Engineering Analysis Systems for Cyber Security

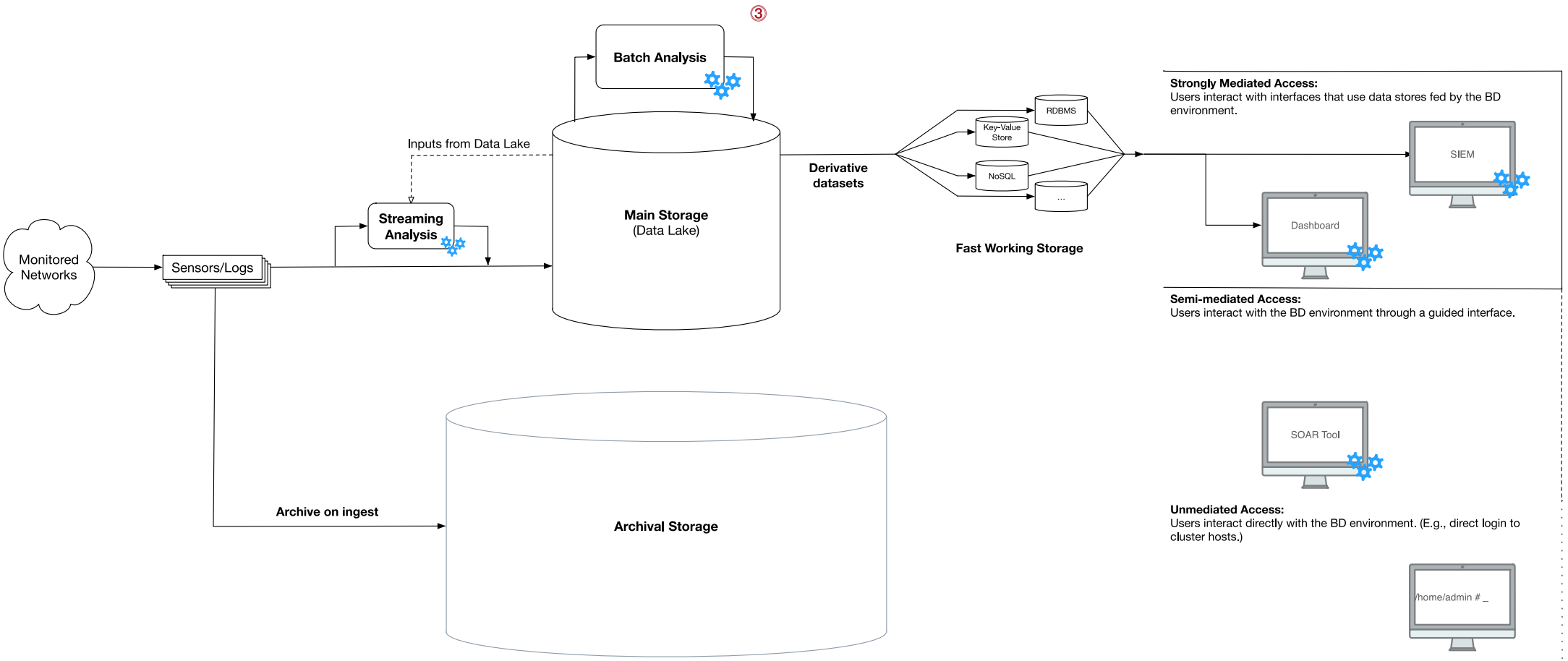
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Copyright Information

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-0426

Big Data (BD) Environments - A Reference Architecture for Cyber Security Operations



User Roles

Realtime analysts

Realtime analysts process incoming events with an emphasis on efficiency and rapid response. They should have all the data they need to do their jobs readily available, without having to think about the details of its storage and retrieval.

Non-realtime analysts

Non-realtime analysts use their experiences performing realtime analysis to create/extend new tools or automate manual workflows for improved effectiveness. They require access to the BD environment, but are not data administration/analysis experts.

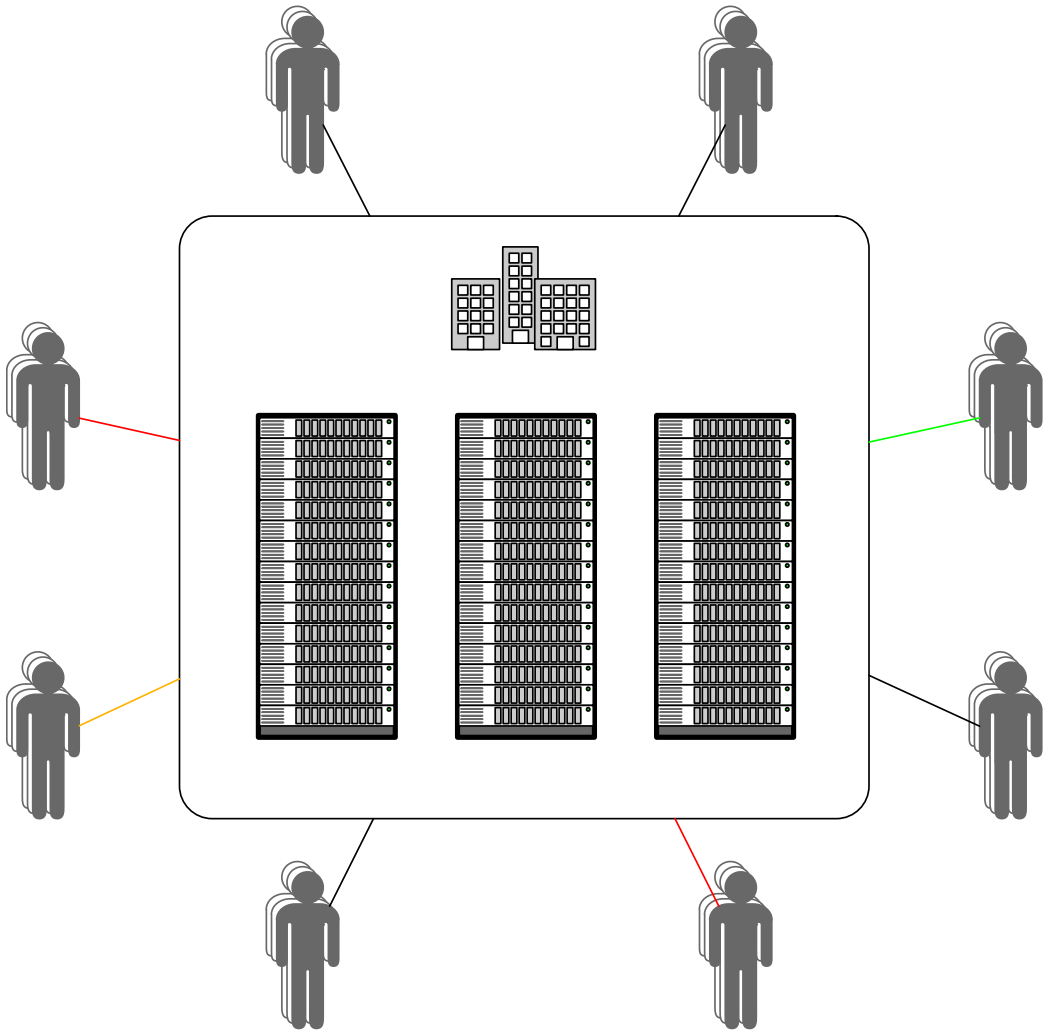
Data scientists

Data scientists Specialize in data manipulation and analysis. They may sometimes appreciate guided access to a BD environment, but require the ability to perform arbitrary transformations on data.

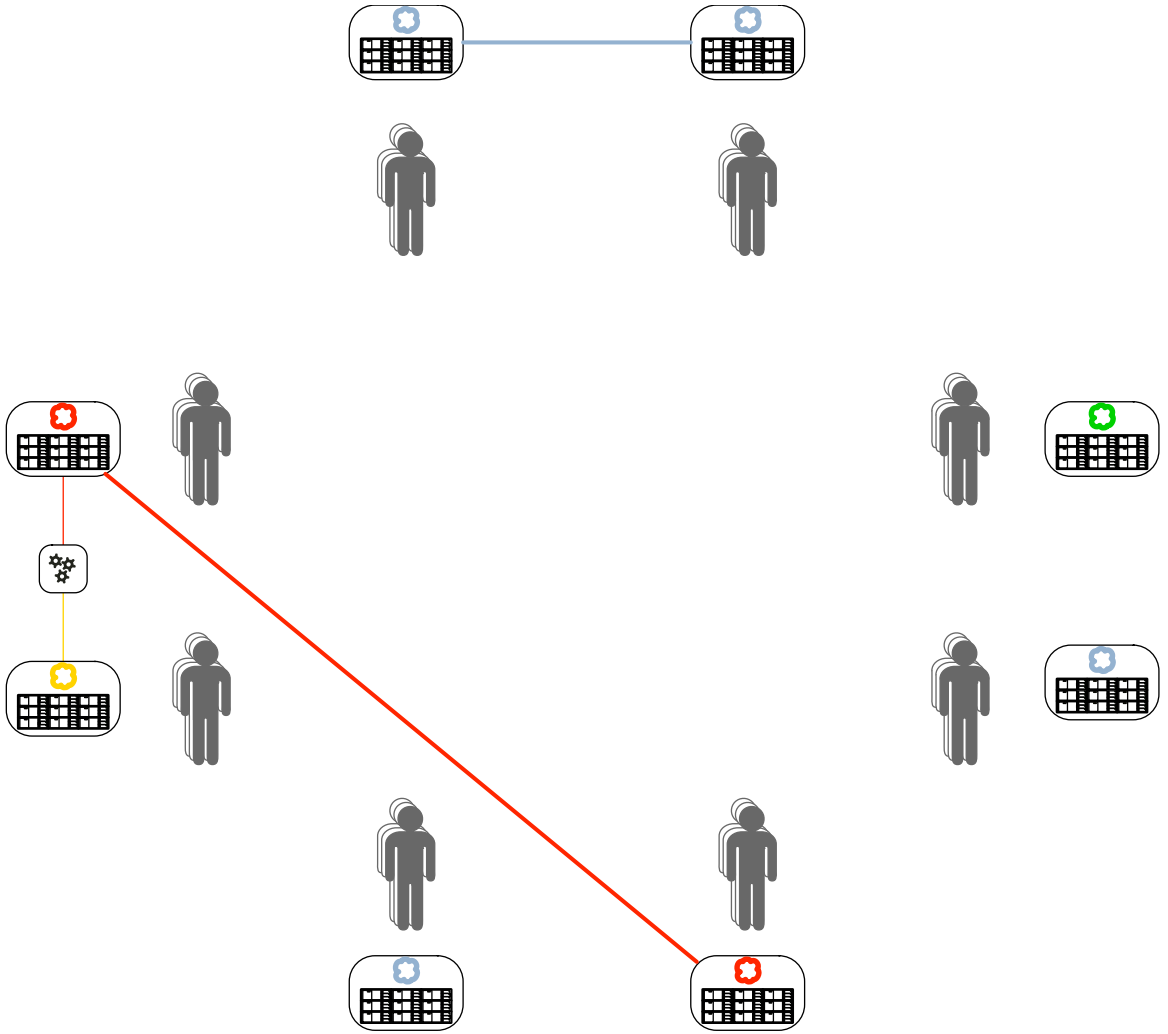
Administrators

Administrators make changes to the BD environment itself to make it run more effectively for other stakeholders.

Multitenant Model of Big Data Processing



Parallel Tenant Model of Big Data Processing



Aggregation-only Big Data Ingest