Information Sharing for the Financial IT Infrastructure: the case of collaborative security

Roberto Baldoni

Università degli Studi di Roma “La Sapienza”

baldoni@dis.uniroma1.it, http://www.dis.uniroma1.it/~baldoni/

SDCI 2012 Winter School

17/01/2012

Focus and structure of the talk

- Financial Critical Infrastructure
- Massive event processing: sense and respond applications
- Agilis: An Internet-Scale Distributed Event Processing System for Collaborative Detection of Cyber Attacks
  - Collaborative Detection of scanners
- Collaborative detection of coordinated portscanning
- Event processing for Correlating Frauds
- Handling privacy

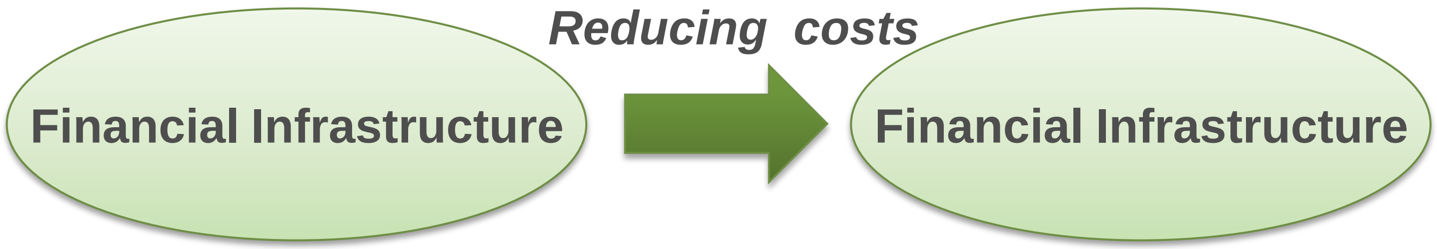
Financial Critical Infrastructure

Critical Information Infrastructure Protection

Critical Financial Infrastructure

off-the-shelf hardware

IP convergence



Reducing costs

Financial Infrastructure

Financial Infrastructure

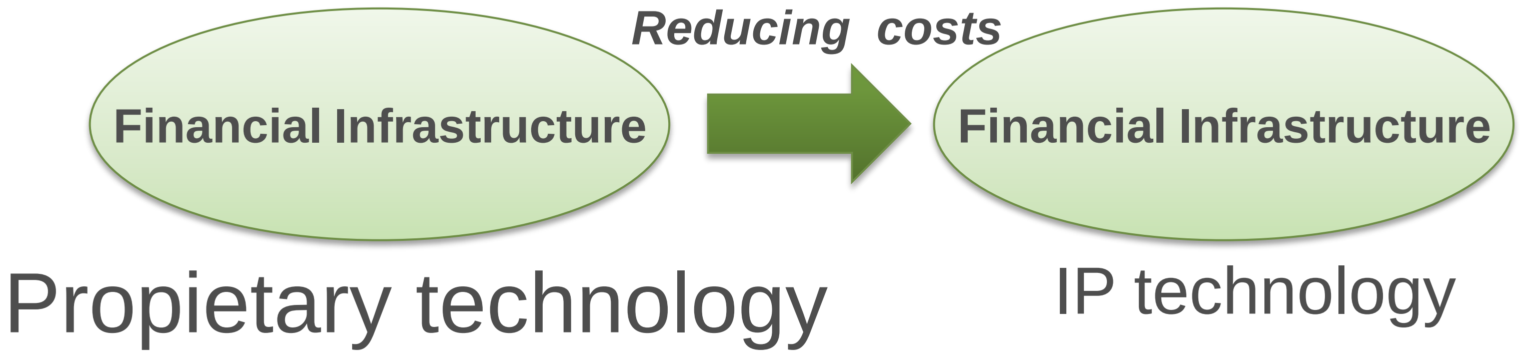
Propietary technology

IP technology

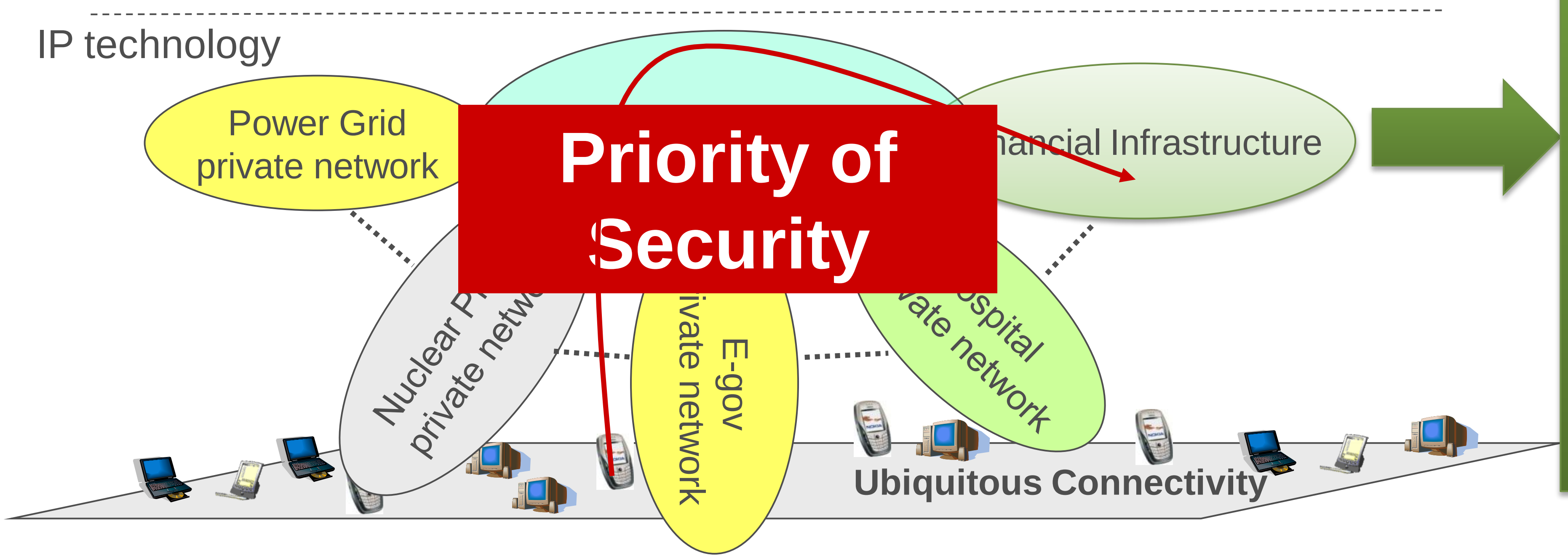
Critical Financial Infrastructure

off-the-shelf hardware

IP convergence



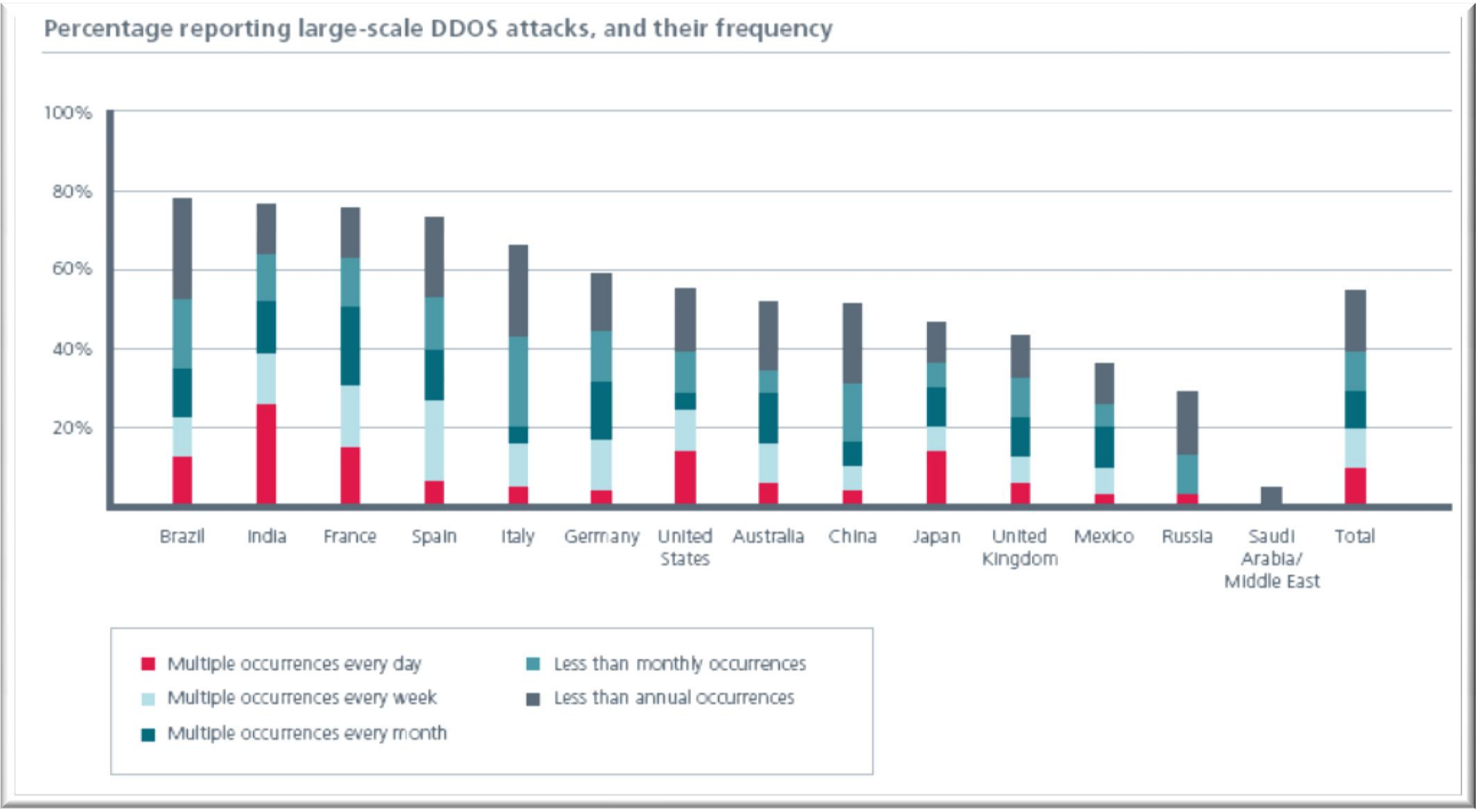
Growing intersection with the Internet



- ❑ Webification of critical financial services
- ❑ Cross domain interactions
- ❑ Heterogeneous data and systems

Critical Financial Infrastructure: DDoS

- render internet-based financial services unreachable from legitimate users.
- Use of Botnet
- Three examples of DDOS campaign in Cyberwarfare:
  - Estonia 2007
  - Georgia 2008
  - Iran. Stuxnet wo

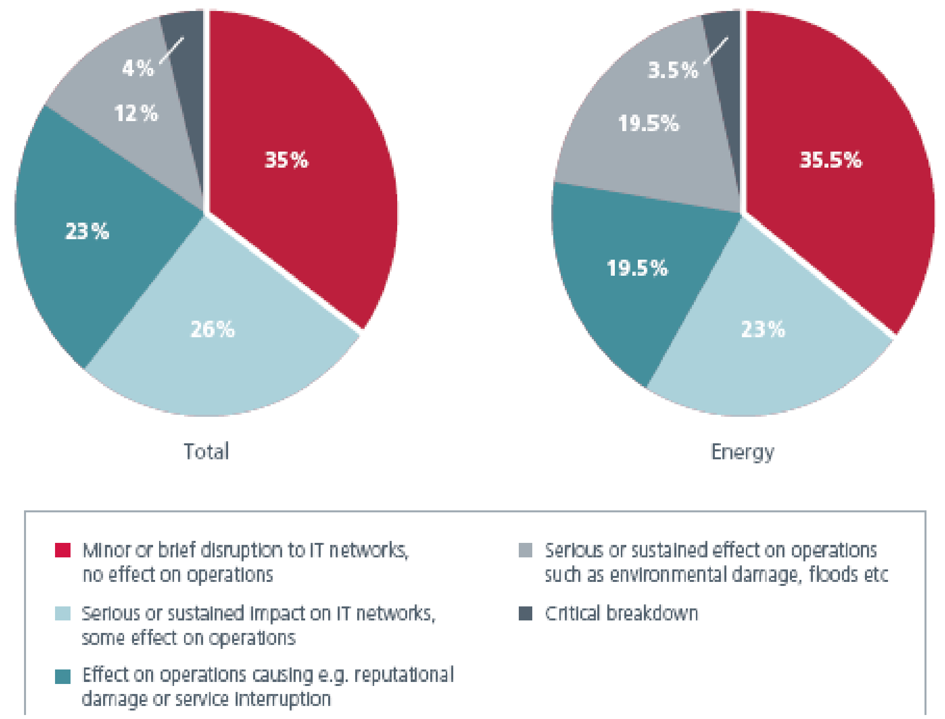


Percentage reporting large-scale DDOS attacks, and their frequency

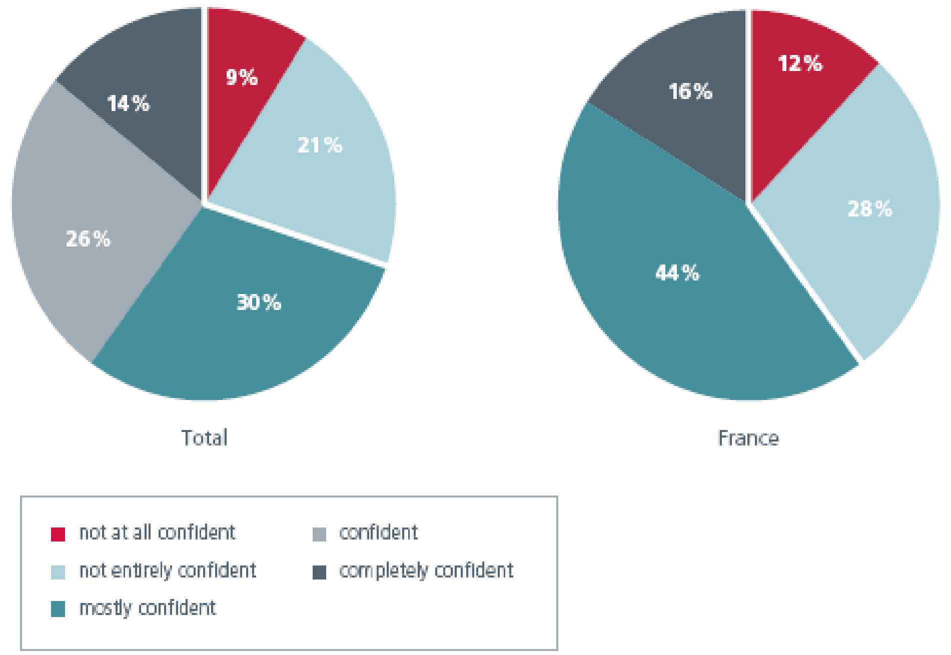
Critical Financial Infrastructure: DDoS

- cost of downtime from major attacks exceeds U.S. $6 million per day
- damage to reputation
- loss of personal information about customers
- One out of five DDos attacks is accompanied with an extorsion

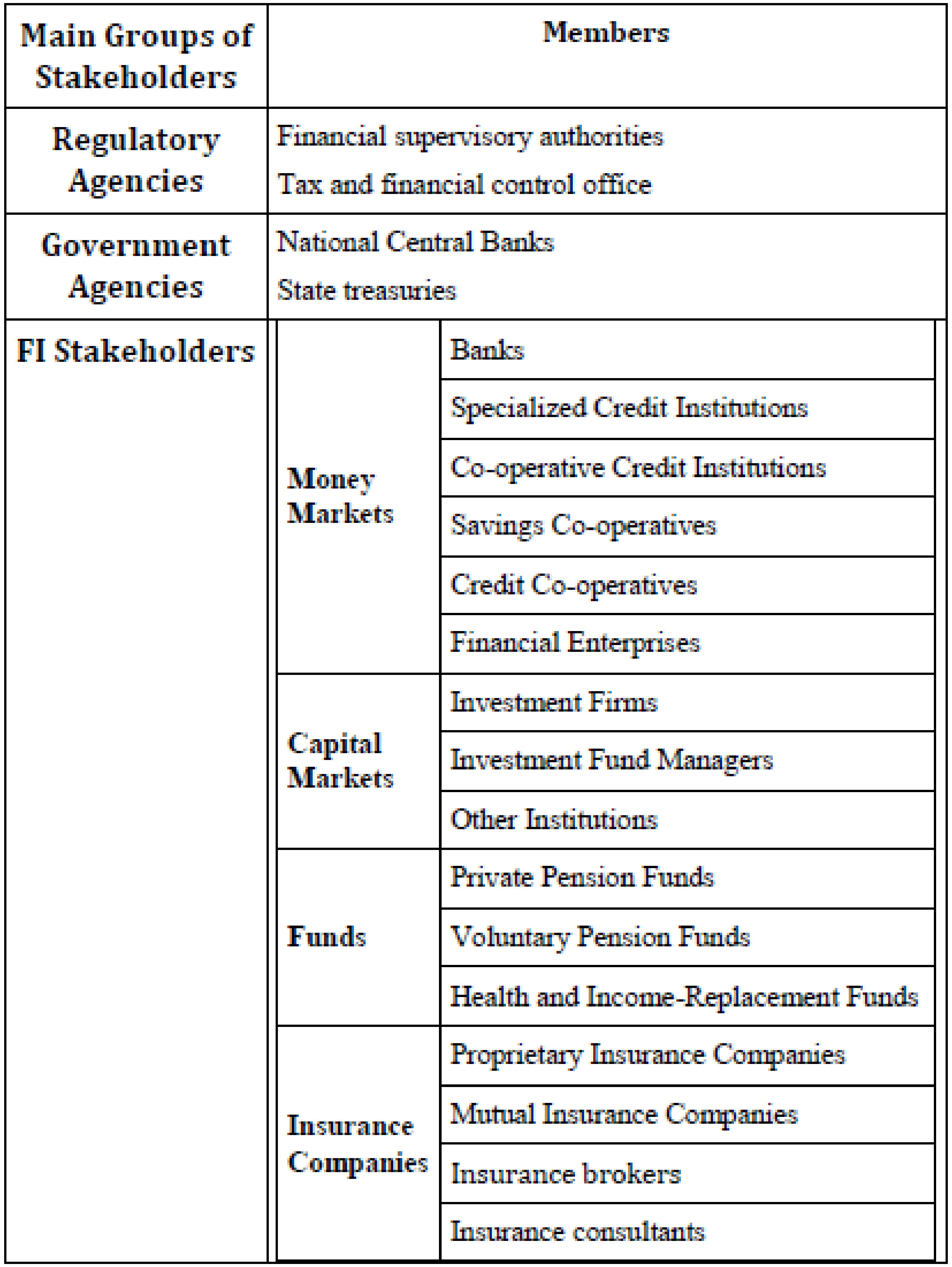
Impact of large-scale DDOS attacks



Confidence that banking and financial services could withstand a major cyberattack



McAfee report 2010 “in the crossfire: critical infrastructures in the age of cyber war “



Main Groups of Stakeholders	Members	
Regulatory Agencies	Financial supervisory authorities Tax and financial control office	
Government Agencies	National Central Banks State treasuries	
FI Stakeholders	Money Markets	Banks
		Specialized Credit Institutions
		Co-operative Credit Institutions
		Savings Co-operatives
		Credit Co-operatives
		Financial Enterprises
	Capital Markets	Investment Firms
		Investment Fund Managers
		Other Institutions
	Funds	Private Pension Funds
		Voluntary Pension Funds
		Health and Income-Replacement Funds
	Insurance Companies	Proprietary Insurance Companies
		Mutual Insurance Companies
		Insurance brokers
		Insurance consultants

Fig. 1.2: Main Stakeholders of the Financial Industry

Attacks targeted to financial institutions [7] are typically performed in order to

- gain unauthorized access to sensitive or confidential information
- disrupt normal business
- create costly distractions
- steal funds
- reduce confidence

Potential damage and possible consequences that may occur when systems supporting critical financial operations

- services and benefits interruption
- sensitive data disclosure
- data integrity corruption
- money and information theft
- commercial structures and financial systems bankruptcy
- international business transactions failure
- markets destabilization
- unauthorized access and/or modification of personal information
- confidence and reputation loss

Standard Solutions for Securing the Financial Infrastructure

- The relevance of security requirements in the financial context is highlighted by the Basel II accord.

- Damages caused by security breaches within the financial IT infrastructure fall within the operational risk category

- Financial institutions and their customers can voluntarily comply with widely recognized international certifications, such as the Payment Card Industry Data Security Standard (PCIDSS) .

IT Dependability and security requirements

Availability: the capacity to access systems, networks and critical data for the infrastructure survival anytime even if the infrastructure is operating under extreme conditions

Reliability: the capacity to ensure that a system or network will perform its intended functions without failures when operated under specific conditions for a specified time interval

Authentication: identify a user that is appropriate to the specific information and service type

Access control: only authorized users can access system and network resources

Data and message confidentiality: only authorized users can access protected data and messages

Data and message integrity: data managed by systems and messages transmitted over the network are not altered by unauthorized users or non guaranteed software or hardware

Reliable message delivery: avoid message loss and replication, and guarantee ordered delivery, along with the ability to provide verifiable proof of delivery to both the endpoints of a communication

Non repudiation: provide verifiable proof of message delivery to both the endpoints of a communication, in order to ensure that the sender of a message can not deny having sent the message and that the recipient can not deny having received the message

Securing Transactions: SWIFT

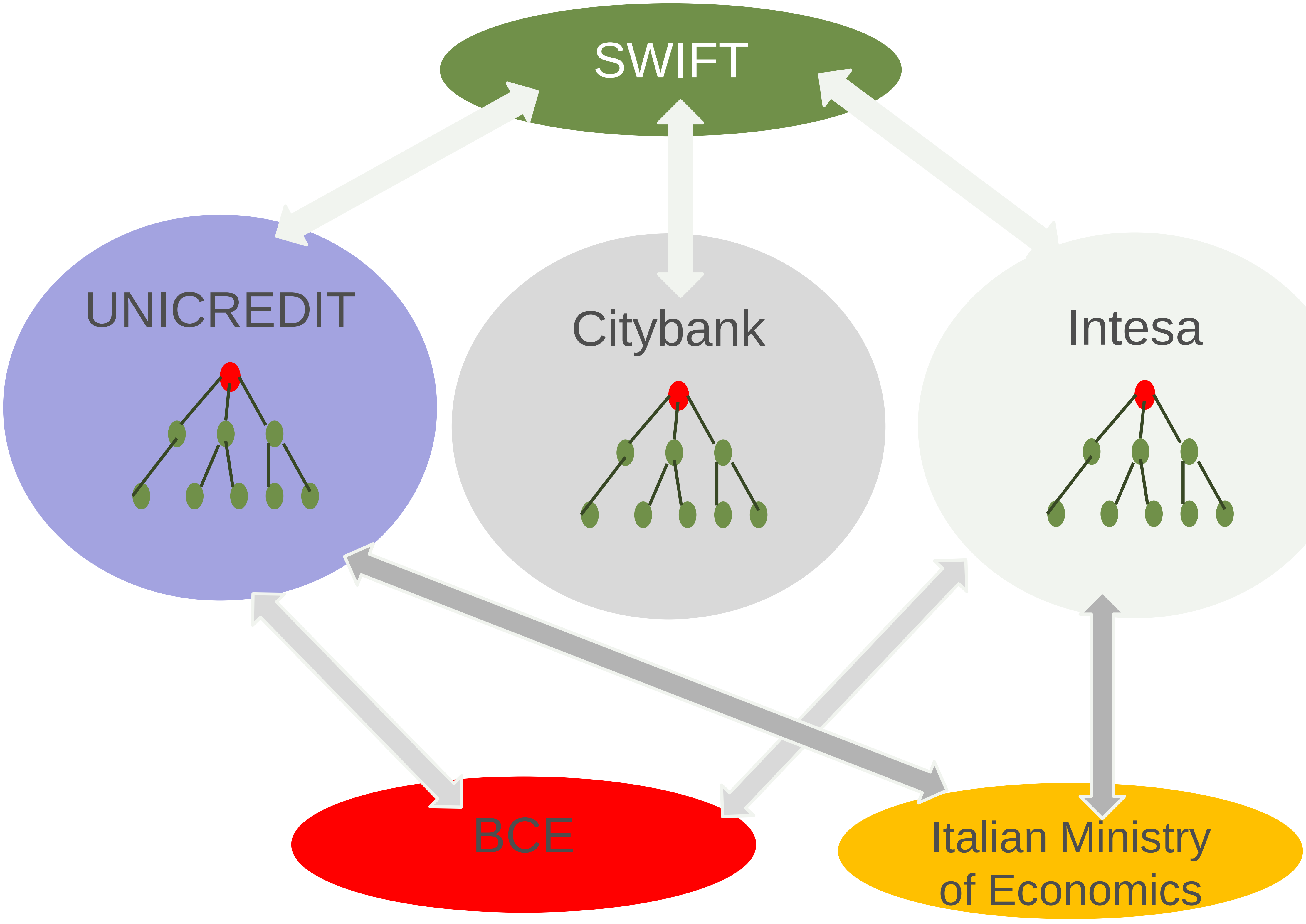
SWIFT (Society forWorldwide Interbank Financial Telecommunication) is the most important worldwide financial communication infrastructure, founded in 1973 that enables the exchange of messages between banks and other financial institutions.

SWIFT is a private network (SWIFTNet) which provides the platform, products and services to connect and exchange financial information among financial organizations spread all over the world.

SWIFT is responsible for providing a fast, secure, available and accurate means of transferring a variety of financial transactions.

SWIFT provides a centralized store-and-forward mechanism including the transaction management.

Current financial Infrastructure Topology



Collaborative Cyber Security in Financial Ecosystem

- A payment card fraud (2008)

- 100 compromised payment cards used by a network of coordinated attackers retrieving cash from 130 different ATMs in 49 countries worldwide, totaling 9 million of US dollars.

- High degree of coordination, half an hour to be executed

- evade all the local monitoring techniques used for detecting anomalies in payment card usage patterns.

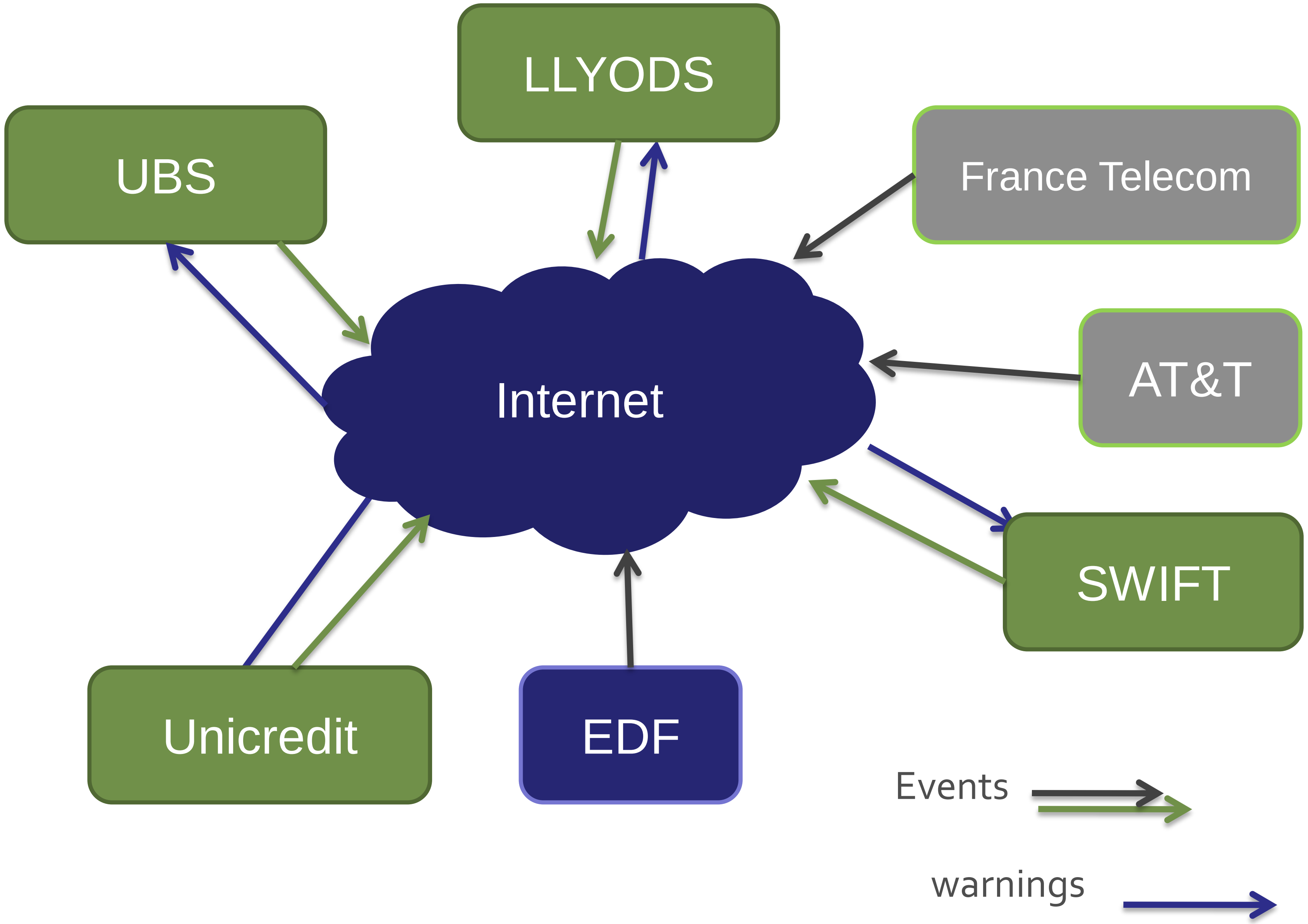
- The fraud has been detected only later, after aggregating all the information gathered locally by each financial institution involved in the payment card scam

Collaborative Cyber Security in Financial Ecosystem

- Distributed Denial Of Service Attack (2007, Northern Europe)
- render web-based financial services unreachable from legitimate users.
- DDoS attack targeted a credit card company and two DNS.
- Internet restored only after several trial-and-error activities carried out manually by network administrators of the attacked systems and of their Internet Service Providers (ISPs).
- Long preparation time (days), short attack time (seconds)

Barriers to Collaboration

- **Understanding the economics**
- **Trust and privacy issues**
- **Legal Issues**



Information Sharing

- Previous century has been characterized by a legislation framework centered on privacy

- The term "information sharing" gained popularity as a result of the 9/11 Commission Hearings. President Bush mandated agencies to implement policies to "share information" across organizational boundaries. Homeland Security Presidential Directive 7 (2003)

- The federal government asked to establish sector specific information sharing organizations to share information, within each sector, about threats and vulnerabilities to that sector for damage mitigation and quick reaction

- Information Sharing and Analysis Centers (ISACs)

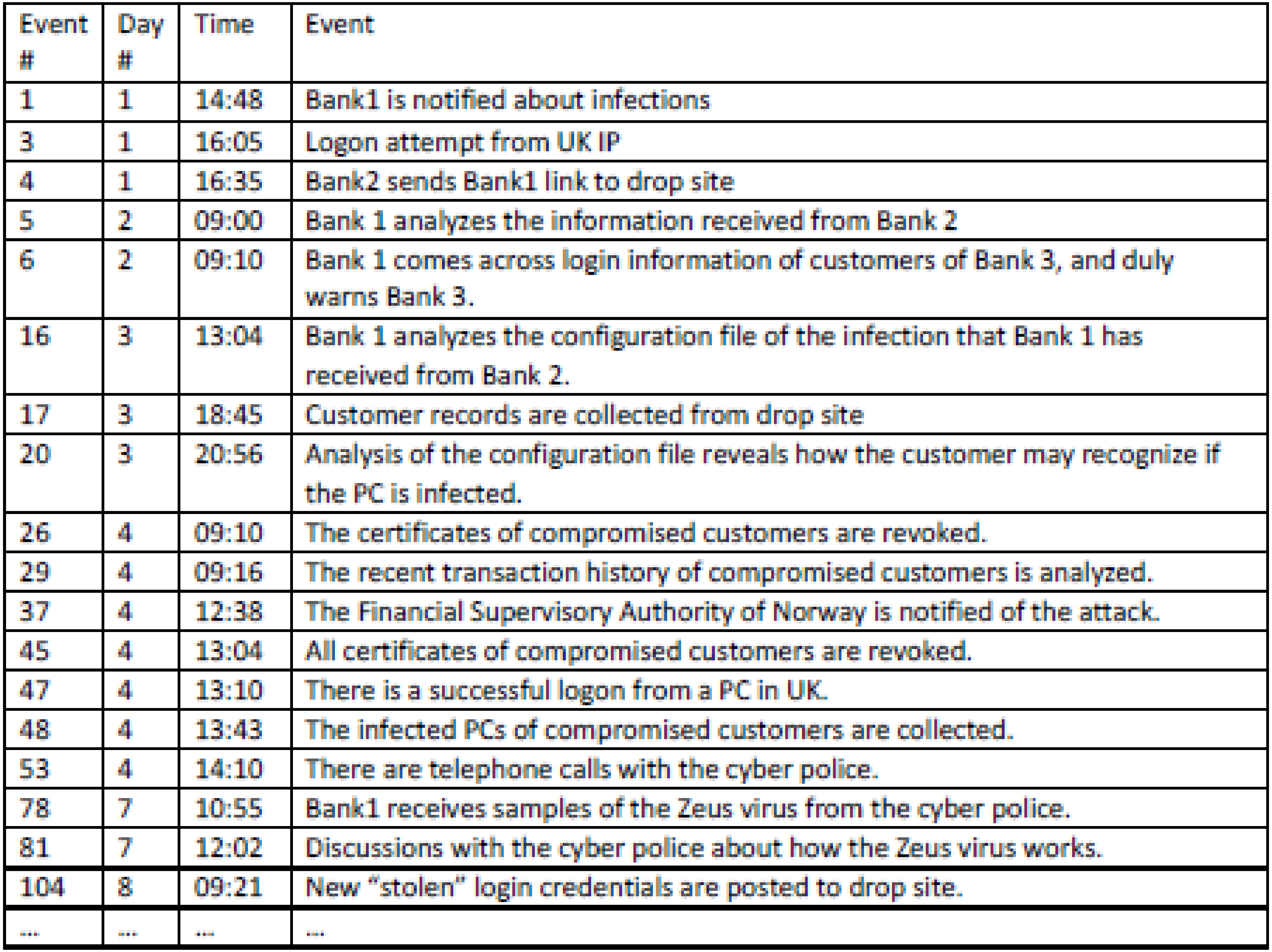
- Financial Service Information Sharing FS/ISAC

ISAC

An ISAC is a trusted, sector specific entity which performs the following functions:

- provides to its constituency a 24/7 secure operating capability that establishes specific information sharing/intelligence requirements for incidents, threats and vulnerabilities
- collects, analyzes, and disseminates alerts and incident reports to it membership based on its sector focused subject matter analytical expertise
- helps the government understand impacts for its sector
- provides an electronic, trusted capability for its membership to exchange and share information on cyber, physical and all threats in order to defend the critical infrastructure
- shares and provides analytical support to government and other ISACs regarding technical sector details and in mutual
- information sharing and assistance during actual or potential sector disruptions whether caused by intentional, accidental or natural events

Anatomy of an incident: Value n. 1 of Information Sharing



Event #	Day #	Time	Event
1	1	14:48	Bank1 is notified about infections
3	1	16:05	Logon attempt from UK IP
4	1	16:35	Bank2 sends Bank1 link to drop site
5	2	09:00	Bank 1 analyzes the information received from Bank 2
6	2	09:10	Bank 1 comes across login information of customers of Bank 3, and duly warns Bank 3.
16	3	13:04	Bank 1 analyzes the configuration file of the infection that Bank 1 has received from Bank 2.
17	3	18:45	Customer records are collected from drop site
20	3	20:56	Analysis of the configuration file reveals how the customer may recognize if the PC is infected.
26	4	09:10	The certificates of compromised customers are revoked.
29	4	09:16	The recent transaction history of compromised customers is analyzed.
37	4	12:38	The Financial Supervisory Authority of Norway is notified of the attack.
45	4	13:04	All certificates of compromised customers are revoked.
47	4	13:10	There is a successful logon from a PC in UK.
48	4	13:43	The infected PCs of compromised customers are collected.
53	4	14:10	There are telephone calls with the cyber police.
78	7	10:55	Bank1 receives samples of the Zeus virus from the cyber police.
81	7	12:02	Discussions with the cyber police about how the Zeus virus works.
104	8	09:21	New "stolen" login credentials are posted to drop site.
...	...	...	...

Value of Information Sharing

- Value n.2: Knowledge dissemination
- Value n.3: Increase likelihood of discovery
- Value n.4: Illicit transactions that span banks
- Value n.5: Shared platform for systems development
- Value n.6: Economies of scale
- Value n.7: Aggregate threat picture
- Value n.8: Uniform reporting

Information Sharing

- Information sharing is a behavior and not only a technology. It includes:
  - Cultural: the “will” to share and to collaborate
  - Governance: the importance define instruments for information sharing
  - Policy: the importance to define rules for sharing
  - Economic: understanding the value of sharing

- Technologically speaking we can do now things that 5 years ago were not achievable

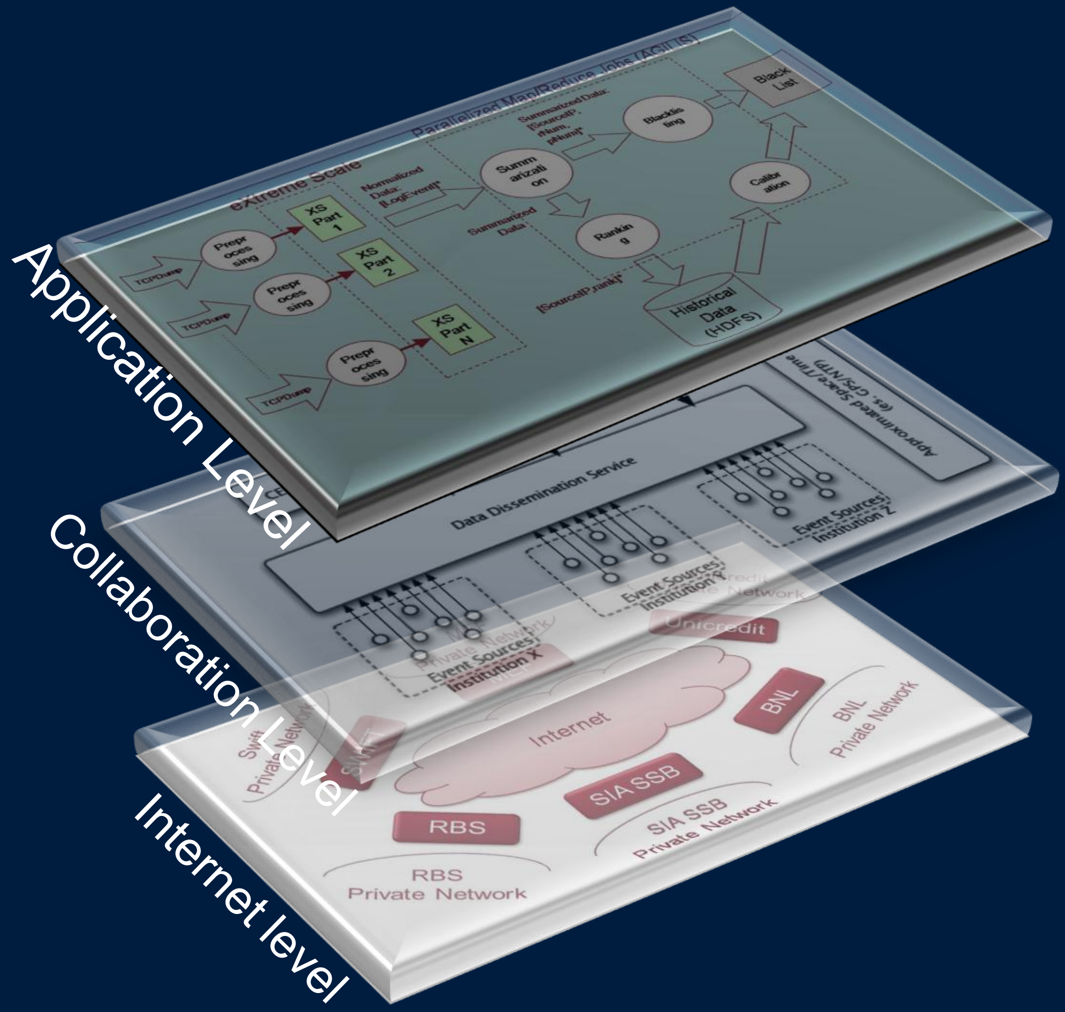
Roberto Baldoni
Gregory Chockler
Editors

Collaborative Financial Infrastructure Protection

Tools, Abstractions, and Middleware

Springer

Collaborative sense and response applications



Sense-and-Response applications: Massive event processing

- **Monitoring**
- **Continuous Control**
- **Command and Control**
- **Mashup services**
- **Business intelligence**

#haiti #need -RT

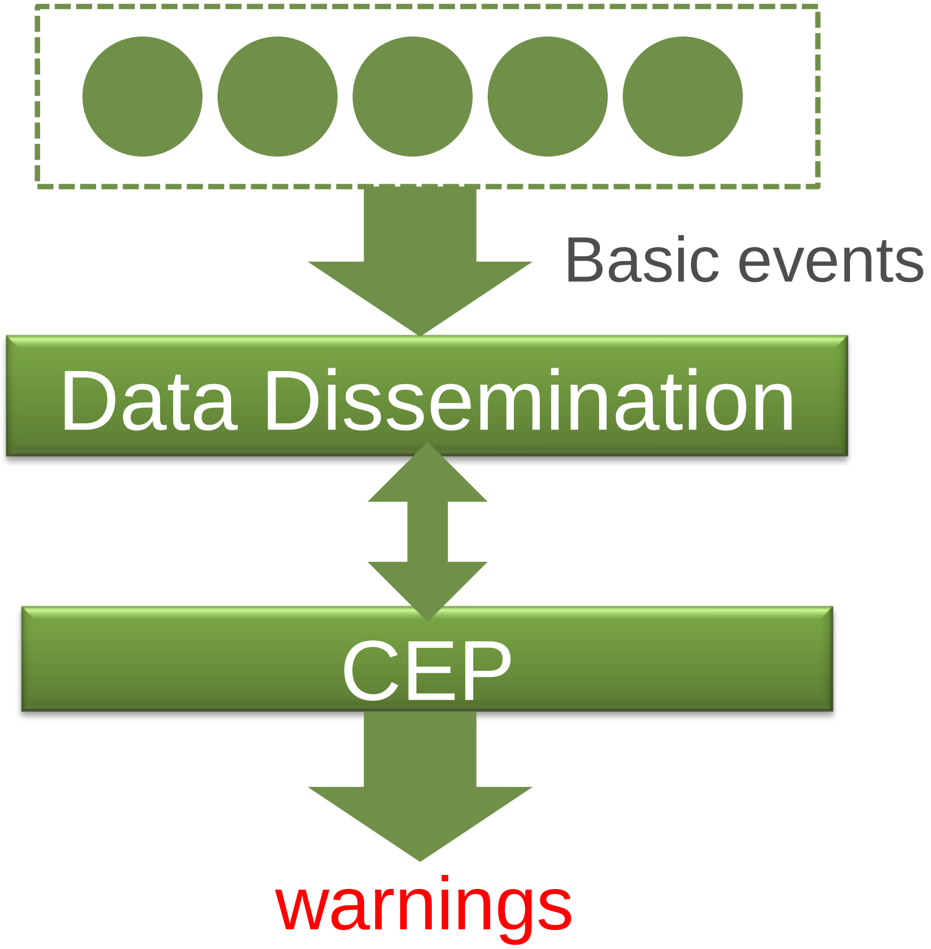
TWEET	START CASE
#haiti #need food water med shelter #loc Delmas 33 and nazon	start a case
#haiti #need food,H20, Help #loc Mariani #4	start a case
#haiti #need food water #loc Croix des Bouquets	start a case
#haiti #need tents, blankets, water, food meds for infection milk for babies, children #loc Butte Boyer 54	start a case
#haiti #need dead body removal #loc Carrefour 54	start a case
#haiti #need food,h20,tents,airbeds #loc Tom Gato, Fondwa, Route de Jacmel, Léogâne #contact **sourceofhopeministries@yahoo.com** (509)3648-3084	start a case
#haiti #need food water x2 reps #loc 18.449035,-72.681487 L'Acul village area of Leogane #date Jan 30 2010 18:01 #src	start a case

#haiti #have -RT

TWEET	START CASE
check out #need #have #haiti (in Drupal) **http://dev.haiti-earthquake-information.org /en/need-have-offer**	start a case
#haiti #need flight #have food for #loc Jacmel from #loc Miami	start a case
# #haiti use 1 main hashtag per twt: #imok, #ruok, #need, #offer or #have, #open [road, store or other], #close [road, store or other]	start a case
#haiti use 1 main hashtag per twt: #imok, #ruok, #need, #offer or #have, #open [road, store or other], #close [road, store or other]	start a case
#haiti use 1 main hashtag per twt: #imok, #ruok, #need, #offer or #have, #open [road, store or other], #close [road, store or other]	start a case
# #haiti use 1 main hashtag per twt: #imok, #ruok, #need, #offer or #have, #open [road, store or other], #close [road, store or other]	start a case
#haiti use 1 main hashtag per twt: #imok, #ruok, #need, #offer or #have, #open [road, store or other], #close [road, store or other]	start a case

Structure of a sense-respond application

- Sensors
- Event Notification
- Complex Event Processing



- Application level Correctness factors
  - Accuracy (no false warning)
  - Completeness (no detection of actual warning)
  - Timeliness (no late warning)

Collaborative sense-and response applications

- Some warning cannot be detected only correlating local information
- Events coming from different organizations over distinct administration boundaries;
- Sharing information potentially improves correctness factors:
  - Improved accuracy
  - Improved completeness
  - Better timeliness
- Additional problems (real)
  - Data privacy
  - Data retention

Examples of Collaborative sense-and-respond applications

- Collecting Network Anomalies [Huang et al, SIGMETRICS 2007]

- *known, documented network disruptions are reflected in the BGP routing data* within that network

- network-wide analysis can expose classes of network disruptions that are not detectable with existing techniques

- correlating different routing streams in real-time to localize network disruptions

Examples of Collaborative sense-and-respond applications

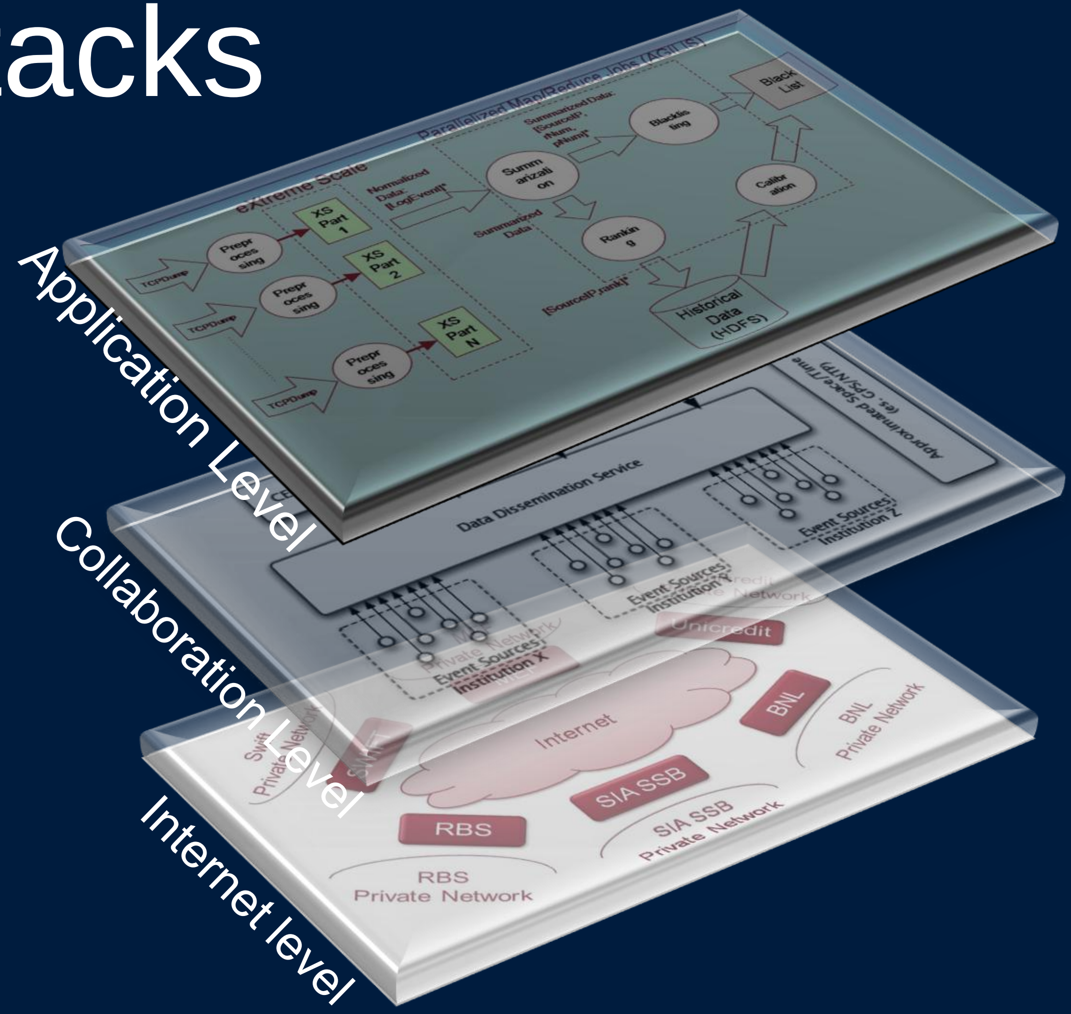
- Smart Mobility
- Project involving Sapienza Univ. of Rome, Microsoft, Municipality of Rome

- live google map (continuous queries)
- Events injected by traffic operators (local media, local transportation companies), traffic, citizens etc.
- Target: reducing the time to destination by assisting the person during the trip

- Platform based on MS Azure to optimize workload changes

Agilis: An Internet-Scale Distributed Event Processing System for Collaborative Detection of Cyber Attacks

IBM and Sapienza



Collaborative Cyber Security: CoMiFin Platform

- CoMiFin offers to FIs a platform for gaining the benefits of community-based collaboration over a “business social network”

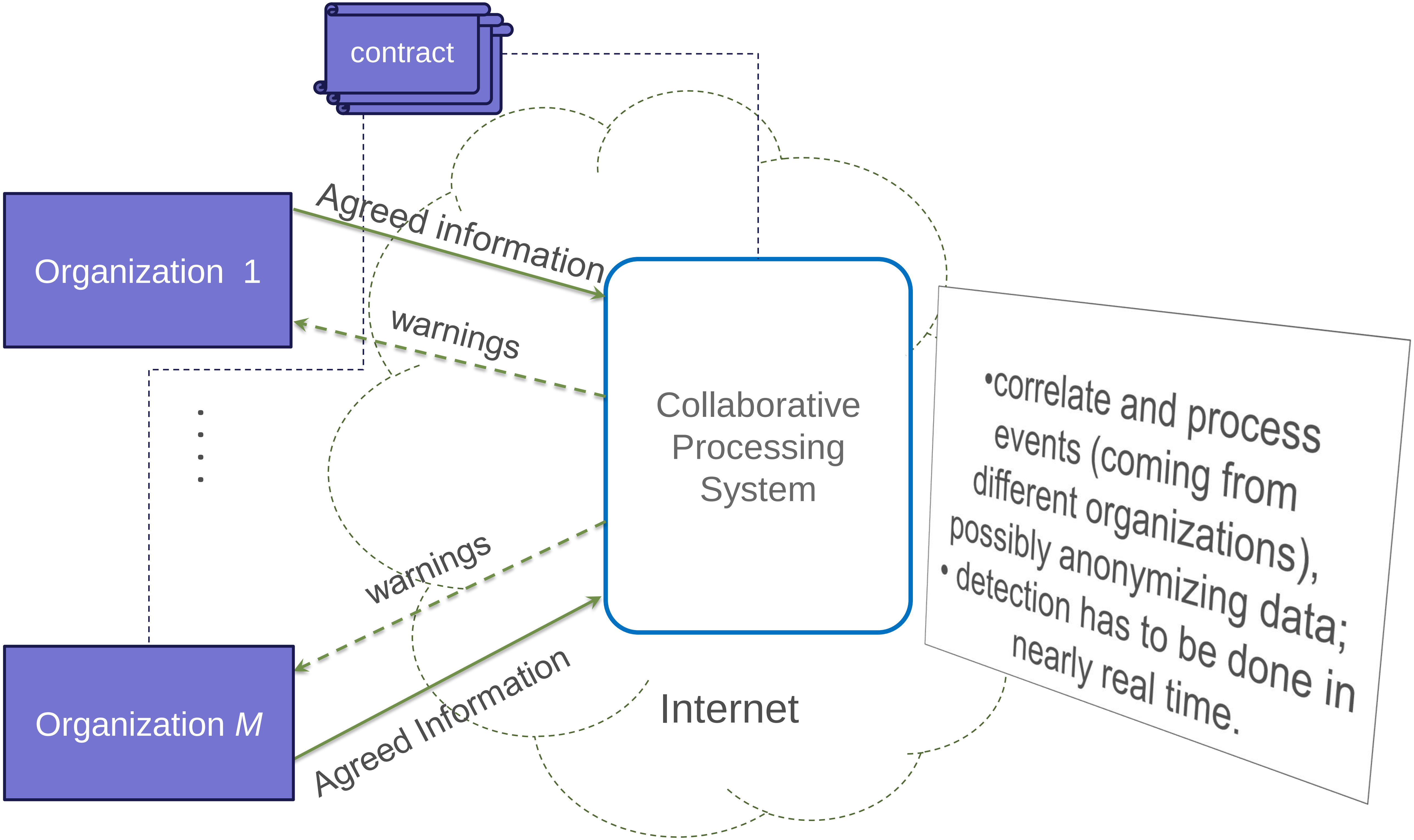
- CoMiFin platform addresses needs considered important in the financial operator community (such as: information security, data privacy, SLA, contractual relationship for entering a community, “certified” anonimity, …)

- CoMiFin project had been submitted to three Financial Advisory Board (FAB) meeting evaluation sessions that have highlighted its possible business value in real financial use cases. Some FAB members: SWIFT, SIA-SSB, IMI-SAN PAOLO, BANK OF ITALY, UBS.

Collaborative Cyber Security: CoMiFin platform

- CoMiFin platform can be potentially useful for addressing the following business use cases
  - Monitoring and reaction to threats (MitM, Stealty Scan , Phishing, …)
  - Black/white lists distribution (for credit reputation, trust level, …)
  - Anti-terrorism lists (with name check VAS)
  - Anti money laundering monitoring
  - Risk management support

- Some Requirements due to use cases:
  - uneven workload along the time
  - High throughput
  - high computational power
  - Large storage capabilities
  - Timeliness



contract

Organization 1

Agreed information

warnings

⋮

Organization *M*

warnings

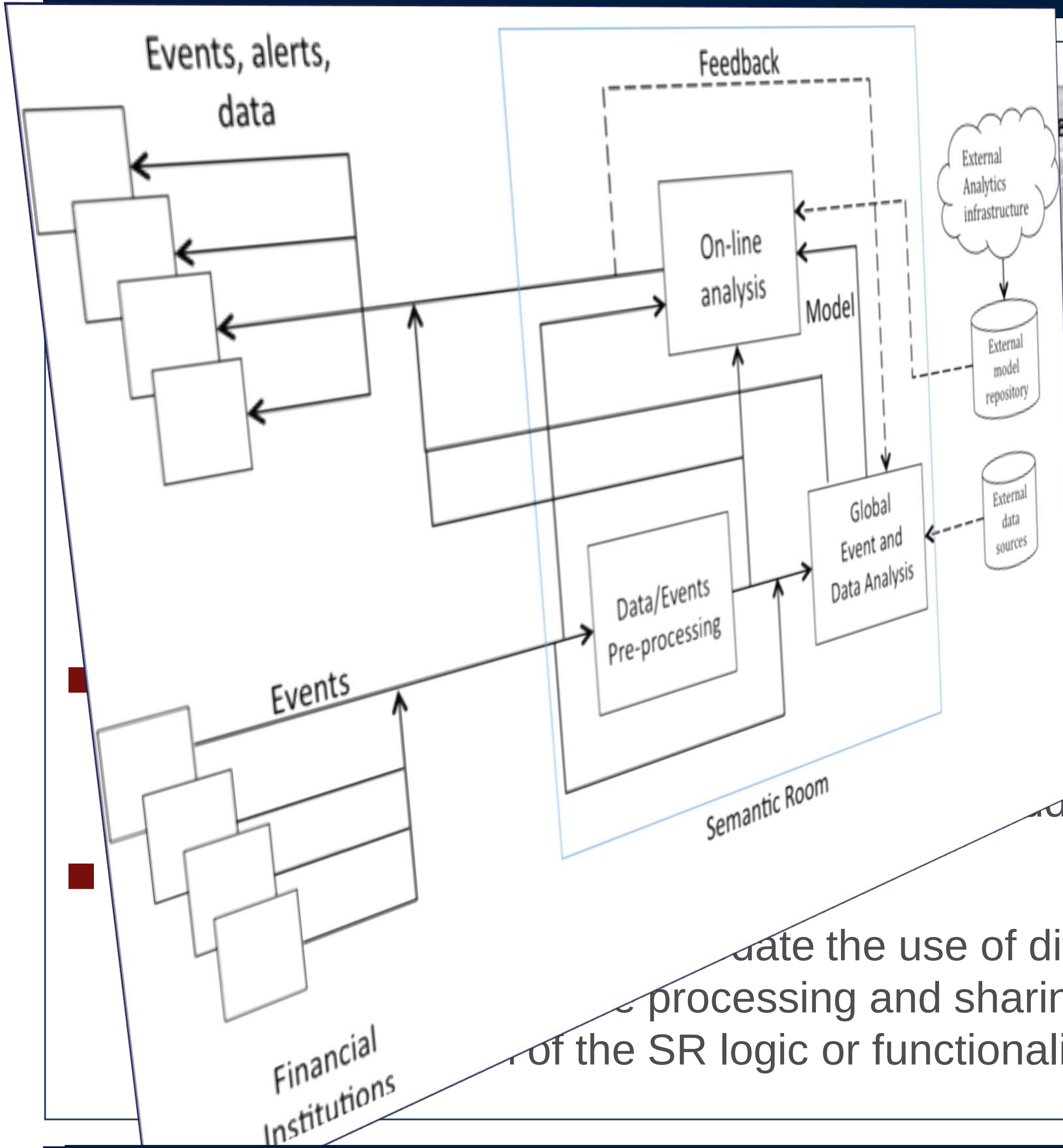
Agreed Information

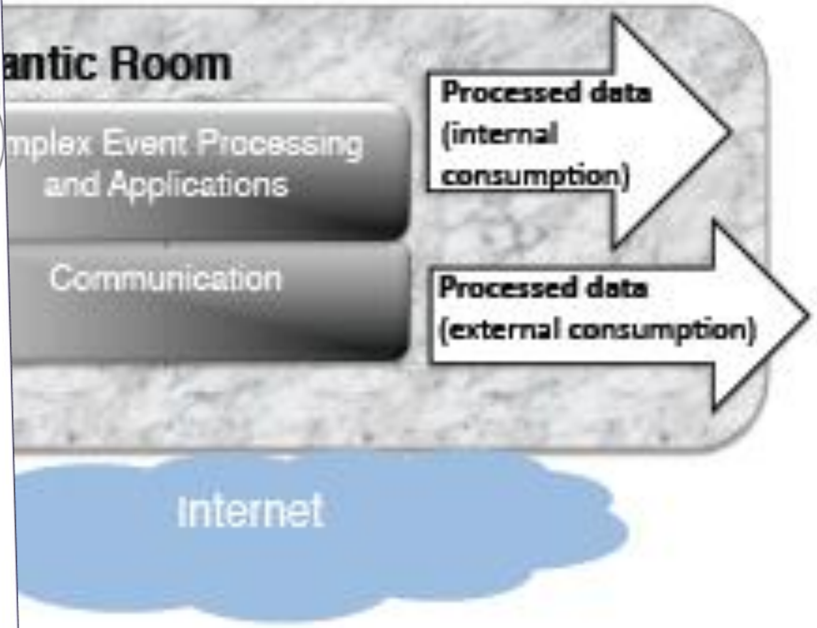
Collaborative Processing System

Internet

- correlate and process events (coming from different organizations), possibly anonymizing data;
- detection has to be done in nearly real time.

The notion of semantic room


Events, alerts, data
Feedback
External Analytics infrastructure
On-line analysis
Model
External model repository
Global Event and Data Analysis
External data sources
Data/Events Pre-processing
Events
Semantic Room
Financial Institutions


antic Room
mplex Event Processing and Applications
Communication
Processed data (internal consumption)
Processed data (external consumption)
Internet

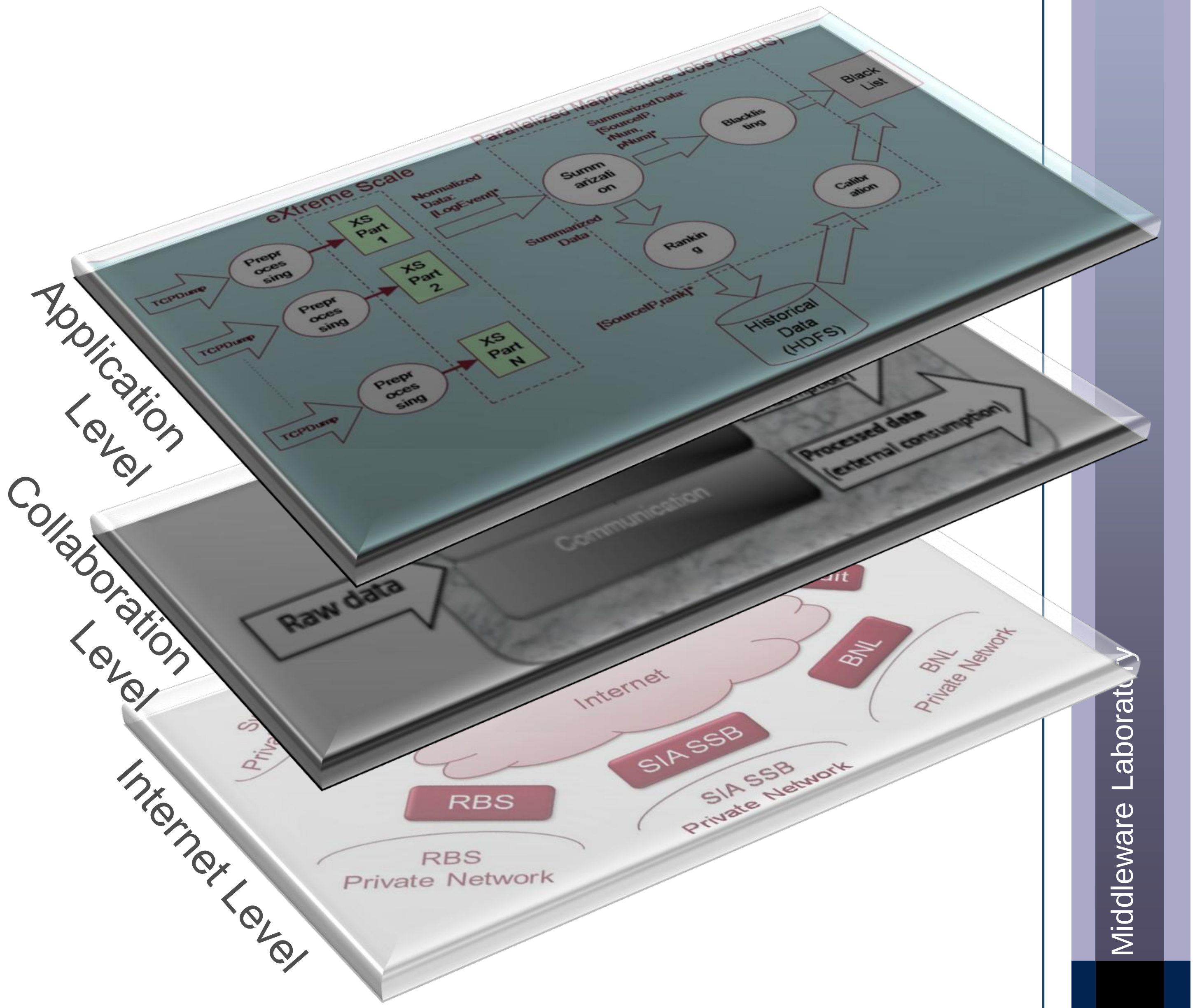
d software requirements a tted into the SR.

meet (e.g, large-scale stealthy dle attacks)

date the use of different technologies for the e processing and sharing within the SR (i.e., the of the SR logic or functionality).

The notion of semantic room: relationship with cloud

- Private cloud
  - Deployment of the semantic room through the federation of computing and storage capabilities at each member
  - Each member brings a private cloud to federate
- Public Cloud
  - Deployment of the semantic room on a third party cloud provider
  - The third party owns all computing and storage capabilities
- Hybrid approach



Data Management problems in the semantic room

- Jurisdiction and regulation (Where and how will data be governed?)
- Ownership of Data (Who owns the data in the semantic room?)
- Data Portability
- Data anonymization
- Data Retention/Permanence (What happens to data over time?)
- Security and Privacy (How is data secure and protected?)
- Reliability, Liability and Quality of Service of the partner of the semantic room
- Government Surveillance (How much data can the government get from a semantic room?)
- …………………..

Example of semantic room: Ingredients

WebSphere eXtreme Scale (WXS): in-memory distributed storage

High-level language for processing logic: Jaql (SQL-like, supports flows)

Distributed processing runtime: MapReduce

Distributed file system for long-term storage: HDFS

Agilis consists of a distributed network of processing and storage elements hosted on a cluster of machines (also geographycally dispersed)

Data Dissemination: Agilis

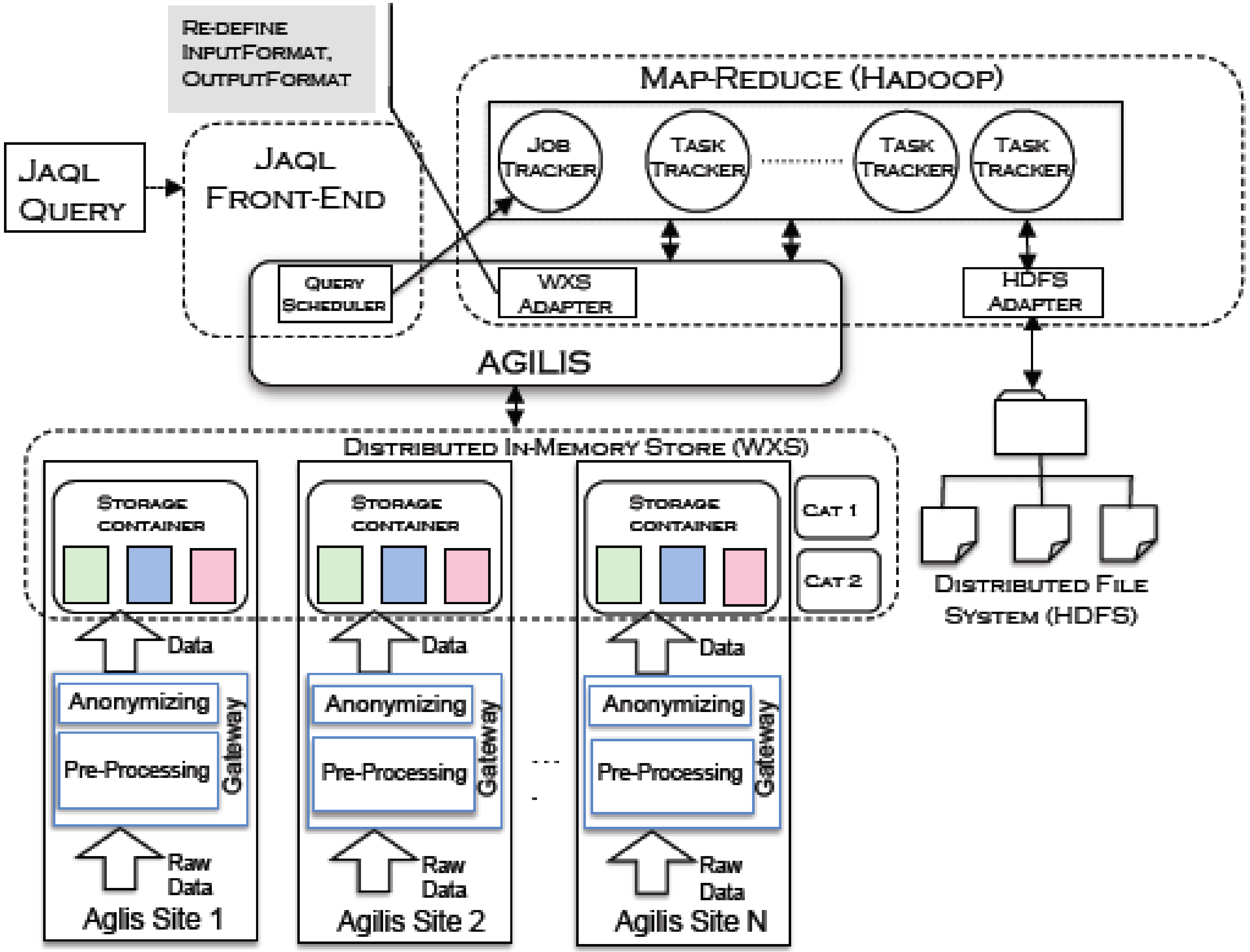
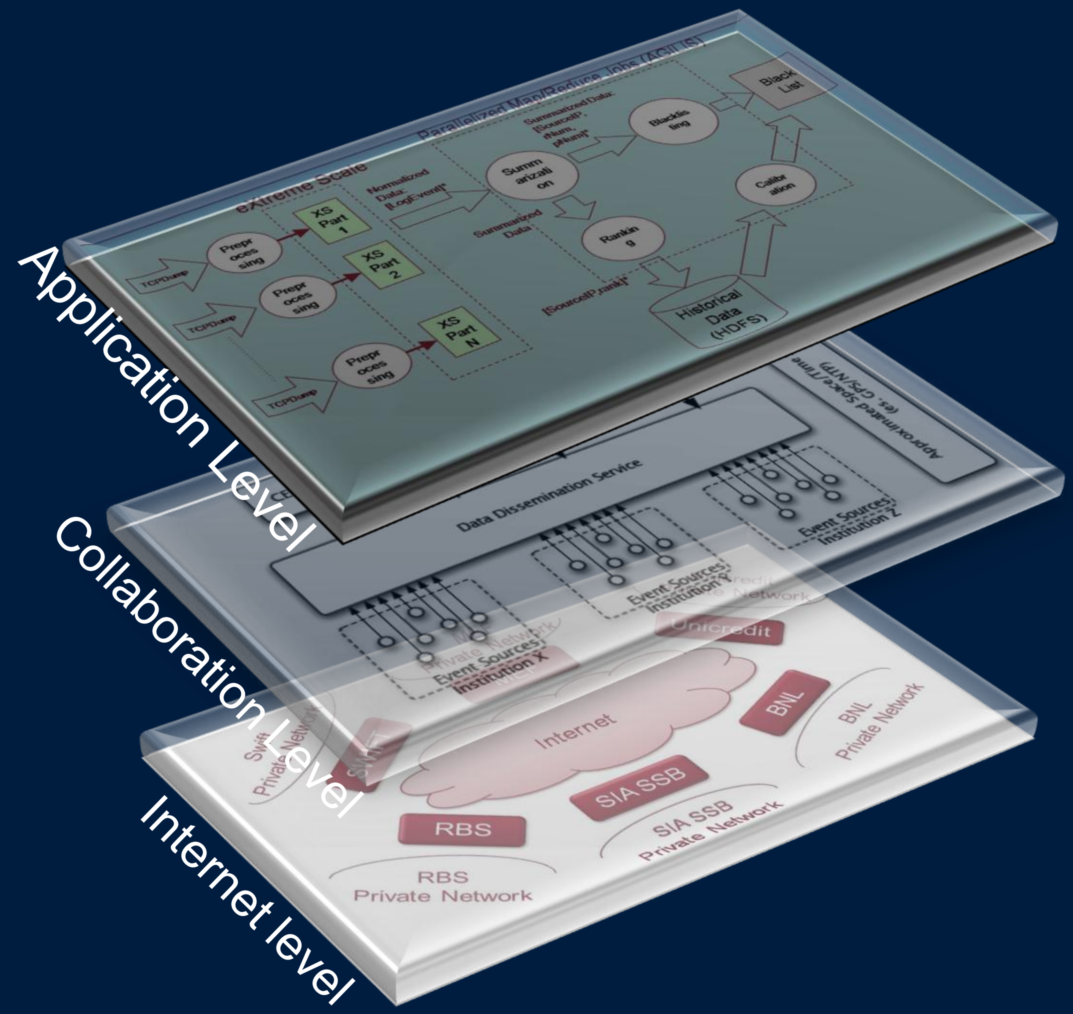


Figure 1: The Components of the Agilis Runtime

Related work

- IBM System S [ICDCS 06]
  - high cost of ownership
  - Centralized data management
  - No cooperative approach
- Cooperative Intrusion Detection Systems (e.g. Dshiels)
  - Correlation among local warnings
  - High cost of ownership
  - Obscure data management

Collaborative Detection of Scanners using Agilis and Esper



Collaborative Stealthy scan

Attacker performs port scanning simultaneously at multiple sites trying to identify TCP/UDP ports that have been left open. Those ports can then be used as the attack vectors

Added value of collaboration:

- Ability to identify an attacker trying to conceal his/her activity by accessing only a small number of ports within each individual domain

Action taken:

- black list IP addresses
- update historical records

Collaborative Stealthy scan detection

Attack subjects:

- External web servers in DMZ’s of the SR members

Pattern:

- “Unusually” high number of requests
- Originating from a particular source IP address, and
- Directed to distinct (machine, port) pairs

Action taken:

- Matching source IP’s are banned from the future access to external web servers

detection algorithms

R-SYN

[L. Aniello, G. Lodi, R. Baldoni, *Inter-Domain Stealthy Port Scan Detection through Complex Event Processing*, EWDC '11]

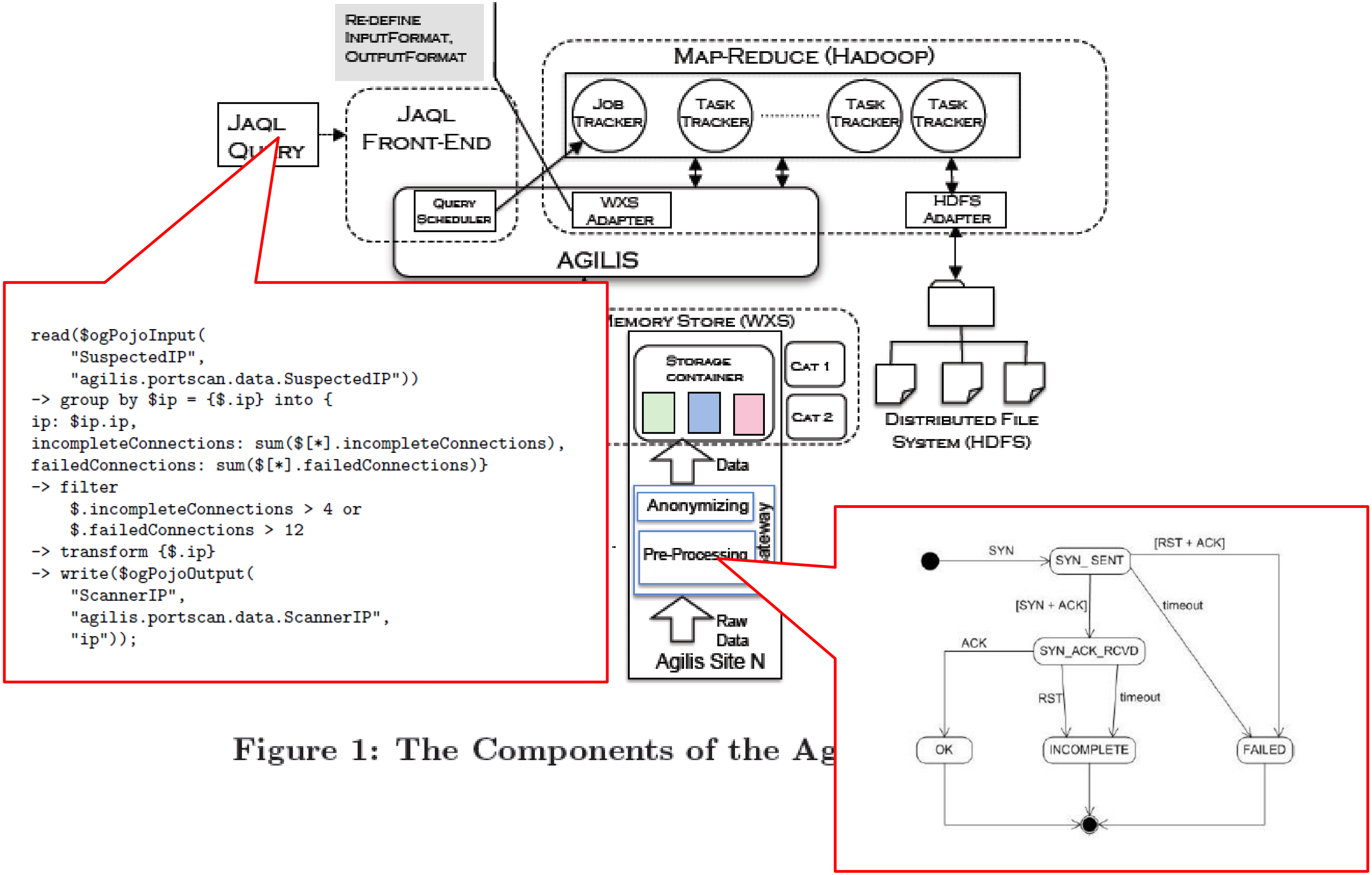
- ranked-based, combine together three distinct techniques
- sub-algorithms
  - ✓ half open connection detection
  - ✓ horizontal and vertical portscan detection
  - ✓ entropy-based failed connection detection

Line Fitting

[L. Aniello, G. Lodi, G. A. Di Luna and R. Baldoni,
A Collaborative Event Processing System for Protection of Critical Infrastructures From Cyber Attacks, SafeComp '11]

- scanners don't repeatedly scan the same TCP port
- plot failed connections count on an endpoints/attempts plane and look for best fitting line
- scanners exhibit a roughly horizontal fitting line

Collaborative Port Scan detection with Agilis



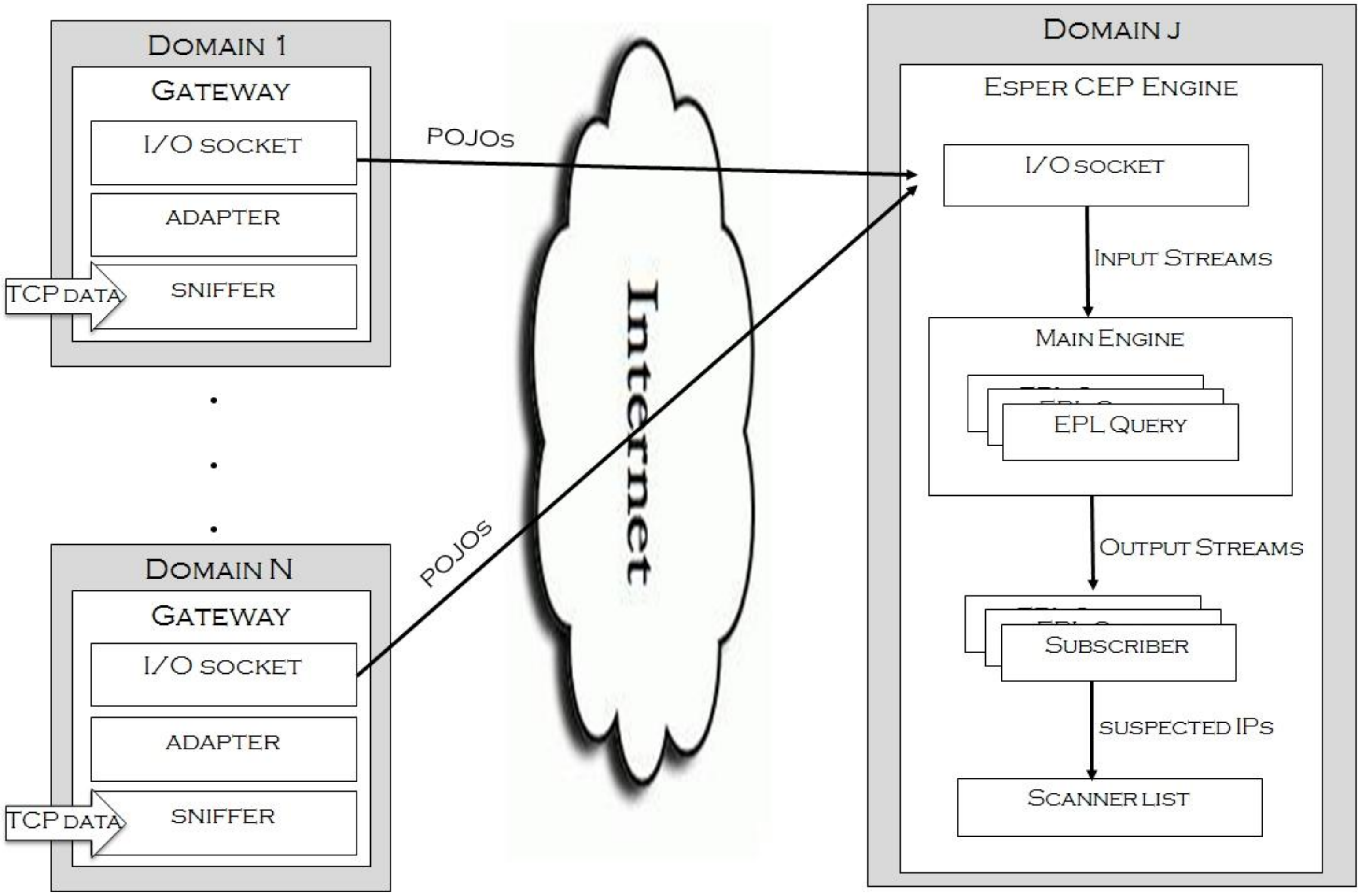
```
read($ogPojoInput(
    "SuspectedIP",
    "agilis.portscan.data.SuspectedIP"))
-> group by $ip = {$.ip} into {
ip: $ip.ip,
incompleteConnections: sum($[*].incompleteConnections),
failedConnections: sum($[*].failedConnections)}
-> filter
    $.incompleteConnections > 4 or
    $.failedConnections > 12
-> transform {$.ip}
-> write($ogPojoOutput(
    "ScannerIP",
    "agilis.portscan.data.ScannerIP",
    "ip"));
```

Figure 1: The Components of the Ag

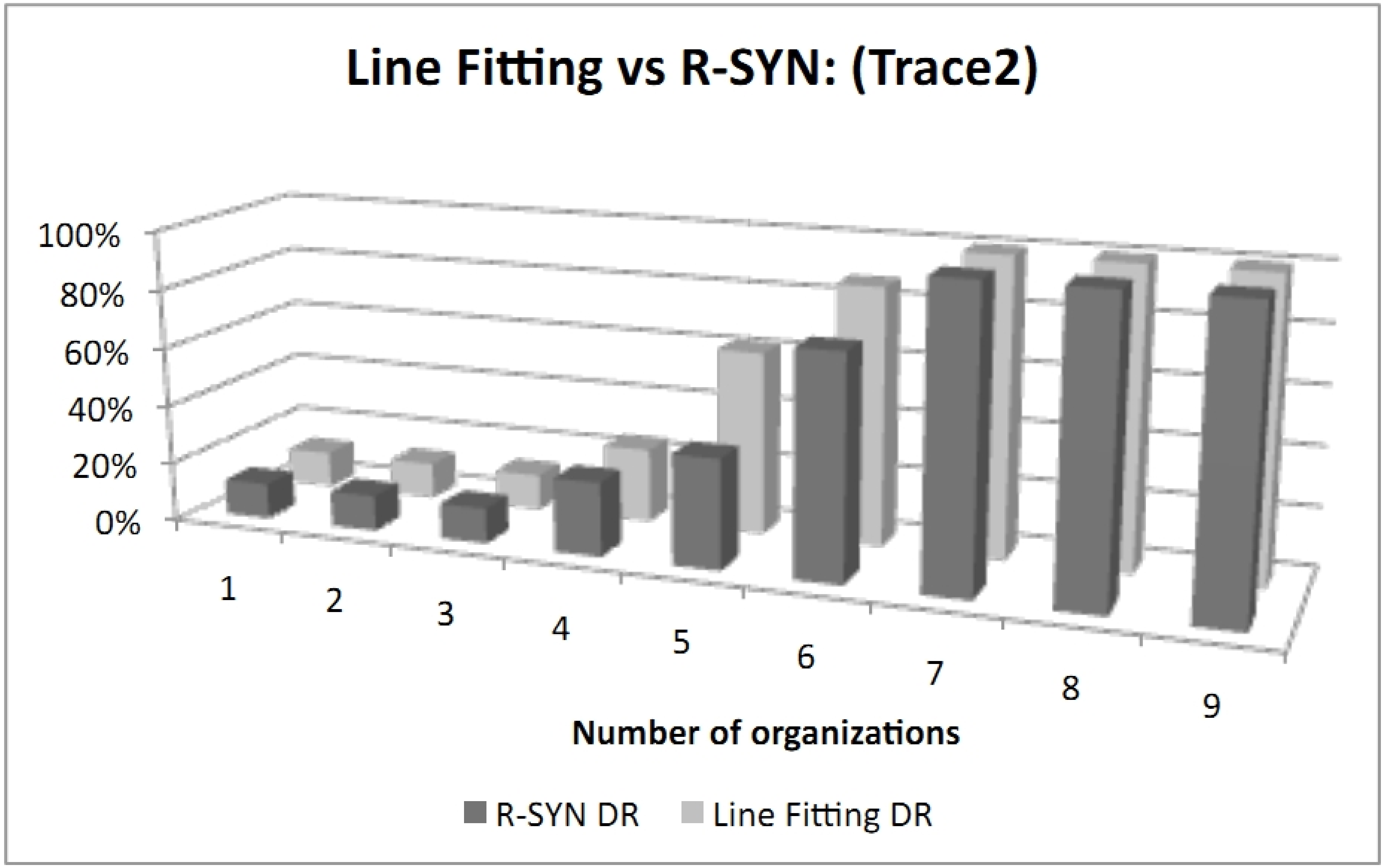
collaborative portscan detection

inter-domain stealthy portscan detection

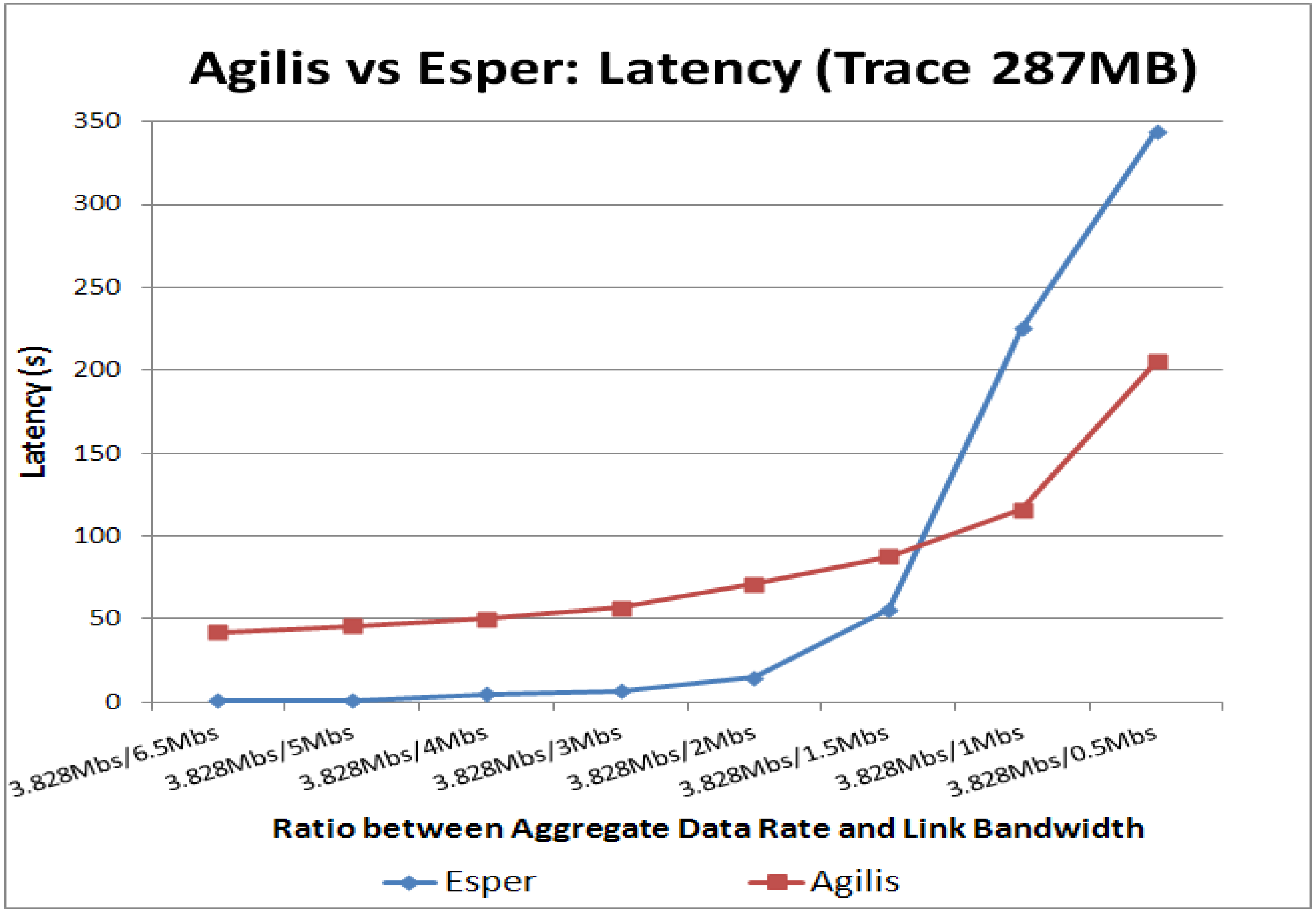
correlate network traffic data coming from distinct domains



Esper evaluations – detection accuracy

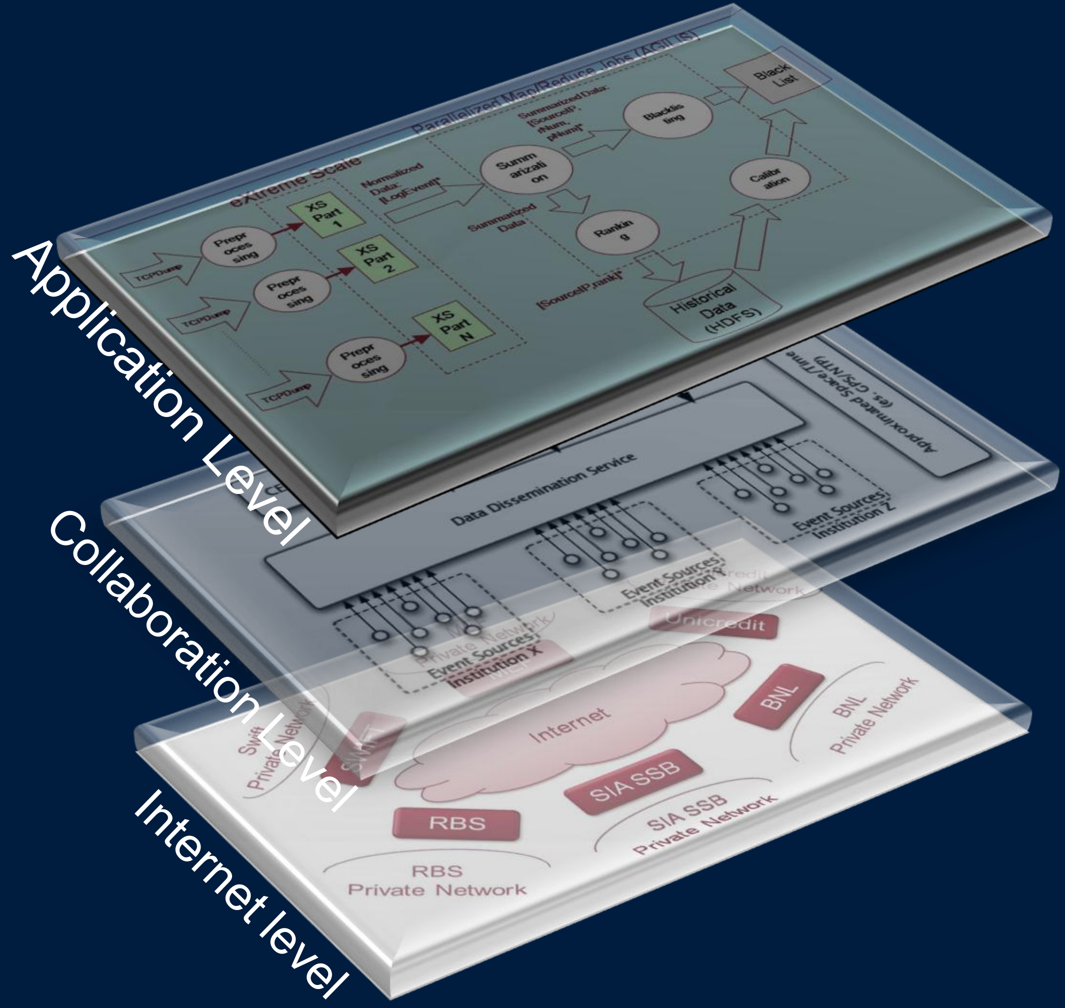


Agilis vs Esper detection latency



Correlating frauds through complex event processing

Sapienza and MEF



Find out possible (spatial/temporal) correlation patterns among single isolated applications

- They do not exchange information with each other
- Data are apparently uncorrelated
- **Sipaf**: Credit card frauds
- **Sirfe**: Counterfeit banknotes

From the two applications we extracted three main data flows concerning

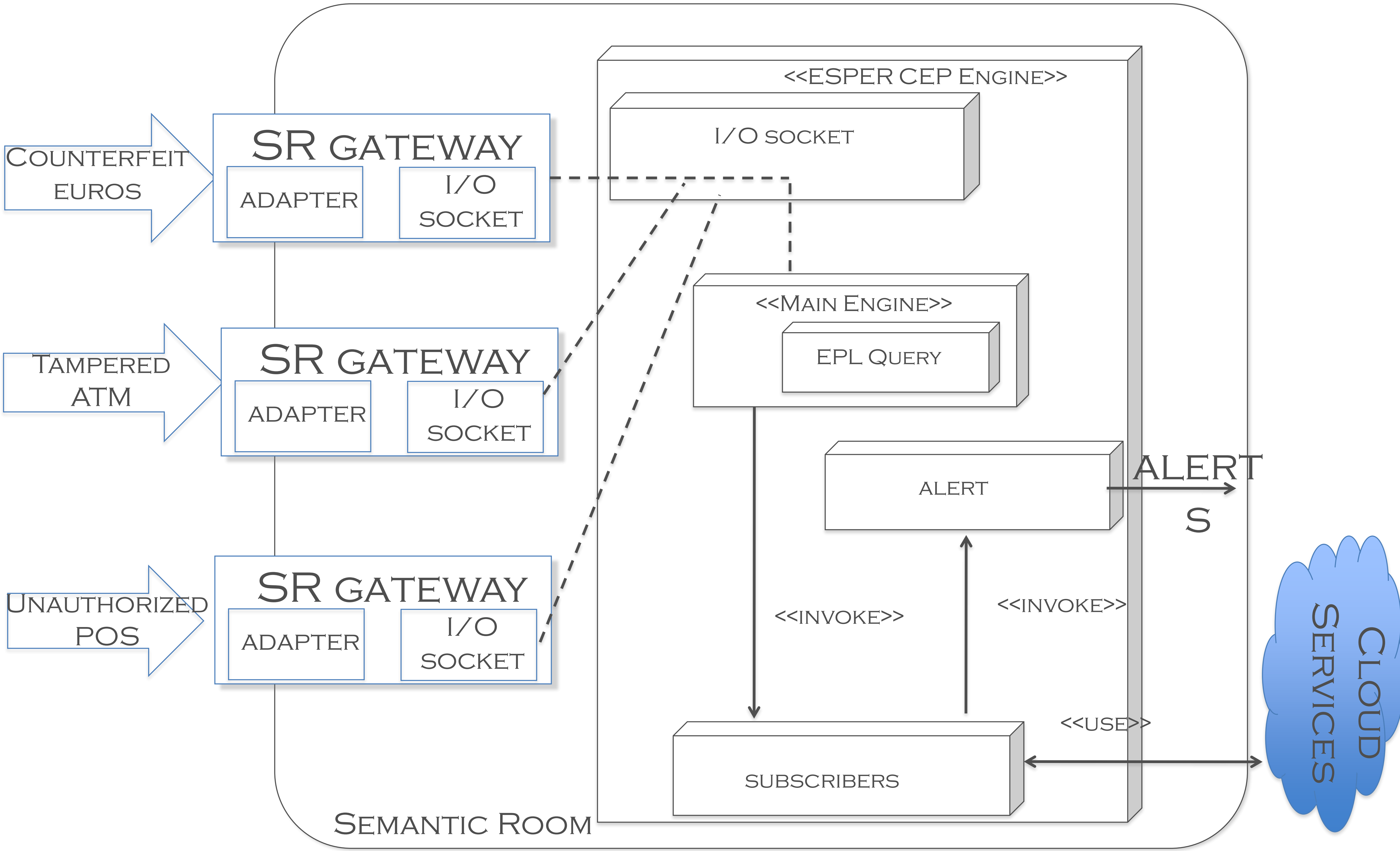
- Counterfeit Euros (from Sirfe)
- Tampered ATM (from Sipaf)
- Unauthorized POS (from Sipaf)

We did not consider unauthorized credit card transactions

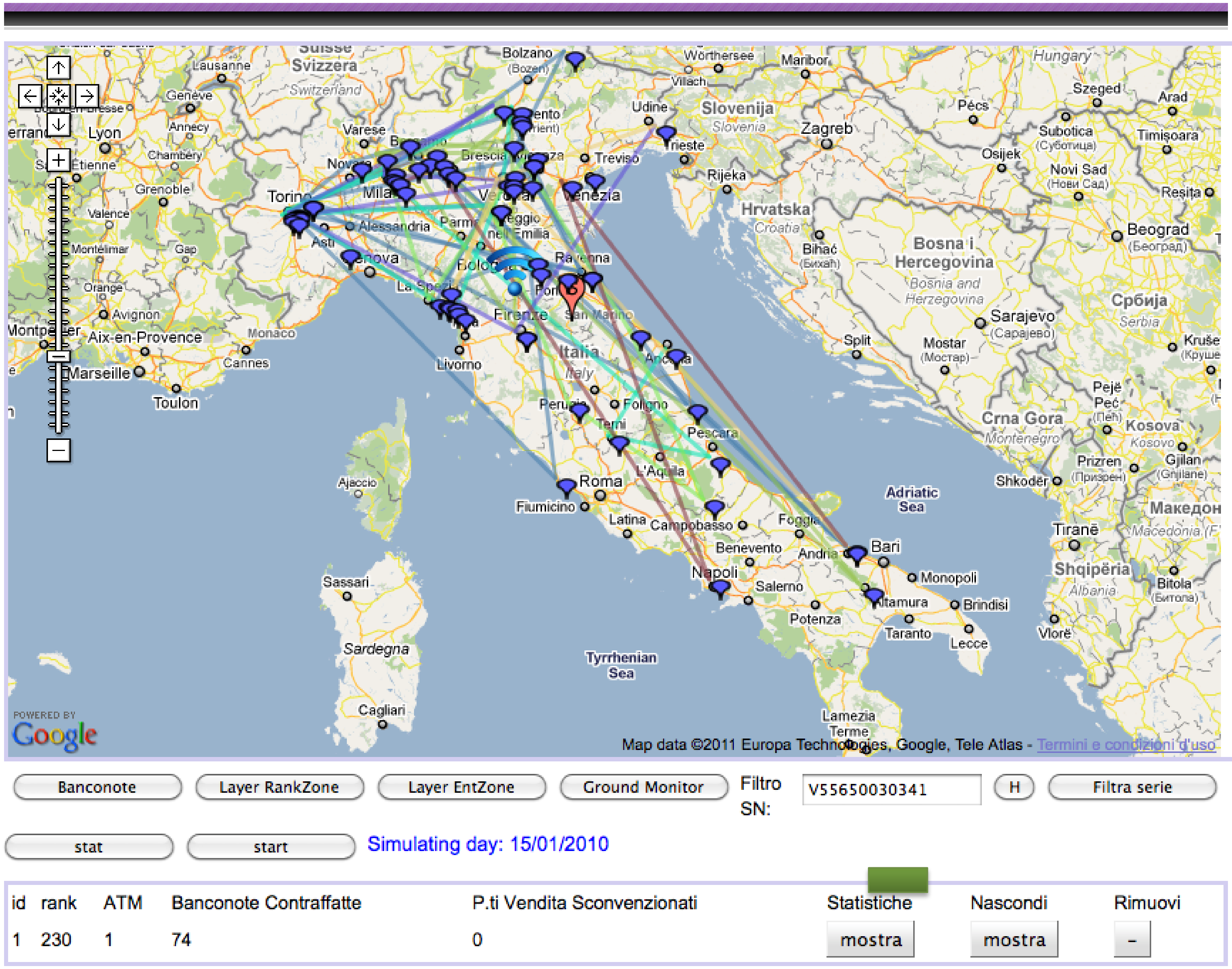
- due to unavailability of important data such as Italian location

We have identified the following possible correlations

- Mainly based on geo-localization on the entire Italy
  - GeoAggregation
    - Identifies “hot areas”, i.e., areas (1 Km x 1 Km approximately) characterized by a high number of crime episodes of the three previously mentioned types
    - Data from Sirfe and Sipaf are correlated based on the location
    - Scores are assigned to the three data flow types and a threshold mechanism is used to identify red (high concentration), yellow (medium concentration) and green areas (low concentration)
  - Crime Entropy
    - Identifies areas characterized by a high number of **different** crime episodes
    - Data from Sirfe and Sipaf are correlated based on the location
      - White areas correspond to high entropy and then high number of different episodes



COUNTERFEIT EUROS
TAMPERED ATM
UNAUTHORIZED POS
SR GATEWAY
ADAPTER
I/O SOCKET
SR GATEWAY
ADAPTER
I/O SOCKET
SR GATEWAY
ADAPTER
I/O SOCKET
<<ESPER CEP ENGINE>>
I/O SOCKET
<<MAIN ENGINE>>
EPL QUERY
ALERT
ALERTS
<<INVOKE>>
<<INVOKE>>
<<USE>>
SUBSCRIBERS
CLOUD SERVICES
SEMANTIC ROOM

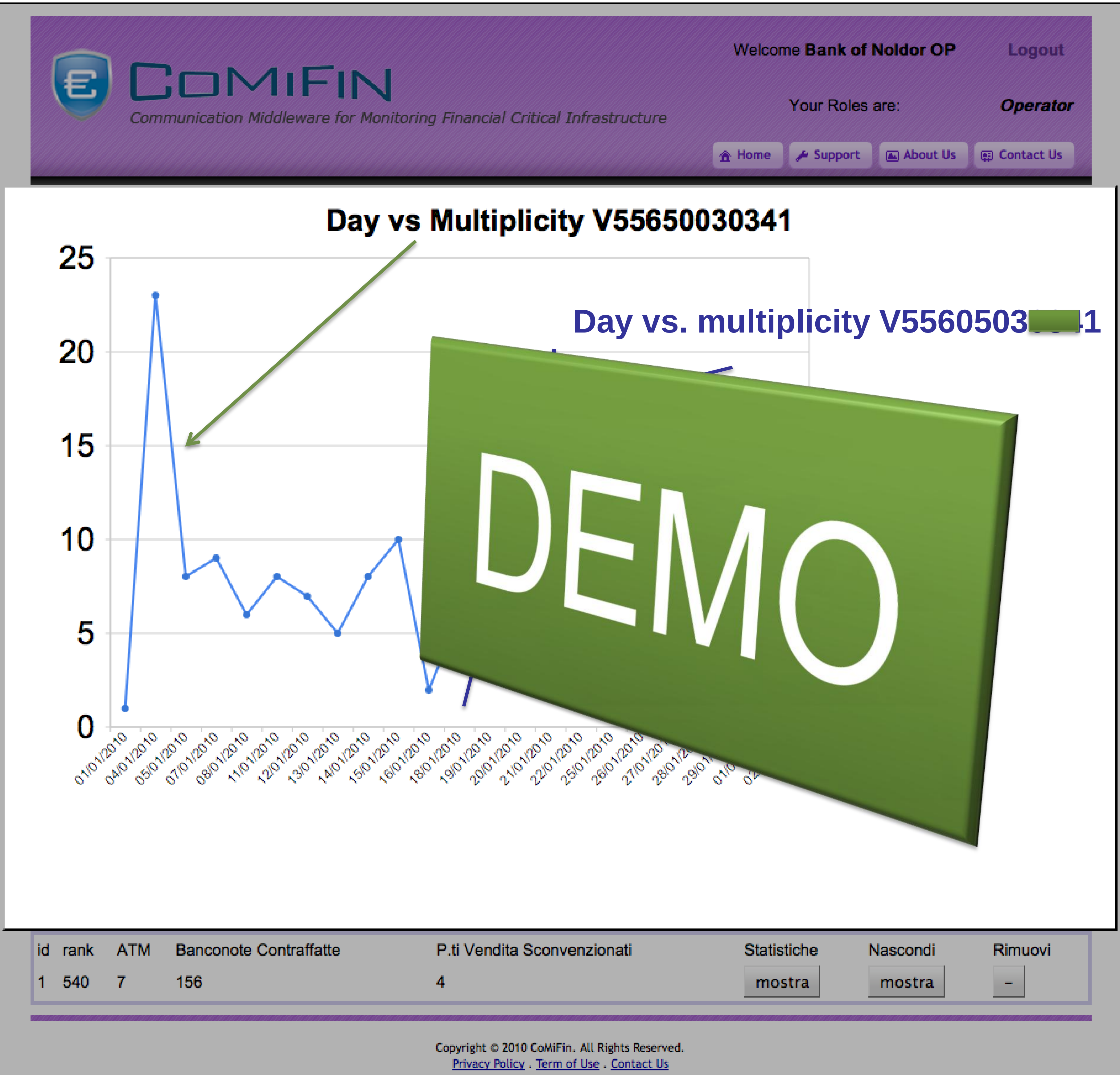


Filtro SN: V55650030341

Simulating day: 15/01/2010

id	rank	ATM	Banconote Contraffatte	P.ti Vendita Sconvenzionati	Statistiche	Nascondi	Rimuovi
1	230	1	74	0	mostra	mostra	–

Privacy Policy . Term of Use . Contact Us



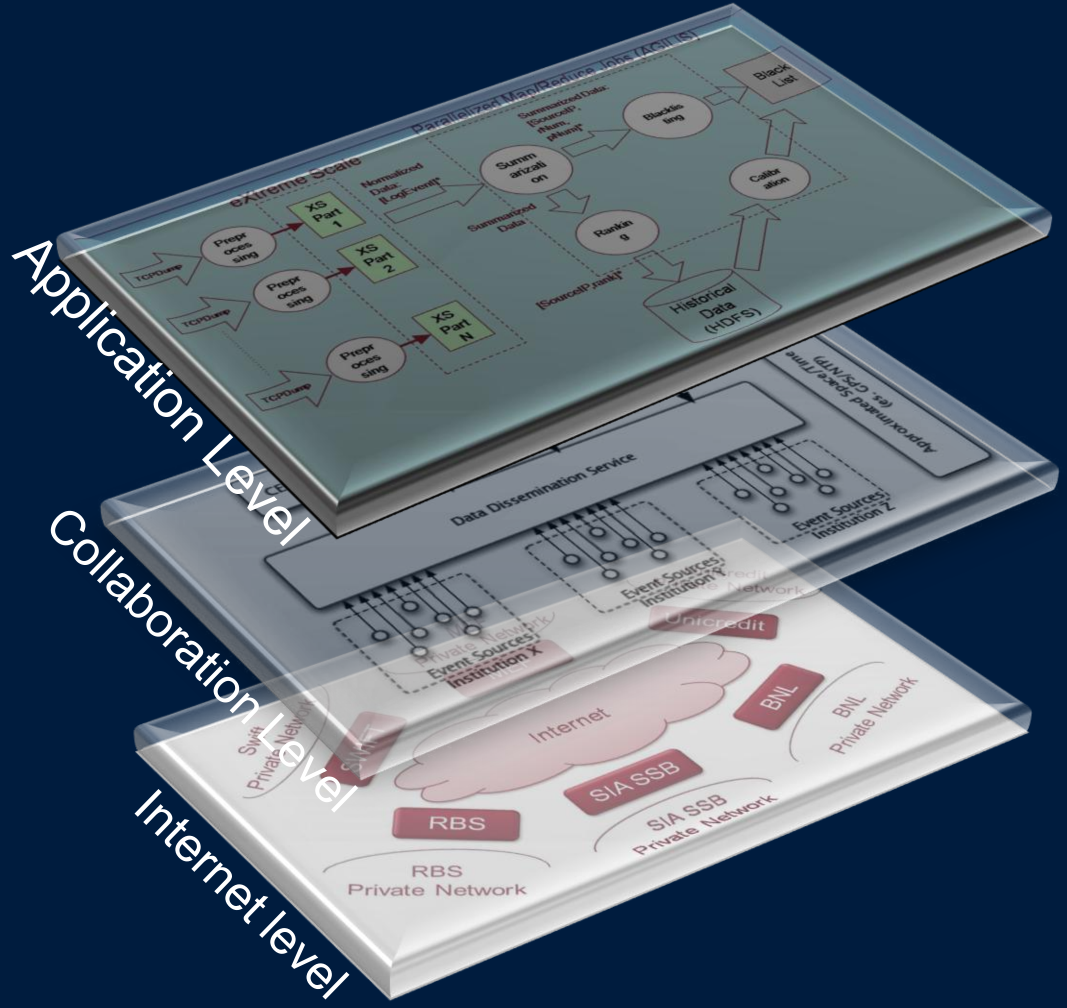
Welcome **Bank of Noldor OP**

Your Roles are: ***Operator***

id	rank	ATM	Banconote Contraffatte	P.ti Vendita Sconvenzionati	Statistiche	Nascondi	Rimuovi
1	540	7	156	4	mostra	mostra	-

Privacy Policy . Term of Use . Contact Us

Privacy Preserving Collaborative Architectures



Motivations

Banks cloud exploit the benefits of a collaborative data processing for timely discovery of customers (or any other third party) performing malicious activities against banks' IT infrastructures;

Not all customers misbehave; sensitive data of honest customers are to be kept secret (i.e., sensitive data are not disclosed or linked to the owner of the data) during the collaborative data computation, with respect to the other competitive banks that can potentially exploit the knowledge of those data for their advantage

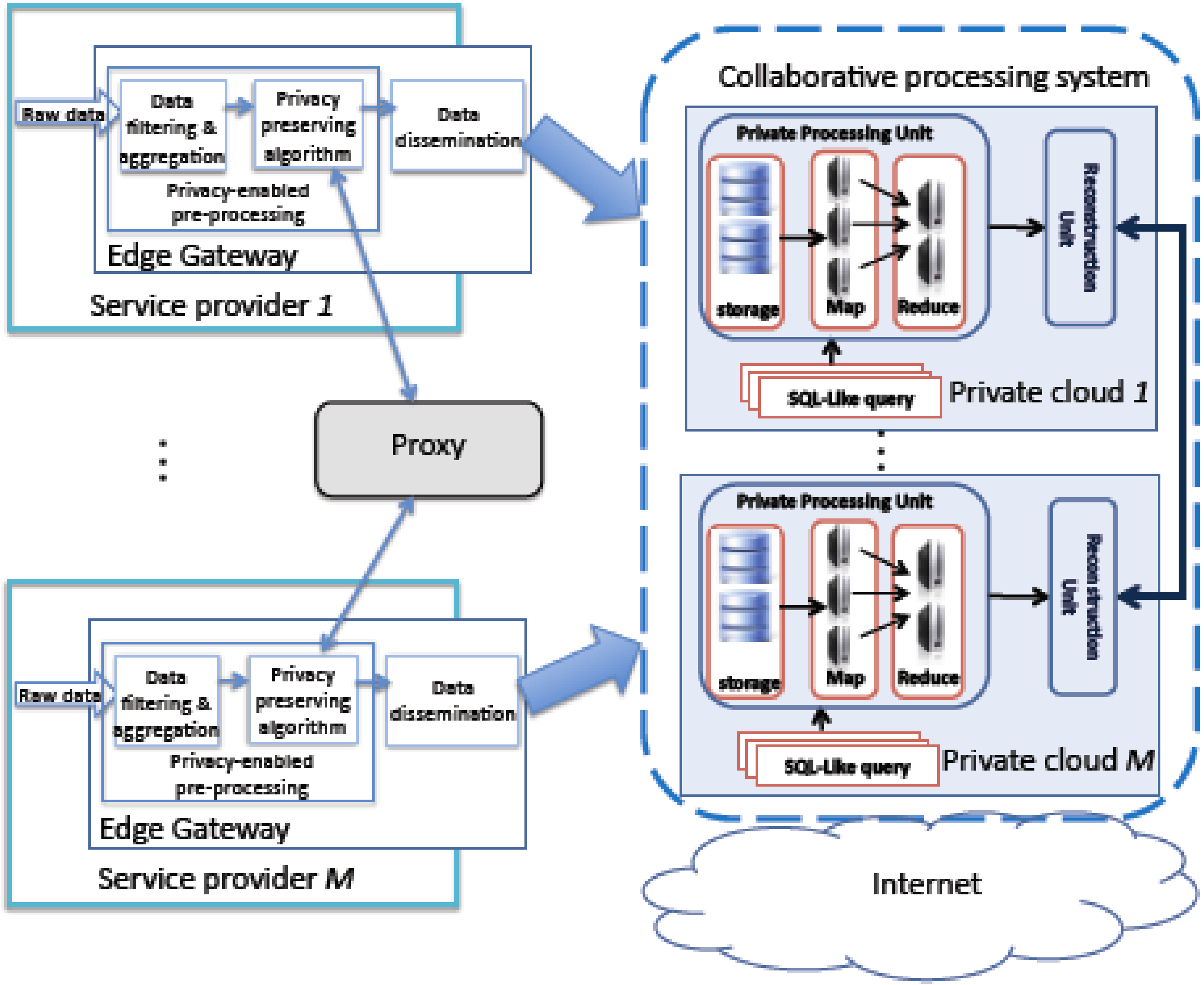


Figure 1. The privacy preserving architecture

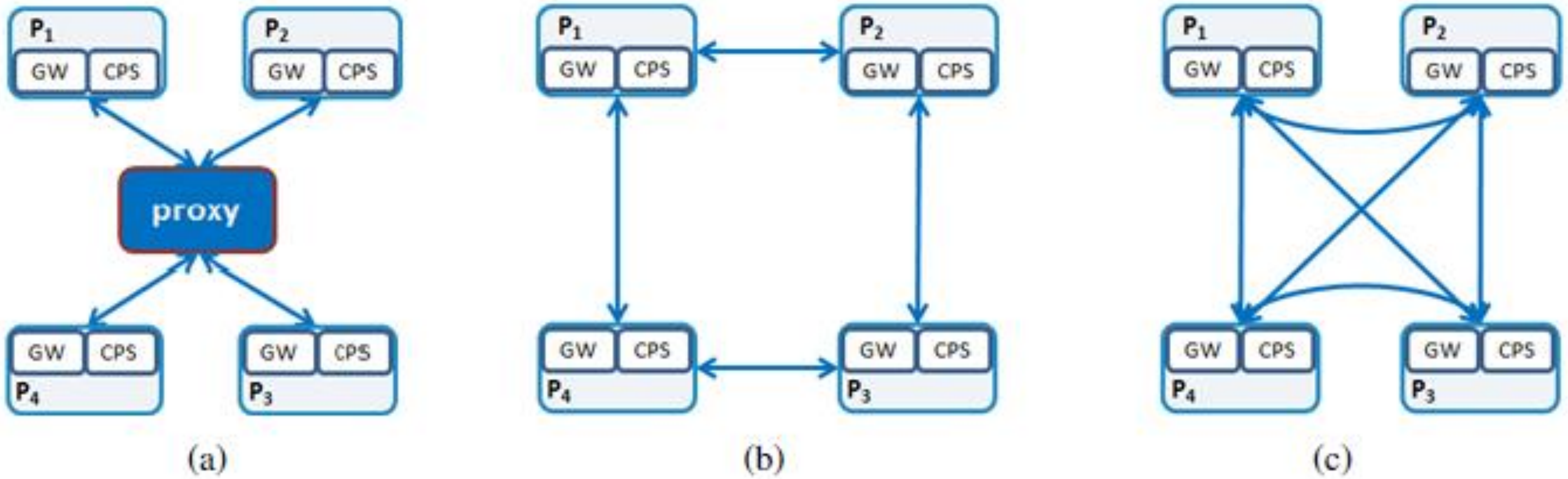


Figure 2. Privacy preserving architecture life cycle: (a) Privacy-enabled pre-processing phase , (b) Data Dissemination phase, (c) Reconstruction phase.

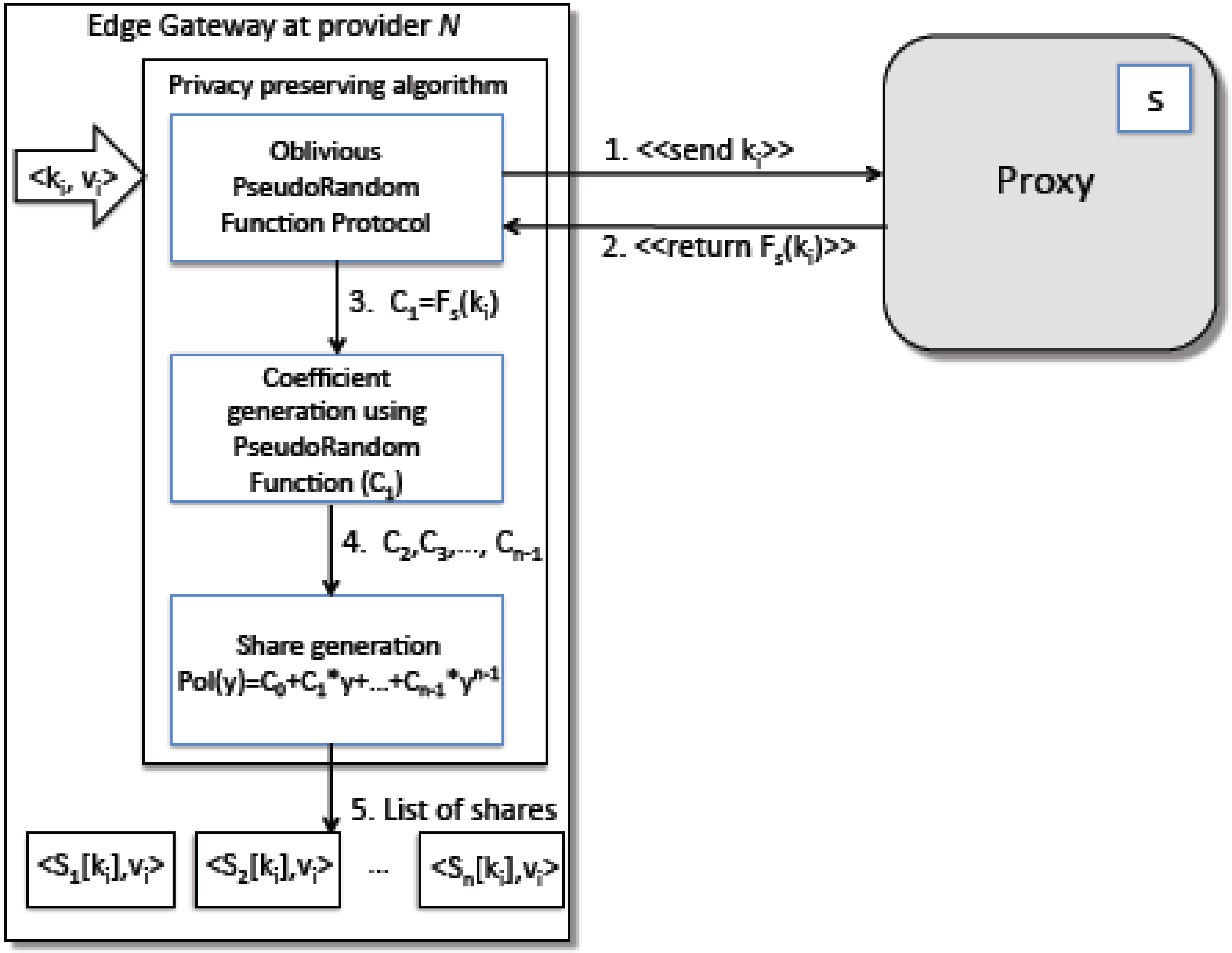

Edge Gateway at provider *N*
Privacy preserving algorithm
$<k_i, v_i>$
Oblivious PseudoRandom Function Protocol
1. $<<$send $k_i>>$
2. $<<$return $F_s(k_i)>>$
Proxy
s
3. $C_1=F_s(k_i)$
Coefficient generation using PseudoRandom Function (C_1)
4. $C_2, C_3, \dots, C_{n-1}$
Share generation
$Pol(y)=C_0+C_1*y+\dots+C_{n-1}*y^{n-1}$
5. List of shares
$<S_1[k_i],v_i>$
$<S_2[k_i],v_i>$
...
$<S_n[k_i],v_i>$

Figure 3. Privacy preserving algorithm

Thanks

- Comifin partners, MEF Project, Microsoft Project
  - Giorgia Lodi, Leonardo Querzoni, Leonardo Aniello, Silvia Bonomi, Luca Montanari, Marco Platania, Giuseppe di Luna, Hani Qusa, Roberto Beraldi
  - Mirco Marchetti, Michele Colajanni,
  - Vita Bortnikov, Gregory Chockler, Eliezer Dekel, Gennady Laventman, Alexey Roytman
  - Luca Nicoletti, Andrea Baghini