



REAL-TIME DDOS ATTACK DETECTOR

By: Ankur Wahi



Objective – DDoS attack Detector

- Ingest

- *Read a file from local disk and write to a message system.*

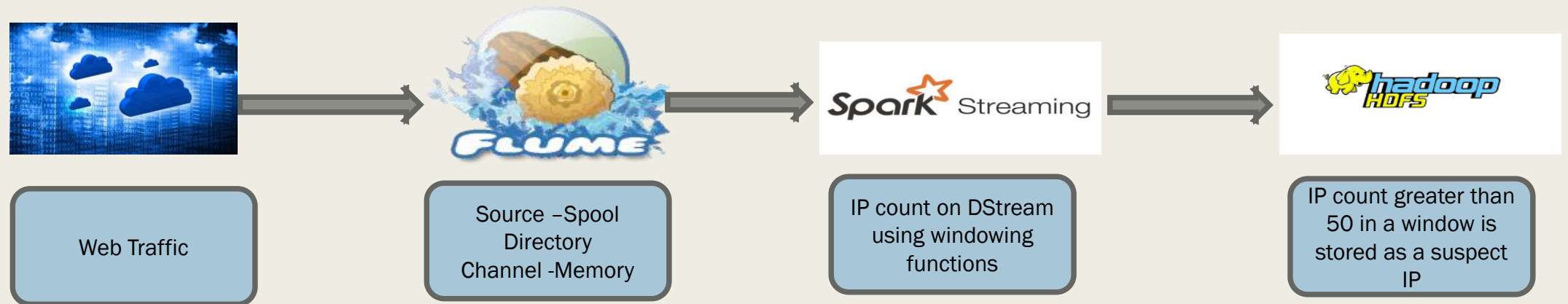
- Detection

- *Write an application which reads messages from the message system and detects whether the attacker is part of the DDOS attack*
 - *Once an attacker is found, the ip-address should be written to a results directory which could be used for further processing*
 - *An attack should be detected one to two minutes after starting*

Project Tech Stack

- Environment
 - *HDP sandbox 2.5*
- Messaging System
 - *Flume*
- Processing Framework
 - *Spark Streaming*
- Storage
 - *HDFS*

Project Architecture



Production Architecture

