**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.

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

- The aggregated data analytics must be performed by autonomous entities such as Active Bundle (AB) that does not invade privacy of other entities
- Accessing other entities should be cost effective i.e. scalable

**SOLUTION**

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

1. Employ simplistic data perturbation for verified 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.

**AUTHENTICATION PROTOCOL FOR AB**

![Figure 3. AB's efficient authentication protocol](image)

**EVALUATION**

Policy enforcement engine is influenced by data analytics module. Say, if an AB wants 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:

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

**ACKNOWLEDGMENTS**

This research is supported by NGCRC.

**REFERENCES**