Assessing the Security of Internet Connected Critical Infrastructures

The Comifin Project Approach

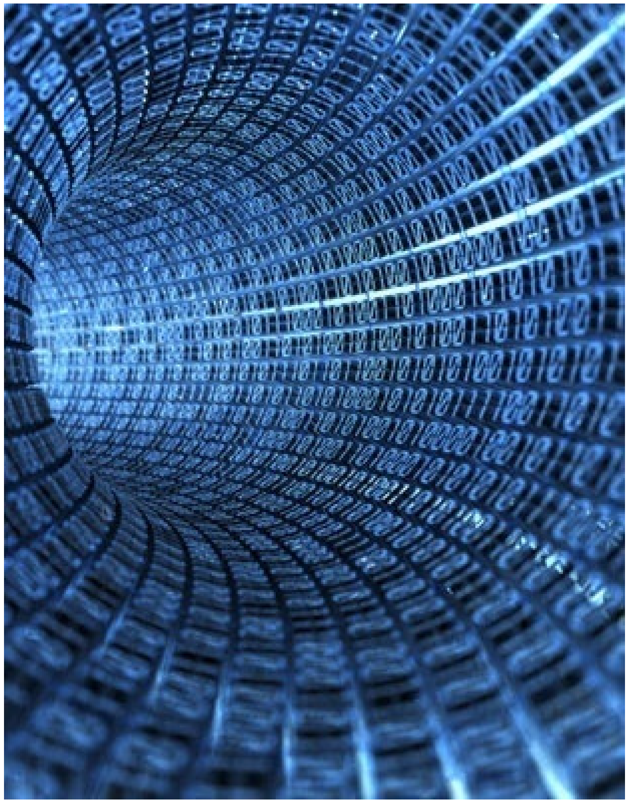
H. Ghani, A. Khelil, N. Suri, G. Csertán, L. Gönczy, G. Urbanics, J. Clarke

Dept of Computer Science, TU Darmstadt, Germany
Optxware, Hungary
WIT, Ireland

Motivation

- ❑ IoT ='s data conduit linking "things"
- ❑ Things … sensors, devices, systems …. and onto comm. links within and across Critical Infrastructures (CI) for sensing, notification and control

➔ IoT resilience (or its lack) affects the CI resilience based on it



Goal: Basing Secure Communications on Insecure IoT

- ❑ Overlays
  - Adds filters
  - Adds routes
  - Adds functionality
  - ➢ Provides buffer to IoT threats ➔ Decouples IoT and CI associations
  - ➢ Provides monitoring of IoT <-> CI

- ❑ P2P etc : Classical approaches offer use of redundant paths and resources…but mostly offers regulated levels of resilience
  - Resources change, routes change
  - Attacks change

➢ Can we enhance IoT-centric overlays based communication to a "metrics" driven <u>adaptive</u> (on-demand QoP) levels of resilience?

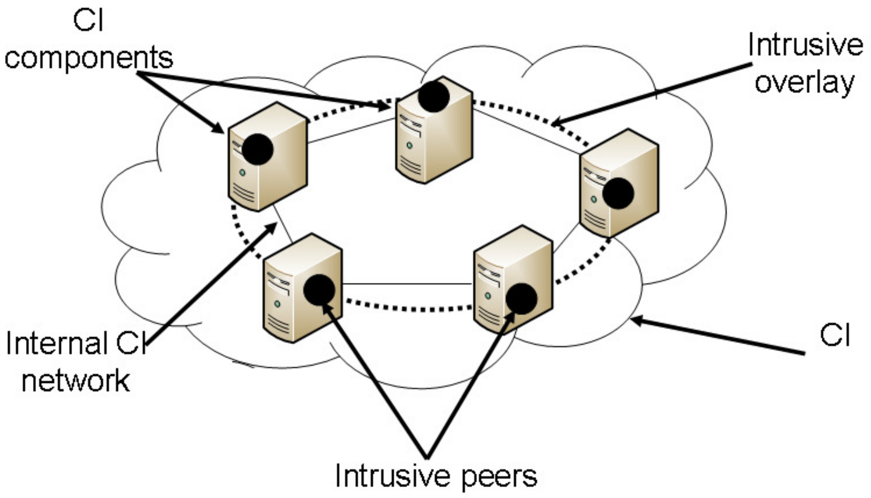
Approach: Metrics Driven Adaptation

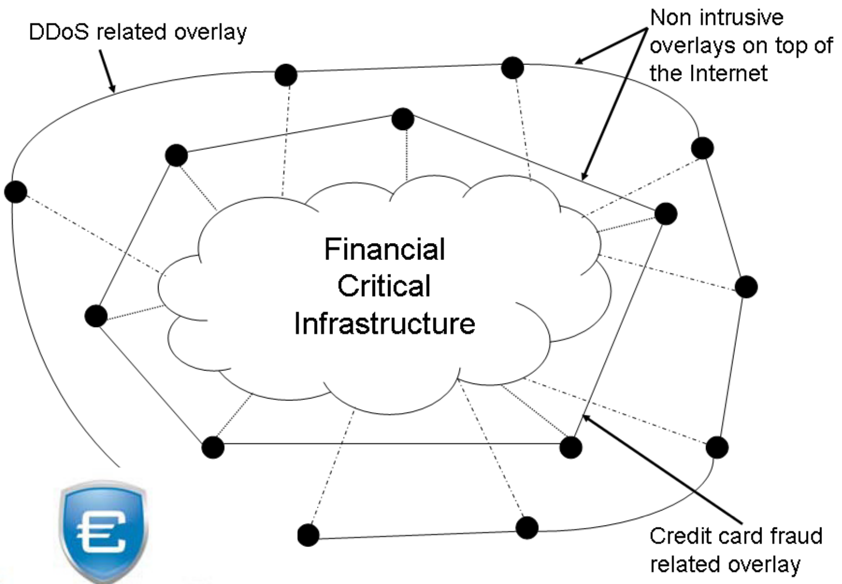
- ❑ Quantify resilience of IoT (sensing and communication) overlays
  - Overlay trust metrics
  - QoP specification with CI application-relevant metrics
- ❑ Utilize the metrics basis to provide adaptation of overlays QoP
  - Design phase (Trustworthiness by Design)
  - Run-time phase (Trustworthiness by Adaptation)

Process

- ❑ Metrics-based scoping of SLAs
- ❑ (Automated) Generation of the monitoring configuration from the metric and SLA definitions
- ❑ Multi-level metric evaluation system to handle complexity utilizing
  - simple arithmetic evaluators
  - simple rule based evaluator
  - complex event processing based evaluator
- ❑ Reference implementation for trustworthiness by adaptation based on run-time metrics monitoring
  - Case Study: P2P-based protection approaches targeting a Financial Infrastructure (FI)

IoT linked CIP Overlay Models (Intrusive, Non-Intrusive)




DDoS related overlay
Non intrusive overlays on top of the Internet
Financial Critical Infrastructure
Credit card fraud related overlay

COMIFIN www.comifin.eu

- ❑ Intrusive Overlays: Dedicated probes, routers, channels …
- ❑ Distributed control systems (SCADA)

- ❑ Non-intrusive Overlays … e.g. P2P: self standing properties - secure, dependable - & decoupled from the CI!
- ❑ CI handled as black-box
- ❑ Non-intrusive approach to realize an additional defense line/layer that implements further/new (usually collaborative) security mechanisms

Trustworthiness Metrics

- Determining appropriate set of metrics requires extensive understanding of the target domain (Savola taxonomy)
  - RoI cost-benefit metrics
  - ISM information security management metrics
  - SDT security, dependability & trust metrics

  ➔ GQM: Goal-Question-Metric (user centric)

- **CoMiFin**: multi-level GQM based evaluation system containing
  - Resource-level metrics: CPU, sensor, net usage
  - Availability metrics: uptime, availability, repair time
  - Communication metrics: encryption strength, latency
  - Overlay specific metrics: k-connectivity etc
  - CI Application SpecificTrust metrics:
    - CI application requirements, responsiveness, quality, privacy, …
    - Trust level of participant CI entity, type/priority of shareable info

Metrics Driven QoP Assessment

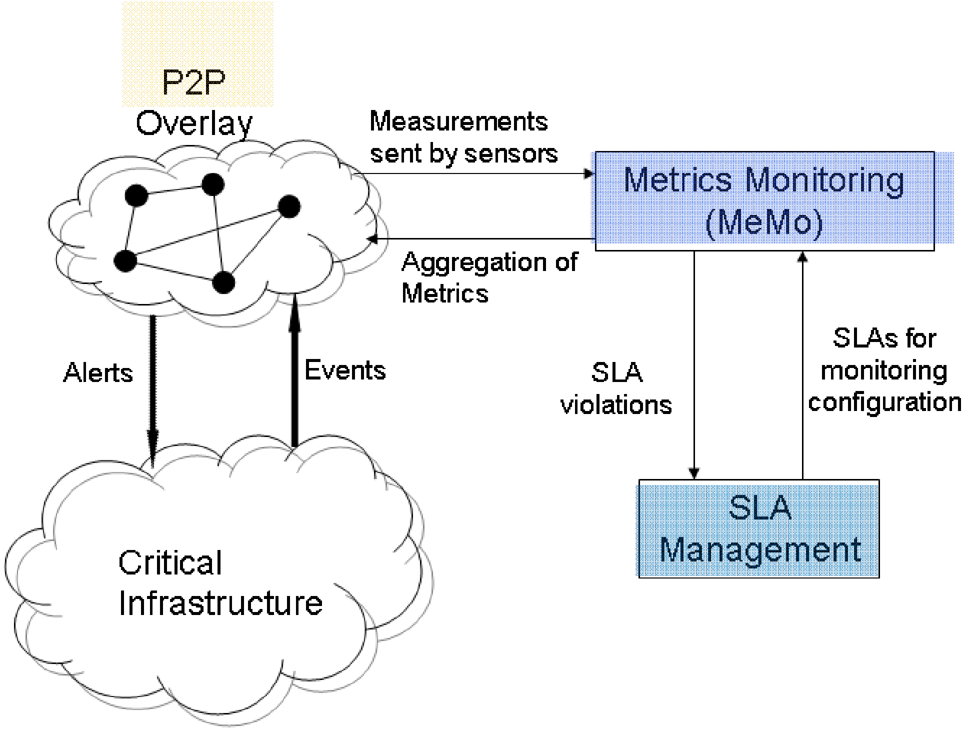
By Design　　　　By Adaptation

- ❑ Application dependent overlay security requirements
- ❑ Metrics set to monitor fulfillment of requirements

- ❑ Usage of metrics for SLA specifications with viability of run-time monitoring (MeMo: Metrics Monitoring)
- ❑ IoT based compliance monitoring on SLA "degree of compliance"
- ❑ SLA violation detection with SLA "adjustments" framework

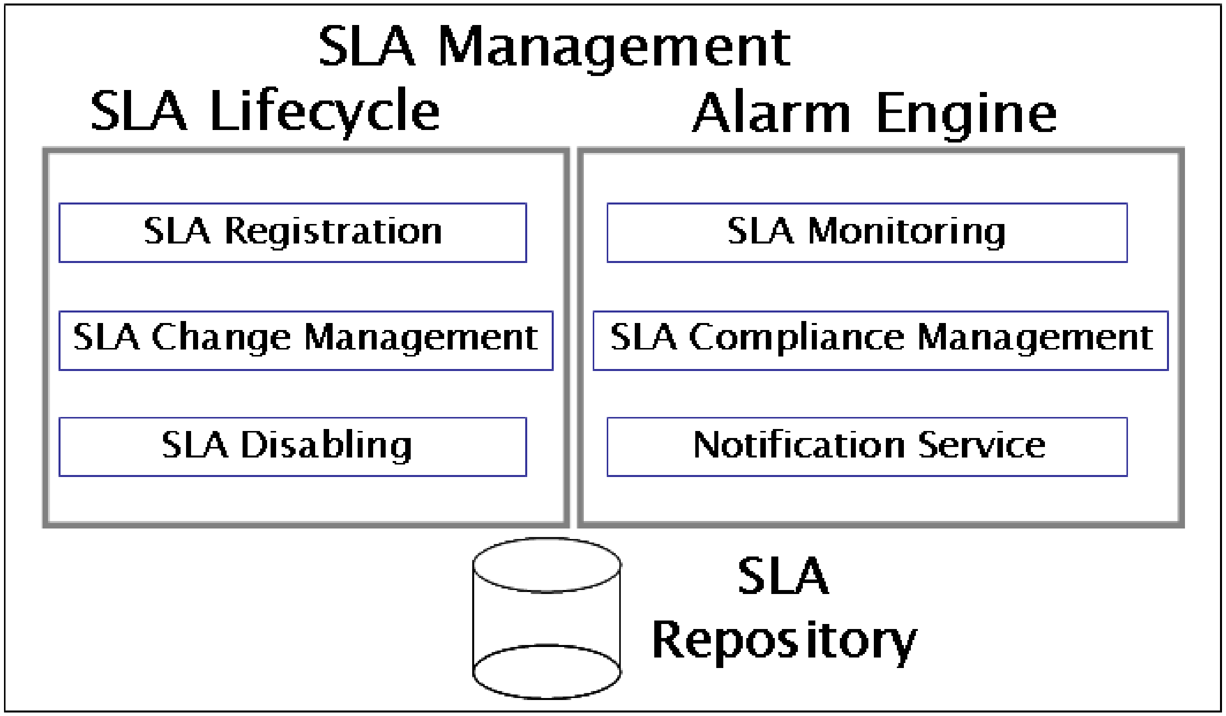
Metric-based QoP Assessment

- Core ideas
  - Metric-based definition of SLAs
  - Run-time metric monitoring & SLA compliance checking



Trustworthiness by Design

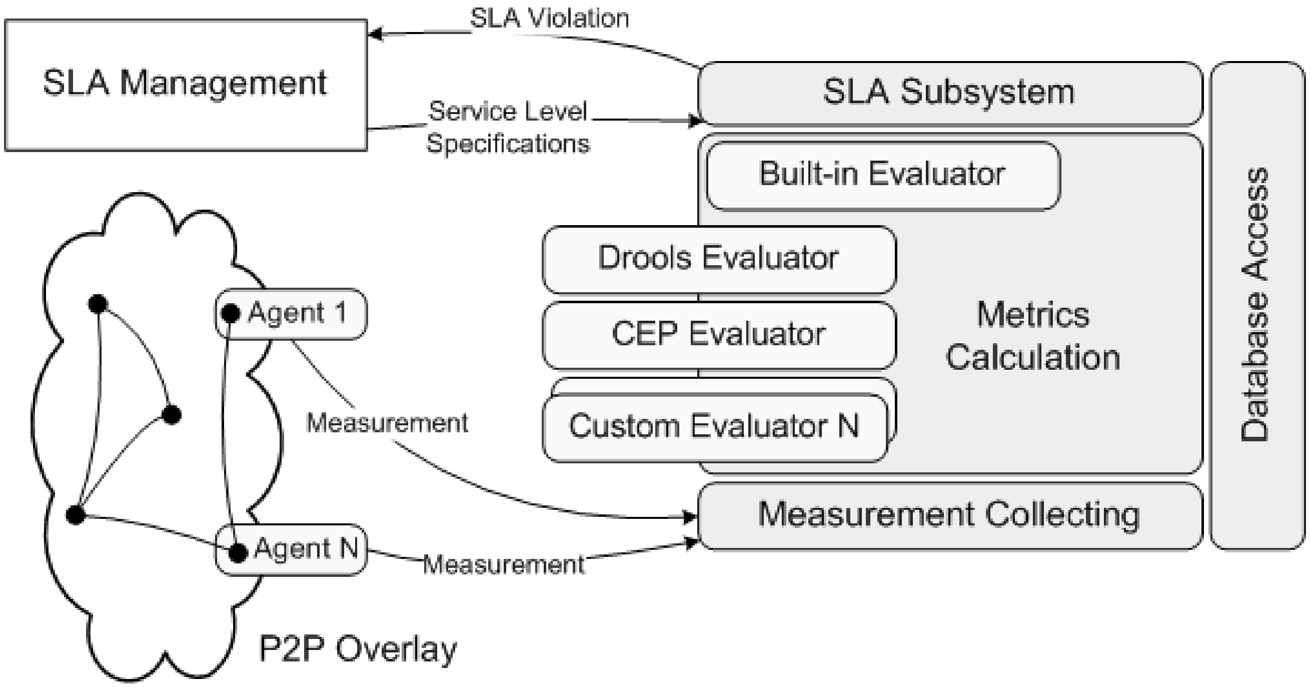
- ❑ Define metric-based SLA to
  - capture user requirements
  - specify guarantees the system is required to provide
  - define penalties for missing specified guarantees
- ❑ Implementation of an SLA Management component



Trustworthiness by Adaptation

Goal: evaluate QoP at run-time and accordingly trigger alerts or overlay reconfigurations to maintain the desired QoP level

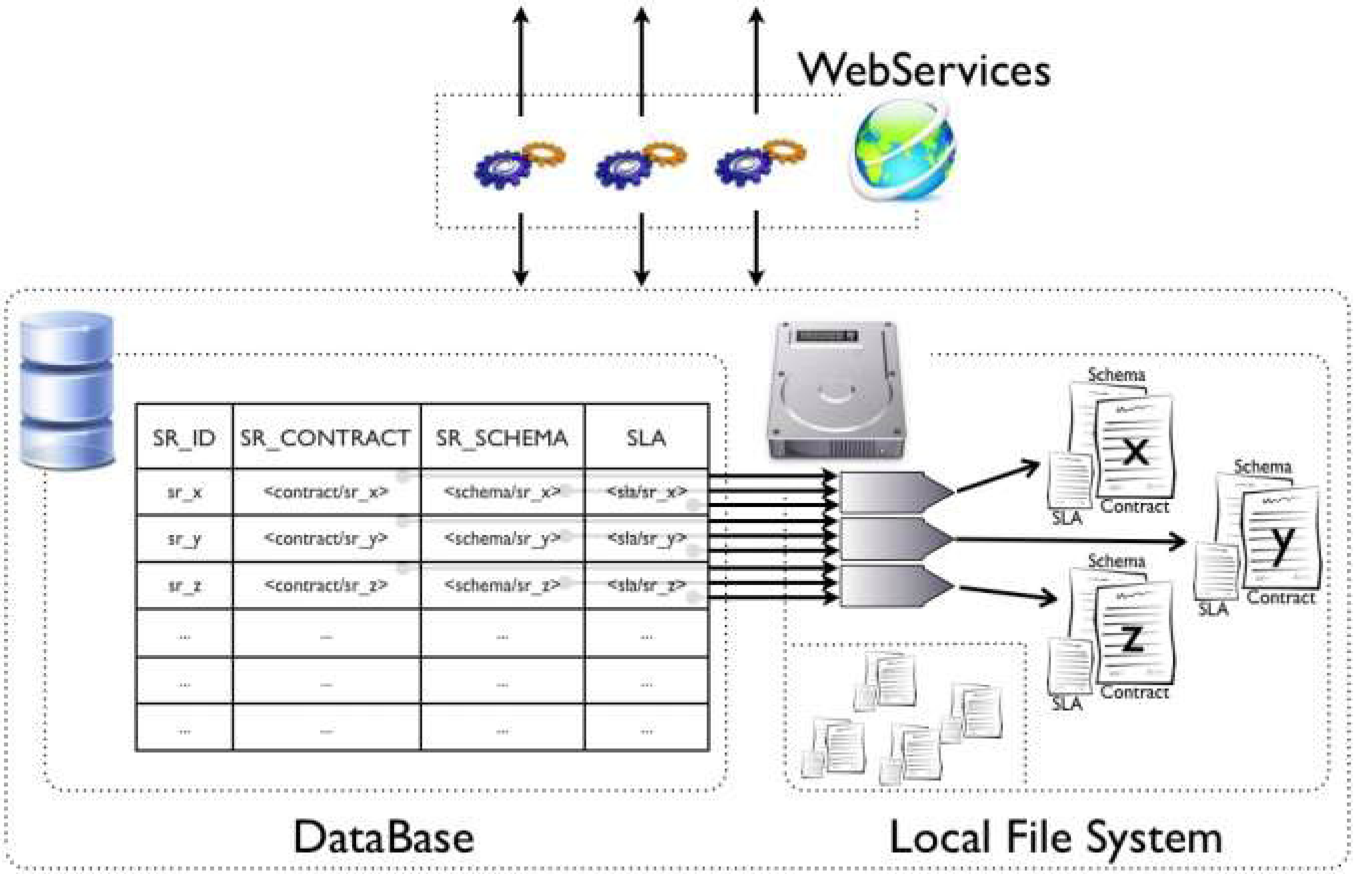
- ❑ Metrics Monitoring (MeMo) approach
  - collects run-time measurements (Drools rule engine)
  - calculates trust metrics (CEP Evaluator – IBM Agilis etc)
  - notifies on SLA violations



Status: Trustworthiness by Adaptation

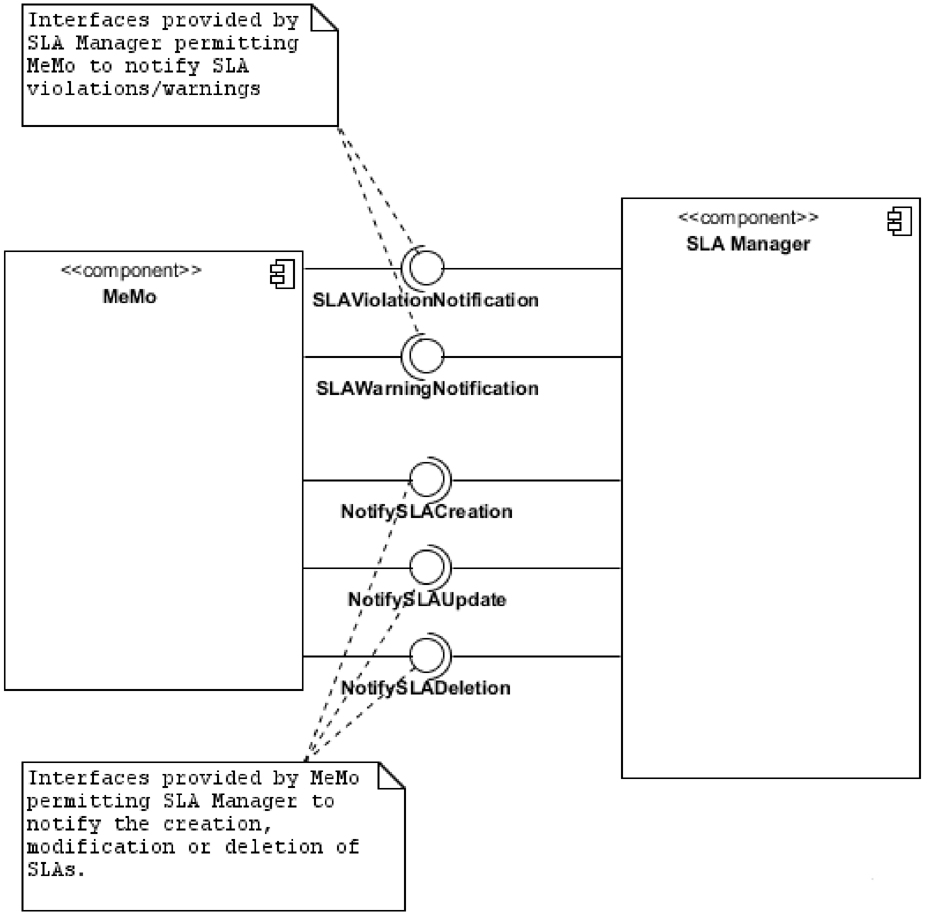
- ❑ Automated Generation of Monitoring Configurations:
  - IoT infrastructures are subject to frequent changes
  - Consistent and coherent model of the system needs to be maintained
  - Forms basis of IT system monitoring and management
- ❑ SLA Manager interacting with MeMo to monitor the degree of compliance with predefined SLAs
- ❑ Interaction with MeMo triggered on FI SLA violations
- ❑ IoT-based monitoring activities of MeMo for detection of SLA violations for reporting & adaptatation to SLA Manager
- ❑ Countermeasure detailing as per penalties stated in the SLA

SLA Generator

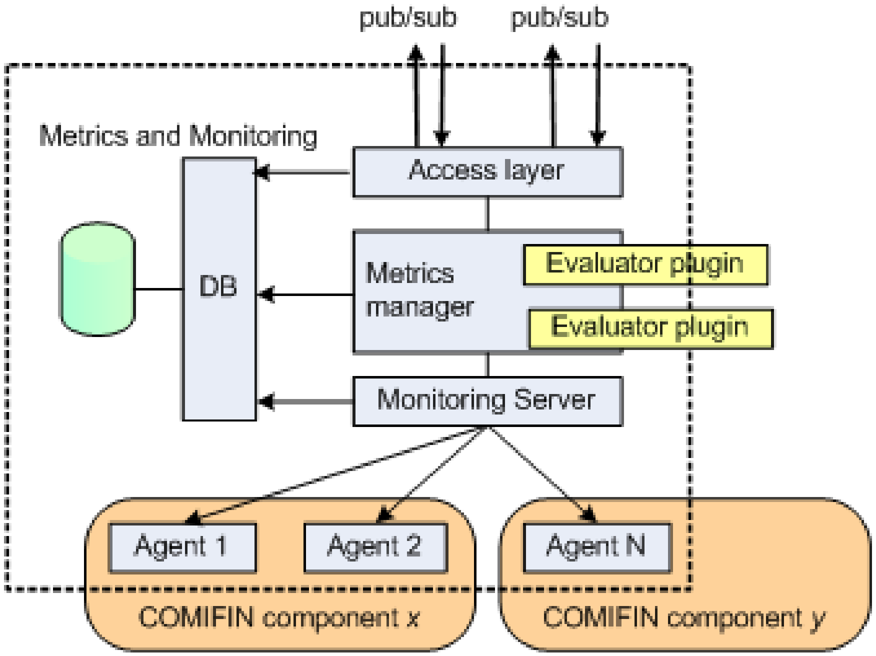


SR_ID	SR_CONTRACT	SR_SCHEMA	SLA
sr_x	<contract/sr_x>	<schema/sr_x>	<sla/sr_x>
sr_y	<contract/sr_y>	<schema/sr_y>	<sla/sr_y>
sr_z	<contract/sr_z>	<schema/sr_z>	<sla/sr_z>
...	...	...	...
...	...	...	...
...	...	...	...

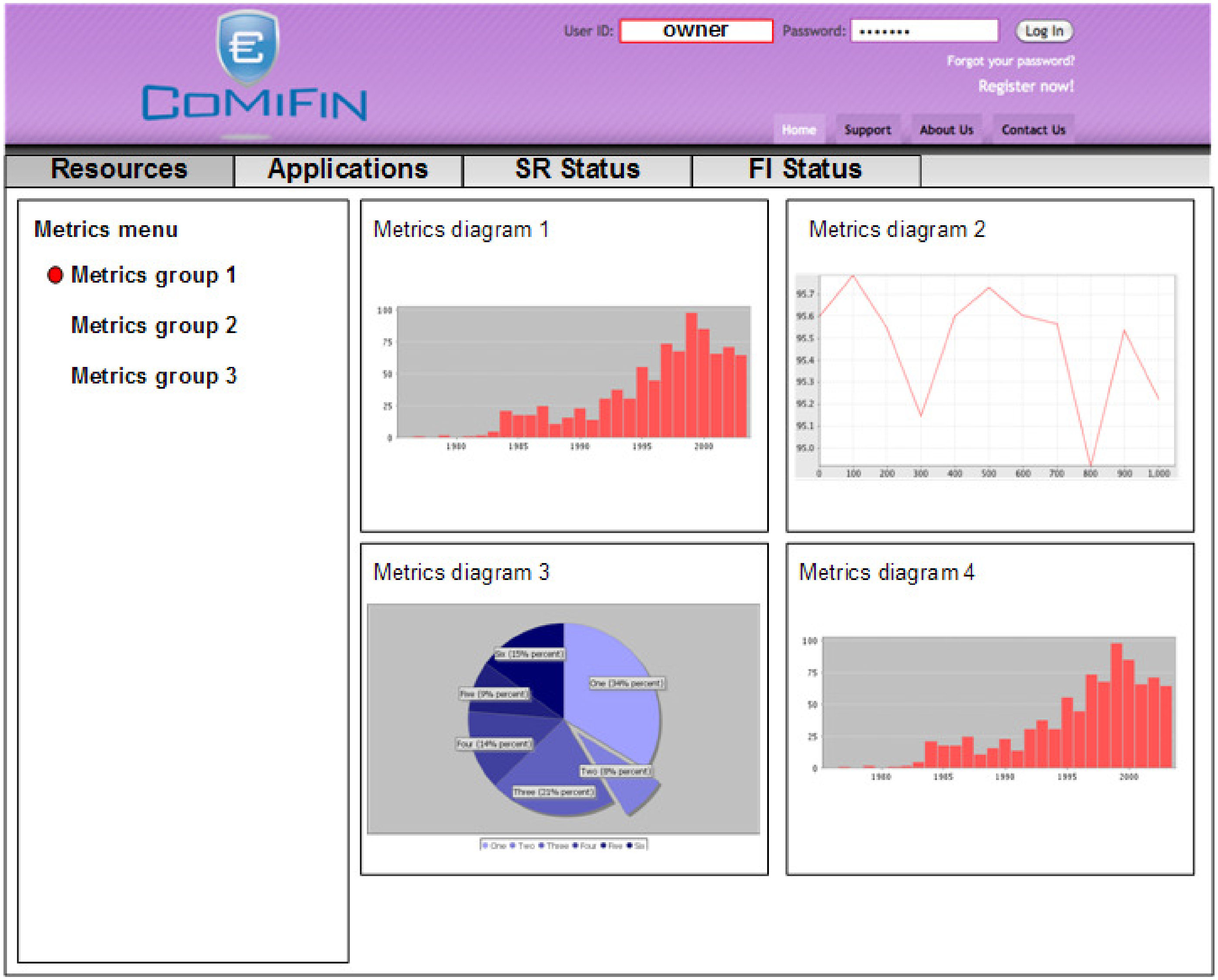
Status: MeMo (SLA Mgr, Evaluator Plug In Rules Engine)


Interfaces provided by SLA Manager permitting MeMo to notify SLA violations/warnings

Interfaces provided by MeMo permitting SLA Manager to notify the creation, modification or deletion of SLAs.



Dashboard Manager



User ID: owner

Password: •••••••

Conclusions and Future Work

- ❑ Status
  - Metric based definition of SLAs (Generalized IoT Model)
  - Semi-automatic generation of monitoring configuration from metrics and SLA definitions
  - Multi-level metric evaluation system to handle complexity
  - MeMo driven SLA Adaptation

- ❑ Future work
  - Formal models of security measurement and Metrics
  - Privacy metrics

- ❑ www.comifin.eu: Communication Middleware For Monitoring Financial Critical Infrastructures