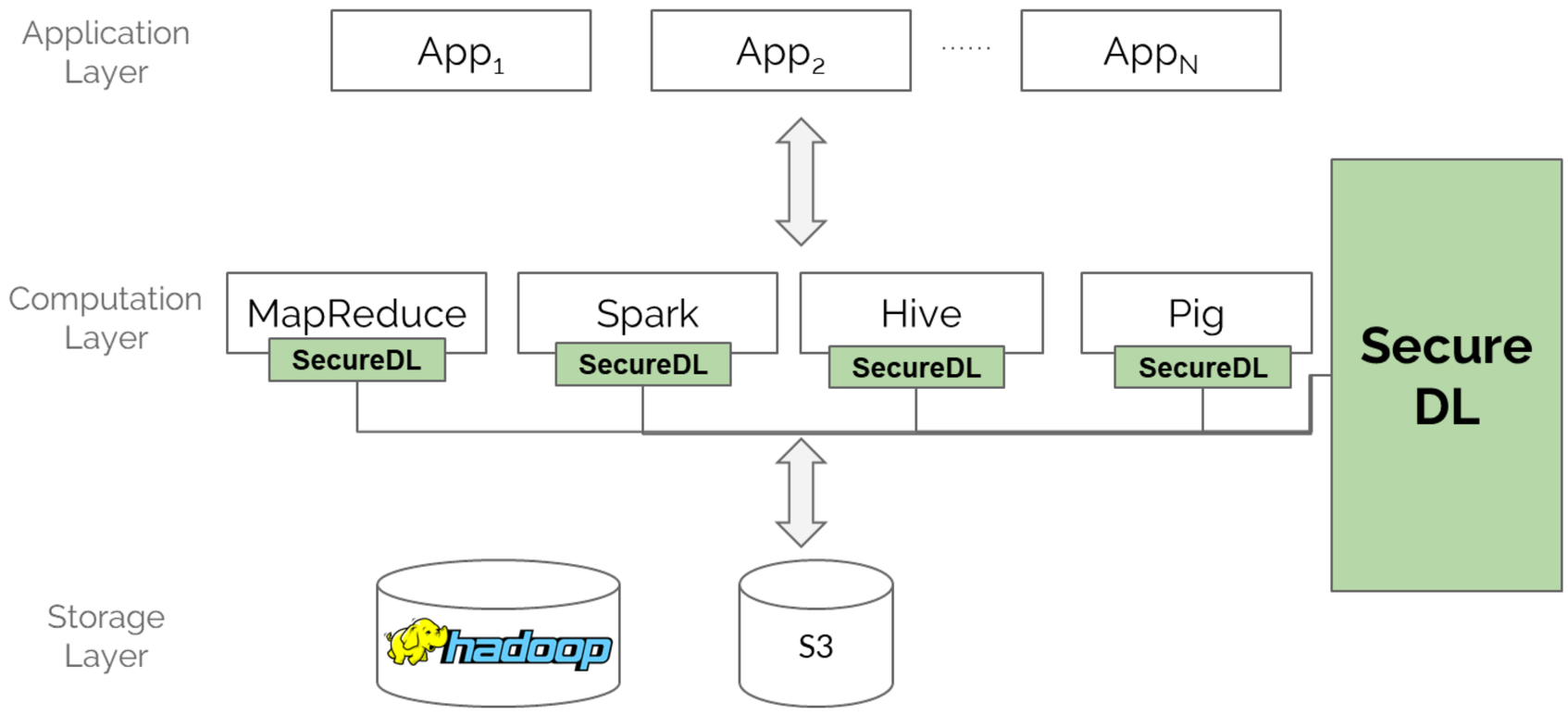
A Data Firewall based Approach for Securing Big Data

Murat Kantarcioglu, University of Texas at Dallas



Problems Addressed:

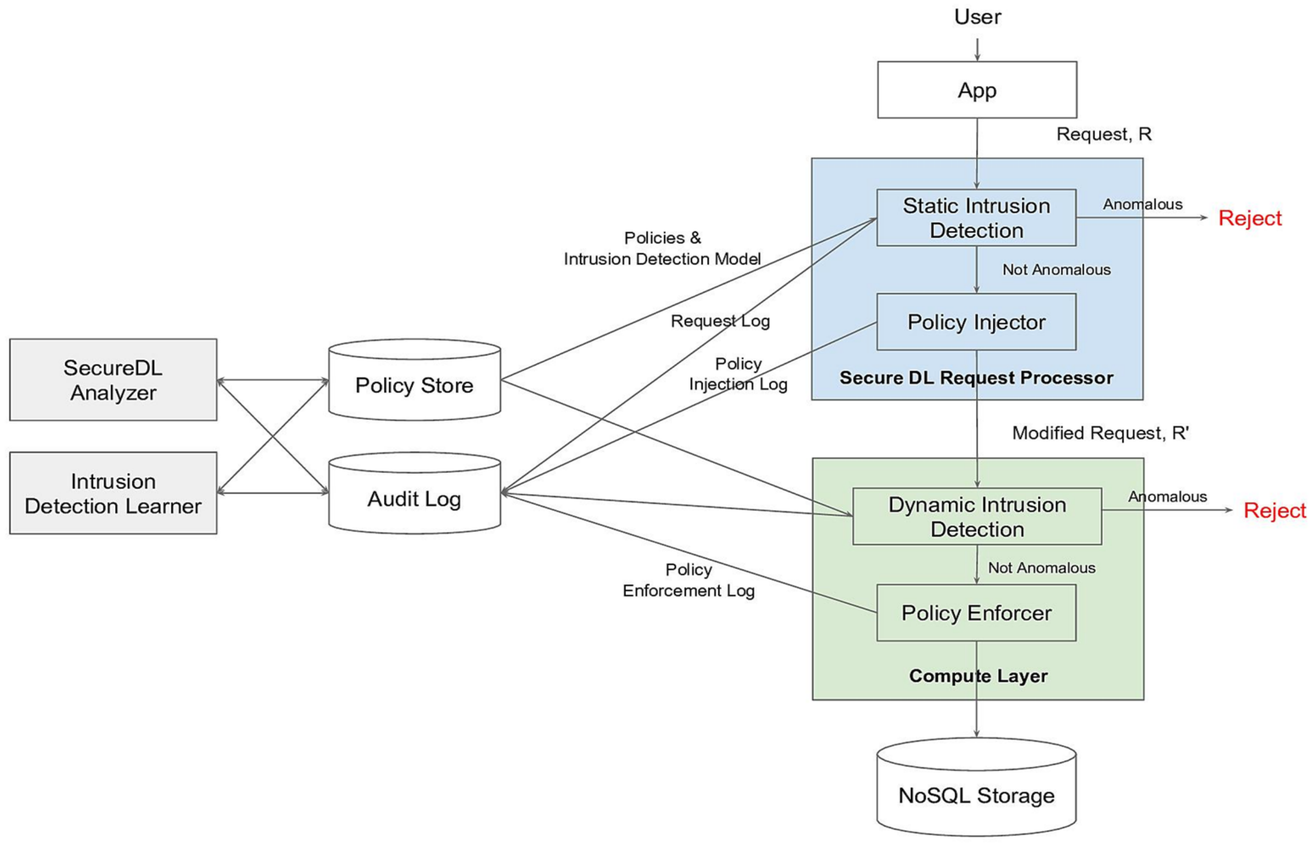
- Need to Protect Big Data Against Cyber Attacks
  - Big Data is critical for many organizations
  - New cyber attacks against big data storage systems
- Need to Comply with New Regulations
  - E.g., EU General Data Protection Directive
- **No simple and effective way to protect big data while complying with regulations across multiple databases**

Proposed Solution:

A data firewall to protect sensitive data against cyberattacks and comply with regulations:

- Advanced Security and Policy Enforcement
- Audit, Compliance Governance for Sensitive Data
- Misuse and Intrusion Detection

Architecture:



Impact on Data Security

- Complex policy enforcement
- Complementary to existing tools
- Intrusion detection
- Transparency
- No code change

Broader Impacts:

- Transitioning to practice by creating a practical big data firewall.
- During our project, we identified important security vulnerabilities in existing NoSQL databases and reported those vulnerabilities.
- Students who participated in the project to learned both big data analytics and cybersecurity related techniques.
- Research results are disseminated in many different forums and publications.