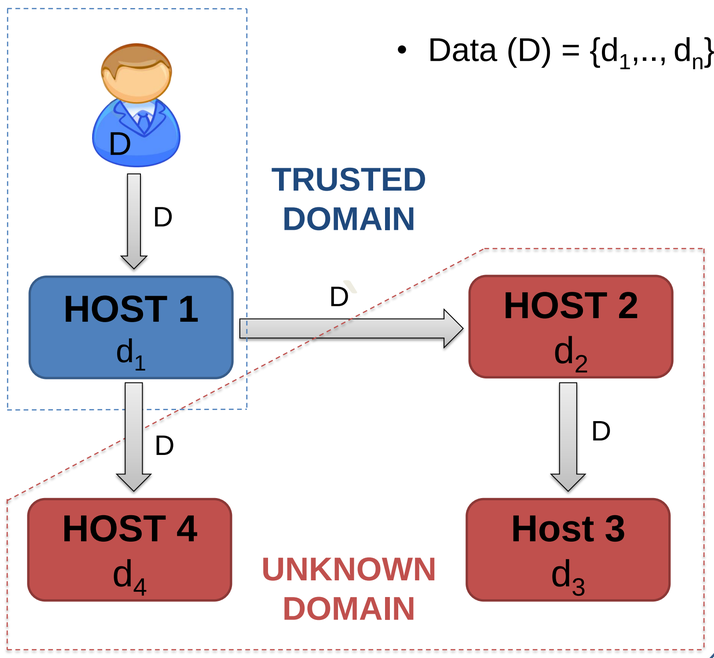
# CERIAS

The Center for Education and Research in Information Assurance and Security

# PD3: Policy–based Distributed Data Dissemination

Rohit Ranchal, Denis Ulybyshev, Pelin Angin, Bharat Bhargava
Computer Science and CERIAS, Purdue University

## MOTIVATION




- Data (D) = $\{d_1,.., d_n\}$

## PROBLEMS

- Opaque data sharing
- Undetected privacy violations
- Lack of policy infrastructure

## OBJECTIVES

- User should be able to define access control policies for data items
- Authorized host should only be able to access data items for which it is authorized
- Unauthorized host should not be able to access any data item

## PROPOSED SOLUTION

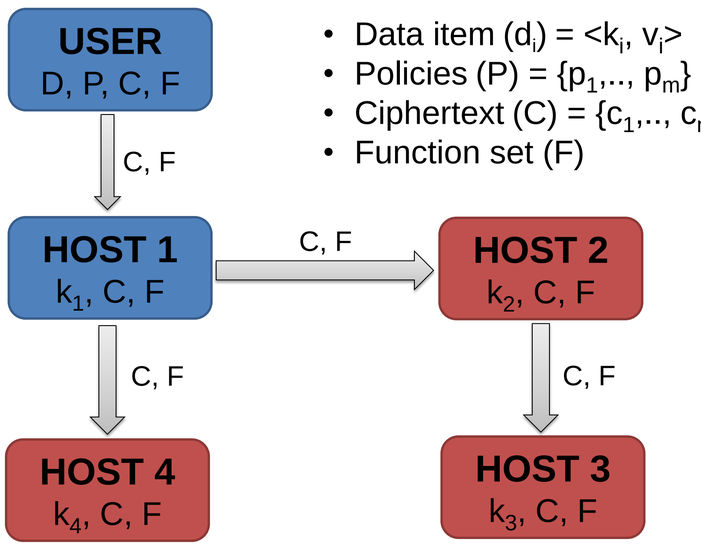
- Encrypt data (C) and define function set (F)
- Share C and F with each host

```
if (host == authorized)
   F(dataRequest, cipherText) = dataItem
```

## REQUIREMENTS FOR F

- Host Authentication
- Policy evaluation (Authorization)
- Key derivation
- Tamper resistance
- Data dissemination

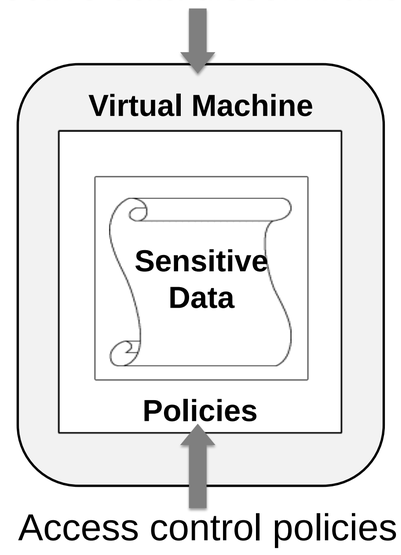
## PROPOSED SOLUTION




- Data item ($d_i$) = <$k_i$, $v_i$>
- Policies (P) = $\{p_1,.., p_m\}$
- Ciphertext (C) = $\{c_1,.., c_n\}$
- Function set (F)

## ACTIVE BUNDLE (AB)

- Self-integrity check
- Policy evaluation and enforcement
- Selective data dissemination




- Access control policies
- Operational policies

## FEATURES

- Data-centric approach
- Policy-based access control
- Independent of trusted third parties
- Independent of source availability
- Ability to operate in unknown environment
- Reduced host liability for extra data

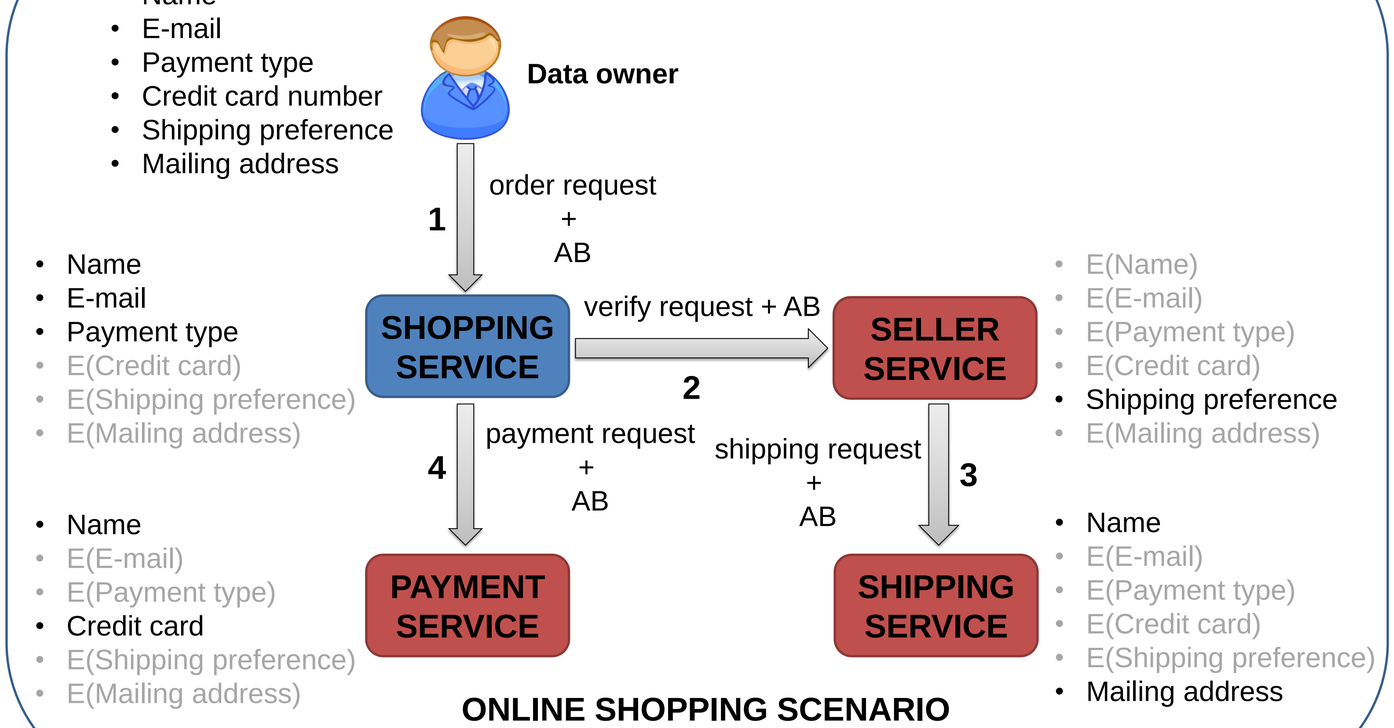
## IMPLEMENTATION

- AB implemented as an executable JAR file
- Apache-thrift based API
- XACML-based policies
- WSO2 Balana-based policy engine
- Node.js-based SOA architecture
- RESTful web-services

*https://code.google.com/p/absoa*

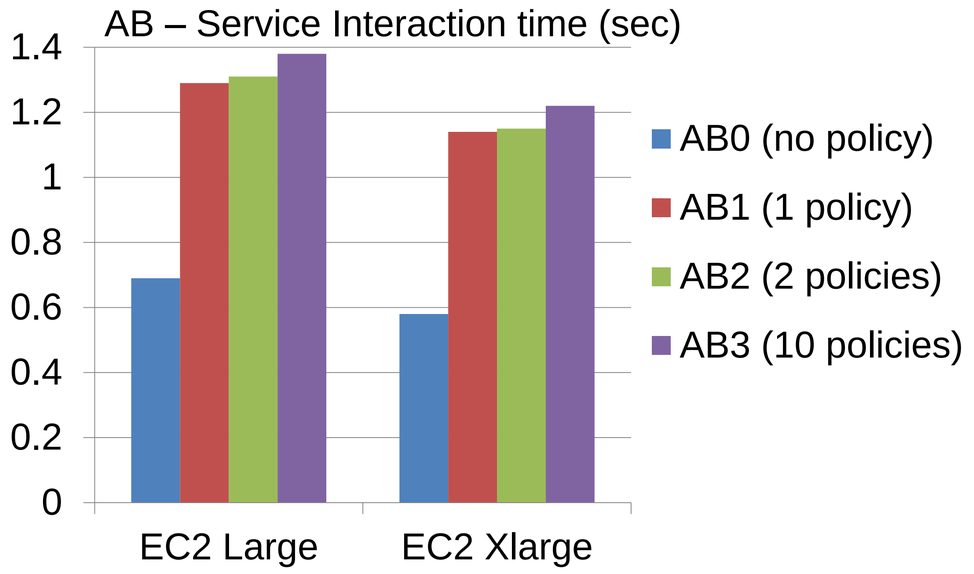
## COMPOSITE WEB SERVICES

- Name
- E-mail
- Payment type
- Credit card number
- Shipping preference
- Mailing address




**ONLINE SHOPPING SCENARIO**

## EVALUATION




## FUTURE WORK

- Comprehensive performance and security evaluation
- Testing other lightweight policy languages and engines
- AB state information exchange and context-aware dissemination using trusted third party
- Other applications (healthcare, vehicle, defense)

**ACKNOWLEDGEMENT:** This research is supported by NGC Research Consortium

PURDUE UNIVERSITY