9-17 hrs)
Patient
Dentist

Problem

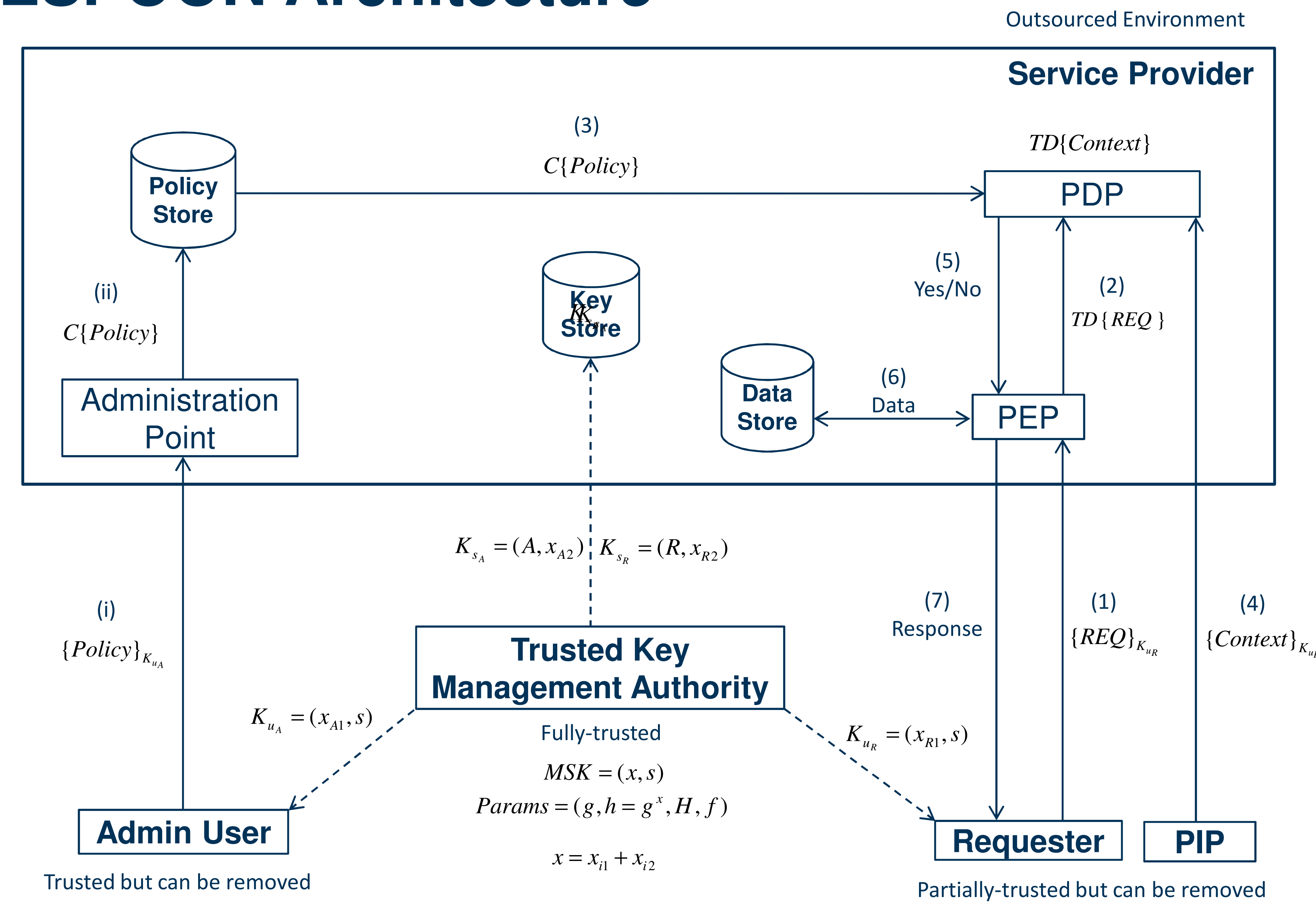


Problem:
How to evaluate encrypted policy against encrypted access request

Proposed Solution

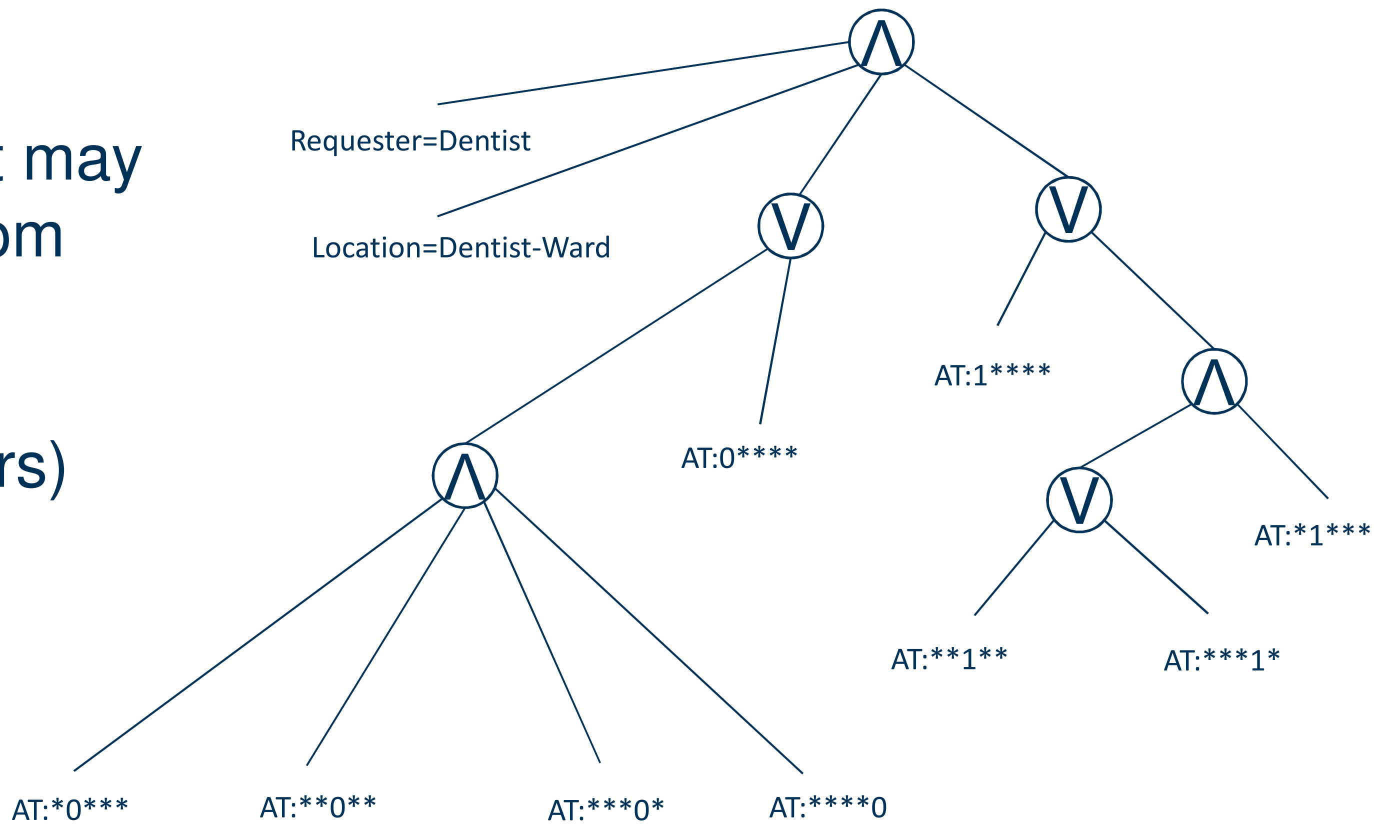
- We name our solution ESPOON (Enforcing Security Policies in OutsOurced eNvironments)
- In ESPOON, the Service Provider is assumed *honest-but-curious*
- ESPOON is capable of handling complex policies involving range queries
- ESPOON is a multiuser scheme in which entities do not share any encryption keys
- A compromised user can be removed without requiring re-encryption of policies

ESPOON Architecture



Policy Representation

Policy:
Only a dentist may get access from dentist-ward between duty hours (9-17 hrs)



AT = Access Time

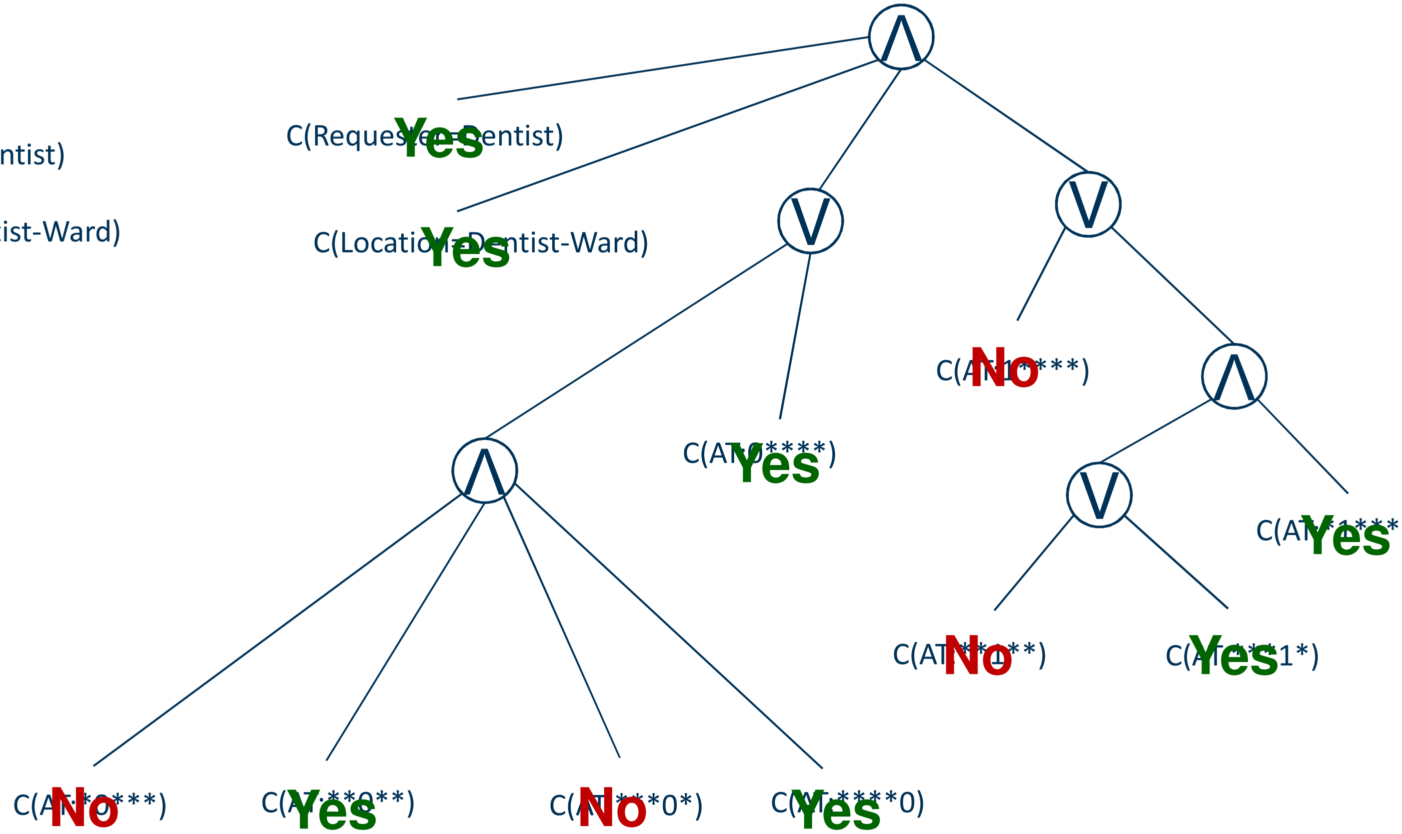
Policy Evaluation

TD(Requester=Dentist)

TD(Location=Dentist-Ward)

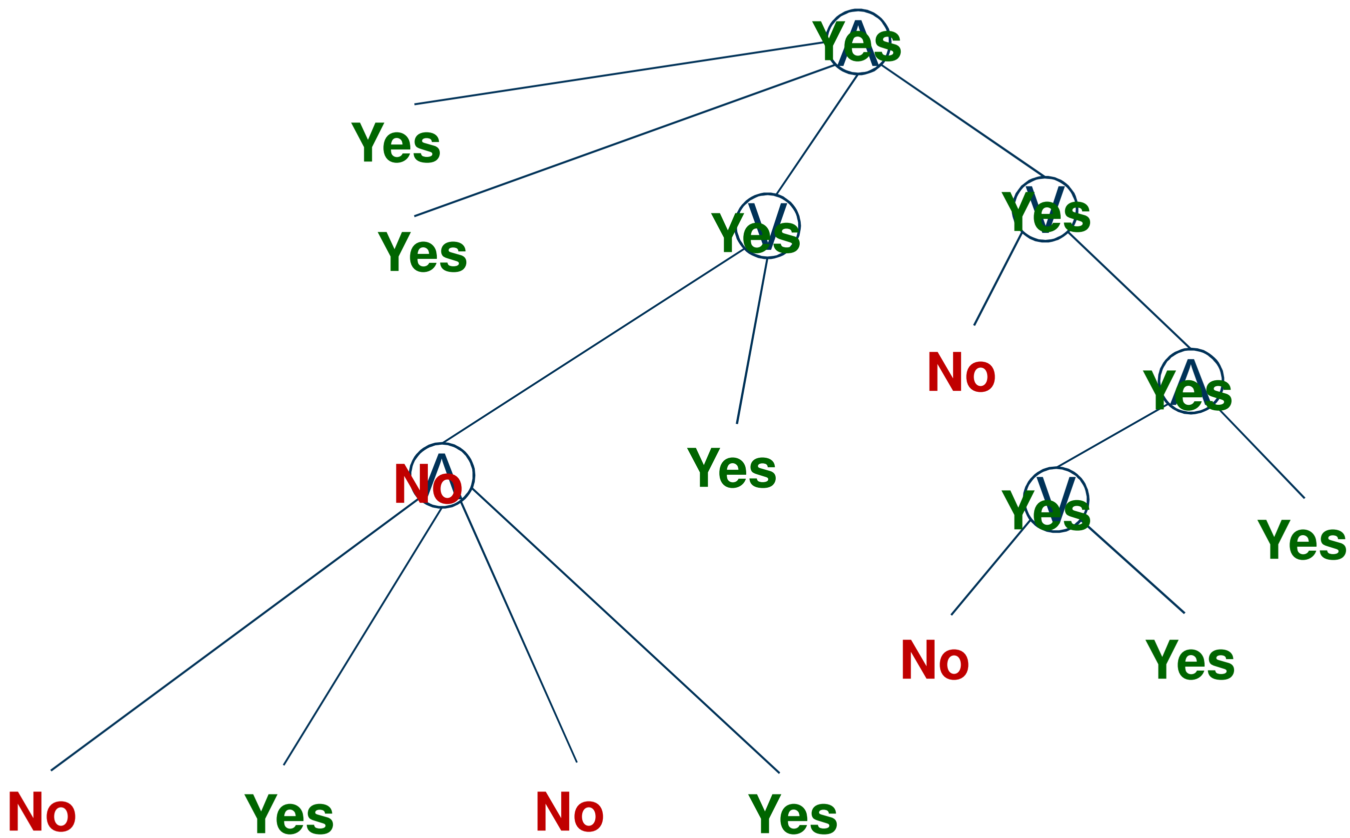
Access Time =10hrs

- TD(AT:0****)
- TD(AT:*1***)
- TD(AT:**0**)
- TD(AT:***1*)
- TD(AT:****0)



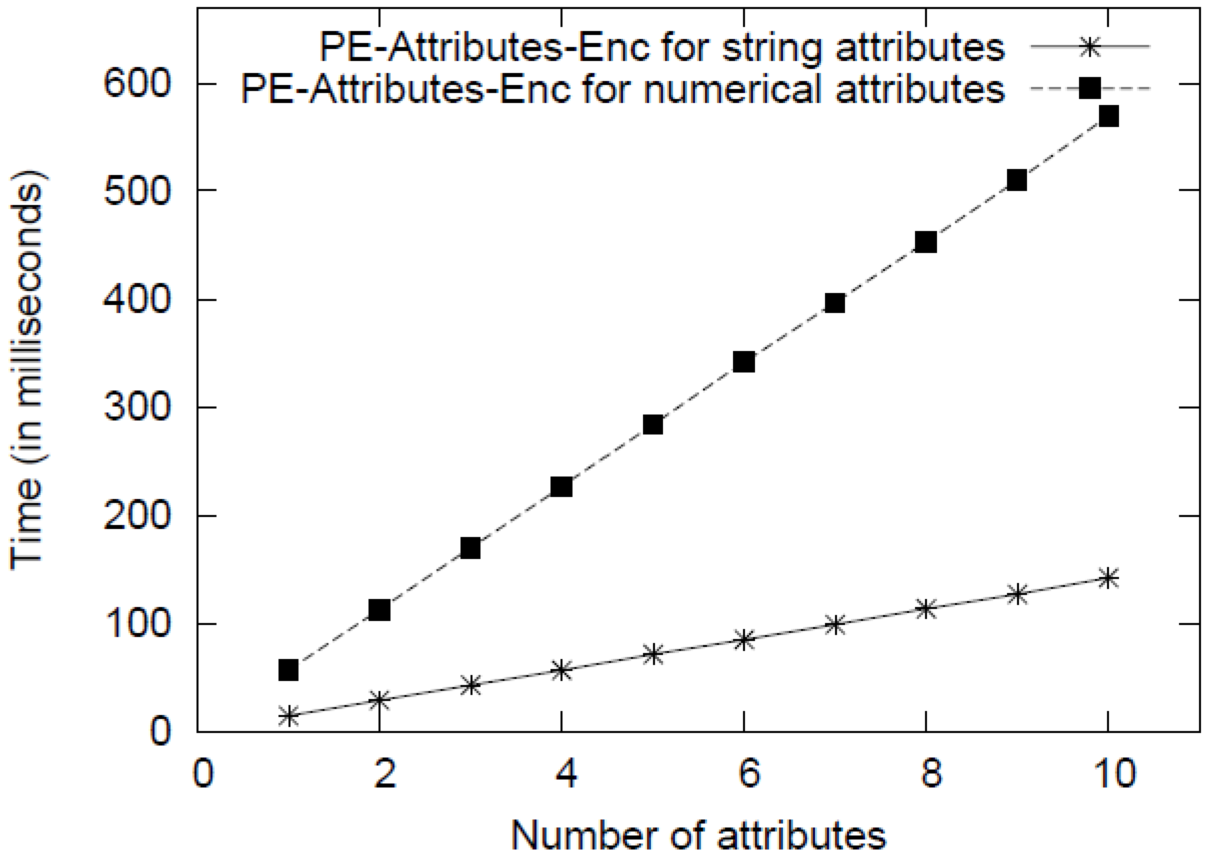
AT = Access Time

Policy Evaluation (2)



Performance Evaluation: Requester

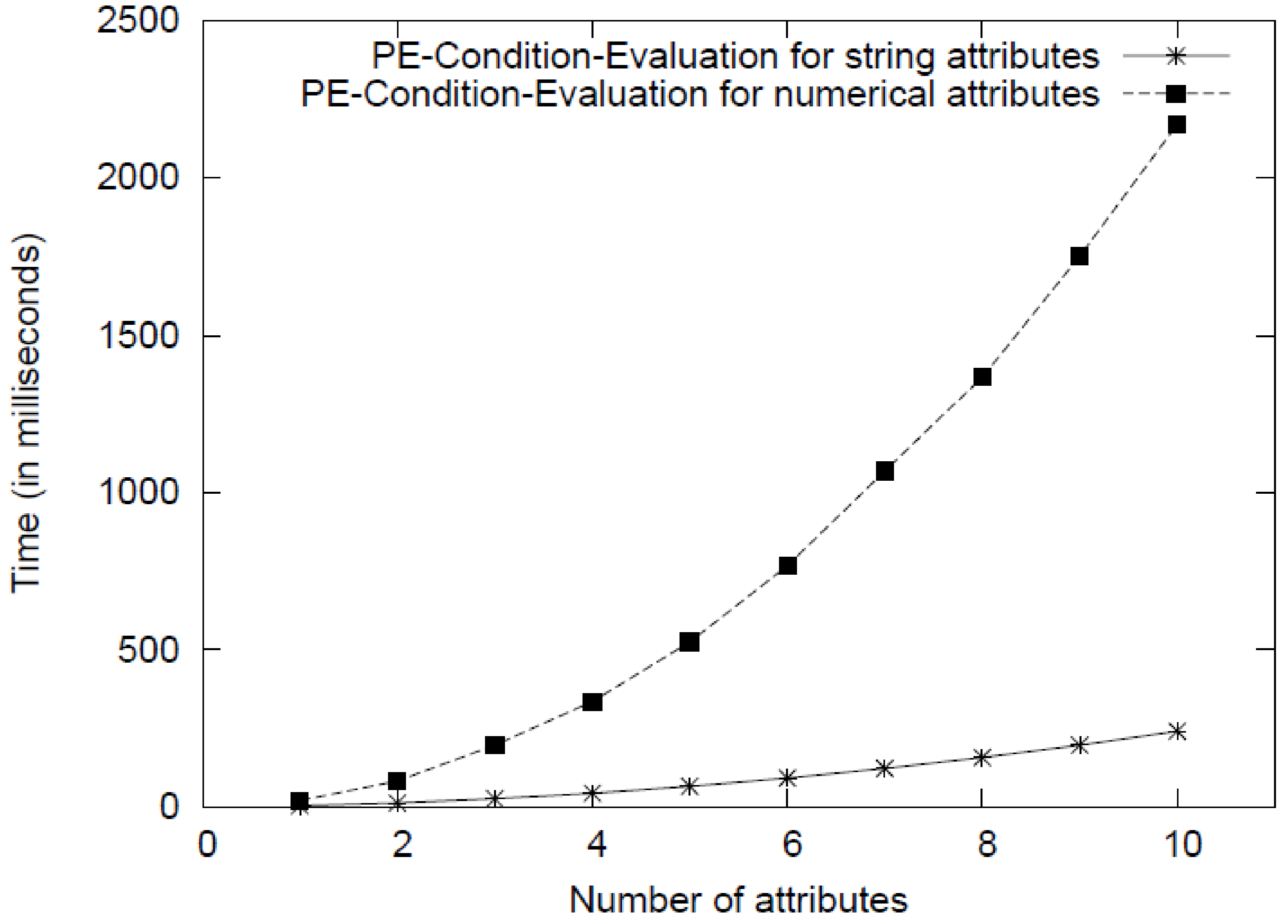
- **String Attribute:** ***O(n)***, n is the number of string attributes
- **Numerical Attribute: *O(ns)***, n is the number of numerical attributes each of size s



Performance Evaluation: Policy Evaluation

- **String Attribute: *O(nm)***, n is the number of string attributes and m is the number of string comparisons

- **Numerical Attribute: *O(nms²)***, n is the number of numerical attributes and m is the number of numerical comparisons each of size s



Related Work

- Schemes supporting access controls in outsourced environments require re-generation of keys and re-encryption of data for any administrative changes [Vimercati et al. CSAW'07 VLDB'07]

- Schemes supporting queries on encrypted data do not support access policies [Dong et al. DBSec'08, Song et al. S&P'00, Boneh et al. EUROCRYPT'04, Curtmola et al. CCS'06, Hwang and Lee LNCS'07, Boneh and Waters TCC'07, Wang et al. SOFSEM'08, Baek et al. ICCSA'08, Rhee et al. JSS'10, Shao et al. Inf. Sci.'10]

- Encrypted data with CP-ABE policy reveals the policy structure [Narayan et al. CCSW'10]

- Hidden credentials schemes do not support complex policies and require parties to be online [Holt et al. WPES'03, Bradshaw et al. CCS'04]

Conclusions and Future Work

- Conclusions
  - ESPOON enforces policies in outsourced environments
  - ESPOON supports complex policies including range queries
  - ESPOON employs a multiuser scheme where users do not share keys
- Future work
  - *Support of full-fledged RBAC style of policies (current focus)*
  - Secure auditing mechanism in ESPOON
  - Support for negative authorisation policies
  - Dynamic updates of attributes within a request

References

- [Asghar *et al.* CCS'11] Muhammad Rizwan Asghar, Giovanni Russello, Bruno Crispo. POSTER:**ESPOON$_{ERBAC}$: Enforcing Security Policies in Outsourced Environments with Encrypted RBAC**. In Proceedings of the 18th ACM conference on Computer and communications security, CCS '11, pages 841-844, New York, NY, USA, 2011. ACM.

- [Asghar *et al.* ARES'11] Muhammad Rizwan Asghar, Mihaela Ion, Giovanni Russello, Bruno Crispo. **ESPOON: Enforcing Encrypted Security Policies in Outsourced Environments**. The Sixth International Conference on Availability, Reliability and Security (ARES), Austria, Vienna, 22-26 August 2011, pages 99-108. IEEE, 2011 (***Full paper acceptance rate was 20%***).

Thank You!

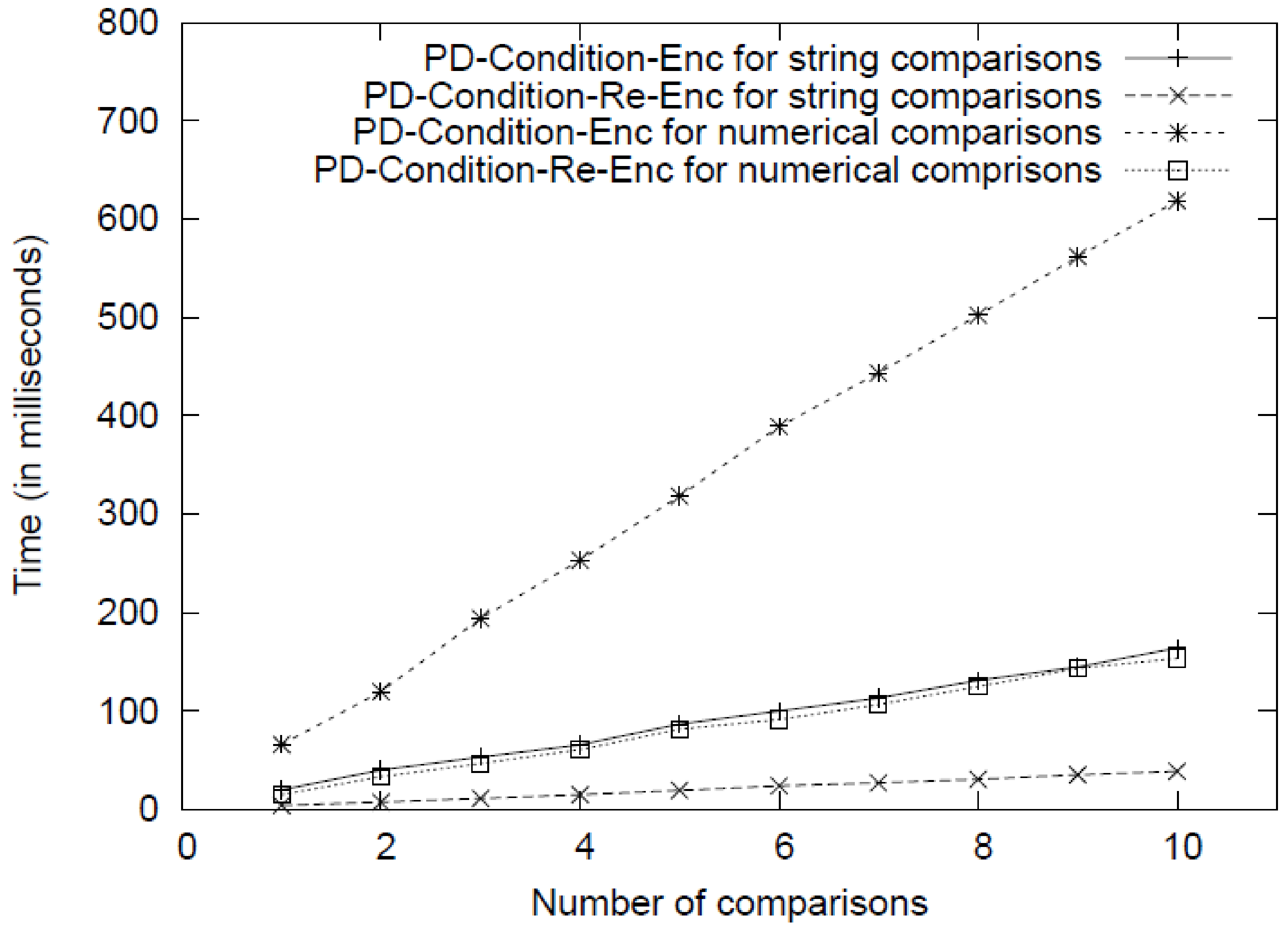
Any Questions?

asghar@disi.unitn.it

Performance Evaluation: Policy Deployment

- **String Comparison:** For both enc and re-enc: ***O(n),*** n is the number of string comparisons

- **Numerical Comparison:** For both enc and re-enc ***O(ns)***, n is the number of numerical comparisons each of size s



Key Distribution

- A Trusted Key Management Authority (KMA) is initialised with security parameters to generate
  - Master secret key **x** and s
  - Public parameters (g, $h=g^{\mathbf{x}}$, H, f)
- For each user i, the KMA
  - randomly generates x_{i1}
  - calculates $x_{i2} = \mathbf{x} - x_{i1}$
- Finally, the KMA securely transmits
  - $K_{U_i} = (x_{i1}, s)$ to user i
  - $K_{S_i} = (x_{i2}, i)$ to the Server Provider

Policy Deployment: Admin User Side

$$\{e\}_{K_{U_A}} = \begin{cases} \hat{c}_1 = g^{r_A + \sigma_A}, \sigma_A = f_s(e) \\ \hat{c}_2 = \hat{c}_1^{x_{A1}} \\ \hat{c}_3 = H(h^{r_A}) \end{cases}$$

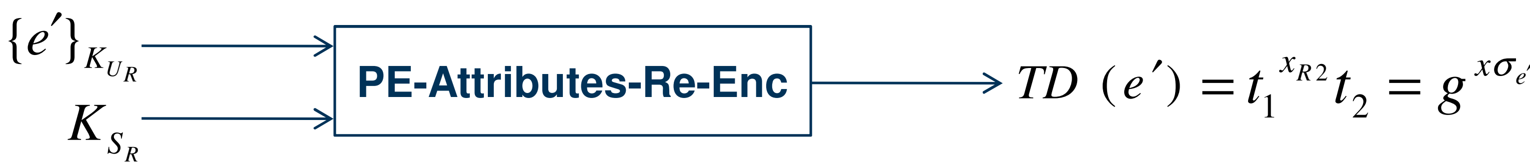
Policy Deployment: Service Provider Side

$$c(e) = \begin{cases} c_1 = (\hat{c}_1^{x_{A2}}).\hat{c}_2 = (g^{r_A+\sigma_A})^x = h^{r_A+\sigma_A} \\ c_2 = \hat{c}_3 = H(h^{r_A}) \end{cases}$$

Request: Requester Side

$$\{e'\}_{K_{U_R}} = \begin{cases} t_1 = g^{-r_{a'}+\sigma_{a'}}, \text{ where } \sigma_{a'} = f_s(e') \\ t_2 = h^{r_{e'}} g^{-x_{R1} r_{e'}} g^{-x_{R1}\sigma_{e'}} = g^{x_{R2} r_{e'}} g^{-x_{R1}\sigma_{e'}} \end{cases}$$

Request: Service Provider Side



Policy Evaluation