SecSWIM - Security Analyzer for System Wide Information Management

F. Morlang

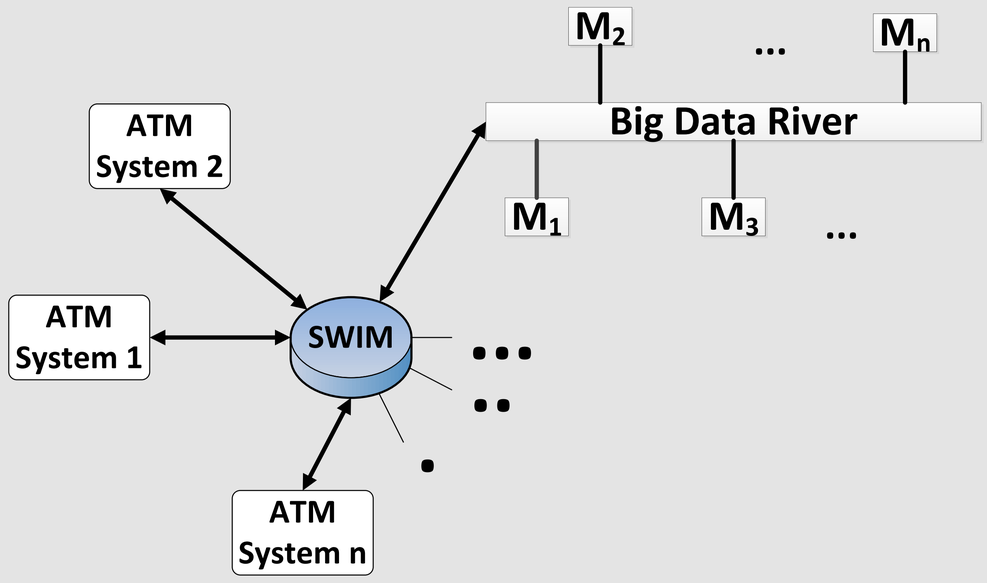
Deutsches Zentrum für Luft- und Raumfahrt e. V., Institut für Flugführung

Ziel

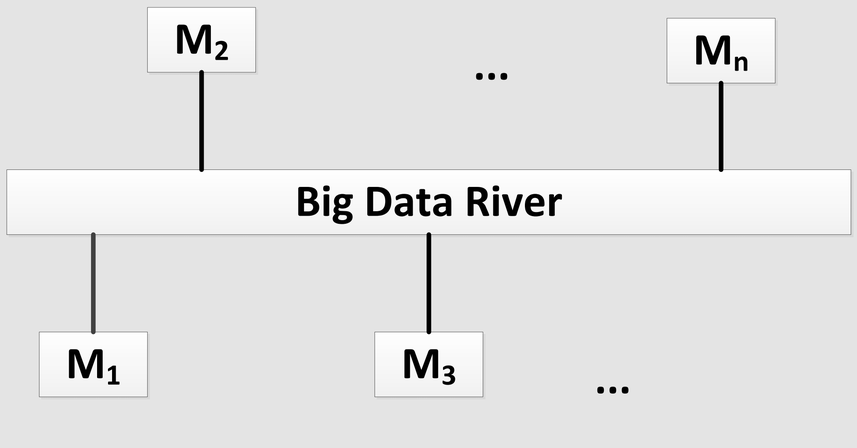
- Identifikation von Web Service Angriffen
  - Coercive Parsing
  - XML eXternal Entity (XXE) Angriffe
  - WS-Addressing Spoofing
  - XML Signature Wrapping
  - …
  - ..
  - .

Ansatz

- Datenanalysesystem als teilnehmendes SWIM Subsystem

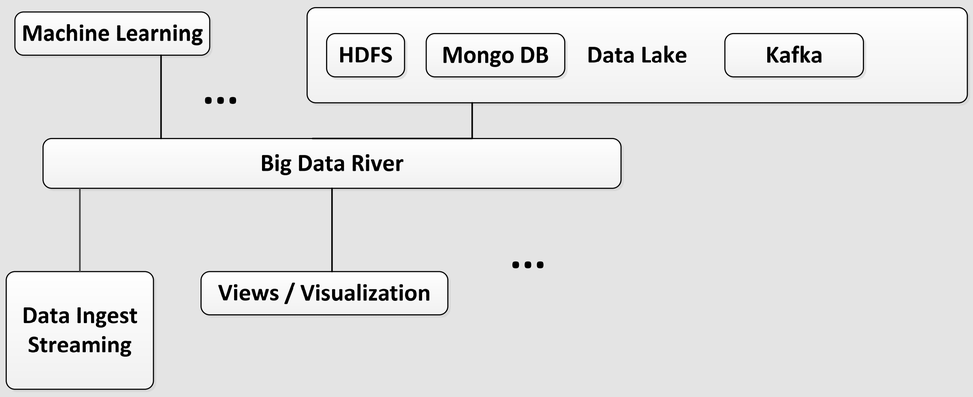


- Modulbasierte serial-in-the-large-iterative-in-the-small Machine Learning Big Data River Lösung



Umsetzung

- Modulsequenzierung Data River/Data Lake



- SOAP Message Klassifikation unter Berücksichtigung von
  - Service Identifier
  - Subnetzmask
  - Nachrichtenlänge
  - Übertragungsdauer
  - Headerlänge
  - …
  - ..
  - .
- Einstufungen
  - Angriff
  - In Ordnung
  - Undefiniert
- Neuronales Netz Multilayer Perzeptron Klassifikation

$$K \in X = \{Angriff, in\ Ordnung, undefiniert\}$$

Deutsches Zentrum für Luft- und Raumfahrt

Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR)

Institut für Flugführung

Lilienthalplatz 7, 38108 Braunschweig, Deutschland

Telefon +49 531 295-2523 | Frank.Morlang@dlr.de