Security in Cloud / Edge / Fog Computing

Alessandro Carrega

TNT Lab – DITEN
University of Genoa

Information

- 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

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

    https://teams.microsoft.com/l/team/19%3a-Dtnw_NHUAl1AjZZV4HixIifmU8gywbskeeQwSV--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)*.

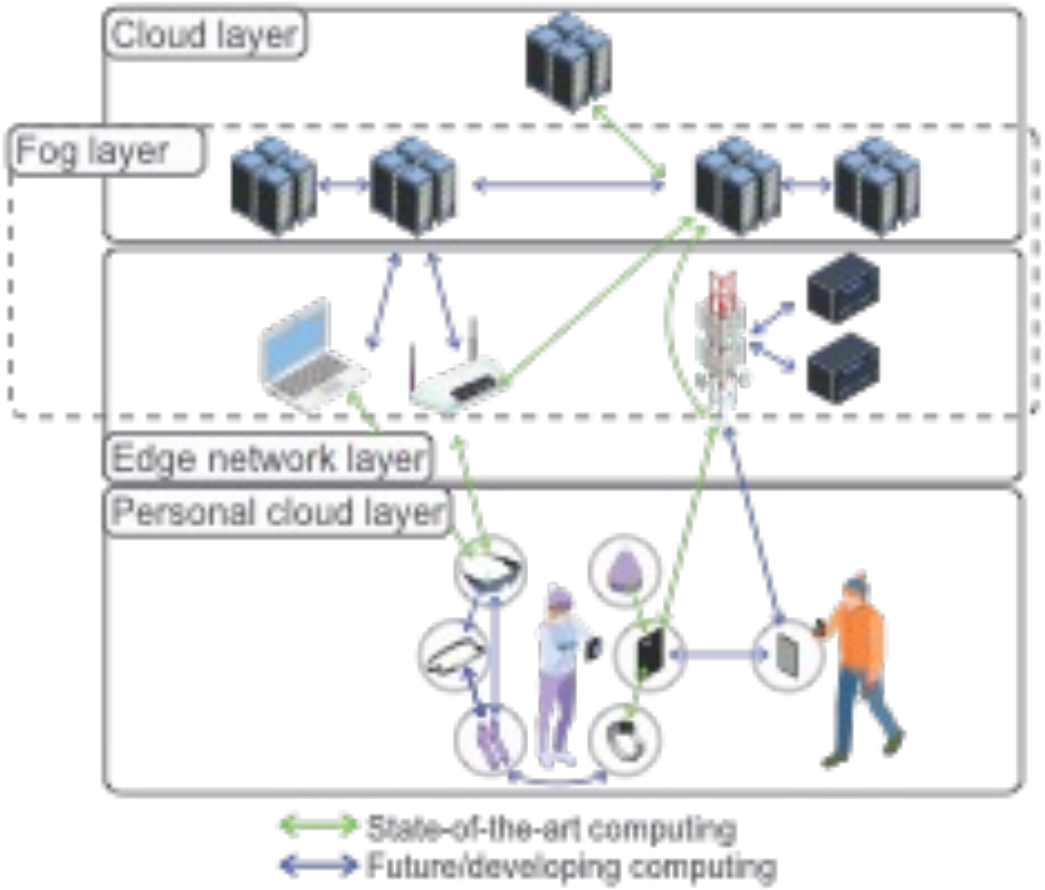
Introduction 1/4

- As of today, security and privacy issues have become a major concern when Cloud providers holding large amounts of data and essential applications share them with customers.
- Currently, most attention in each computing model is on protecting users' privacy from unauthorized groups or individuals gaining access and hindering attacks.
- Keeping data integrity intact and also maintaining it is a very vital aspect.

Introduction 2/4

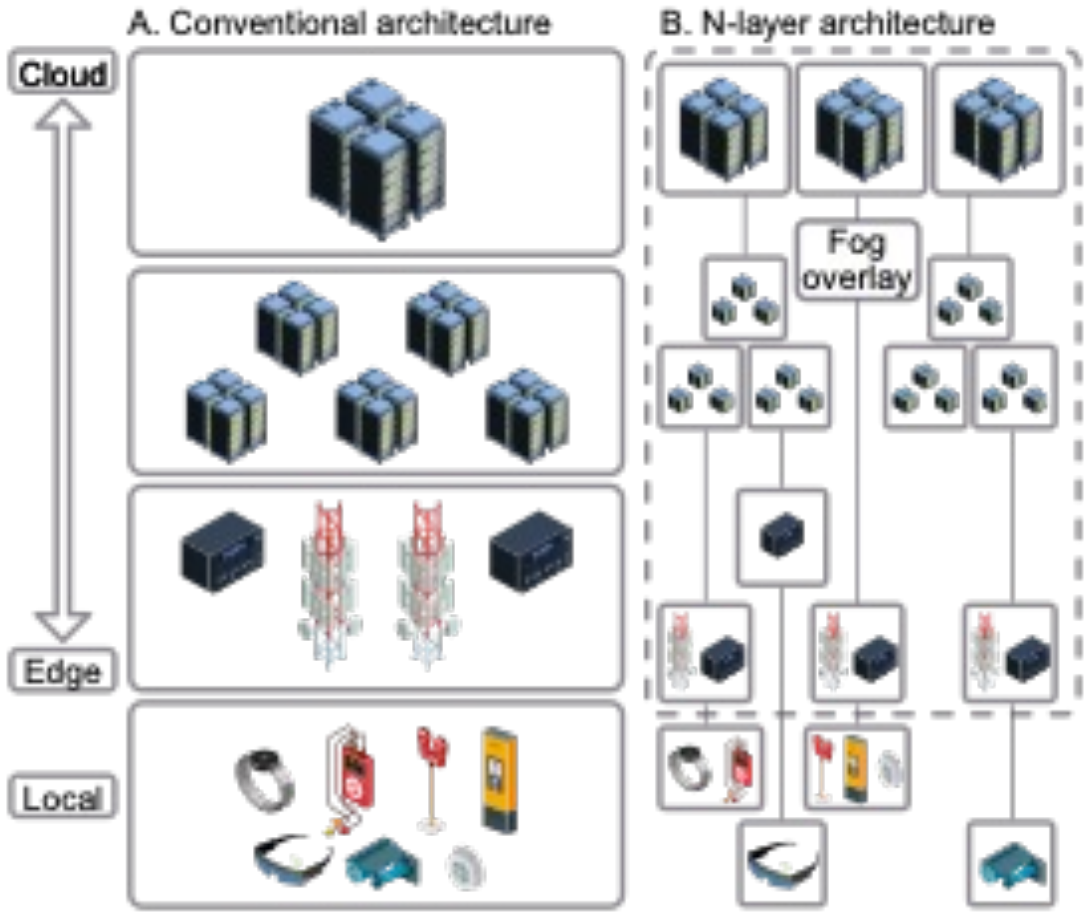
- 5 different features relating to security and privacy aspects are raised:
  - integrity,
  - accountability,
  - confidentiality,
  - availability, and
  - preservation of privacy.

Introduction



Various components involved in computing architecture.

Introducion



Most commonly analysed computing architectures.

Paradigm Comparison

Attributes	Cloud Computing	Edge Computing	Fog Computing
Architecture	Centralized	Distributed	Distributed
Expected Task Execution Time [1]	High	High-Medium	Low
Provided Services	Universal services	Often uses mobile networks	Vital for a particular domain and distributed
Security	Centralized (guaranteed by the Cloud provider)	Centralized (guaranteed by the Cellular operator)	Mixed (depending on the implementation)
Energy Consumption	High	Low	Varying but higher than for Edge
Identifying location	No	Yes	Yes
Main Providers	Amazon and Google	Cellular network providers	Proprietary
Mobility	Inadequate	Offered with limited support	Supported
Interaction in Real-Time	Available	Available	Available
Latency	High	Low	Varying but higher than for Edge
Bandwidth Cost	High	Low	Low
Storage capacity and Computation	High	Very limited	Varying
Scalability	Average	High	High
Overall usage	Computation distribution for huge data (Google MapReduce), Apps virtualization, Storage of data scalability	Control of traffic, data caching, wearable applications	CCTV surveillance, imaging of subsurface in real-time, IoT, Smart city, Vehicle-to-Vehicle (V2X)

[1] Importantly, Edge may provide higher results but only for computationally simple tasks (benefiting in terms of communication latency), while Fog would provide higher computational speed maintaining the latency (for, e.g., AR/VR applications). Executions in the Cloud would always provide the worst results as the computational unit is geographically distant from the user, which would naturally require tremendous communication overheads compared to geographically closer locations.

Cloud Data Security 1/2

- Protection and restoration guides for data and centers for Cloud services, and data involved in transmissions or transfers must always be protected.
- Need for simple yet robust mechanisms that offer a smooth method of learning about Cloud service capabilities before deployment
  - Align with Cloud security features during establishing stage.
- Issues such as service level negotiation, information traffic, and especially data security.

Cloud Data Security 2/2

- Important for Cloud service suppliers to properly protect customers' data stored in Cloud to reduce or eliminate security shortcomings.
- Techniques used in encrypting data must be very strong to guarantee better data security and implement authentication mechanisms that monitor other information access.
- Access control through data encryption should be established so that only rightfully selected employees can reach data.

Cloud Data Privacy 1/7

- Public Cloud faces more privacy threat
  - are very different based on their Cloud model variants.
- Proliferation of information, malicious usage by an unauthorized person, and incapability to control by clients.
- Clients' sensitive documents stored in Cloud can be reached by attackers using file's hash codes, with help of a mechanism used in duplicating information.

Cloud Data Privacy 2/7

- Risks about privacy are regarded from several angles, such as access control, Cloud systems, customers, and stored information.
- Knowing data privacy and other relating privacy principles will enormously assist in dealing with known threat concerns.
- One vital setback holding some organizations from moving to Cloud is fear of losing classified data through information leakage.

Cloud Data Privacy 3/7

- People's privacy is breached either knowingly or unknowingly. Accessing a person's private data without their knowledge or authorization is strongly considered an invasion of privacy.
- Different trends can occur, such as open disclosure, privacy attack, data violation, and other means of attacks.
- Privacy leakage can be very damaging, but privacy issues can be managed with (see next slide):

Cloud Data Privacy

Trust

- Disclosing data of an individual or organization is a breach of privacy.
- Pivotal role in decreasing or eliminating fear.
- Various standards every customer can agree to but their concern is to see minimal or zero breaches of privacy at a reasonable scale.

Cloud Data Privacy

Access Control 1/2

- Cloud systems present massive issues, such that an unauthorized person or group of individuals can obtain access if not properly addressed.
- Made functional by establishing management policies, checks on multi domain, and providing strong management keys.

Cloud Data Privacy

Access Control 2/2

- An effective way is by answering:
  - **Who?** Privileged persons to access certain data and who not to.
  - **What?** Some detailed data are not made accessible to every worker. So what specific files are permitted for whom?
  - **When?** Some data are needed for a period of time, and that period must strictly be controlled when that information has been accessed.

Cloud Data Privacy

Encryption

- Of data needs to be sufficiently strong to protect privacy of client's files.
- Weak encryption of data poses a serious challenge to Cloud privacy.

Edge Data Security 1/5

- Data integrity, confidentiality, and attack detection are common goal and reasons for data security.
  - Issues such as information breach and information loss are resolved by outsourcing information under control, non-fixed storage, and sharing responsibility.
  - Data duties are allowed to be carried out securely by customers.
- Presently, it is still challenging to identify works on Edge Computing security, and privacy since many academics do mostly focus on Cloud or Fog paradigms.
- Major aim of information security in Edge systems is to securely move data and ease heavy load by creating a shared model with a smoothly operating system.
  - Very acceptable shared information security and lightweight designs are developed for both end-users and remote nodes.

Edge Data Security 2/5

- Key responsibility in safeguarding customers' secrets and upholding confidence involved, especially at Edge network, should be rendered.
  - e.g., a digitalized building constructed with many IoT devices, which can be a prime target due to its huge quantity of personal data produced.
- More regarded approach to protect privacy of customers and gain their confidence is to make sure that data processing occurs at Edge network or node of house.

Edge Data Security 3/5

Confidentiality

- In case of mobile clients intending to use services of mobile applications, is always taken seriously, and some clients find it difficult to decide whether to use it.
- Very high risk posed by providers of services gaining unpermitted passage to classified information.
  - During data transmission in a distributed or unsecured network later stored and processed in Edge distributed network.
- Data security has constantly been breached.
  - Restricting access today to project confidentiality is achievable due to some newly created mechanisms.

Edge Data Securiy 4/5

Detecting Attacks *1/2*

- Edge systems can operate smoothly with assistance of Edge nodes where Edge applications are located to offer maximum standard services.
  - Entire Edge system is free from abnormalities or threats.
- Edge node consists of harsh surroundings with an inadequate security guarantee, exposing Edge nodes to threats.
- Performance of an Edge system can massively be hindered when threats from one Edge node are mismanaged and might subsequently extend to another Edge node.

Edge Data Security 5/5

Detecting Attacks 2/2

- Finding a quick solution can be hard because of weight of threat that spreads across Edge nodes.
- Added costs would be incurred to find baseline reason for problem, and even recovery might take a while.
- Regular checks must be performed to detect any previous potential or imminent attacks.

Edge Data Privacy 1/6

- Accessing system does not reflect trust.
- Averagely accepted systems store important data, resulting in critical privacy leakage.
  - Examples of clients' data stored are personal information, location, and identity.
- Focus areas to be discussed herein any order include privacy, identity, and location privacy safeguarding.

Edge Data Privacy 2/6

- Edge computing always raises much concern in stark contrast to other existing computing models protecting information.
  - e.g., leakages relating to Edge data privacy, are daunting.
- Edge information center, services, infrastructure suppliers, and even certain clients are potential weak link or at least establishments you cannot fully trust with such interwoven computing/cellular networks.
- Act of keeping safe private information of clients is an obligation that requires very close attention.

Edge Data Privacy 3/6

Protection of Data Privacy

- At Edge nodes, huge amounts of data belonging to clients are retrieved from applications and other users' pieces of equipment.
  - Collected information is then processed and analysed.
- Despite trustworthiness of Edge computing nodes, they can still display some level of vulnerability.
- Classified information such as an individual's medical data must be top secret.
- Information privacy protection is very important to avoid leakage at nodes of Edge computing.

Edge Data Privacy 4/6

Identity Privacy

- Compared to Cloud systems, especially Mobile Cloud, Edge models still lack adequate research attention in protecting identity of customers well.
- Identity privacy protection is a major concern for several organizations and even individual customers.
- Third-party identity-designed model is said to still pose vulnerability.

Edge Data Privacy 5/6

Location Privacy 1/2

- Several software and services from Worldwide Web render functional capabilities based on location.
- For a client to gain access when they want to use services in Edge computing, that client must deliver their location as required by service provider.
- Breaching data location through possible leaks.
  - Dynamic distribution in location privacy protection in a mobile model of social internet platforms.
  - Model can sort out visitors with low trust levels within a certain range of social interactions.

Edge Data Privacy 6/6

Location Privacy 2/2

- Breaching data location through possible leaks.
  - Social interactions.
  - Dividing customers' data location (unidentifiable) and personalities in individual storage systems.
  - Separation enables service provider to hide customers' location data safely.
  - Importance of model is that even if an attacker manages to breach one of storage facilities, for example, data location, it will not pose a major threat since identity of client is not leaked or exposed.

Fog Data Security 1/3

- Some attacks usually threaten private and government entities since they function in Cloud, Edge, and Fog computing.
- To offer a level of protection to architecture, a Threat Intelligence Platform (TIP) is important to be developed.
- Data security is most prioritized aspect in industrial sector, especially as information must be safeguarded.
- Intelligent equipment and sensor devices are deployed to reduce threats and security attacks extensively.
- Feature about heterogeneity and geographical sharing impacts implementation of Cloud security frameworks into Fog computing systems.
- Security challenges: confidentiality, authentication, availability, and information privacy.

Fog Data Security 2/3

- Considering medical field, we see that patients' health history involves classified information and Fog architecture has several nodes that might present some vulnerabilities.
  - Unpermitted access to information when stored or at time of transfer, untrustworthy insiders, and during system distribution of information.
- Fog system by means of cable or wireless network consistently receives information transferred from sensors of medical devices.
- Tampering with patients' personal data, integrity, and device availability is obvious and can occur when communication systems and sensors are targeted. Some through channels as Denial of Service (DoS) can easily be perpetrated due to vulnerabilities found in wireless networks.

Fog Data Security 3/3

- Absence of proper frameworks to control access to Fog nodes that process important information can compromise information through leakage because of account theft, unpermitted access, and possibly some unsafe passage.
- Problems can be mitigated through thorough analysis and stringent rules and regulations to establish standard control mechanisms such as personal systems, selective (limited) encryption, and reciprocated authentication.

Fog Data Privacy 1/2

- Protecting privacy of individuals and enterprises is often a primary concern encountered by Fog paradigm.
  - Especially with Fog nodes positioned near individuals and facilitates gathering of vital information sometimes relating to geographical location, identity, social security numbers, and many.
- Hard to keep centralized monitoring due to distributed nature of Fog nodes.

Fog Data Privacy 2/2

- During transmission, attackers can easily gain access to steal essential information when Fog nodes are not well secured.
- Needed innovate solutions to preserve data privacy.
- Privacy leakage often happens, even though end-users are never in accordance to release their personal information.
- Main areas of clients' privacy: data privacy, location privacy, identity privacy, and usage privacy.

Cloud Challenges 1/12

- Data loss, privacy leakage, multi-tenancy, unpermitted access to management platforms, Internet protocol, injection attacks.
- Potential attacks, letting access control to cybercriminals, granting access to unauthorized services, therefore disclosing several classified data, if not all.

Cloud Challenges 2/12

- Enormous threats when involved with these vulnerabilities and thus affects business too, either directly or indirectly.
- One of most reliable ways to repel threats and attacks is to identify any found and analyse behaviour properly.

Cloud Challenges 3/12

- Multi-tenancy is used in providing services to different customers and organizations with a particular software operating on SaaS provider's servers within architectural design.
- Every user company can use an application that is virtually designed in dividing data and configuring it virtually with help of specially designed software.
- In SaaS model, there is a high risk of vulnerability because clients turn to work with applications of multi-tenancy manufactured by Cloud Service Providers (CSP).
- Maximum-security of customer's data is direct responsibility of Cloud provider since sensitive information such as financial and individual data are hosted in their Cloud system.

Cloud Challenges 4/12

- Managing resources and scheduling work are some methods used by certain Cloud providers, but hardware potential is fully attained through virtualization by CSPs providers.
- Sandboxed setups refer to Virtual Machines (VM) being completely separate. Hardware sharing with clients is considered safe according to mindset.
  - Cybercriminals can gain access to host when sandboxed system has security setbacks.
- Virtualization software is strongly recommended since it is capable of showing recent vulnerabilities in Cloud security, such as retrieving data by targeting a VM on one machine through attacks through cross-Virtual Machine side channel.

Cloud Challenges 5/12

Data Integrity

- Security attention is greatly put on data integrity in Cloud, which means any reply to a data request sent must be from someone with an access privilege.
- Establishing a general basic data integrity standard is important, though it is not still in place.
- Trust is one of those many values that clients are expected to demonstrate in computing facet.
- Today, a lot of companies or institutions encounter issue of trust, and hugely impacts handling of their data.

Cloud Challenges 6/12

Unauthorized Access

- to management platforms and resources.
- Users are exposed to shared technologies often involved in Cloud services.
- An acceptable way of mitigating security solution of such a scenario is by introducing access control, and helps in securing client's personal information and its domain for privacy.
- Cybercriminals can simply have unauthorized access to Cloud service systems because of a single-style authentication model and not very strong authentication mechanisms being used.

Cloud Challenges 7/12

Data loss and Leakage

- Low cost of Cloud services is one reason customers turn to migrate to Cloud, and it is warned that customers should pay attention to their important information since various diverse aspects can easily breach their data security.
- Increased chance of data leakage or loss due to high traffic and usage of Cloud.
- Vulnerabilities and threats in Cloud service are undeniable, posing a great security threat to businesses and institutions.
- It can be frustrating when you cannot retrieve and restore data after accidentally deleting files from Cloud due to a lack of a backup system.

Cloud Challenges 8/12

Malicious Insider

- Every organization has different rules and regulations regarding recruitment policies and employee information.
- Some employees have higher status, which guarantees them privilege of accessing certain essential data within company.
- Based on CSA, they proposed implementation of transparency in general data security and management activities standard, outlining notification procedures during security failures, while using Service Level Agreement (SLA) as a demand for human resource, and finally establishing and exercising strict rules in management of supply chain.
- It may be far easier for a person with malicious ideas to work for a CSP since no one is seen as a suspect.
  - Individual can quickly be involved in malicious events, especially if they have unhindered access to sensitive information, especially if CSP cannot strictly monitor its workers.

Cloud Challenges 9/12

Identity Theft

- Victims or organizations can suffer heavy impact due to weak passwords due to phishing attacks by some attackers who turn to disguise as authentic persons to steal different important data of their victims.
- Sole reason for identity theft is to gain access to sensitive digital resources of individuals and companies by any malicious means.
- Every protected communication within Cloud system happens with access control, and made possible using an encryption key.

Cloud Challenges 10/12

Man-in-the-Middle Attack

- During flow of data from one end to another or between different systems, cybercriminals can easily take advantage and gain access, therefore having control of classified data.
  - Occur when secure socket layer (SSL) is insecure due to inadequate configuration.
  - Specifically, in Cloud systems, hackers can attack communication within information centers.
- Efficient SSL configuration and data analysis among accepted entities can go a long way to significantly lower threat posed by a middle-man attacker.

Cloud Challenges 11/12

DoS attack

- Aims to limit or stop execution of service and from accessing needed data.
- Creates a scenario where actual users partially or fully lack service availability. Whenever right person uses Cloud services to reach data server to access information, access is denied.
- Attacker uses a method in which he constantly congests server of a precise resource through request flooding, and targeted server will then be unable to reply to a legitimate access request.
- Several ways attack can be performed, for example, by way of SQL injection attack, bandwidth wastage, and also by way of incorrectly using model resources.

Cloud Challenges 12/12

Phishing Attack

- one of most common attacks in which criminal turns to impersonate and deceive their victims by leading them to malicious links.
- Flexible for hackers to hide their Cloud hosting of numerous accounts of different clients that uses Cloud services using phishing activities.
- Two kinds of threat divisions in which phishing can be grouped.
- Irresponsible attitude whereby a cybercriminal can also make full use of Cloud services to simply host a site for a phishing attack.
- Cloud computing services and their many accounts can be hijacked.

Edge Challenges 1/5

Data Injection

- When a machine is vulnerable, an attacker can push harmful information to share negative information.
- Act of injecting dangerous data by a malicious attacker into a device is known as poisoning.
- Data can be faked, then used to create fraudulent messages to render nodes of target compromised, and it is called an external forgery, for example, in a modern digital industrial production line where adversary happens to give false machine readings, therefore causing severe functional changes with bad aim to harm devices.

Edge Challenges 2/5

Eavesdropping

- Attacker can mask itself and observe network traffic during transmission and capture data illegally.
- Quite hard to point out type of attack because attacker happens to hide inside platform.

Edge Challenges 3/5

Privacy Leakage

- Absence of strict access control to node of Edge can easily lead to data privacy being tampered with.
- Attack strength is very low.
- Information generated from devices situated at Edge proximity is stored and processed in Edge data building.
- Customers classified these Edge data buildings can leak information since content is known.

Edge Challenges 4/5

Distributed DoS

- Attackers usually take advantage of network protocol vulnerabilities to launch attacks on Edge nodes, causing network damage and restricting resource access and provision of services.
- Attackers carry out these attacks by loading server with many data packets to shut down channel by jamming server's bandwidth.
- Another option is where Cloud data server or Edge systems are being flooded with data packets to massively take out resources .

Edge Challenges 5/5

Permission and Access Control

- Unauthorized access is a major challenge in Edge paradigm.
- Important to know an individual or employee before authorizing them to access any sensitive information in system.
- Achieved by establishing access control protocols.
- Connectivity between several pieces of equipment and other services can be considered secured when access control measures and permission are implemented.

Fog Challenges 1/6

- Cloud paradigm has countermeasures for its security and privacy threats.
  - May not apply to Fog paradigm due to active presence at network Edge of Fog entities.
  - Immediate vicinity where Fog entities operate will confront various threats which may not constitute a good functioning Cloud.
- Security solutions in Fog paradigm are improving and increasing as well.
  - Most of published literature on Fog computing security and privacy does not provide insights with an extensive assessment of various issues.

Fog Challenges 2/6

Trust Issue

- Fog systems face trust design challenges due to reciprocal demand for trust and distributed nature of their network.
- Cloud computing platforms are different since they already consist of pre-designed security models that match industrial security requirements, granting customers and enterprises some trust measures within Cloud system.
- Not for Fog computing networks which are more exposed and liable to security and privacy attacks.
- Even though same security mechanism can be deployed to every Fog node that makes up Fog computing network, distributed design also makes it quite challenging to resolve trust problems.

Fog Challenges 3/6

Malware Attacks

- Infecting Fog computing system with a malware attack is a very high-level challenge in network.
- Carried out to steal sensitive data, breach confidential information, and even refuse service with help of a virus, spyware, Trojan horse, or Ransomware.
- To assist Fog computing applications in mitigating these malicious attacks, authentic defence mechanisms for virus or worm detection and advanced anti-malware must be introduced.

Fog Challenges 4/6

- *Computation—Data Processing*
- Fog nodes often receive data collected from end-user equipment, processed, sent to Cloud system, or end-user pieces of equipment are forwarded information transmitted from Cloud.
- After various processes, data sent from end-users to Cloud systems and data sent from Fog nodes to Cloud are different in size and nature.
- Several providers have these Fog nodes, making them hard to be trusted due to many security and privacy shortcomings arising after processing of data.

Fog Challenges 5/6

Node Attack

- Attacker engages physically by targeting to capture vulnerable nodes.
- When attacker can decide to alter whole node, cause defects to hardware, or steal sensitive information from Fog nodes by digitally sending messages and causing sensor nodes distortion of classified data.
- Damaging effects on nodes of Fog network, and observing these node sensors will help identify issues and deploy some node capturing defence of algorithmic cryptography.

Fog Challenges 6/6

Privacy Preservation

- There is a huge concern as customers using CSP, IoT, and wireless systems face data leaks of personal information.
- Not easy to preserve privacy in Fog network due to closeness of Fog nodes to customers' environment, and it can also facilitate gathering plenty of vital information such as identity, location, and utility usages.
- Privacy leakage can also occur when communication between Fog nodes becomes more frequent.

Major Attacks 1/10

- Vulnerabilities, threats, or security attacks can appear differently in different paradigms, and there exists no specific way of solving various security issues.
- Several designed models must be considered to safeguard a Cloud, Edge, or Fog computing system.
- Help creating a joint force of many reliable layer defence models.

Major Attacks

Layer	Brief Description	Attack	Specifics of Paradigm/Main Proposed Countermeasures		
			Cloud	Edge	Fog
Application	Data inclined applications faces attacks and if breached, unpermitted access on websites is reached. Malware is of different forms, e.g., Trojan horses and viruses. An illegal software used to access legitimate information. Attacks HTTP [117].	HTTP Flood	Application monitoring is highly recommended. Web Application Firewalls (WAF), Anti-virus, privacy protection management [118].	Filtering mechanisms and intrusion detection systems [26].	HTTP-Redirect scheme [119].
		SQL Injection	SQL injection detection using adaptive deep learning [120].	Modifying circuits to minimize information leakage by adding random noise or delay, implementing a constant execution path code and balancing Hamming weights [121].	SQL injection detection using Elastic-pooling [122].
		Malwares	Use of Antivirus Softwares [118].	Signature-based and behavior-based detection [123].	Mirai botnet detector [119].

Major Attacks

Layer	Brief Description	Attack	Specifics of Paradigm/Main Proposed Countermeasures		
			Cloud	Edge	Fog
Session/Presentation	"It is defined as a pool of virtualized computer resources." Virtualization offers better usage of hardware assets with an opportunity for additional services avoiding extra costs for infrastructures. Customers are provided with virtual storage [124].	Hyper- visor	Strong configurations, up-to-date Operating System (OS).	Computational Auditing	Robust Authentication scheme.
		Data leakage	Encrypt stored data/use secured transmission medium, e.g., SSL/TLS, Virtual Firewall [125]	Homomorphic Encryption [126].	Isolation of user's data, Access control strictly based on positions [114].
		VM-Based	Anti-viruses, anti-spyware to monitor illegal events in guest OS [127].	Identity and Authentication scheme such as Identity-Based Encryption (IBE) [126].	Intrusion detection and prevention mechanism use for anomaly detection, behavioral assessment, and machine learning approach in classifying attacks [119].

Major Attacks

Layer	Brief Description	Attack	Specifics of Paradigm/Main Proposed Countermeasures		
			Cloud	Edge	Fog
Transport	"Provides a total end-to-end solution for reliable communications". The two main protocols are TCP and UDP. The smooth performance in communication strongly depends on TCP/IP between user and server [128].	TCP Flood	Firewalls, SYN Cache [129].	SYN cookies [130].	Integrated Firewalls [131].
		UDP Flood	Graphene design for secure communication [132].	Response rate for UDP packets should be reduced [131].	Response rate for UDP packets same as in Edge, should be reduced [131].
		Session hijacking	AES-GCM symmetric encryption [132].	User light-weight authentication algorithm [130].	Encrypting communication using two-ways or multi-purpose authentication [92].

Major Attacks

Layer	Brief Description	Attack	Specifics of Paradigm/Main Proposed Countermeasures		
			Cloud	Edge	Fog
Network	The routing of data packets across different networks from a source to an end node, is performed by the network layer [133].	DoS attack	Intrusion Detection System (IDS) [134], Access Security	Network Authentication mechanisms	Deploy routing security and observing the behaviour of nodes [135].
		MITM	Data Encryption [118].	Time stamps, encryption algorithm [121].	Use of Authentication schemes [114].
		Spoofing attacks	Identity Authentication [118].	Secure trust schemes [39].	Secured identification and Strong authentication [39].

Major Attacks

Layer	Brief Description	Attack	Specifics of Paradigm/Main Proposed Countermeasures		
			Cloud	Edge	Fog
PHY/MAC	The manner how types of equipment are physically hooked up to a wired or wireless network system and can be sorted for physical addressing with the help of a designated MAC address [136].	Eaves-dropping	Encryption, Cryptography [137]	Data Encryption using asymmetric AES scheme [121].	Protection of identity by use of IBC [138].
		Tampe-ring	Detection of behavioural pattern	Observe manner of behaviour [137].	Multicast authentication as PKI [67].
		Replay attack	Dynamic identity-based authentication model [139].	Authentication mechanisms [140].	Key generation approach [140].

Major Attacks 7/10

- As of now, end devices do not involve any established security measures.
- During data transmission, security vulnerabilities are likely to be present.
  - Vulnerability research is underway to understand different ways an end device or layer can face an attack.
  - Research projects must be carried out extensively and in-depth when studying attacks and their aspects.
- At each layer, security vulnerabilities are safeguarded differently.
- Basic security demands such as confidentiality, authenticity, integrity, and not least, availability.
- Cryptography is suggested for data confidentiality in stopping data leakages to illegitimate persons.
  - Need additional computation power, therefore causing latency.
  - Users and end-devices have proximity to each other.
    - e.g., FNs pose some level of reach to individuals' data, especially where information is generated. Data processed in FNs are significant security-wise due to their sensitivity more than data being processed in Cloud servers, thus requiring enhanced protection.

Major Attacks 8/10

- Overall, Cloud, Edge, and Fog paradigms consist of applications, resources, and a massive quantity of end-devices within a given centralized or decentralized area, existing together and inter-communicating.
- Huge potential for vulnerabilities in security and privacy does exist.
- One good way of screening systems for possible vulnerabilities is by auditing security standards.

Major Attacks 9/10

- Vulnerabilities in any system might expressly grant attackers partial or full access to cause severe harm.
- If data are breached, it can expose critical information of individuals or organizations, and an attack can cause serious malfunctioning of an entire network and create disruptions.
- Main target of gaining access to sensitive data is threats, seizures, or vulnerabilities of examined paradigms, whether joint or apart.

Major Attacks 10/10

- Vulnerabilities can be properly discovered with right tools and approaches.
- Despite constant search for vulnerabilities in systems by attackers (hackers/cybercriminals), there are up-to-date, sophisticated countermeasures to mitigate such threats, internal or external.
- Each vulnerability has a specific mechanism to counter its threats and attacks.
- Vulnerabilities turn to undermine security and privacy of related paradigms, exposing them (data) to potential security attacks and privacy leakages.