CYBER TALENTS

MOROCO_ENSA_TEAM

Secur'IT Cup MENA & Africa 2021

Internet of Things (IoT) Forensic Data Analysis using Elasticsearch, Logstash, Kibana and Blockchain Technology

MOROCO_ENSA_TEAM

Année universitaire 2017/2018

Outline

I. Research Summary

II. Proposed method

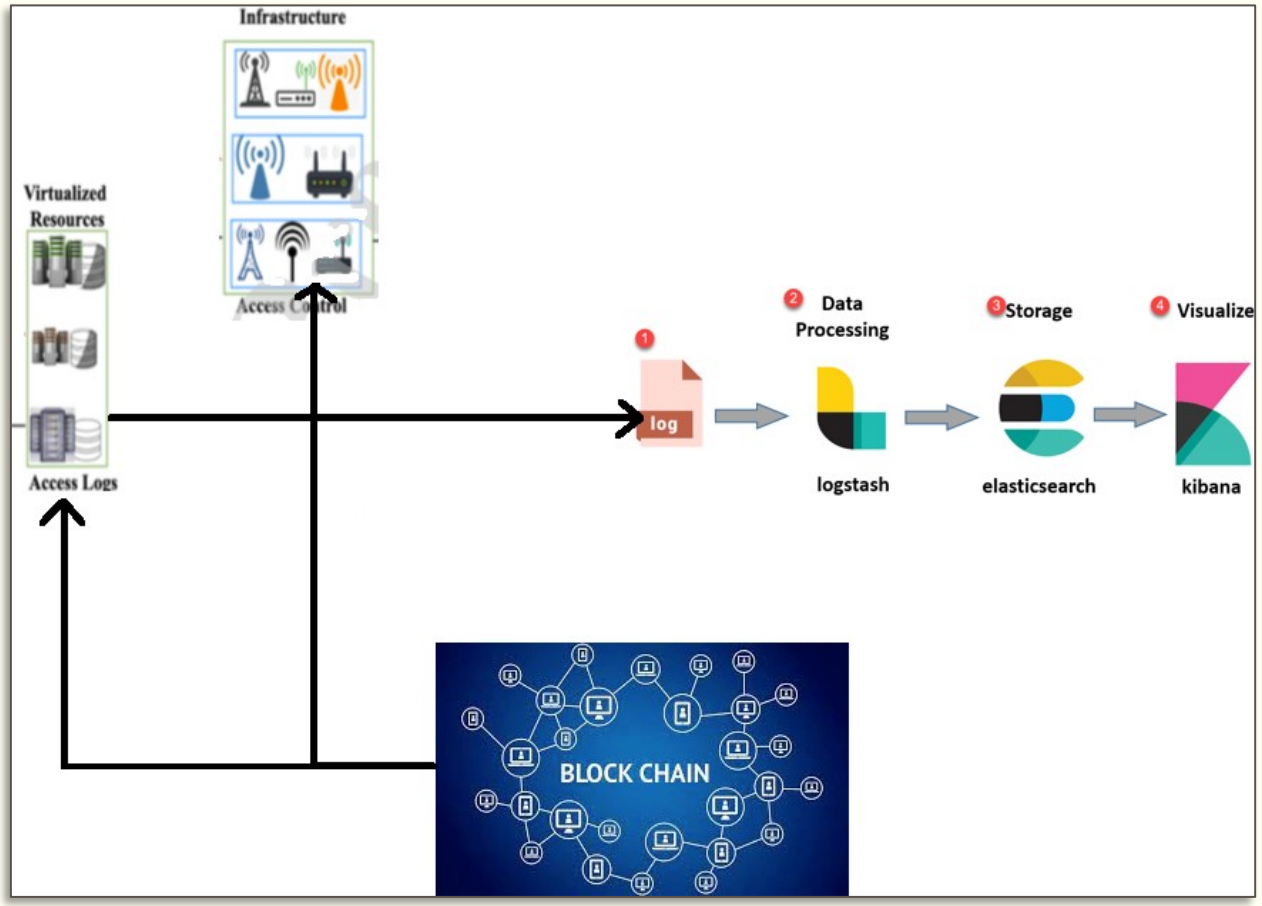
I- Research Summary

In the past decade, the Internet of Things (IoT) has emerged and has been of great importance in the digital world arousing the interest of the scientific community. The requirements of new small intelligent devices brought numerous security and privacy concerns. For that reason, detecting adversaries and attacks in an IoT platform using digital forensics requires intense data analysis and computational intelligence from fetching and validating systems logs, blockchain information assessment, etc. Testing and training are performed recurrently over various information acquired from the IoT environment to identify the presence of such adversaries. Trust, authorization and authentication-based information analysis and outcomes are significant in decision-making toward security.

I- Proposed method

Stage 1:

- **Collect the logs using Logstash and recover the log file from the devices in real time in Elasticsearch and the Blockchain.**

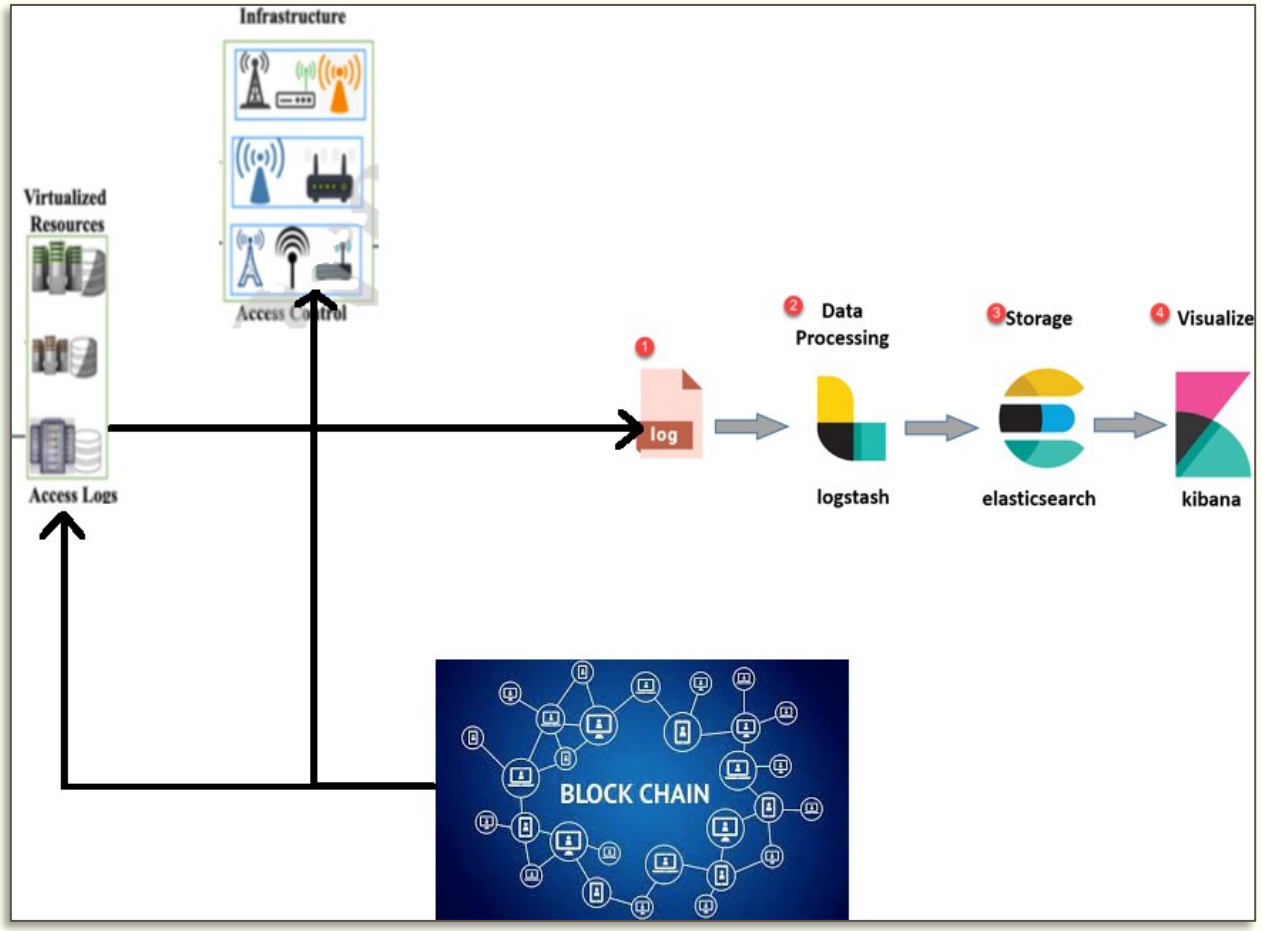


Source : Internet

I- Proposed method

Stage 2:

- **Store the data in blockchain to ensure that the log file is not modified.**

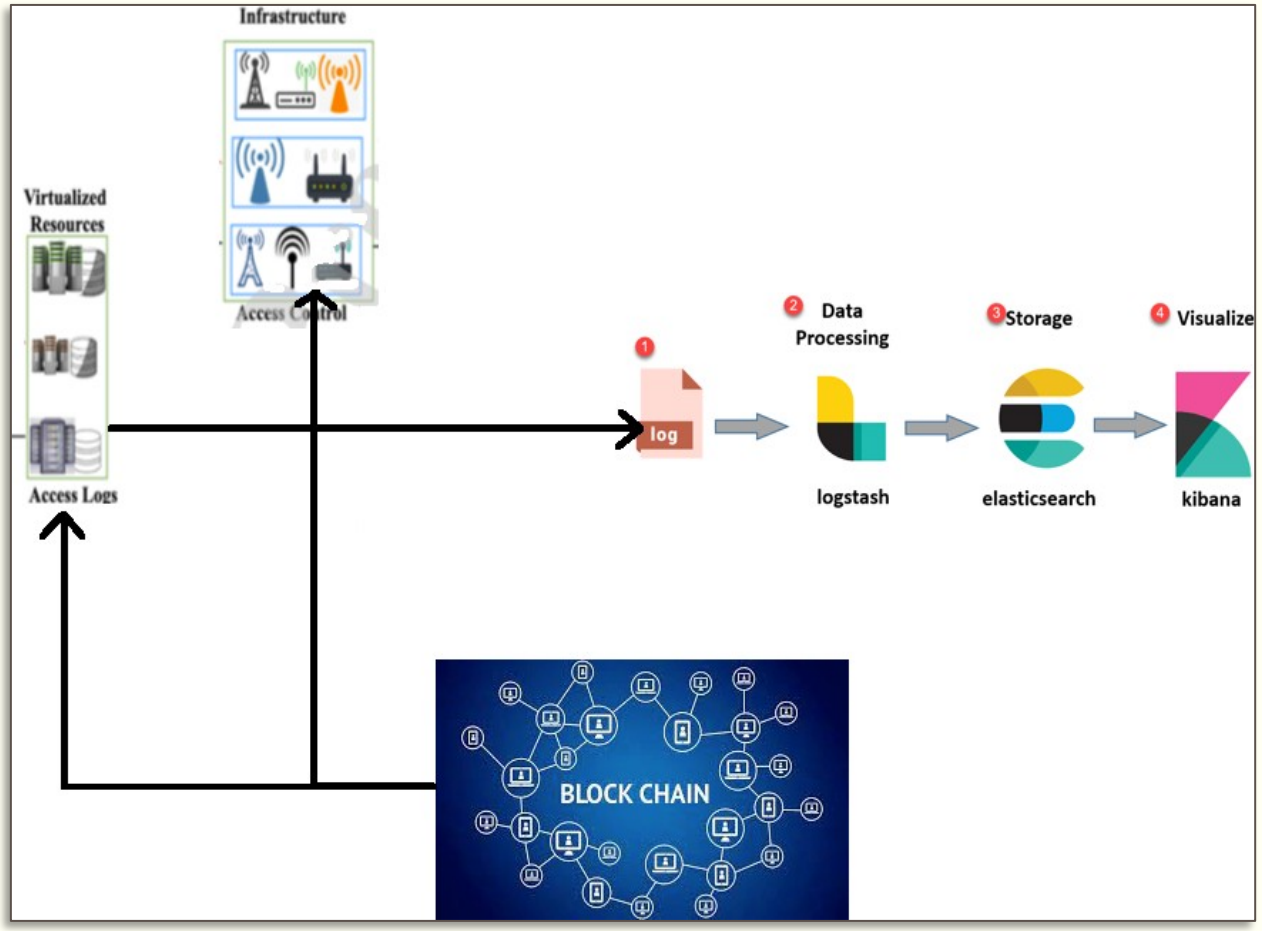


Source : Internet

I- Proposed method

Stage 3:

- **Store the data form Elasticsearch to make it easy to analyse it using Kibna**

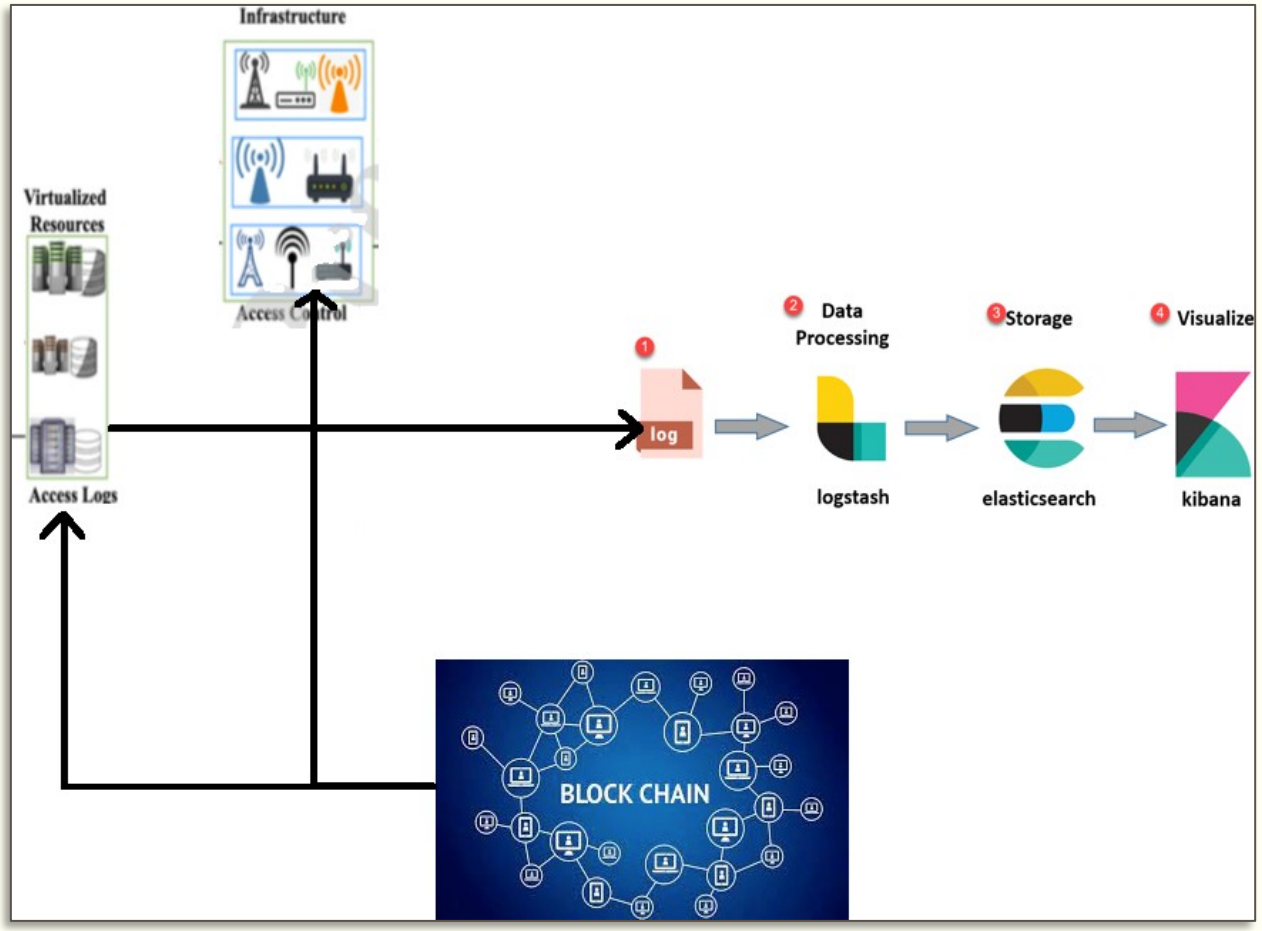


Source : Internet

I- Proposed method

Stage 4:

- **The analysis logs: Using Kibana to facilitate the process of forensic.**



Source : Internet