Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 160 (2019) 734–739

Procedia Computer Science

www.elsevier.com/locate/procedia

The 3rd International workshop on Recent advances on Internet of Things: Technology and Application Approaches(IoT-T&A 2019)
November 4-7, 2019, Coimbra, Portugal

# Security and Privacy Issues in Cloud, Fog and Edge Computing

Shalin Parikh, Dharmin Dave, Reema Patel, Nishant Doshi*

*Pandit Deendayal Petroleum University, Gandhinagar,India*

**Abstract**

The advent of technologies like IoT and 5G brought a new computing paradigm called cloud computing into the world. Cloud computing has become the main platform for data warehousing and processing. However, storing data into the cloud has its own set of challenges and security concerns. Moreover, with increasing data being generated from each device; the traditional cloud computing paradigm has become ineffective in addressing problems like high latency, bandwidth limitation, and resource limitation. So, new computational paradigms like edge and fog computing are proposed to solve the former's issues at the device itself or near the device. Both these paradigms provide computing and memory storage options close to the device itself. Despite their advantages, no system is perfect. In this paper, I list down the different privacy and security problems in all three computing paradigms and their proposed solutions.



*Keywords:* Cloud Computing; Fog Computing; Edge Computing; Security; Privacy; Internet of Things (IoT)

## 1. Introduction

Over the last decade, cloud computing has emerged as the leading platform for storing and processing huge amounts of data. It has its spread into many industries like healthcare, education, real estate, finance, manufacturing, etc. Industries deploy their data to the cloud instead of keeping it on their local machines.

With the advent of technologies like 5G and IoT, traditional cloud computing is becoming ineffective in addressing problems like high latency, resource allocation, and bandwidth limitation [1]. According to a report by Cisco Global

* Corresponding Author. Tel.:+917923275458;
*E-mail address: Nishant.Doshi@sot.pdpu.ac.in*

1877-0509 
10.1016/j.procs.2019.11.018

Cloud Index, IoT devices will generate approximately 500 ZB of data by the year 2019 [2]. New technologies like edge and fog computing have come into play for the data management of IoT devices and smart applications.

Edge computing is an IT architecture that enables data from IoT devices to be processed at the device itself or near the device. The data is processed near the device at a local computer or server and not the main cloud data center. All the edge devices then push the received data to the cloud storage repository [1].

Fog computing and edge computing are used interchangeably because both involve an intermediate level of processing and storage. However, the key difference between the two is the location of computing. In fog computing, the Local Area Network (LAN) acts as a gateway where as in an edge environment, computing is done at smart devices by devices like Programmable Automation Controllers (PACs) .

The outline of the paper is as follows: Details about cloud computing architecture, its security and privacy concerns, and its solutions are in section 2. Section 3 and 4 have similar details like section 2 for edge computing and fog computing respectively. Section 5 ends with a conclusion and future scope of the computing technology.

## 2. Cloud Computing

It is the outsourcing of data storage and processing. Information hosted by a user resides on the global network of data centers rather than on a local server. It is a subscription-based service where the user has to pay monthly fees for the type of service environment he/she wants. Cloud computing enables users to access their files from remote locations and eliminates the hassle of buying expensive hardware for computation and storage [3].

Its main characteristics are Broad Network Access (BNA), resource allocation, and elasticity. BNA allows the user to access data from remote locations through standard platforms like mobiles, laptops, etc. Resources are allocated dynamically according to the tenants demand. Elasticity means that the resources can be scaled upwards and downwards according to the need [3].

Despite having so many features, the security of the cloud remains one of its most important prospects. Every cloud architecture has different privacy and security concerns. For security and protection of the cloud, security personnel look at the vulnerabilities in the architecture and the attacks that can happen to exploit it.

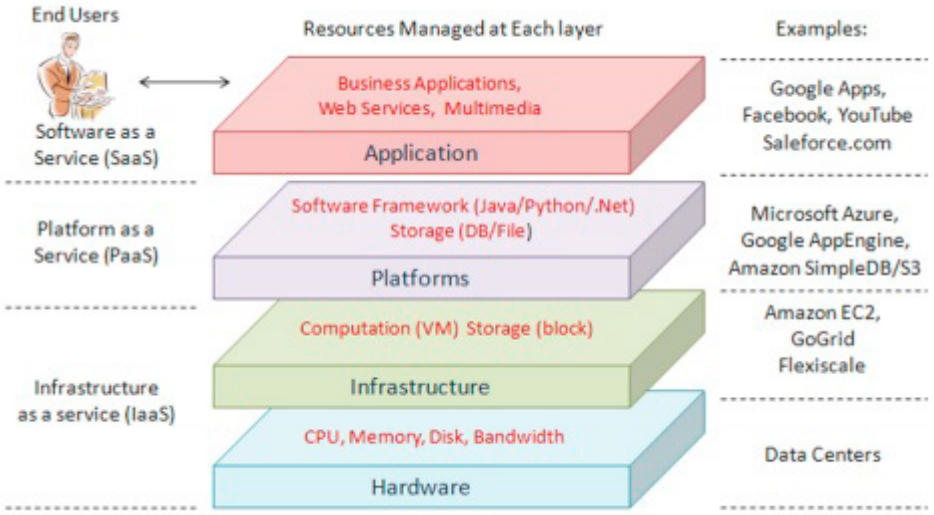


Fig. 1. Cloud Computing Architecture and it's three service models [4]

Some of the attacks on cloud computing include [5]:

1. Denial of Service (DoS) attack: In this attack, the illegitimate user sends excessive messages to the network for authentication requests from invalid return addresses to prevent other legitimate users from accessing the cloud service.
2. Injection of cloud malware: In this attack, a malicious service or virtual machine is injected into the system. The user tricks the cloud to consider the new service implementation as an instance of the system itself.
3. Communication interception: A person can intercept the communication between two users and exploit it.

It has three service architectures as shown in figure 1, namely:

1. Infrastructure as a Service (IaaS): In this system, the Cloud Service Provider (CSP) provides users the hardware infrastructure as a virtual interface to host their data. The users use their own operating systems (OS) and applications and perform processing, networking and storing on their deployed applications [6]. Hardware resources like CPU, Memory, Disk, Bandwidth are provided in this architecture.

   Security issues in this architecture are: [6]
   1. Unauthorized control over who can access confidential data
   2. Data theft by a malicious user in the system
   3. Inability to monitor cloud activities and applications
   4. Monitoring virtual machines from the host machine
   5. Monitoring a virtual machine from another virtual machine

   Solutions for security issues in this architecture are: [6]
   1. Monitoring the network
   2. Implementation of firewalls
   3. Segmentation of network

2. Platform as a Service (PaaS): In this system, users can create, test, run and manage their applications. Users are provided with a base OS and some development software along with the infrastructure to develop applications. Resources like software frameworks and storage are managed here as shown in figure 1.

   Security issues in this architecture are: [7]
   1. Absence of Secured Software Development Process with CSPs
   2. Recovery and backup from system failure or outage
   3. Inadequate provisions in Service Level Agreement (SLA)
   4. Legacy applications provided by the vendors

   Solutions for security issues in this architecture are: [7]
   1. Encapsulation of access control policies
   2. Trusted Computing Base (TCB) which is a collection of secure files acts as an added layer over the OS
   3. Authorization enforcement for admission requests

3. Software as a service (SaaS): In this system, all the infrastructure, OS and applications are provided by the cloud vendors themselves. It is also called as ‘on-demand software’. Users can use the software over the web by paying for a subscription. Users can access its services through a web browser [8]. The resources managed are business applications, web services, multimedia, etc. as shown in figure 1.

   Security issues in this architecture are: [8]
   1. Inability to maintain compliance standards regularly
   2. Inability to assess CSP’s operations
   3. Inefficient authorization and authentication
   4. Data losses and data breaches

   Solutions for security issues in this architecture are: [7]
   1. Encryption of user data
   2. Recovery Facilities
   3. Email security from spams and malware
   4. Backup of user data on system outage

## 3. Edge Computing

In an edge computing paradigm, the data generated by the smart devices or sensors are stored in the device itself or closer to the device and not sent to the cloud. It is preferred over traditional cloud computing because it provides real-time data computation without latency. It also enables faster responsiveness, faster processing, and smaller network traffic. Filtering out sensitive data to be sent to the cloud center at the edge device adds a security level for the data. Edge is any device that acts as an intermediary between the sensor and the cloud.

Key features of edge computing are reduced latency and mitigated bandwidth limits. Moving the workload closer to the user reduces the effect of limited bandwidth at a location. Edge computing can be used in a variety of areas like data analytics, real-time monitoring, Network Function Virtualization (NFV) and network monitoring [9]. Running NFV on edge layers maximizes efficiency and minimizes cost. Device data can be analyzed on the device itself and a condensed form of the data can be sent to the centralized cloud.

In edge computing architecture, the lowest level of the architecture is formed by the data sources as shown in figure 2. These data sources include sensors, actuators, appliances or data from third-party systems. These data sources communicate over IoT protocols to a nearby edge gateway at the device itself or near the device via any transport layer protocol [9]. These edge gateways preprocess the accumulated data before transmitting it to the cloud. They act as a security level from unauthorized access from other devices or users.

Some of the attacks on edge computing include [10]:

1. Eavesdropping: A malicious user can hide its presence and monitor the network to steal user data.
2. Denial of Service (DoS) attacks
3. Data tampering attack: In this attack, the hacker can tamper the data sent during communication or tamper the data kept in storage.

Despite its advantages, it has some privacy and security problems namely: [9]

1. Weak credentials for protection make the system vulnerable to malicious users
2. Insecure communication between devices
3. Recovery and backup of data during a system outage
4. Untimely reception and implementation of updates
5. Limited network visibility
6. Absence of user selective data gathering

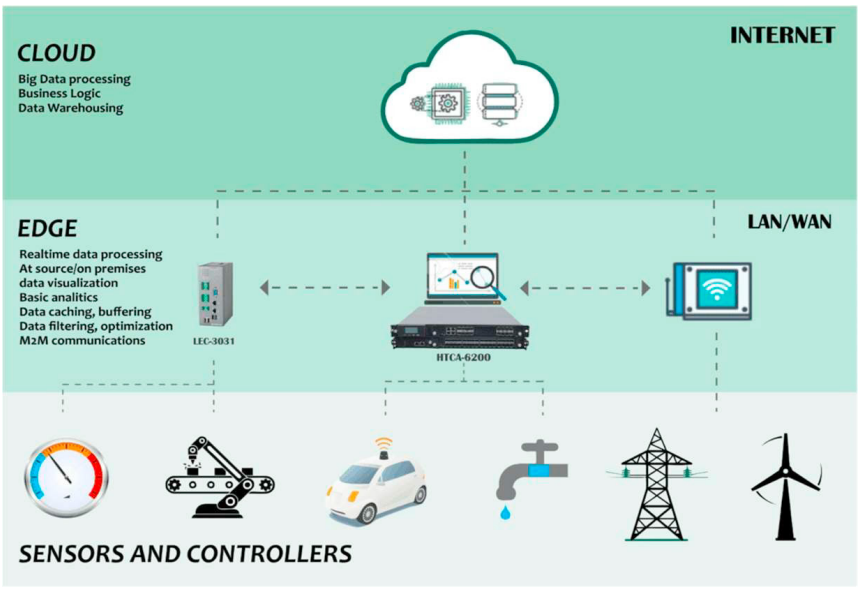


Fig. 2. Edge Computing Architecture [11]

Solutions for edge computing are: [12]

1. Equip all edge nodes with the same level of security as the network
2. Continuous monitoring and visibility of the network to be provided to the user in an interactive interface
3. Encryption and access authorization of data
4. Intrusion Detection System (IDS): It detects unauthorized access to the system and alerts the user.
5. Lightweight cryptographic algorithms along with a hardware performance monitor
6. User Behaviour Profiling (UBP) with Decoy Technique: General behavior of the users are monitored and maintained and any discrepancy from the desired behavior will provide the user with bogus information

## 4. Fog Computing

Fog computing or fogging is a similar cloud architecture like edge computing with an intermediate level between the data source and the cloud. In fog computing, it is done at fog nodes that collect data from various edge devices.

Its key features include awareness of edge location, less latency, mobility support, real-time interaction, heterogeneity, and interoperability [12]. In fog computing, the finest edge nodes are selected at the network edge. These nodes provide reduced latency and support for real-time interaction. Fog nodes can interoperate to provide services together. Fog nodes support the mobility of the edge identity to a new host location.

It is a three-tier system as shown in figure 3. The lowest tier is formed by edge devices like sensors, actuators, vehicles or data-generating applications. Above the edge devices, in the second tier; fog nodes are situated which collect data from numerous edge devices. The fog servers collect data from the edges via transport layer protocols like WiFi or Bluetooth. They handle requests from the edges in real-time and serve as a bi-directional gateway between the cloud and the edge devices. Generally, fog nodes are formed by routers or base stations. The topmost tier is the cloud data center which gets the data from the fog nodes.

Some of the attacks on fog computing include [12]:

1. Denial of Service (DoS) attacks
2. Virtual Machine based attacks
3. Side-channel attack: In this attack, the device's cryptography is reverse engineered by collecting information about its cryptographic algorithms.
4. Session hijacking: A user session is intercepted and hijacked by another user for getting access to user data and services

Despite fog's advantages, there are some privacy and security concerns namely: [12,14]

1. Limited Network Visibility
2. Ineffective ways of attack detection
3. Absence of user selective data collection
4. Virtualization issues
5. Multitenancy issues
6. Malicious fog node issues

Solutions for fog computing are: [12,14]

1. UBP with Decoy technique
2. Encryption of data
3. Virtual machine monitor
4. Modified decoy technique: It is a modification of the original decoy technique where fake data and fake nodes are provided to the malicious user. When these users run the fake files, hidden batch files collect their identity information like the Mac address.
5. Trusted Platform Module (TRM): Here an extra root key is shared between cloud and edge and the cloud can only access the data which is protected by the key. Rest of the data cannot be accessed by the cloud.

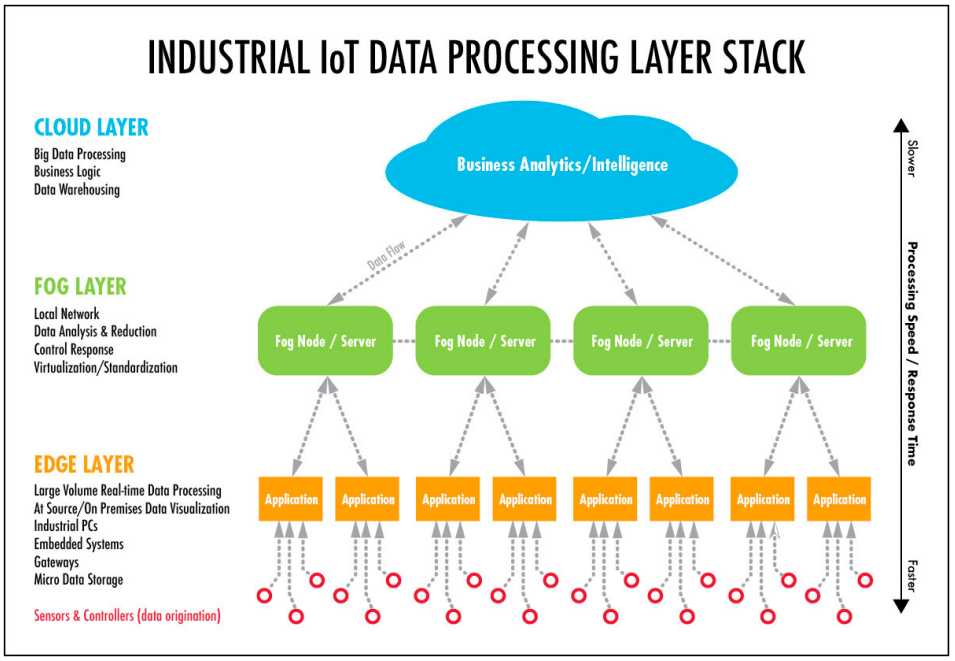


Fig. 3. Fog Computing Architecture [11]

## 5. Conclusion and Future Scope

Internet of Things (IoT) is an ever-growing field. With increasing data and data generating devices we will have to move from traditional computing techniques to new powerful techniques. Fog and edge computing have started replacing traditional cloud computing for the computation of data from IoT devices. But with a myriad of data coming shortly soon, we will have to discover new computation techniques keeping in mind the security and privacy of the user data first before anything else.

In the future, edge and fog computing should replace traditional cloud computing as much as possible. Research can be done to reduce the latency and the bandwidth requirement even further without compromising with the security of the system. The system should work autonomously after setting it up initially with all the requirements.

## References

[1] Weishong Shi, Jie Cao, Quan Zhang, Youhuizi Li, and Lanyu Xu "Edge Computing: Vision and Challenges" *IEEE Internet of Things Journal*, Vol. 3, No. 5, 2016, pp. 637-646
[2] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html
[3] Nidal Hassan Hussein and Ahmed Khalid "A survey of Cloud Computing Security challenges and solutions" *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 14, No. 1, 2016, pp. 52-56.
[4] http://cloudcomputingnet.com/cloud-computing-architecture
[5] Ajey Singh, Dr. Maneesh Shrivastava "Overview of Attacks on Cloud Computing" *International Journal of Engineering and Innovative Technology (IJEIT)*, Vol. 1, No. 4, 2012, pp. 321-323
[6] Sultan Aldossary and William Allen "Data Security, Privacy, Availability, and Integrity in Cloud Computing: Issues and Current Solutions" *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 7, No. 4, 2016, pp. 485-498.
[7] Pushpa B. Rajegore and Swapna G. Kadam "Issues & Solution of SAAS Model in Cloud Computing" *IOSR Journal of Computer Engineering (IOSR-JCE)*, pp. 40-44
[8] Jiale Zhang, Bing Chen, Yanchao Zhao, Xiang Cheng, and Feng Hu "Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues*" IEEE Access*, 6, 18209-18237
[9] Daojing He, Sammy Chan, and Mohsen Guizani "Security in the Internet of Things Supported by Mobile Edge Computing" *IEEE Communications Magazine*, 2018, pp. 56-61
[10] Praveen Kumar, Nabeel Zaidi, and Tanupriya Choudhur "Fog Computing: Common Security Issues and Proposed Countermeasures" *5th International Conference on System Modeling & Advancement in Research Trends*, 2016, pp. 311-315
[11] https://www.winsystems.com/cloud-fog-and-edge-computing-whats-the-difference
[12] Saad Khan, Simon Parkinson and Yongrui Qin "Fog computing security: a review of current applications and security solutions" *Journal of Cloud Computing: Advances, Systems and Applications*, 2017