Data Center Security
Literature Review

Ziliang Zhang, 2020, UCR EE252

1. Introduction
2. Taxonomy
3. Definition
4. Method
5. Evaluation
6. Discussion

Introduction - Background (Lecture 8)

- Multi-tenant Data Center Vulnerability
  - Timing of attacks - surge of power
  - Side channels - acoustic, voltage
  - Noise - fan, server, thermal
- Attacks
  - Surge vlotage in one server causing massive meltdown (ohm’s law)
  - Power attacks: PFC (Power Factor Correction) induced spikes
- Defense
  - Side channel defsence - mesure power without the power meter - but potentially caused physical security

Introduction - other aspects

- Lecture covers attacks from overloading server power, this research focus on other two types (physical, hacking) as well
- More discussion includes both technical perspective (2/3 of entire list), and social perspective* (1/3 of entire list)

- reason to include social point of view: necessary means to provide protection on a higher level; broader discussion happened in domain of personal information; debate over governmental intervention

Taxonomy

Definition	Technical		[3], [5], **[14]**, [15], [18], [19], [24], **[29]**
	Legislative		[7], **[14],** [17], [22], [27], **[29]**
Method	Technical	Architecture	[1], [4], [6], [16], [25]
		Algorithm	[2], [9], [10], [13], [20], [26]
	Legislative	Social Act	[11], [31]
		Enacted Law	[28], [30]
Evaluation			[8], [12], [21], [23]

Older paper like 14 and 29 tends to discuss both technical and legislative

			2014 and prior	2015	2016	2017	2018	2019	2020
Definition	Technical		[3](2011), [5](2010), [14](1967), [29](1968)	[15]		[24]	[19]		[18]
	Legislative		[7](2011), [14](1967), [29](1968)	[22]				[17]	[27]
Method	Technical	Architecture	[1](2008), [16](2014)		[4], [6]	[25]			
		Algorithm	[2](2014)	[10]		[9], [20], [26]	[13]		
	Legislative	Social Act	[11](2009)	[31]					
		Enacted Law	[28](2014), [30](1965)						
Evaluation	Technical					[8], [23]	[21]		
	Legislative		[12](2011)						

12 paper from 2014 and prior (7 from last 10 years)

2015: 4, 2016: 2, 2017: 7, 2018: 3, 2019: 1, 2020: 2

31 paper in total

Definition of Problem

[3], [5] “Cloud Computing Security Research”

Data Center at the foundation of all 4 layers

Issue in every step:

Data Transmission, Virtual Machine Security,

Network Security, Data Security,

Data Privacy, Data Integrity, Data Location,

Data Availability, Data Segregation,

Security Policy and Compliance, Patch management.

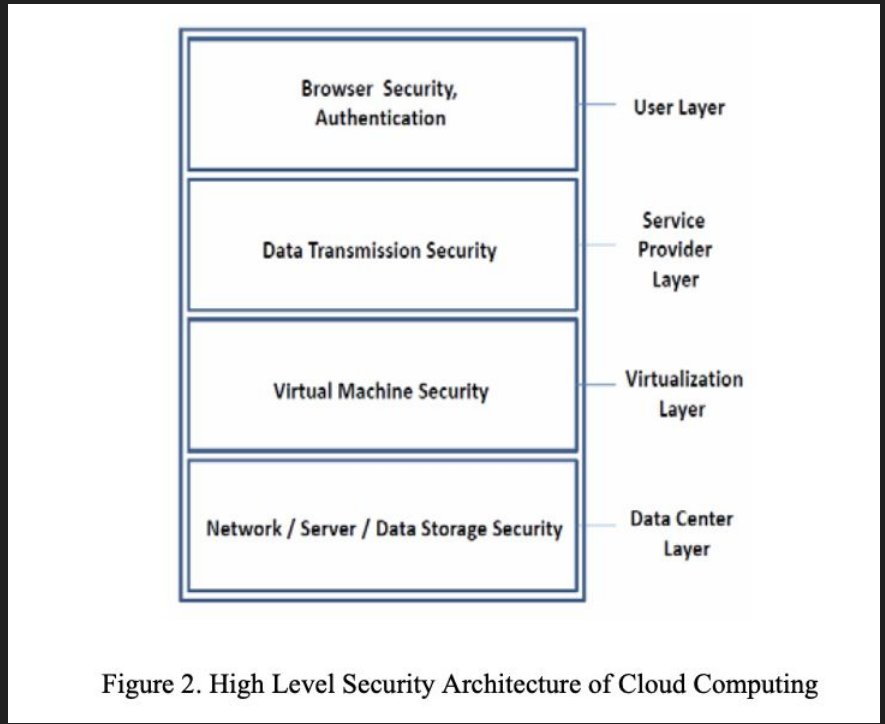


Figure 2. High Level Security Architecture of Cloud Computing

Definition of Problem

Future path for research:

Service Level Agreements (SLA's), Cloud Data Management & Security,

Data Encryption, Migration of virtual Machines, Interoperability,

Access Controls, Energy Management, Multitenancy,

Server Consolidation, Reliability & Availability of Service,

Common Cloud Standards, Platform Management

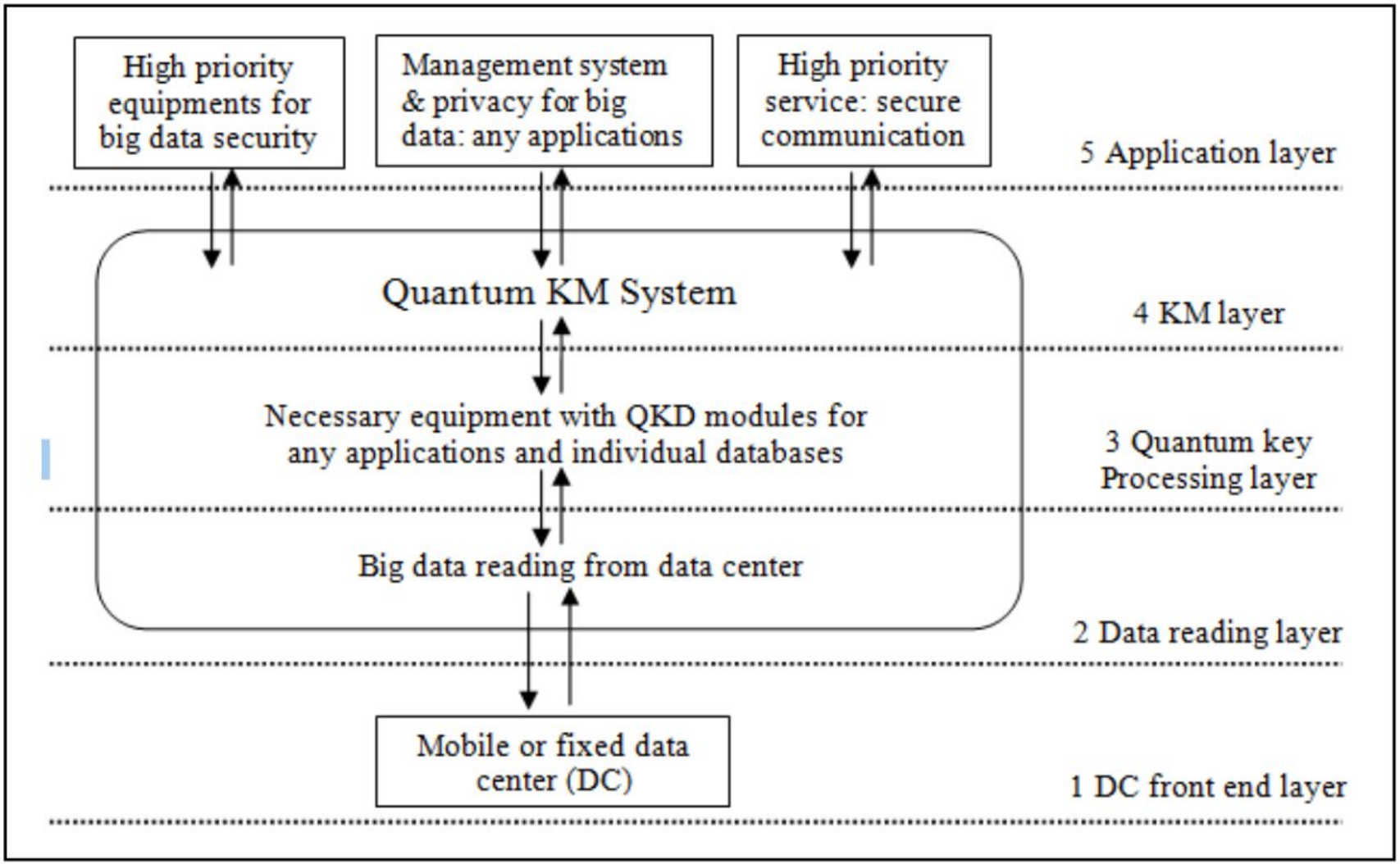
Definition of Problem

[15] “Mobile Data Center Autentication Security Issue”

“security protocols and other privacy issues based on authentication protocols use only bitwise operations but these operations are not suitable for big data” [15]

“In this research, quantum bits (qbits) operations seem that mobile data centers get big data security and privacy very quickly and efficiently” [15]

“When multiple authentication and re-authentications are used in the data center, passive attacks will be increasing”


High priority equipments for big data security
Management system & privacy for big data: any applications
High priority service: secure communication
5 Application layer
Quantum KM System
4 KM layer
Necessary equipment with QKD modules for any applications and individual databases
3 Quantum key Processing layer
Big data reading from data center
2 Data reading layer
Mobile or fixed data center (DC)
1 DC front end layer

Method - Architecture

[16] “Privacy Preserving Hybrid Storage in Cloud Data Center”

HVSTO, distributed structure to preserve privacy even parts of storage units are compromised

Hybrid Storage: a local solid-state disk equipped with every node of virtualization cluster and the distributed storage.

Efficiency of Mapping: instead of “Chain mapping”, use of a direct index metadata for mapping a virtual block to a physical block, satisfy fast retrieval between communication of distributed storage

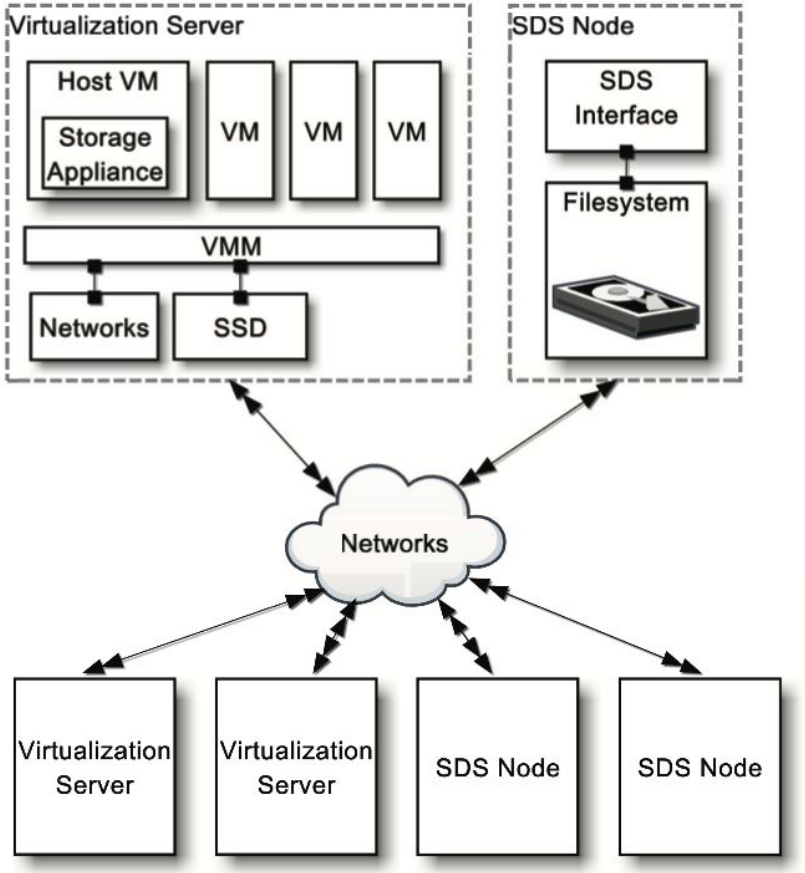


Fig. 2. Hivo consist of the storage appliance in virtualization servers and the shared distributed storage(SDS)

Method - Algorithm

[9] “Intra-Day Security Check”

1)Create page cache entity files according to maximum parallel access and index one as the active proxy service, others as standby proxy service. All exchange proxy services exist in permanent processes and the page cache entity file is the carrier of the exchange proxy service.

2)National, branch and provincial dispatching centers separately perform data preparation, gathering local plan data, including load forecasting, power generation plan, tie-line plan, maintenance plan and section limit data, communicate with local exchange proxy service and push the data.

3)After the proxy service in national, branch and provincial dispatching centers receives the data, the received data is indexed and stored in the cache entity file

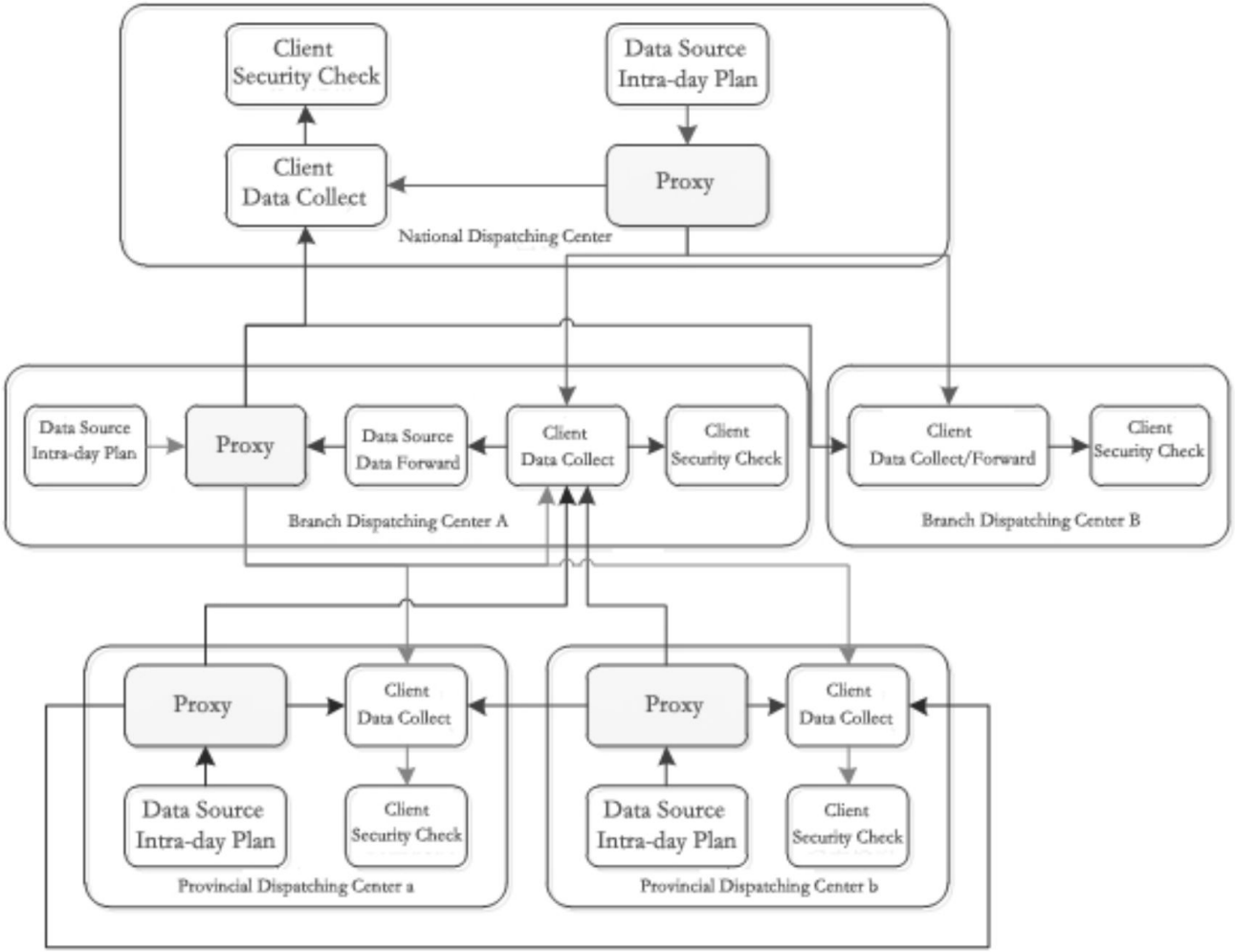


Figure 2 Multi-Dispatching Center Security Check Data Sharing Process Based on Proxy Service

Evaluation

[12], “Risk-neutral evaluation of information security investment on data centers”

simulation of attack on:

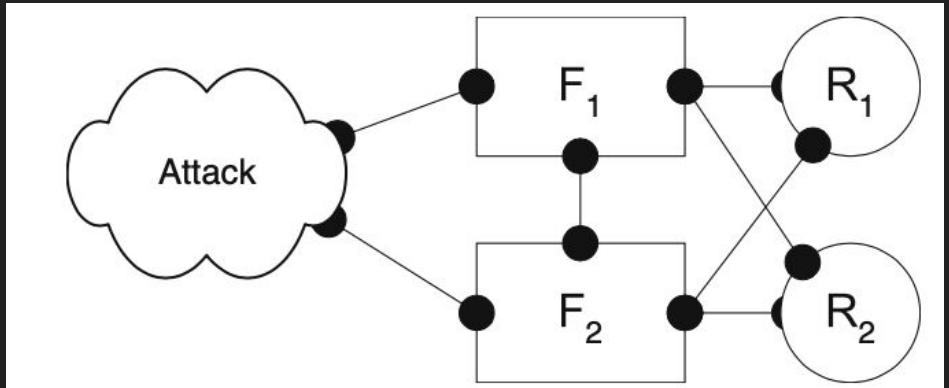
one-tier network, Two-tier Multi-Homed network, Single filter (1F), Multiple serial filter (mSF), Multiple parallel filter (mPF), Interface filter (mIF)

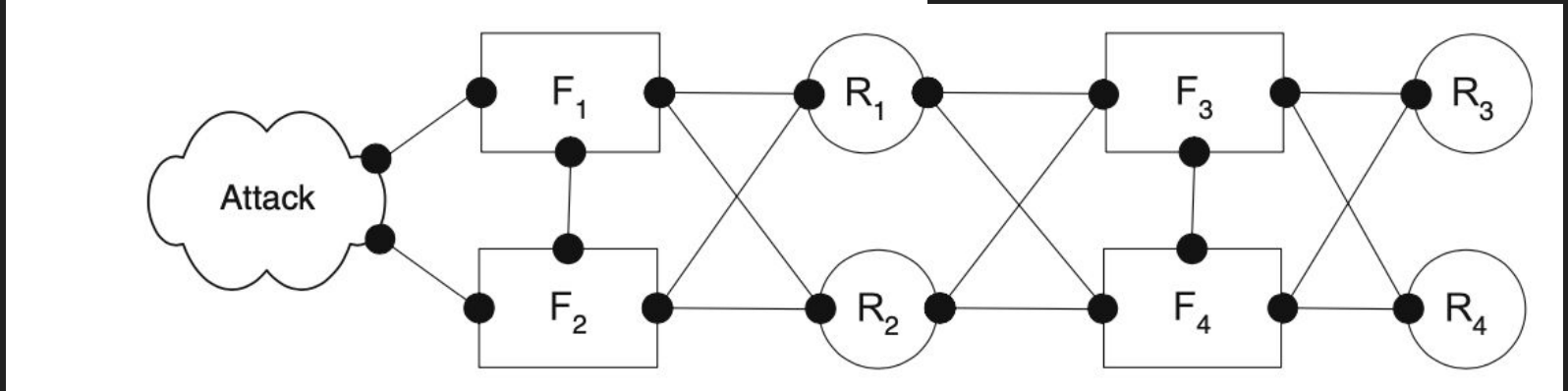
calculate the accumulative probability of insecurity:

Algorithm API, Algorithm OSI

Example of one-tier and two-tier attack model

F: filer, R: resource





Discussion

Trends Identification:

Technical

1) More specific security system/algorithm in data center

2) Virtualization of Storage, Distributed Storage are the prevalent in improving security in data centers

Legislative

1) Governmental Interference vs. Individual Solution

2) Specific areas of information should not be generalized when making new laws - medical data

Discussion

Current Progress

100% Complete the Introduction, taxonomy and Definition; writing of the last tree sections is on-going but finished the review of all paper

Future Plan

12/10 - Complete the last 3 sections of writting

12/11 - All Deliverables including Appendixes and Paper folder will be submitted to ilearn

Q&A