Deutsche Telekom Laboratories

DAI-Labor TU Berlin

Anomaly Detection and Early Warning System (ADEWaS)

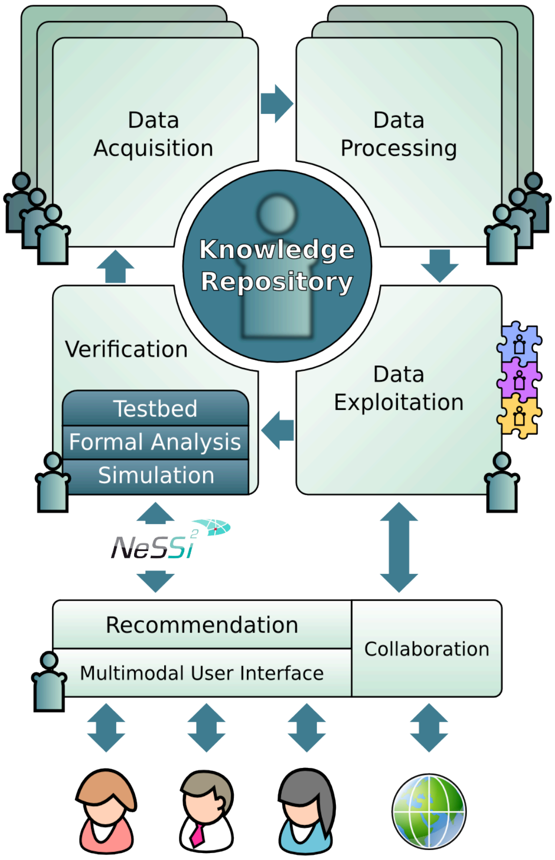
ADEWaS is a project funded by Deutsche Telekom Laboratories for developing an early warning system, which detects and failures at their early stages for telecommunication services and infrastructures. Telecommunication services, applications and infrastructure elements creates huge amount of audit trails that, if properly analyzed, carries clues in the form of anomalies. Timely detection and analysis of these anomalies may result in beneficial early warning messages for detection of attacks, failures and misuse.

In this project, the DAI Laboratory realizes a multiagent system (MAS) used to detect anomalies and create warning at early stages.

The ADEWaS MAS has the following major tasks;

1. Collect data from various sources, e.g. server log files, intrusion detection systems, and transaction system.
2. Translate the various data formats used by data source into a common format.
3. Provide a semantic description for the system, data and detection results.
4. Supply data to anomaly detection approaches.
5. Present detection results, generate warnings and realize alert and notification mechanisms.

The ADEWaS MAS is designed to work with a variety of anomaly detection approaches. The project partners Ben-Gurion University of the Negev and Deutsches Forschungszentrum für Künstliche Intelligenz implement those approaches. The approaches range from unsupervised, statistical approaches to supervised, machine learning approaches.



The approach developed within ADEWaS project is comprised of different categories of agents. The Data Acquisition agents are distributed among the network, encapsulate data sources and provide the raw data to Data Processing agents. These agents fulfill different tasks such as the annotation of raw data, the conversion to a common format, but also provision and notification mechanisms for other ADEWaS components, such as the detection agents. These agents belong to the category Data Exploitation and provide detection results that can be reviewed and verified with the help the user.

Contact:
DAI-Labor, Technische Universität Berlin
Prof. Dr. Sahin Albayrak
Telephone: +49 (0) 30 - 314 74000
Fax: +49 (0) 30 - 314 74003
sahin.albayrak@dai-labor.de

CC SEC Manager im DAI-Labor:
Seyit Ahmet Camtepe, Ph.D.
Telephone: +49 (0) 30 - 314 74117
E-Mail: ahmet.camtepe@dai-labor.de

CC SEC Security