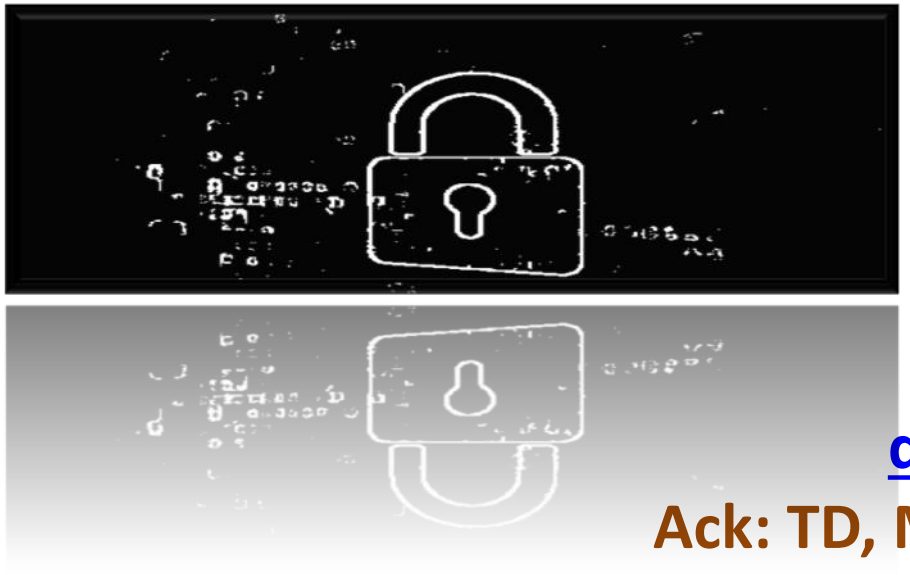
FRISC Winter School 2015

Cloud Security: Intrusion Detection in Virtual Environment



Dhiren Patel

NIT Surat, India

dhiren@coed.svnit.ac.in

Ack: TD, MR, AJ, BB, CM, HP, FRISC, UIDAI

NIT Surat – Computer Engineering Department

- NIT Surat (53 years), CSE Department (24 years)
- National Institute of Technology (NITs), one in each state (~20+10)
- Indian Institute of Technology (IITs), total (~6+9)
- NIT Surat – CSE Intake: 90 BTech students, 25 MTech students
- Current PhD students ~20 (Full Time, Part Time (faculty QIP), Project)
- Faculty (??? Small group – 11 + 16 teaching assistants)

Research at NIT Surat - CSE

- Information Security:
- Information Security Education & Awareness, Biometric based IDMS, Security in Cloud computing (IDS, in-VM), Security in WSN (Data aggregation, FHE/PHE, ABE), Security in IoT (IDM and Privacy), PKI Trust Mgt and Secure e-Voting …
- Computer Vision:
- Image/Video Compression, Machine Learning, Digital Archival (e.g. Hampy temples), Biometrics template generation and storage, Data mining …

Hampi temples, Karnataka, India

Collaborations

- C-DAC Mumbai – Critical Infrastructure Protection (SCADA security), Biometrics
- City University London – Cyber Security, Virtual Identity
- British Telecom UK – Cloud Security and Trust
- University of Oslo – Identity Management, PKI and Trust
- University of Denver USA – Proof of Work, PPDM
- IIT Bombay, IIT Kanpur – DA for JoSAA
- HP Labs Palo Alto – Green ICT

Researching Research: Are we going the right way?

- Mischa Dohler (2008, CTTC, Barcelona, Spain)
- (Now – at Kings College London)
- **Research:** *… is the process of going up alleys to see if they are blind*
- infinite number of problems but only finite resources,
- challenges is to say no
- **Development:** *… is too boring for research and never sufficiently fast for marketing*
- challenge is to deliver
- **Market:** *… is to make people buy things they don't actually need*
- challenge is to predict

Problems first!!!

- Mathematics poses problem first and then tries to find solution
- **Engineering often tries to find a solution to a problem which is not yet known**
- leads to hype as solutions are hoped to fit all problems
- solutions are neither cheap nor simple

- **Academic Efforts:** challenge is to focus on important issues in research,
- **Industrial Efforts:** challenge is to be on time, i.e. not too early and not too late

the challenges of performing rigorous research

- identify common errors and biases that may be contributing to the rise in irreproducible/irresponsible research.
- Ioannidis (2005 – PLOS medicine) -- Why most published research findings are false?
- The probability that a research claim is true may depend on study power and bias, the number of other studies on the same question, and, importantly, the ratio of true to no relationships among the relationships probed in each scientific field.

Green ICT

- Focus: to reduce the cost and power consumption of IT system and maximize energy efficiency during the system's lifetime
- Reshaping focus: mobilizing ICT sector to save energy is a great idea
- being a facilitator - help decreasing consumption of transportation, even if ICT increases

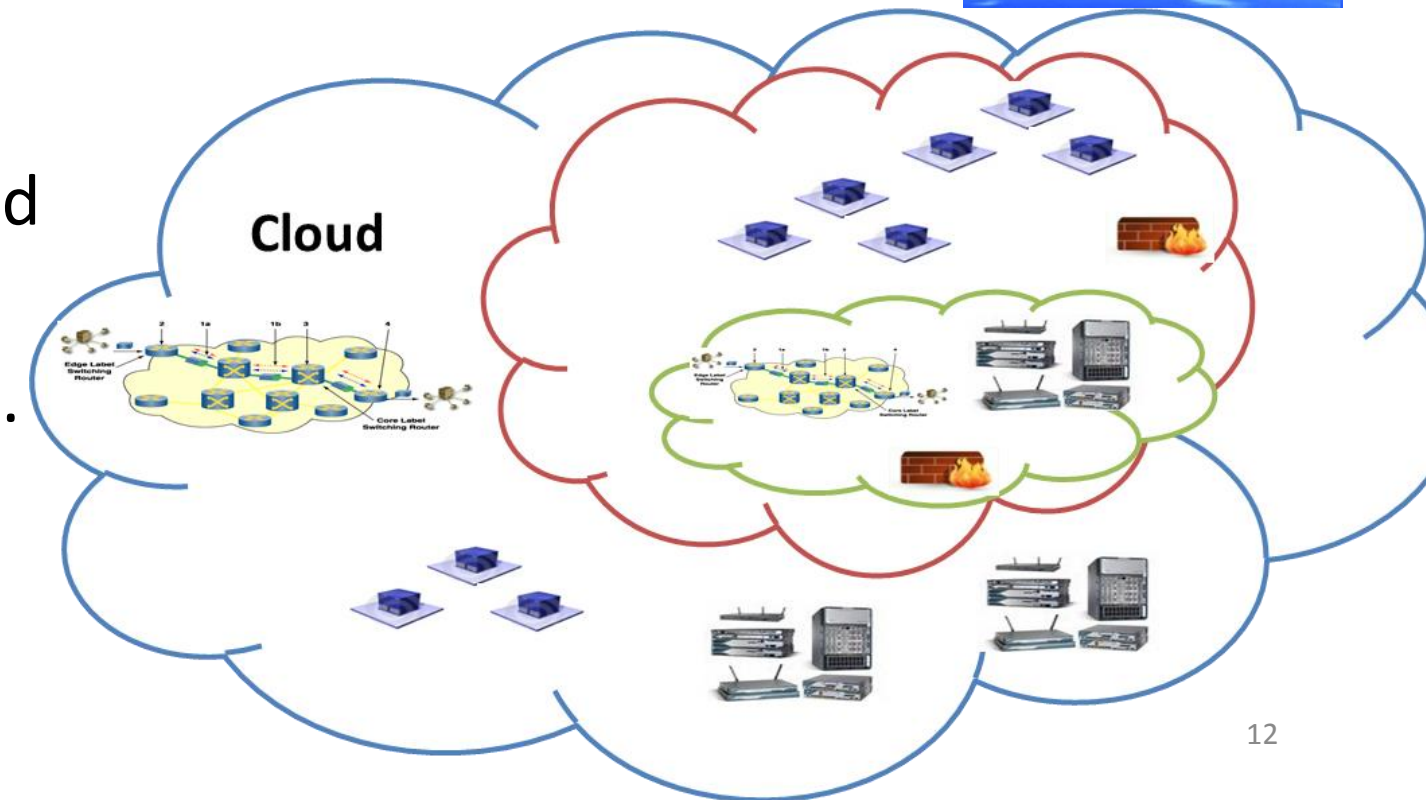
Imagination is more important than knowledge

- E.g. Blackle instead of Google likely saves more energy

Cloud Computing: Definition

- A pay-per-use model for enabling convenient
- on-demand network access
- to a shared pool of configurable computing resources
- that can be rapidly provisioned and released with minimal management effort or service provider interaction.

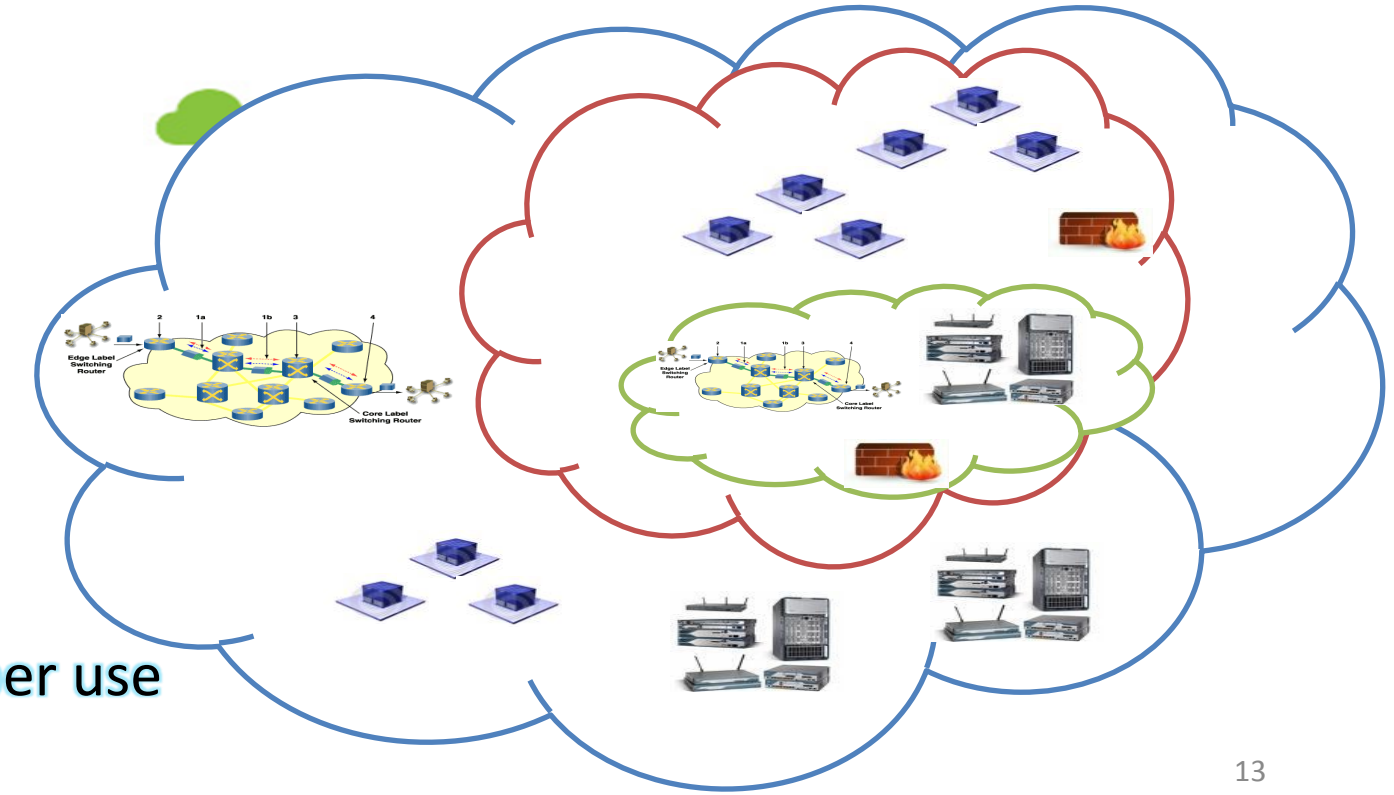
(ref: NIST)



Cloud computing delivers

- infrastructure,
- platform, and
- software applications as services,
- made available to consumers as
- subscription-oriented in a
- pay-as-you-go model

……(like Utility computing)



- From client server to cloud
- Dynamic, Shared Infrastructure,
- Automated/elastic, Scalable, Pay per use

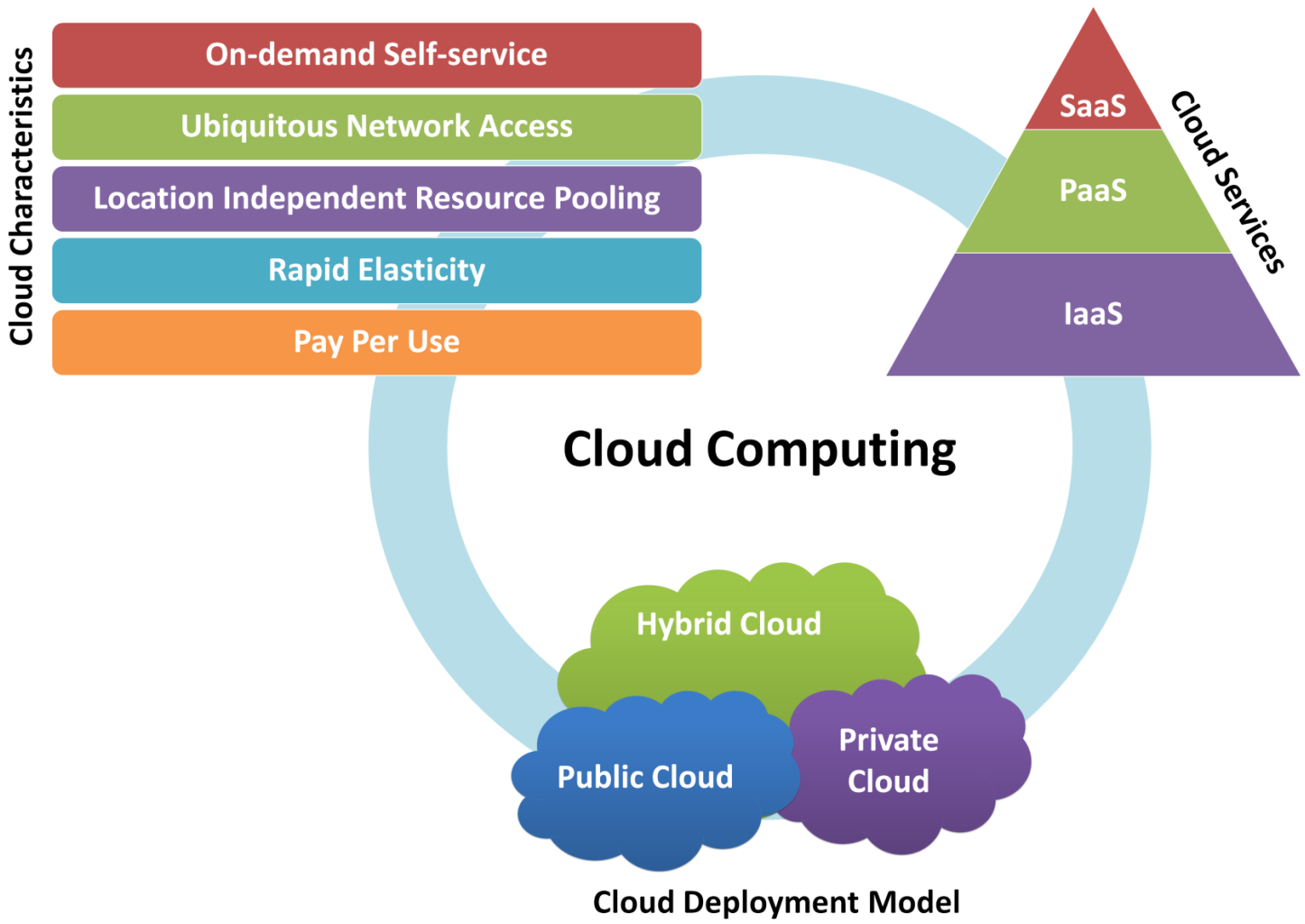
Cloud and Virtualization

- Virtualization; a key enabling technology for Cloud,
- significantly increased the utilization of computing capacities
- It has pushed computing paradigm from
- multi-tasking to multi-operating-system computing

Cloud shifting

- computing is migrating from personal computers sitting on a person's desk (or lap) to large, centrally managed datacenters
- Cloud datacenters consist of thousands of machines and disks that must be allocated (and later reallocated) to particular applications, with machines failing regularly and demand constantly changing. How do cloud providers monitor and provision services?
- cloud storage systems are increasingly used to store valuable business data and intensely private data, and even mix data from different individuals on the same servers.
- what steps can be taken to ensure the privacy of that data and to reassure users that their data will not be inadvertently released to others?
- Governance, Risk management, Compliances (Cloud GRC)

Cloud Computing: Characteristics, Services, Deployment models

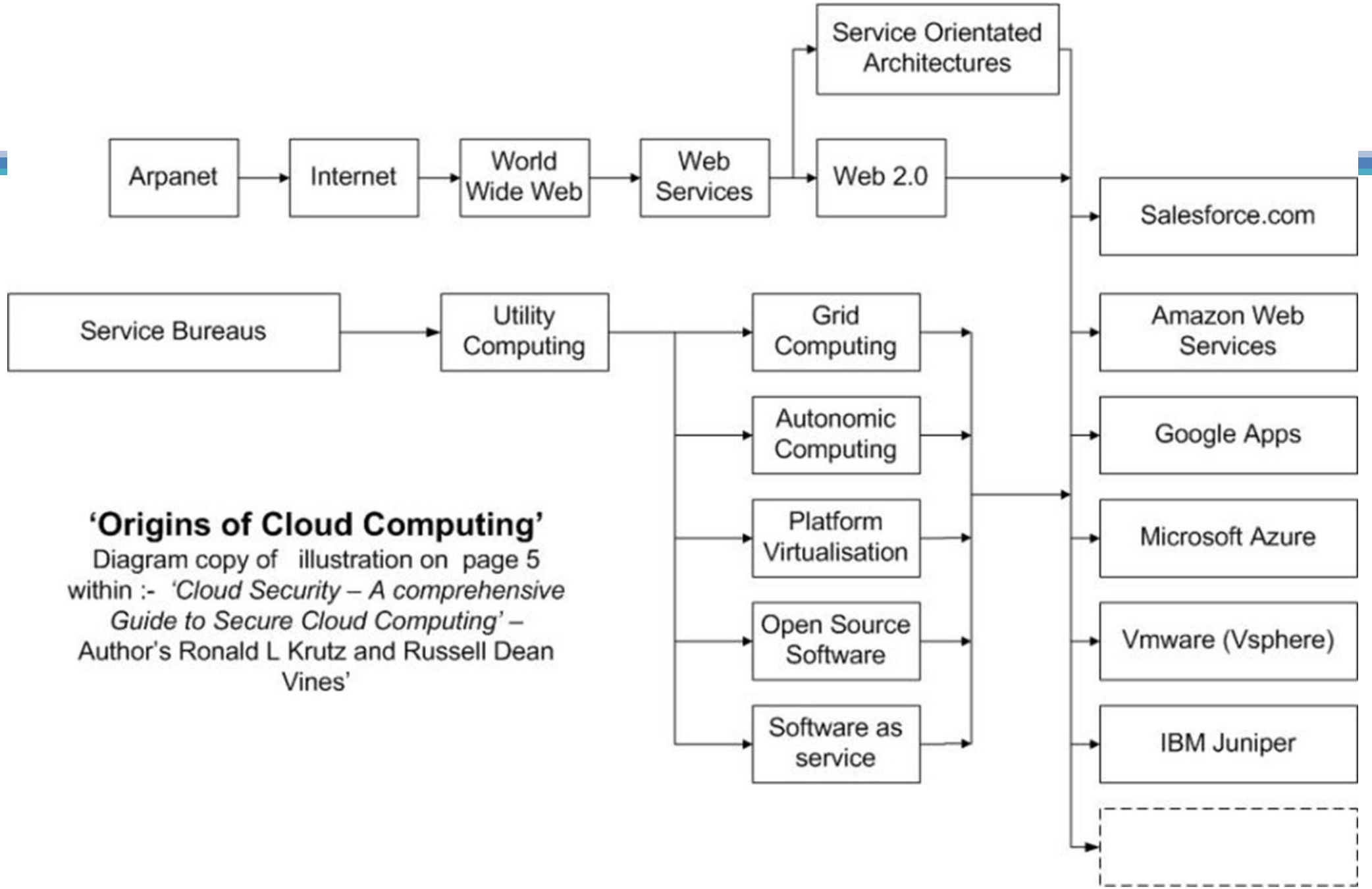


Obvious benefits

- **Providers' view**
- Since substantial numbers of end users are inactive, the service provider reaps the benefits of the economies of scale from statistical multiplexing,
- **Users' view**
- from having data and services available from any location,
- from having data backups centrally managed,
- from the availability of increased capacity when needed,
- from usage-based charging (pay-per-use)
- <averts the need for a large one-off investment in hardware,
  sized to suit demand that requiring future upgrading>

Cloud computing – basic keywords

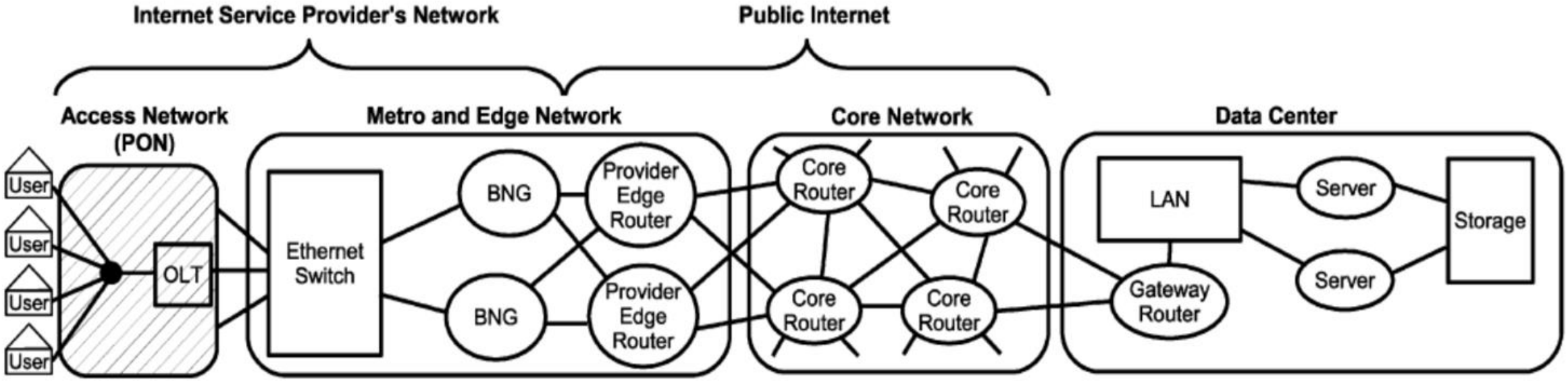
- Compute Server, Data Center …
- Thin client (zero client)
- XaaS
- X = Infrastructure, Platform, Software, Data, Network (strict/loose, QoS), Drawing …
- Virtual machine (VM)
- VM Instances (cpu, memory, os), VM size
- Golden image
- Scaling – Horizontal / Vertical
- Physical Data Centre, Virtual Data Centre
- Resource pooling, granularity



'Origins of Cloud Computing'

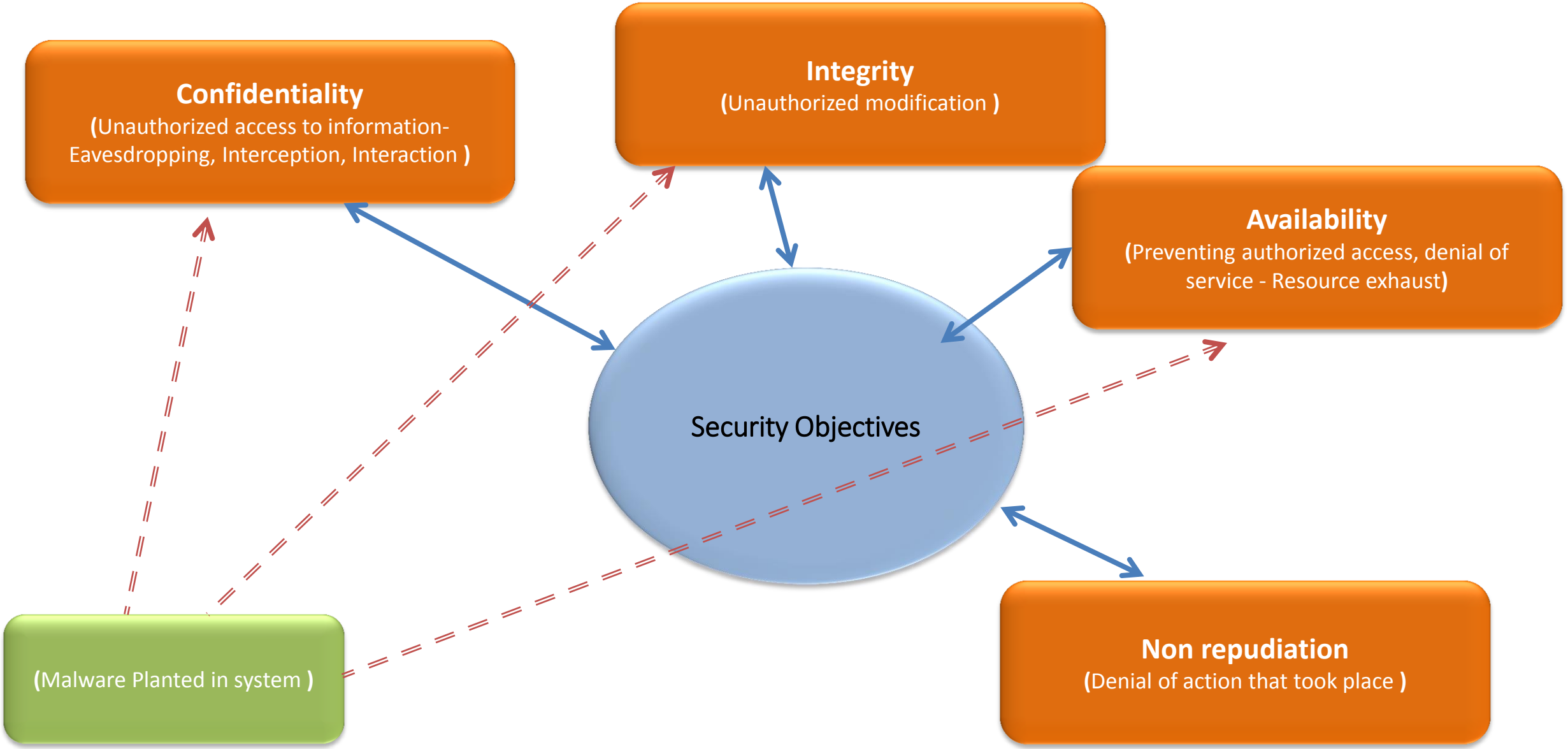
Diagram copy of illustration on page 5 within :- *'Cloud Security – A comprehensive Guide to Secure Cloud Computing'* – Author's Ronald L Krutz and Russell Dean Vines'

Offering over Networks …..



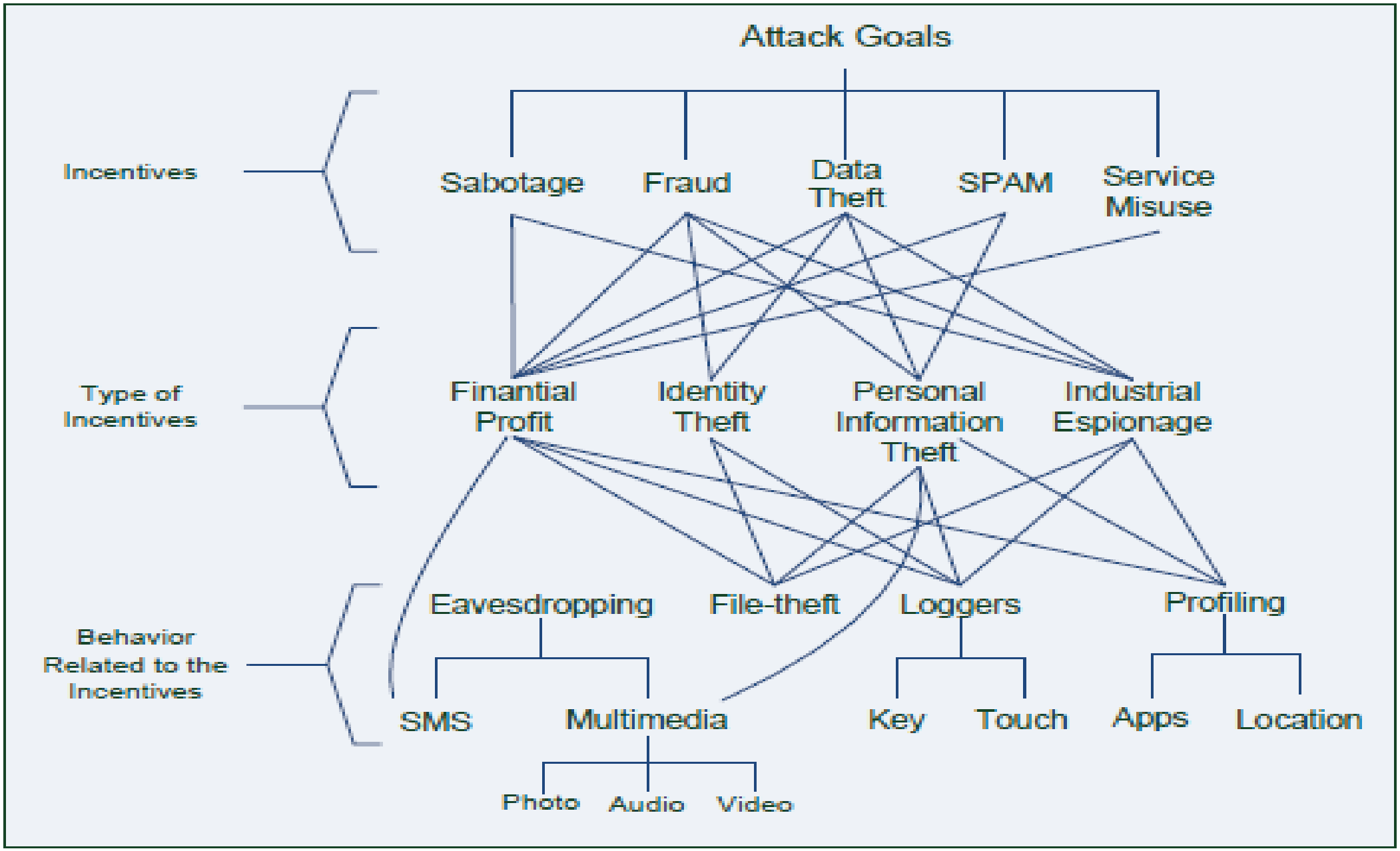
IoT evolution….

Security Challenges



CIA: Threats and Attacks

Malware attack goals, incentives, behaviour



Evolving Threat landscape....

	Conventional threats	Advanced Persistent Threats (APT)
Who are the attackers?	Opportunistic hacker	Well-resourced determined adversary
What they target?	Personal information, Credit card data, Bank data	High value digital assets: e.g. IPR, National Security data, Critical Infrastructure Control, Trade secrets, Source code, R&D details, etc.

	conventional	APT
What do they do with Information ? Who Buy?	Information could be used or sold to many interested parties	Pursued or sold to a defined party
Target?	Broad based attacks	Selected target (individual, organization, government)
Why?	Financial gain, Identity theft, Fraud, Recognition,	Damage to critical infrastructures, Market manipulation, Strategic /Competitive advantage, politically driven
How?	Gain entry by attacking perimeter	By exploiting end users, end points, attack using multiple vectors

	conventional	APT
Malware used?	Typically off-the-self malware, Propagate malware broadly	Often custom designed, tailored malware Targeted use of malware for one organization/system, create diversions, establish back doors
Skills required?	Traditional technical skills	Reconnaissance; in depth knowledge of organization's people, business process, network etc.
Reaction to counter measures?	Move to an easier target	Modify attack to pursue target further

Modern attacks

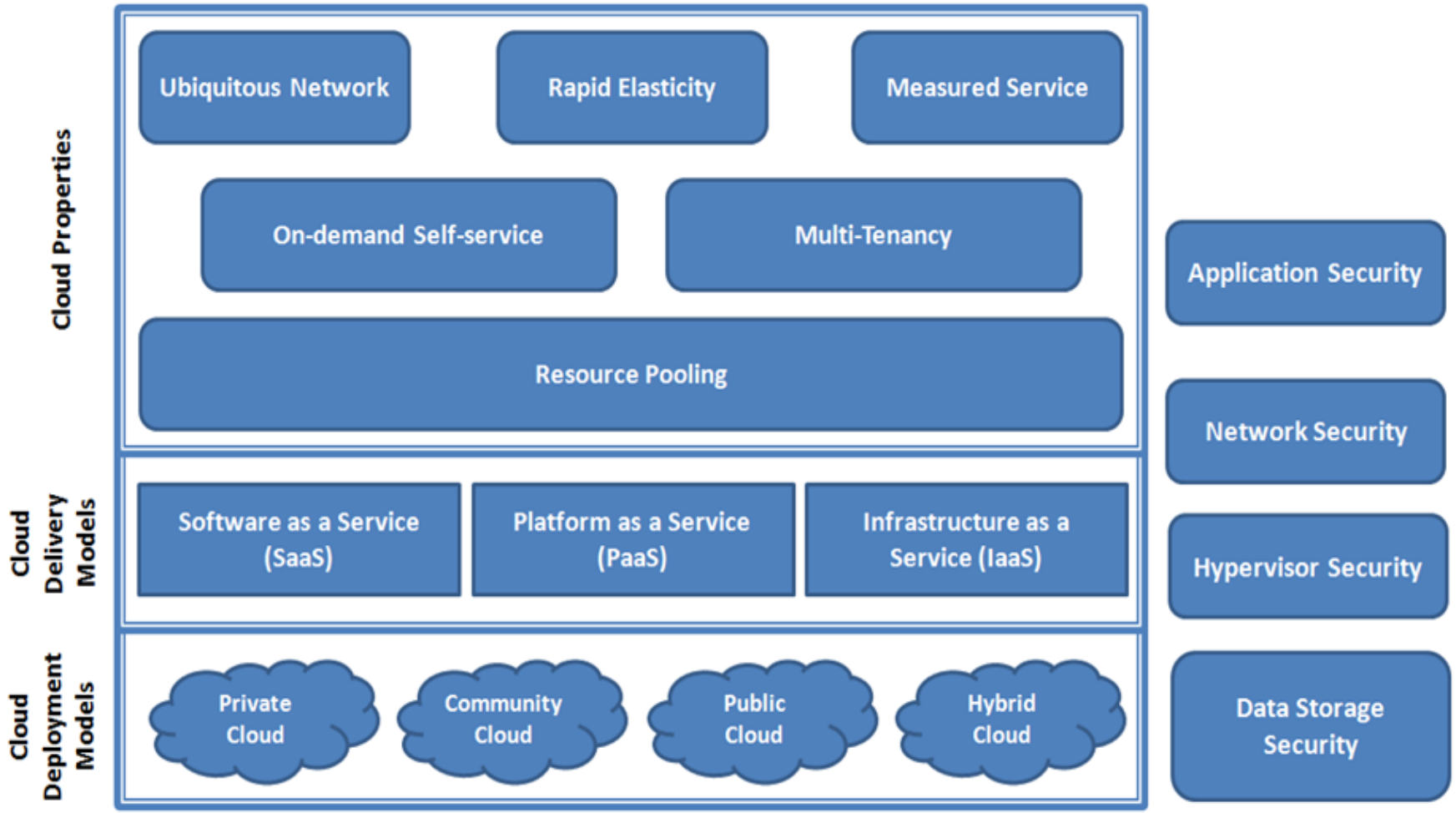
- StuxNet //a targeted multi-purpose data collection tool
- Regin //sophisticated malware toolkit
- Targets:
- Telcos, Govt. setups, Political hqs, people
- Among computers infected worldwide by Regin, 28 percent were in Russia, 24 percent in Saudi Arabia, 9 percent each in Mexico and Ireland, and 5 percent in each of India, Afghanistan, Iran, Belgium, Austria and Pakistan (Wiki)
- Operators: G/N????

Security strategy – Perimeter Defense?? Inadequate today……

Security Threats for the Cloud

- Threat 1: Abuse and Nefarious Use of Cloud computing
- Threat 2: Insecure Interfaces and APIs
- Threat 3: Malicious Insiders
- Threat 4: Shared Technology Issues
- Threat 5: Data Loss or Leakage
- Threat 6: Account or Service Hijacking
- Threat 7: Unknown Security Profile

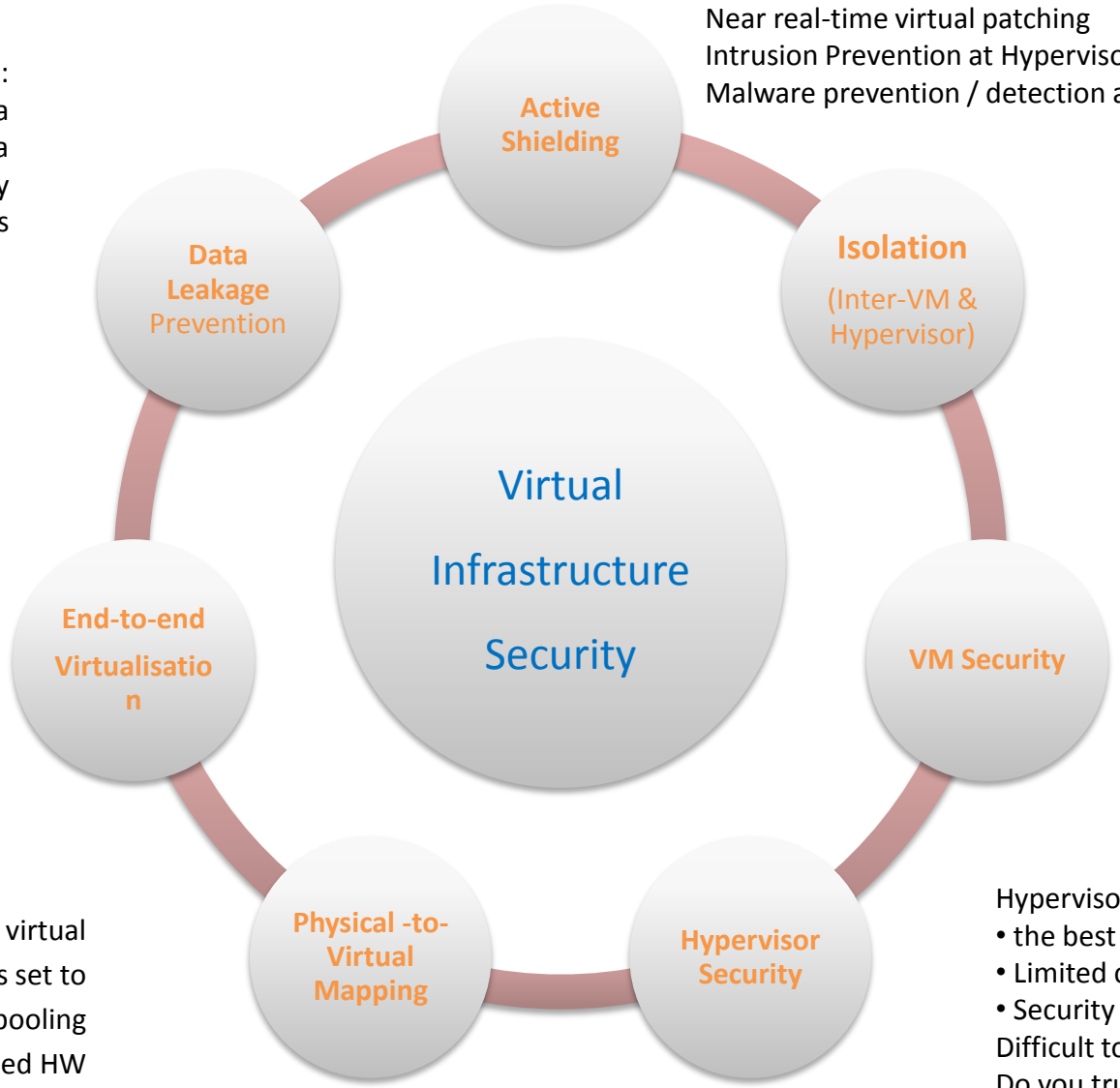
Security requirement at various levels of Cloud



Cloud Security challenges

CSPs don't:
• allow clients to classify data
• offer different levels of security based upon data sensitivity
• offer DLP services

Near real-time virtual patching
Intrusion Prevention at Hypervisor level – below Guest OS
Malware prevention / detection at Hypervisor level



Robust at system level (modulo kernel bugs)
Issues at management plane Memory hijacking

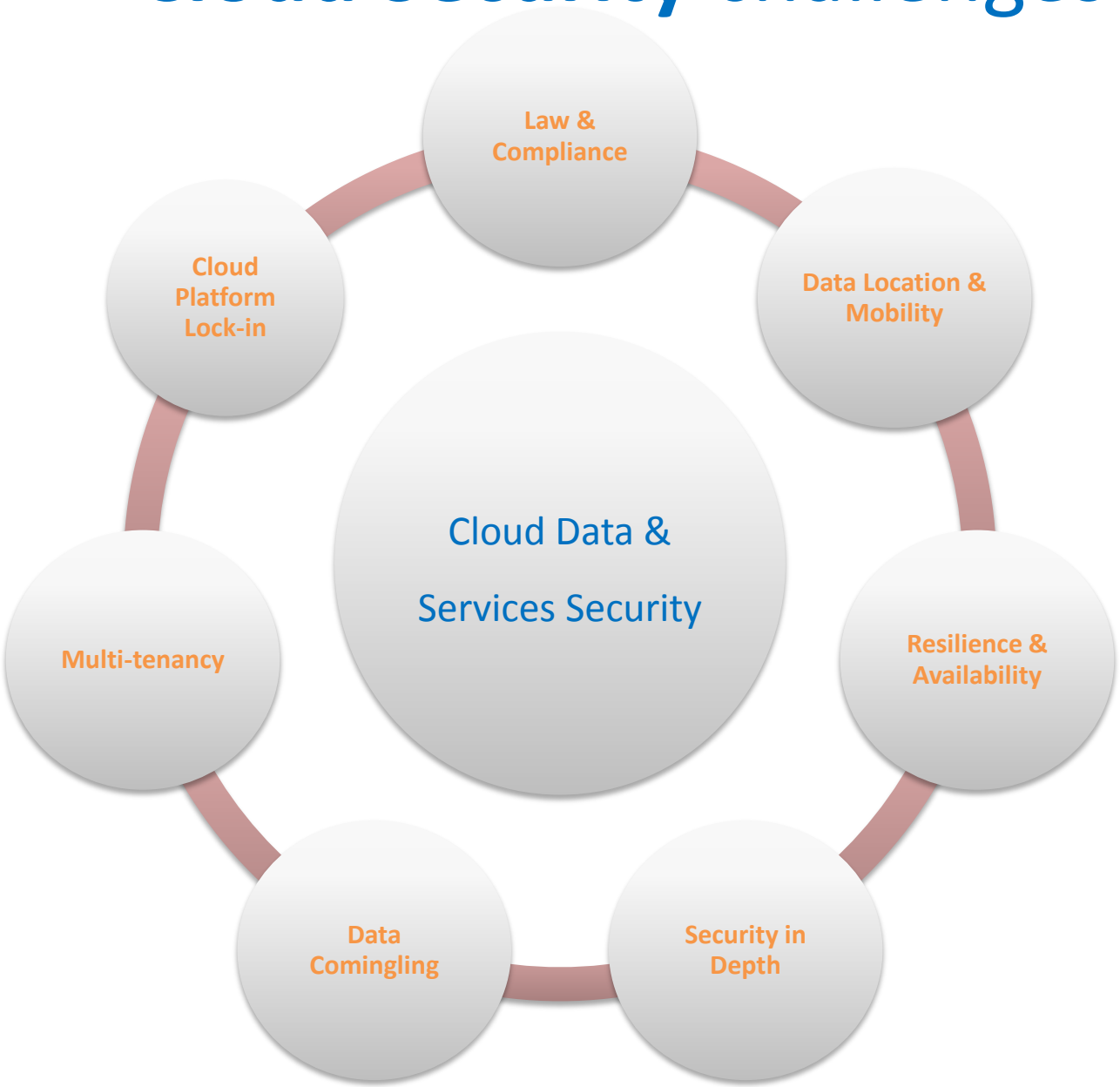
Co-ordinate security policies & provisioning for network & server virtualisation
Location/resource optimisation

Guest OS needs security protection
Resilient VM lifecycle
• dynamic
• at massive scale

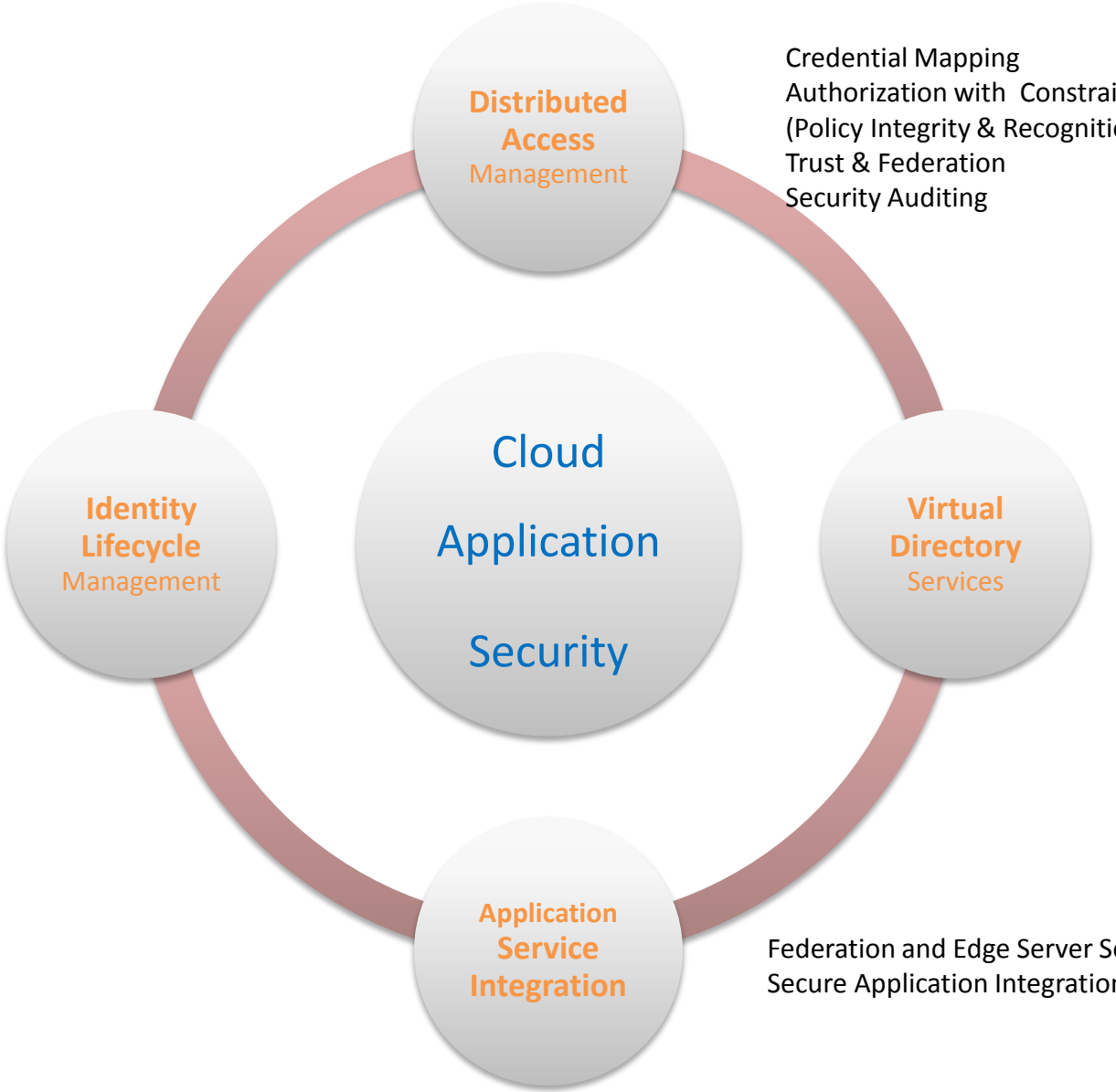
Crypto doesn't like virtual
Current algorithms set to optimise resource pooling
Can't always use specialised HW
Encryption key management

Hypervisor / trusted VM:
• the best place to secure
• Limited compute resources
• Security API standards
Difficult to exploit but high-impact
Do you trust Microsoft?
Do you trust VMWare?

Cloud Security challenges



Cloud Security challenges



Credential Mapping
Authorization with Constrained Delegation
(Policy Integrity & Recognition of Authority)
Trust & Federation
Security Auditing

Provisioning
Identity Integration
User Management
Credential Management
Entitlement Management
Device Credentials, PKI Infrastructure

Active Directory/LDAP - Attributes, Credentials and Groups for Edge servers

Federation and Edge Server Security –
Secure Application Integration Fabric (Secure ESB Gateway)

Application Level Security Issues

- Vulnerabilities in web applications, web browsers or in APIs
  - Injection attacks
- Service availability
  - Temporary/Permanent loss of service
  - DoS/DDoS
- Integrity of workload state
  - Ensure expected results

Network Level Security Issues

- Vulnerabilities in Internet protocols
  - Spoofing and flooding attacks
- Authorization and Access Control
- Network based Intrusions
  - DoS, DDoS affect service availability
- Backdoor Channel Attack
  - Hacker can gain remote access
- Service Hijacking

Virtualization/Hypervisor Level Security Issues

- Vulnerabilities in virtualization
- Virtualization based malware and rootkit
  - Bluepill for AMD-V
  - Vitriol for Intel VT
- Security in Virtual Machine Image Repository

Data Storage Level Security Issues

- Data Integrity, Confidentiality and Availability
- Data Breaches
- Data Recovery
- Data locality
- Data segregation

Test bed @ NIT Surat

- high end servers,
  - IBM blade center
  - 4 blades – 396 GB RAM, 140 cpu cores, 20 TB storage
  - Dell Poweredge R710
    - 2 X Quad Core Processor (Dual Thread)
    - 32GB RAM, 600 GB SAS HDD
  - HP Proliant
    - 2 X Quad Core Processor
    - 8GB RAM, 1TB SATA HDD
- Setup open source Cloud frameworks delivering IaaS
  - Eucalyptus
  - VMware ESXi Server

Data Storage Security Model: Design Goals

- Confidentiality
- Light weight integrity verification
- Flexible security options
- No data duplication

DSSM: Entities

Cloud Service Provider (CSP)

-Central secure data storage repository
-Authorizes data access

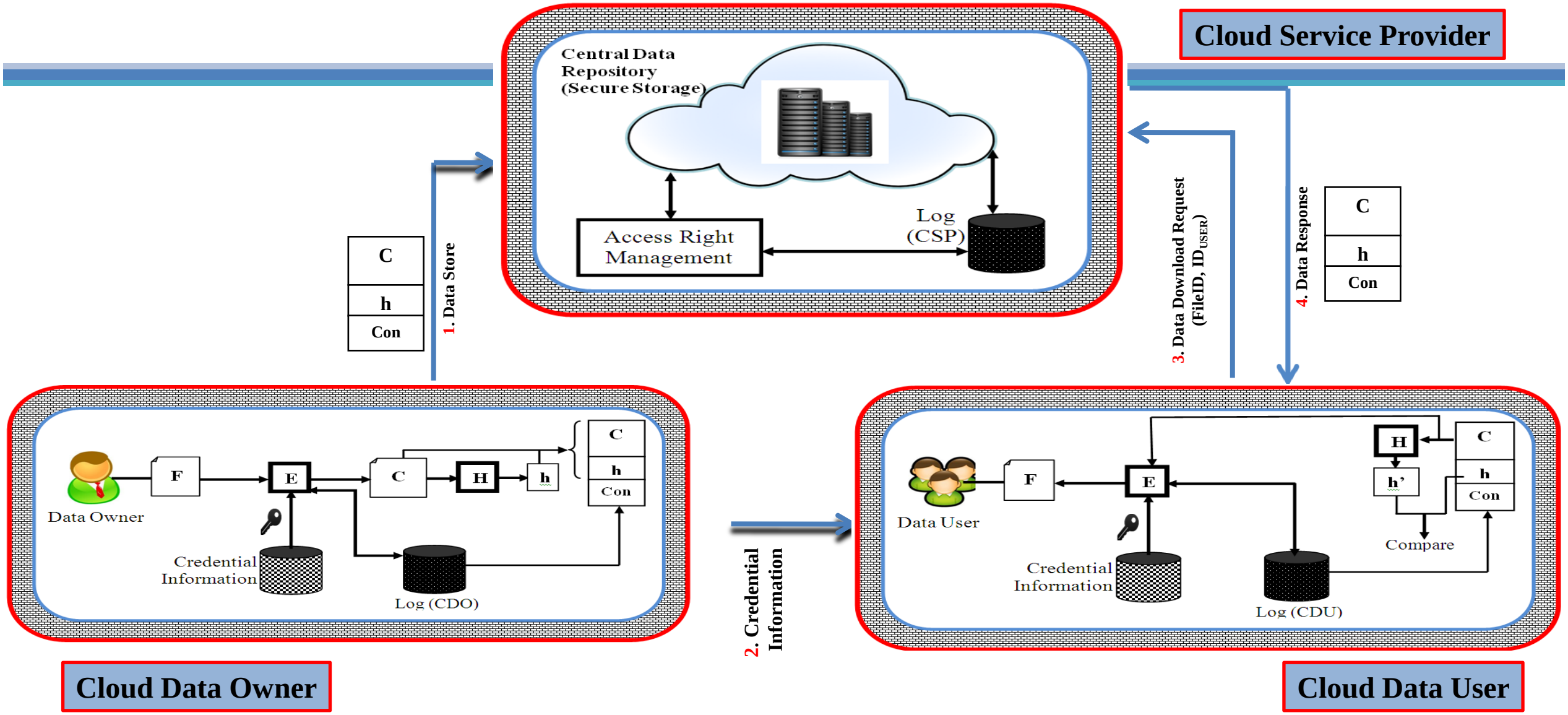
Cloud Data Owner (CDO)

- Generates data
- Passes access rights to other users
- Verifies data

Cloud Data User (CDU)

- Uses data generated by CDO
- Can read or edit data
- Verifies data

DSSM: Simplified Version

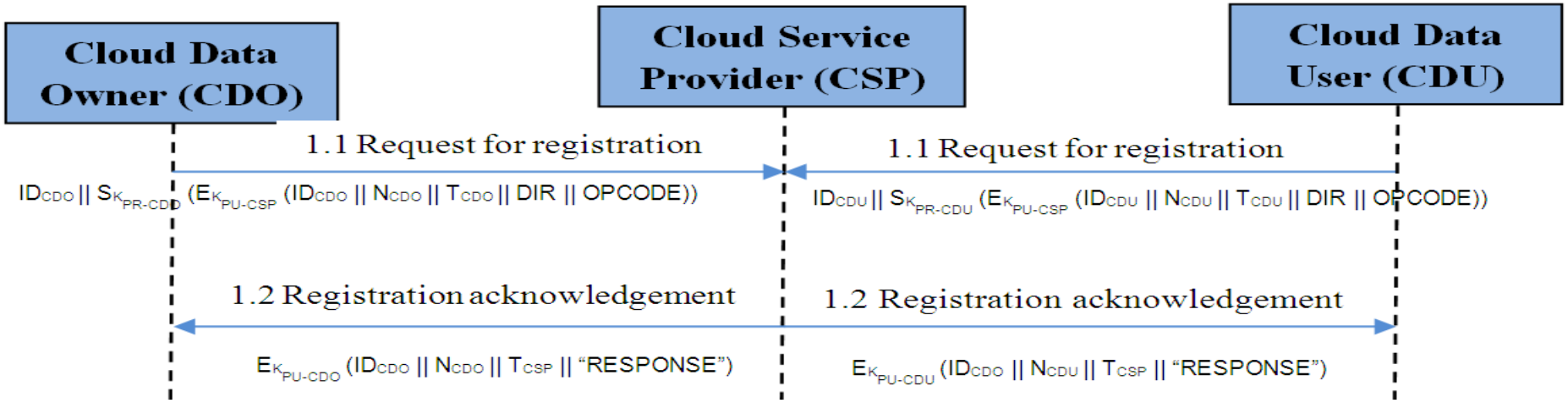


DSSM: Operational Phases

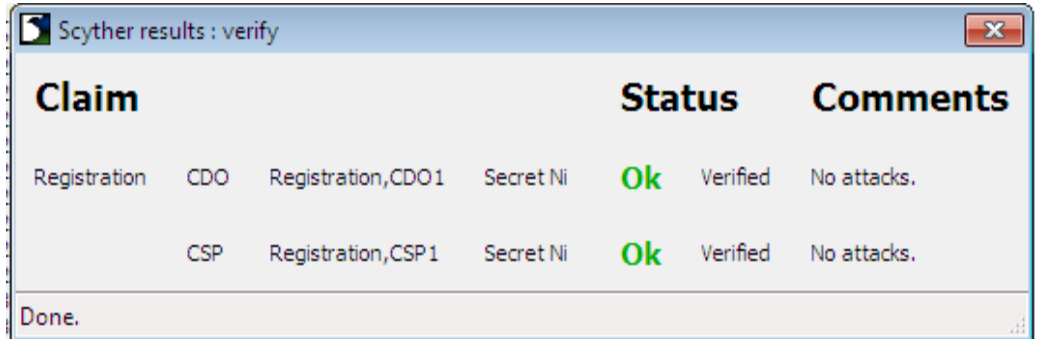
1. Registration
2. Pre-storage
3. Storage
4. Manage Access Rights
5. Data Download
6. Data Verification
7. Data Update
8. Data Delete

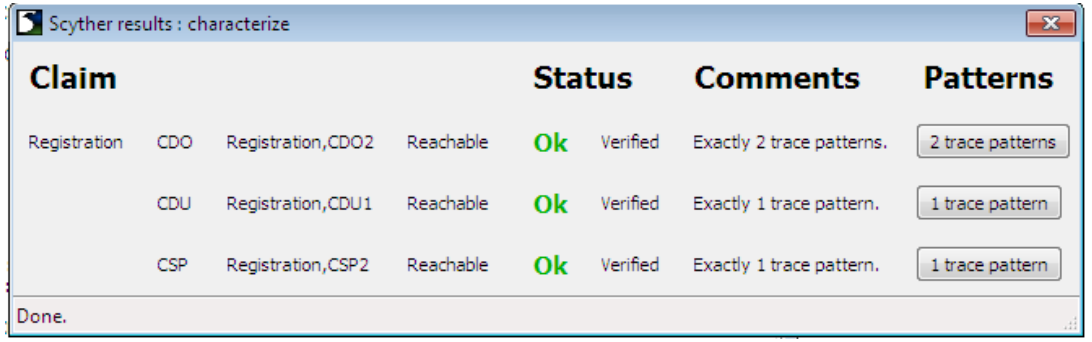
DSSM Phases: Verification Using Scyther

Registration Phase



Sequence Diagram

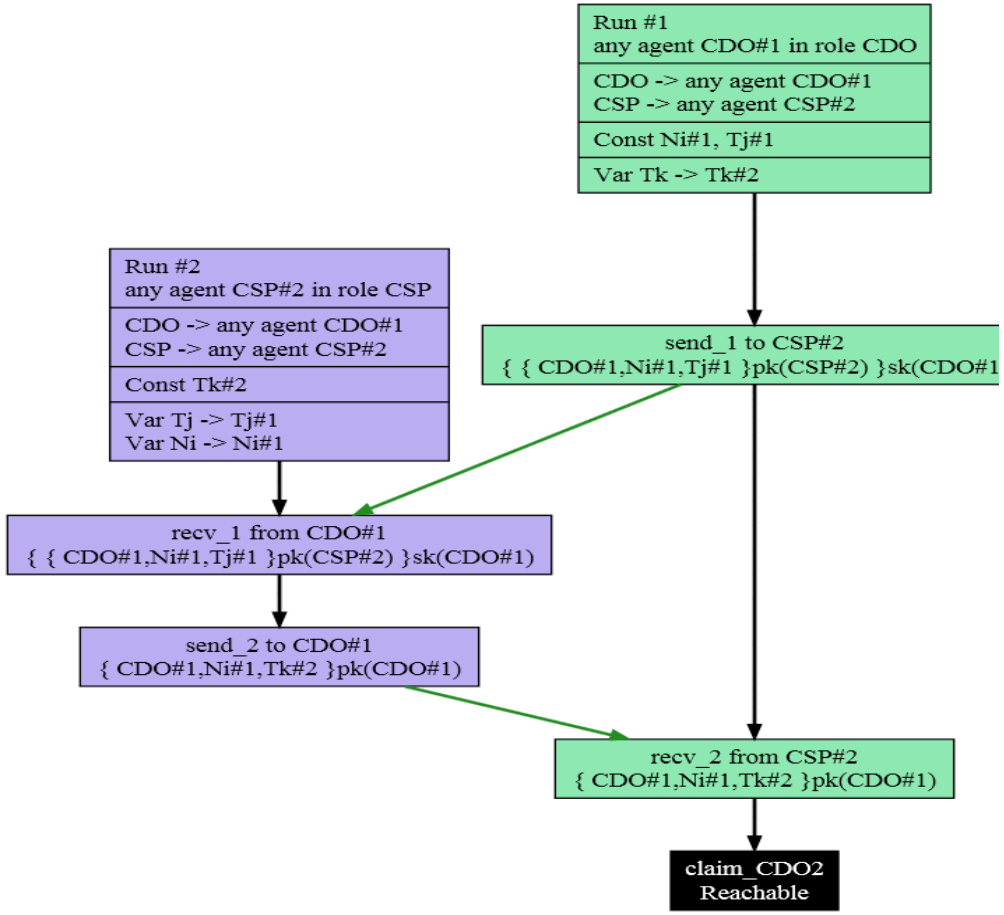




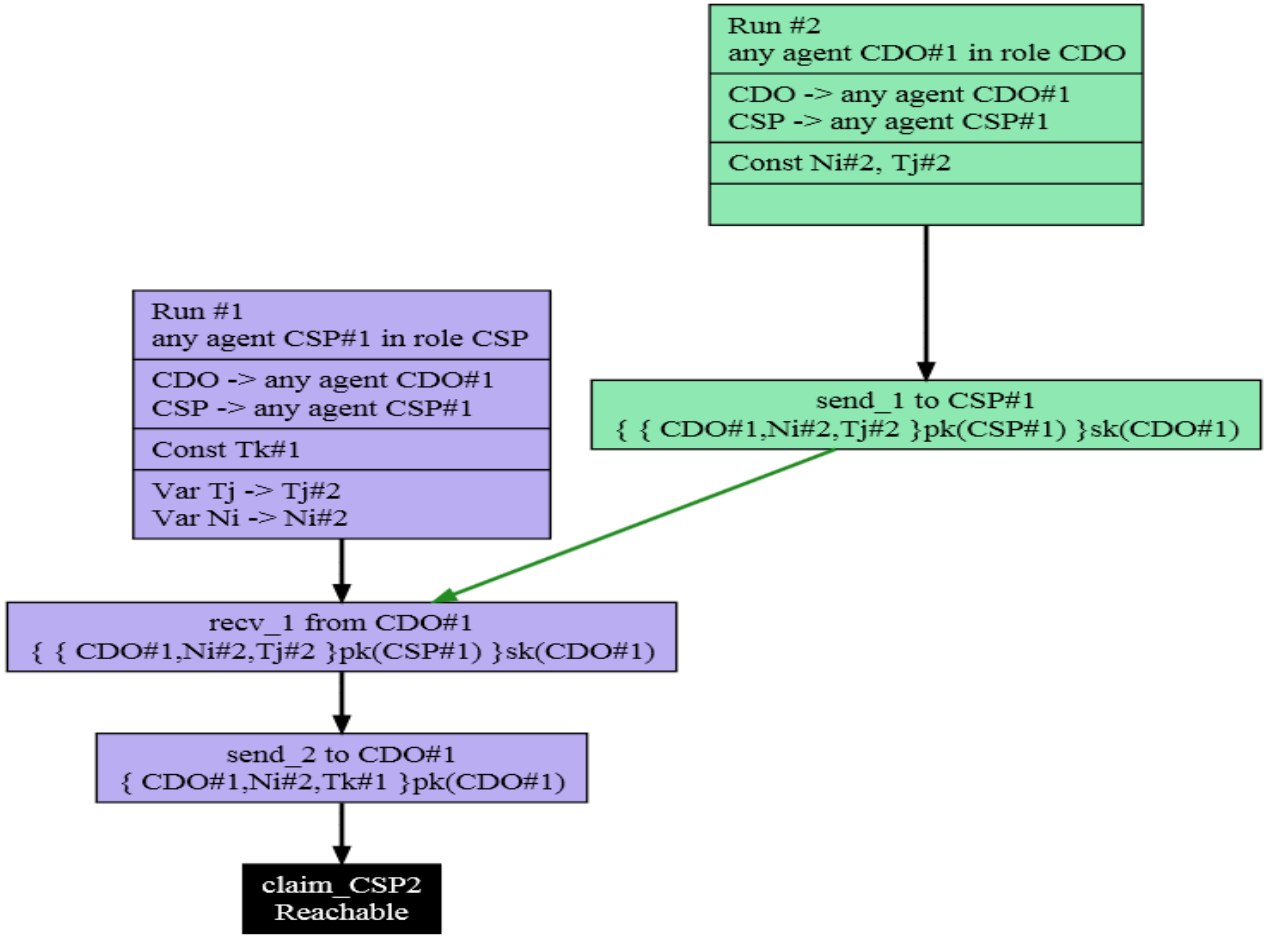
Claim Checks

DSSM Phases: Verification Using Scyther

Registration Phase



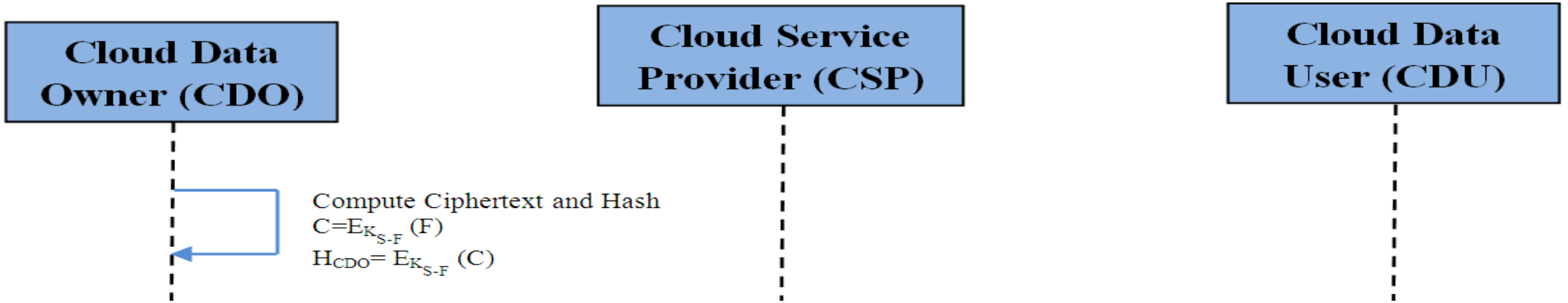
Role CDO



Role CSP

DSSM Phases: Verification Using Scyther

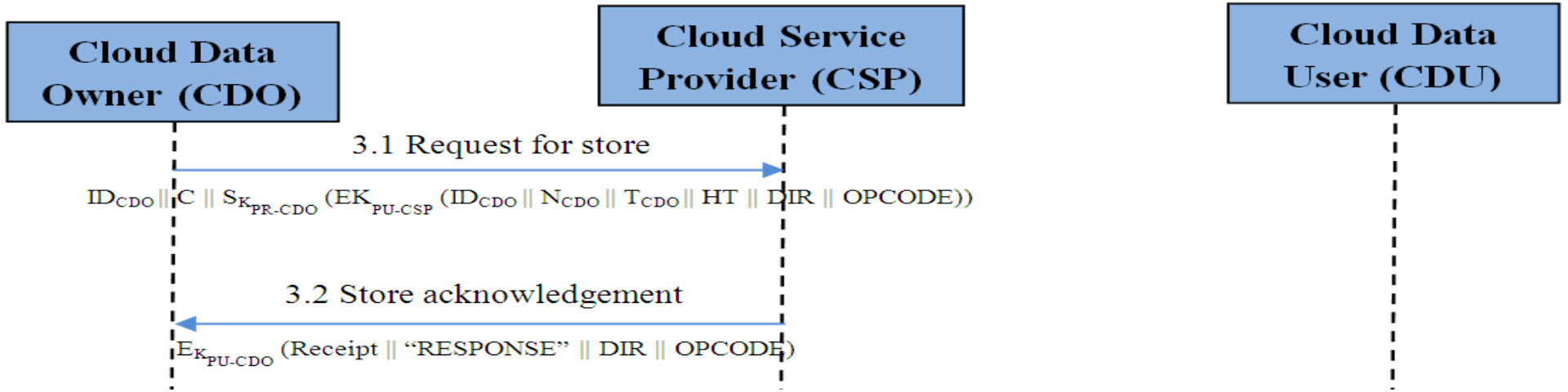
Pre-Storage Phase



Sequence Diagram

DSSM Phases: Verification Using Scyther

Storage Phase



Sequence Diagram

Scyther results : verify

Claim				Status		Comments
Storage	CDO	Storage,CDO1	Secret Ni	Ok	Verified	No attacks.
	CSP	Storage,CSP1	Secret Ni	Ok	Verified	No attacks.

Done.

Scyther results : characterize

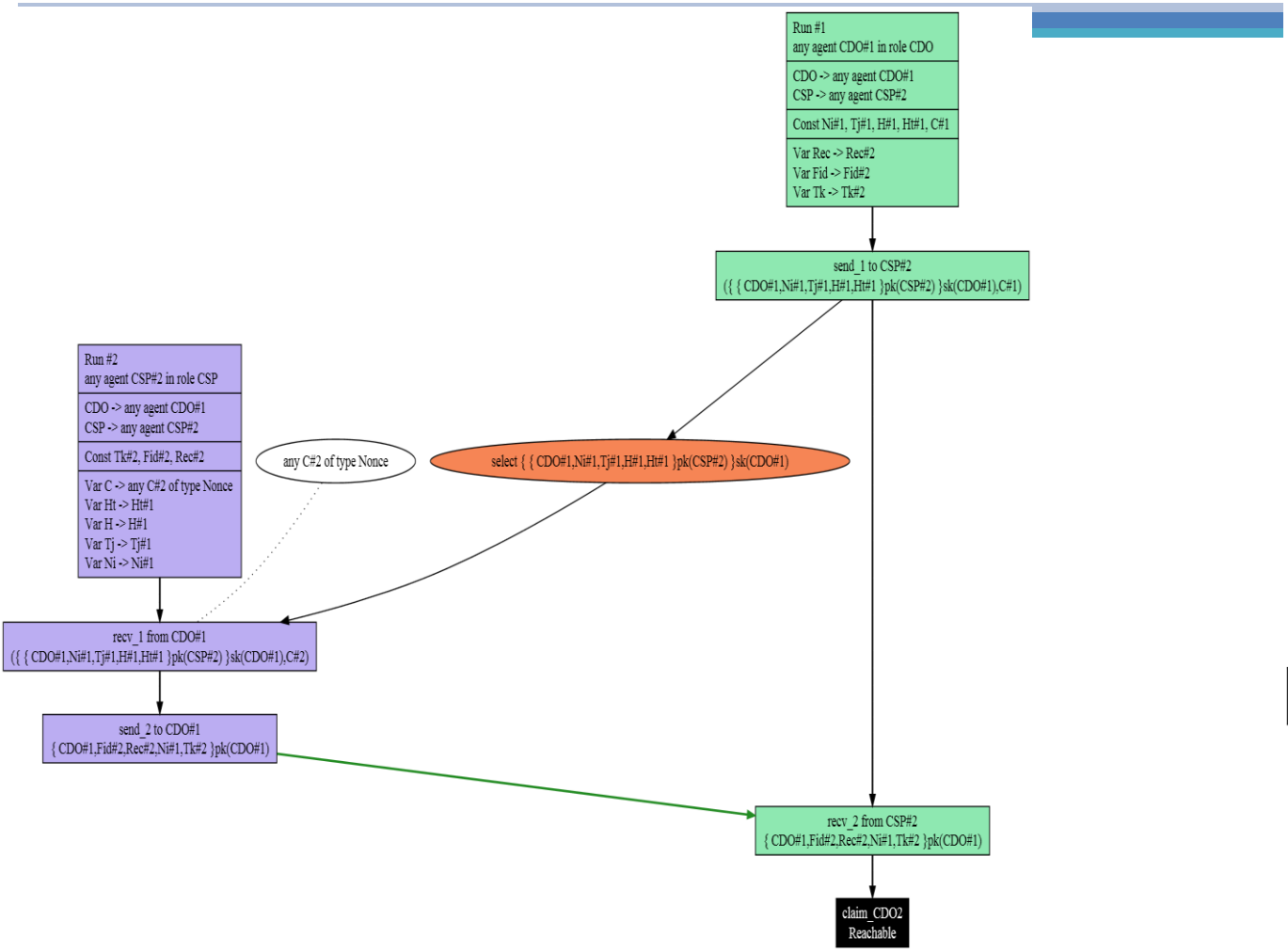
Claim				Status		Comments	Patterns
Storage	CDO	Storage,CDO2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	CDU	Storage,CDU1	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	CSP	Storage,CSP2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern

Done.

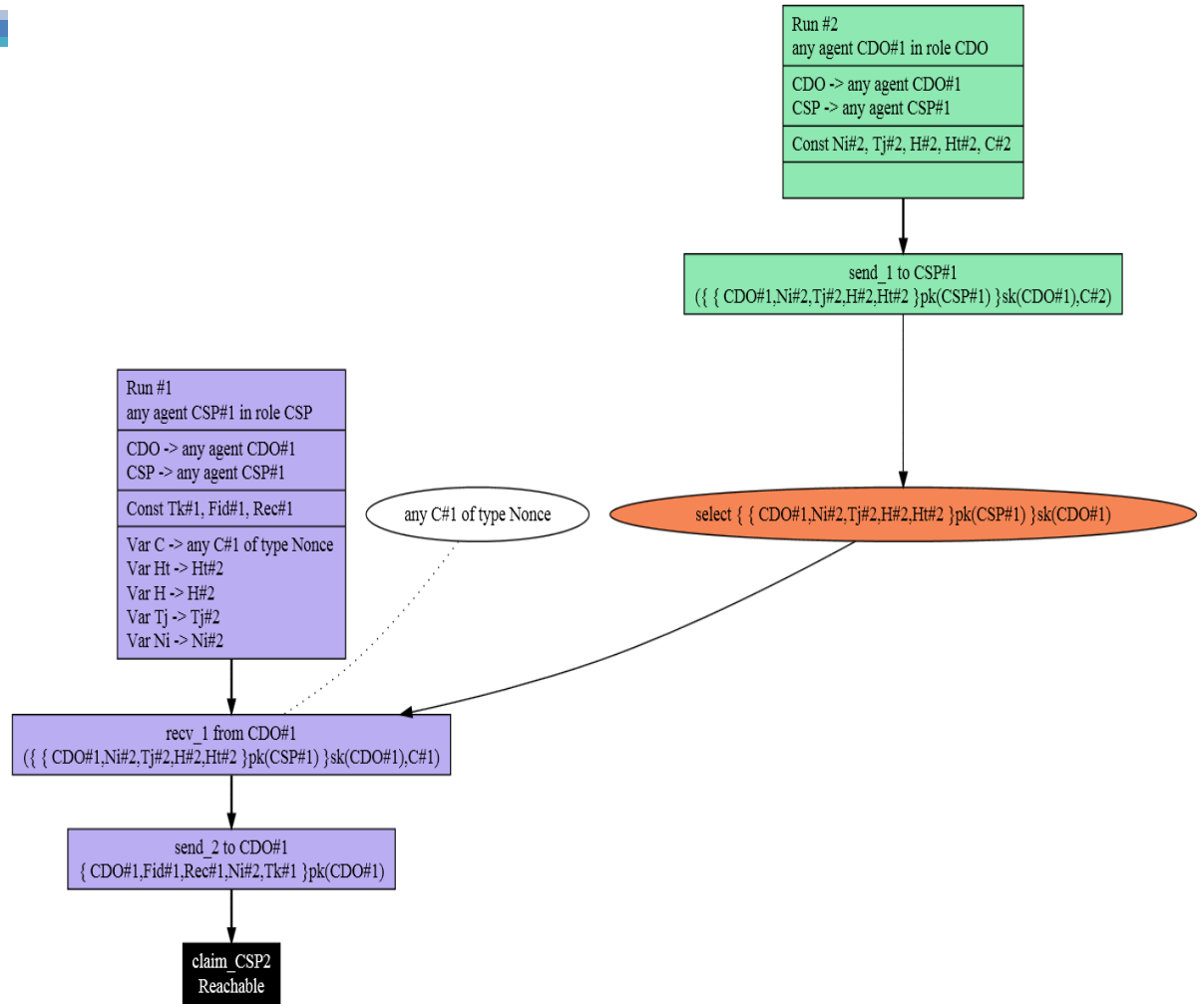
Claim Checks

DSSM Phases: Verification Using Scyther

Storage Phase



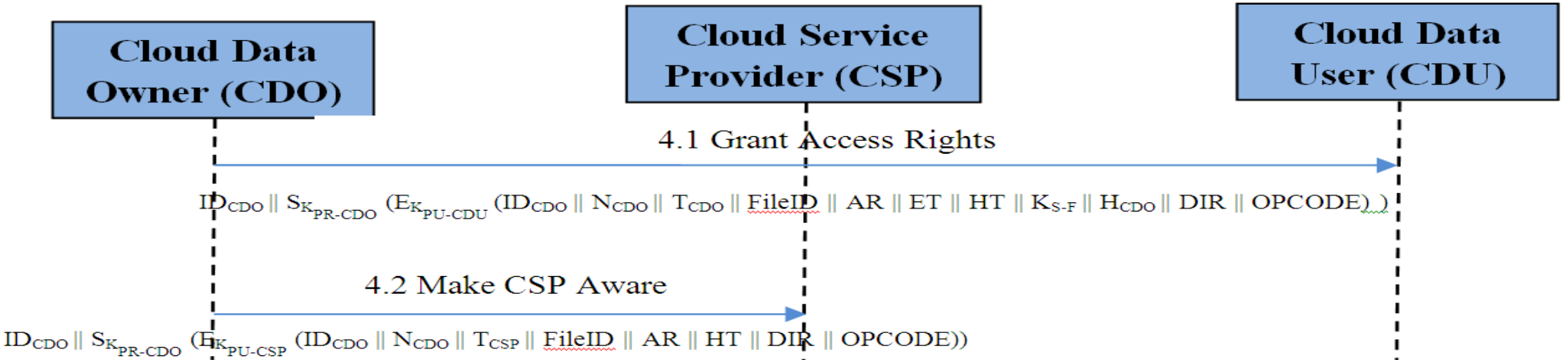
Role CDO



Role CSP

DSSM Phases: Verification Using Scyther

Manage Access Right Phase



Sequence Diagram

Scyther results : verify

Claim				Status		Comments
ManageAccessRights	CDO	ManageAccessRights,CDO1	Secret Kf	Ok	Verified	No attacks.
	CDU	ManageAccessRights,CDU1	Secret Kf	Ok	Verified	No attacks.

Done.

Scyther results : characterize

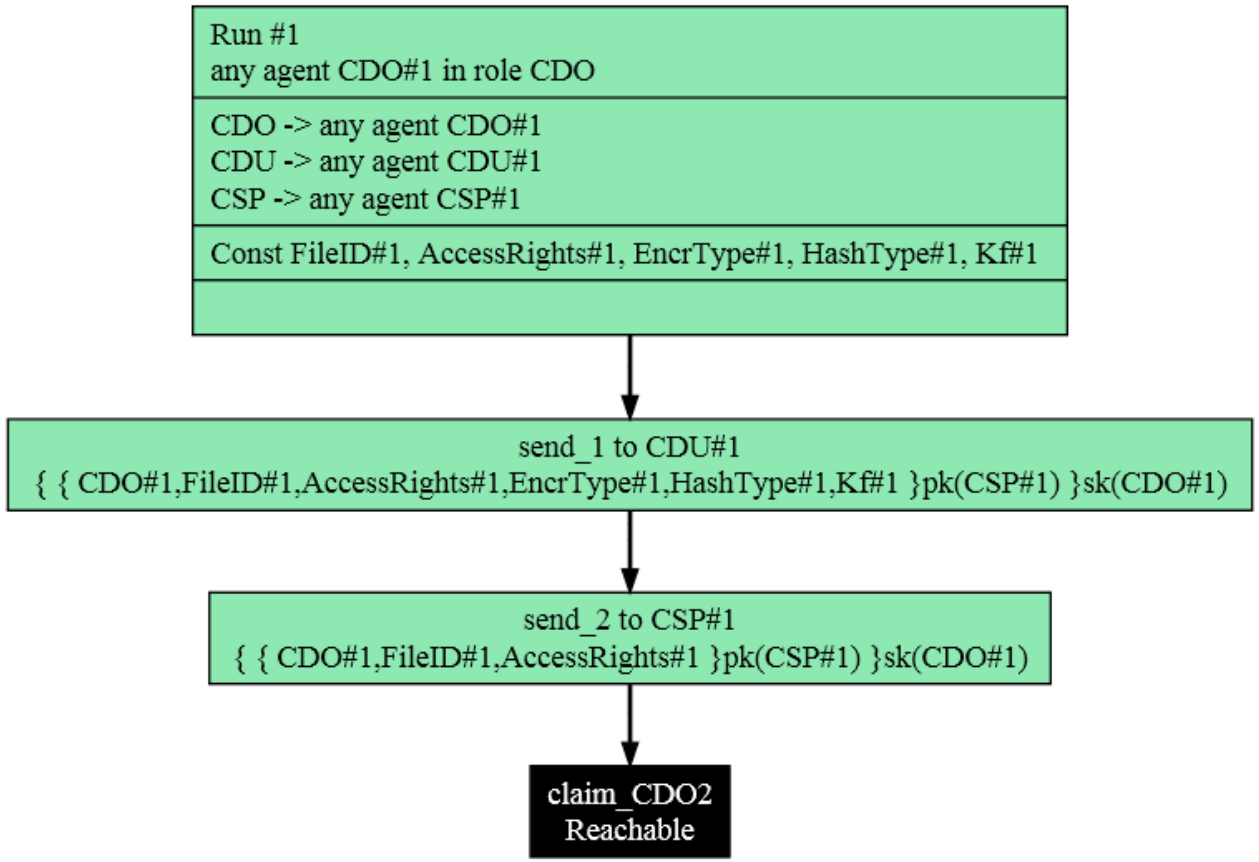
Claim				Status		Comments	Patterns
ManageAccessRights	CDO	ManageAccessRights,CDO2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	CDU	ManageAccessRights,CDU2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	CSP	ManageAccessRights,CSP1	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern

Done.

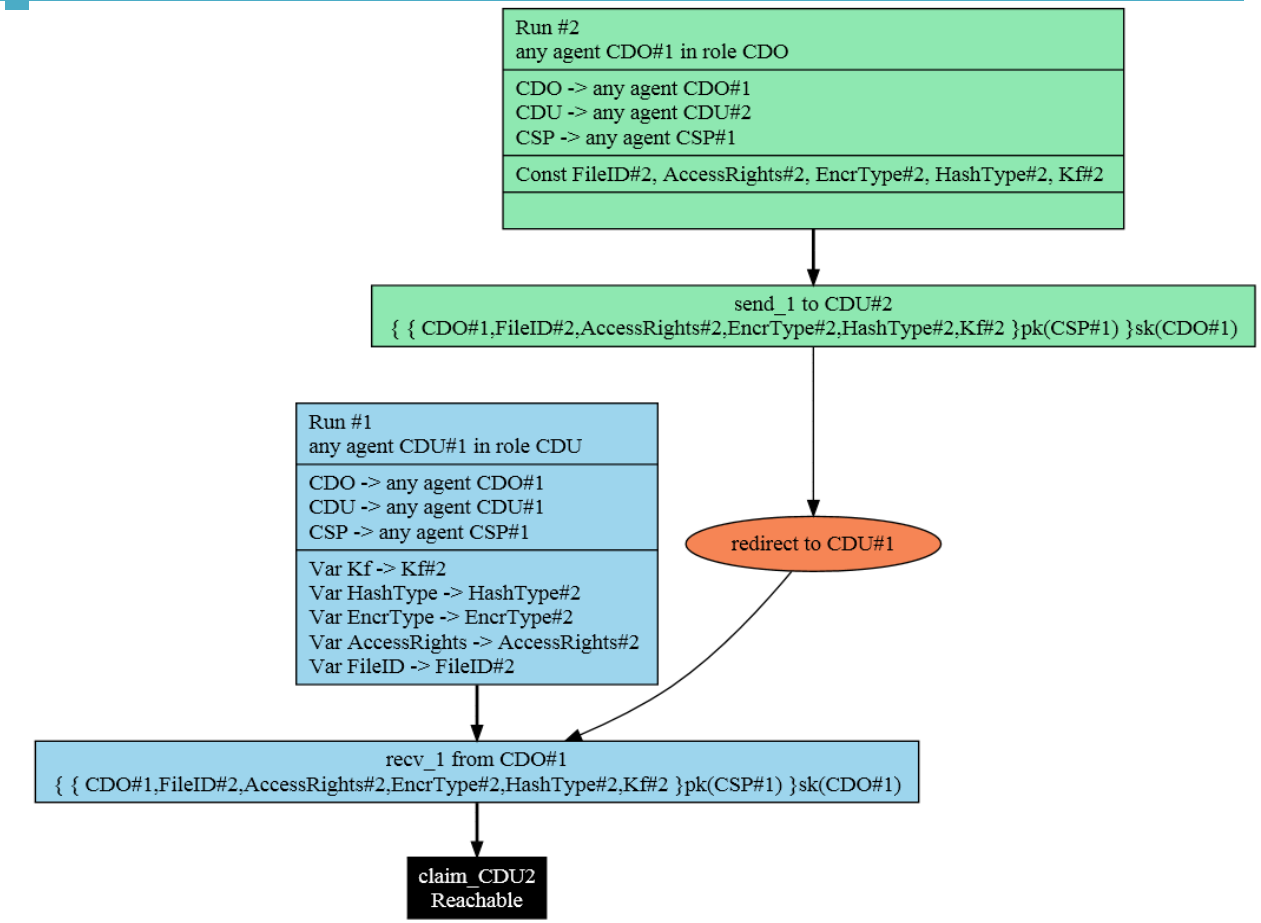
Claim Checks

DSSM Phases: Verification Using Scyther

Manage Access Right Phase



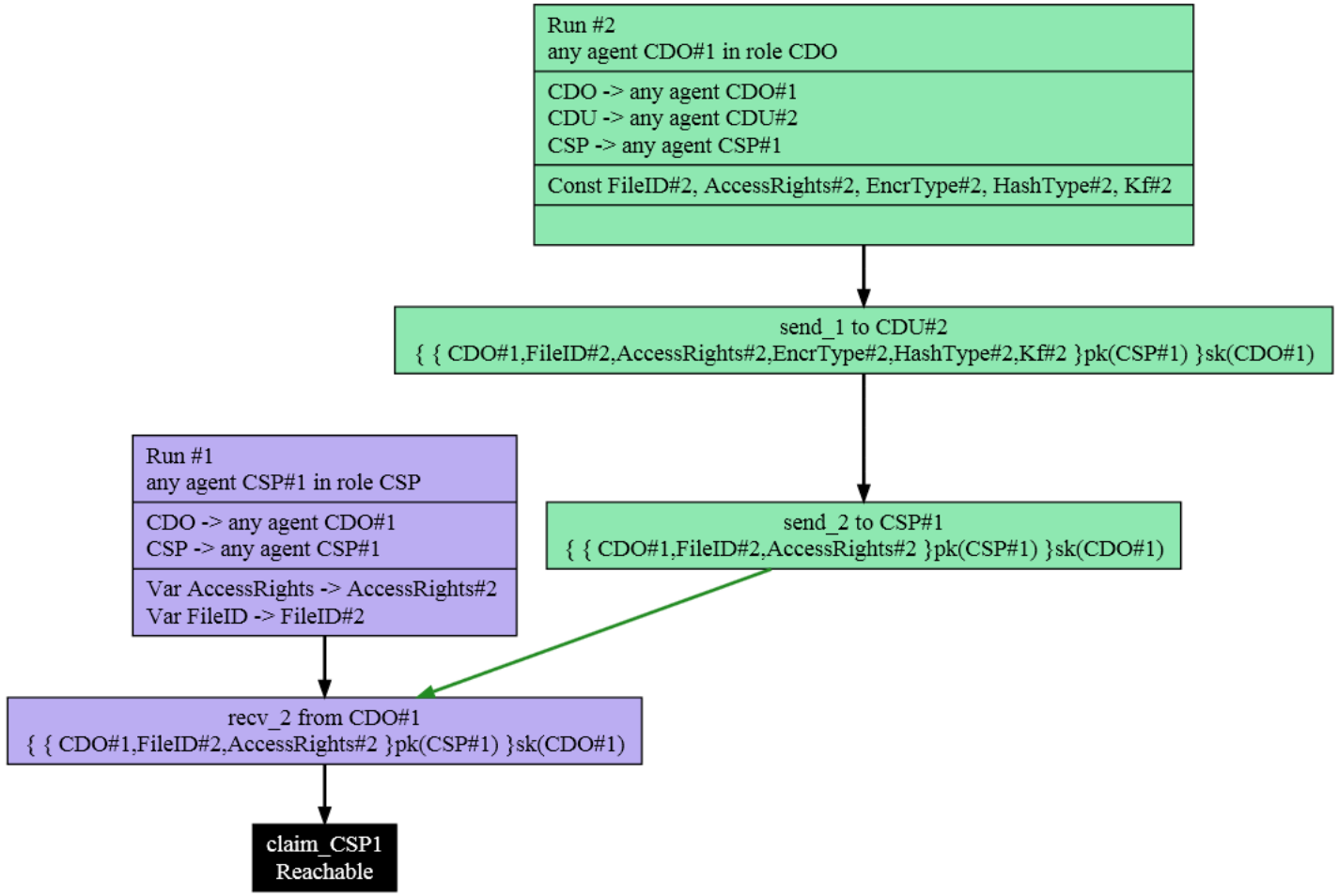
Role CDO



Role CDU

DSSM Phases: Verification Using Scyther

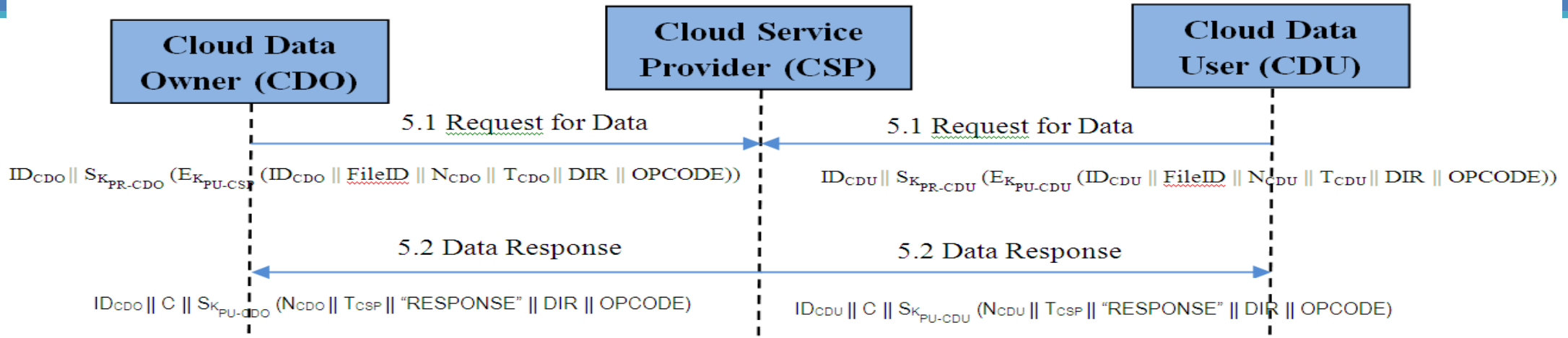
Manage Access Right Phase



Role CSP

DSSM Phases: Verification Using Scyther

Data Download Phase



Sequence Diagram

Scyther results : verify

Claim				Status		Comments
DataDownload	CDO	DataDownload,CDO1	Secret N1	Ok	Verified	No attacks.
	CDU	DataDownload,CDU1	Secret N2	Ok	Verified	No attacks.
	CSP	DataDownload,CSP1	Secret N1	Ok	Verified	No attacks.
		DataDownload,CSP2	Secret N2	Ok	Verified	No attacks.

Done.

Scyther results : characterize

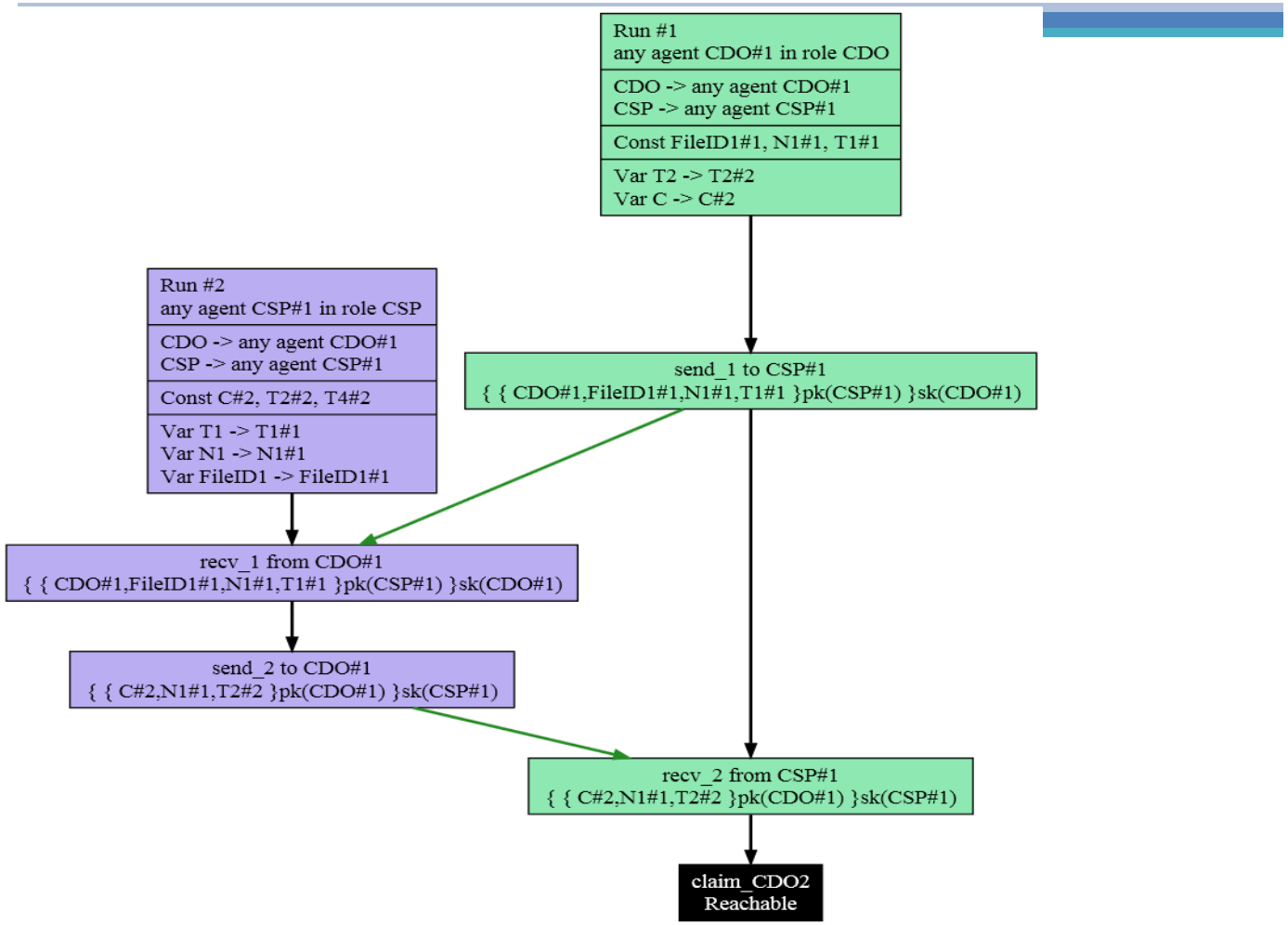
Claim				Status		Comments	Patterns
DataDownload	CDO	DataDownload,CDO2	Reachable	Ok	Verified	Exactly 5 trace patterns.	5 trace patterns
	CDU	DataDownload,CDU2	Reachable	Ok	Verified	Exactly 5 trace patterns.	5 trace patterns
	CSP	DataDownload,CSP3	Reachable	Ok	Verified	Exactly 6 trace patterns.	6 trace patterns

Done.

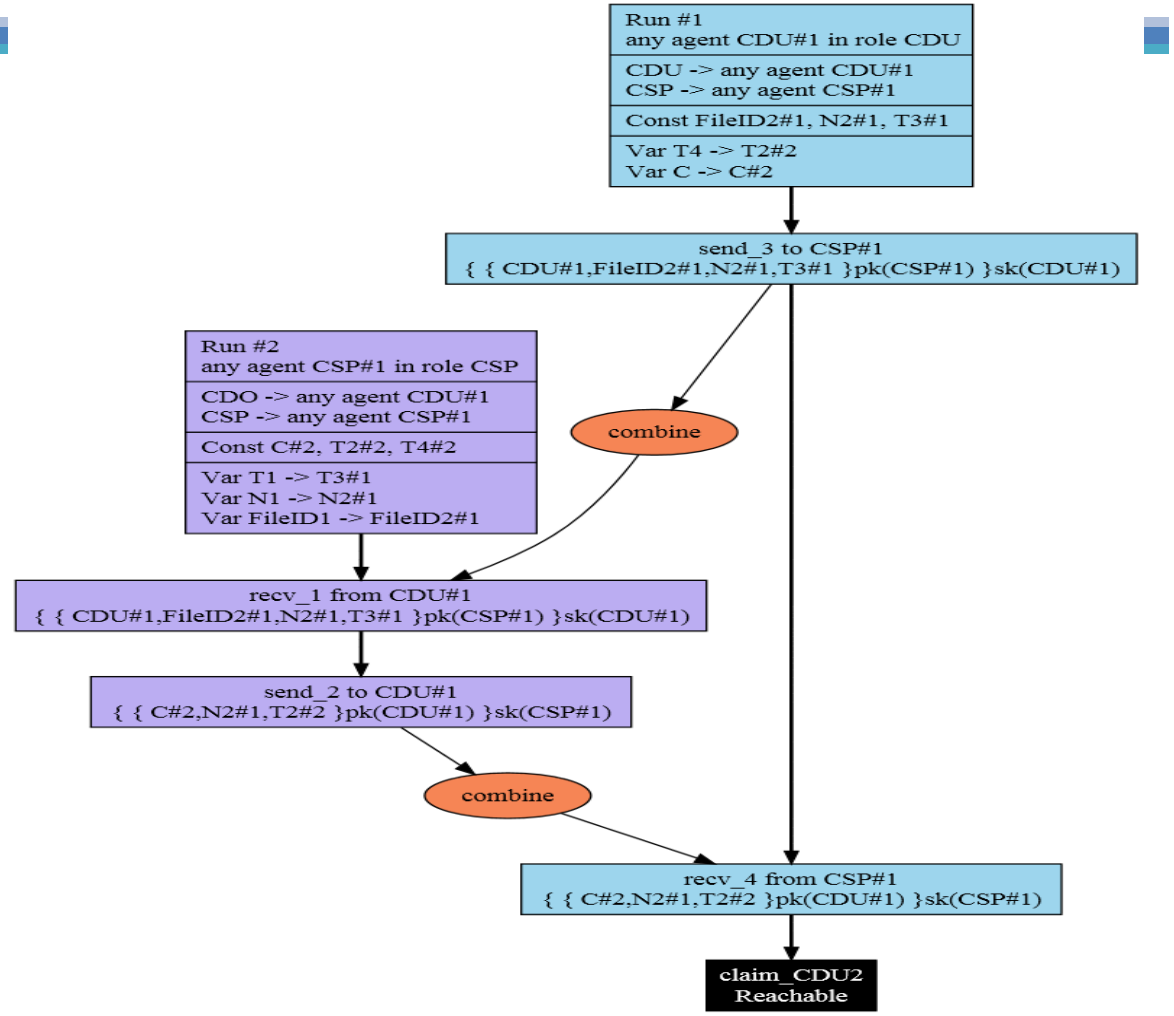
Claim Checks

DSSM Phases: Verification Using Scyther

Data Download Phase



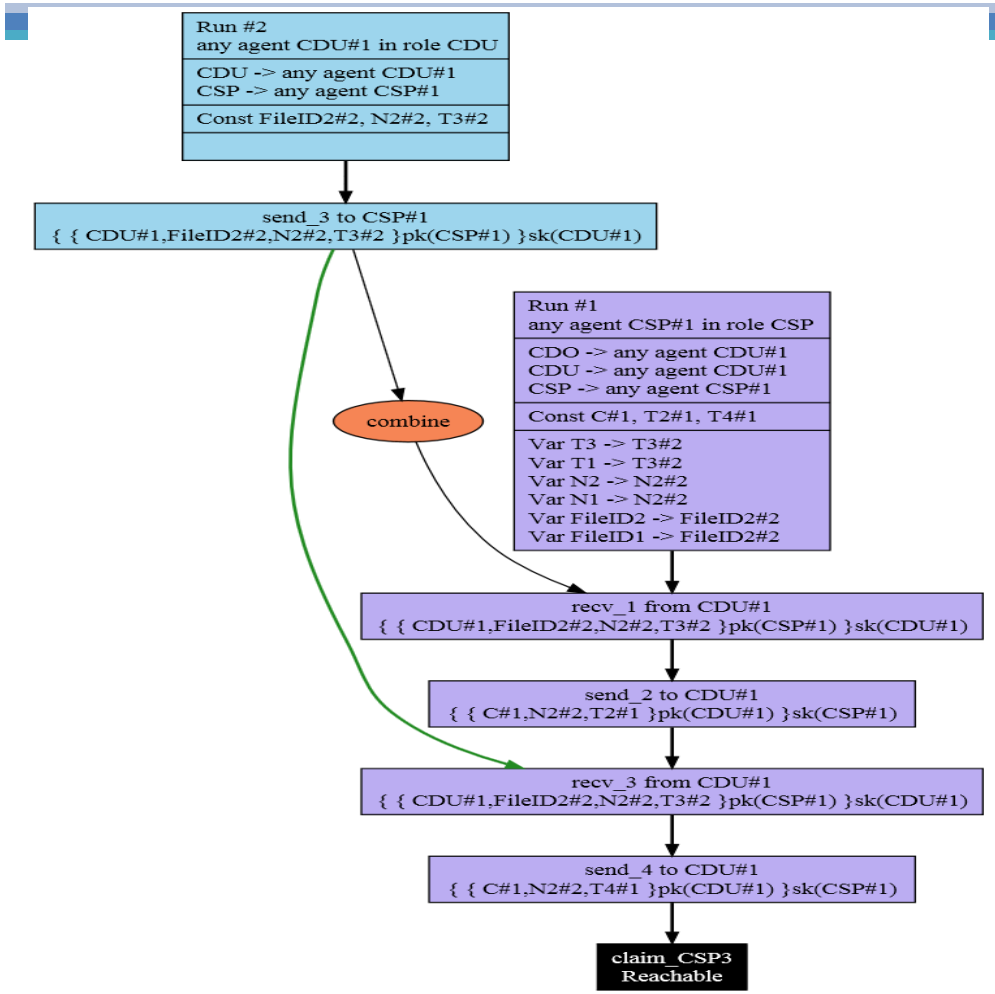
Role CDO



Role CDU

DSSM Phases: Verification Using Scyther

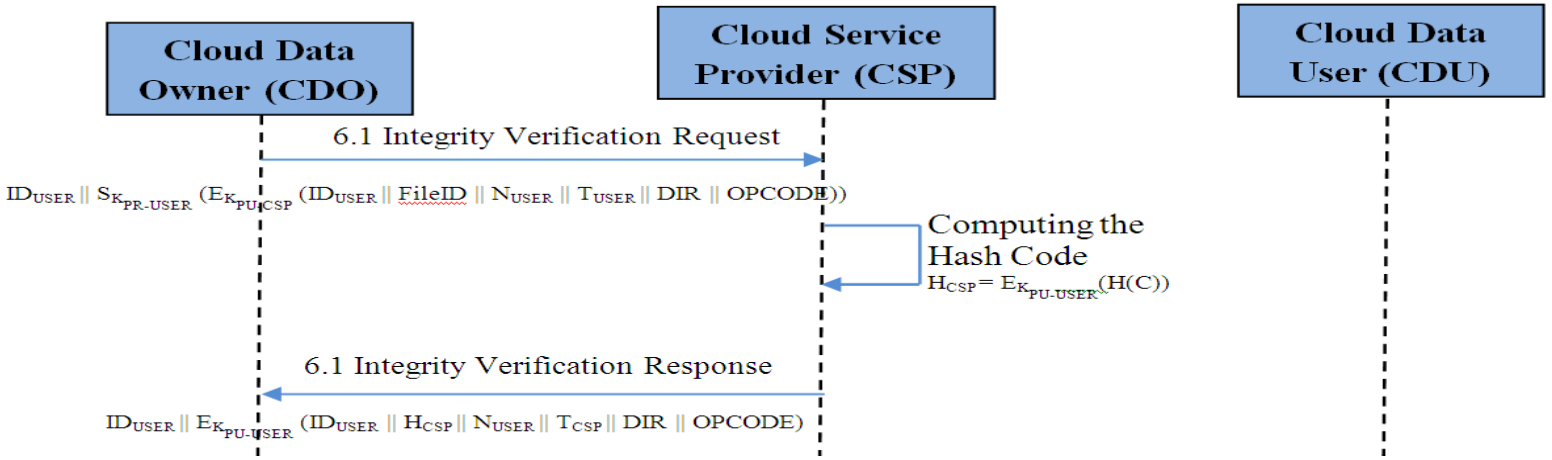
Data Download Phase



Role CSP

DSSM Phases: Verification Using Scyther

Data Integrity Verification Phase



Sequence Diagram

Scyther results : verify

Claim				Status		Comments
DataVerification	CDO	DataVerification,CDO1	Secret N1	Ok	Verified	No attacks.
		DataVerification,CDO2	Secret N1	Ok	Verified	No attacks.
	CDU	DataVerification,CDU1	Secret N2	Ok	Verified	No attacks.
		DataVerification,CDU2	Secret N2	Ok	Verified	No attacks.
	CSP	DataVerification,CSP1	Secret Hcsp	Ok	Verified	No attacks.
		DataVerification,CSP2	Secret Horg	Ok	Verified	No attacks.
		DataVerification,CSP3	Secret N1	Ok	Verified	No attacks.
		DataVerification,CSP4	Secret N2	Ok	Verified	No attacks.

Done.

Scyther results : characterize

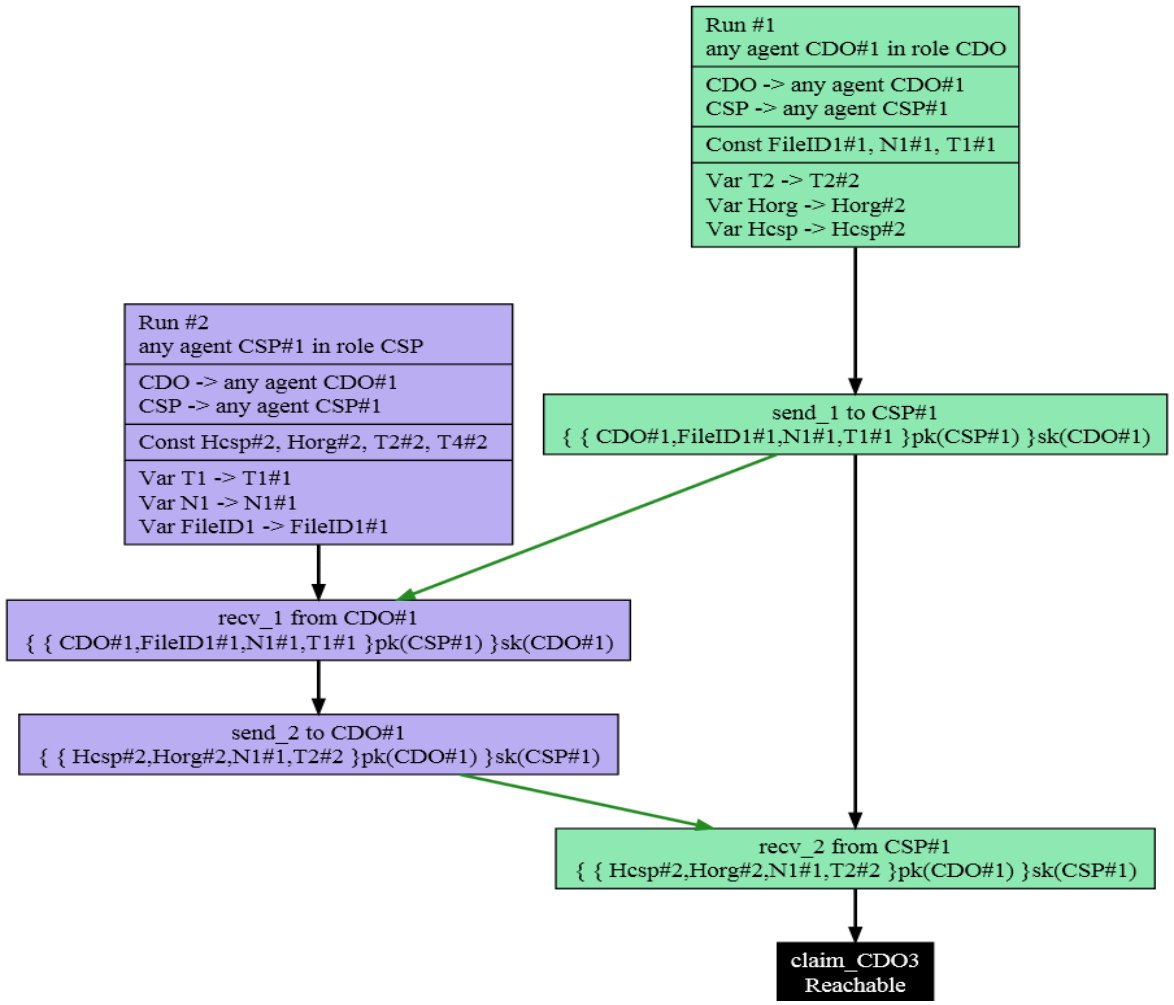
Claim				Status		Comments	Patterns
DataVerification	CDO	DataVerification,CDO3	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	CDU	DataVerification,CDU3	Reachable	Ok	Verified	Exactly 4 trace patterns.	4 trace patterns
	CSP	DataVerification,CSP3	Reachable	Ok	Verified	Exactly 6 trace patterns.	6 trace patterns

Done.

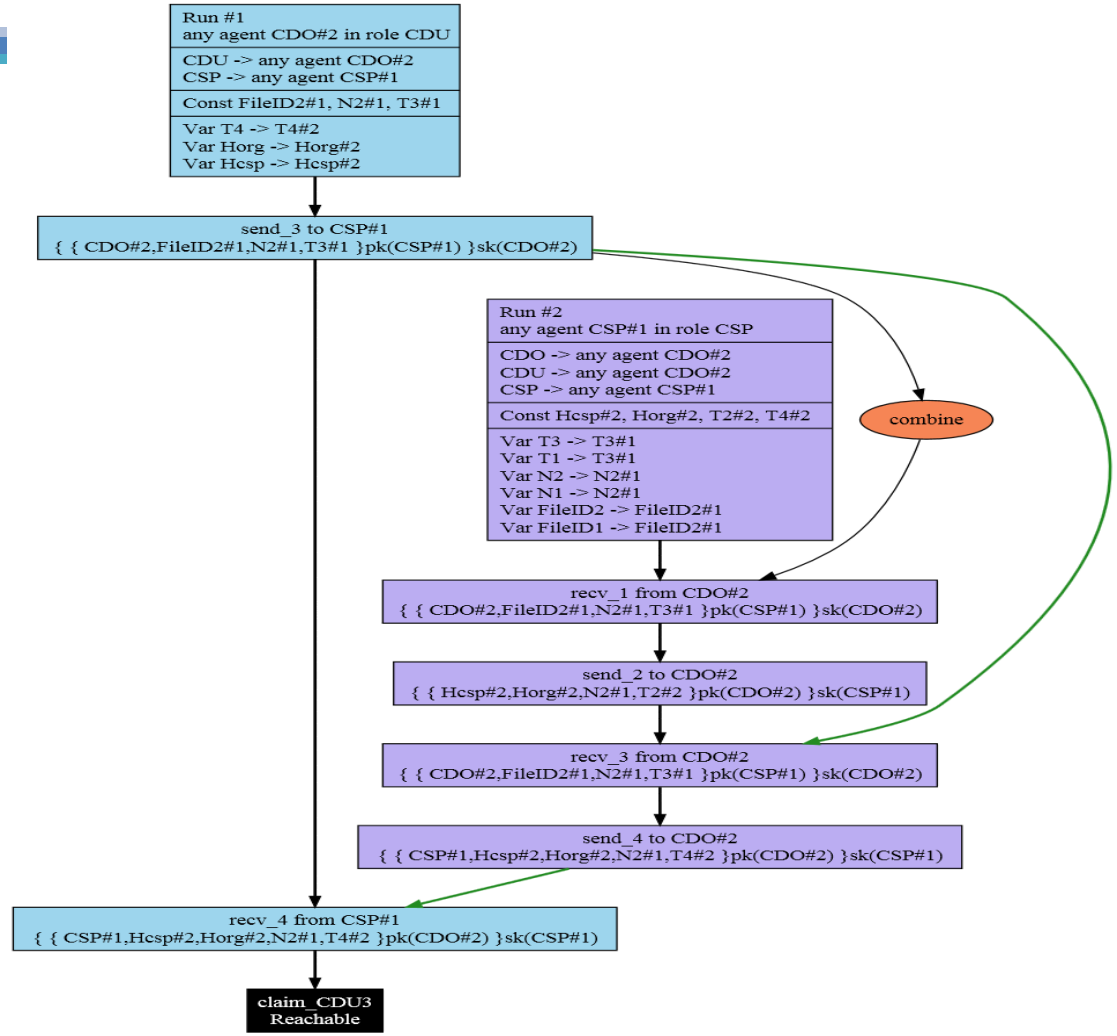
Claim Checks

DSSM Phases: Verification Using Scyther

Data Integrity Verification Phase



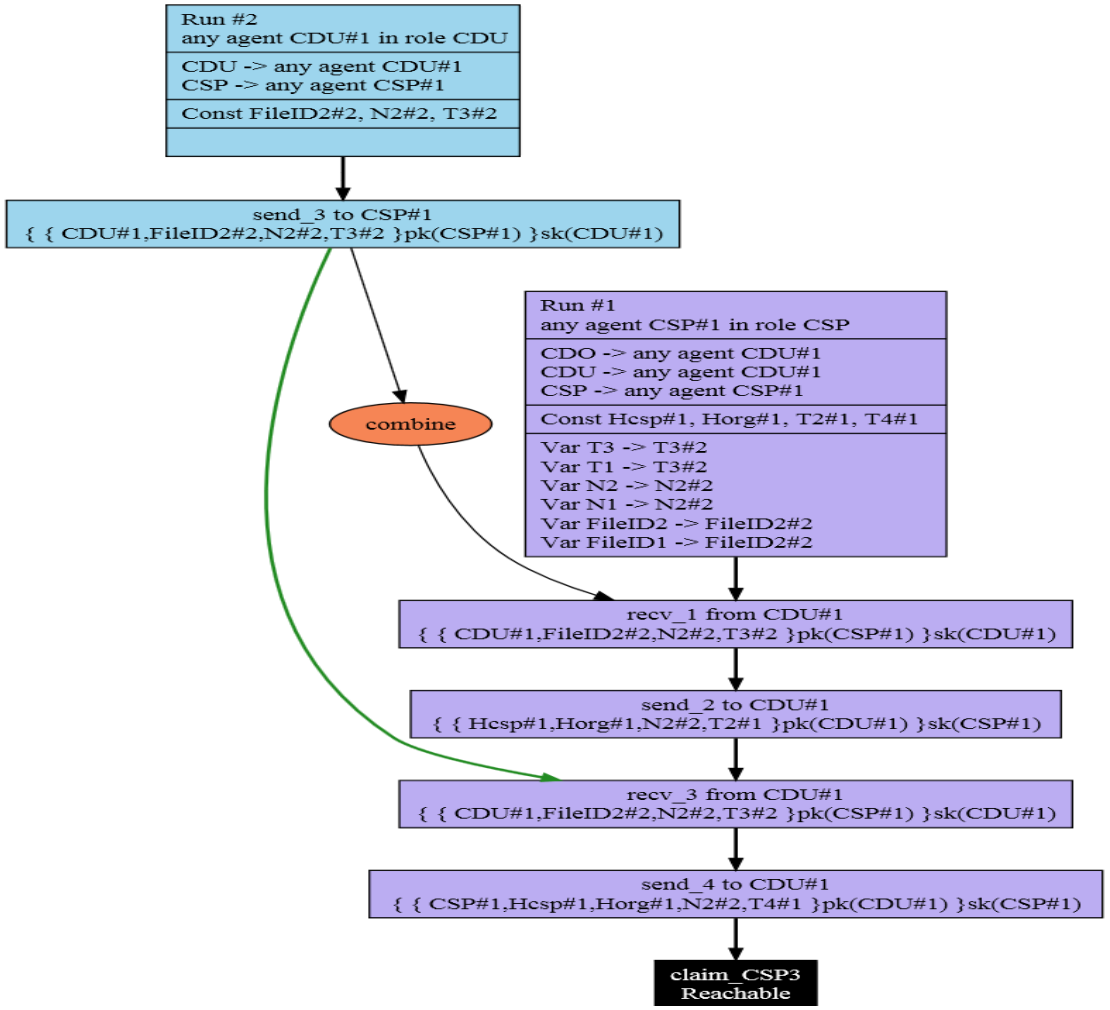
Role CDO



Role CDU

DSSM Phases: Verification Using Scyther

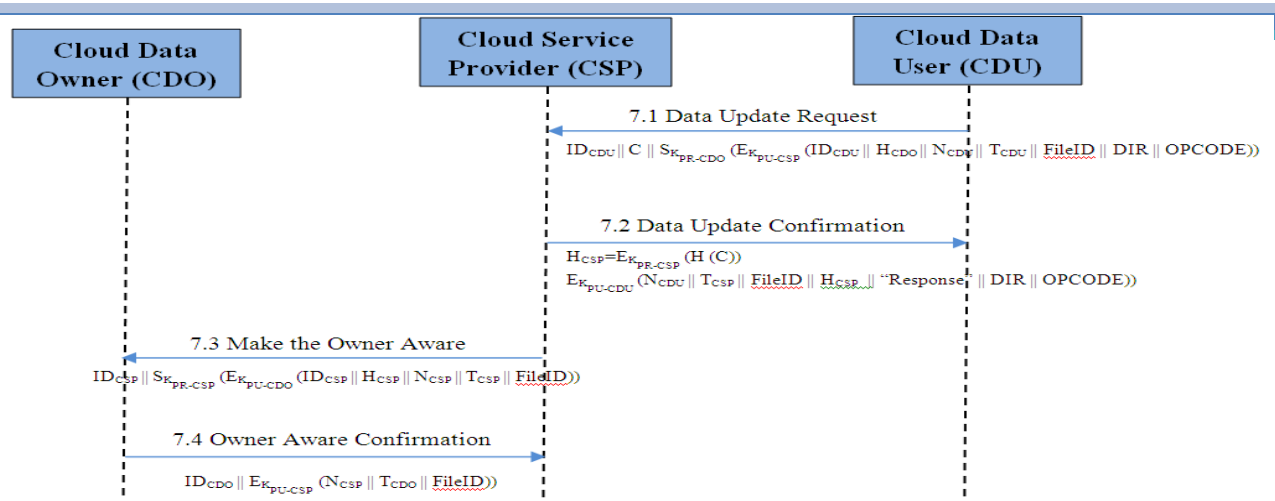
Data Integrity Verification Phase



Role CSP

DSSM Phases: Verification Using Scyther

Data Update Phase



Sequence Diagram

Scyther results : verify

Claim				Status		Comments
DataUpdate	CDO	DataUpdate,CDO1	Secret N2	Ok	Verified	No attacks.
	CDU	DataUpdate,CDU1	Secret N1	Ok	Verified	No attacks.
	CSP	DataUpdate,CSP1	Secret N1	Ok	Verified	No attacks.
		DataUpdate,CSP2	Secret N2	Ok	Verified	No attacks.

Done.

Scyther results : characterize

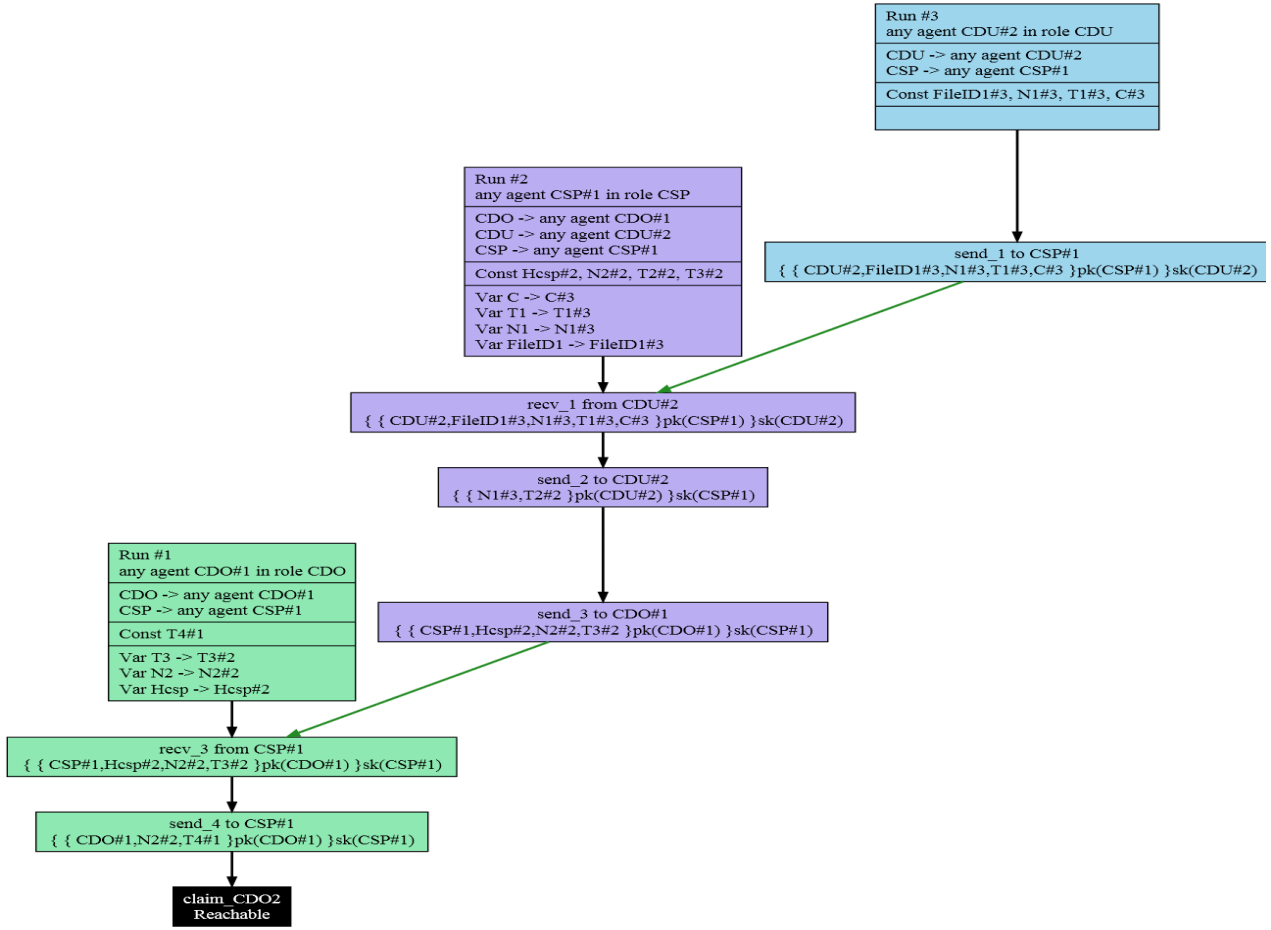
Claim				Status		Comments	Patterns
DataUpdate	CDO	DataUpdate,CDO2	Reachable	Ok	Verified	Exactly 2 trace patterns.	2 trace patterns
	CDU	DataUpdate,CDU2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	CSP	DataUpdate,CSP3	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern

Done.

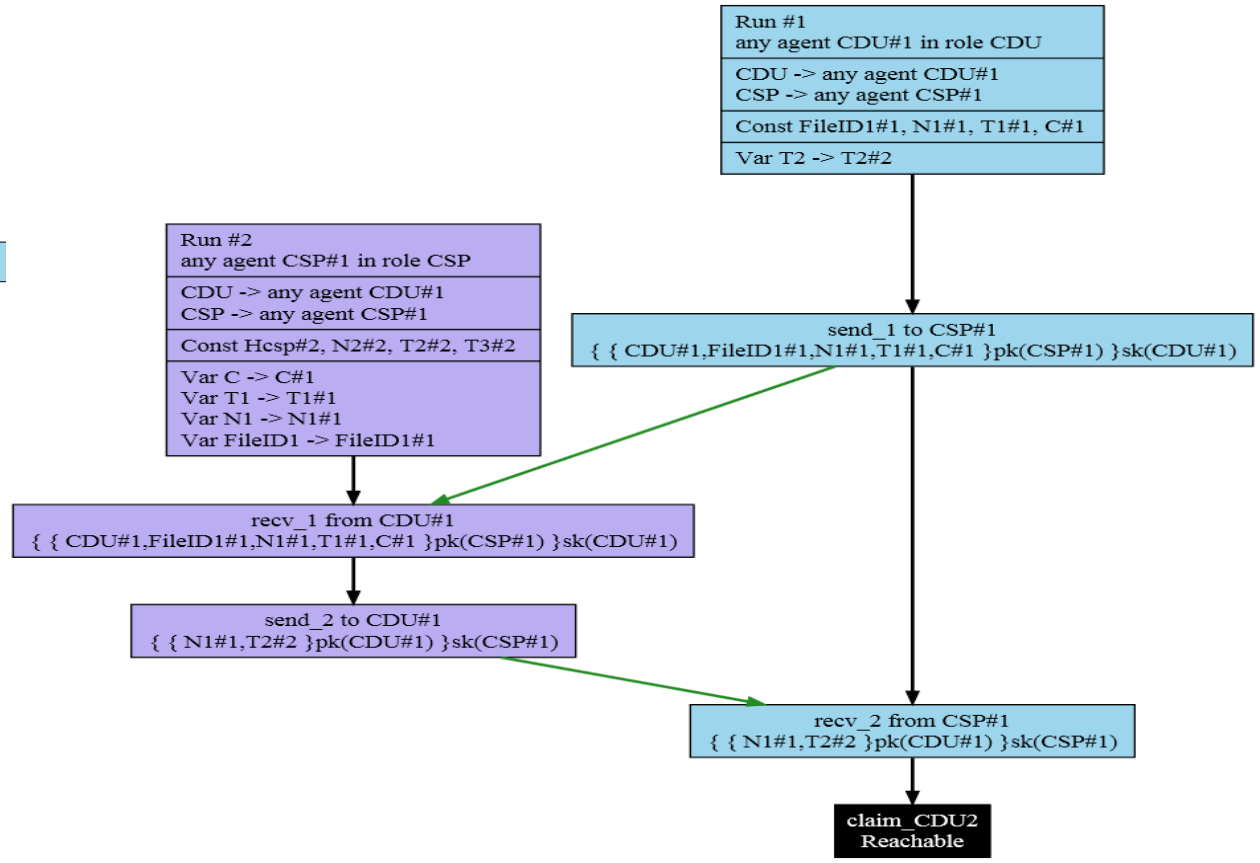
Claim Checks

DSSM Phases: Verification Using Scyther

Data Update Phase



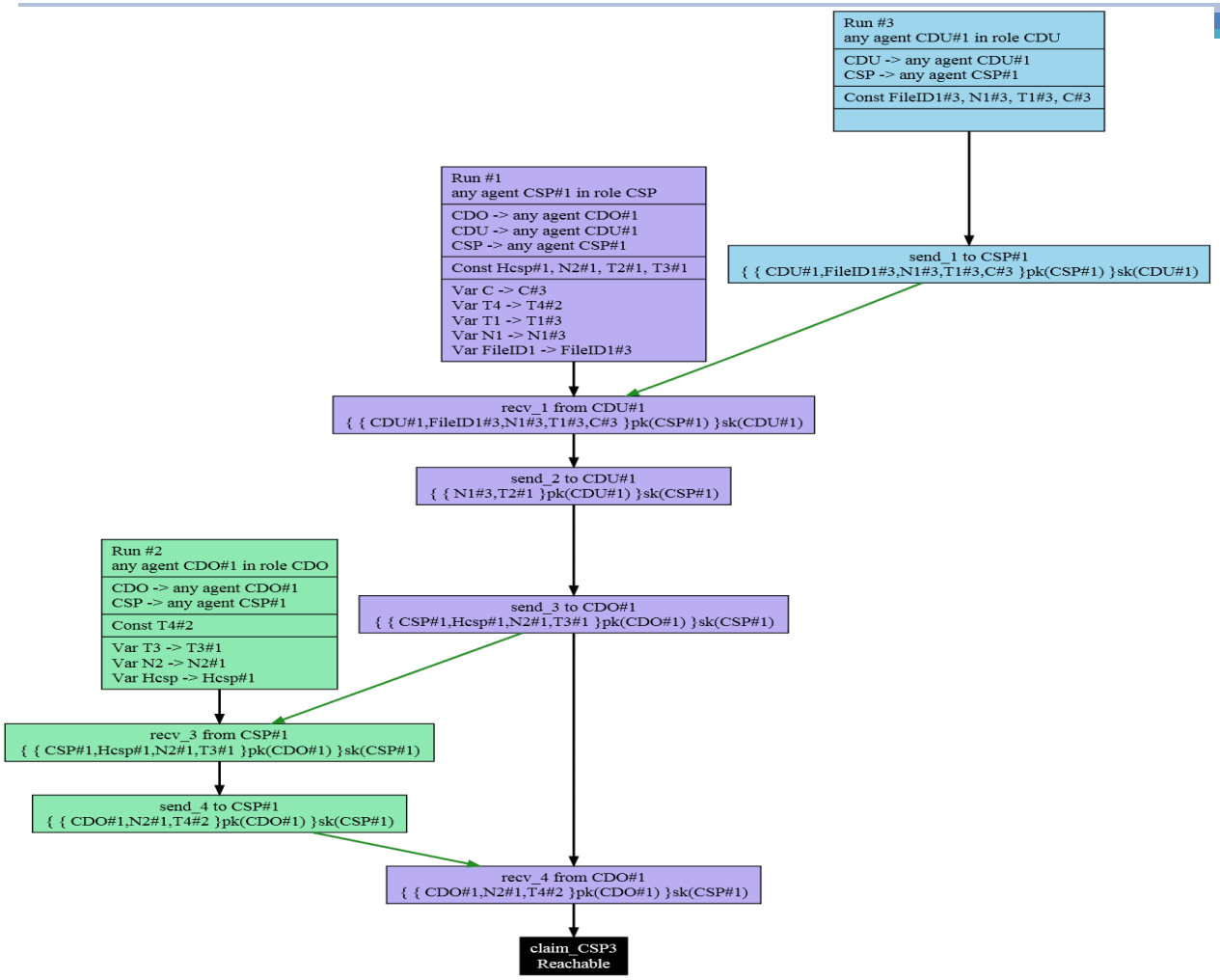
Role CDO



Role CDU

DSSM Phases: Verification Using Scyther

Data Update Phase

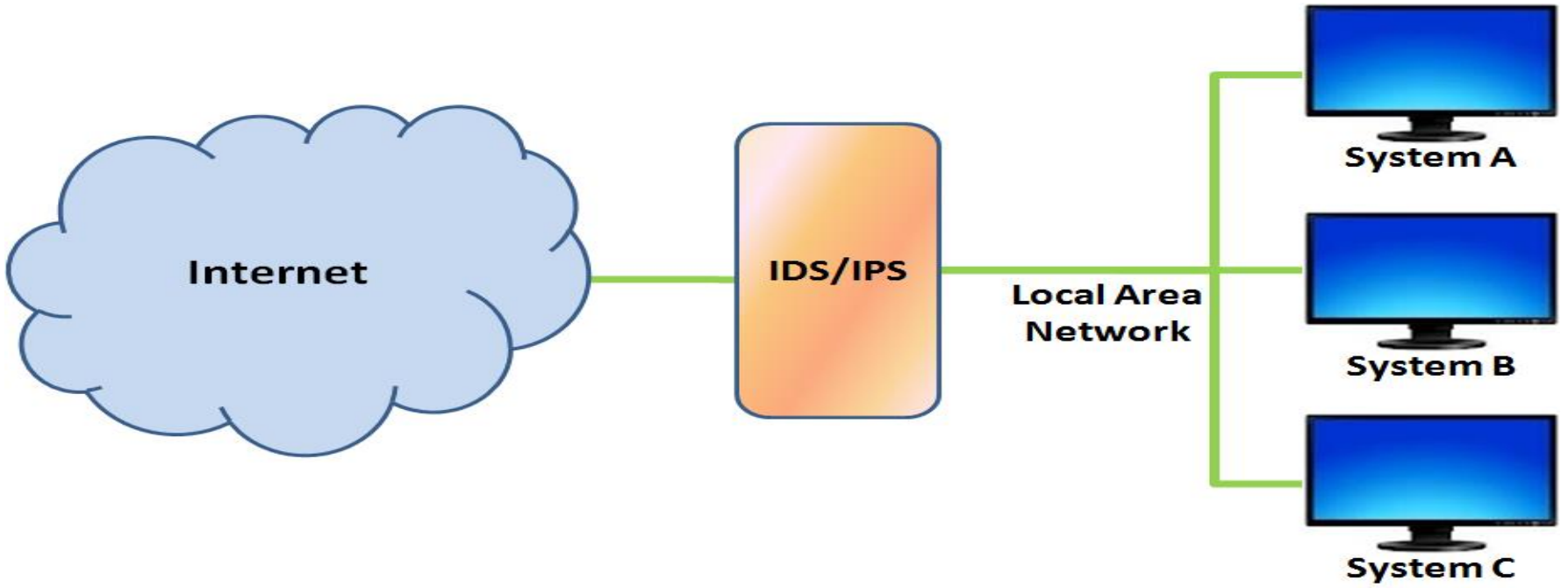


Role CSP

Designing Cloud IDS

Intrusion Detection System (IDS)

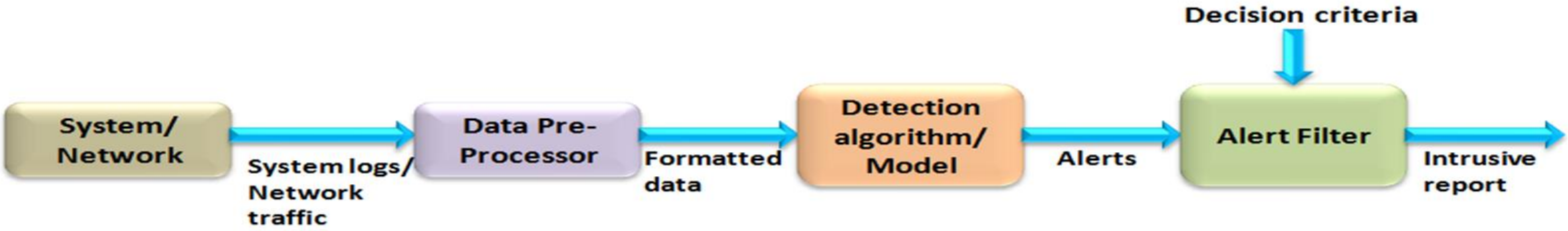
- Intrusion: Any set of actions that attempt to compromise the confidentiality, integrity or availability of a resource.
- IDS - monitors network (or system) for malicious activities.



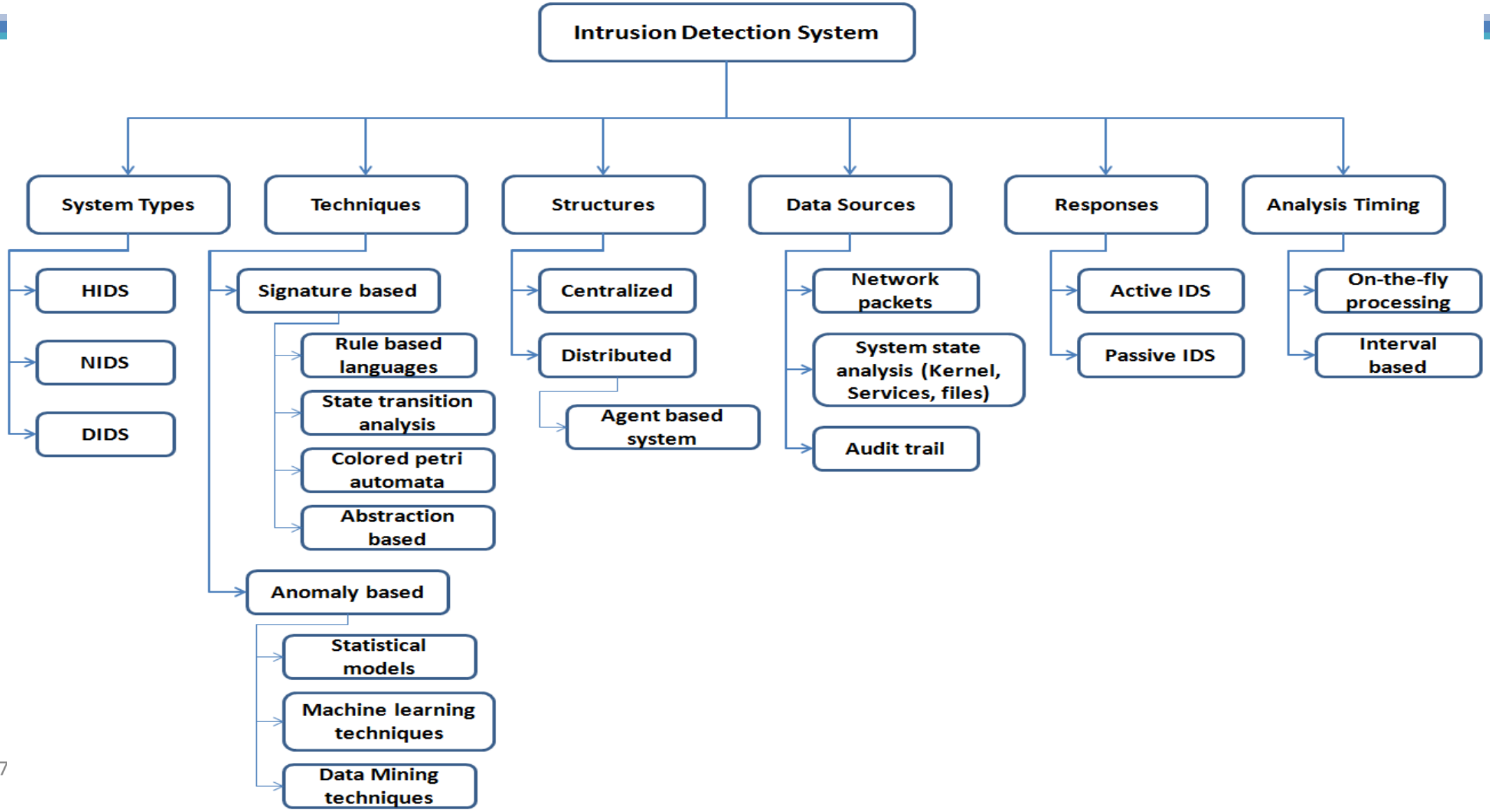
Intrusions in Cloud

- Insider Attack
- Flooding Attack
- User to Root Attack
- Port Scanning
- Attacks on Virtual Machine (VM) or Hypervisor
- Backdoor Channel Attack

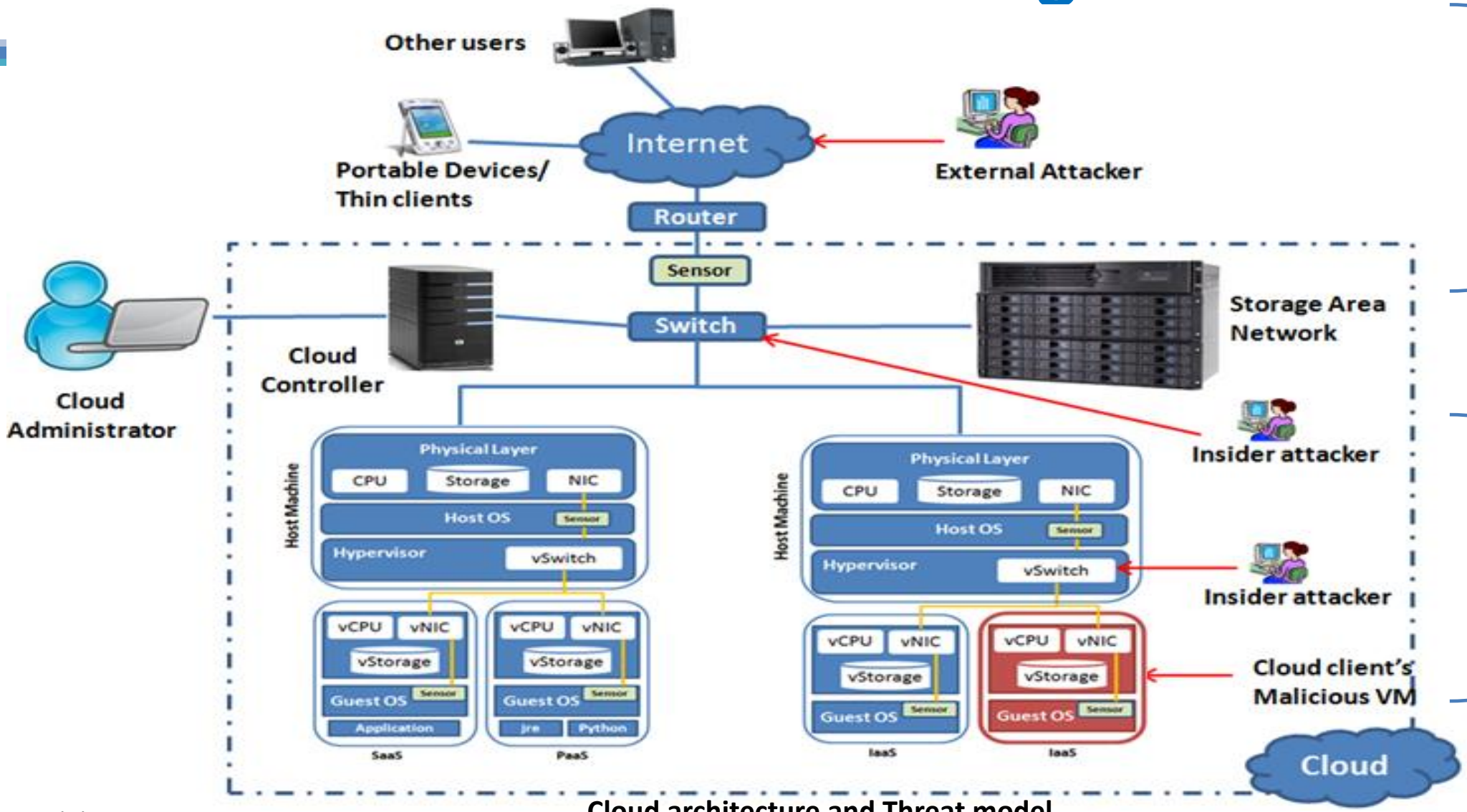
IDS components



IDS Taxonomy



Cloud Challenges



Cloud architecture and Threat model.

Signature and Anomaly Detection

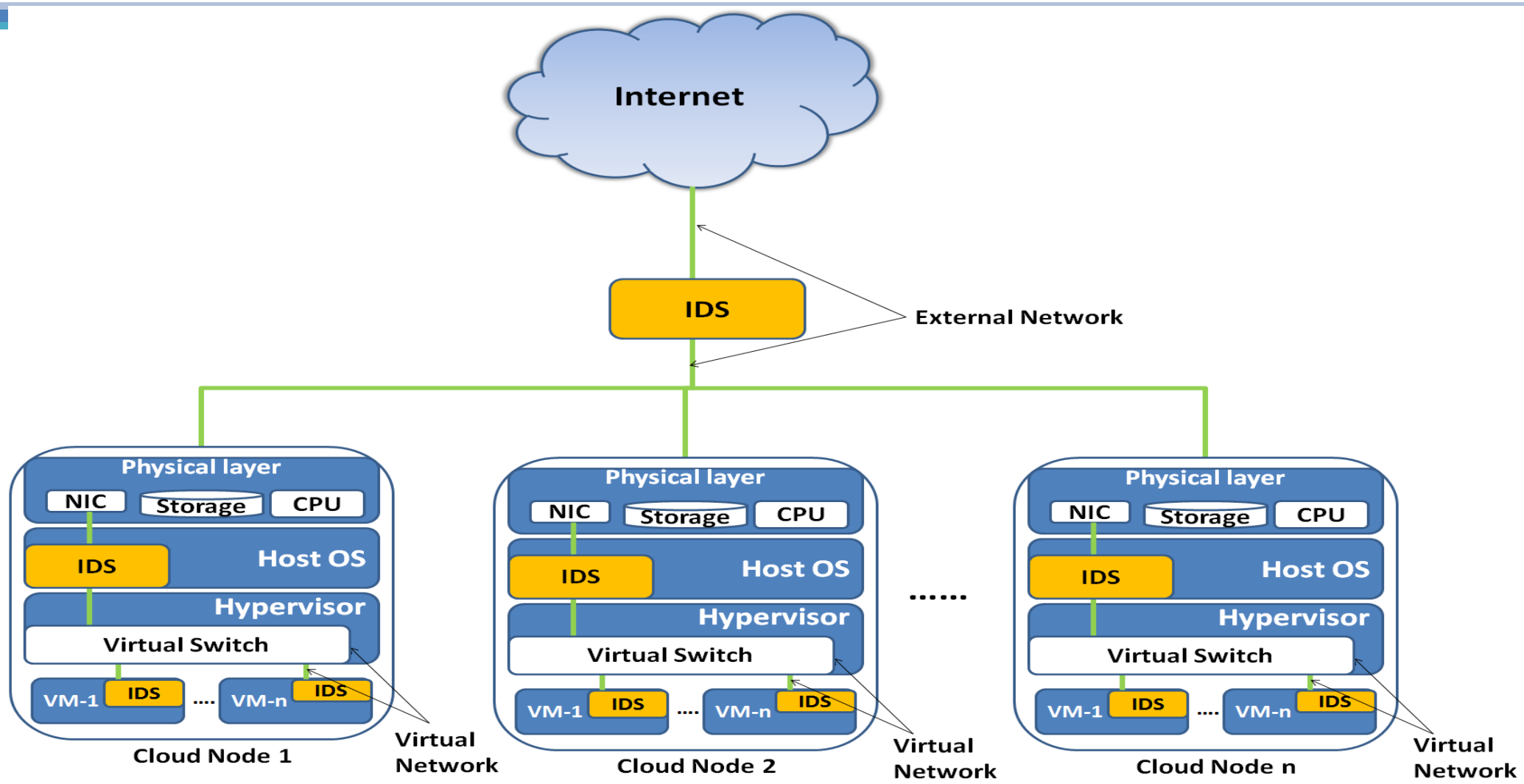
IDS Technique	Characteristics / Advantages	Limitations / Challenges
Signature based detection	• Identifies intrusion by matching captured patterns with preconfigured knowledge base. • High detection accuracy of previously known attacks. • Low computational cost.	• Cannot detect new or variant of known attacks. • High false alarm rate for unknown attacks.
Anomaly detection	• Uses statistical test on collected behavior to identify intrusion. • Can lower the false alarm rate for unknown attacks.	• More time is required to identify attacks. • Detection accuracy is based on amount of collected behavior or features.

Cloud NIDS Challenges: Research Gap

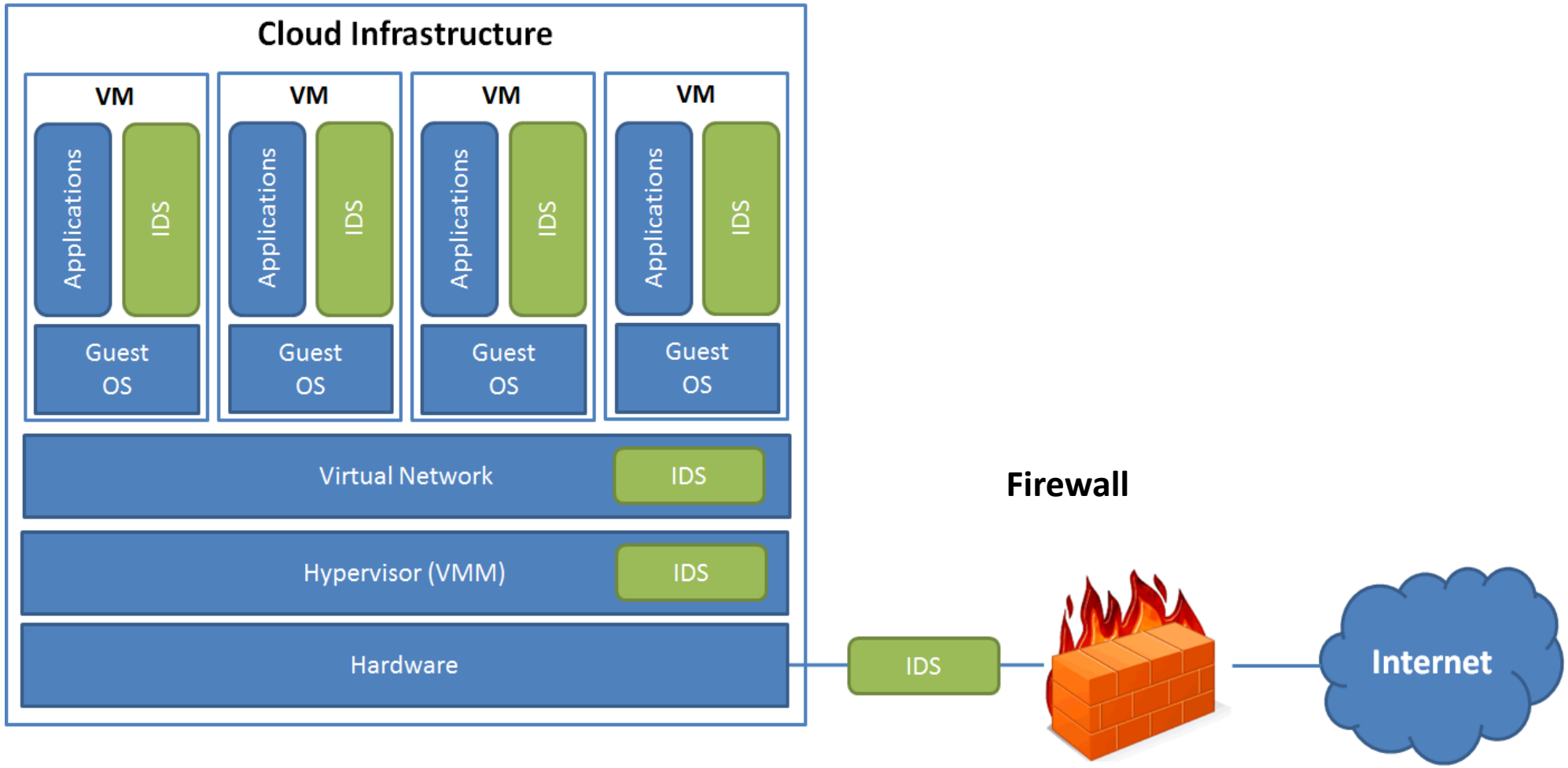
- IDS Deployment
  - Approaches like deploying IDS at individual VMs are vulnerable to host manipulation attacks.
- IDS Techniques

  -- Signature based approaches, Anomaly based approaches
  - Combination of both is required.
- Traditional NIDS challenges: detection rate, detection accuracy, false positives and false negatives
- Inspecting High Volume of Traffic from VMs and Detecting Unknown attacks
  - Efforts include detection of known attacks from large group of VMs
  - Need of detecting unknown attacks in high volume of traffic from large group of VMs.

Cloud IDS: Deployment Strategies



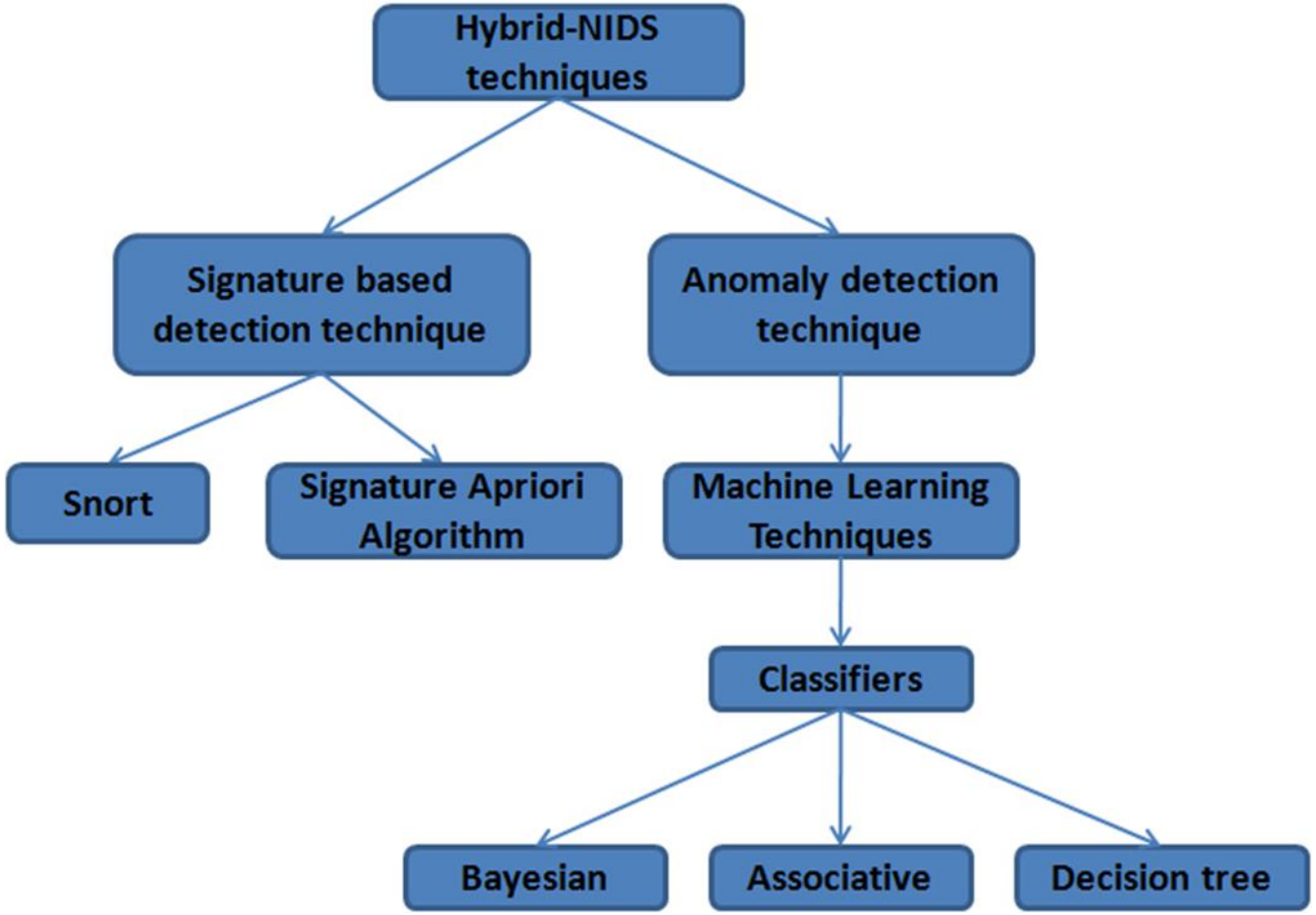
Placement of IDS in Cloud



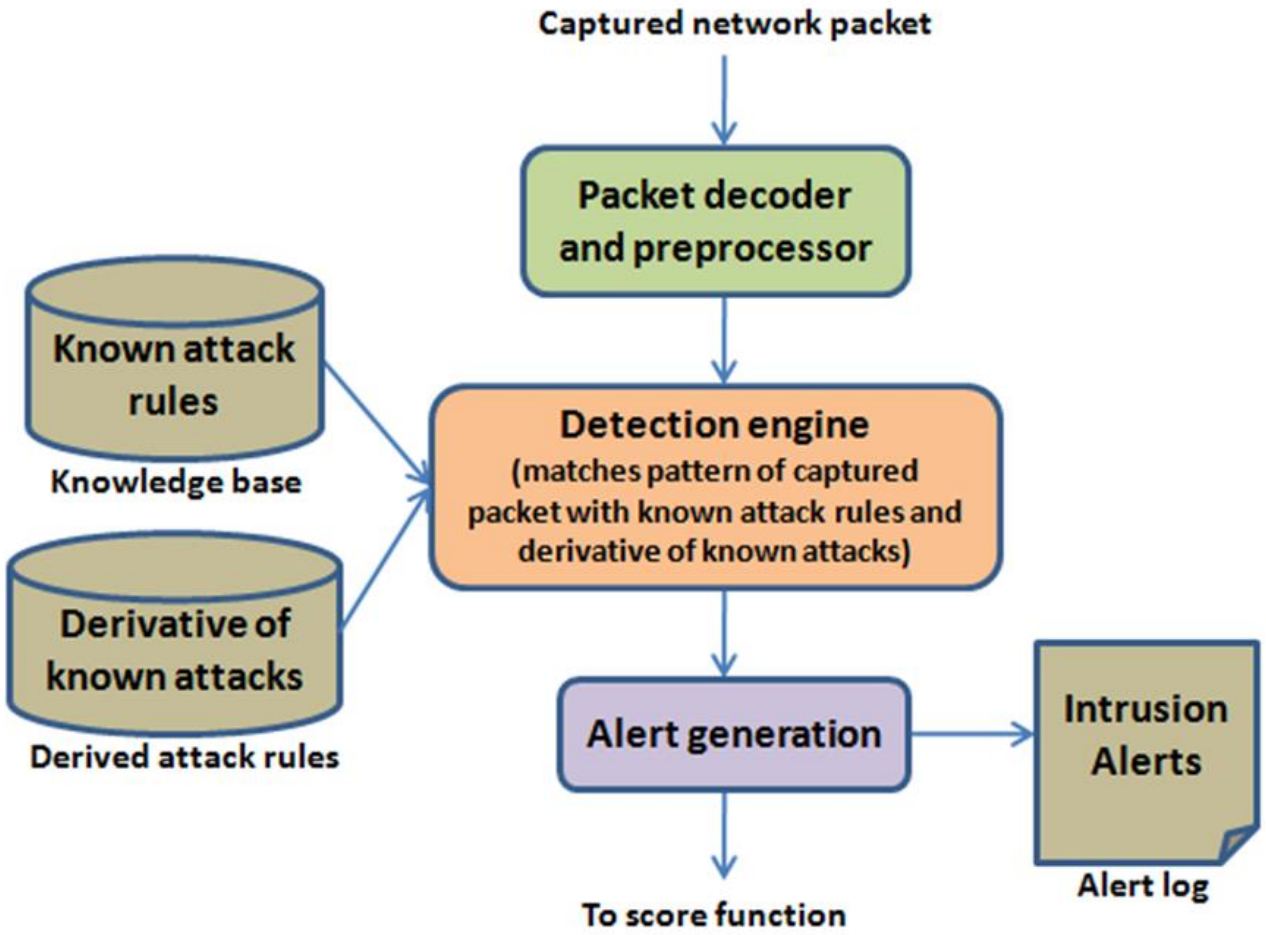
Cloud IDS: Requirements

- Handling high traffic volume from large number of VMs
- Detecting variety of attacks (Low false positives and low false negatives)
- Fast detection
- Scalable
- Resistance to Compromise

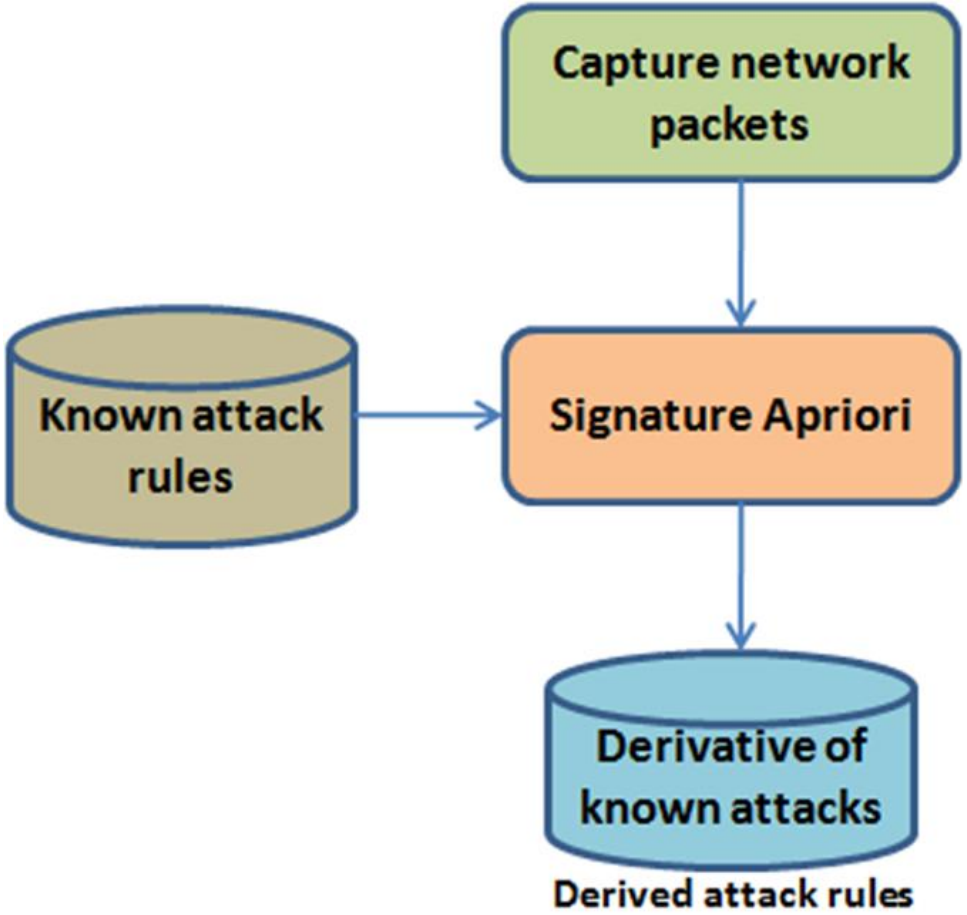
Our approach



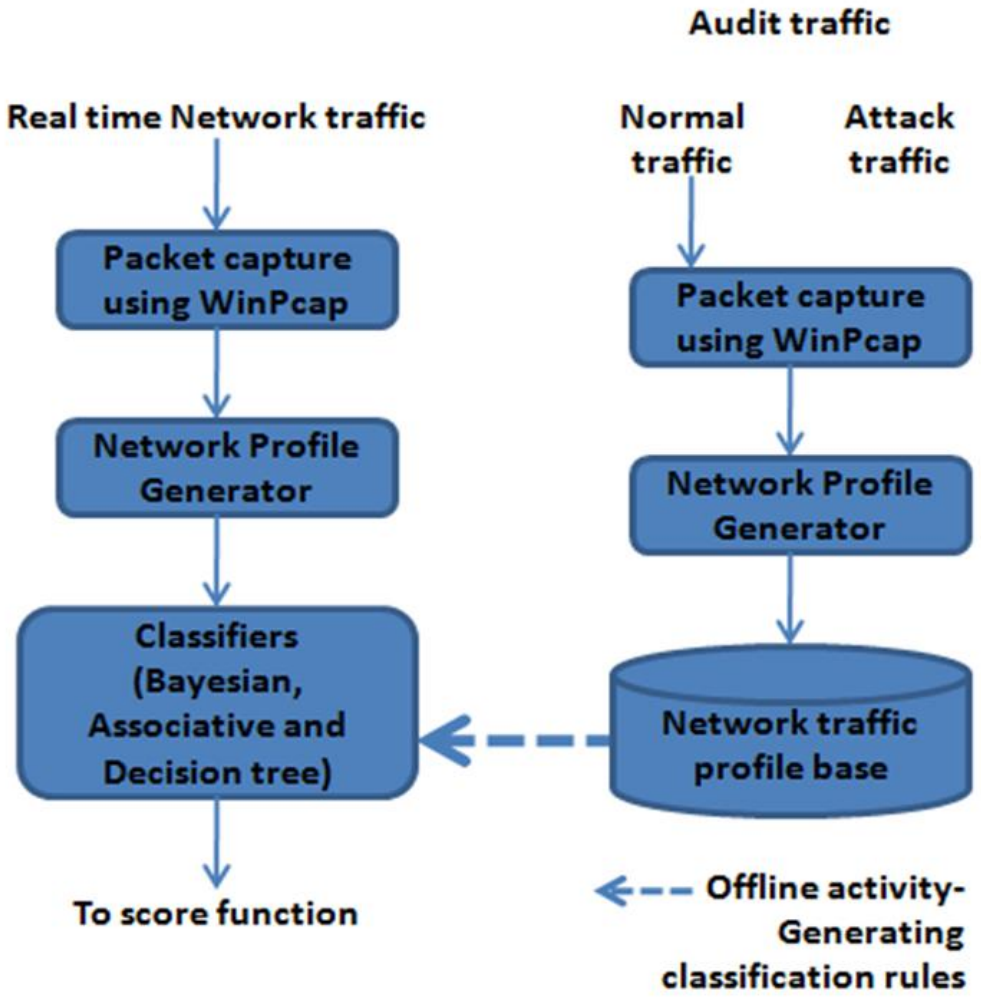
Signature detection



Signature detection: improved



Anomaly detection



Features used for IDS (16 out of 41)

No.	Feature Name	Description	Type
1	duration	length (number of seconds) of the connection	Continuous
2	protocol_type	type of the protocol, e.g. tcp, udp, etc.	Symbolic
3	service	network service on the destination, e.g., http, telnet, etc.	Symbolic
4	flag	number of data bytes from source to destination	Continuous
5	src_bytes	number of data bytes from destination to source	Continuous
6	dst_bytes	normal or error status of the connection	Symbolic
7	land	1 if connection is from/to the same host/port; 0 otherwise	Symbolic
8	wrong_fragment	number of ``wrong'' fragments	Continuous
9	urgent	number of urgent packets	Continuous
10	hot	number of ``hot'' indicators	Continuous
11	num_failed_logins	number of failed login attempts	Continuous
12	logged_in	1 if successfully logged in; 0 otherwise	Symbolic
13	num_compromised	number of ``compromised'' conditions	Continuous
14	root_shell	1 if root shell is obtained; 0 otherwise	Symbolic

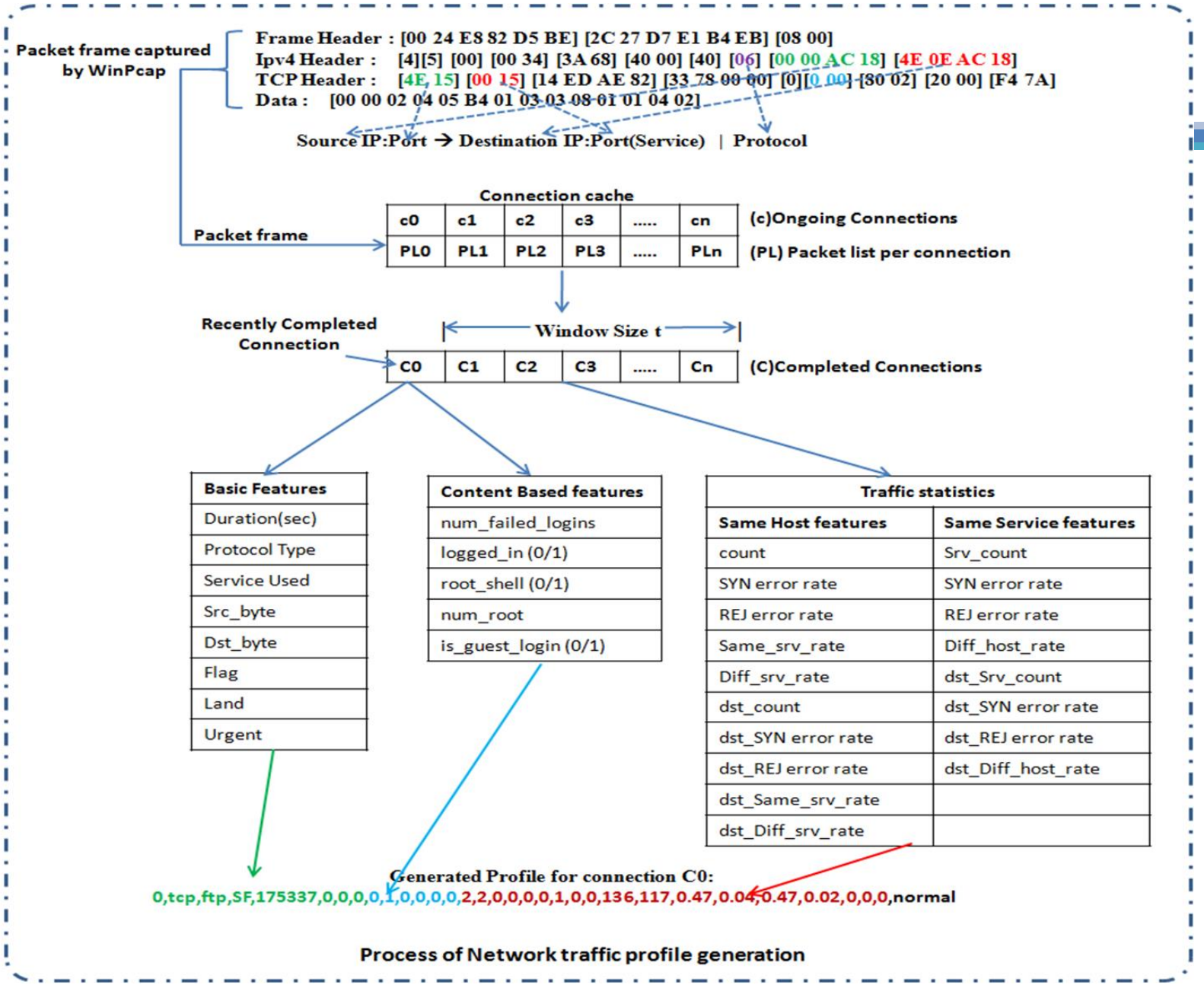
Highlighted Features are used in our H-NIDS

Features

No.	Feature Name	Description	Type
15	su_attempted	1 if ``su root'' command attempted; 0 otherwise	Symbolic
16	num_root	number of ``root'' accesses	Continuous
17	num_file_creations	number of file creation operations	Continuous
18	num_shells	number of shell prompts	Continuous
19	num_access_files	number of operations on access control files	Continuous
20	num_outbound_cmds	number of outbound commands in an ftp session	Continuous
21	is_host_login	1 if the login belongs to the ``hot'' list; 0 otherwise	Symbolic
22	is_guest_login	1 if the login is a ``guest'' login; 0 otherwise	Symbolic
23	count	number of connections to the same host	continuous
24	srv_count	% of connections that have ``SYN'' errors	continuous
25	serror_rate	% of connections that have ``REJ'' errors	continuous
26	srv_serror_rate	% of connections to the same service	continuous
27	rerror_rate	% of connections to different services	continuous
28	srv_rerror_rate	number of connections to the same service	continuous

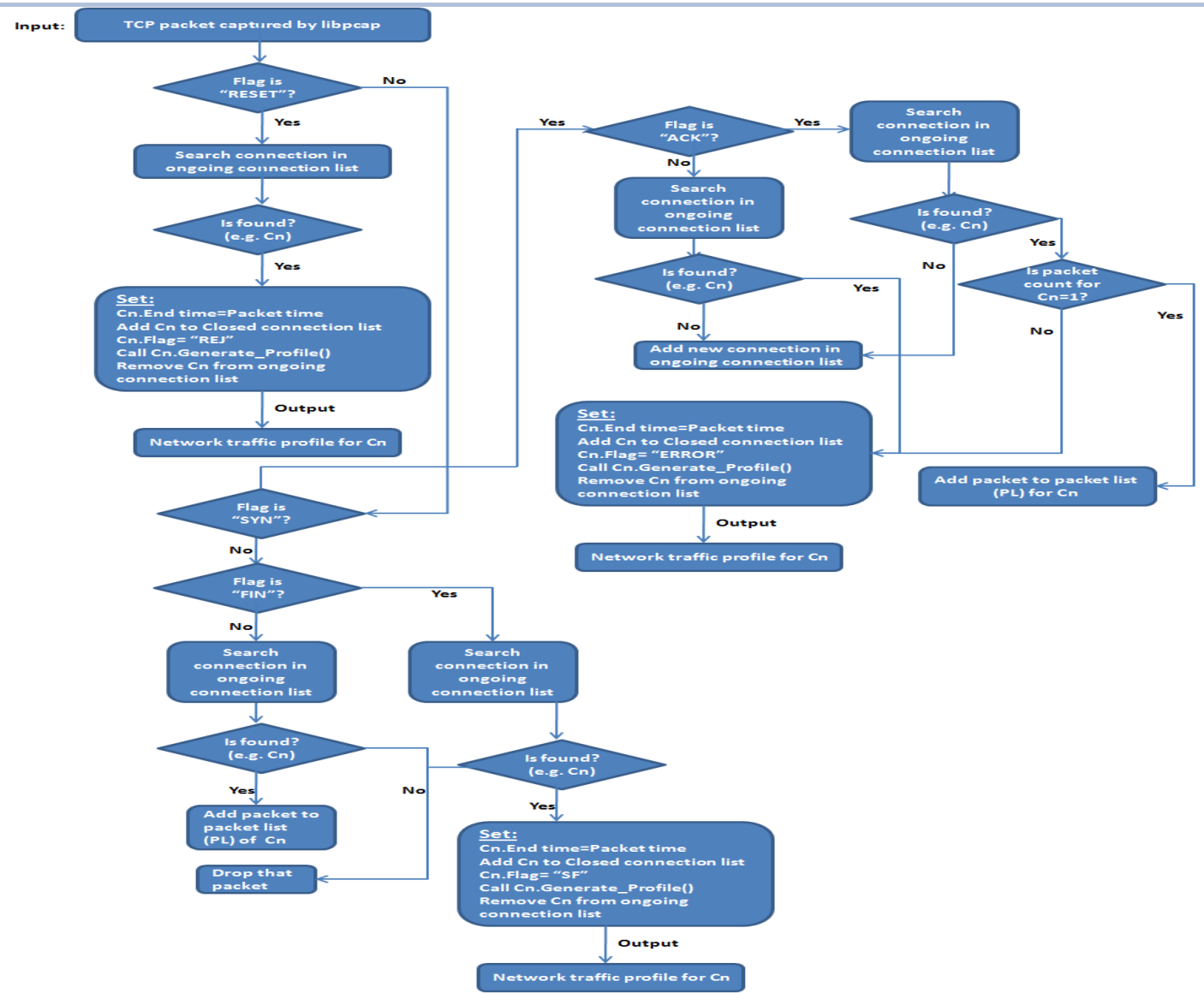
Features

No.	Feature Name	Description	Type
29	same_srv_rate	% of connections that have ``SYN'' errors	continuous
30	diff_srv_rate	% of connections that have ``REJ'' errors	continuous
31	srv_diff_host_rate	% of connections to different hosts	continuous
32	dst_host_count	dst host count count of connections having the same destination host	continuous
33	dst_host_srv_count	count of connections having the same destination host and using the same service	continuous
34	dst_host_same_srv_rate	% of connections having the same destination host and using the same Service	continuous
35	dst_host_diff_srv_rate	% of different services on the current host	continuous
36	dst_host_same_src_port_rate	% of connections to the current host having the same src port	continuous
37	dst_host_srv_diff_host_rate	% of connections to the same service coming from different hosts	continuous
38	dst_host_serror_rate	% of connections to the current host that have an S0 error	continuous
39	dst_host_srv_serror_rate	% of connections to the current host and specified service that have an S0 error	continuous
40	dst_host_rerror_rate	% of connections to the current host that have an RST error	continuous
41	dst_host_srv_rerror_rate	% of connections to the current host and specified service that have an RST error	continuous

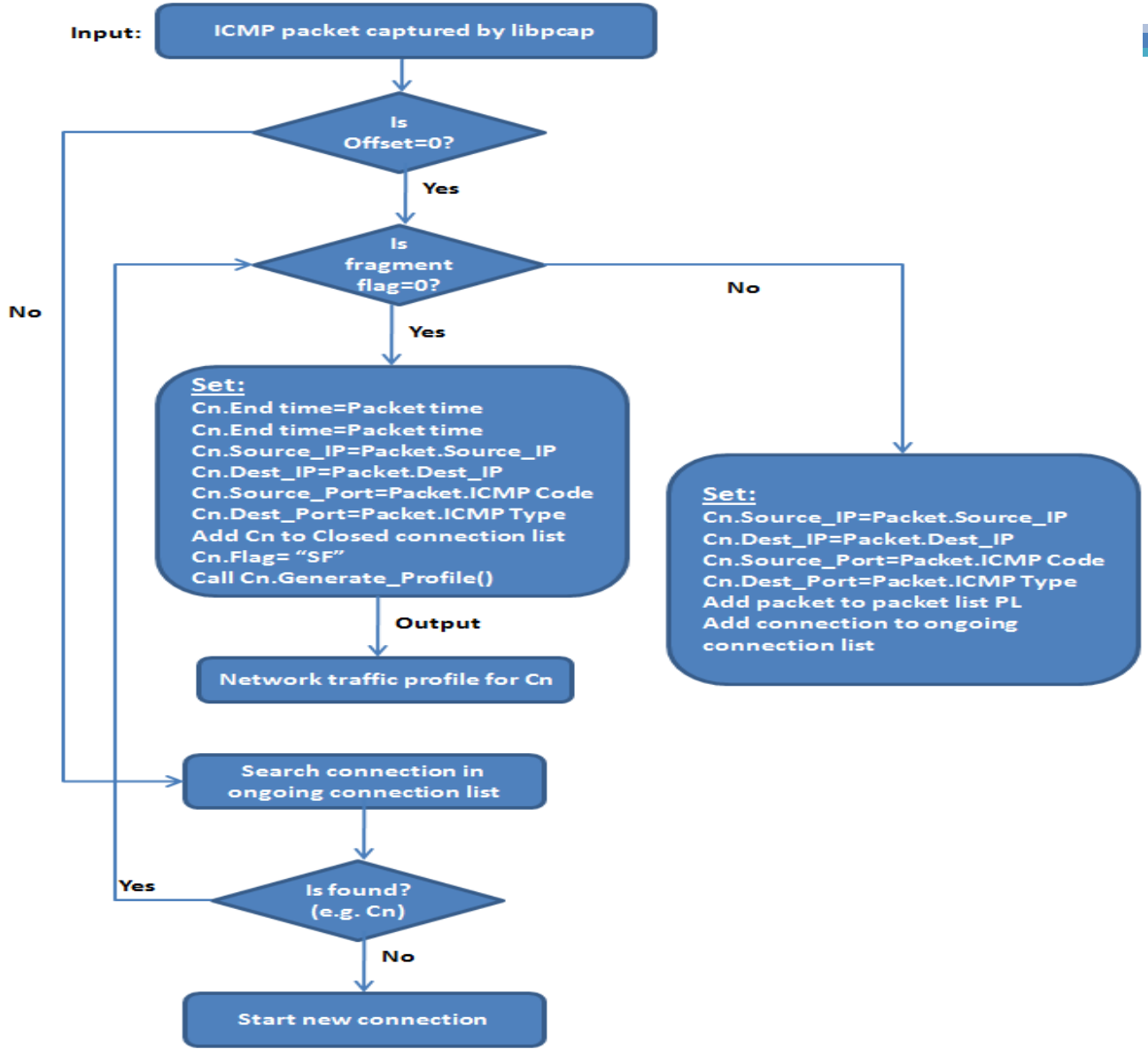


Process of Network traffic profile generation

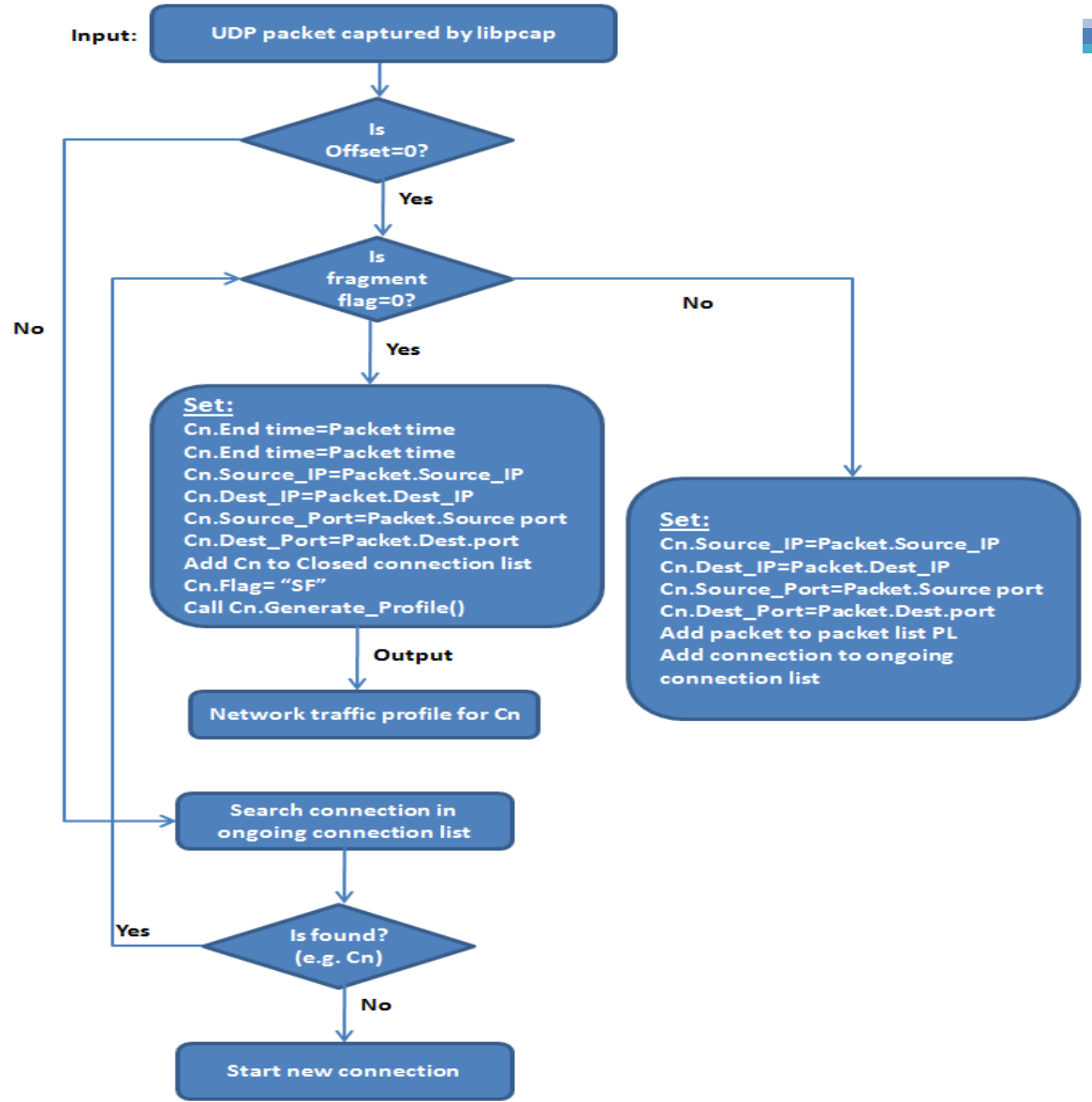
Network traffic profile generation for TCP Connection



Network traffic profile generation for ICMP Connection



Network traffic profile generation for UDP Connection



Example: Bayesian Classifier

- Predicts class label by calculating following probabilities for packet *X*:
  - P(Class= “Intrusion”) = 9/14 = 0.643.
  - P(Class = “Normal”) = 5/14 = 0.357.
- The probability of observing test packet *X*, given that the class holds,
  - P(Protocol Type=“TCP” | Class=“Intrusion”) = 2/9 = 0.222.
  - P(Protocol Type = “TCP” | Class = “Normal”) = 3/5 = 0.6.
  - P(Service = “SMTP” | Class = “Intrusion”) = 4/9 = 0.444.
  - P(Service = “SMTP” | Class = “Normal”) = 2/5 = 0.4.
  - P(Flag = “S0” | Class = “Intrusion”) = 6/9 = 0.667.
  - P(Flag = “S0” | Class = “Normal”) = 1/5 = 0.2.
  - P(Land = “0” | Class = “Intrusion”) = 6/9 = 0.667.
  - P (Land = “0” | Class = “Normal”) = 2/5 = 0.4.
- Hence,
  - P(X|Class=“ Intrusion”)=0.22 x 0.44 x 0.67 x 0.67= 0.04.
  - P(X|Class= “Normal”) = 0.6 x 0.4 x 0.2 x 0.4 = 0.02
  - P(X|Class=“Intrusion”) x P(Class=“Intrusion”) = 0.028.
  - P(X|Class=“Normal”) x P(Class=“Normal”) = 0.007.

- Packet *X* is considered as an Intrusion Since Intrusion probability is higher.

Example: Associative Classifier

- Input: Minimum support: 7%, Minimum confidence: 60%.

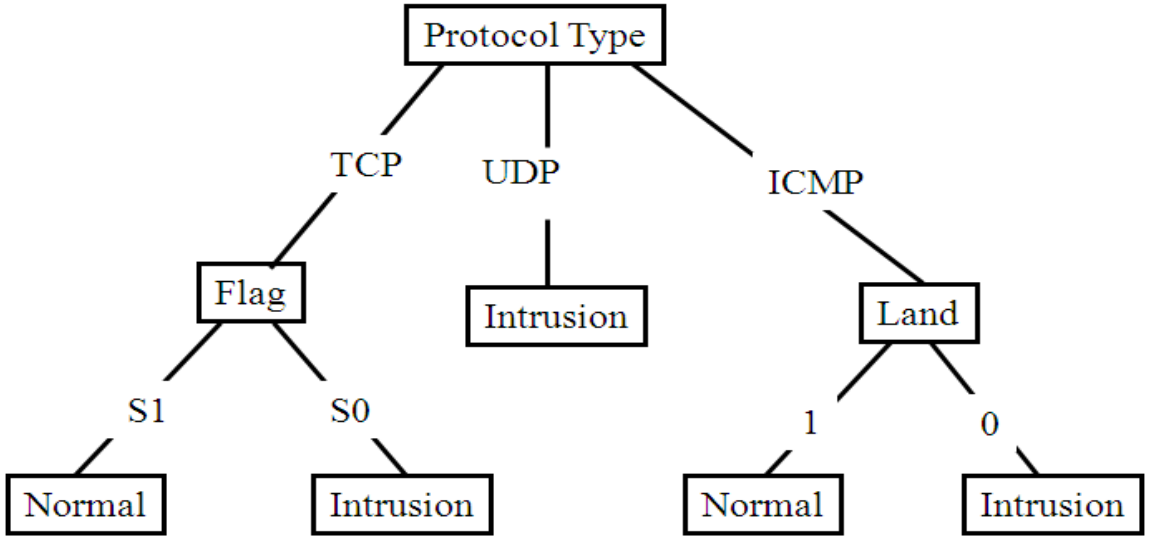
Frequent set in packet *X*	**Support (%)**
{TCP, Normal}	21.42
{TCP, Intrusion}	14.28
{SMTP, Normal}	14.28
{SMTP, Intrusion}	28.57
{S0, Normal}	7.15
{S0, Intrusion}	35.71
{0, Normal}	14.28
{0, Intrusion}	42.85
{TCP, SMTP, Normal}	7.15
{TCP, SMTP, Intrusion}	7.15
{TCP, S0, Intrusion}	14.28
{TCP, 0, Normal}	14.28
{TCP, 0, Intrusion}	7.15
{TCP, SMTP, S0, Intrusion}	7.15
{TCP, SMTP, 0, Normal}	7.15

Rule	**Support (%)**	**Confidence (%)**
{TCP, S0} -> {Intrusion}	21.42	100
{TCP, 0} -> {Normal}	14.28	100
{TCP, 0} -> {Intrusion}	14.28	100
{TCP, SMTP, S0} -> {Intrusion}	28.57	100
{TCP, SMTP, 0}-> { Normal}	7.15	100
{TCP, SMTP, 0}-> {Intrusion}	35.71	100

- Packet *X* is considered as an Intrusion since number of rules having Intrusion label for packet X are higher that rules having normal.

Example: Decision Tree Classifier

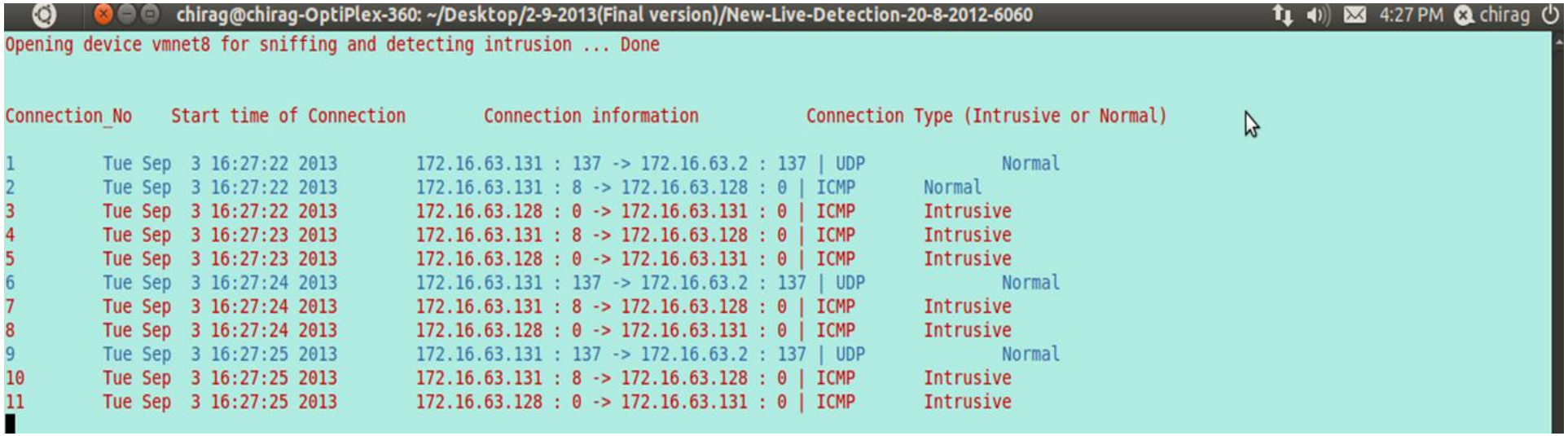
- Generates tree using sample dataset and finds prediction rules.

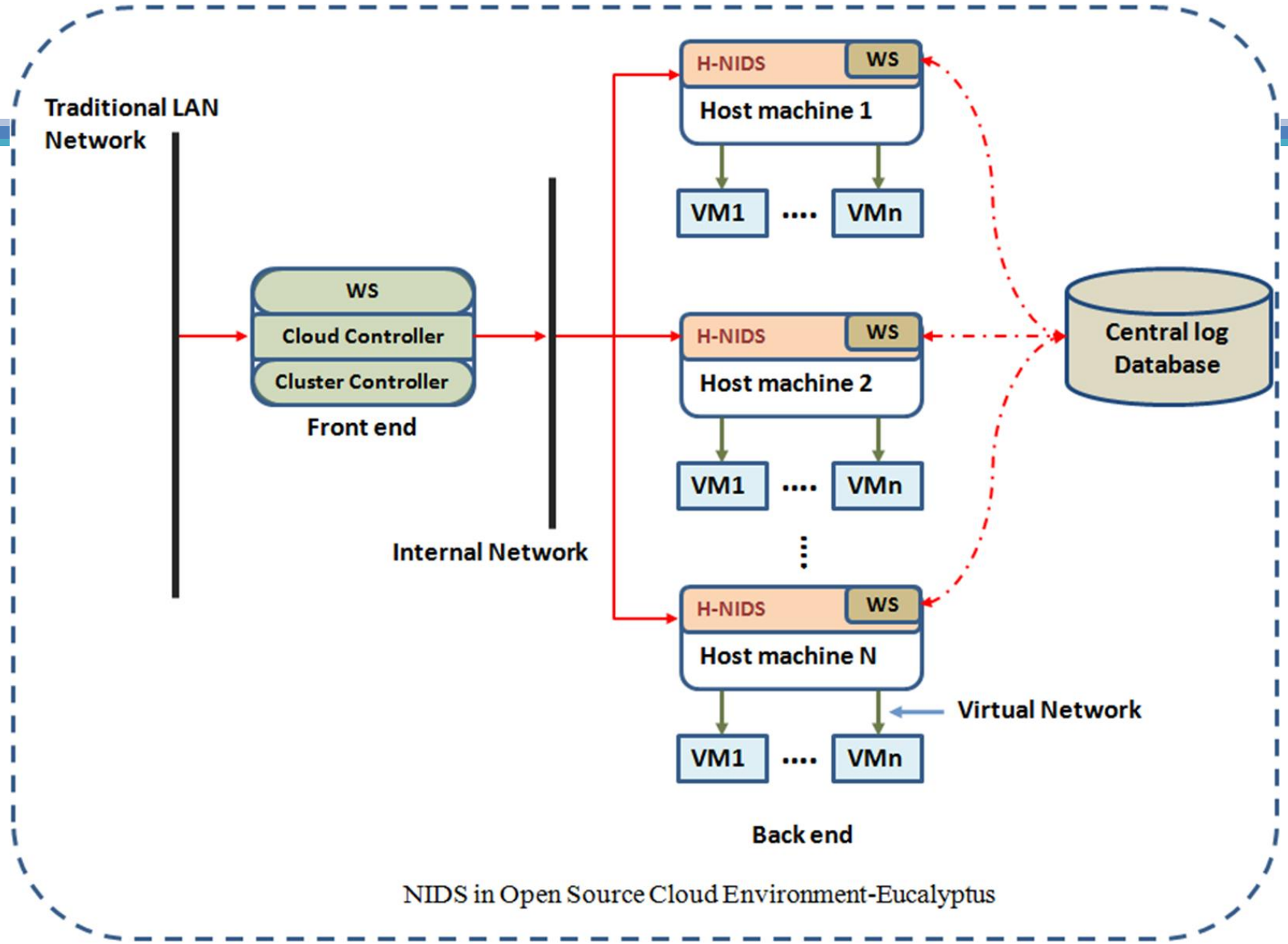


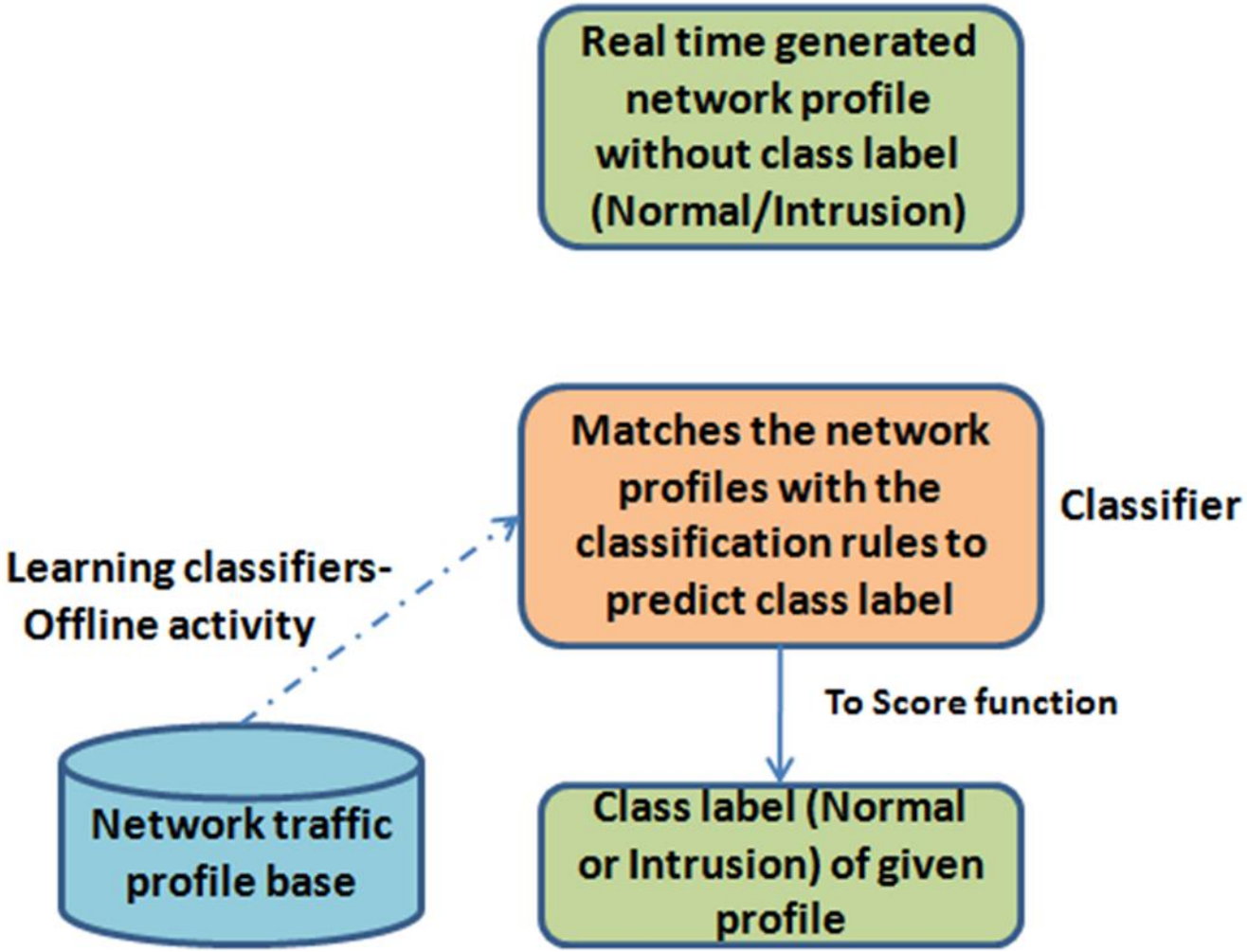
Rule	Prediction
If Protocol Type=TCP AND Flag=S1, Then	Normal
If Protocol Type=TCP AND Flag=S0, Then	Intrusion
If Protocol Type=UDP, Then	Intrusion
If Protocol Type=ICMP AND Land=1, Then	Normal
If Protocol Type=ICMP AND Land=0, Then	Intrusion

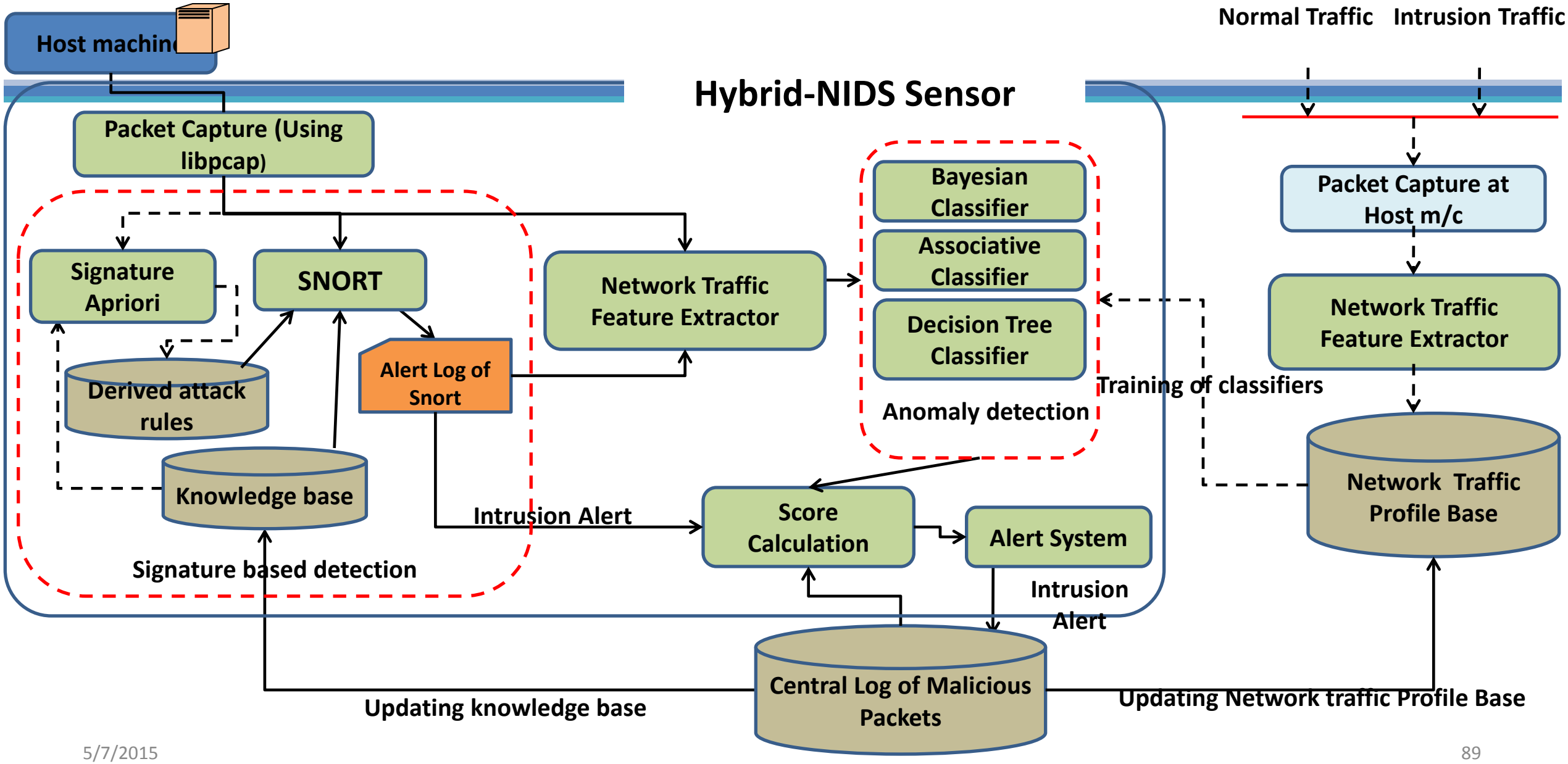
- Packet *X* = (Protocol Type=TCP, Service=SMTP, Flag=S0, Land=0).
- Rule number 2 is matched with packet *X*. Therefore, *X* is classified into Intrusion class.


train_live.txt (~/Desktop/2-9-2013(Final version)/New-Live-Detection-20-8-2012-6060) - gedit
4:13 PM chirag
Open
Save
Undo
train_live.txt
0,TCP,912,ERROR,1384,368,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,47200,1,0.00,0.00,0.00,0.00,0.00,1.00,0.00,46943,3,0.00,1.00,0.00,0.33,0.00,0.33,0.00,0.00,intrusion.
0,TCP,912,ERROR,1384,368,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,47201,1,0.00,0.00,0.00,0.00,0.00,1.00,0.00,46944,3,0.00,1.00,0.00,0.33,0.00,0.33,0.00,0.00,intrusion.
0,TCP,912,ERROR,1384,368,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,47202,1,0.00,0.00,0.00,0.00,0.00,1.00,0.00,46945,3,0.00,1.00,0.00,0.33,0.00,0.33,0.00,0.00,intrusion.
0,TCP,912,ERROR,1384,368,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,47203,1,0.00,0.00,0.00,0.00,0.00,1.00,0.00,46946,3,0.00,1.00,0.00,0.33,0.00,0.33,0.00,0.00,intrusion.
0,TCP,912,ERROR,1384,368,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,47204,1,0.00,0.00,0.00,0.00,0.00,1.00,0.00,46947,3,0.00,1.00,0.00,0.33,0.00,0.33,0.00,0.00,intrusion.
0,TCP,912,ERROR,1384,368,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,47205,1,0.00,0.00,0.00,0.00,0.00,1.00,0.00,46948,3,0.00,1.00,0.00,0.33,0.00,0.33,0.00,0.00,intrusion.
0,TCP,912,ERROR,1384,368,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,47206,1,0.00,0.00,0.00,0.00,0.00,1.00,0.00,46949,3,0.00,1.00,0.00,0.33,0.00,0.33,0.00,0.00,intrusion.
0,UDP,5355,SF,50,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,609,5917,0.00,0.00,0.00,0.00,0.04,0.96,1.00,5813,11598,1.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,normal.
0,UDP,137,SF,78,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,611,22733,0.00,0.00,0.00,0.00,0.95,0.05,0.97,27942,45176,0.81,0.21,0.00,0.02,0.00,0.00,0.00,0.00,normal.

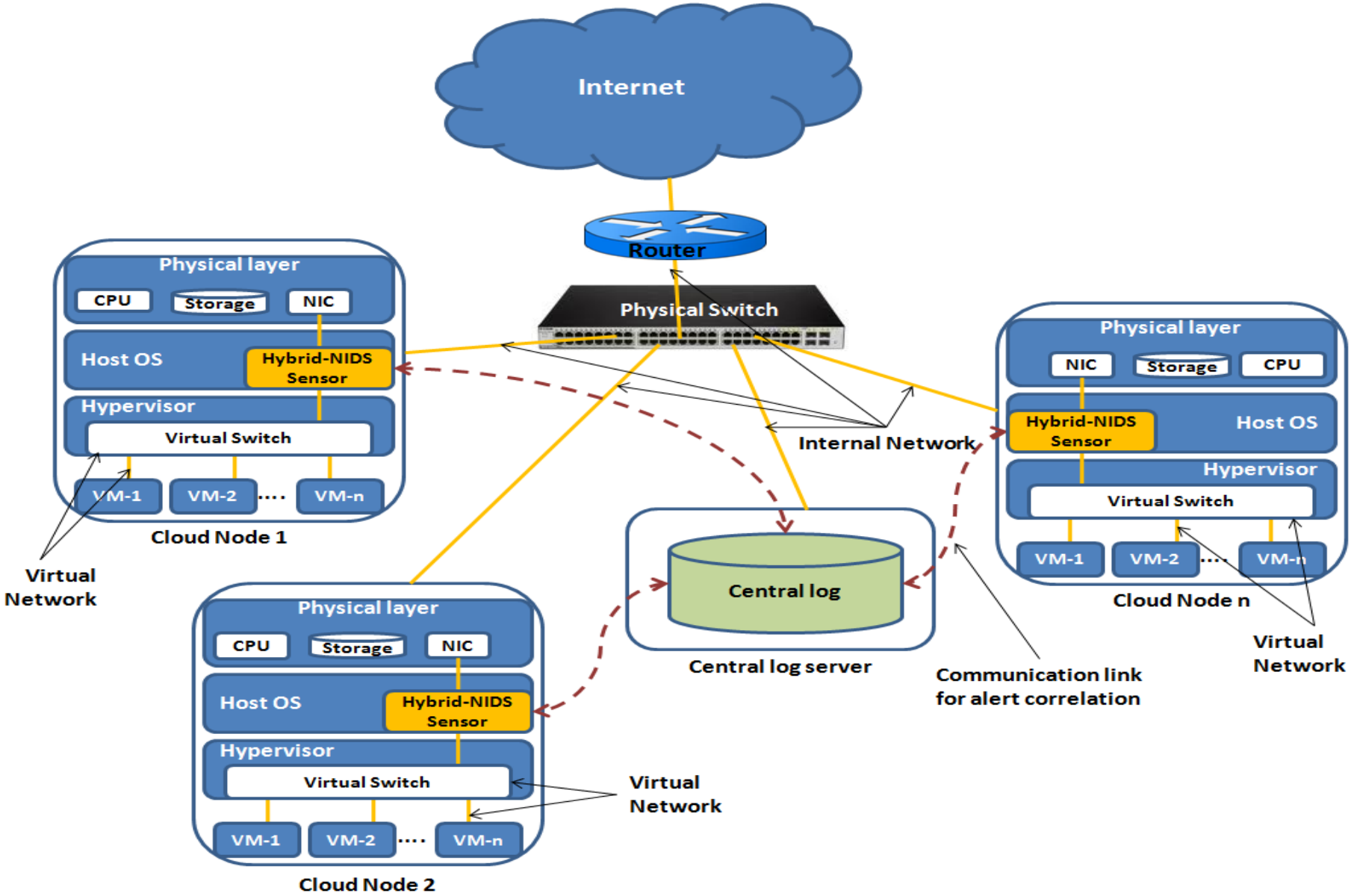

chirag@chirag-OptiPlex-360: ~/Desktop/2-9-2013(Final version)/New-Live-Detection-20-8-2012-6060
4:27 PM chirag
Opening device vmnet8 for sniffing and detecting intrusion ... Done
Connection_No Start time of Connection Connection information Connection Type (Intrusive or Normal)
1 Tue Sep 3 16:27:22 2013 172.16.63.131 : 137 -> 172.16.63.2 : 137 | UDP Normal
2 Tue Sep 3 16:27:22 2013 172.16.63.131 : 8 -> 172.16.63.128 : 0 | ICMP Normal
3 Tue Sep 3 16:27:22 2013 172.16.63.128 : 0 -> 172.16.63.131 : 0 | ICMP Intrusive
4 Tue Sep 3 16:27:23 2013 172.16.63.131 : 8 -> 172.16.63.128 : 0 | ICMP Intrusive
5 Tue Sep 3 16:27:23 2013 172.16.63.128 : 0 -> 172.16.63.131 : 0 | ICMP Intrusive
6 Tue Sep 3 16:27:24 2013 172.16.63.131 : 137 -> 172.16.63.2 : 137 | UDP Normal
7 Tue Sep 3 16:27:24 2013 172.16.63.131 : 8 -> 172.16.63.128 : 0 | ICMP Intrusive
8 Tue Sep 3 16:27:24 2013 172.16.63.128 : 0 -> 172.16.63.131 : 0 | ICMP Intrusive
9 Tue Sep 3 16:27:25 2013 172.16.63.131 : 137 -> 172.16.63.2 : 137 | UDP Normal
10 Tue Sep 3 16:27:25 2013 172.16.63.131 : 8 -> 172.16.63.128 : 0 | ICMP Intrusive
11 Tue Sep 3 16:27:25 2013 172.16.63.128 : 0 -> 172.16.63.131 : 0 | ICMP Intrusive


Traditional LAN Network
WS
Cloud Controller
Cluster Controller
Front end
Internal Network
H-NIDS
WS
Host machine 1
VM1
VMn
H-NIDS
WS
Host machine 2
VM1
VMn
H-NIDS
WS
Host machine N
VM1
VMn
Central log Database
Virtual Network
Back end
NIDS in Open Source Cloud Environment-Eucalyptus

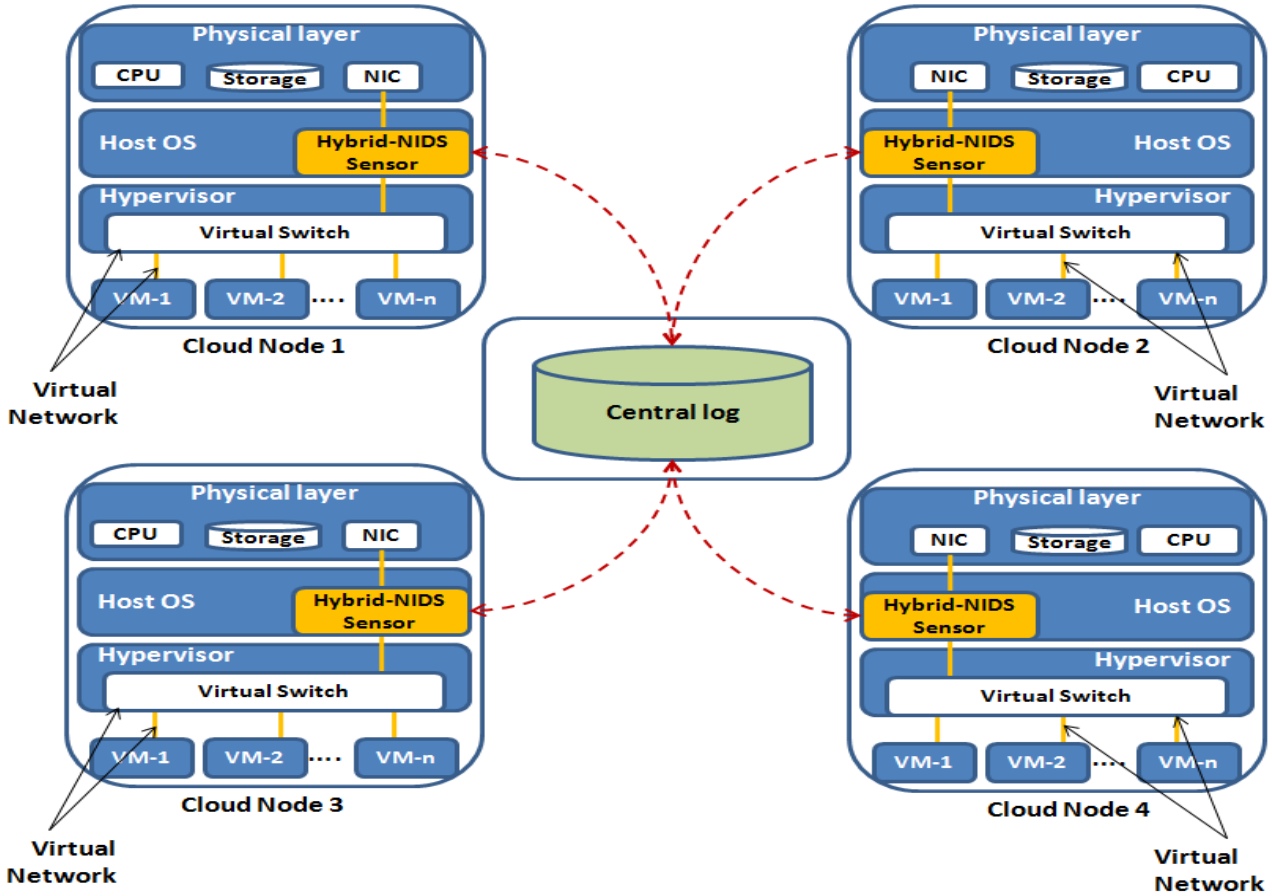

Real time generated network profile without class label (Normal/Intrusion)
Matches the network profiles with the classification rules to predict class label
Classifier
Learning classifiers- Offline activity
To Score function
Network traffic profile base
Class label (Normal or Intrusion) of given profile


Host machine
Hybrid-NIDS Sensor
Normal Traffic
Intrusion Traffic
Packet Capture (Using libpcap)
Signature Apriori
SNORT
Network Traffic Feature Extractor
Bayesian Classifier
Associative Classifier
Decision Tree Classifier
Anomaly detection
Packet Capture at Host m/c
Network Traffic Feature Extractor
Training of classifiers
Derived attack rules
Alert Log of Snort
Knowledge base
Intrusion Alert
Score Calculation
Alert System
Network Traffic Profile Base
Signature based detection
Intrusion Alert
Central Log of Malicious Packets
Updating knowledge base
Updating Network traffic Profile Base

Security Framework



Detection of Distributed Attack



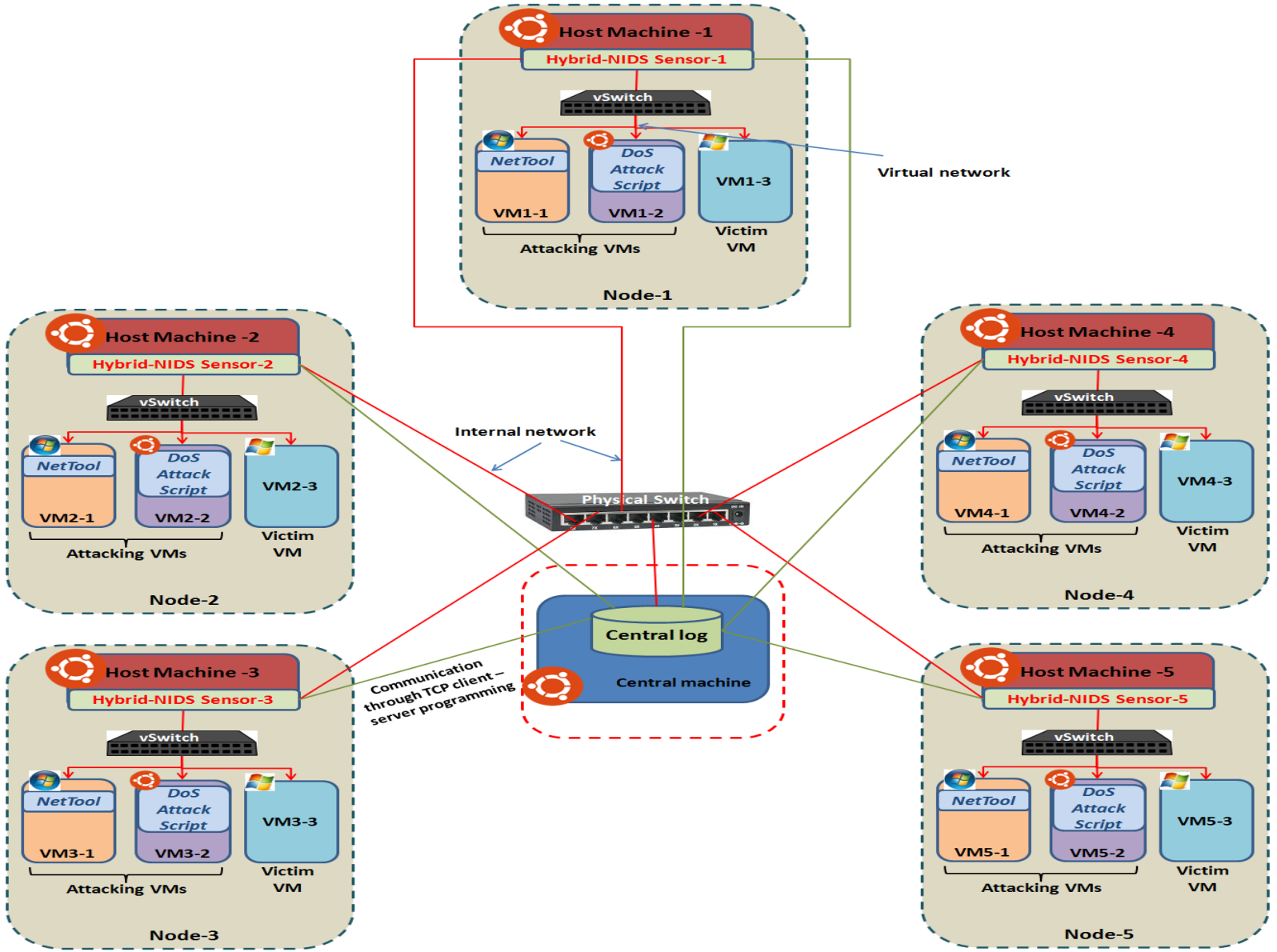
- checks central log to find weather same alerts has come from other sensors within the given time frame (*TF*).

$$Majority\ vote\ (Intrusion) = \frac{Number\ of\ sensors\ sends\ same\ alert\ to\ Central\ log}{Number\ of\ sensors\ in\ whole\ Cloud}$$

$$Majority\ vote\ (Intrusion) \begin{cases} \geq t, & Considered\ as\ distributed\ attack \\ < t, & Considered\ as\ an\ attack\ only\ on\ relevant\ host \end{cases}$$

t – Threshold, e.g. 0.5, half number of sending same alert

Validation Test Setup



Simulation experiments

Experiment No.	Attacking VM	Victim VM	Attack Type and Tools
1	VM1-2	VM1-3	Hping, Portscan, TCP-SYN flooding
2	VM1-1	VM1-3	UDP flooder, Xpinger, HTTP flooder (DoS), Fishing port scanner, Fast port scanner, FTP scanner, Fastest host scanner
3	VM1-1 and VM1-2	VM1-3	UDP flooder, Xpinger, HTTP flooder (DoS), Fishing port scanner, Fast port scanner, FTP scanner, Fastest host scanner, Hping, Portscan, TCP-SYN flooding

Performing attacks on a single VM.

Simulation Experiments

Experiment No.	Attacking VMs	Victim VMs	Attack Type and Tools
1	VM1-2, VM2-2 and VM3-2	VM1-3, VM2-3 and VM3-3	TCP-SYN flooding
2	VM1-2, VM2-2, VM3-2 and VM4-2	VM1-3, VM2-3, VM3-3 and VM4-3	TCP-SYN flooding
3	VM1-2, VM2-2, VM3-2, VM4-2 and VM5-2	VM1-3, VM2-3, VM3-3, VM4-3 and VM5-3	TCP-SYN flooding
4	VM1-1, VM2-1 and VM3-1	VM1-3, VM2-3 and VM3-3	UDP flooder, Xpinger, HTTP flooder (DoS), Fishing port scanner
5	VM1-1, VM2-1, VM3-1 and VM4-1	VM1-3, VM2-3, VM3-3 and VM4-3	UDP flooder, Xpinger, HTTP flooder (DoS), Fishing port scanner
6	VM1-1, VM2-1, VM3-1, VM4-1 and VM5-1	VM1-3, VM2-3, VM3-3, VM4-3 and VM5-3	UDP flooder, Xpinger, HTTP flooder (DoS), Fishing port scanner

Performing attacks on multiple VMs at a time

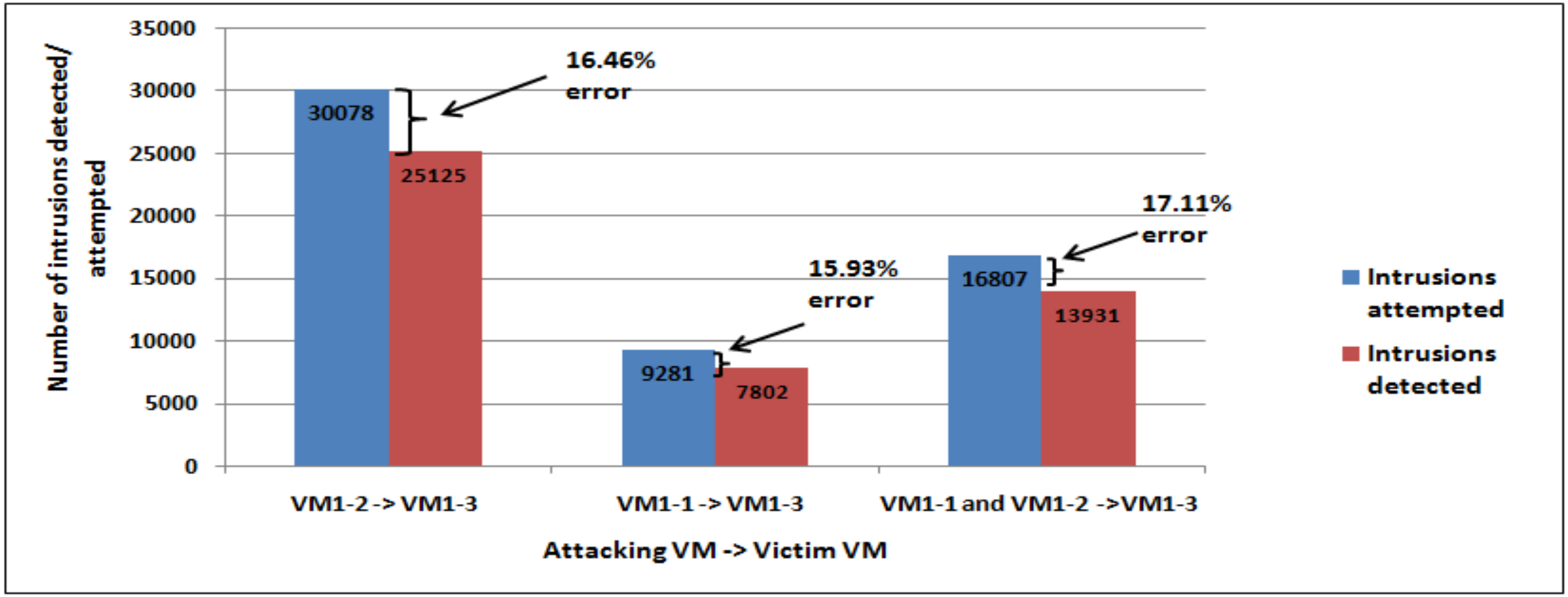
Offline: Simulation Experiments

	Training Dataset (used to train classifiers and generating classification rules)	**Testing Dataset** (applied to classifiers for predicting class label)
Test-1	KDD99(10%) training dataset	KDD99 test dataset
Test-2	KDD99 (100%) training dataset	KDD99 test dataset
Test-3	CAIDA + DARPA	CAIDA + DARPA

Evaluation Parameters (metrics)

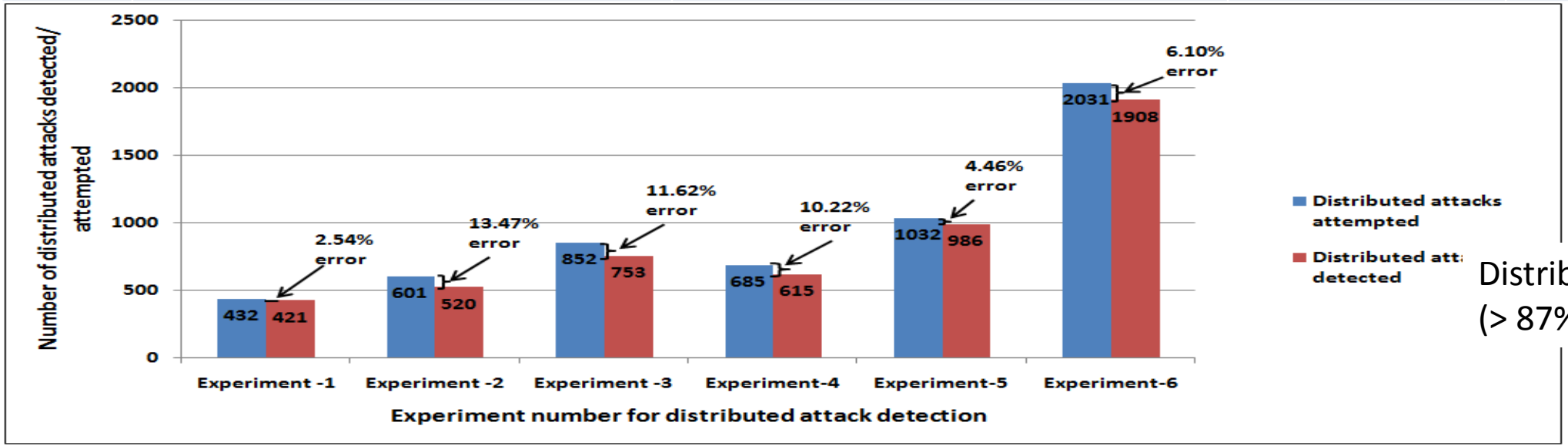
- True Positive Rate (TPR) = number of intrusions correctly detected/total number of intrusions (in test dataset)
- False Positive Rate (FPR)= number of normal records (in test dataset) detected as intrusions
- True Negative Rate (TNR)= number of normal records (in test dataset) are identified as normal
- False Negative Rate (FNR)= number of intrusions (in test dataset) are identified as normal
- Accuracy= number representing true predictions

Results: Real time simulation



Results: Real time simulation

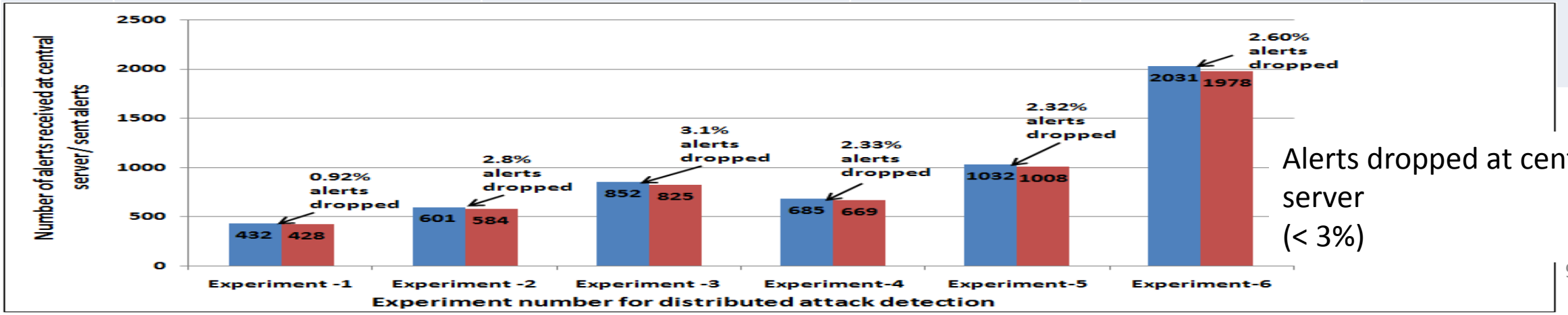
Exp. No.	Attacking VMs	Victim VMs	Number of alerts sent to *central server*	Number of alerts identified as distributed attacks
1	VM1-2, VM2-2 and VM3-2	VM1-3, VM2-3 and VM3-3	432	421
2	VM1-2, VM2-2, VM3-2 and VM4-2	VM1-3, VM2-3, VM3-3 and VM4-3	601	520
3	VM1-2, VM2-2, VM3-2, VM4-2 and VM5-2	VM1-3, VM2-3, VM3-3, VM4-3 and VM5-3	852	753
4	VM1-1, VM2-1 and VM3-1	VM1-3, VM2-3 and VM3-3	685	615
5	VM1-1, VM2-1, VM3-1 and VM4-1	VM1-3, VM2-3, VM3-3 and VM4-3	1032	986
6	VM1-1, VM2-1, VM3-1, VM4-1 and VM5-1	VM1-3, VM2-3, VM3-3, VM4-3 and VM5-3	2031	1908



Distributed attacks detected (> 87%)

Results: Real time simulation

Exp. No.	Attacking VMs	Victim VMs	Number of alerts sent to *central server*	Number of alerts received at *central server*	Number of alerts dropped at *central server*
1	VM1-2, VM2-2 and VM3-2	VM1-3, VM2-3 and VM3-3	432	428	4
2	VM1-2, VM2-2, VM3-2 and VM4-2	VM1-3, VM2-3, VM3-3 and VM4-3	601	584	17
3	VM1-2, VM2-2, VM3-2, VM4-2 and VM5-2	VM1-3, VM2-3, VM3-3, VM4-3 and VM5-3	852	825	27
4	VM1-1, VM2-1 and VM3-1	VM1-3, VM2-3 and VM3-3	685	669	16
5	VM1-1, VM2-1, VM3-1 and VM4-1	VM1-3, VM2-3, VM3-3 and VM4-3	1032	1008	24



Alerts dropped at central server
(< 3%)

Results: Offline Simulation (TPR > 98%)

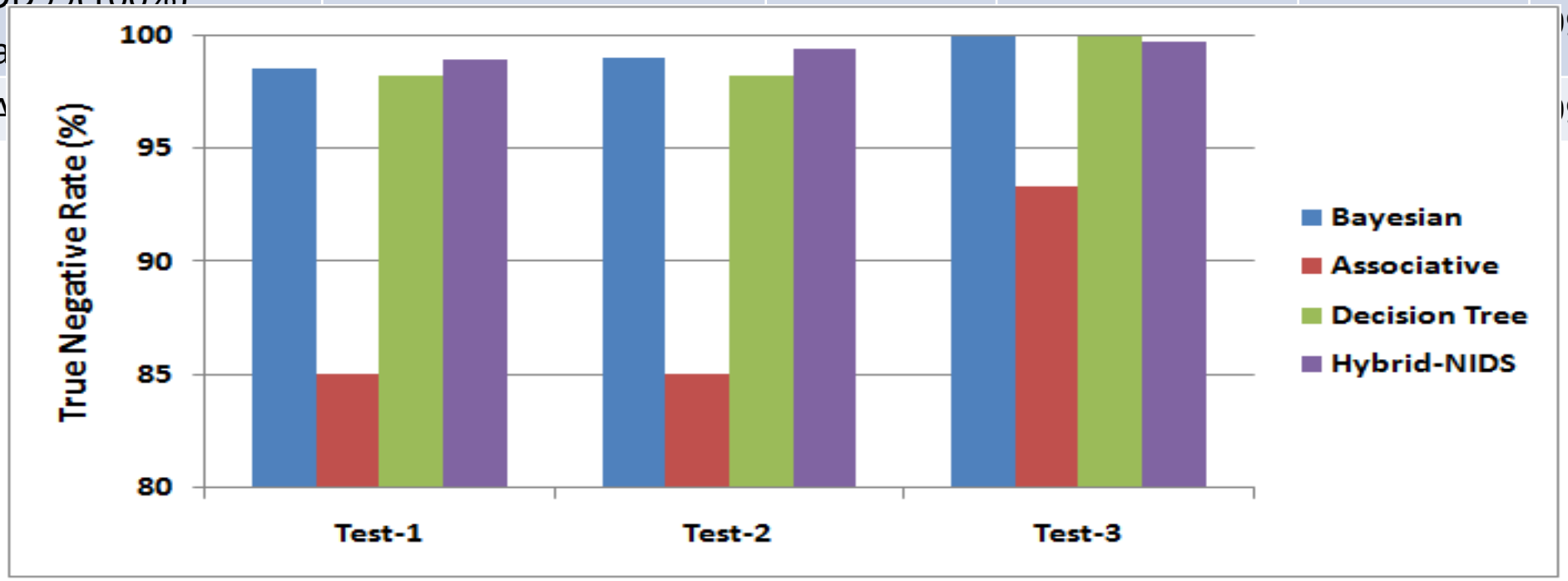
	Training Dataset	Testing Dataset	True Positive Rate (%)			
			Bayesian	Associative	Decision Tree	Hybrid-NIDS
Test-1	KDD99(10%) training dataset	KDD99 test dataset	96.05	97.60	97.20	98.04
Test-2	KDD99(100%) training dataset	KDD99 test dataset	98.79	99.92	99.62	99.56
Test-3	DARPA + CAIDA	DARPA + CAIDA	99.96	99.75	99.71	99.96

Results: Offline Simulation (FPR < 1.05%)

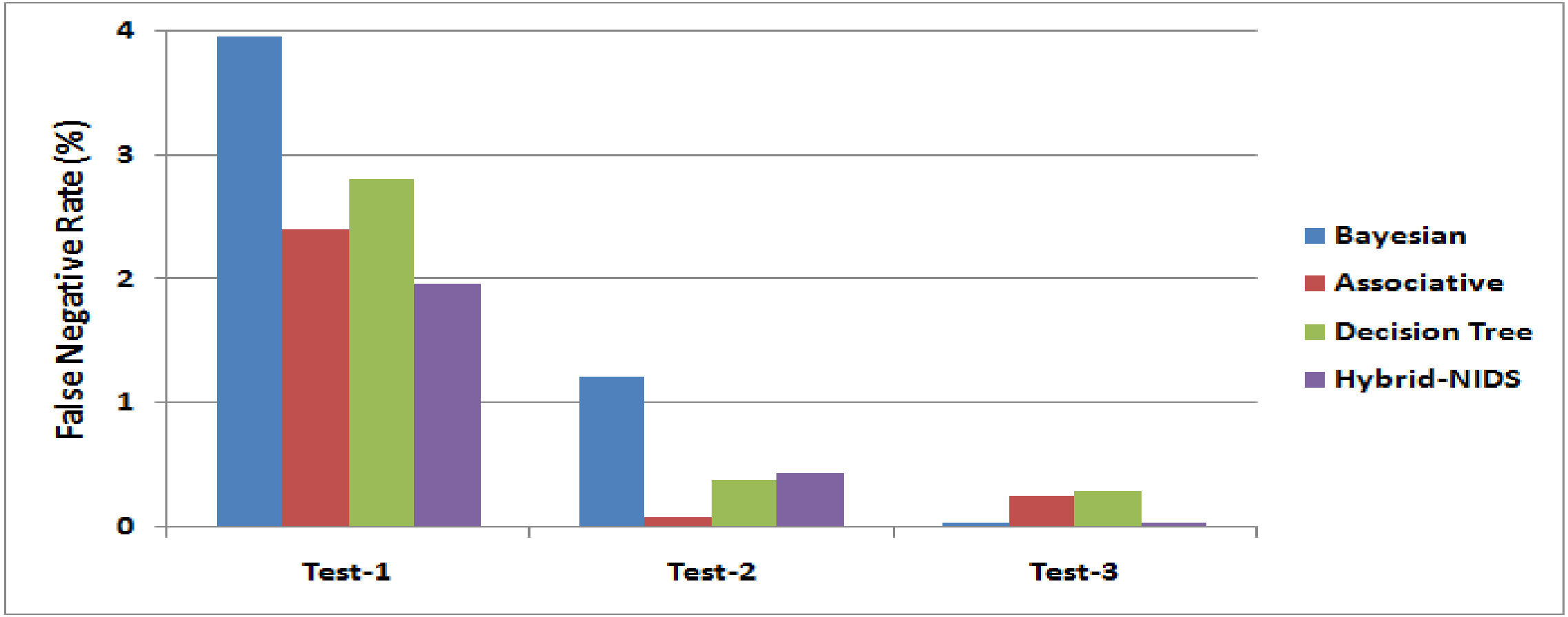
	Training Dataset	Testing Dataset	True Positive Rate (%)			
			Bayesian	Associative	Decision Tree	Hybrid-NIDS
Test-1	KDD99(10%) training dataset	KDD99 test dataset	1.46	14.97	1.76	1.04
Test-2	KDD99(100%) training dataset	KDD99 test dataset	1.02	14.97	1.76	0.63
Test-3	DARPA + CAIDA	DARPA + CAIDA	0.08	6.68	0.05	0.3

Results: Offline Simulation (TNR > 98%)

	Training Dataset	Testing Dataset	True Positive Rate (%)			
			Bayesian	Associative	Decision Tree	Hybrid-NIDS
Test-1	KDD99(10%) training dataset	KDD99 test dataset	98.54	85.03	98.24	98.96
Test-2	KDD99(100%) tra					9.37
Test-3	DA					9.70

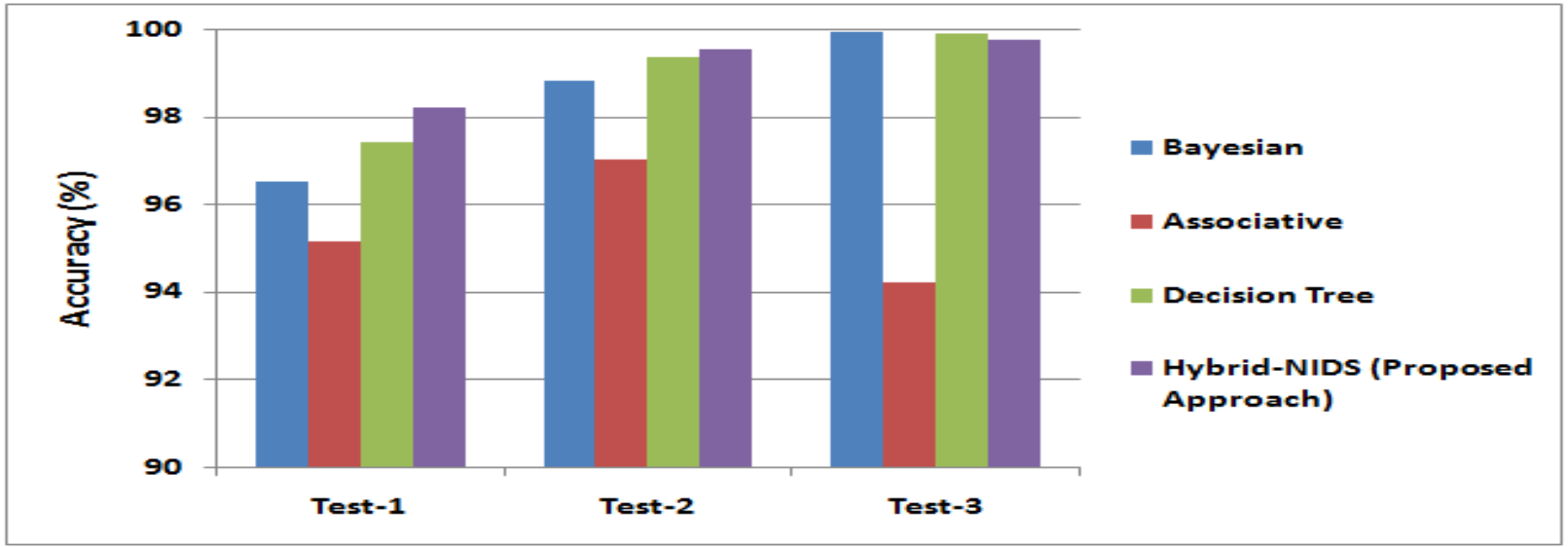


Results: Offline Simulation (FNR < 2%)



Results: Offline Simulation (Accuracy > 98%)

	Training Dataset	Testing Dataset	True Positive Rate (%)			
			Bayesian	Associative	Decision Tree	Hybrid-NIDS
Test-1	KDD99(10%) training dataset	KDD99 test dataset	96.53	95.15	97.4	98.22
Test-2	KDD99(100%) training dataset	KDD99 test dataset	98.82	97.02	99.35	99.52
Test-3	DARPA + CAIDA	DARPA + CAIDA	99.93	94.23	99.91	99.74



Results: Offline Simulation (Detection time)

	Training Dataset	Testing Dataset	Detection time (Seconds)
Test-1	KDD99(10%) training dataset	KDD99 test dataset	19
Test-2	KDD99(100%) training dataset	KDD99 test dataset	19
Test-3	DARPA + CAIDA	DARPA + CAIDA	88

(Detection time is derived on a VM having 32 GB RAM and 2 Core CPU)

- Hybrid-NIDS takes about 19 seconds for inspecting 0.31 million connection profiles.

Results: Overall Performance

Tests	True Positive Rate (%)	False Positive Rate (%)	True Negative Rate (%)	False Negative Rate (%)	Accuracy (%)
Test-1	98.04	1.04	98.96	1.96	98.22
Test-2	99.56	0.63	99.37	0.44	99.52
Test-3	99.96	0.3	99.7	0.04	99.74
Weighted Average	**99.28**	**0.61**	**99.39**	**0.72**	**99.33**

Comparative Analysis

Author/ Year	Technique/Dataset	True positive rate (%)	False alert rate (%)	Accuracy (%)
L. Ibrahim *et al.* /(2013)	SOM-ANN/ KDD, NSL-KDD	92.37	4.67	NA
L. Wang *et al.* / (2013)	Attribute weighted Clustering/ KDD	95.1	5.23	NA
Y. Long *et al.* /(2013)	Fuzzy-SVM/ KDD	88.2	4.5	NA
A. Kannan *et al.* / (2012)	Genetic Algorithm + Fuzzy-SVM / KDD	96.53	3.13	98.51
N Hubballi *et al.* / (2012)	BIRCH Clustering/ KDD	96.97	NA	97.25
R. Naidu *et al.* / (2012)	SVM/KDD	98.03	3.65	NA
Hybrid-NIDS (our proposal)/ (2014)	**Associative, Bayesian and Decision Tree/ KDD, DARPA and CAIDA**	**99.28**	**0.61**	**99.33**

NA- Not Available

Cloud IDS Requirement Analysis

- Requirement 1 - R1: Handling High Traffic Volume
- Requirement 2 - R2: Detecting variety of attacks With least false alerts
- Requirement 3 - R3: Fast detection
- Requirement 4 - R4: Scalability
- Requirement 5 - R5: Securing Cloud components (VM, Host m/c, Cloud Controller)
- Requirement 6 - R6: Resistance to compromise

Cloud IDS Requirement Analysis

Author/ Year	R1	R2	R3	R4	R5	R6
S. Roschke *et al.* [26]/ (2009)	✓	×	✓	×	P	×
Bakshi *et al.* [22]/ (2010)	×	×	✓	✓	✓	✓
Mazzariello *et al.* [12]/ (2010)	✓	×	✓	P	×	×
C. C. Lo *et al.* [13]/ (2008)	✓	✓	×	NA	×	×
Gul *et al.* [14]/ (2011)	×	×	✓	×	P	×
Sandar *et al.* [15]/ (2012)	✓	×	✓	NA	×	×
Yassin *et al.* [24]/ (2012)	NA	×	✓	NA	NA	×
Houmansadr *et al.* [25]/ (2011)	NA	×	✓	NA	NA	×
Vieira *et al.* [16]/ (2010)	×	✓	×	✓	×	✓
Lee *et al.* [17]/ (2011)	×	✓	✓	NA	✓	×
Dastjerdi *et al.* [20]/ (2009)	×	NA	NA	✓	×	NA
Dhage *et al.* [27]/ (2012)	✓	✓	×	✓	×	×
Kholidy *et al.* [23]/ (2012)	✓	×	×	×	✓	✓
S. Ramteke *et al.* [18]/ (2012)	×	✓	✓	×	P	×
S. Gupta *et al.* [19]/ (2013)	✓	✓	✓	×	P	×
F. Idrees *et al.* [21]/ (2013)	✓	P	✓	×	✓	×
Our Framework: Hybrid-NIDS (2014)	✓	✓	✓	✓	✓	**P**

(P: Partially satisfy, ✓: completely satisfy, ×: do not satisfy, NA: Not applicable)

Dark cloud: detection and mitigation

- To build hypervisor based security framework to monitor and detect in-VM user's malicious activity

Adversary Model

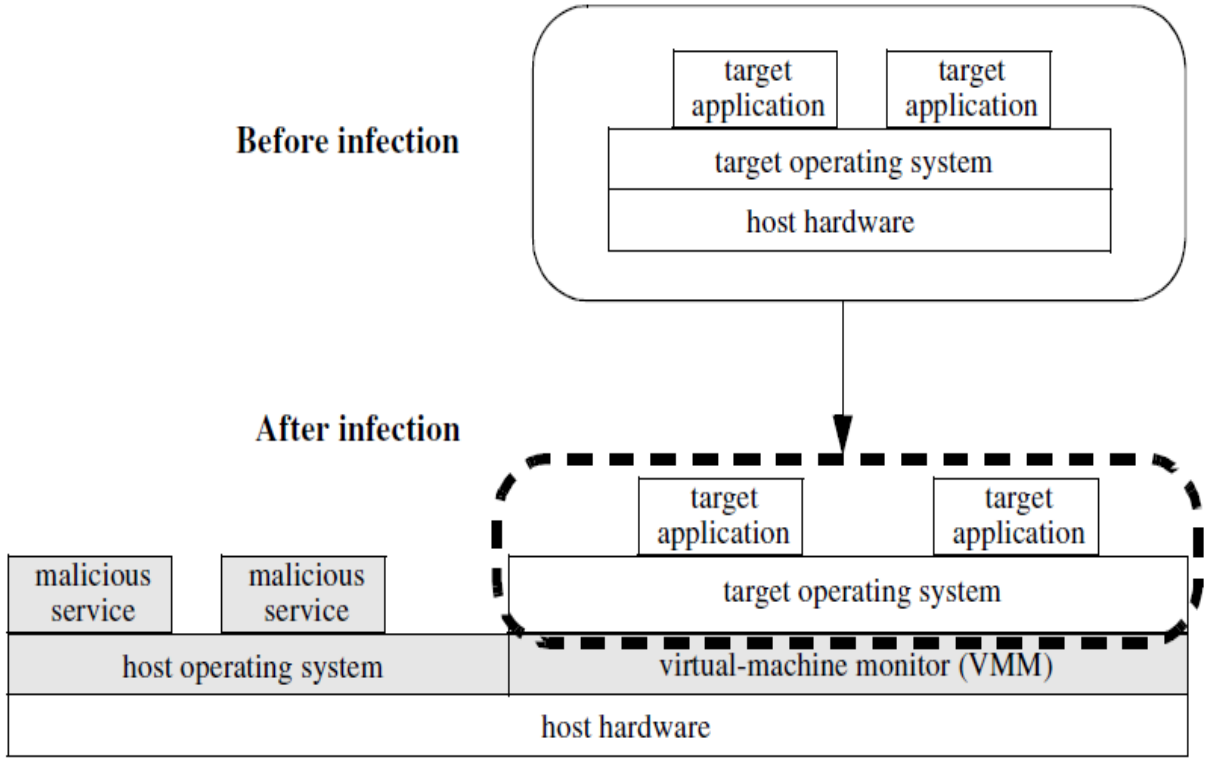
- Goal
  - hosts malicious code on cloud resources
- Capability
  - restricted by capabilities of the VMs
- Communication Channel
  - VM access – SSH, RDP etc.
  - no direct control over cloud firewall
  - can not intercept communication between VMs and hypervisor

Security Threats in Virtualization

- VM Escape
- VM Monitoring from the host
- VM Monitoring from another VM
- Communication between VMs or between VMs and host
- Denial of Service
- Guest-to-Guest attack
- External modification of a VM
- External modification of the hypervisor
- VM based Rootkit (VMBR)/Malware

VM based Rootkit (VMBR) & Malware

- VM based Rootkit
  - Blue Pill
  - SubVirt



Virtual Machine Subverting

- VM based Malware
  - DKSM (Direct Kernel Structure Manipulation)

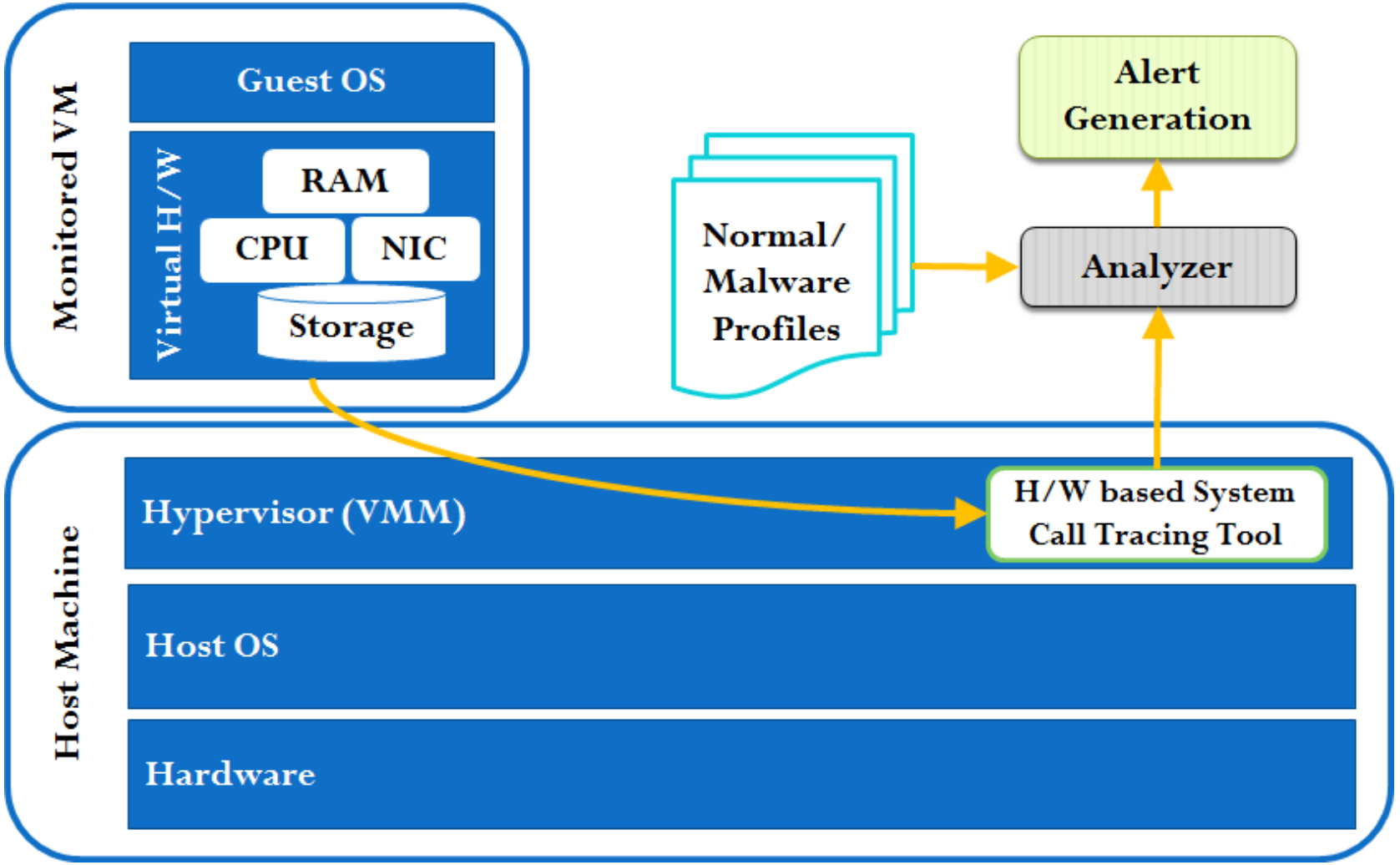
Direct Kernel Structure Manipulation (DKSM)

- DKSM is an attack which can effectively subvert and confound existing VM introspection tools.
- Most of existing VMI tools rely upon the fact that the underlying guest OS is conforming to certain behaviors and idioms
  - It uses set of data structures of guest OS being introspected as templates to interpret VMM-level VM observation
- With DKSM it is possible to compromise a guest such that the kernel's use of any field of its data structures (or templates) could be potentially modified.

Research Progress

- <Jan. 2011 - Dec. 2012>
  - VMI Libraries to bridge the semantic gap
  - VM system call tracing approaches
- <July. 2013>
  - Malware Detection using System Calls
  - Malware Detection at Hypervisor level in Cloud
- <Dec. 2013>
  - Data representation – Vector Space Model with tf-idf
  - Generating behavioral model
- <July. 2014>
  - SVM with RBF kernel for classification
  - Live detection framework on stand alone system

Dark cloud detection and Mitigation system framework



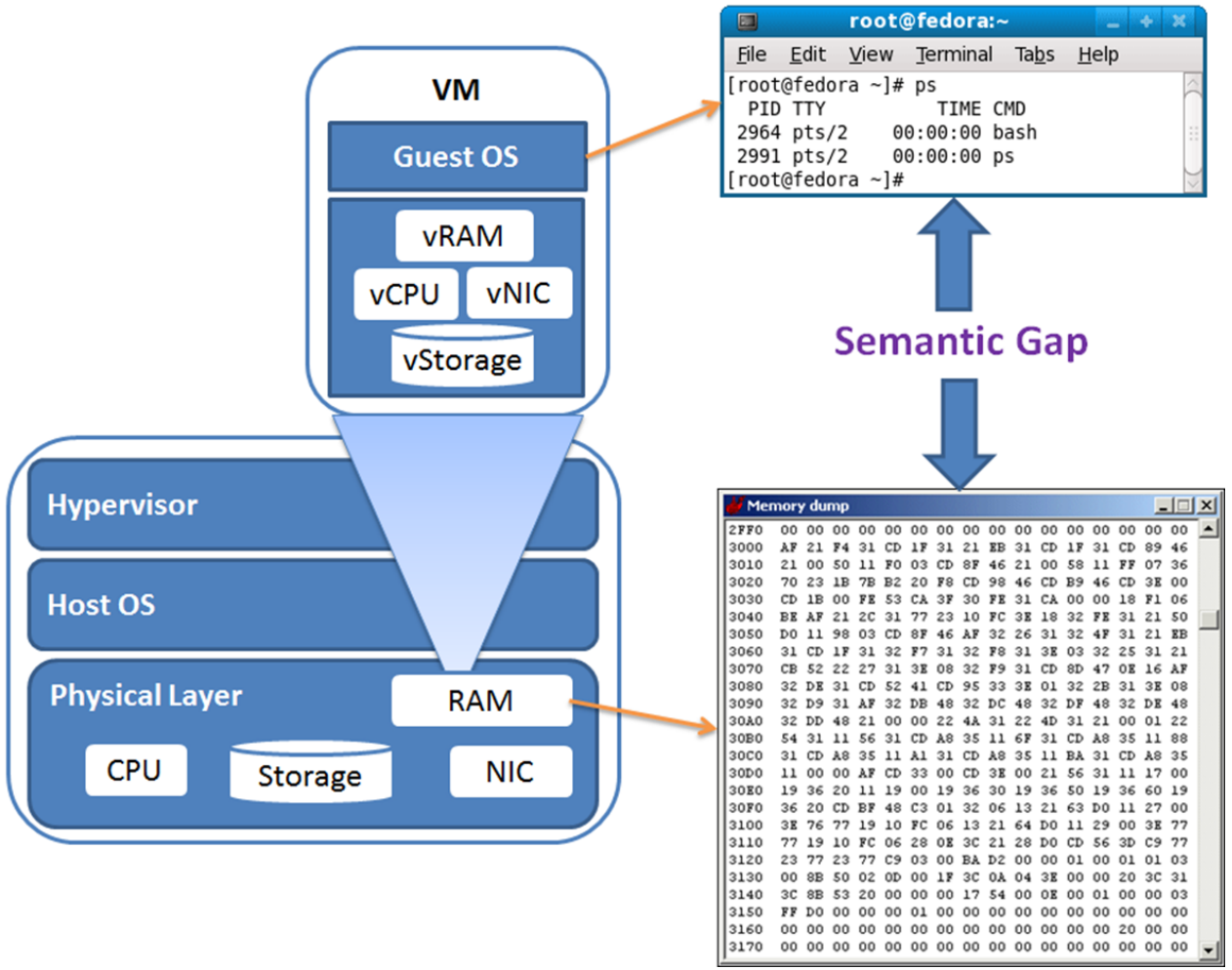
Virtual Machine Introspection

- Virtual Machine Introspection is a technique to monitor and analyze the guest operating system state from outside.
  - It enables monitoring of VMs from the outside, at a hypervisor level
  - from the outside of VM, at a hypervisor level, only hardware-level raw byes can be observed
  - from inside the VM, we can view high-level entities such as processes, I/O requests, and system calls
  - The difference in view is called the semantic gap

VMI - Semantic Gap

- Pfoh et al. present three view-generation patterns to bridge semantic gap
  - Out-of-band delivery
    - semantic knowledge is delivered by an external function
    - VMM may make use of a previously delivered symbol table based on the guest OS kernel
  - In-band delivery
    - an internal component creates a view and delivers this view to the VMM
  - Derivation
    - derives information through semantic knowledge of the hardware architecture

Semantic Gap

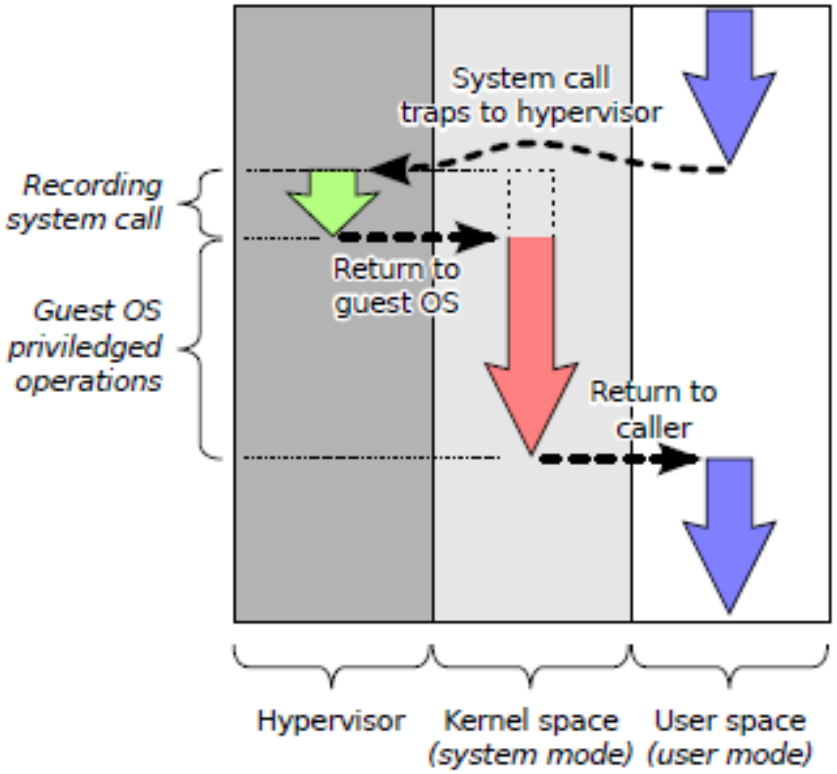


Nitro

- Nitro [] extends the Linux Kernel Virtual Machine (KVM) to support system call trapping for VMI applications.
  - It can trace all system call mechanisms of Intel x86 architecture.
  - Works for Windows, Linux 32-bit and 64-bit guests.
  - Uses derivation approach to bridge semantic gap.
  - Properties: Guest OS independent, Evasion Resistant.
  - Consists of QEMU monitor and set of Linux kernel modules.
  - Modifies KVM to support new commands.

Nitro – System Call Trapping Mechanisms

- Forces system interrupts for which trapping is supported by the Intel Virtualization Extensions (VT-x)

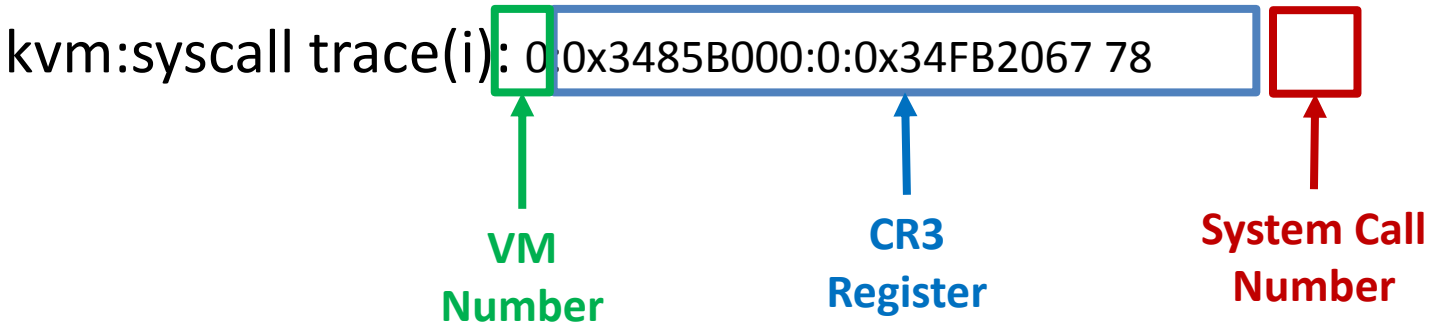


Control flow of a system call that traps to the hypervisor

Nitro

- Process identification
  - Which process created the system call is identified by CR3 register.
- Guest OS portability
  - Nitro depends on hardware knowledge only
- Evasion Resistant
  - VMI mechanism of Nitro is rooted in hardware and each involved piece of VM state is protected against manipulation.

Extracting Values from Nitro output



Modified Vector Space Representation

Sample list of system calls

Open	1
Close	2
Read	3
Write	4
Exit	5
Time	6
mmap	7
Idle	8
Unknown	9

Sample system call traces

S1: 1, 3, 3, 3, 4, 4, 2, 5

S2: 2

S3: 1, 3

2-gram Representation (term-size 2)

	1, 3	2, 5	2, 9	3, 3	3, 4	4, 2	4, 4	9, 9
S1:	1	1	0	2	1	1	1	0
S2:	0	0	1	0	0	0	0	0
S3:	1	0	0	0	0	0	0	0

Vector Space Model Representation

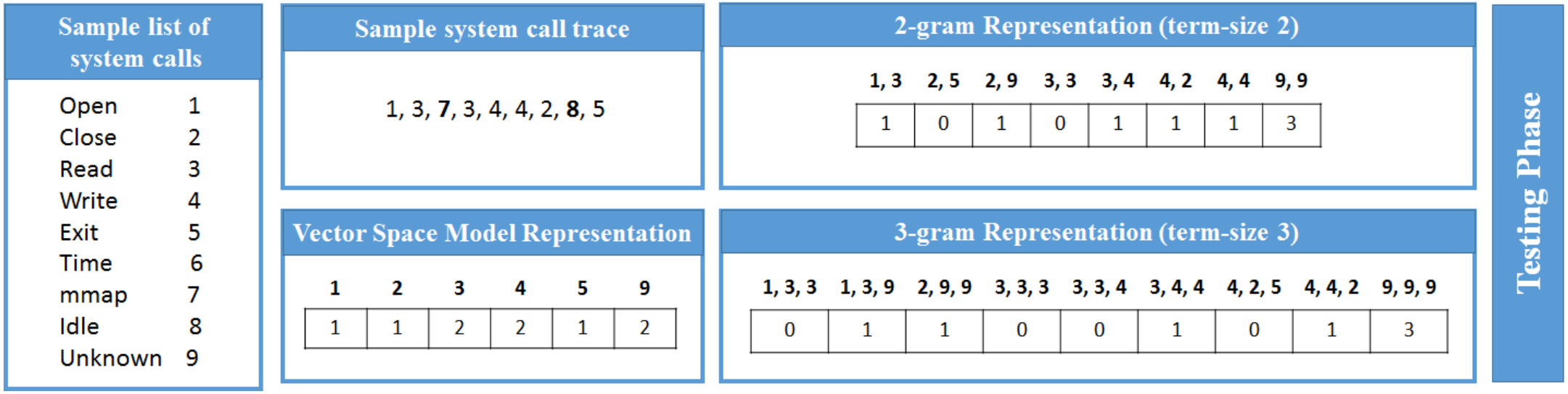
	1	2	3	4	5	9
S1:	1	1	3	2	1	0
S2:	0	1	1	0	0	0
S3:	1	0	1	0	0	0

3-gram Representation (term-size 3)

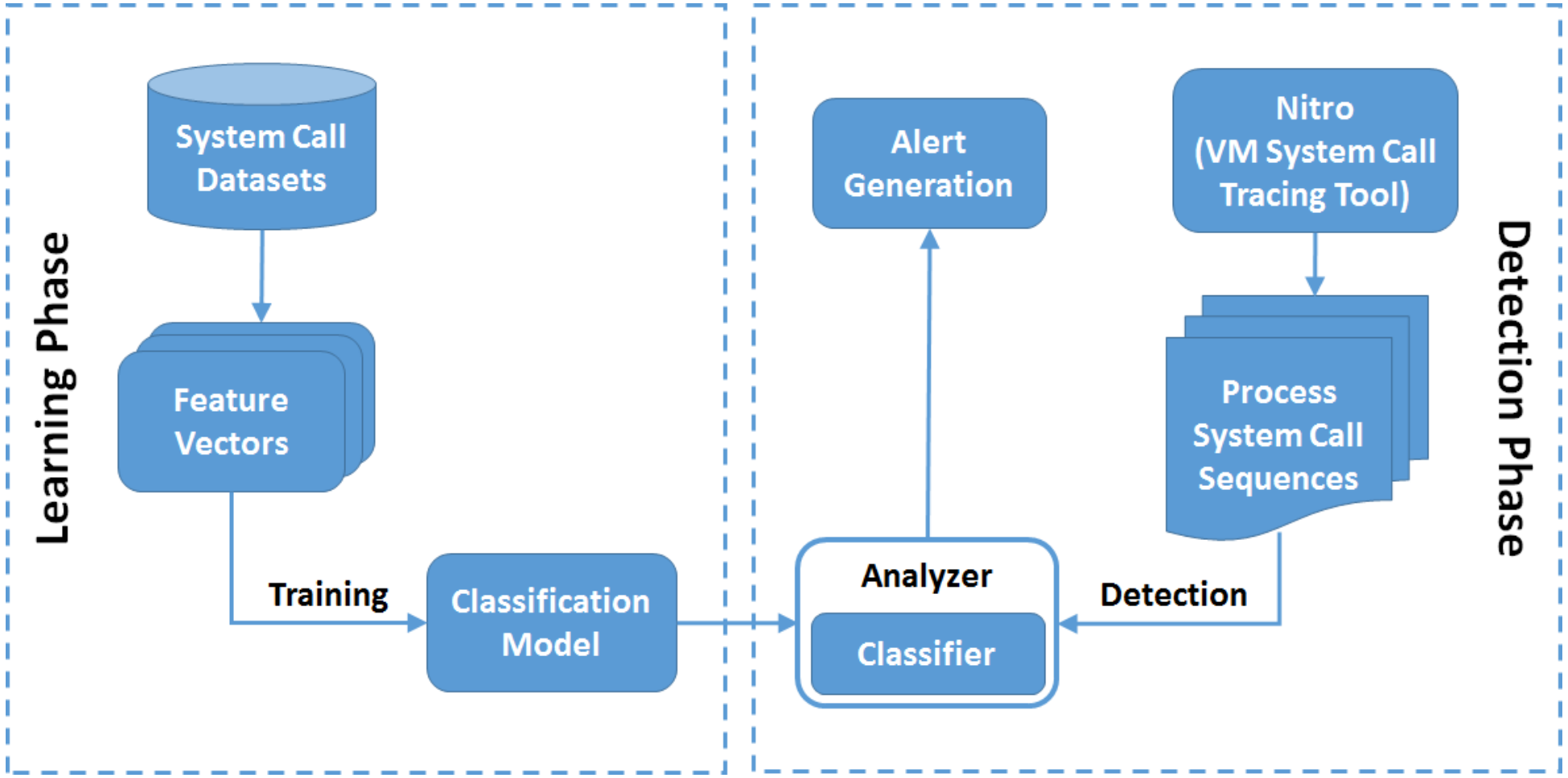
	1, 3, 3	1, 3, 9	2, 9, 9	3, 3, 3	3, 3, 4	3, 4, 4	4, 2, 5	4, 4, 2	9, 9, 9
S1:	1	0	0	1	1	1	1	1	0
S2:	0	0	1	0	0	0	0	0	0
S3:	0	1	0	0	0	0	0	0	0

Training Phase

Modified Vector Space Representation (Cont…)



System Phases



Learning Phase (Datasets used)

Dataset	Number of System Call Traces	Number of System Call
Malware	5,855	3,28,99,160
Goodware	612	65,55,20,685
Malware-Test	1,133	1,31,88,452
Anubis-Good	36	44,127
Total	7,838	70,16,52,424

Term-Size

- Number of features generated for different term-size

Term-Size	Number of Features
1	65
2	2,188
3	27,508

Evaluation Metrics

		Actual Class		
		Malware	**Goodware**	**Total**
Predicted Class	**Malware**	TP	FP	TP + FP
	Goodware	FN	TN	FN + TN
	Total	TP + FN	FP + TN	

Confusion Matrix

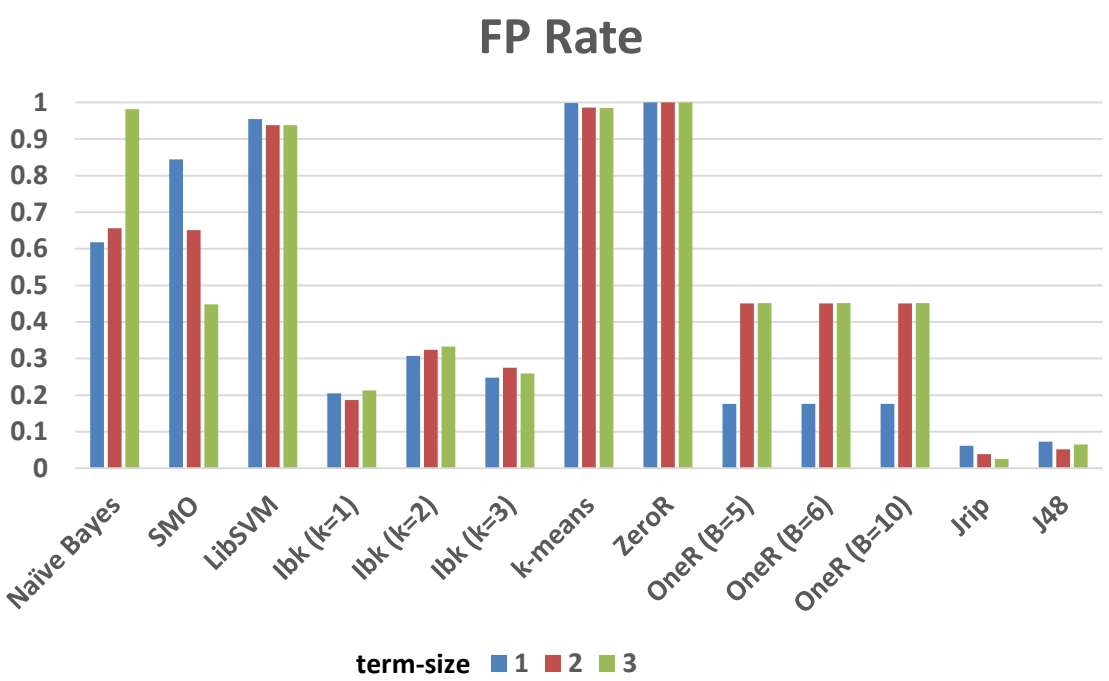
- $Precision = \frac{TP}{TP+FP}$
- $Recall = \frac{TP}{TP+FN}$
- $Accuracy = \frac{TP+TN}{TP+FP+TN+FN}$
- $FP\ Rate = \frac{FP}{FP+TN}$
- $F\ Measure = \frac{2}{\frac{1}{Precision}+\frac{1}{Recall}}$

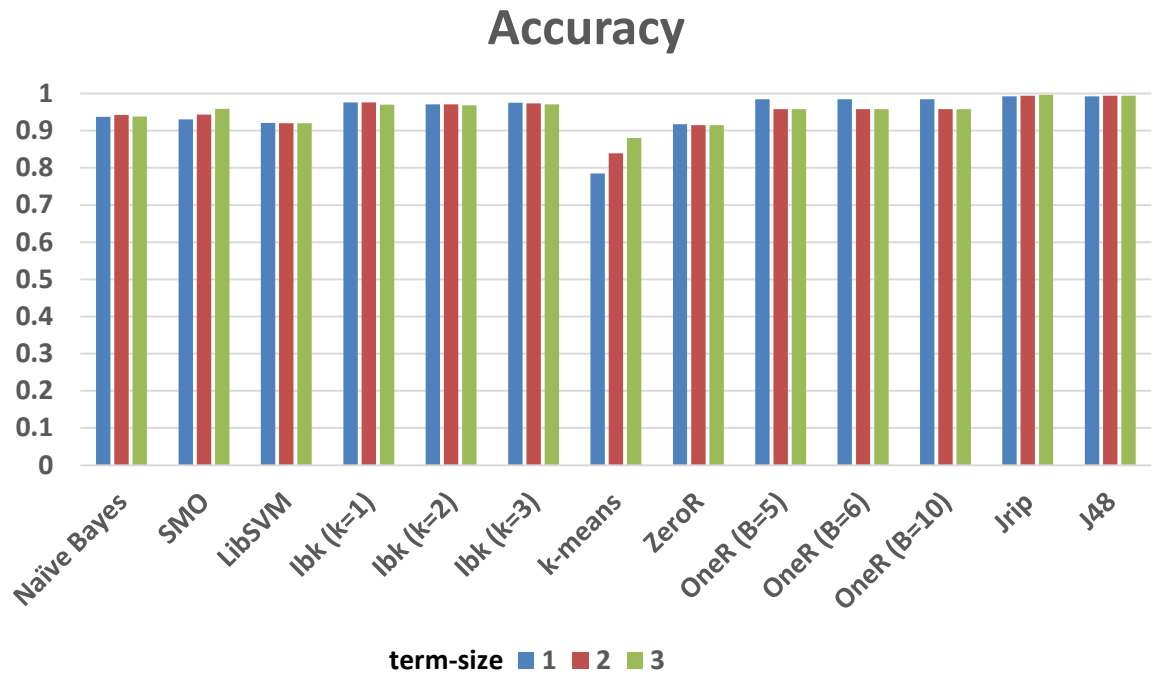
Evaluation

- Algorithms Selected in Weka for Experiments

Sr. No.	Category	Algorithm	Option Selected
1	Bayes	Naïve Bayes	--
2	Function	Sequential Minimal Optimization (SMO)	Polynomial Kernel
3		Support Vector Machine (LibSVM)	Radial Basis Function (RBF) Kernel, gamma=0.5, loss=0.001
4	Lazy	k-nearest neighbors (IBk)	k=1, 2, 3
5	Meta	Classification via Clustering – SimpleKMeans	k=2
6	Rules	ZeroR	--
7		OneR	minBucketSize(B) = 5, 6, 10
8		JRip	Folds=3
9	Trees	J48	confidenceFactor=0.25, minNumObj=2

Results

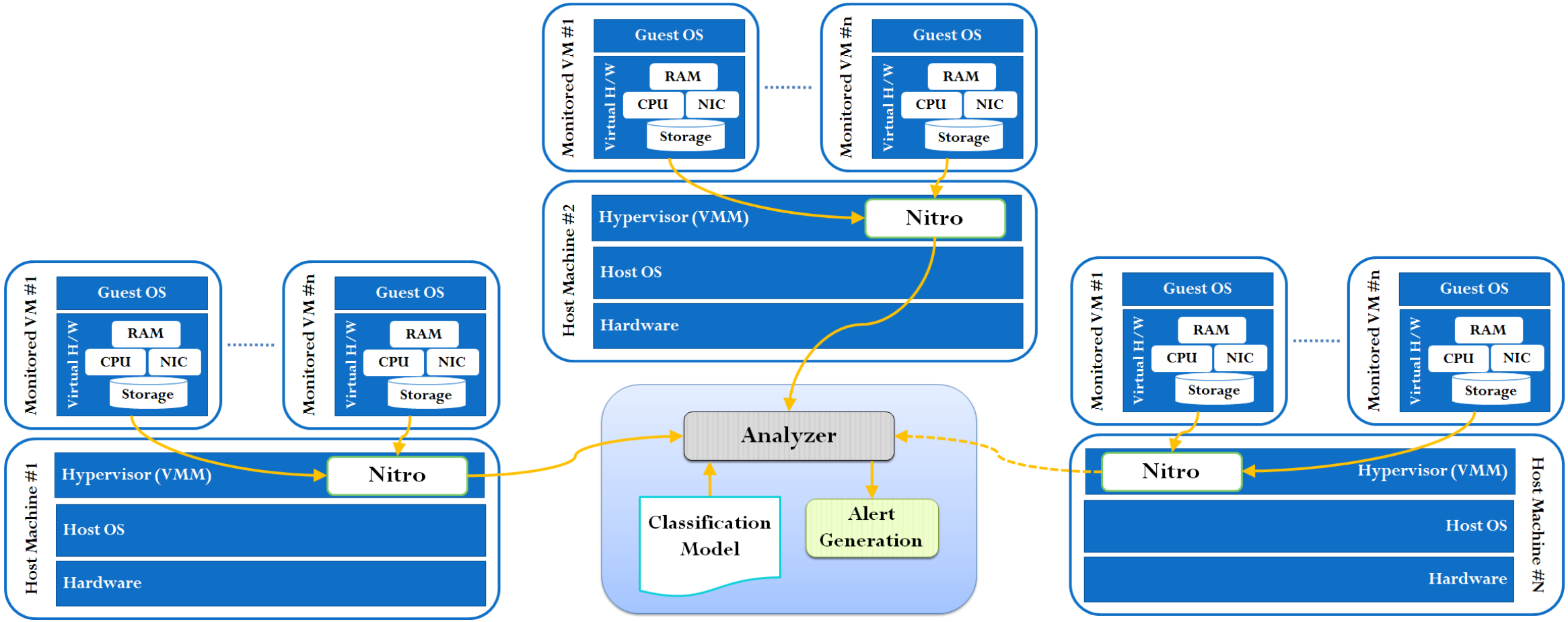

FP Rate
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Naïve Bayes
SMO
LibSVM
Ibk (k=1)
Ibk (k=2)
Ibk (k=3)
k-means
ZeroR
OneR (B=5)
OneR (B=6)
OneR (B=10)
Jrip
J48
term-size 1 2 3

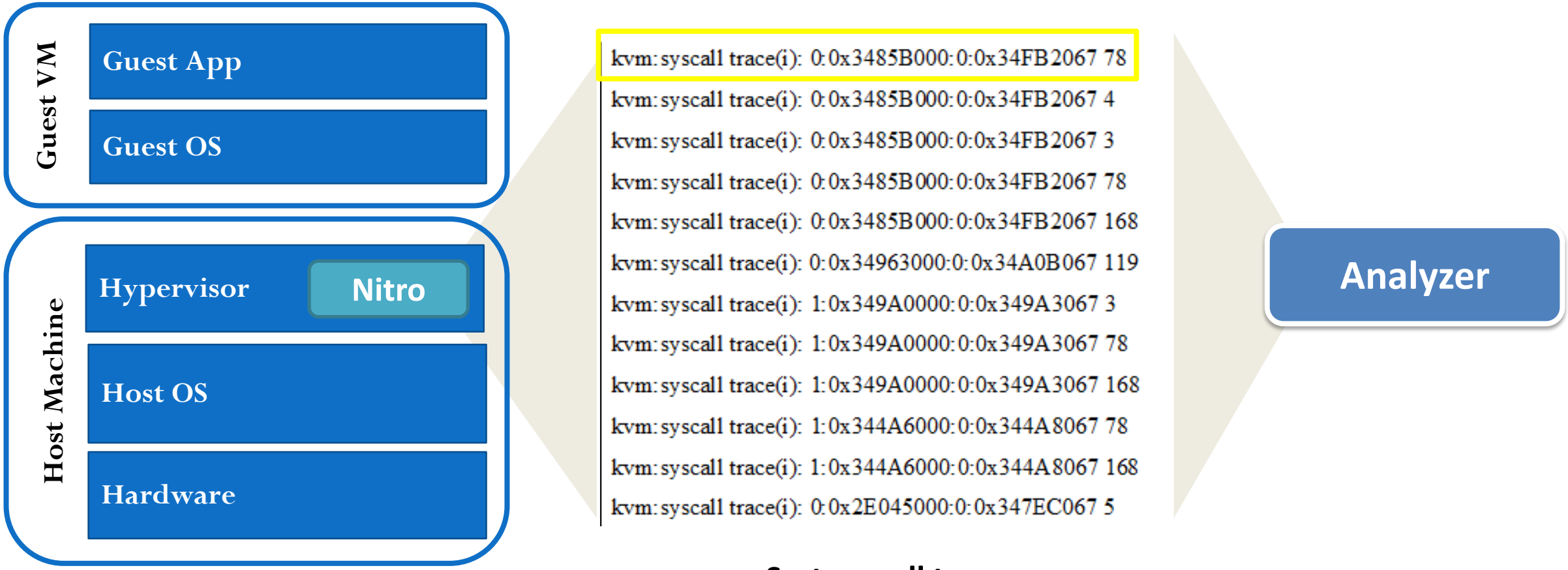

Accuracy
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Naïve Bayes
SMO
LibSVM
Ibk (k=1)
Ibk (k=2)
Ibk (k=3)
k-means
ZeroR
OneR (B=5)
OneR (B=6)
OneR (B=10)
Jrip
J48
term-size 1 2 3

Live Detection Framework

DETECTION PHASE

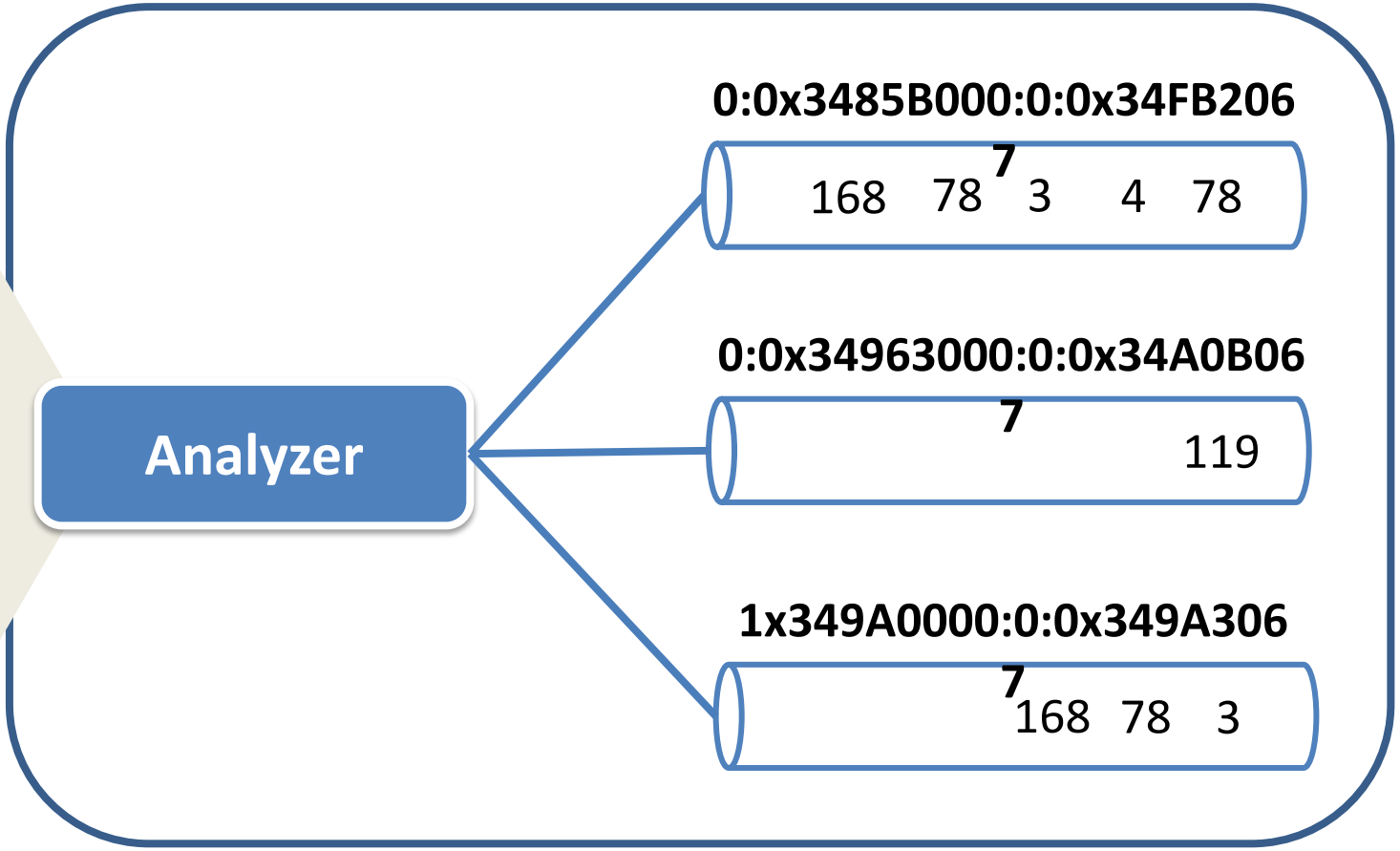
System Architecture



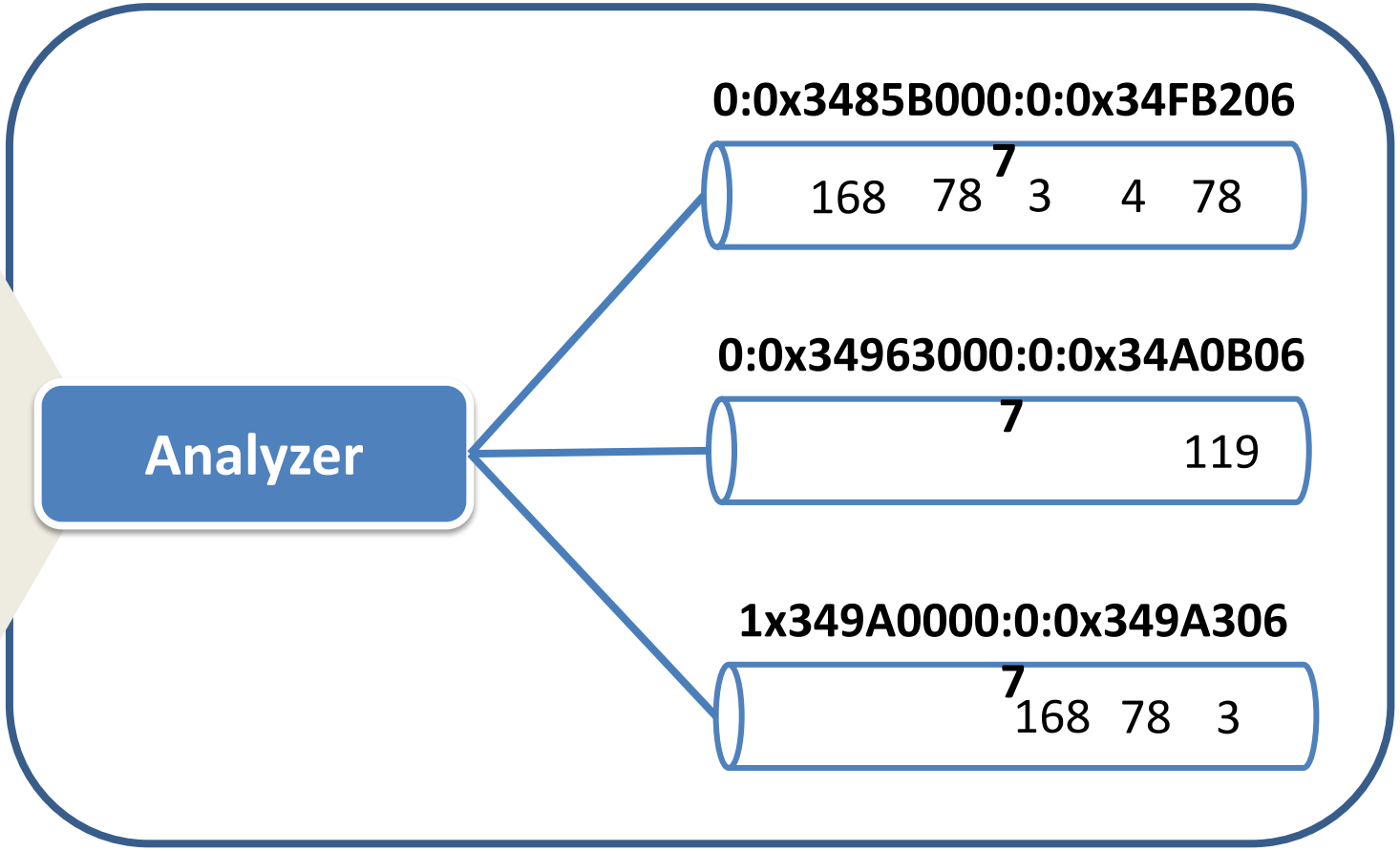


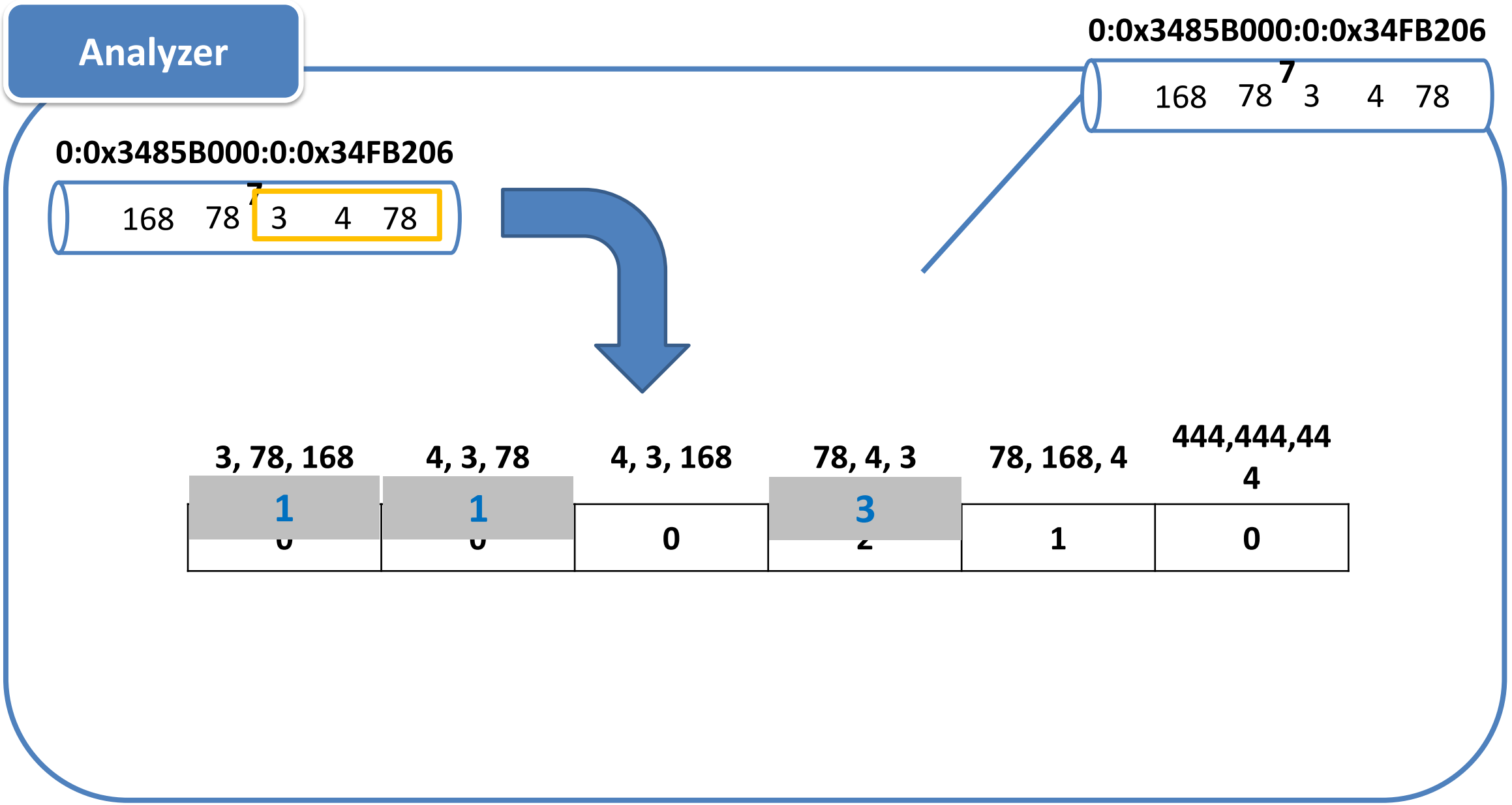
System call trace

```
kvm:syscall trace(i): 0:0x3485B000:0:0x34FB2067 78
kvm:syscall trace(i): 0:0x3485B000:0:0x34FB2067 4
kvm:syscall trace(i): 0:0x3485B000:0:0x34FB2067 3
kvm:syscall trace(i): 0:0x3485B000:0:0x34FB2067 78
kvm:syscall trace(i): 0:0x3485B000:0:0x34FB2067 168
kvm:syscall trace(i): 0:0x34963000:0:0x34A0B067 119
kvm:syscall trace(i): 1:0x349A0000:0:0x349A3067 3
kvm:syscall trace(i): 1:0x349A0000:0:0x349A3067 78
kvm:syscall trace(i): 1:0x349A0000:0:0x349A3067 168
kvm:syscall trace(i): 1:0x344A6000:0:0x344A8067 78
kvm:syscall trace(i): 1:0x344A6000:0:0x344A8067 168
kvm:syscall trace(i): 0:0x2E045000:0:0x347EC067 5
```



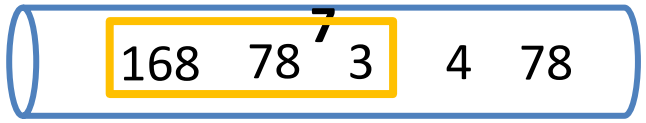
```
kvm:syscall trace(i): 0:0x3485B000:0:0x34FB2067 78
kvm:syscall trace(i): 0:0x3485B000:0:0x34FB2067 4
kvm:syscall trace(i): 0:0x3485B000:0:0x34FB2067 3
kvm:syscall trace(i): 0:0x3485B000:0:0x34FB2067 78
kvm:syscall trace(i): 0:0x3485B000:0:0x34FB2067 168
kvm:syscall trace(i): 0:0x34963000:0:0x34A0B067 119
kvm:syscall trace(i): 1:0x349A0000:0:0x349A3067 3
kvm:syscall trace(i): 1:0x349A0000:0:0x349A3067 78
kvm:syscall trace(i): 1:0x349A0000:0:0x349A3067 168
kvm:syscall trace(i): 1:0x344A6000:0:0x344A8067 78
kvm:syscall trace(i): 1:0x344A6000:0:0x344A8067 168
kvm:syscall trace(i): 0:0x2E045000:0:0x347EC067 5
```

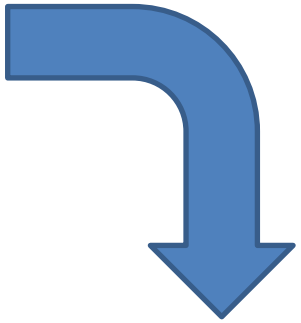



Analyzer
0:0x3485B000:0:0x34FB206
168 78 7 3 4 78
0:0x3485B000:0:0x34FB206
168 78 7 3 4 78
3, 78, 168
4, 3, 78
4, 3, 168
78, 4, 3
78, 168, 4
444,444,444
1
1
0
3
1
0
0
0
2

Analyzer

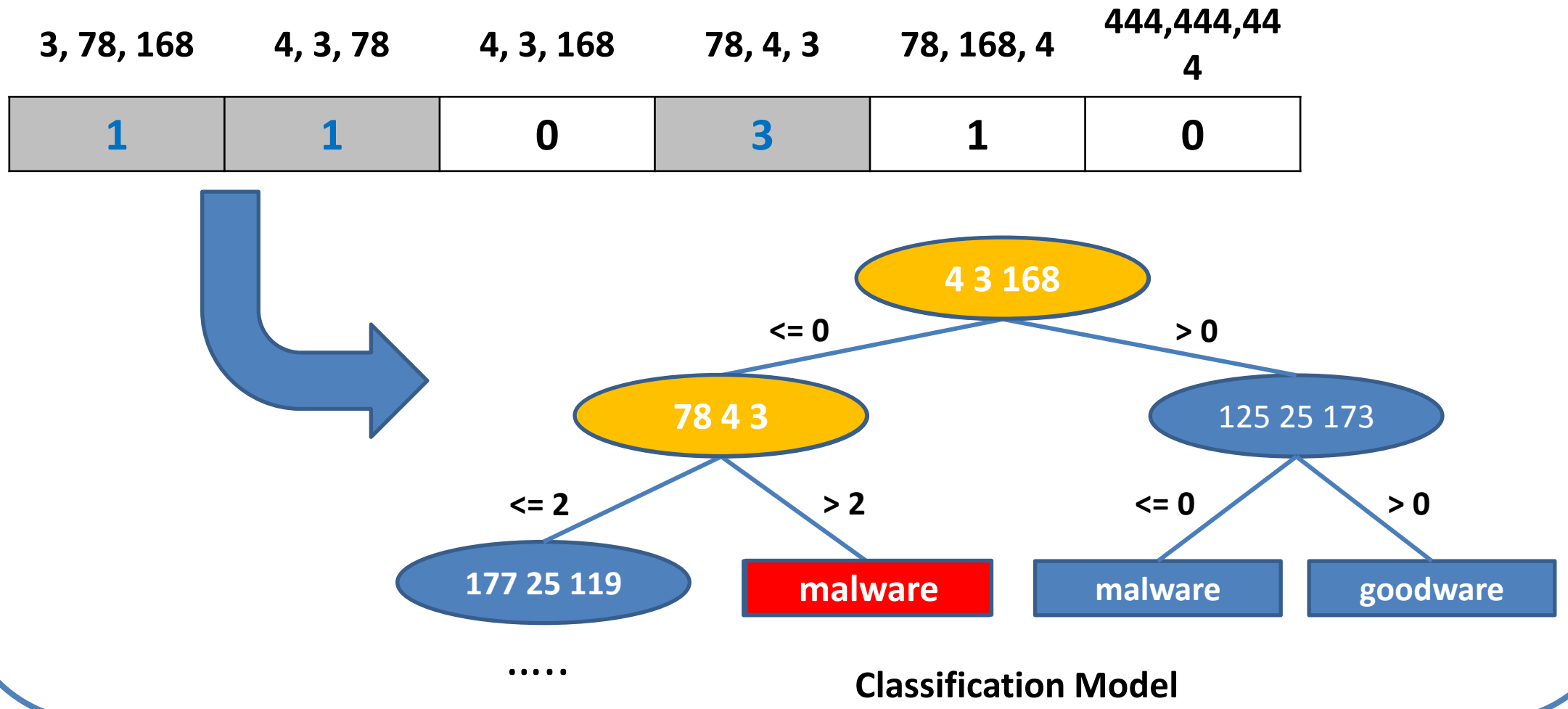
0:0x3485B000:0:0x34FB206





3, 78, 168	4, 3, 78	4, 3, 168	78, 4, 3	78, 168, 4	444,444,444
1	1	0	3	1	0

Analyzer


3, 78, 168
4, 3, 78
4, 3, 168
78, 4, 3
78, 168, 4
444,444,444
1
1
0
3
1
0
4 3 168
<= 0
> 0
78 4 3
125 25 173
<= 2
> 2
<= 0
> 0
177 25 119
malware
malware
goodware
.....
Classification Model

System Call Tracing of VM

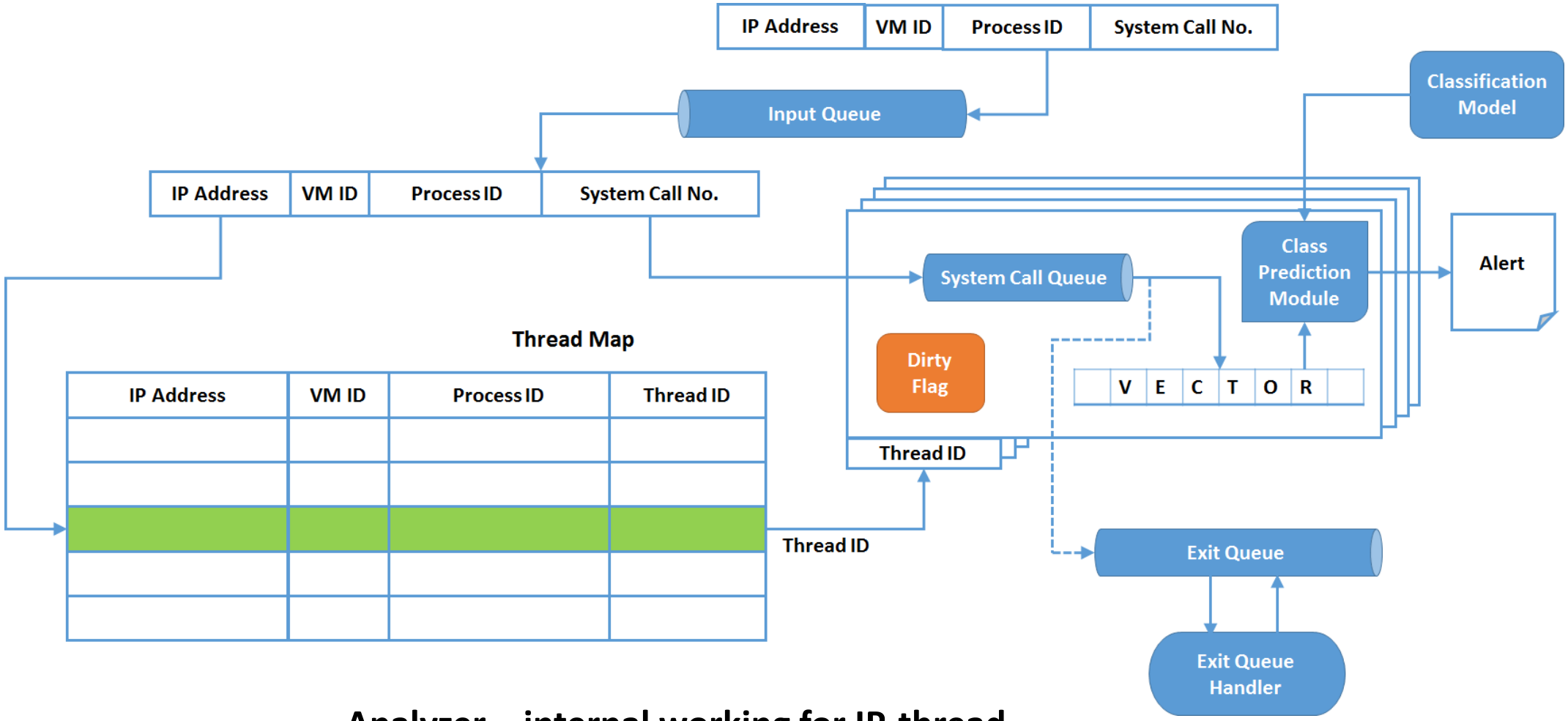
- Nitro Output and Message Format

172.16.10.100 11:0x3485B000:0:0x34FB2067 78

IP Address 172.16.10.100
VM Number 11
Process ID 0x3485B000:0:0x34FB2067
System Call 78

Extracting Values from Nitro output

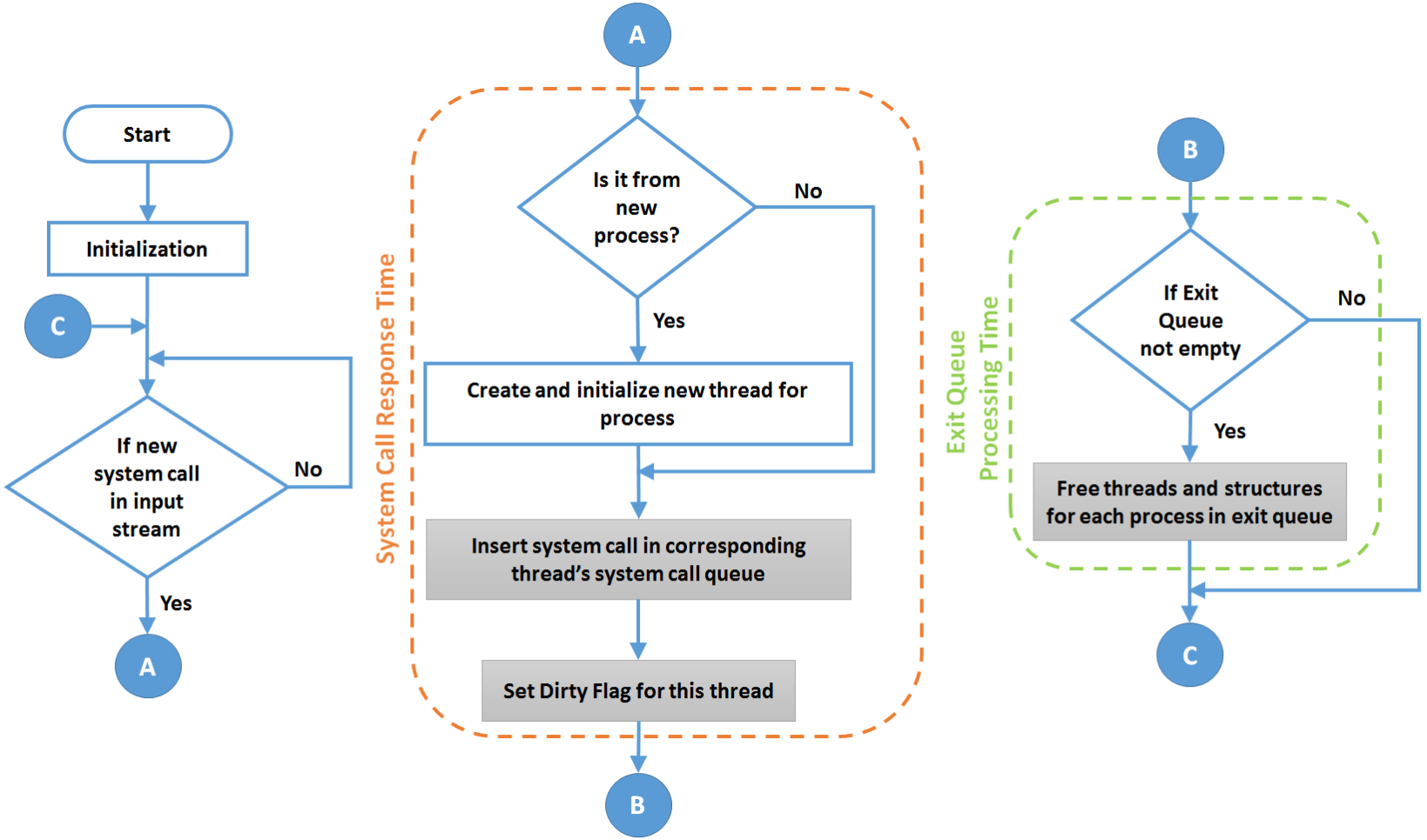
Analyzer



Analyzer – internal working for IP-thread

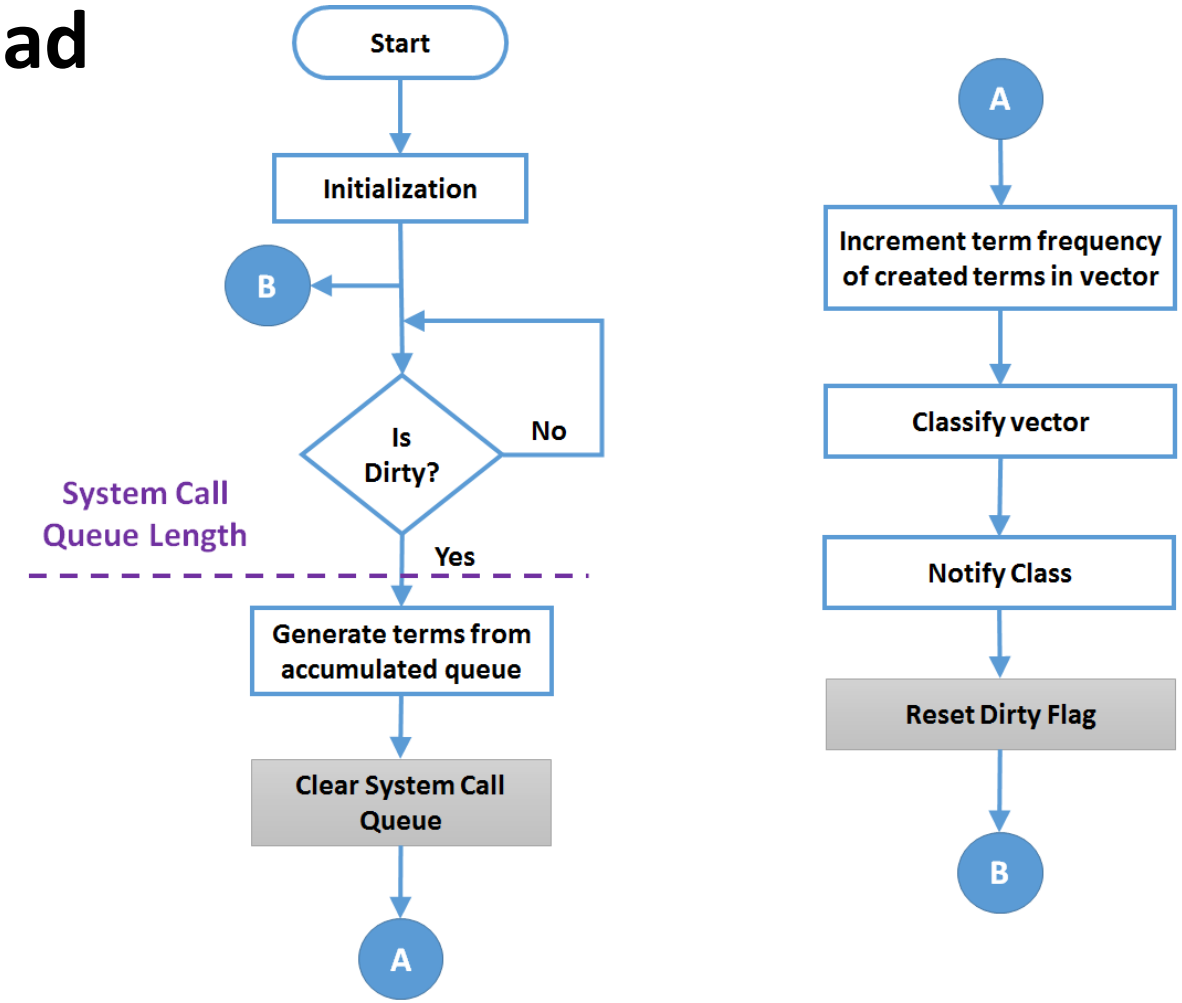
Flow Charts

- **IP-thread**



Flow Charts

- **Process-thread**



Experimental Setup

- Experiments are conducted on four physical machines with following evaluation settings

- J48 model for term-size 3
- 4 Host and 4 VMs
- PCMark05 Benchmark

Evaluation Metrics

Average Response Time:

- This is the time taken for an arrived system call to be inserted in its corresponding system call queue.
- This primarily measures the performance of the IP-thread.

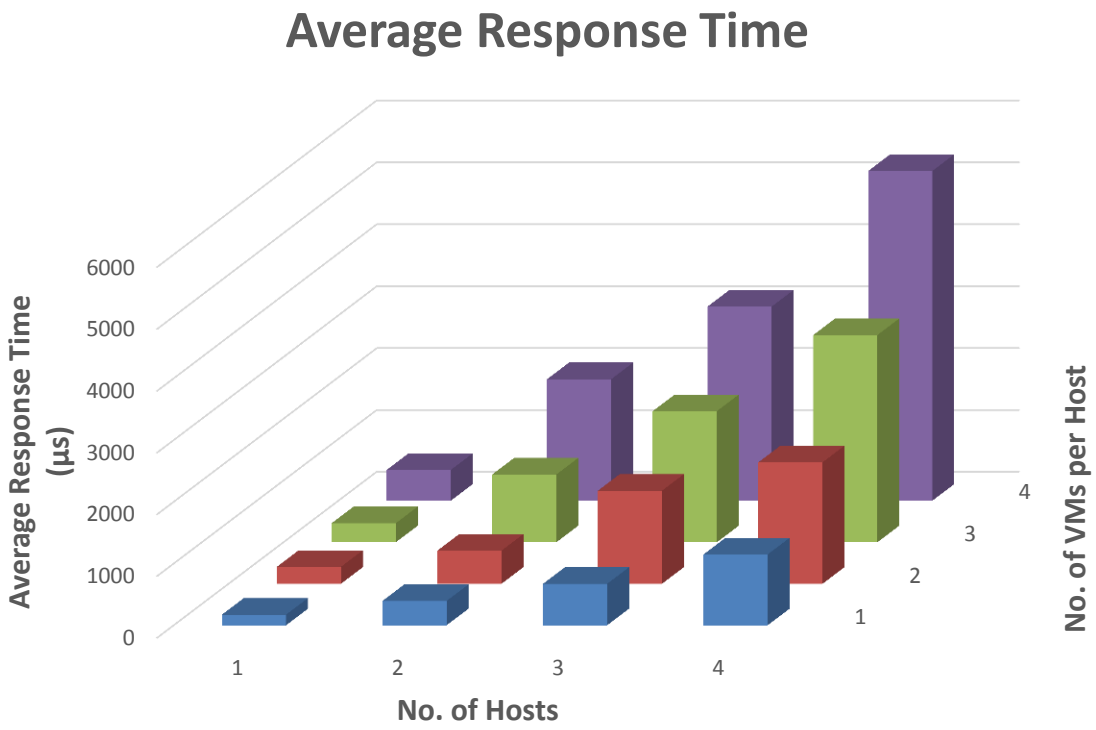
Average System Call Queue Length:

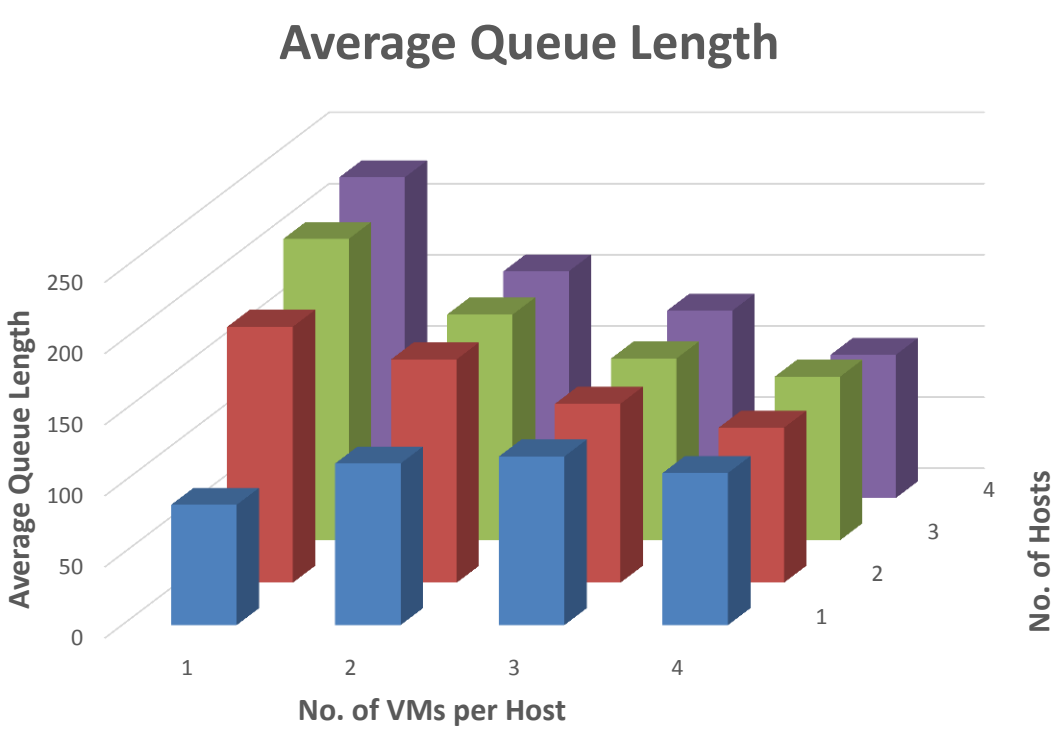
- This is the average number of system calls that are waiting in System Call Queue between process classifications.
- This primarily measures the performance of the process thread.

Average Exit Queue Processing Time:

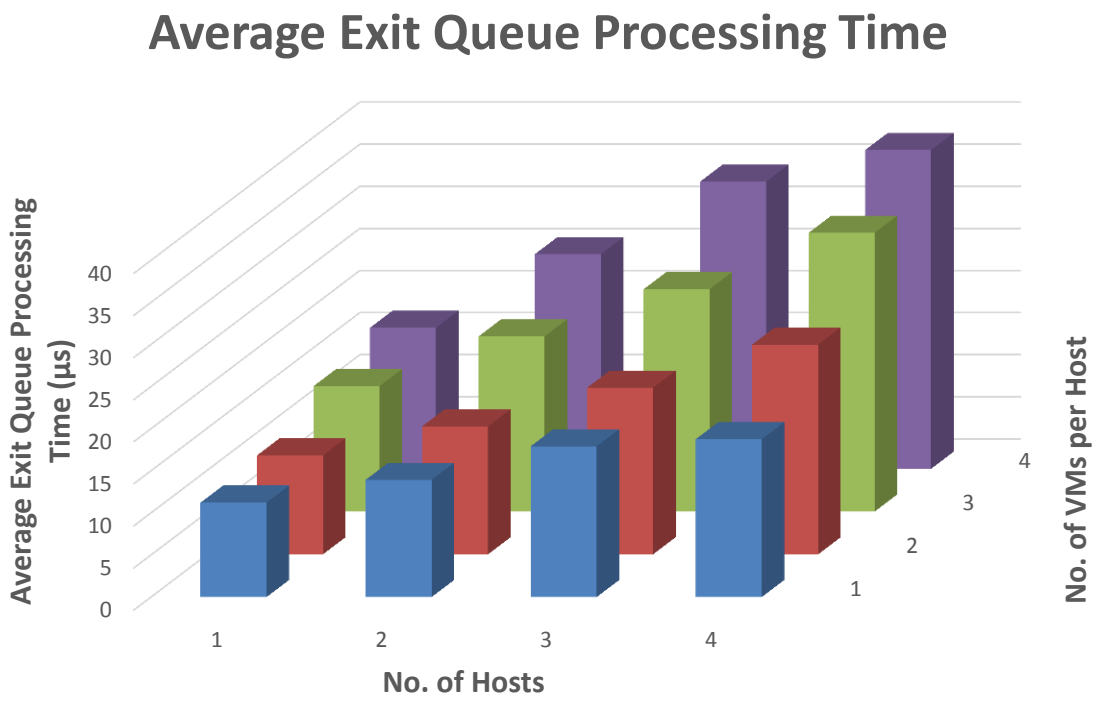
- This is the average time required to process the exit queue.
- Its processing comprises of vanishing each thread's entry in global data structures and deleting the thread itself.

Results


Average Response Time
Average Response Time (µs)
0
1000
2000
3000
4000
5000
6000
1
2
3
4
No. of Hosts
1
2
3
4
No. of VMs per Host


Average Queue Length
Average Queue Length
0
50
100
150
200
250
1
2
3
4
No. of VMs per Host
1
2
3
4
No. of Hosts

Results


Average Exit Queue Processing Time
Average Exit Queue Processing Time (µs)
0
5
10
15
20
25
30
35
40
1
2
3
4
No. of Hosts
No. of VMs per Host
1
2
3
4

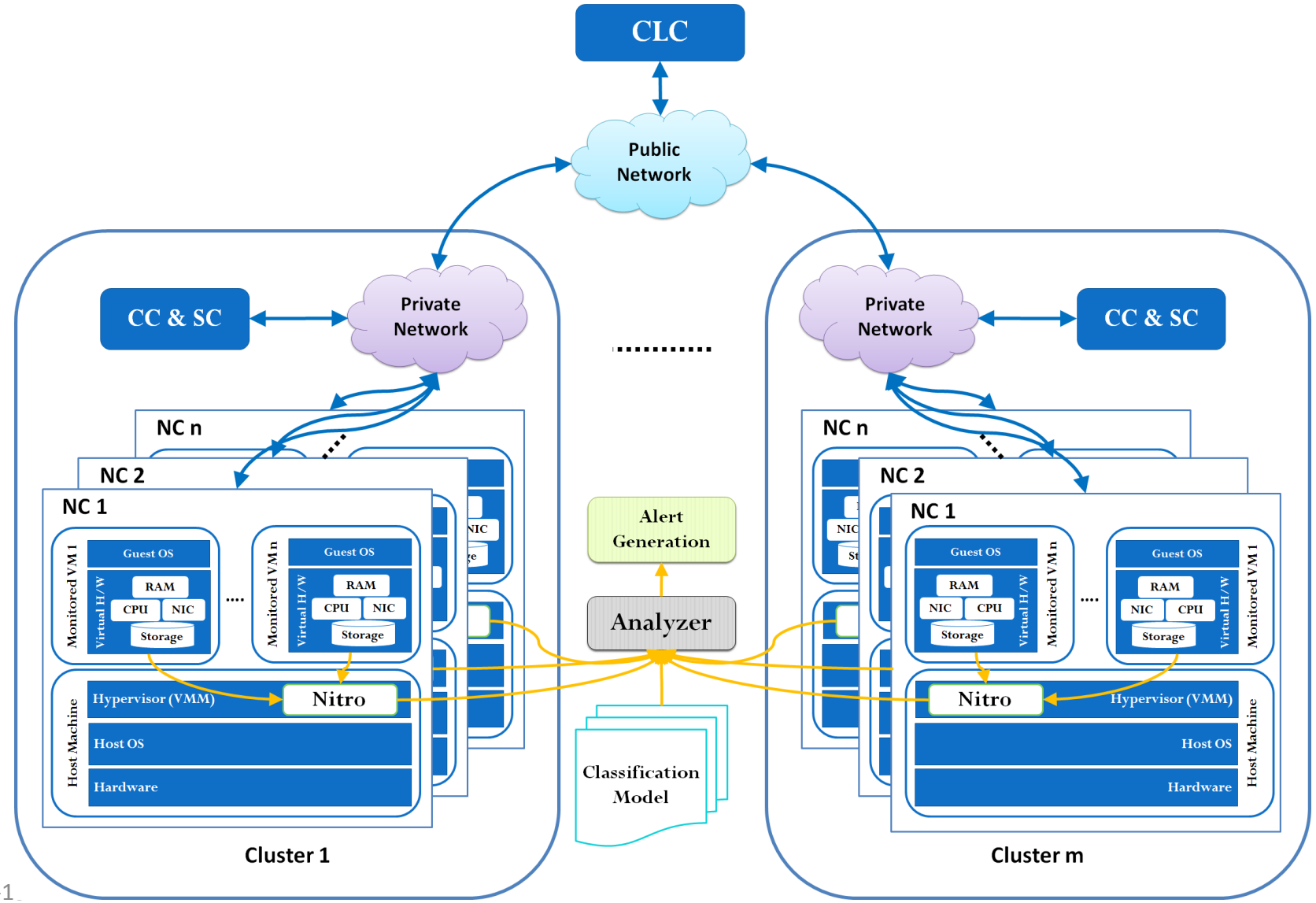
Results

No. of Hosts	No. of VMs per Host			
	1	2	3	4
Average Response Time (µs)				
1	171.4583	273.505	308.7123	497.5357
2	393.318	535.83	1097.573	1968.95
3	670.581	1506.907	2123.313	3142.323
4	1146.657	1966.56	3353.89	5329.327
Average Queue Length				
1	84.5989	113.6147	118.5947	106.9597
2	179.8713	157.0267	125.834	108.9777
3	211.7717	158.7543	127.797	114.9903
4	225.1947	159.186	131.5773	100.6157
Average Exit Queue Processing Time (µs)				
1	11.2167	11.74763	14.8883	16.74843
2	13.91587	15.19053	20.8002	25.50297
3	17.90413	19.78753	26.40057	34.10403
4	18.74457	24.9128	33.1067	37.85697

Standard Deviation

- Average Response Time: 2.42%
- Average Queue Length: 3.16%
- Average Exit Queue Processing Time: 4.30%

System Integration in Eucalyptus Cloud

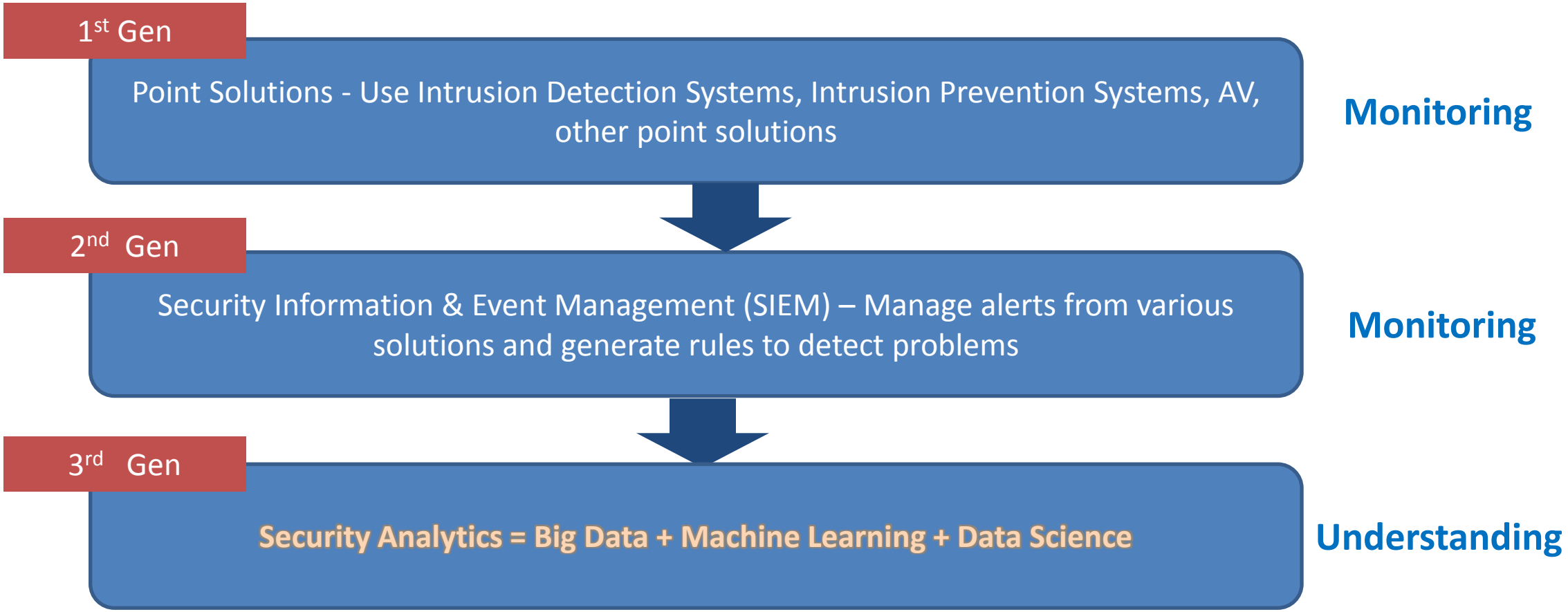


CLC – Cloud Controller
CC – Cluster Controller
SC – Storage Controller
NC – Node Controller

In-VM security - Conclusion

- VMI based security framework for cloud to detect in-VM malicious activity
- Represented system call dataset in modified vector space representation
  - Evaluated applicability of representation with Weka workbench
  - Deduced J48 algorithm as classification algorithm
- Evaluated live detection system with multiple VM(s) running on multiple Host(s)
- Integration of Nitro in Eucalyptus Cloud
- Work in progress: Automate the monitoring and Alert generation module

Looking into the future



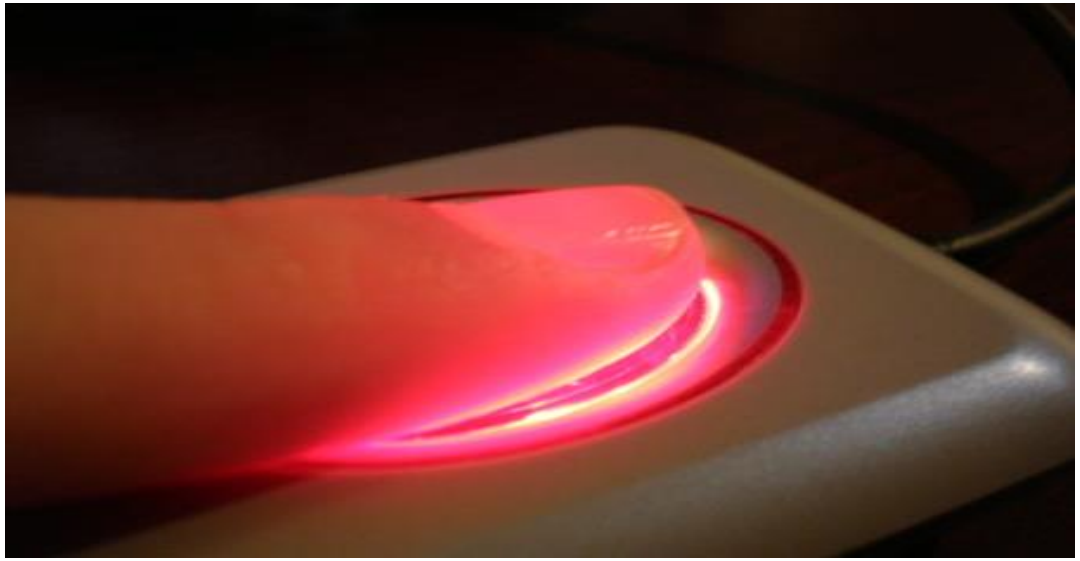
Open problems

- IoT

India UID Project

LBIMS

- Large Scale Identity Management System
- Large scale Biometric Identity Management System
- Large scale (~1.2B subjects, ~4 Trillion transactions/day)



India UID initiative

- Unique ID (UID)
- UID Project Name – Aadhaar <support>
- Unique Identification Authority of India (UIDAI)

- In India, inability to prove identity is one of the biggest barriers preventing the poor from accessing benefits and subsidies

Aadhaar Authentication Vision

To empower residents of India with a *unique identity and a* digital platform to authenticate anytime, anywhere

A digital online verification platform, to enable residents to prove their identity and for service providers to confirm that the residents are 'who they say they are'

Why?

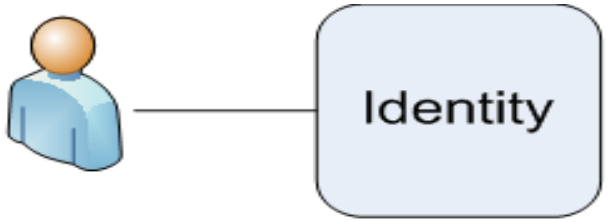
- Every time individuals try to access a benefit or service, they must undergo a full cycle of identity verification
- Different service providers have different requirements in the documents they demand, the forms that require filling out, and the information they collect on the individual.
- Such duplication of efforts due to '*identity silos*' increase overall cost of identity verification and cause inconvenience

UID – Core Objectives

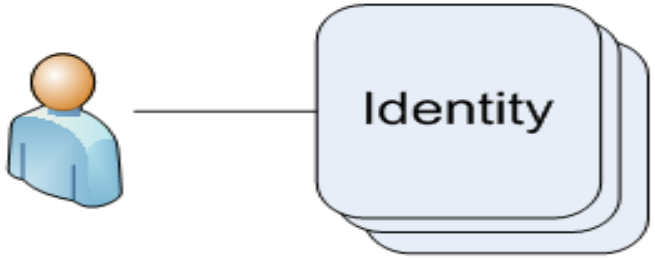
- The ID should be available to all residents of the country.
- The system should ensure that each resident gets only one ID, hence making it unique.
- The system should ensure that only the owner of the ID can use the ID to make a transaction.
- The system should be capable of electronically authenticating residents so that the government/private service delivery systems can ascertain identity of their customers.
- Authentication should be available online anytime, anywhere, so that the ID is recognized across the country over networks, thereby improving service delivery.

Avoid

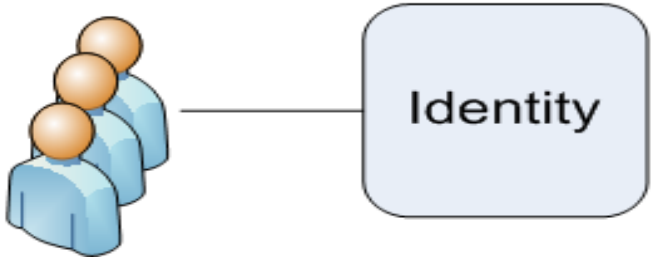
One Person – One Identity



One Person – Multiple Identities



Multiple Persons – One Identity



- **Fake Identities**: Identities created using fake documents of subjects that actually do not exist or identities of subjects who no longer exist.

Why Biometric?

- Identity systems that rely only on demographic fields (e.g. name, DOB, address) and personal reference checks are identity surrogates and vulnerable to forgery, falsification, theft, loss, and other corruption.
- Since biometric markers such as fingerprints, iris patterns etc. are unique to people, they can be used to ensure uniqueness.

Purpose

- Aadhaar system is built purely as an "*Identity Platform*" that other applications, Government and private, can take advantage of.
- identity infrastructure for delivery of various social welfare programs and for effective targeting of these services.
- Aadhaar system has grown in capability and more than 700 million Aadhaar numbers have been issued so far using the system.

Aadhaar enrolment

seeks the following demographic and biometric information:

1. Name
2. Date of birth (or Age)
3. Gender
4. Address
5. Mobile Number and Email (optional)
6. Ten fingerprints, two iris scans, and photograph
7. For children under five years old, Aadhaar number and name of the guardian (Father/Mother/Guardian)

Process to ensure no duplicates

- Registrars send the applicant's encrypted data packet to the UIDAI data centres for de-duplication.
- Aadhaar enrolment system performs a search on key demographic fields and on the biometrics for each new enrolment, to ensure uniqueness.
- 1:N search

Aadhaar Value proposition

- **For residents** – Aadhaar system provides a single source of identity verification across the country for its entire population
- **For Governments** - Eliminating duplication under various schemes is expected to save substantial money for the government exchequer.
- It also provides governments with accurate data on beneficiaries, enable direct benefit programs, and allow government departments to coordinate and optimize various schemes.

Aadhaar Value Praposition

- **For Service Agencies** – Uniqueness characteristic of Aadhaar number helps agencies such as banks, telecom companies, insurance companies, etc clean out duplicates from their databases, enabling significant efficiencies and cost savings.
- For agencies focused on cost, Aadhaar online authentication and e-KYC services greatly help lower KYC costs.

Insights

- When the system needs to scale to a billion people with diverse cultural, economic, and educational background, it is essential that the system be made simple from the perspective of data, processes, and its structure.

Privacy by Design

- The approach of storing intelligence in identification numbers was developed to make filing, manual search and book-keeping easier prior to the advent of computers.
- This is no longer necessary, since centralized database management systems can index the records for rapid search and access without having to section data by location or date of birth.
- Aadhaar number is a random number with no built-in intelligence or profiling information.
- A 12-digit number was chosen based on the identification needs of the population in the next couple of centuries
- Aadhaar authentication only responds with a 'Yes' or 'No' response and no resident data is sent back.

Privacy by Design

- **Minimal Data with No Linkage**
- In addition to having minimal data (4 attributes – name, address, gender, and date of birth - plus 2 optional data – mobile, email), this central database does not have any linkage to existing systems/applications that use Aadhaar

Privacy by Design

- **No Pooling of Data**
- It has no linkage information (such as PAN number, Driver's License Number, PDS card number, EPIC number, etc) to any other system.
- This design allows transaction data to reside in specific systems in a federated model.
- This approach allows resident information to stay in distributed fashion across many systems owned by different agencies.

Privacy by Design

- **Yes/No Answer for Authentication**
- it does not provide any scheme to ask questions such as "*what is the address of resident whose Aadhaar number is ...?*". Aadhaar authentication allows applications to "verify" the identity claim by the resident while servicing them while still protecting their data privacy.

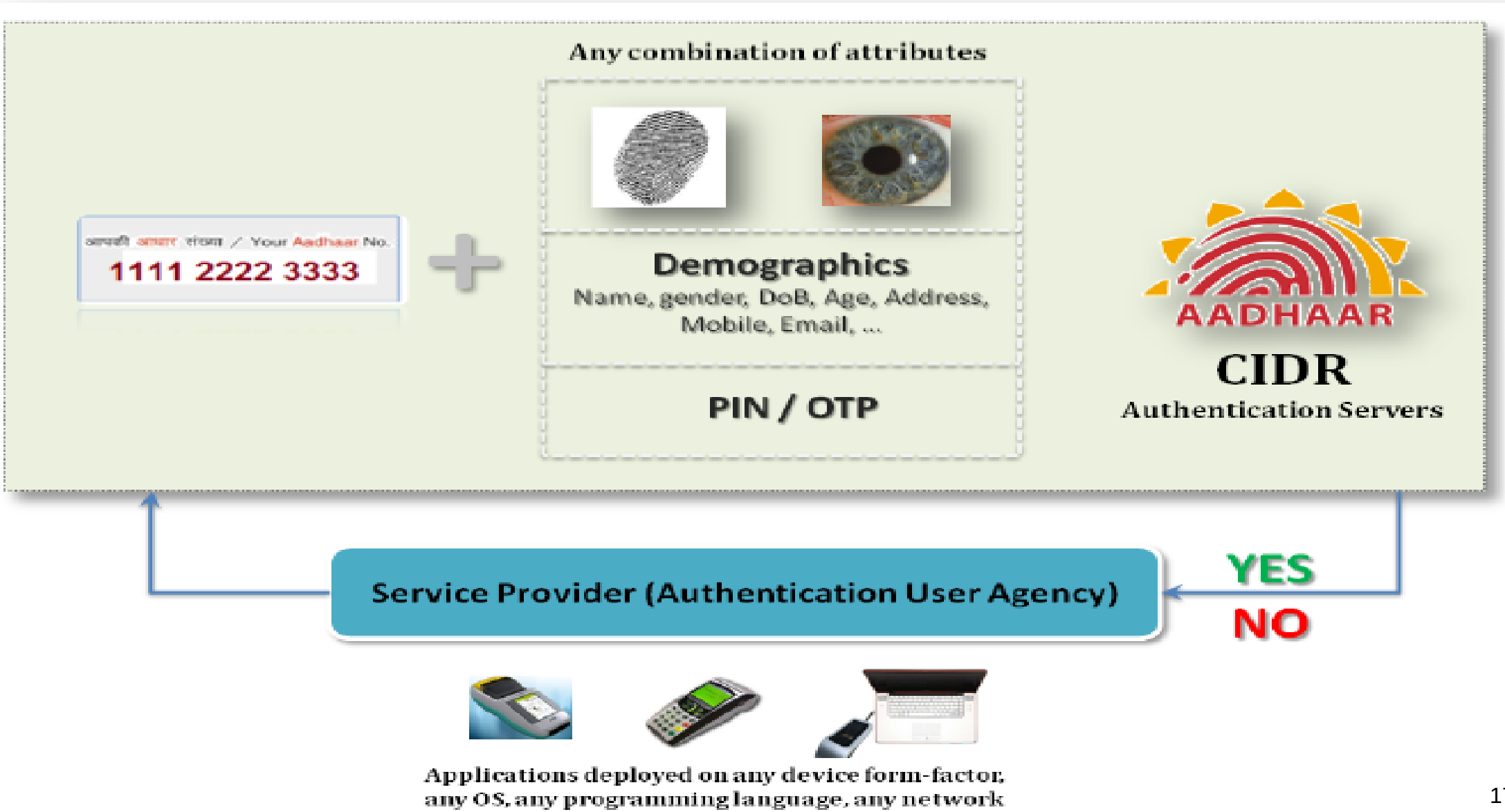
Privacy by Design

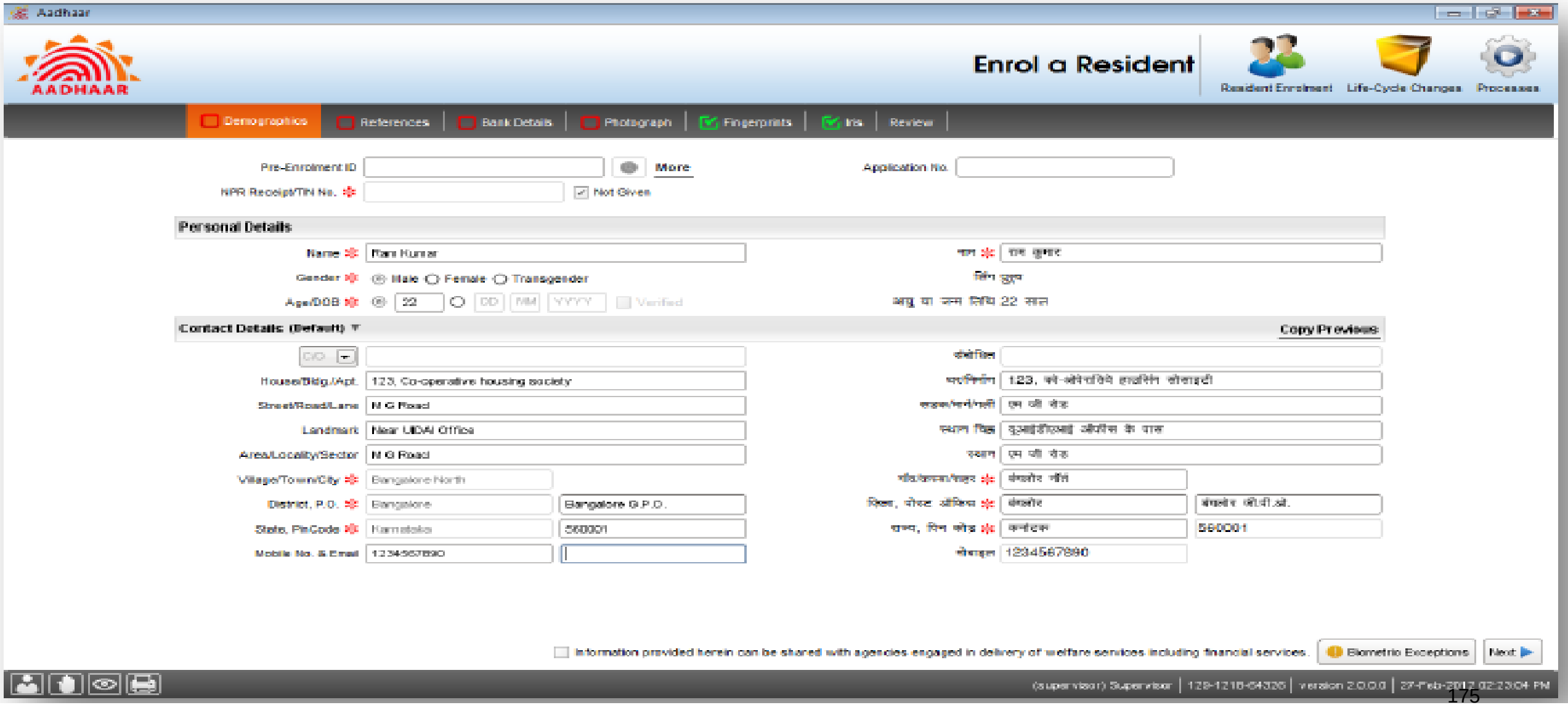
- **Explicit Resident Consented e-KYC**
- For every Aadhaar e-KYC request, only after successful resident authentication, demographic and photo data is shared in electronic format (via biometric/OTP authentication resident explicitly authorizes UIDAI to share electronic version of Aadhaar letter instead of sharing physical photocopies).

Privacy by Design

- **No Transaction History**
- does not have any knowledge of the transaction
- not designed to keep track of specific transaction details such as depositing money or obtaining pension or anything else

Aadhaar Authentication




Aadhaar
AADHAAR
Enrol a Resident
Resident Enrolment
Life-Cycle Changes
Processes
Demographics
References
Bank Details
Photograph
Fingerprints
Iris
Review
Pre-Enrolment ID
More
Application No.
NPR Receipt/TIN No.
Not Given
Personal Details
Name
Ram Kumar
Gender
Male
Female
Transgender
Age/DOB
22
DD
MM
YYYY
Verified
Contact Details (Default)
Copy Previous
C/O
House/Bldg./Apt.
123, Co-operative housing society
Street/Road/Lane
N G Road
Landmark
Near UIDAI Office
Area/Locality/Sector
N G Road
Village/Town/City
Bangalore North
District, P.O.
Bangalore
Bangalore G.P.O.
State, PinCode
Karnataka
560001
Mobile No. & Email
1234567890
Information provided herein can be shared with agencies engaged in delivery of welfare services including financial services.
Biometric Exceptions
Next
(supervisor) Supervisor
Version 2.0.0.0


AADHAAR
Enrol a Resident
Resident Enrolment
Life-Cycle Changes
Processes
Demographics
Photograph
Review
Score
Score

Aadhaar technology backbone

Design for scale –

- Aadhaar system is expected issue more than 1.2 billion identities and will continue to grow as the resident population expands.
- Since every new enrolment requires biometric de-duplication across the entire system, every component needs to scale to very large volumes.
- System must handle hundreds of millions of transactions across billions of records doing as many biometric matches every day!!!!!!
- Network and data centre load balancing and multi-location distributed architecture for horizontal scale are critical to such massive scalability

Mobility and Ease

- Any Place
- Any Network
- Any Provider
- Any Device

Authentication

- Supports answering the question “is a person s/he claims to be”
- Verifies resident information (demographics and/or biometrics) for a given Aadhaar number
- Online identification verification service that is lightweight, ubiquitous, and secure
- Only a “yes or no” is returned as part of the response

Authentication

Supports multi-factor authentication using

- biometrics (fingerprint, Iris)
- One time pin (OTP)
- and combinations thereof

Supports all types of networks, protocols and devices

- GPRS, Edge, 3G, Wi-fi, LAN, WAN, Broadband etc
- Personal computer, mobile, PoS terminals, etc.
- Works with assisted and self-service applications

Secure

- Data encrypted at source
- Data tamper proof
- Network security and encryption
- Security connectivity from device to UIDAI data centre
- Data audited

Scalable

- Authentication data is about 500bytes -2.5Kb
- Devices cost comparable to hand held devices
- Under 1 sec in CIDR and 4-5 secs round trip
- Can handle 100+ million authentication a day
- Low cost, universal, easily deployable

Service Usage Illustrations

Type 1 – Demographic Only – Single Factor

- AUA beneficiary database cleanup
- Periodic KYC/beneficiary verification
- Address, Date of Birth verification

Type 2 – OTP Only – Single Factor

- Authentication for internet- and mobile- based transactions
- Cases where deployment of biometric technology is difficult or not practical

Service Usage Illustrations

Type 3 – Biometrics Only – Single Factor

- Authenticating residents at point of delivery
- Periodic verification of pensioners' database
- Attendance management
- Adding new beneficiary / customer
- Financial transactions

Service Usage Illustrations

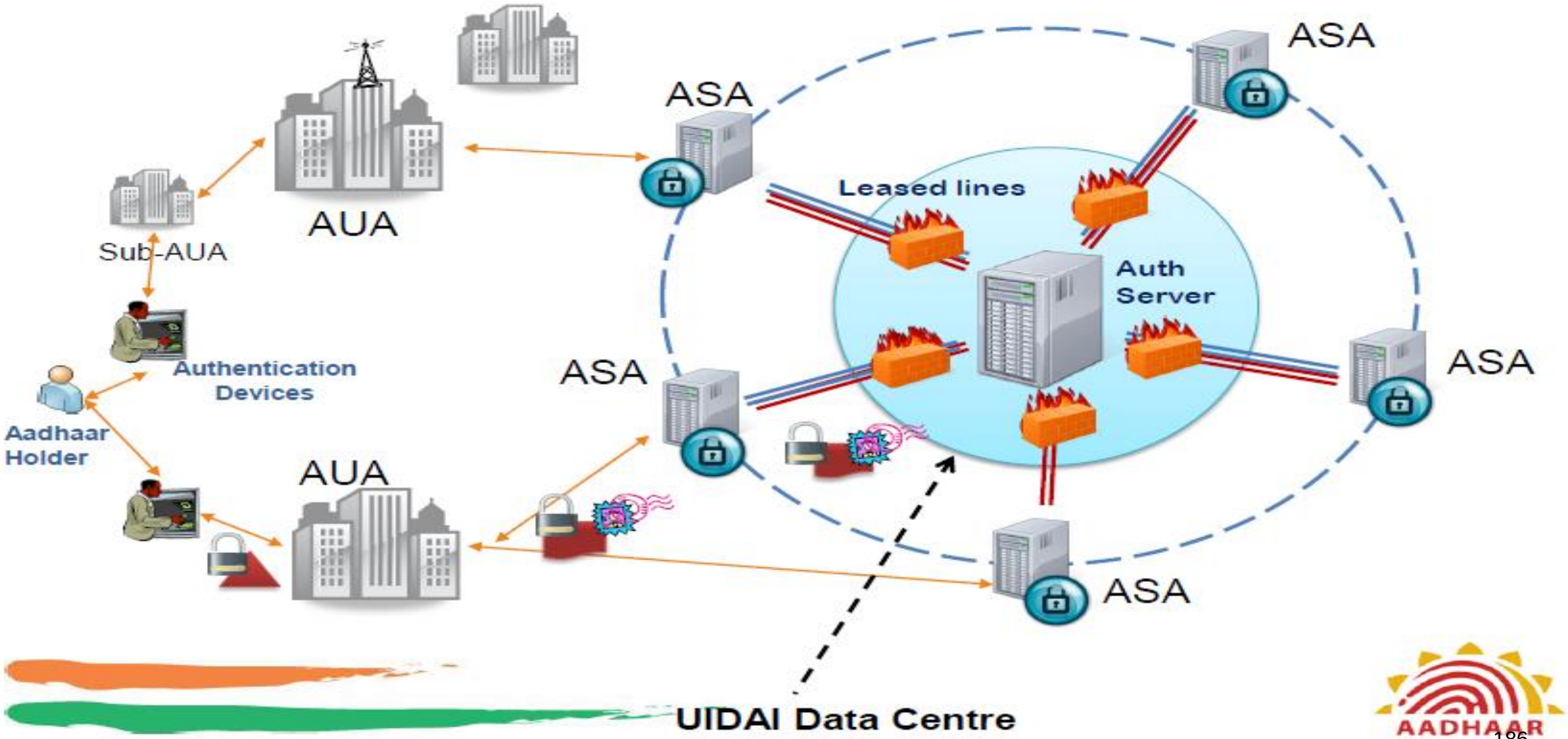
Type 4 – Biometric (Fingerprint/Iris) & OTP – Two Factors

- Where higher assurance levels may be required such as:
- High Value Financial transactions
- Accountability tracking (example – authenticating officials in charge for inspection in service delivery programs such as PDS & NREGA
- Access to restricted/high security areas

Type 5 – Fingerprint + Iris + OTP – Three Factors

- Access to very high security areas such as army base, nuclear plants etc

Authentication Ecosystem (Overview)



Summary of Authentication User Agencies

Sector	Live/on-boarded	In process	Total
Banking and Financial Services	56	33	89
Central Govt. Departments	6	2	8
State Govt. Departments	12	7	19
Credit Bureaus	1	2	3
Insurance Sector	5	7	12
Telecom Industry	5	3	8
Information Technology	4	13	17
Private sector (new applications)		23	23
Total	89	90	179

Aadhaar Authentication Enabled Applications

- **Public distribution system**
- **MGNREGA & Social Security Pensions**
- Mahatma Gandhi National Rural Employment Guarantee Act
- **Attendance Tracking**
- **Social Welfare Schemes (*Scholarships, Slum Rehabilitation etc)***
- **Property Registration**
- **AEPS for financial transactions**
- Aadhaar Enabled Payment Systems – 40+ Banks
- **Credit Bureaus for De-duplicaton & KYC**
- **Insurance Sector for establishing identity & KYC**
- **Telecom Industry for establishing identity & KYC**
- **Certificate of Liveliness – 5 Million pensioners (retired old people) of India**

Passenger Check in Using Authentication

Systems proposed in each compartment

Passenger Inputs:
1.Seat No
2.Finger Print

N

Verification by TTE

- Authentication by UIDAI in first stage.
- TTE checks only passengers not authenticated

Y

Check in Output
1.Last 4 digit of UID
2. Tick /OK

Instant Money Transfer

A

Mobile wallet

A

Deposit Money

Aadhaar	Amount (Rs)
9856 2543 6845	5000

A

Transfer Money

B

Withdraw Money

Acknowledgement SMS

sends SMS, DateofBirth*Full Name *, 9971888888

- **Thank You for your Time and Attention**