Challenge Detection in Cloud Computing

Noor Shirazi

07/02/2013

AIT Austrian Institute of Technology • ETRA Investigación y Desarrollo • Fraunhofer Institute for Experimental Software Engineering IESE • Karlsruhe Institute of Technology • NEC Europe • Lancaster University • Mirasys • Hellenic Telecommunications Organization OTE• Ayuntamiento de Valencia • Amaris

Cloud Computing

Cloud computing is an on-demand service model for IT provision, often based on virtualization and distributed computing technologies. Cloud computing architectures have:

- highly abstracted resources
- near instant scalability and flexibility
- near instantaneous provisioning
- shared resources (hardware, database, memory, etc)
- ‘service on demand’, usually with a ‘pay as you go’ billing system
- programmatic management (eg, through WS API)

Source: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing

Motivation

SEcure Cloud computing for CRitical infrastructure IT

- Everything goes cloud
  - E-government
  - Traffic control system
  - Health Care
  - Consumer data (Dropbox, Google docs, etc)
  - Soon all kinds of applications (inc. CI) without us noticing it
- Requirements for cloud applications vary
  - Commercial ones mainly to deal with load peaks and to get on-demand hardware resources (scalability & elasticity)
  - CI pose much stronger requirements in terms of security, resilience, legal and data protection etc, than commercial applications.
- What is the problem?
  - These services are potential target for challenges such as cyber attacks, information disclosure, Malwares, DDoS etc.
  - Do existing controls such as (ACL, FW, ADT) to protect data and services work with cloud service elasticity & scalability?
  - Root cause analysis, attack attribution etc.

Overall SECCRIT Objectives → Output

SEcure Cloud computing for CRitical infrastructure IT

Legal Guidance on Data Protection and Evidence

Risk Assessment and Management Methodology

Policy Specification Methodology and Tool

Cloud Assurance Profile and Evaluation Method

Anomaly Detection Techniques and Tools

Policy Decision and Enforcement Tools

Cloud Resilience Management Framework

Tools for Audit Trails and Toot Cause Analysis

Cloud Security Guidelines

Demo 1: Storage and Processing of Sensitive Data

Demo 2: Hosting Critical Urban Mobility Services

SECCRIT Objectives

SEcure Cloud computing for CRitical infrastructure IT

Objective:Understanding Cloud Behaviour

- Suitable tools that allow for an efficient way to retrieve relevant information from the cloud system to evaluate the normal system behavior , and to drive the actual operation state, which then need to attribute responsibility in case of service failures. (monitoring, forensic analysis, anomaly detection, root cause analysis, resilience analysis in various layers)

Requirements:

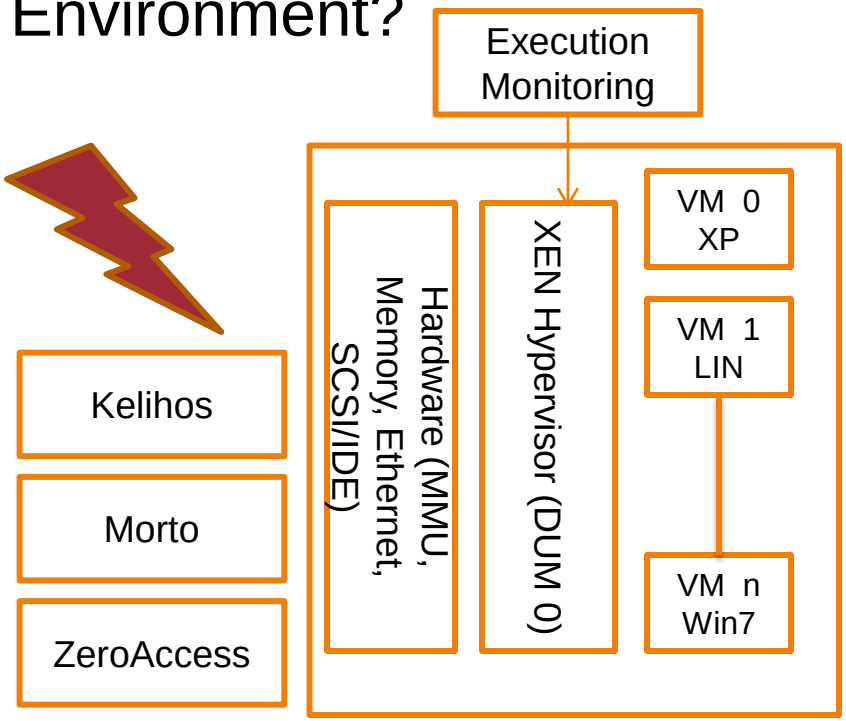
- We analyze the viability of the state-of-the-art anomaly detection techniques (ADTs) in elastic cloud deployment scenarios.
- Develop ADTs that are robust to properties of cloud and can accommodate dynamic behavior of cloud infrastructure.
- Two important perspectives will be used to develop ADTs:
  - Network level perspective: Able to capture all traffic from several customers.
  - System level perspective: Able to capture service level semantics.
- Develop software implementation of techniques for demonstration.

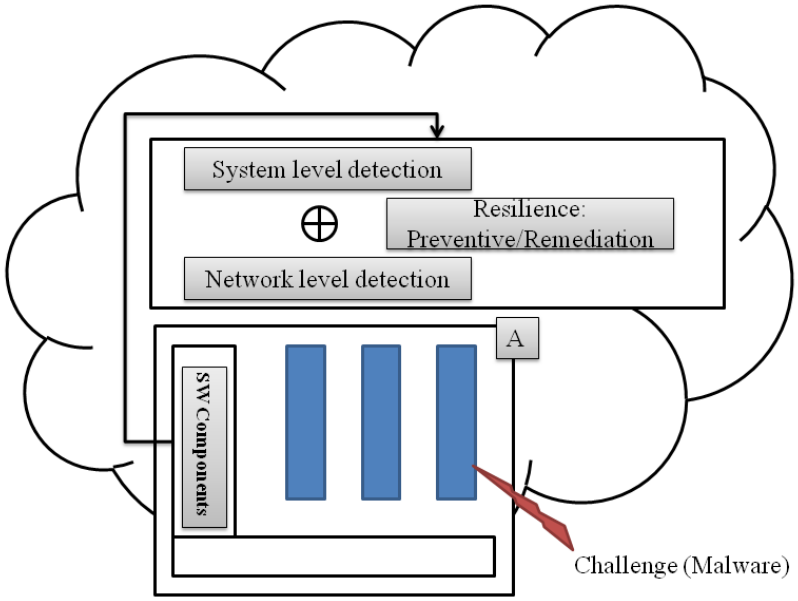
Key Challenges

- Defining a representative normal behaviour is challenging
- The boundary between normal and anomalous behaviour is often not precise
- The exact notion of an anomaly is different for different application domains
- Normal behaviour keeps evolving
- Evaluation of anomaly detection techniques
- Can anomaly detection systems be developed for such elastic cloud environments, and how should they be operationally applied?

Potential Solution

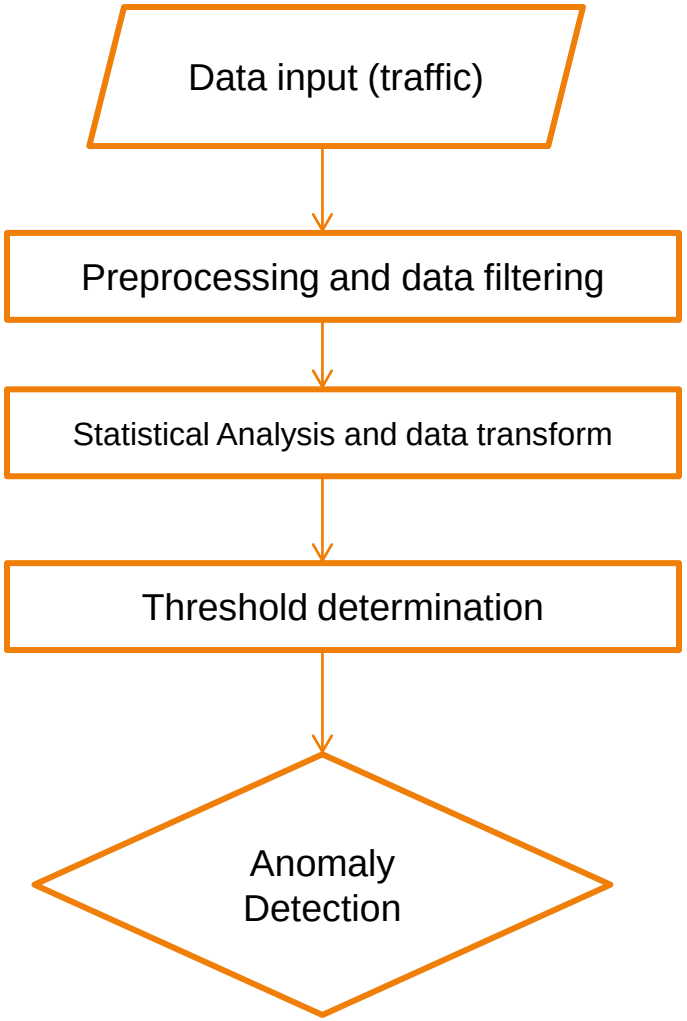
Approaches exist to learn the behaviour of traffic in near real-time, we will investigate whether such techniques could be applied, given the dynamic nature of a cloud Environment?



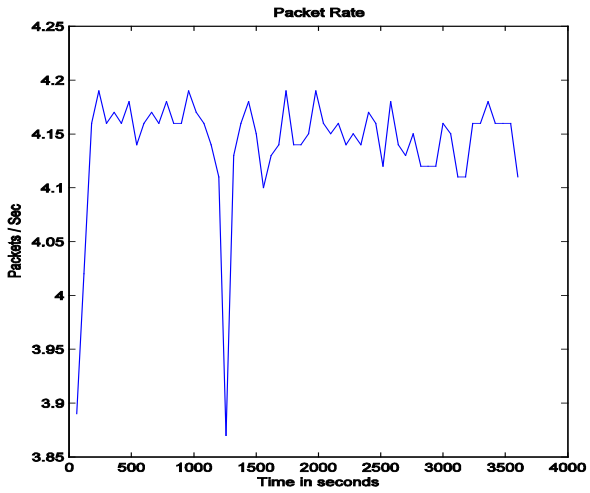


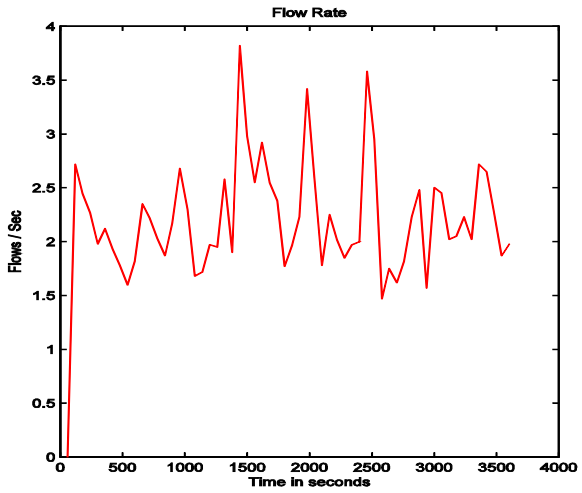
N/W Level: Statistical Approach

- The strength is to detect unknown attacks.
- Derive model of normal behaviour and detect divergence.
- Can detect known and unknown malicious activities likewise.
- The normal profile has been derived based on different information such as system calls on a single host, payload byte patterns in received traffic, or volume and entropy information over the traffic in a whole network



Network level analysis



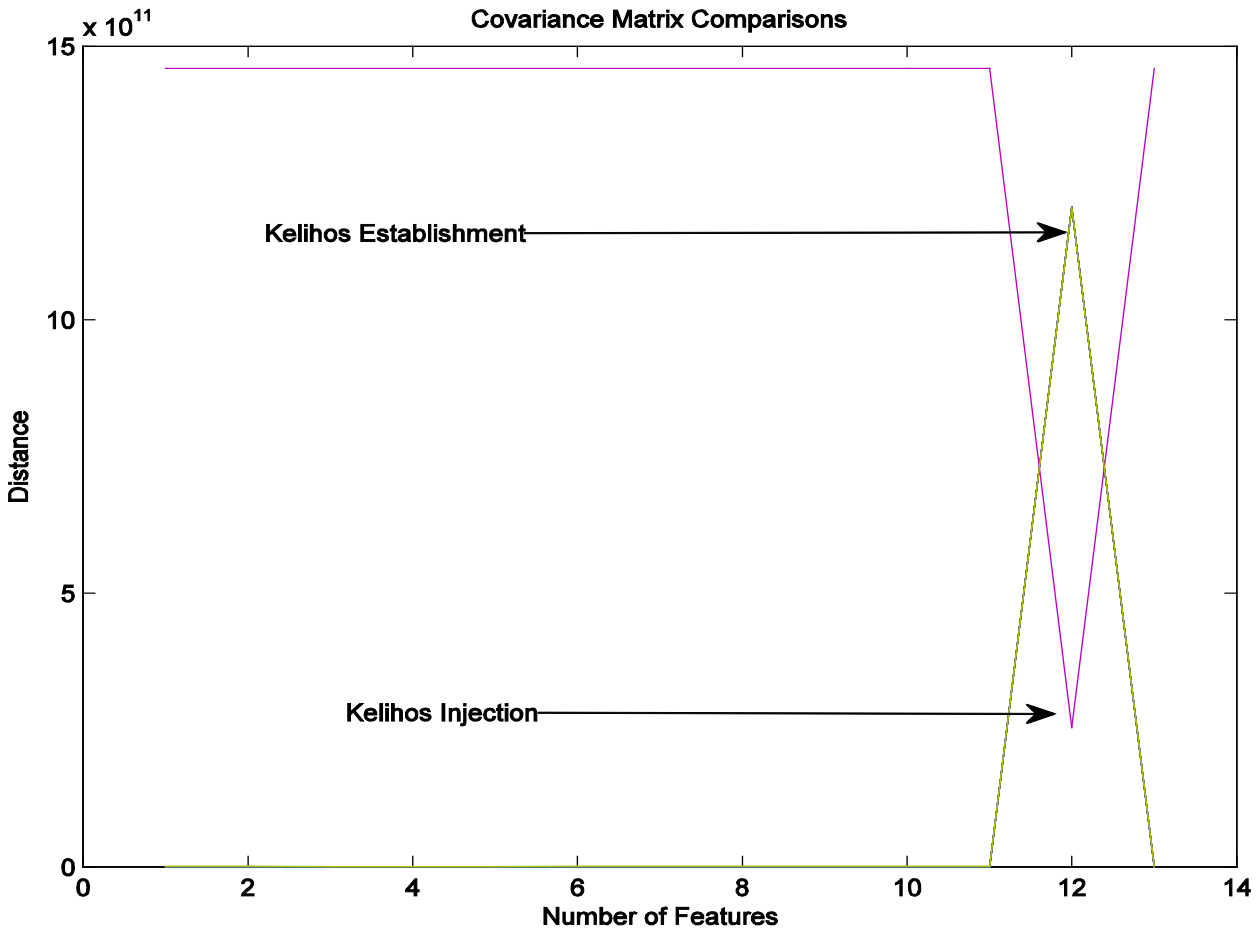


The goal is to identify some traffic parameters, which can be used to describe the network traffic and that vary significantly from the normal behavior to the anomalous one

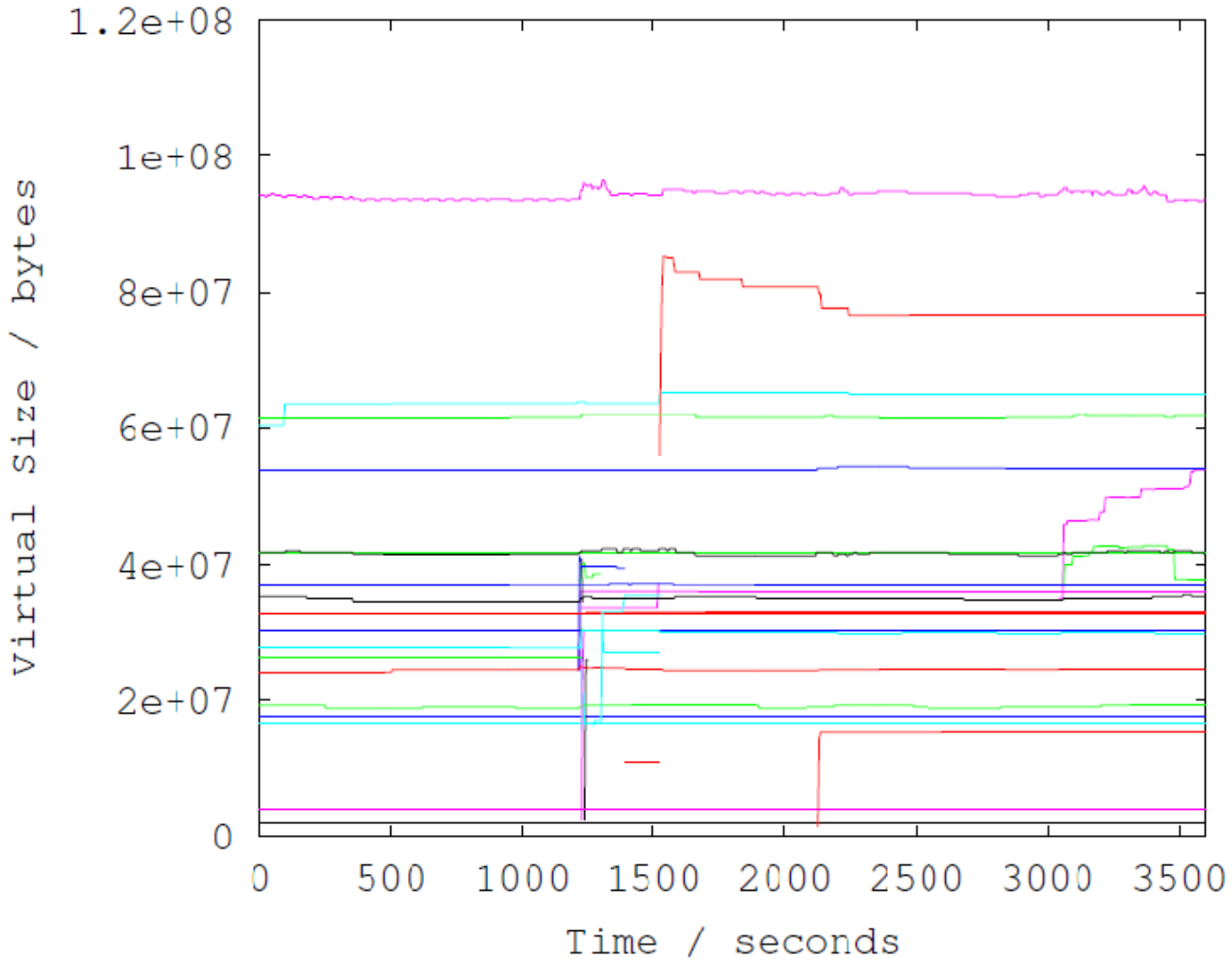
- Packet length
- Inter-arrival time
- Flow size
- Number of packets per flow

For each parameter we can consider (Mean Value, Variance and Distribution function)

Covariance Matrix Analysis



System level analysis



SEcure Cloud computing for CRitical Infrastructure IT

Contact

Noor Shirazi, Andreas Mauthe & David Hutchison
Lancaster University
01524 510380
n.shirazi@lancaster.ac.uk

AIT Austrian Institute of Technology • ETRA Investigación y Desarrollo • Fraunhofer Institute for Experimental Software Engineering IESE • Karlsruhe Institute of Technology • NEC Europe • Lancaster University • Mirasys • Hellenic Telecommunications Organization OTE• Ayuntamiento de Valencia • Amaris