2018 - AIP - B88-055 - Privacy-preserving Autonomous Aggregate Data Analytics in Untrusted Cloud - Ganapathy Mani

CERIAS

The Center for Education and Research in Information Assurance and Security

Privacy-preserving Autonomous Aggregate Data Analytics in Untrusted Cloud

Ganapathy Mani, Denis Ulybyshev, Bharat Bhargava, Jason Kobes*, Puneet Goyal$

Computer Science & CERIAS, Purdue University; NGC*; IIT Ropar$

PROBLEM STATEMENT

Intelligent Autonomous Systems (IAS) should be able to conduct data analytics on-the-fly and update their governing policies based on those analytics.

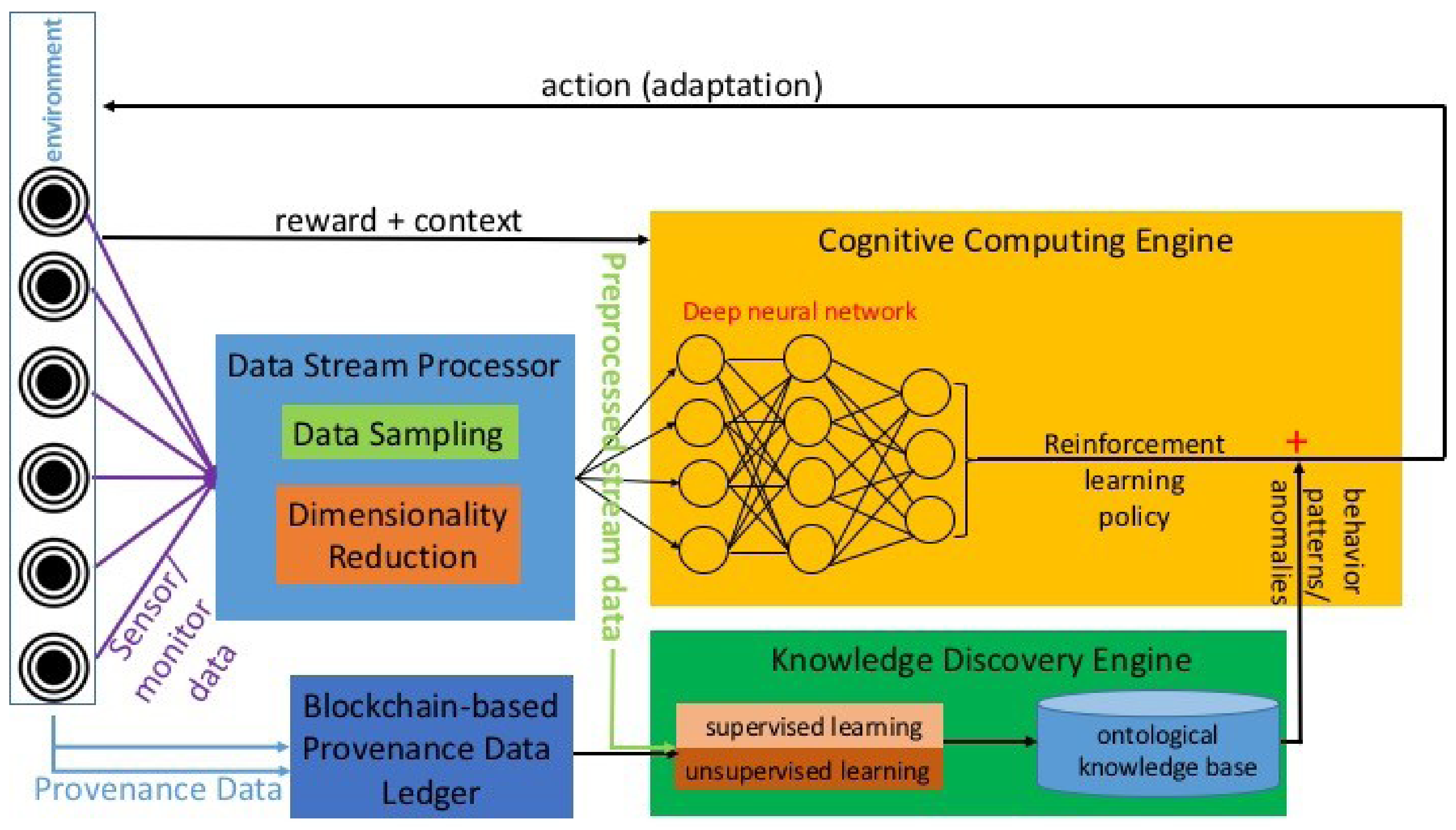

Figure 1. Comprehensive conceptualization of Intelligent Autonomous Systems

IAS (Figure 1) should follow these rules to stay efficient:

- The aggregated data analytics must be perform by autonomous entities such as Active Bundle (AB) that does not invade privacy of other entities
- Accessingotherentitiesshouldbecosteffectivei.e. scalable

SOLUTION

We propose two solutions to tackle the problems of privacy and scalability:

1. Employsimplisticdataperturbationforverified entities.
2. Allow neighboring peers to authenticate access to autonomous entities requesting access.

BACKGROUND

AB (Figure 2) has the following properties:

- Self-enforcement of security policies
- Secure data dissemination with selective release of data
- Wrapped with access control policies and operational control policies.

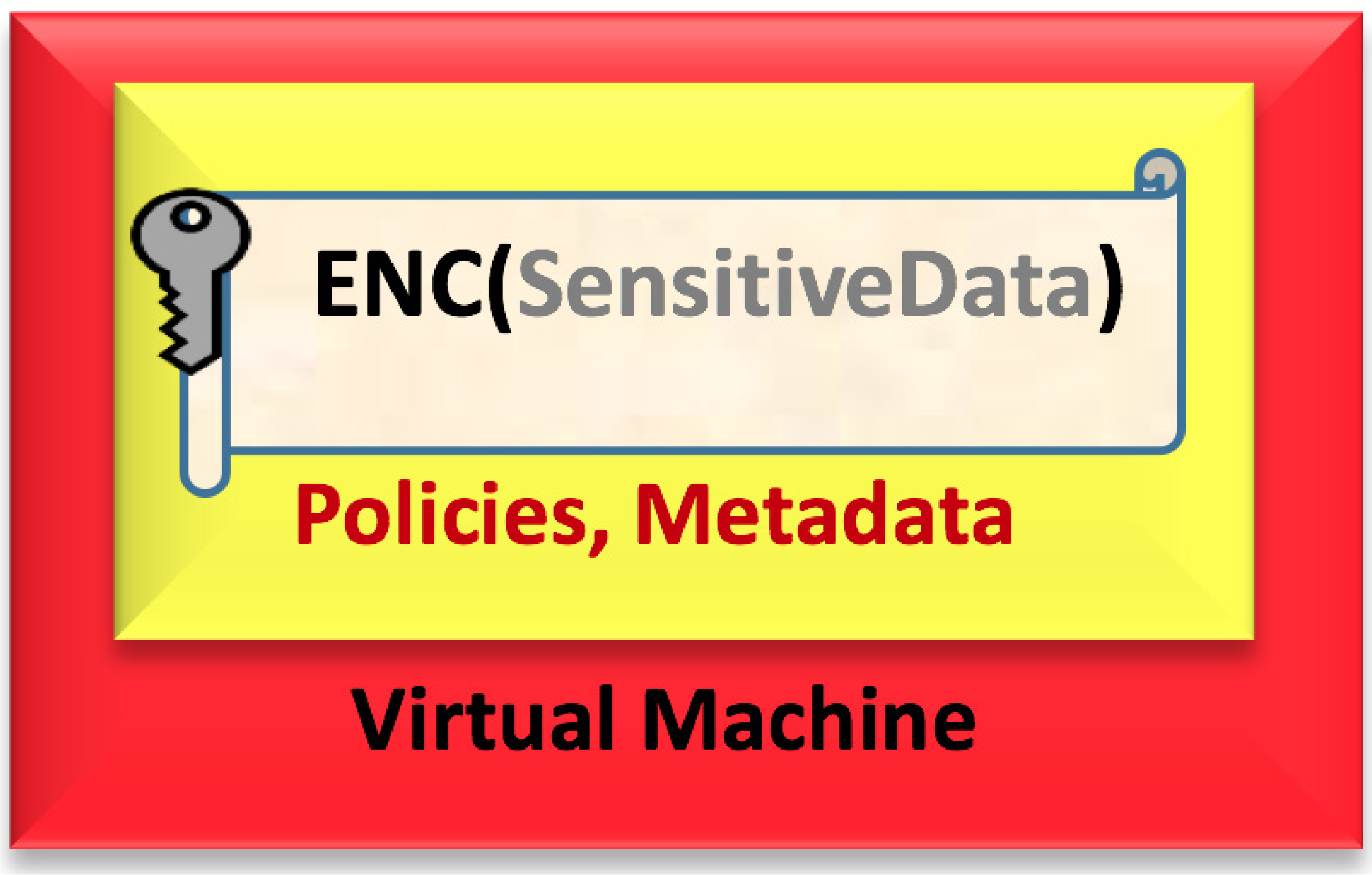

Figure 2. Active Bundle

AUTHENTICATION PROTOCOL FOR AB

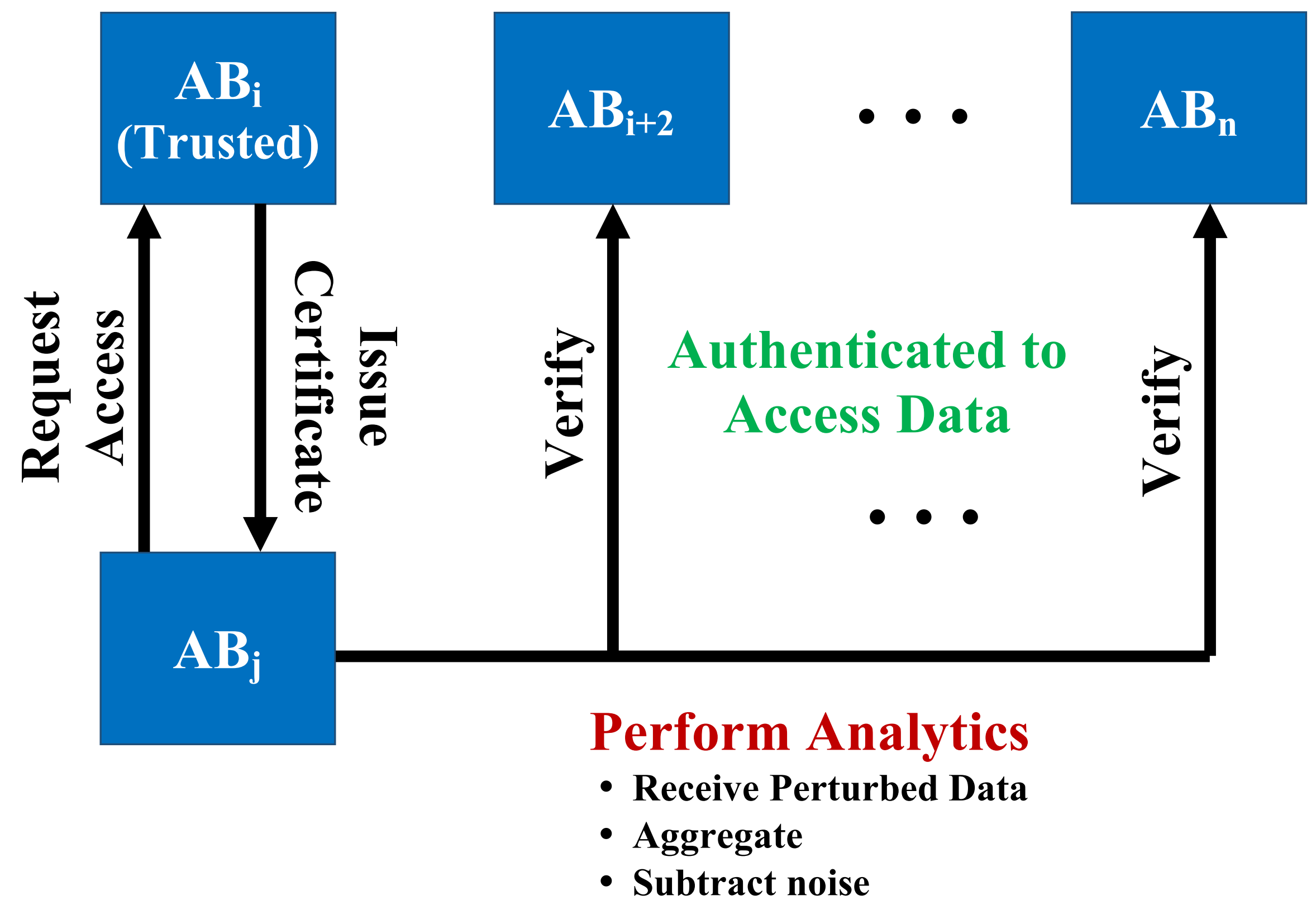

Figure 3. AB's efficient authentication protocol

```
Data: $AB_i$ and $AB_j$ as inputs
Result: Certificate issued/denied/issued with
        restrictions
if $Type(AB_i)$ is same as $Type(AB_j)$ then
    if $Trust(AB_i)$ is greater than $Trust(AB_j)$ then
        Generate authentication certificate;
        Issue the certificate to $AB_j$;
    else
        Generate Certificate with restrictions (only
          access encrypted data);
    end
else
    Deny the request;
    Report to administrator;
end
```

Algorithm 1. Active Bundle

The algorithm verifies the trust level of AB and allows it to acquire data from other similar ABs.

AUTONOMOUS ACTIVE BUNDLE

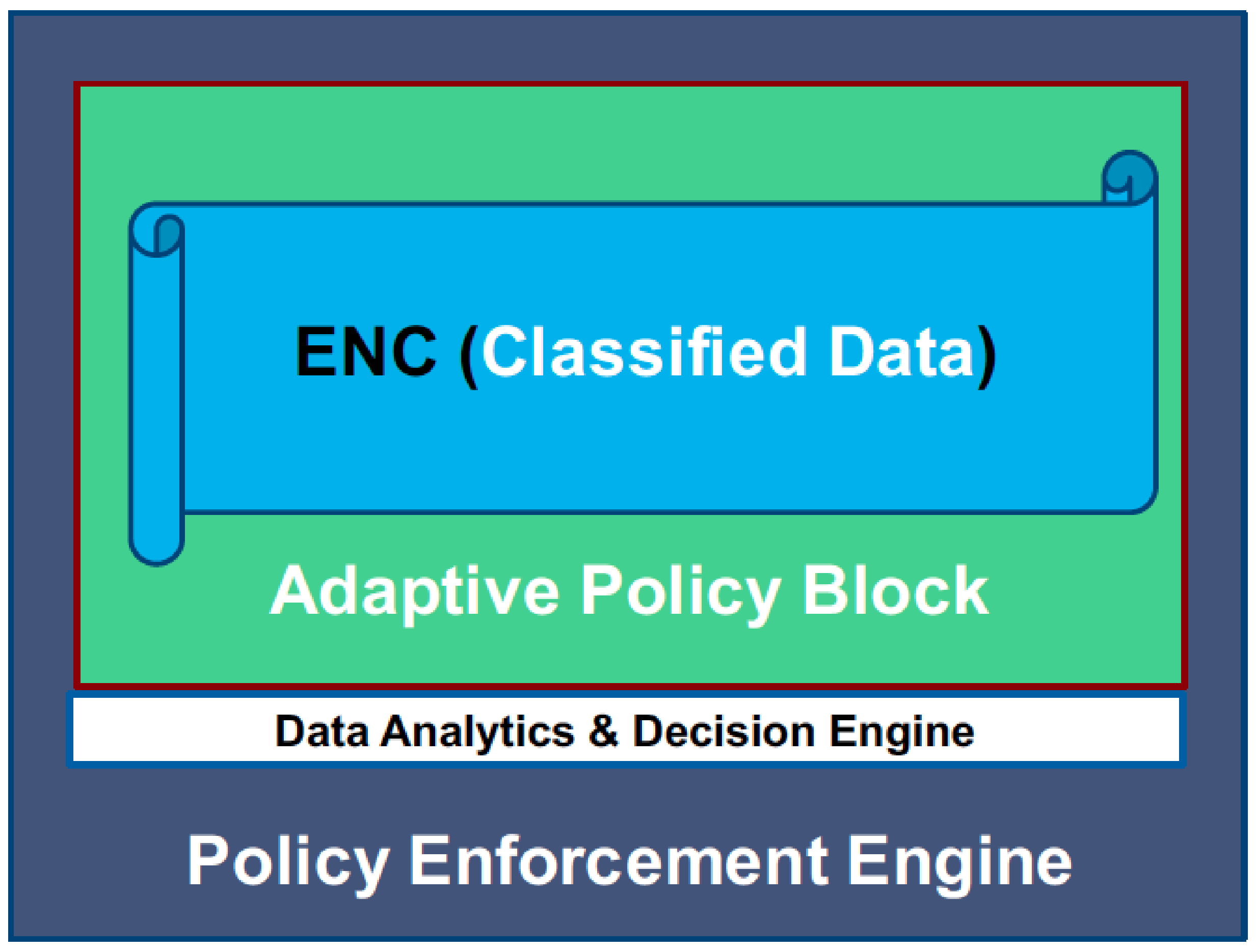

Figure 3. Active Bundle

Policy enforcement engine is influenced by data analytics module. Say, if an AB want to aggregate the average of age, it adds R perturbation to the original data,

$$\text{Total} = (\text{Age}_1 + R) + \text{Age}_2 + \ldots + \text{Age}_n$$

then the requesting AB can obtain real average

$$\text{Average} = (\text{Total} - R) / 2.$$

EVALUATION

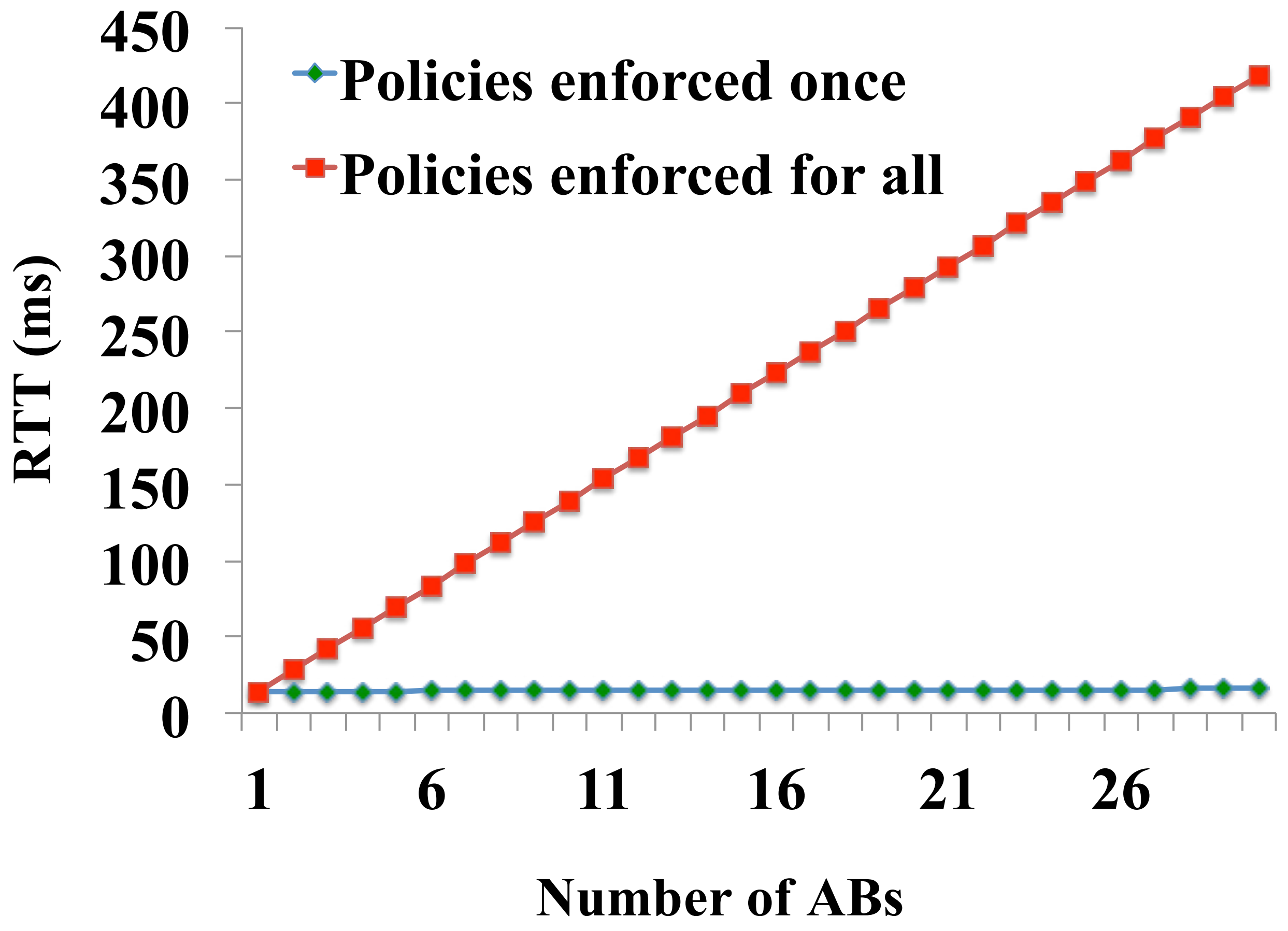

Figure 4. AB with and without one time policy enforcement

ACKNOWLEDGMENTS

This research is supported by NGCRC.

REFERENCES

[1] Ranchal, Rohit, et al. "Protection of identity information in cloud computing without trusted third party." Reliable Distributed Systems, 2010 29th IEEE Symposium on. IEEE, 2010.

PURDUE UNIVERSITY Discovery Park

CERIAS