Assessing the Security of Internet Connected Critical Infrastructures (The CoMiFin Project Approach)

UNIK 4750 Spring 2016

Raul Khaydarshin

CoMiFin

- Communication Middleware for Monitoring Financial Critical Infrastructure (FI)
- EU project
- Research area – Critical Infrastructure Protection(CIP) focusing on Critical Financial Infrastructure(CFI)
- Key objective – prove advantages to have cooperative approach in rapid detection of threats
- Demonstrated by addressing problem of protection CFI

Critical Infrastructure

- Infrastructure which disturbance can cause considerable material,financial and in extreme cases human loss

Problem statement

- Evaluate and assess the trustworthiness of **CIP** mechanism deployng sensing nodes and communication overlays(P2P for this case study)
- To quantitatively measure the level of Quality of Protection(QoP) there is demand fo application-dependent **metrics**
- Metrics must be defined for :

design phase | *run-time phase*

Trustworthiness (i.e. dependability and security)
by

Design **Repair**

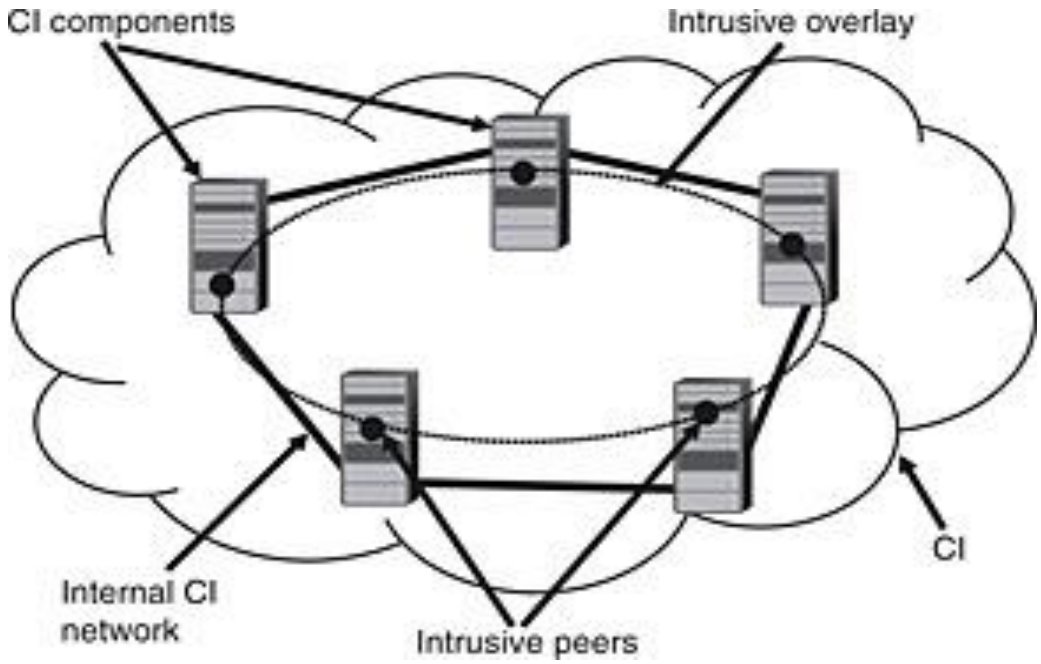
Architecture and System Model

- For IoT based CIP there exist 2 fundamential P2P based protection approaches :

INTRUSIVE vs **NON-INTRUSIVE**

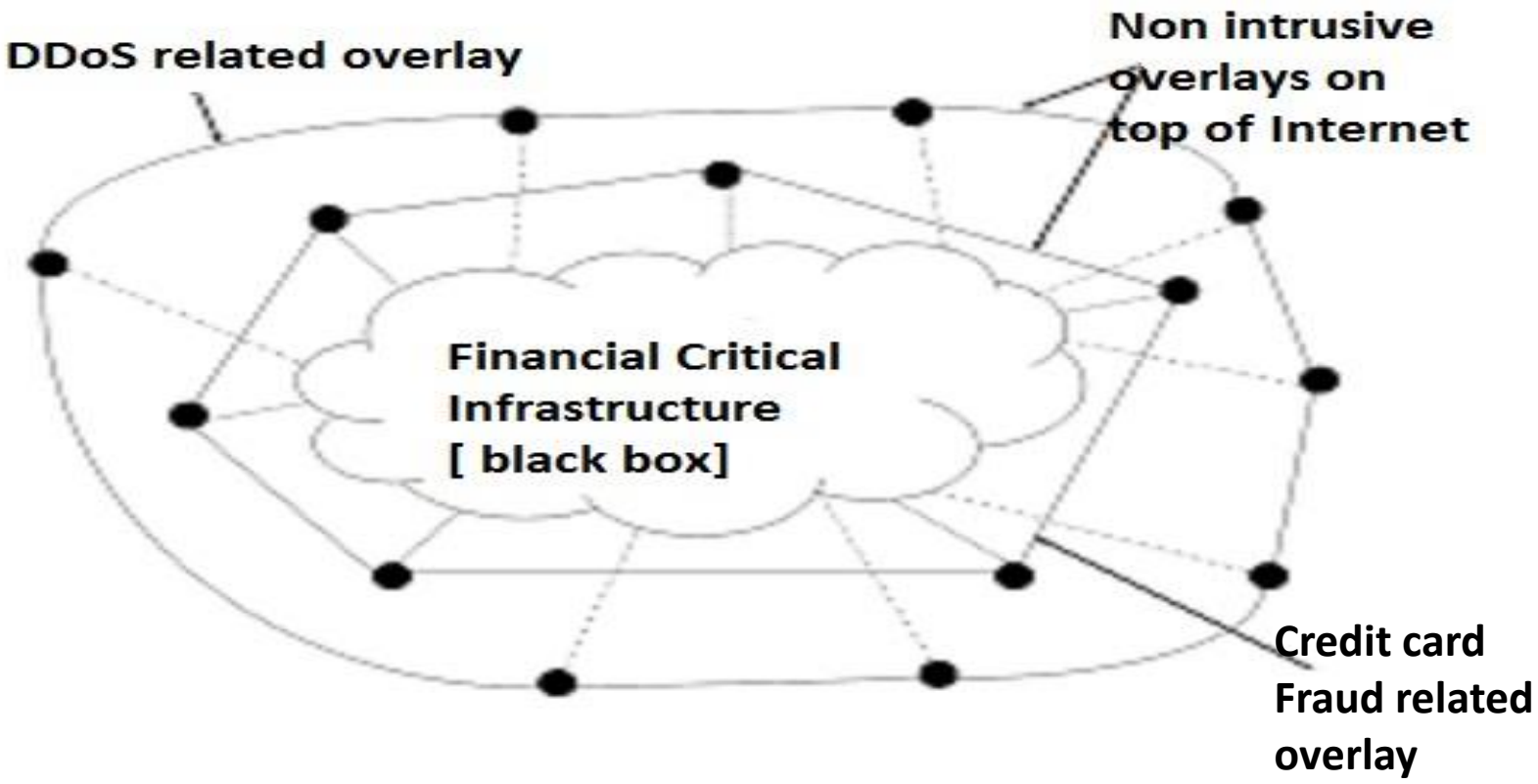
INTRUSIVE APPROACH

- Protection mechanisms are embedded in CI
- For CFI no access to existing CI can be provided



NON-INTRUSIVE APPROACH

- Deploying additional secure/dependable P2P overlay , decoupled from CI
  - meet specific requirements of non-intrusiveness of underlying CI
  - avoid introducing new vulnerabilities



P2P-based Protection of FI

- *Cooperative issue between FI components*

  this is novel approach benefitting from

  advantages of collaborative defense work

  of different independant institutions

  Helps to mitigate DDoS attacs

Disseminate local knowledge of QoP level of FIs.

P2P for FI validation

- Secure Overlay Services (SoS) , aims at preventing DoS attacks through the usage of a secure overlay tunneling[2]
- Web Server protection (WebSoS),utilizes overlay networks in order to allow authenticated users to access web servers even if they are under a congestion-based DDoS attack[3]
- Utilization of P2P architectures for collaborative intrusion and malware detection[4]
- P2P defensive schemes based on novel algorithms for anomaly detection that should be facilitated by cooperation[5,6]
- P2P schemes that are used to disseminate info about malicious IP through some publish/subscribe model[7]
- Emphasizing 2 inherent resilience mechanisms of P2P networks which are path redundancy and data replication[8]

Measuring and controlling IT security through metrics

- Metrics are prerequisite for understanding, improving and validation/sertifying security of CI

- CoMiFin for FI protection used user-centric *GQM – Goal-Question-Metric appoach(widely accepted metrics definition methodology)*

from here following categories of metrics are identified :

- Resource level	CPU usage,memory,disk usage
- Availability	mean uptime,mean repair time
- Communication	strength of applied encryption,ratio encrypted/signed content,transfer time,latency
- Application specific	version ,updates
- Overlay specific	proximity properties ,K-connectivity
- Trust	trust level measurements

Service Level Agreement(SLA)

An SLA is part of the contract between the service provider and its consumers. It describes the provider's commitments and specifies penalties if those commitments are not met. [9]

Metric-based QoP Assessment

Metric-based definition of SLAs

Run-time monitoring

design

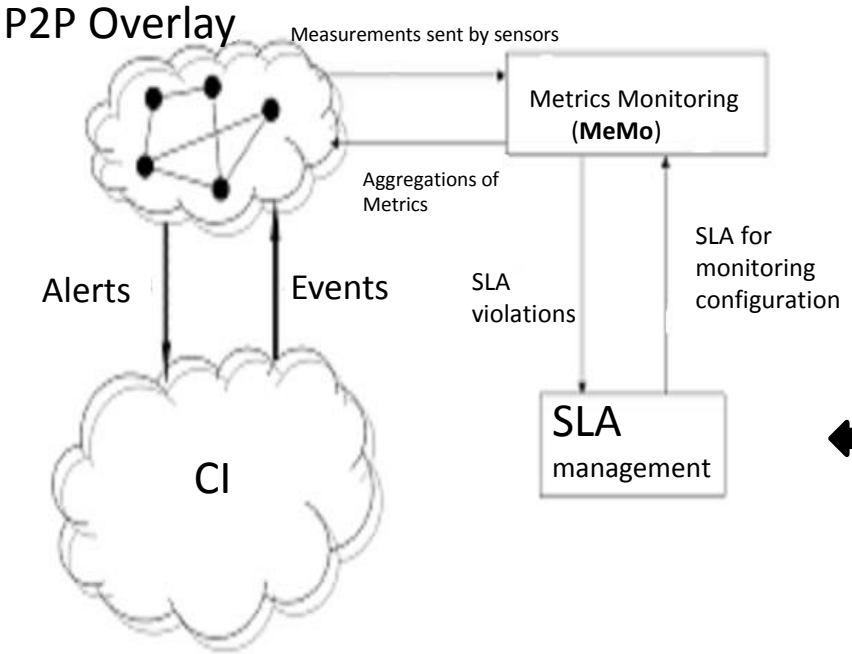
1. Define application dependent security requirements for the overlay
2. Define a set of metrics in order to monitor the fulfillment of the predefined requirements

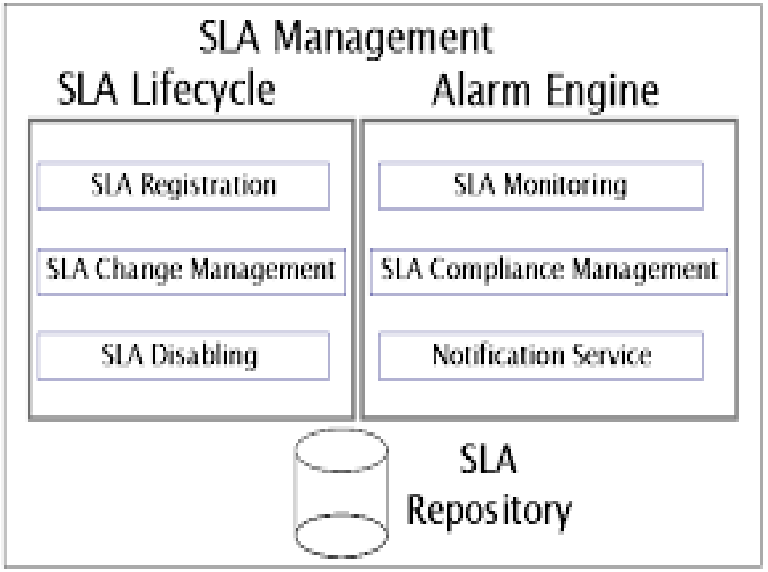
run-time

3. Based on the defined metrics, determine clear and unambiguous SLAs which fulfillment can be monitored at run-time by Metrics Monitoring (MeMo)
4. IoT-based run-time monitoring of the degree of compliance with the defined security related SLAs
5. Any SLA violations can be detected so that appropriate decisions can be taken according to the penalties defined by the SLA

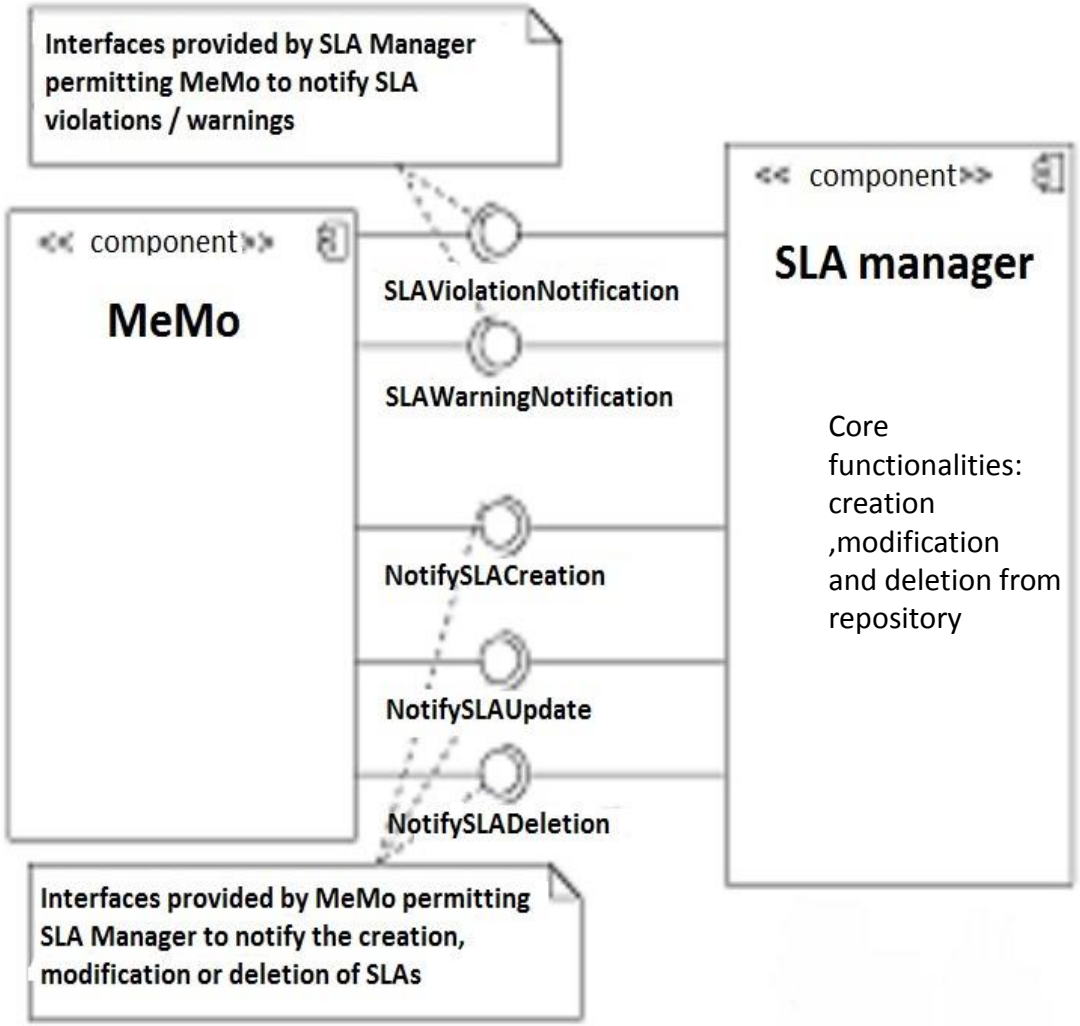
Trustworthiness by Design

- Defining metric-based SLA in order to capture user requiremets
- Defining guarantees system is required to provide
- Penalties in case of not reaching specified guarantees





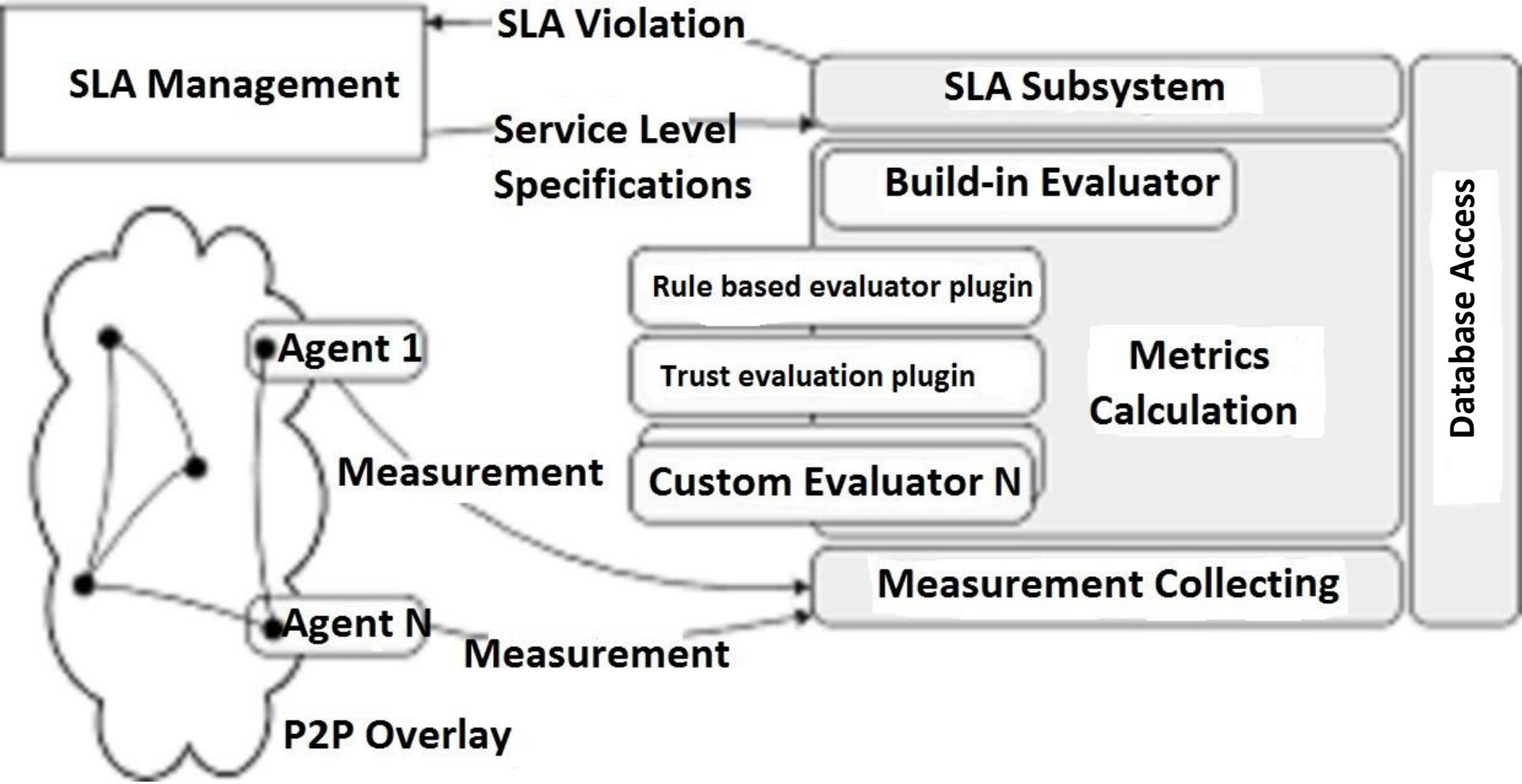
Trustworthiness by Design 2



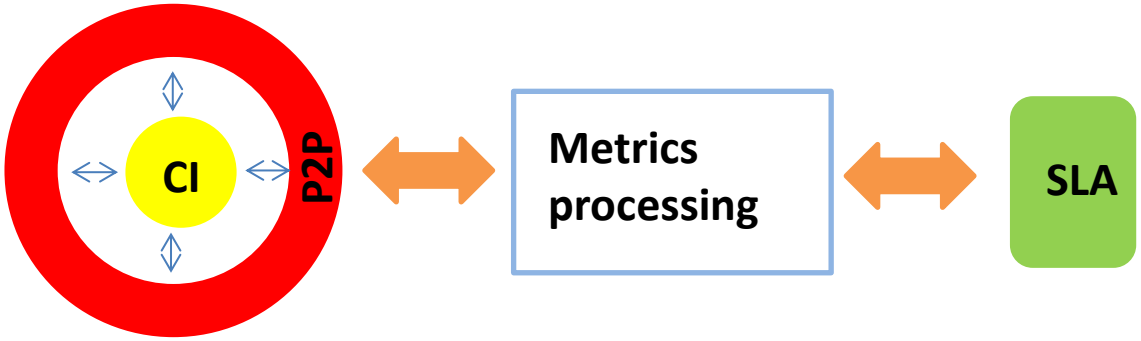
-set of web services assuring interactions with MeMo

Provided *Required by SLA Manager*

Trustworthiness by Repair



Conclusions



- Presentation of metric-based definitions of SLAs
- Generation of the monitoring configuration out of the metrics and SLA definitions
- Multi-level metric evaluation system to handle complexity (plug-in concept)

-Quality of robustness and protection mechanisms of P2P layer should be also measured and validated agains SLAs

-Future work needs to be done(privacy protection ,) …

-Open for critic / room for error …

REFERENCES

[1] Assesing the Security of Internet Connected Critical Infrastructures(The CoMiFin Project Approach). Hamza Chani,Abdelmajid Khelil,Neeraj Suri,György Csertan,Laszlo Gönczy, Gabor Urbanics, James Clarke.Tehchnishe Universität Darmstadt,Germany.2014.

[2] A. Keromytis et al. SoS: An architecture for mitigating ddos attacks.IEEE Journal on Selected Areas of Commn., Vol. 22, 176-188,2004.

[3] D. Cook et al. WebSoS: protecting web servers from ddos attacks. InProc. of ICON'03, pp. 461-466, 2003

[4] M. Marchetti et al. P2P architecture for collaborative intrusion and malware detection on a large scale. In Proc. Intl. Conf. on InformationSecurity, pp. 475-490, 2009.

[5] D. J. Malan and M. D. Smith. Host-based detection of worms through peer-to-peer cooperation. In Proc. of WORM'05, pp. 72-80, 2005.

[6] C. Dumitrescu. A peer-to-peer approach for intrusion detection. in Proc. of CCGRID'06, vol. 1, pp. 89-92, 2006.

[7] R. Janakiraman et al. Indra: a peer-to-peer approach to network intrusion detection and prevention. In Proc. WET ICE'03, pp. 226–231, 2003.

[8] D. Germanus et al. Increasing the resilience of critical scada systems using peer-to-peer overlays. In Intl. Symposium on Architecting Critical Systems, LNCS 6150, pp. 161-178, 2010.

[9] Avraham Leff,James T. Rayfield,and Daniel M. Dias Grid Computing.IBM T.J.Watson Research Cente IEEE Computer Society ,2003.