Security Issues in Cloud / Edge / Fog Computing

Alessandro Carrega

TNT Lab – DITEN
University of Genoa

Information 1/2

- Lecturer: **Dr. Alessandro Carrega**.
  - *Email*: alessandro.carrega@unige.it.
  - *Skype*: alessandro.carrega@gmail.com.
  - *Telegram / Whatsapp*: **3487485497**.
- Duration: **20 hours**.
- Language: **English**.
- Lesson in site and remote (Teams).

Information 2/2

- Dedicated Teams channel:
  - **PhD STIET Cyber security approaches for Cloud/Edge Environments**

    https://teams.microsoft.com/l/team/19%3a-Dtnw_NHUAl1AjZZV4HixlifmU8gywbskeeQwSV--uk1%40thread.tacv2/conversations?groupId=bdafff5c-0ab9-44b2-aef2-5a14e1dd6e15&tenantId=6cd36f83-1a02-442d-972f-2670cb5e9b1a
- GitHub repository:
  - https://github.com/tnt-lab-unige-cnit/phd-stiet-cyber-security-approaches-cloud-edge-environments
- Optional homework.
  - Available in Teams and GitHub.
- Final Exam with 3 options:
  - **Theoretical**: *short survey with 3 papers*.
  - **Pratical**: *2 exercises*.
  - **Quiz**: *100 multiple choice questions (**60%** to pass the exam)*.

Key Features

Key Features	Cloud	Fog	Edge
Compute, storage, and networking capabilities	✓	✓	✓
Virtualization and Multitenancy	✓	✓	✓
Elastic compute/ Resource pooling	✓	✓	✓
Large scale and long-term processing, storage, and networking	✓	-	-
Centralized operations	✓	-	-
Fast response time, low latency, and location awareness	-	✓	✓
Mobility support	✓	✓	✓
Short-term, small-scale processing, storage	✓	✓	✓
Decentralized infrastructure	-	✓	✓
Dense geographic distribution	-	✓	✓
Data Service at the edge	-	✓	✓
Real-time interactions and proximity to end-users	-	✓	✓

Cloud Security

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[22]	2019	Cloud component threats, attacks & vulnerabilities	120	2010–2017	Systematic identification and classification of threats to cloud security from the side of the Cloud Service Provider, CSP category	1)Systemic identification and classification of non-malicious threats. 2)Further exploration of threats under the CSC category, as well as other cloud stakeholder categories
[23]	2019	virtualization-related issues	132	2010–2018	Vulnerabilities, threats, and attacks in virtualization components of cloud systems	1)Improvements in secure virtualization mechanisms for cloud and related computing technologies, such as fog and edge

Cloud Security

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[25]	2018	Security issues at different levels of cloud architecture	23	2009–2018	Cloud security issues at different levels of cloud virtualization: communication, computational and SLA levels of the cloud.	1) Application, network and host level security mitigations
[27]	2017	Threats to cloud adoption along with current solutions	34	2009–2015	Cloud attack vectors, attack solutions with industry examples. Also provides analysis of main threats to cloud adoption	1)The use of containers as a more secure option, though they could introduce new security issues. 2) Mechanisms to protect users from attacks by infrastructure owners. 3) Hardware based attestation and homomorphic methods.

Cloud Security

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[2]	2017	Security issues in cloud components	6	2012–2015	Risks and solutions for mitigation of vulnerabilities in the cloud components. Security is framed as a combined responsibility of all the associated actors.	1)Security models for systems development life cycle (SDLC) for cloud consumers. 2)Challenges, requirements and impacts of effective security awareness and training on the side of the CSC
[28]	2015	Public and private cloud issues focusing on data issues	15	2010–2013	Access and Data utilization management where access control and encryption are highlighted as important elements of data security	1) Trust mechanisms, authentication, and verifications of the point of multi sourced data origin- as mechanisms for improved data security

Cloud Security

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[29]	2015	Cloud novel and architectural issues	126	2011–2014	Multilevel discussion on cloud security issues (communication, architectural and SLA levels).	1)Privacy preservation and SLA security solutions
[30]	2016	Challenges in public and private clouds	146	2009–2014	Communication, architectural and compliance issues. Also, vulnerabilities in mobile cloud computing	1)Proposal for a three-tier security solution architecture, 2) Research into elements such as vendor-lock in multi-Cloud, and emerging cloud-related technologies and applications (such as fog, edge, SDN, NFV)
[31]	2014	Vulnerabilities, threats and attacks in cloud and industry perspectives	227	2009–2012	Threats and challenges from both academic and industry perspective with real-life examples incidents.	1)Malware camouflage. 2) Cloud auditability and accountability 3) Privacy preservation. 4) Trust-based security models. 5) BYOD management

Cloud Security

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[32]	2014	Privacy preservation issues in e-Health	98	2010–2013	Approaches for preservation of the privacy of patient health data.	1)Improvements in available encryption and policy-based approaches such as PKE and secure provenance techniques.
[33]	2014	Secure remote storage and computation for data security.	91	2009–2012	Virtualization, authentication, integrity, availability, accountability, and privacy of remote storage/computation	1)Task configuration automation for use with cloud providers. 2) Techniques for CSP accountability. 3) Public verifiability
[34]	2013	Analyses of cloud attacks and Intrusion detection systems	16	2009–2013	Discussion on various cloud attacks to confidentiality, integrity and availability; and recommended intrusion detection/ prevention systems in the cloud scenario	1)Improvements in Host based IDS, Network based IDS, and Distributed IDS

Cloud Security

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[35]	2013	Cloud Vulnerabilities Threats, and Attacks at different layers	49	2009–2012	Presented security issues that hinder cloud adoption and their enabling technologies	1)Multi-level data security models. 2)Reputation and content-based trust 3) Privacy preservation. 4) Cryptographic key management 5) Cloud governance
[36]	2013	Cloud security issues due to cloud its business model: SLA, Trust and Data	15	2009–2012	Present conventional and new challenges due to the cloud's business model that largely encourages non-transparency to end users, specifically of public cloud	1)SLA amendment models. 2) Accountability. 3) Cloud service model re-engineering. 4)End-user centric mechanisms for data integrity

Cloud Security

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[37]	2013	Basic concepts of security, privacy, authentication and trust management	70	2009–2012	Foundational survey on fundamental security, trust and privacy concerns, discussing the complex relationship between the three elements. A brief discussion on suggested solutions.	(1) Tans-border data flow restriction issues such as liabilities, difficulty knowing geographic location of data, migration, data remanence, auditing, accountability and availability, as relates to this issue. (2) Security as a service
[38]	2013	Security issues on the basis of cloud main security requirements.	54	2009–2012	Generic attribute-driven methodology representative of cloud security, privacy and trust based on confidentiality, integrity, availability, accountability, and privacy-preservability.	1)The relationship between extreme privacy and accountability

Cloud Security

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[14]	2013	Threats, Attacks and Vulner-abilities in cloud service models	64	2009–2012	Cloud-related threats, vulnerabilities, and coun-termeasures, service level security views from end users' perspective	1) Reengineering of solutions to virtualization and data security issues to match the cloud's complexity.
[39]	2013	Hypervisor security and vulnerabilities	19	2009–2011	Characterization of different dimensions of hypervisor vulnerabilities to understand potential attack paths and where the defenses should be focused.	1)Hypervisor security mechanisms.
[40]	2012	Security issues due to cloud characteristics	4	2009–2011	Survey on cloud service models, cloud deploy-ment models and related security requirements. Issues related with cloud storage further discussed.	(1) Virtualization (2) End to end security (3) Cloud-application security (4) Information assurance (5) Trust models

Cloud Security

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[42]	2011	Security issues in cloud IaaS	68	2009–2011	Foundational discussion on cloud security issues; from the networking, virtualization, and physical sides of cloud IaaS networks.	(1) Security of VM images, isolation, secure networking in virtual networks (2) Trust and auditability
[43]	2011	Cloud computing security models and strategies	1	2009–2011	Security models such as multiple-tenancy model, risk accumulation model, cube model; along with associated risks due to stakeholders in a cloud network	1) Security risks due to privileged and malicious CSPs, SLA amendment, models for multi-cloud security, reputations and trust management, proactive alarm systems for malicious activity.
[44]	2011	Security issues due to cloud infrastructure and components	1	2009–2011	Issues and existing security approaches to secure infrastructure and applications.	(1) Multilevel solutions (2) Availability and performance mechanisms (3) Service disruption defenses (4) Self-defending VM

Cloud Security

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[45]	2011	Cloud-specific vulnerabilities and risks	2	2009–2011	Foundational review of general security issues and cloud-specific issues from various perspectives. Emphasis on vulnerabilities and risks factors in cloud computing.	1) Security controls in a cloud setting
[46]	2011	Security issues related to SaaS, PaaS and IaaS	41	2009–2010	Summarized cloud security issues based on service delivery models (i.e., IaaS, PaaS, SaaS); and mainly focus on SaaS.	1) More research exploration in PaaS and IaaS.

Cloud Security

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[47]	2010	CSP-related security concerns	3	2008–2010	CSA-related security requirements. Issues such as data ownership, legal problems, privacy and multi-location data storage also highlighted	1) Multi-location data issues, cloud application security, infrastructure Security, improved strategies for availability, accountability, auditability and trust management.
[48]	2010	Trust in the cloud environment.	13	2008–2010	Issues in cloud computing that exacerbate trust such as outsourcing, resource sharing access management and reliance on third parties.	1) Data-centric security mechanisms, management of semantic heterogeneity trust management frameworks and secure provisioning.

Cloud Security

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[24]	2019	Security requirements, threats, vulnerabilities	312	2010–2019	Unified taxonomy for security requirements, threats and vulnerabilities in cloud	1)Trust based security models. 2)How does cloud security impact emerging cloud-enabled applications such as IoT, SDN, and NFV?
[26]	2017	All general aspects of cloud security	174	2010–2015	Cloud underlying technologies, security issues, threats, attacks and suggested solutions	A unified or holistic security solution that meets most security goals of the cloud
[41]	2012	Data and Communication security issues	29	2009–2010	Data, communication, trust, multi-tenancy, account control and insider threats issues	(1) Improvements in cryptographic methods in terms of computational overheads (2) Trusted third party (3) Authentication mechanisms.

Cloud Security

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[6]	2012	Threats due to multitenancy in PaaS	56	2009–2010	Security of Platform as a Service (PaaS) with a focus multitenancy-related risk	1) Enforcement of security policies on external untrusted code in development environments, safe thread termination, fault administration and installation isolation and resource accounting

Fog/Edge Security 1/5

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[49]	2018	Trust, architectural and related trust issues.	93	2013–2017	Offer detailed discussion on trust. Key fog issues include authentication, access control, malicious attacks, privacy and secure communications	Service availability, secure shared technology, trust management models, malicious fog nodes, strong identity verification mechanisms, secure fog node orchestration
[50]	2018	Fog and edge environment threats	125	2013–2016	Security challenges in edge paradigms, along with available solutions in literature. Recommend synergistic approach to new solution engineering.	Identity and authentication management, access control security in edge environments, protocol and network security, trust management, intrusion detection and forensics in fog computing

Fog/Edge Security 2/5

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[51]	2017	Authentication and trust in the Fog layer	61	2014–2017	Foundational survey on main security and privacy issues along with recommended solutions in fog environments such as trust, malicious attacks, secure communication and end user privacy	Authentication-as-a service, mobility, trust mechanism reengineering such as certificates and Public-Key Infrastructure (PKI) modifications.
[52]	2017	Survey of fog application security issues	144	2014–2017	Foundational survey focusing on security of fog apps. Virtualization, web security, communication, data security, wireless security and malware issues are main issues discussed.	Privacy preservation, malicious insider detection and mitigations, authentication, and the use of advanced encryption standards with improved resource consumption

Fog/Edge Security 3/5

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[5]	2017	Privacy preservation in fog-based vehicular networks	149	2011–2016	Survey on assurance, privacy preservation, and incentive-driven fog-based vehicular crowd sensing; issues discussed include parking navigation, road surface monitoring and traffic collision reconstruction.	Secure mechanisms for incentive-driven crowd sensing, secure tasking and crowd sensing reporting, privacy-preserving navigation, data security and privacy in fog nodes, trust mechanisms
[53]	2017	Security and privacy issues in IoT environments	14	2013–2015	Main issues to fog and edge security are network security, data security, access control and privacy. Emphasis is on data and location privacy.	Privacy preservation, specifically location and data privacy techniques.

Fog/Edge Security 4/5

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[54]	2015	Fog system access and identity management	39	2013–2014	Foundational paper focused on a few security elements in fog computing such access issues and attacks such as the man-in-the-middle attack. A 'typical' man-in-the-middle attack scenario is demonstrated	Computation and storage security mechanisms, smart grid security, SDN security in vehicular networks Mitigation of the Man-in-the-middle attacks in fog and edge environments.
[55]	2015	General foundational survey in fog security and privacy	48	2013–2014	Foundational survey for understanding fog security. Wireless and network security issues, trust and authentication highlighted as main concerns in fog.	Reputation-based trust model, modification of traditional authentication techniques in light of power limitations of fog, rogue fog nodes.
[56]	2015	General survey of fog applications and Issues	55	2014–2014	Enlightens secure design attributes of fog systems, and issues due to fog system design.	Secure design recommendations for fog systems and applications

Fog/Edge Security 5/5

R1	Y1	F1	P1	S1	Key Contribution	Suggested Research Directions
[57]	2015	General review of security issues and solutions in fog and edge systems	6	2013–2014	Examines and analyzes available IoT security issues such as those of fog nodes and IoT nodes and Man-in-the-middle attacks.	Efficient collection and analysis of logs in IoT environments for situational security situations
[58]	2015	Fog forensics	23	2013–2014	Review of fog forensic issues in cloud and fog environments; laying foundation for understanding forensics in this paradigm.	Cross border data and regulatory issues, and Man in the Middle attacks in fog and edge environments,
[21]	2014	Authentication and Encryption	31	2013–2014	Foundational paper on fog issues. Lay solid foundation for the understanding of security and privacy issues and solutions in fog computing.	Public key infrastructure (PKI) based solutions for authentication, multicast authentication, Diffie-Hellman key exchange, and other encryption schemes.

Solutions

Area	Summary of Recommended Solutions
Attacks and Intrusions	Strong authentication and authorization mechanisms, intrusion prevention/detection systems, proper configuration of SSL, strong VM isolation, use of secure hypervisors techniques such as monitoring hypervisor activities, use of secure web (https), encryption, anti-malware programs, rigorous data backups vulnerability patching, system restore points
Software	Malware solutions, lightweight intrusion detection systems, multitenant software platform security, Secure code, vulnerability patching, regular platform software updates, API security.

Solutions

Area	Summary of Recommended Solutions
Internet and the Web	Periodic auditing, firewall, anti-virus protection, intrusion prevention systems, encrypted communication, mutual/multi-factor authentication
Network and Wireless	Intrusion detection systems, firewall, authentication and encrypted communications, key management, secure routing, private network wireless security protocols, multi-factor authentication, isolating compromised nodes

Solutions

Area	Summary of Recommended Solutions
Virtualization	Intrusion prevention system, secure run time environments, live VM migration and security frameworks for VM migration, VM privacy mechanism, General VM management systems, multifactor authentication, intrusion detection systems, user data isolation, attribute/identity-based encryption, role-based access control model, user-based permissions models, process isolation
Trust	Trust models such as public key infrastructure-based trust model, evidence-based trust model, reputation-based trust model, SLA verification-based trust model, evidence-based trust model, policy-based trust, data anonymization, auditing and accreditation by auditing standards, recommendations from cloud trust authority

Solutions

Area	Summary of Recommended Solutions
Data Security	Encryption and cryptographic models, bilinear pairing, signature verification, trusted third party, encryption, assured deletion, threshold secret sharing, erasure correcting Code, data redundancy, proxy re-encryption schemes, attribute based encryption, better security schemes for resident data, file assured deletion schemes, encrypted communication, mutual/Multi-factor authentication, Policy enforcement Security inside design architecture Encryption Secure key management Obfuscation Data Masking Data classification Network monitoring
Compliance and Legal	Unified regulatory compliance frameworks, trust models, embedding security and privacy parameters into SLA, improving current SLA models

Solutions

Area	Summary of Recommended Solutions
Privacy preservation	Authentication and session key management, encryption, certificate aggregate signcryption, user-level key management and update mechanisms, location-based encryption, cryptographic puzzles, regulation, position-based encryption,
Access Manage-ment and Insider Threats	Identity management frameworks, role-based access control scheme, decentralized access control for cloud storage, use of extensible access control markup languages, Use of hierarchical attribute-based cryptography, multifactor authentication and recovery, role based multi-tenancy access control, multi-tenancy authorization model for collaborative clouds, digital identity management, user managed access protocol, strong and secure anonymization technique