



Cloud Computing (CS60118)

(Spring 2020-2021)

Introduction

Dr. Sudip Misra

Professor

**Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur**

Email: smisra@sit.iitkgp.ernet.in

Website: <http://cse.iitkgp.ac.in/~smisra/>

Research Lab: cse.iitkgp.ac.in/~smisra/swan/

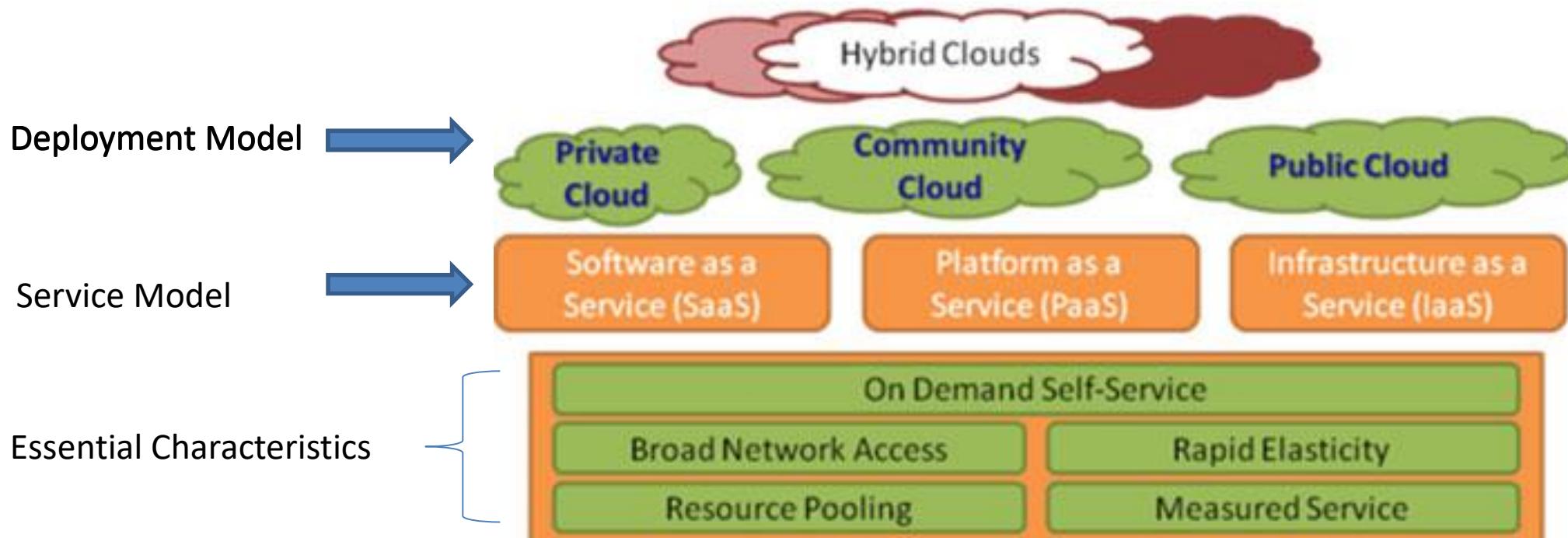
Introduction

- Though the farmers are growing same crops for centuries, the ever changing weather conditions, soil fertility, pests and diseases etc. still affects the final outcome.
- Information Technologies and tools.
- Information Communication Technology(ICT)
- That latest and most promising area of ICT is Cloud Computing.

Cloud Computing

- The term “cloud computing” refers to the fact that users do not really need to know who is providing those services and the cloud hid all the technicalities from them.
- less manpower and zero maintenance.
- Cloud computing, it has three different deployment models namely private, public and hybrid.
- Cloud computing offers the following basic models to deliver the services.
 - Software as a Service (SaaS)
 - Platform as a Service (PaaS)
 - Infrastructure as a Service(IaaS)

Cloud Computing Framework



Source: Tseronis, Lewin, Garbas and Mell (2010, p.15)

Current Challenges in Indian Agriculture

- Poor knowledge about the weather forecast, pests and diseases.
- Deficient production information.
- Not enough sales and distribution information.
- Poor ICT infrastructure and ICT illiteracy.
- Lack of awareness among farmers about the benefits of ICT in agriculture.
- Insufficient power availability in rural areas.

Applications

- Cloud computing can help with real-time computation, data access, and storage to users without having to know or worry about the physical location and configuration of the system that delivers the services.
- Some of the specific uses are as follows:-
 - Crop-related information:
 - ❖ It can capture information related to all crops grown in the recent past, and thus can help farmers make decisions on what to grow next.
 - ❖ **Weather information:** The cloud can store region-specific weather information and as well as the weather forecast for specific durations.

Applications

- **Soil Information:** Apart from soil profile, it can also provide a trend of soil in the past, which will help in predicting the trend in future. For example, is the soil turning acidic/alkaline, or, what other changes in nature and composition of soil can be seen.
- **Monitoring Growth:** This enables growth patterns to be compared with past growth patterns.
- **Farmers' Data:** Region-wise farmer data can be captured, monitor and study the involvement of local farmers. This can help in the identification of core agricultural areas, which are helpful for policymakers while framing their strategies.

Applications

- **Expert Consultation**
- **E-commerce** People from rural areas are unable to sell their own produce directly to the market. Many middlemen pop up in between the retail and production ends, which ultimately leads exploitation of the farmers. Through the agricultural management information system of cloud computing, farmers can sell their produce directly to the end users/retailers.
- **Practical Information Sharing:** Scientists working at agriculture research stations can share their own discoveries and suggestions regarding modern techniques for cultivation, usage of fertilizers in the cloud.

Advantage

- Less or no expenditure.
- On-Demand
- Measured service
- **Data management.** The data will be managed by the service provider, a team of professionals. That guarantees a better and organized management of data.
- **Data readiness.** This provides data from the e-data bank databases to its entire stakeholder at any time and at any location.

Advantage

- **Local and global Communication.** This makes the communication between different users much faster, easier and cheaper. Also the communication will be secured.

- **Rural-urban migration.** A major problem of Andhra Pradesh is rural-urban migration. It can be reduced as this provides its services all over the state and may also all over country at any time no matter how remote the place is. This will also help in controlling unemployment problem in the state and country.

Advantage

- **Security.** It provides an enhanced security as the resources will be stored in cloud and will be maintained centrally by the service providers. Thus, it is not a cause of concern for its users.
- **Motivation.** It will motivate the farmers and researchers to get involved more and more into agriculture as any communication will be result oriented. That will result in overall development of this sector in the nation.
- **Reduction of technical issues.** It cuts short the man power, maintenance and infrastructure requirement drastically, as it will be provided by the service providers.

Advantage

➤ **Overall economy.** Implementation of cloud computing in agriculture sector will help in uplifting the agricultural sector of the country. That will boost the overall development of the economy. It is due to the mass involvement of different stakeholders, as the system will monitor and deliver progress report whenever and wherever needed.

Challenges

- Conflict in different country laws. It demands a careful selection of the provider and may also require negotiation in drawing an effective agreement between the service providers and State.
- Another concern is the security and privacy. The nation may not be willing to hand over sensitive data to a third party.
- Cloud computing demands high bandwidth internet connectivity. For example, the current international bandwidth of Andhra Pradesh is 325Mbps, which is just sufficient to cater the basic needs in the state only, for entire India more than 1200Mbps is needed.

Challenges

- Lack of resources/expertise/ knowledge
- Availability of IT resources at different locations in vast country like India
- Availability of uninterrupted power supply
- Security of data and services.

Solutions by Cloud Computing

- Sending advisory audio and text messages based on weather forecasts, crop calendars, pest and disease prevention/control and market alerts.
- Provides early warnings on upcoming weather conditions such as cyclones, drought and rain.
- Provides market price information so that farmers can get the best possible price.
- Provides information on new seeds, inputs and technology.

Solutions by Cloud Computing

- Farm Produce Traceability.
- Farm Data Management system can enables large agriculture businesses to have complete control over their farming processes and visibility across different stakeholders
- **Farmer Advisory Services.**
 - Sending advisory audio and text messages based on weather forecasts, crop calendars, pest and disease prevention/control and market alerts.
 - Provides early warnings on upcoming weather conditions such as cyclones, drought and rain.
 - Provides market price information so that farmers can get the best possible price.
 - Provides information on new seeds, inputs and technology.
- **Monitoring & Evaluation**

Solutions by Cloud Computing

- **Supply Chain Management.**
 - Forecast the volume and plan the harvest schedule based on the yield estimation, crop area and crop calendar.
 - Digitization of various farmer organizations and farmer groups.
 - Tracks the current location of the produce through GPS tracking.
- **Market Linkage**
 - Enable farmers to participate in global markets by providing visibility to the buyer.
 - Informing the farmer of available markets and prevailing prices.
 - Connects farmers and buyers through a common portal.

Solutions by Cloud Computing

➤ Financial Services.

- Comprehensive management of all financial services in agriculture value chain including credit, crop insurance, collections and payments.
- Digitization all financial transactions with the farmers to provide transparency and accuracy of their operations for accessing credit.
- Minimize the risk of financial institutions to provide crop loans to the farmers by aiding in establishing farmers' credit worthiness and real-time monitoring of the crop growth and yields.
- Integration with digital and mobile wallets.

Case study 3:
Krishi Pragati Foundation
(KPF)

use **SourceTrace** to give digital solution

Case study: Krishi Pragati Foundation (KPF)

About(KPF)

- Non-profit organization supported by Tata Trusts .
- Specializes in fresh agri produce supply chain and helps to bridge the gap between farmers and consumers.

Objective of KPF. Is to maximize producers' share in the consumer price through establishing direct market linkages for farmers without any intermediaries.

Use of cloud by KPF. KPF is using **SourceTrace** to give digital solution.

- SourceTrace is a global leader in providing digital solutions to agriculture and food businesses.

Case study: Krishi Pragati Foundation (KPF)

SourceTrace gives SAAS solution and agri value chain management software make farming sustainable, supply chains efficient and bring transparency and traceability into food trade across 32 countries.

➤ **CLICK of a button.** Available on click of a button of Smart phones/tablets /intelligent mobile devices are fast replacing manual, paper-based methods in today's global supply chains.

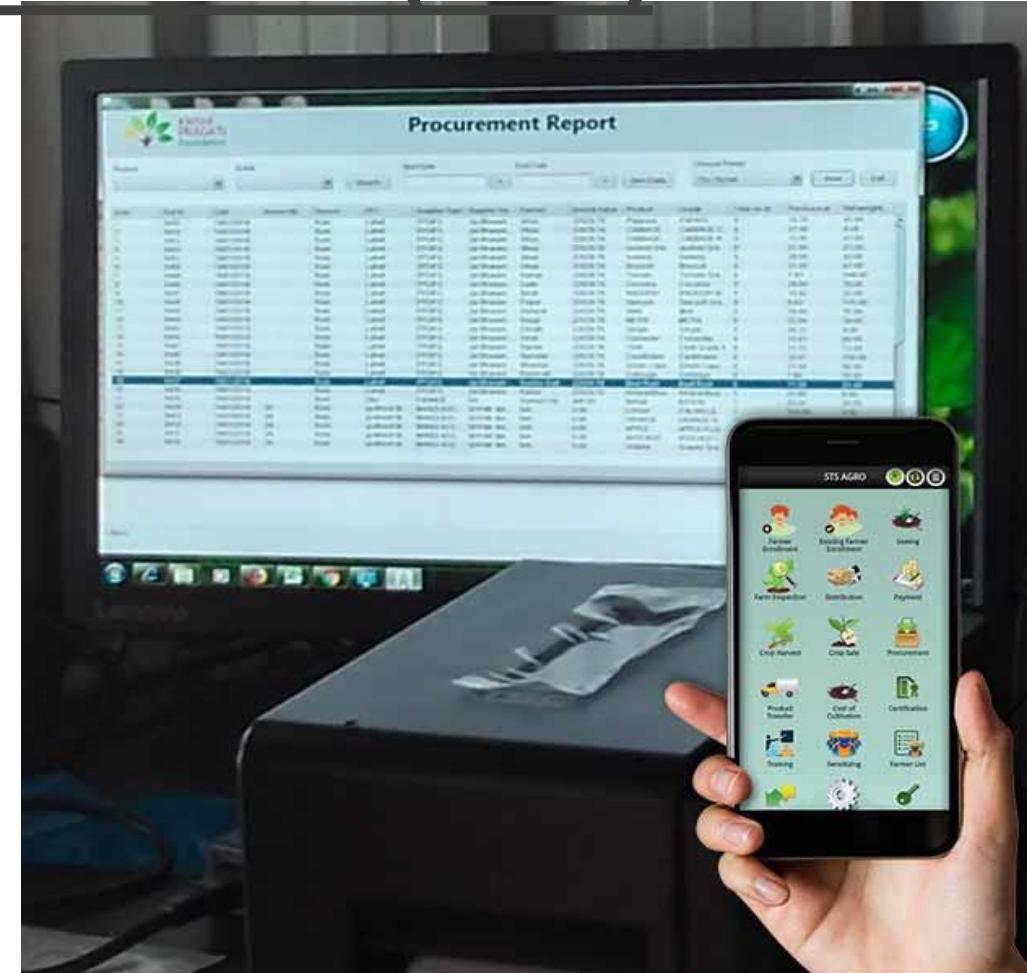


Image Source: www.sourcetrace.com/

Digitisation of supply chain. It means collecting and recording all end-to-end data of the company instantly and digitally, which also makes this data retrievable at any point of time.

- Digitisation of supply chains means that companies will have greater data gathering, reporting and analytics capabilities.
- Digitisation allows a basis for sharing goals and values instantaneously and continuously across organisations
- In short, digitization of the supply chain has the potential to dramatically lower costs, increase product availability, and even create new markets unknown or unavailable prior to the availability of key technologies

USE OF CLOUD COMPUTING BY KPF

➤ Advantage.

- Decreases manpower requirement
- Breaking down collaboration barriers between organisations
- Paperless
- Information is available in real-time and can be shared freely
- Creates a visible, transparent and ‘agile’ supply chain.
- Bridging gap between farmer and consumer.
- SourceTrace application generated a ‘QR code’, which appears as a sticker on the packages. A customer interested in tracing the source of the produce can simply scan the code and avail information of its source.



Image Source: www.sourcetrace.com/

Conclusion

- The Cloud computing is a game changing phase of IT that is not only impacting the way computing services are and will be delivered but also the way in which users will use IT.

- A move to the Cloud, however, requires a well planned strategy as there are many business and technical constraints that need to be mitigated.



Image Source: www.sourcetrace.com/

References

- 'Use of Cloud Computing in Agricultural Sector, a Myth Or Reality',
<https://www.researchgate.net/publication/307608027>, International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 10, October – 2013
- 'From Smart Farming towards Agriculture 5.0: A Review on Crop Data Management', 3 February 2020.
- <http://www.krishipragati.org/>
- <http://www.sourcetrace.com/>



Cloud Computing (CS60118)

(Spring 2020-2021)

Introduction

Dr. Sudip Misra

Professor

**Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur**

Email: smisra@sit.iitkgp.ernet.in

Website: <http://cse.iitkgp.ac.in/~smisra/>

Research Lab: cse.iitkgp.ac.in/~smisra/swan/



CLOUD COMPUTING
IN
Healthcare

Introduction

- In Today's real world technology has become a dominant crucial component in every industry including healthcare industry.
- The benefits of storing electronically the records of patients have increased the productivity of patient care and easy accessibility and usage.
- But many fears and security measures regarding patient records storing remotely is a concern for many in health care industry. .
- Despite of a common belief that certain boundaries and security issues of the cloud would hinder the shift, the healthcare industry is taking an initiative to move to these cloud based platforms. Today many doctors and hospitals are moving to-wards these clouds in order to provide better healthcare ser-vices to their patients.

Cloud Computing in Healthcare

- In recent years cloud computing technologies are on rise in the health care industries.
- The demand for cloud technologies in healthcare sector is increasing day by day. The environment in the healthcare sector is changing rapidly than ever before due to the increase in the demand for delivering the most effective medical services for a low cost of money which has increased the competition between the various healthcare providers.
- Cloud technologies provide opportunities to healthcare sectors in order to improve their services for the patients, to improve the operational facilities, to share information in an easy way, and to cut down the costs. Hence with the help of cloud computing in healthcare a doctor can access his patients records even if they are miles away.
- Thus the use of cloud technologies in healthcare can be proved as a boon for the patients all around the world.

Benefits of Cloud Computing in Healthcare

- **Mobility of records**: In some cases a person's health information can be required by two or more health institutions in that case by implementation of cloud technologies a person's health information can be easily synchronized and shared at the same time.
- **Speed**: Enables faster and accurate access to all the important information for the healthcare services providers and the history of their patients.
- **Security and Privacy**: By using cloud computing is mainly used for storage of medical records online. Use of encryption of data and protocols etc.
- Reduction of costs.
- Cost Savings
- Scalability/Flexibility
- Availability of data at all time.
- Easy updation of patient data.

Fears of Cloud Computing in Healthcare

- **Privacy and security challenges**: Always the data maintained in the cloud may contain either personal, private or confidential information regarding a person's health status and his health records which ought to be properly safe-guarded in order to prevent the misuse of this information and their disclosure.
- Disadvantage of using a public cloud is that it lacks the control and the security policies required for a health organization.
- Data Portability is another biggest challenge that some of the healthcare organizations face in adopting the' is the concern regarding the ability to transition to another cloud vendor or back to the healthcare cloud technologies organization without interrupting operations or introducing conflicting claims to the data.
- **Service Reliability**: Day to day growing reliance on distributed network based solutions are only increasing the difficulties and complexities of securing and maintaining the data in these dynamic environments. The dependence of this healthcare industry on availability and reliability of information can be a matter of life and death.

Fears of Cloud Computing in Healthcare

- Disaster recovery is a component of service reliability that focuses on processes and technology for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure in case of a disaster.
- Performance is another factor which is having a impact on slow adoption of cloud computing in healthcare industries.
- Dependency.
- Essentially need an Internet Connection which is not feasible in todays healthcare setups in all hospitals.
- Lack of Standards.
- Continuously Evolving.

Current state of Healthcare

- The healthcare industry has traditionally underutilized technology as a means of improving the delivery of patient care. Even today, organizations still rely on paper medical records and handwritten notes to inform and make decisions.
- This lack of access costs the healthcare industry millions of dollars each year in duplication and waste.
- Sharing of patient data among clinicians, departments and even patients is rare and complex.
- Patients today are better advocates for their own healthcare; they are more educated to their diseases and increasingly demand access to the latest technologies. As a result, demands for access to personal patient records are increasing and organizations need to keep up.
- When citizens can access bank accounts from anywhere in the world, withdraw money, get balances and make payments, it is hard for them to understand why they cannot have universal access to their secure health information.

Drivers for using cloud in Healthcare

- **Government Incentives.** Governments around the world are providing financial incentives for healthcare facilities to adopt new technologies such as electronic health records.
- Delivery of Cost-effective Healthcare
- **Clinical Innovation.** Healthcare is always striving to innovate to adopt new technologies that drive better patient care, born out of the cost and complexity of rolling out new technologies.
- **Big Data Growth.** Healthcare has become the best example of big data. As the amount of digital information increases, the ability to manage this data becomes a growing problem.
- Administrative Simplification.

Mobile Health

- Mobile health or mHealth usually uses mobile technologies as the basic elements for health research and delivering the healthcare services.
- It is like EHR(electronic health record (EHR) is a digital version of a patient's paper chart) with more advantages and functionality.
- In the future years to come these mobile systems will be able to retrieve and update the data that is stored in the electronic health records by the utilization of latest cloud technologies.
- The major advantage of using mobile technologies with cloud technologies is its mobility and easy sharing of the information.

Conclusion

- Cloud computing is changing our lives in many ways at a very quick pace.
- There are several reasons as discussed above for the utilization of cloud technologies in healthcare industry. The cloud computing solutions in healthcare can help the physicians to stay in touch with their patients and examine their health condition effectively at a low cost.
- There may be some concern regarding the security and other issues of data but still as every problem has a solution in the similar way these issues too will be overcome.
- It is always remembered that cloud computing is still a developing technology, which implies that in the future years the services it offers will be greater than our expectations or beyond our imagination.

References

- “Ahmed Meri Kadhum and Mohamad Khatim Hasan”, Assessing the Determinants of Cloud Computing Services for Utilizing, Health Information Systems: A Case Study. Vol.7 (2017) No. 2 , ISSN: 2088-5334
- “G.Nikhita Reddy, G.J.Ugander Reddy ”. Study of Cloud Computing in HealthCare Industry. <https://www.researchgate.net/publication/260126664>, 10 September 2014.
- “*By Hitachi Data Systems*”, W H I T E P A P E R: How to Improve Healthcare with Cloud Computing. May 2012



Cloud Computing (CS60118)

(Spring 2020-2021)

Introduction

Dr. Sudip Misra

Professor

**Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur**

Email: smisra@sit.iitkgp.ernet.in

Website: <http://cse.iitkgp.ac.in/~smisra/>

Research Lab: cse.iitkgp.ac.in/~smisra/swan/

CLOUD COMPUTING

IN

INDUSTRY

Introduction

- Cloud adoption is a growing reality across the industries. This calls for a fundamental paradigm shift in how business models and IT services are planned, built, and orchestrated. Bundling IT services into highly standardized packages and the industrialization of IT will lead to the next level of operational excellence with a direct impact on manufacturing business models.
- Cloud computing offers innumerable opportunities for manufacturers to enter new markets and to enhance customer satisfaction.
- New developments in products and services such as cloud-managed tools, home appliances, and other smart devices are only the first steps towards cloud-based business models.
- In short, successful manufacturing companies strive to increase customer value and gain a competitive advantage by enriching existing products with cloud services.

Cloud Deployment in Industries

- Cloud Computing offers innumerable opportunities for manufacturers to enter new markets and to enhance customer satisfaction.
- The industries is now and will remain highly affected by the digital transformation. Companies affected by new digital trends are faced with increasing demands for new products and services that cannot be completely met by the company's existing IT.
- In order to benefit from cloud computing, expand markets, and defend existing ones, IT departments will be responsible for the operation and support of cloud services as well as enabling IoT business in the foreseeable future.

Cloud Deployment in Industries

- Manufacturers will have to define a clear and consistent cloud strategy with publicly and privately available cloud services in order to be able to act appropriately as a cloud provider and/or consumer.
- In addition, the orchestration (integration) of various deployment models required to provide a consistent appearance to consumers places the IT department in the role of a cloud broker.
- A cloud broker as an entity manages the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers

Cloud Deployment in Industries

Cloud provider strategy

- As a cloud provider, the manufacturing company's IT department has to handle both the private cloud services for own business as well as public cloud services for consumers and other users.
- As a first step, the manufacturer should start the cloud journey by providing cloud services from a private cloud to the company's internal IT consumers/business units.
- At this stage, it As a second step, the manufacturing companies may extend their existing private cloud to a hybrid cloud by integrating it with one or more public clouds.
- Cloud services can be developed in the private cloud and then extended to the customers and (business) partners via the public cloud

Cloud Deployment in Industries

Cloud consumer strategy

- Many industries are still relying on legacy IT systems and private cloud services rather than public cloud services.
- Use of public or hybrid clouds should be addressed in the IT or cloud strategy in gaining benefits from the use of cloud services such as increased agility, decreased time-to-market or flexible costing.
- However, as a minimum the company's general compliance and security guidelines have to be enforced in cases where public cloud services are unavoidable.

Cloud Benefits in Industries

- Affordable data storage solutions
- Flexibility
- Data Security
- Backup and Recovery
- Automated Upgrades
- Enhanced Customer Support
- Scalability
- Data accessibility
- Low Maintenance
- Information is always available, even with different geographical locations

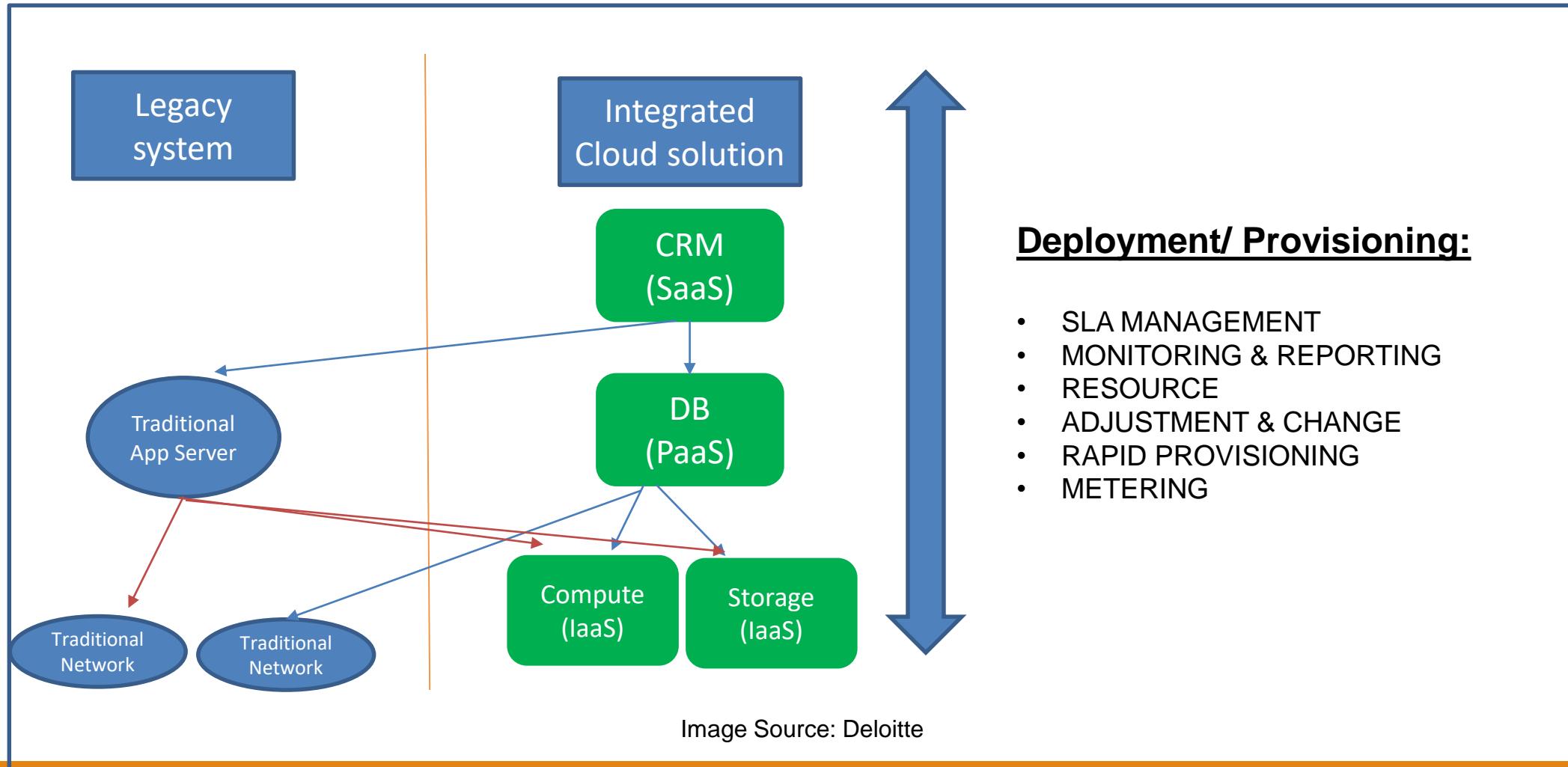
Cloud Disadvantage in Industries

- NETWORK CONNECTION DEPENDENCY
- LOSS OF CONTROL
- SECURITY
- Sharing company secrets with third party.
- **Downtime.** Downtime can lead to lost customers, data failure, and lost revenue.
- **Vendor Lock-In.** This is big issue. Although most cloud service providers assure that it is a breeze to use the cloud and integrate your business needs with them, disengaging and moving to the next vendor is still a huge problem.
- Limited Control and Flexibility

Cloud Orchestration

- **Cloud orchestration** Combination of IT or cloud services from multiple system components, which can be IT resources (e.g., technologies such as OS, middleware) or other cloud services.
- A company needs to set up a governance unit for the arrangement, coordination, and management of cloud and dependent non-cloud IT resources.
- To build, offer, and maintain orchestrated cloud services, the IT department has to take the role of a central provider and broker.

Cloud Orchestration



Cloud Orchestration

- No cloud service may be integrated into the corporate IT environment without the explicit involvement of the IT department. The company's management team must empower the IT department to:
 - Enforce cloud governance,
 - Set standards,
 - Evaluate and determine solutions for the cloud,
 - Remain responsible for architecture management, IT service management, supplier management, and compliance.
- As a broker of cloud services, the IT department has to ensure strict adherence to compliance guidelines for all cloud services consumed by the company and its subdivisions.

Conclusion

- In Industry use and implement more and more cloud offerings, IT organizations need to have a clear vision for the cloud journey in order to realize future manufacturing business models as well as to maintain and further build up their competitive advantage.
- IT departments must address the question of how to handle private and public clouds as well as how to integrate them into a hybrid cloud. They are to be encouraged to develop a comprehensive cloud strategy to ensure that the cloud activities support the business goals and focus on gaining the maximum business value from the incorporation of cloud services into the enterprise environment.
- Cloud strategy must ensure focus on gaining the maximum business value from the incorporation of cloud services into the enterprise environment.

References

- ‘Manufacturing Industry in Cloud Computing Era: Case Study’, ‘Department of Industrial Management, University of Vaasa, Vaasa, Finland’ , Y. Hao , P. Helo, 978-1-5386-0948-4/17/\$31.00 ©2017 IEEE.
- https://www.cisco.com/c/en_in/products/cloud-systems-management/intersight/demos.html
- https://www2.deloitte.com/content/dam/Deloitte/de/Documents/technology/Cloud_Strategy.pdf



Cloud Computing (CS60118)

(Spring 2020-2021)

Federation, Presence, Identity and Privacy in Cloud

Dr. Sudip Misra

Professor

Department of Computer Science and Engineering

Indian Institute of Technology Kharagpur

Email: smisra@sit.iitkgp.ernet.in

Website: <http://cse.iitkgp.ac.in/~smisra/>

Research Lab: cse.iitkgp.ac.in/~smisra/swan/

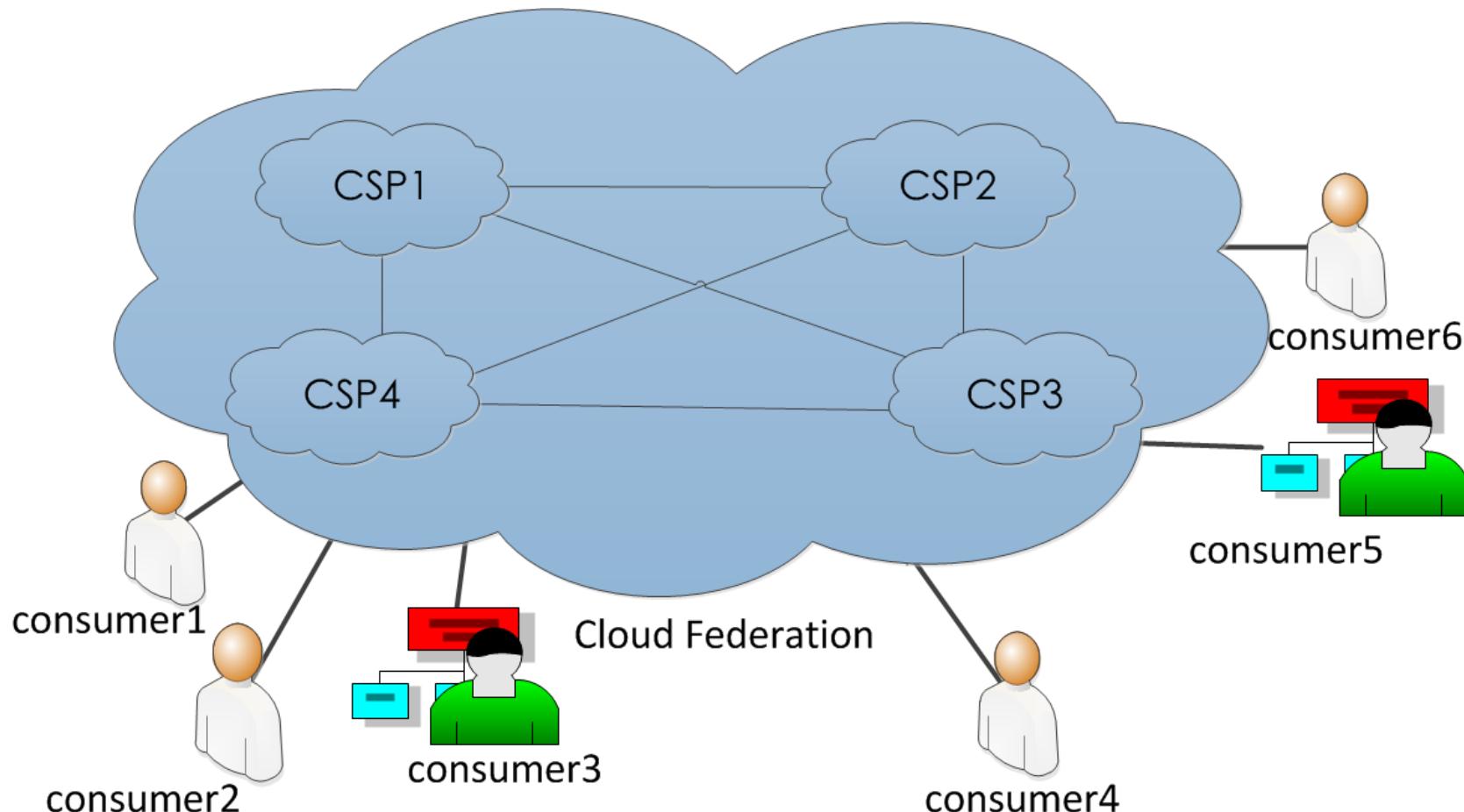
Contents

- Cloud Federation
- Privacy in Cloud

Cloud Federation

- Cloud federation is a geographically dispersed community, where many heterogeneous and autonomous cloud service providers cooperate and share resources to reach a common objective defined in the federation contract.
- The federation contract specifies the rules and policies that should be followed during the provision of services to consumers.
- It is an inter-cloud organization where multiple cloud service providers come under a single umbrella.

Cloud Federation (contd)



Objectives of Cloud Federation

- Dynamically expand resources to fulfill consumer demand.
- Resource lending.
- Integration of different types of cloud services in a single frame.
- Provision of reliable and required Quality of Service fulfilled services.
- Minimization of Service Level Agreement (SLA) violations.

Advantages of Cloud Federation

- Performance Guarantee – Resource lending helps to fulfill the demanded performance requirements of cloud service consumers.
- Service Availability Guarantee – Integration of different cloud service providers help to migrate services not only from one service provider, but also from disaster-prone area to a safe location.
- Convenience -- Cloud federation provides convenience and a unified view of services to the consumers.
- Dynamic Workload Distribution – Cloud federation distributes the service demand of the consumers into geographically distributed data centers of different cloud service providers.

Cloud Federation Models

- Semantics-based
- Market-oriented
- Reservoir
- Service-layers-oriented

Semantics-based Cloud Federation Model

- It is a theoretical federation model based on semantics and Infrastructure as a Service.
- It focuses on the interoperability of the components of different cloud service providers.
- Ontology is used to provide interoperability.

Market-oriented Cloud Federation Model

- This model focuses on the commercialization of infrastructure resources to fulfill the demand of the service market.
 - Four components used in this model are as follows --
 - Clouds – used for the provision of services.
 - Application broker – a middleware interface for communication between consumers and cloud service providers.
 - Cloud coordinator – a component located at each cloud in the federation and maintains the integrity of the federation.
- Concentrator – it acts as the market of resources and services.

Reservoir

- It is a cloud federation project of IBM.
- It provides a cloud federation framework to provide Software as a Service to the cloud providers.
- The objective of this framework is to help the isolated cloud service providers in overcoming the difficulties faced during the provision of services to the consumers.
- The four functional aspects provided by Reservoir are –
 - Automatic and fast installation of different services and applications.
 - Elasticity.
 - Continuous optimization.
 - Independence of virtualization technologies.

Service-layers-oriented Cloud Federation Model

- This federation model focuses on the relationships of IaaS, Paas and SaaS of cloud.
- Services are isolated as layers.
- It integrates not only different heterogeneous resources, but also different services of clouds.
- It provides a framework for information flow and parameter translations among different cloud service layers.
- Additionally, provides a framework where brokers perform different service scheduling for providing services to the consumers.

Geneva Framework of Cloud Federation

- This framework is developed by Microsoft to focus the issues of cloud federation.
- It is a claim-based framework and provides a common framework for accessing applications and other systems seamlessly.
- Multiple cloud service providers use this framework to interact with each other.
- Developers use this model for developing different authentication protocols that will work on existing corporate identity systems such as Active Directory, LDAPv3-based directories etc.

XMPP and XCP for Cloud Federation

- Cloud federations are based on Internet Engineering Task Force (IETF) standard Extensible Messaging and Presence Protocol (XMPP) and interdomain federation using the Jabber Extensible Communications Platform (Jabber XCP).
- Jabber XCP is a highly scalable, extensible, available, and device-agnostic presence solution built on XMPP and provides a programmable platform for adding presence and messaging services to the existing applications and services for creating new presence-based solutions.
- Messages are exchanged within different XMPP servers.

Advantages of XMPP

- Decentralized – anybody can configure their own XMPP server.
- Uses open standard.
- Multiple implementation of clients and servers are present in XMPP.
- Secure -- Simple Authentication and Security Layer (SASL) and Transport Layer Security (TLS) are used to provide security.
- Flexible and extensible for incorporating different types of applications, services and systems.

Levels of Cloud Federations

- There are four levels of cloud federations based on the ability to exchange XML stanza and messages among XMPP servers.
- The four levels of cloud federations are ---
 - Permissive federation
 - Verified federation
 - Encrypted federation
 - Trusted federation

Permissive Cloud Federation

- In this federation, an XMPP server accepts connection request from other XMPP servers without verifying identity.
- DNS lookups or certificate checking is not present in this federation.
- Domain spoofing is the major problem in this federation.
- In domain spoofing an unauthorized third party can pretend to be another authorized domain.

Verified Cloud Federation

- In this federation, an XMPP server accepts connection request from other XMPP servers after verifying identity.
- It uses DNS lookups and domain specific key exchange to verify the identity of other XMPP servers.
- Domain spoofing is not present in this federation.
- The connection among different XMPP servers are verified but not encrypted.
- DNS poisoning attacks are the major problems in this federation.

Encrypted Cloud Federation

- In this federation, an XMPP server accepts connection request from other XMPP servers after verifying identity and connection requests are encrypted.
- Transport Layer Security (TLS) and digital certificates are used for providing security .
- XEP-0220 defined server Dialback protocol is used for identity verification.
- Server Dialback prevents the address spoofing present in the XMPP networking.

Trusted Cloud Federation

- In this federation, an XMPP server accepts the connection request from other trusted XMPP servers .
- Root certification authority (CA) makes trusted the XMPP server by providing a digital certificate.
- The authenticating server authenticates digital certificates before accepting the connection request.
- In this federation, trusted digital certificates provides strong security compared to other cloud federations.
- DNS poisoning attacks are avoided in trusted cloud federation.
- Trusted cloud federation is difficult to manage due to its complexity.

Future of Cloud Federation

- The objective of the cloud federation is to seamlessly interact between people, devices, information feeds, documents, application interfaces, and cloud service providers.
- It enables cloud service providers and software developers to integrate and deploy efficient, easily scalable, fault-tolerant and heterogeneous cloud services.
- The use of XMPP and XEP protocols help the individual cloud service providers to overcome the issues of scalability, failure of services and easy migration of services from one provider to another.

Privacy in Cloud

Difference Between Privacy and Security

- Privacy of the data ensures the appropriate use of personal data under different circumstances.
- Security is the set of practices used to ensure confidentiality, availability and integrity of data.
- Security techniques are used to ensure privacy of data.

Introduction

- Data privacy is the crucial aspect of any business organizations and individuals.
- Outsourcing of data in the cloud creates challenges in data privacy.
- Adoption of cloud services depends on the maintenance of data privacy in the cloud.
- Different business organizations refrain to adopt cloud services due to data privacy.
- Therefore, privacy in cloud is required to increase the chances of cloud service adoption.

Challenges of Cloud Privacy

- Consumers' perspectives---
 - Do not know the location of their data stored in the cloud.
 - Who can or can't access the data.
 - Who keeps data.
 - What is really happening when a request for data deletion sent to the provider.
 - Whether CSP sells their data or not.
- CSP Perspectives –
 - Due to support of multi-tenancy features, the cloud service provider has to ensure that data of one tenant is not accessed by other tenant.
 - Public and hybrid cloud service providers are more prone to cloud privacy risk.

Cloud Privacy Laws and Legislations

- The different universally accepted laws and legislations published to manage the cloud privacy are ---
 - Fair Information Practices
 - European Directive 95/46/EC
 - USA Health Insurance Portability and Accountability Act (HIPAA)
 - USA Gramm–Leach–Bliley Act

Types of Private Data

- Personally identifiable information (PII) – used to identify an individual. It includes --
 - Key attributes -- name, phone number, social security or national identity number, email address and passwords.
 - Quasi-identifier – These attributes are used for linking anonymized dataset with other datasets and then identifying individuals such as ZIP code, date of birth, address etc.

- Sensitive Information --
 - Membership data – provides information about the membership into political, religious and other different communities.
 - Demographic characteristics -- nationality, gender, education level, job position, criminal record.
 - Finance data-- credit card number, account balance, financial transaction traces.
 - Health data -- medical record, diseases, diagnostics, medical images, prescriptions

Fair Information Practices (FIP)

- FIP is developed by USA to provide data protection and privacy.
- FIP defined data protection principles are ---
 - Data collection limitation
 - Purpose specification
 - Purpose use limitation
 - Individual participation
 - Visibility and transparency
 - Compliance of data
 - Accountability of data

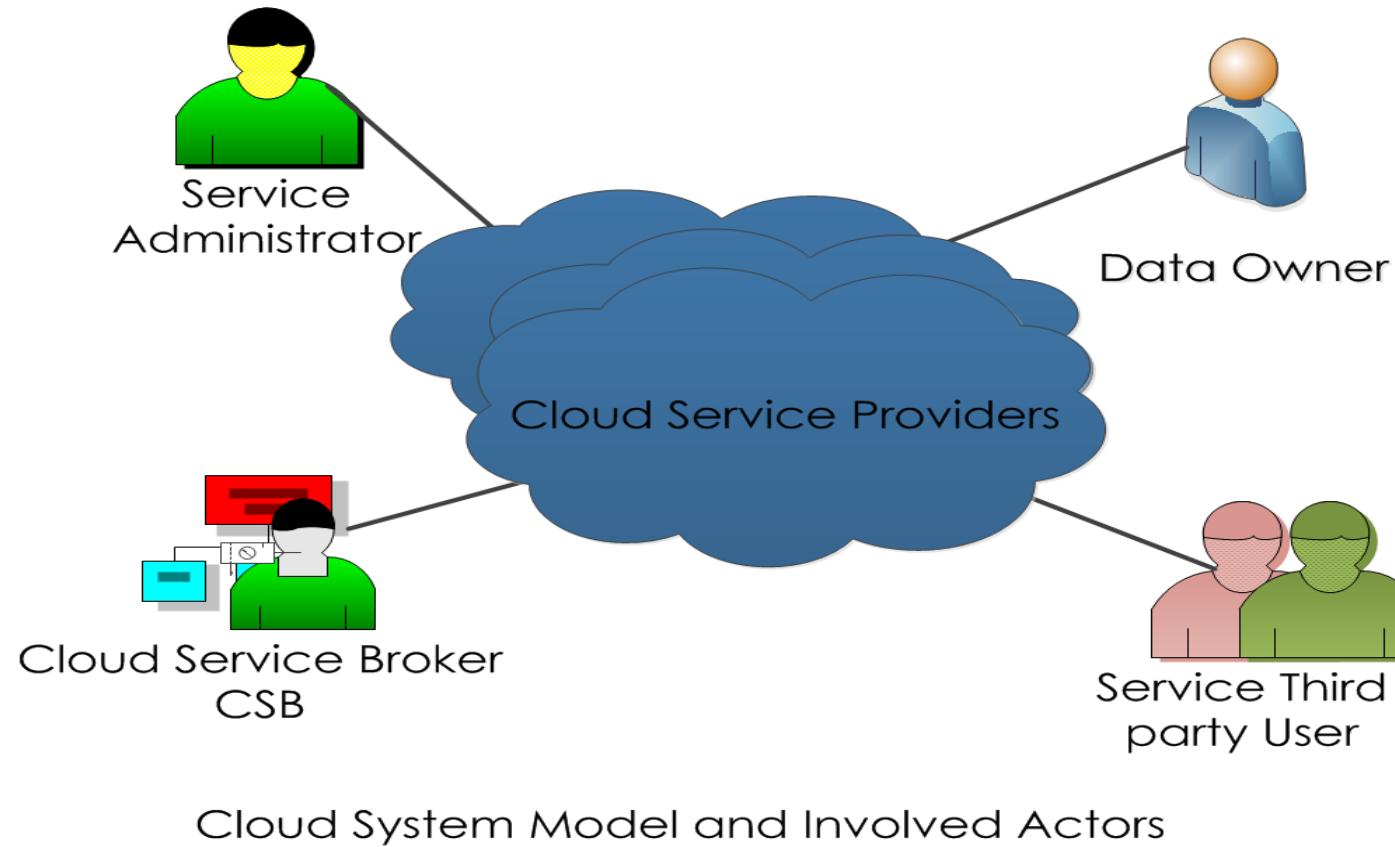
Privacy Issues in Cloud

- The privacy issues in cloud cover the following attributes –
 - Involved Actors
 - Lack of user control
 - Dynamic nature of the cloud environment
 - Compliance with laws and user's preferences
 - Accountability

Involved Actors

- The actors involved in handling data stored in cloud are ---
 - Data owner
 - Cloud service provider (CSP)
 - Cloud service broker (CSB) – it is an intermediate actor between CSP and data owner.
 - Cloud-based services – These includes application and programs deployed in cloud to provide different types of services such as customer relationship management, document management, cloud storage service etc.
 - Cloud-based service administrator – it is the owner of the service which can be CSP or other third party.
 - Cloud-based service third party

Involved Actors (contd)



Source: shorturl.at/zKPQU

Lack of User Control

- In public cloud data is stored in the remote server of cloud service providers.
- Owner of data is unaware about data processing, data access, storage locations and any privacy violation occurring or not.
- Eg. Users of Dropbox and Mega do not know their actual data handling policy.
- Business data stored in cloud can be used for providing advertisement by CSP.
- The major concern of the data privacy is the lack of user control on the data stored in cloud.
- From provider's perspective revealing of data handling policy may creates threats of consumers data due to multi-tenancy aspect of cloud.

Lack of User Control (contd)

- The reported incidents of data privacy in cloud are ---
- In October 2007, a “Salesforce.com” employee became a victim of a phishing attack and leaked customer list.
- In March 2009, Google revealed documents of users to third parties who do not have the permission to explore the documents.
- In 2010, several Hotmail accounts were hacked.
- In 2011, Amazon customer services were unavailable for several days, and data were lost due to a logical flaw in the cloud storage design.

Dynamic Nature of Cloud Environment

- The dynamic nature of cloud creates problems in data privacy.
- Dynamic algorithms are used for storage and transferring of data in the cloud.
- Transborder cloud imposes several restrictions on data handling policy.
- In transborder cloud, data flows from one country to another.
- Different countries obey different laws for data storage and processing which create issues in data privacy.
- Data replication causes data privacy issues in cloud.
- In data replication, several copies of the same data are made and stored into different servers which may or may not reside in the same country.

Compliance with laws and user's preferences

- Privacy Compliance (PC) is one of the major issue in data privacy in the cloud.
- Privacy Compliance (PC) depends on two factors –
 - Precise definition of the privacy policies
 - Capability of the used enforcement mechanisms
- The cloud service consumer is unaware of the data handling policy used by CSP.
- Cloud service consumers do not aware whether the data operations performed on their data are compliant with the privacy law enforced by the country where the data is actually stored.

Accountability

- According to the definition given by Galway project in the context of business data ---

“Accountability is the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information beyond mere legal requirements, and to be accountable for any misuse of that information.”

- Auditing mechanism is used for accountability of data.
- In cloud, accountability of data is required due to dynamic storage, duplication and transfer of data from one server to another.
- Accountability helps the cloud consumer to know where data are actually located, who is the processor of data, who are accessing their data etc.

Techniques of Data Privacy Protection

- The techniques used for data privacy protection are –
 - Encryption
 - Processing encrypted data
 - Obfuscation
 - Sticky policy
 - Trusted platform module
 - Data segmentation
 - Trusted third party mediator (TTPM)

Encryption

- In encryption, cryptographic solutions are used to encrypt data in the cloud.
- Encryption can be done by either CSP or consumer or both.
- Encryption-decryption key management is one of the issues in encrypting data in cloud.
 - One approach is to keep encryption-decryption kept on the consumer side.
 - Key management is handled by a trusted third party.

Processing Encrypted Data

- Processing of encrypted data in cloud compromises the privacy of data, as data is decrypted before processing.
- To overcome data privacy compromise, processing of encrypted data is proposed.
- In Homomorphic encryption, data processing and query execution is done on the encrypted data.
- The result of Homomorphic encryption is also encrypted.
- The decrypted result gives the same output as if the processing is done on the plain text.
- IBM FHE (Fully Homomorphic Encryption) is one of the Homomorphic technique used in the cloud.

Obfuscation

- Data obfuscation is a privacy preserving technique.
- It is also known as data masking, where masking rules are used for maintaining the data privacy by replacing the actual data with new data. The new data looks like actual data but are unrelated.
- Data obfuscation techniques are ---
 - Data randomization
 - Data Swapping
 - Anonymization

Obfuscation (contd)

- Data randomization – Data is made fuzzy by adding random variables with data. Eg. multiplying a column of data with a secret factor, replacing person identity with pseudo-identity.
- Data swapping – In data swapping, data values are swapped by obeying a predefined rule such that original data can be recovered from the swapped data.
- Data anonymization–
 - Data owner identity is removed from the data and then cloud actors use the data.
 - Data anonymization is subject to linking attack where owner identity is linked with the removed data by using other known databases.

Obfuscation (contd)

➤ Data anonymization–

- To avoid the linking attack, K-anonymization technique is proposed.
- In K-anonymization technique, after removing person identity remaining data is classified into quasi identifier and sensitive attributes.
- quasi identifier data is replaced with less specific data.
- It is called k-anonymous as in this technique each record can not be differentiated with $k-1$ record in the same database.
- Data obfuscation is less secure than encryption but computationally efficient.

Sticky Policy

- Data is attached to a sticky policy.
- The sticky policy determines the authenticated processing request span and authorization.
- Policy enforcement is ensured through policy management components called Policy Decision Point (PDP).
- PDP evaluates the data processing request against predefined sticky policy and decides whether to grant the processing request or not.
- Stick policy is computationally inefficient as data processing request has to be evaluated for each request.

Trusted Platform Module

- Trusted Platform Module (TPM) is a tamper-resistant hardware component developed by the Trusted Computing Group (TCG).
- TPM is responsible to implement all data privacy preserving techniques.
- TPM provides a black box to store data securely.
- However, TPM does not provide secure data processing.
- The disadvantage of TPM based solution is that it is hardware based.
- CSP has to setup TPM hardware at its each data center.

Data Segmentation

- Data segmentation is used to maintain data confidentiality.
- It not only ensure privacy of data but also data associations.
- Data is divided into different sets of blocks and stored into different non-linkable storage .
- In cloud, data segmentation is used to ensure data privacy.
- Data segmentation is performed according to sensitive data associations.
- Data reassembly is also planned along with data segmentation in cloud.

Trusted Third Party Mediator (TTPM)

- TTPM acts as middleman between service consumer and the other cloud actors.
- It is responsible for policy enforcement and data auditing.
- Eg. In E-commerce applications, TTPM is used to build customer trust.
- Cloud TTPM hides the personal identity and sensitive data from other cloud actors.
- TTPM is a trusted third party which acts as trusted root authority in cloud.
- It also helps to manage encryption-decryption key in cloud.

References

- Cloud Computing, Authors: John W. Rittinghouse, James F. Ransome, CRC press, 2017.
- M. R. M. Assis, L. F. Bittencourt, and R. Tolosana-Calasanz, “Cloud Federation: Characterisation and Conceptual Model,” in Proc. of the IEEE/ACM 7th International Conference on Utility and Cloud Computing, December 2014, pp. 585–590.
- A. Ghorbel, M. Ghorbel, and M. Jmaiel, “Privacy in cloud computing environments: a survey and research challenges”, Journal of Supercomputing, June 2017, vol: 73, no: 6, pp. 2763 – 2800.

Thank You!!!



Cloud Computing (CS60118)

(Spring 2020-2021)

Fog Computing

Dr. Sudip Misra

Professor

Department of Computer Science and Engineering

Indian Institute of Technology Kharagpur

Email: smisra@sit.iitkgp.ernet.in

Website: <http://cse.iitkgp.ac.in/~smisra/>

Research Lab: cse.iitkgp.ac.in/~smisra/swan/

Cloud Computing

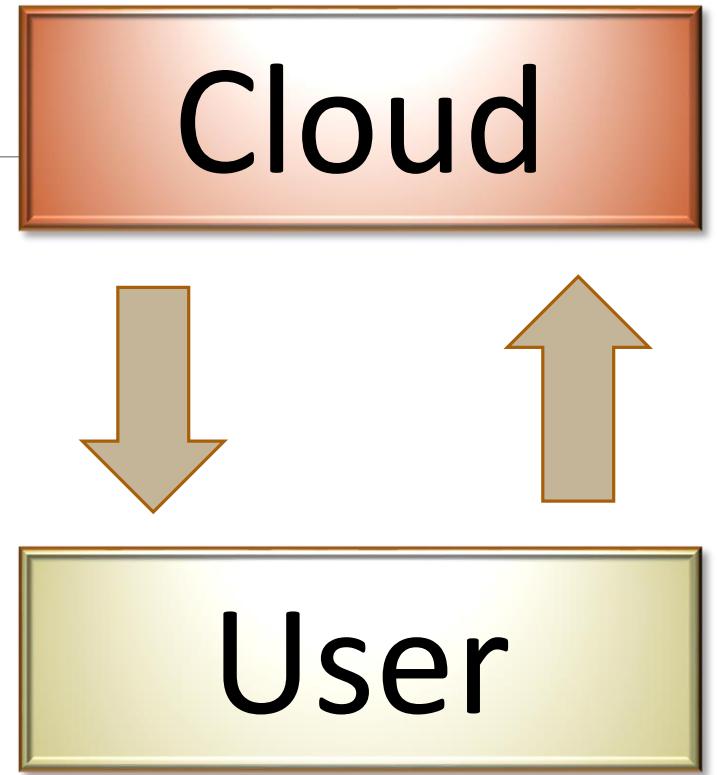
Remote access of applications and data

Device Independent

Virtual services

Scalable computing resources

Reduced capital and maintenance overheads



Cloud Computing Services

Software as a Service (SaaS)

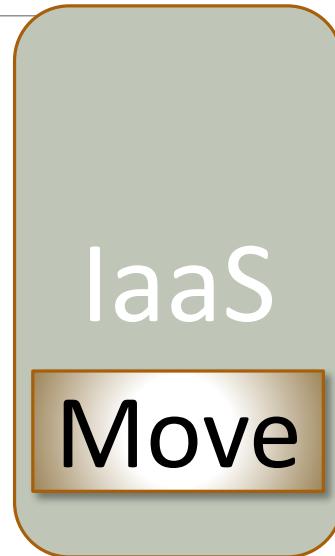
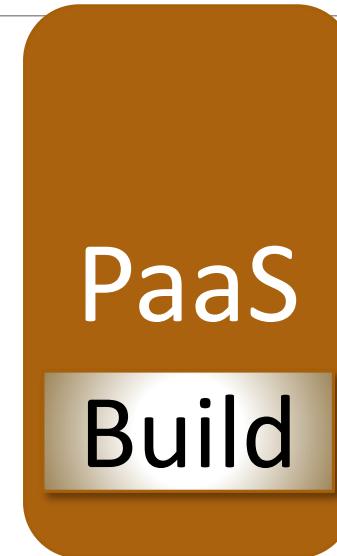
- Ready-made softwares
- Hosted on remote servers
- Example: Google's Gmail, Docs, and Sheets

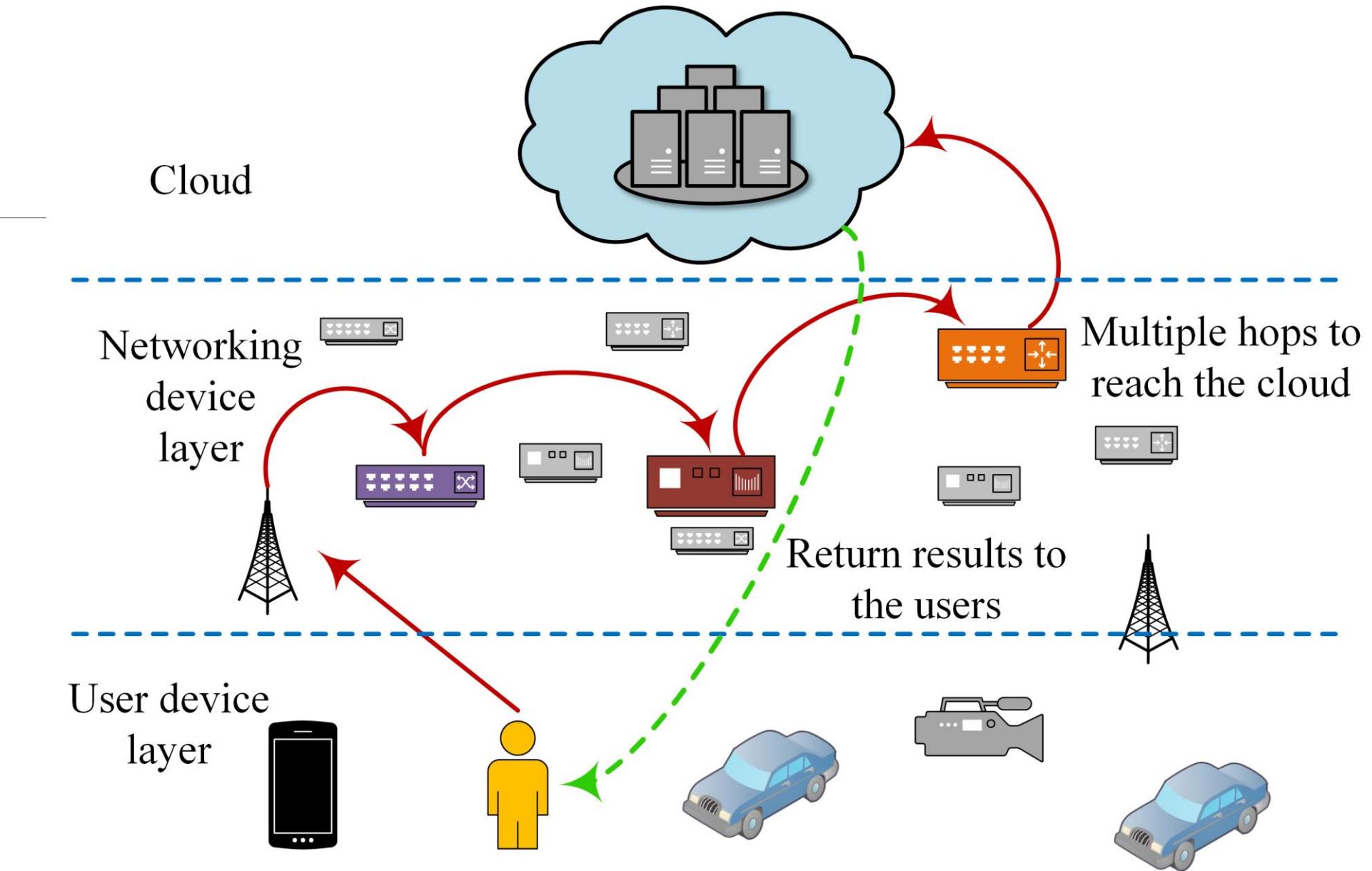
Platform as a Service (PaaS)

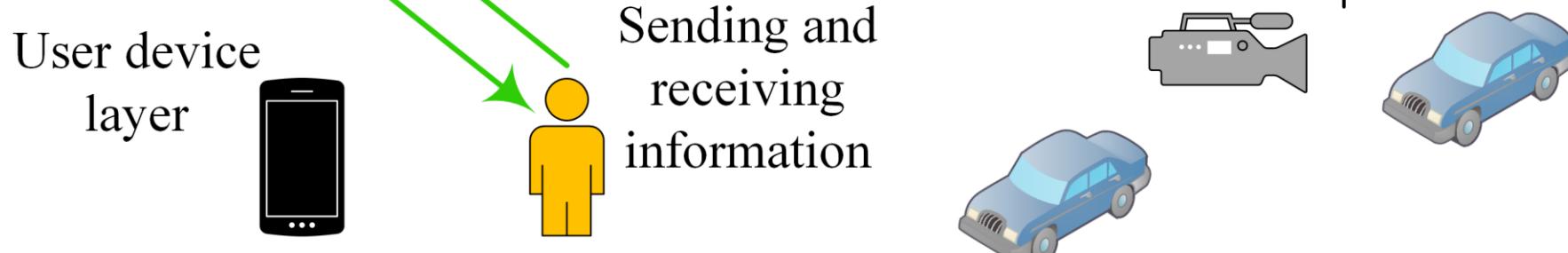
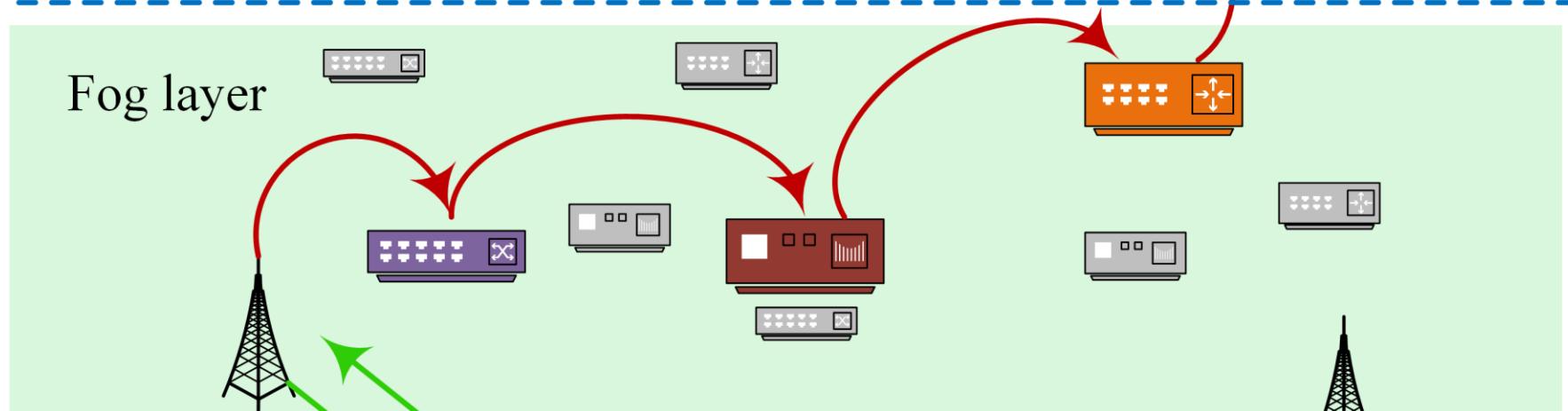
- Framework for developing applications
- Most web hosting solutions
- Example: Google App Engine

Infrastructure as a Service (IaaS)

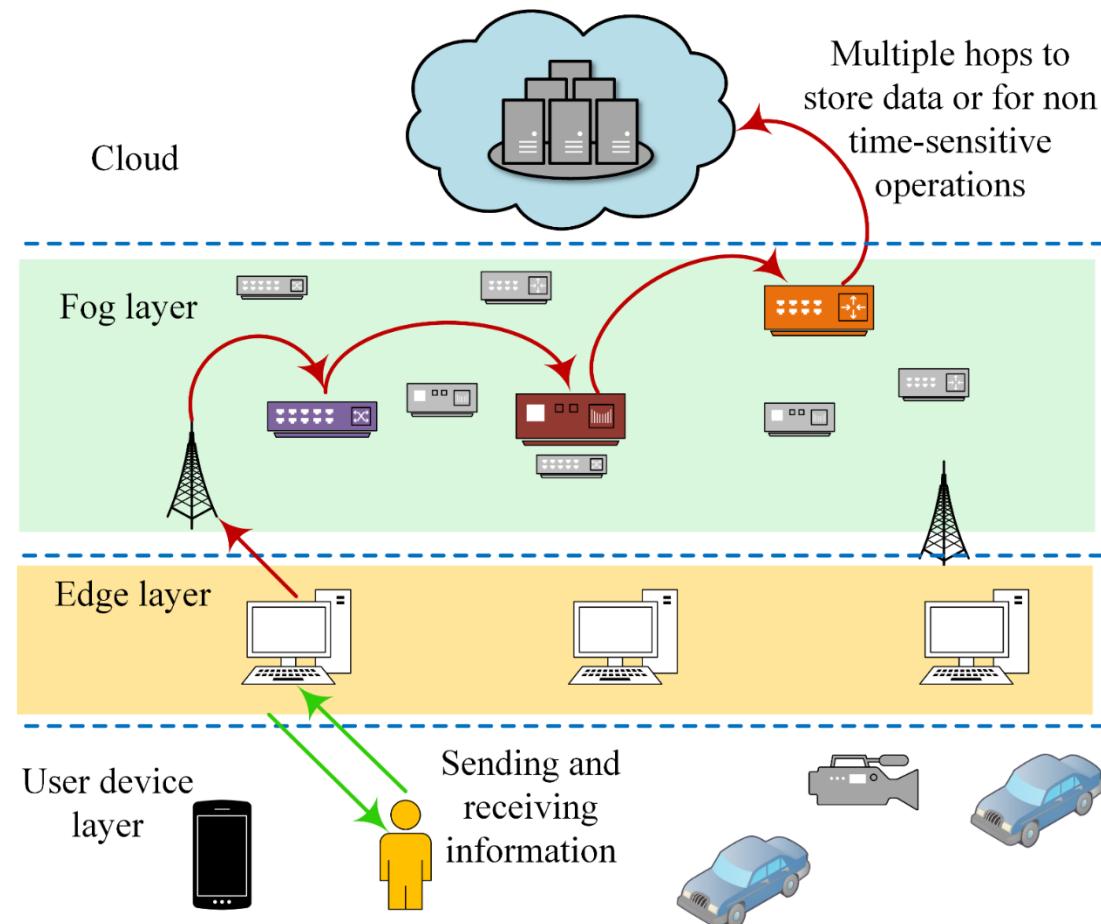
- Outsource for storages, servers, data center space, and cloud networking
- Illusion of on-premises infrastructure
- Example: Microsoft Azure, GoGrid







Fog vs Edge Computing



Fog vs Edge Computing

Both bring data and intelligence to the edge of the network

Edge computing is limited to embedded systems and close to the data sources

Edge computing does not transmit data to the network (issue with cloud communication)

Edge provides results in real-time

Fog computing operates on the LAN level for generalized applications

Fog computing provides results in near real-time

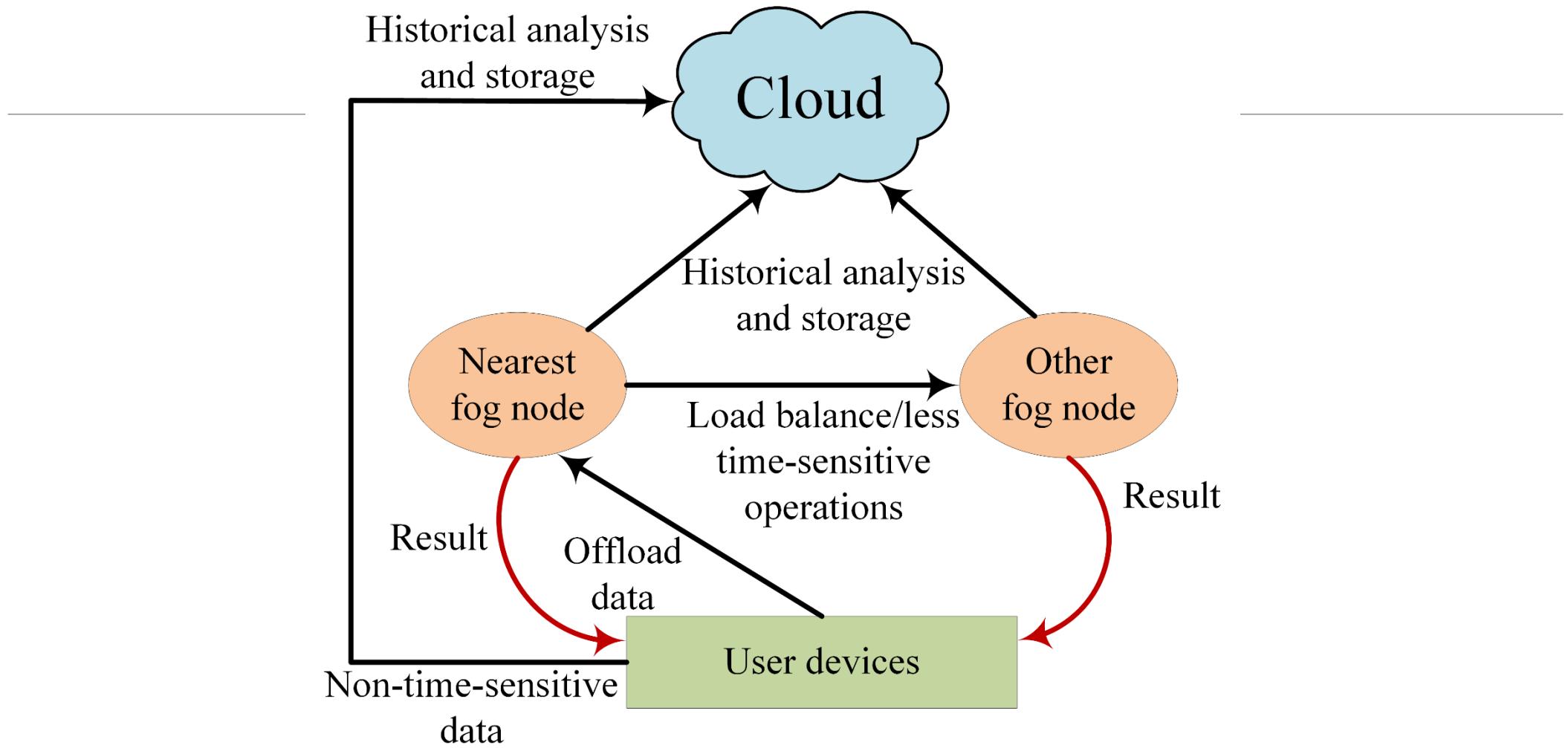
Fog Computing

*The fog **extends the cloud** to be closer to the **things that produce and act on IoT data**. These devices, called **fog nodes**, can be deployed anywhere with a network connection: on a factory floor, on top of a power pole, alongside a railway track, in a vehicle, or on an oil rig. Any device with **computing, storage, and network connectivity** can be a fog node. Examples include industrial **controllers, switches, routers, embedded servers, and video surveillance cameras**.*

-Cisco

Cisco white paper:

https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf



Advantages

Minimize latency

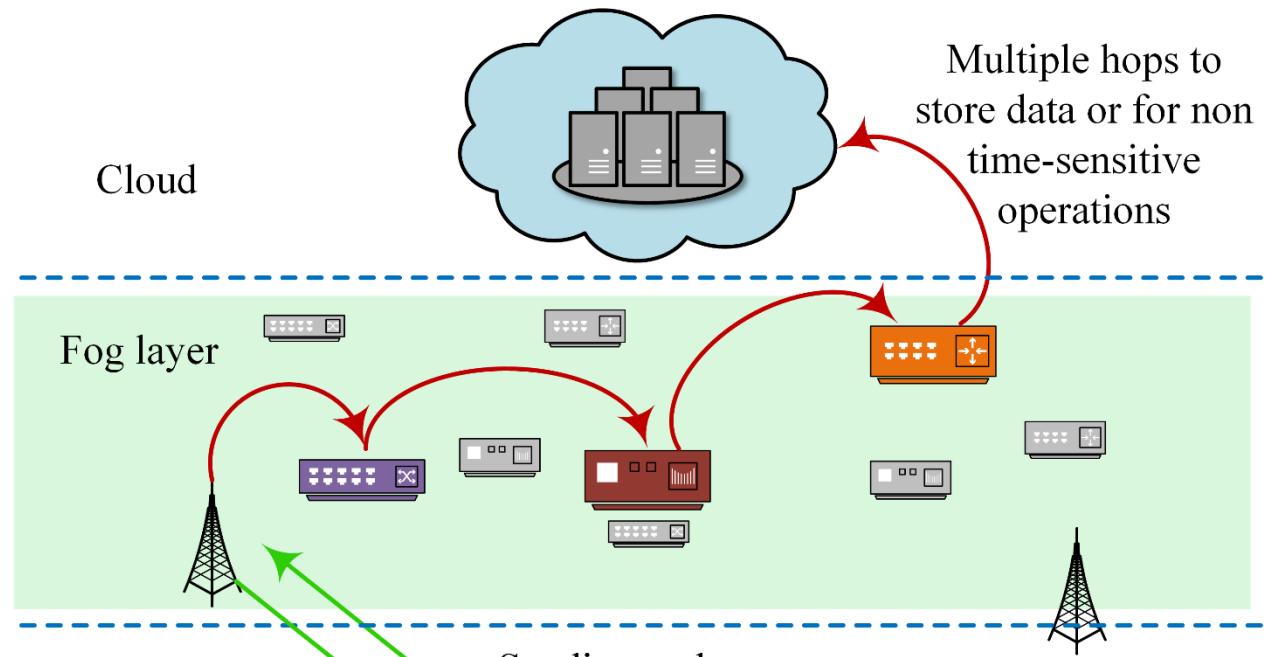
Bandwidth conservation

Enhanced security

Reliable operations

Spatially aware data

Optimized movement of data



Minimize Latency

Time-sensitive operations

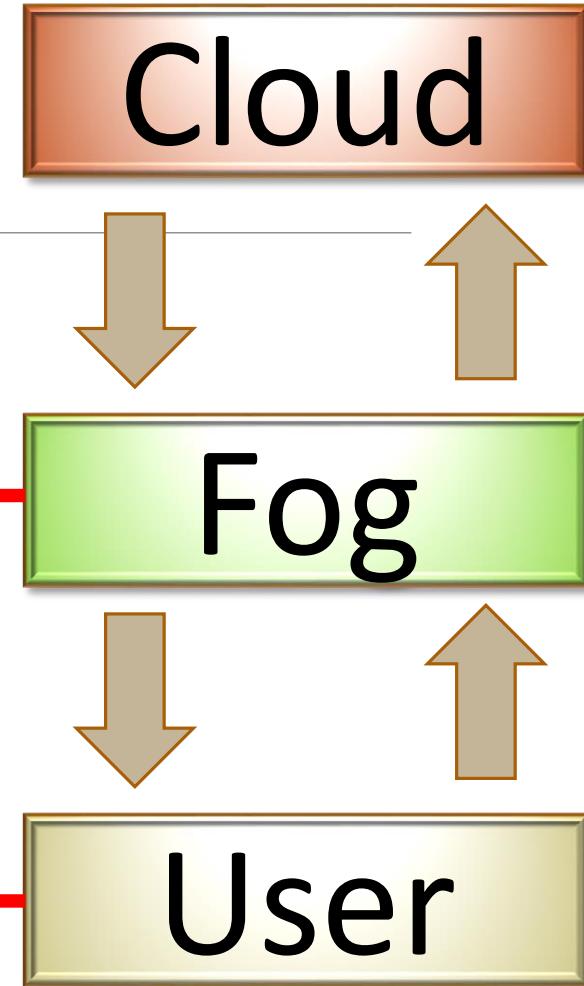
Operation on sensor data closer to end devices

Reduced transmission time

Tradeoff between execution speed
of cloud and fog

Execution of
time-sensitive
data

*“Analyzing data close to the device that collected the data
can make the difference between **averting disaster** and a
cascading system failure.”*



Bandwidth Conservation

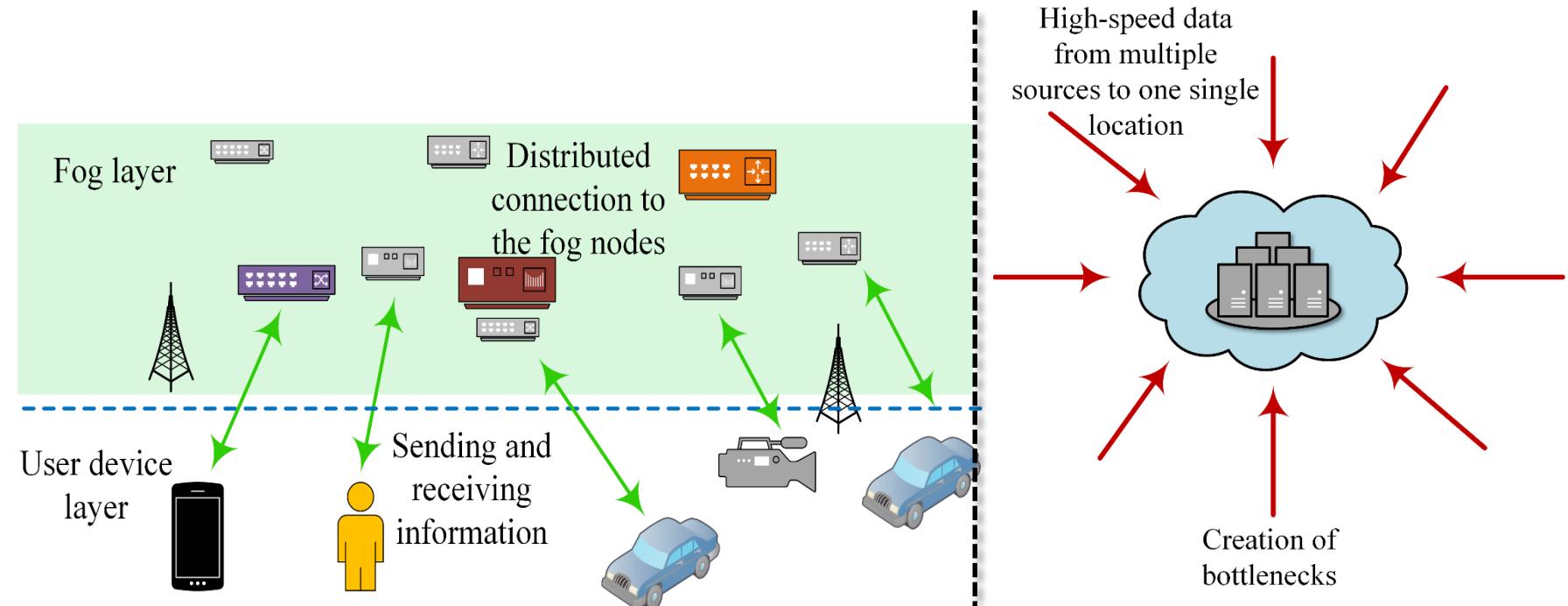
IoT devices generate huge amount of data

Not practical to send everything to the cloud

Not all applications need cloud level processing/storage

Possibility of bottlenecks

Reject/postpone services



Enhanced Security

Data travels through multiple networks to reach the cloud

Spatially, data travels long distances

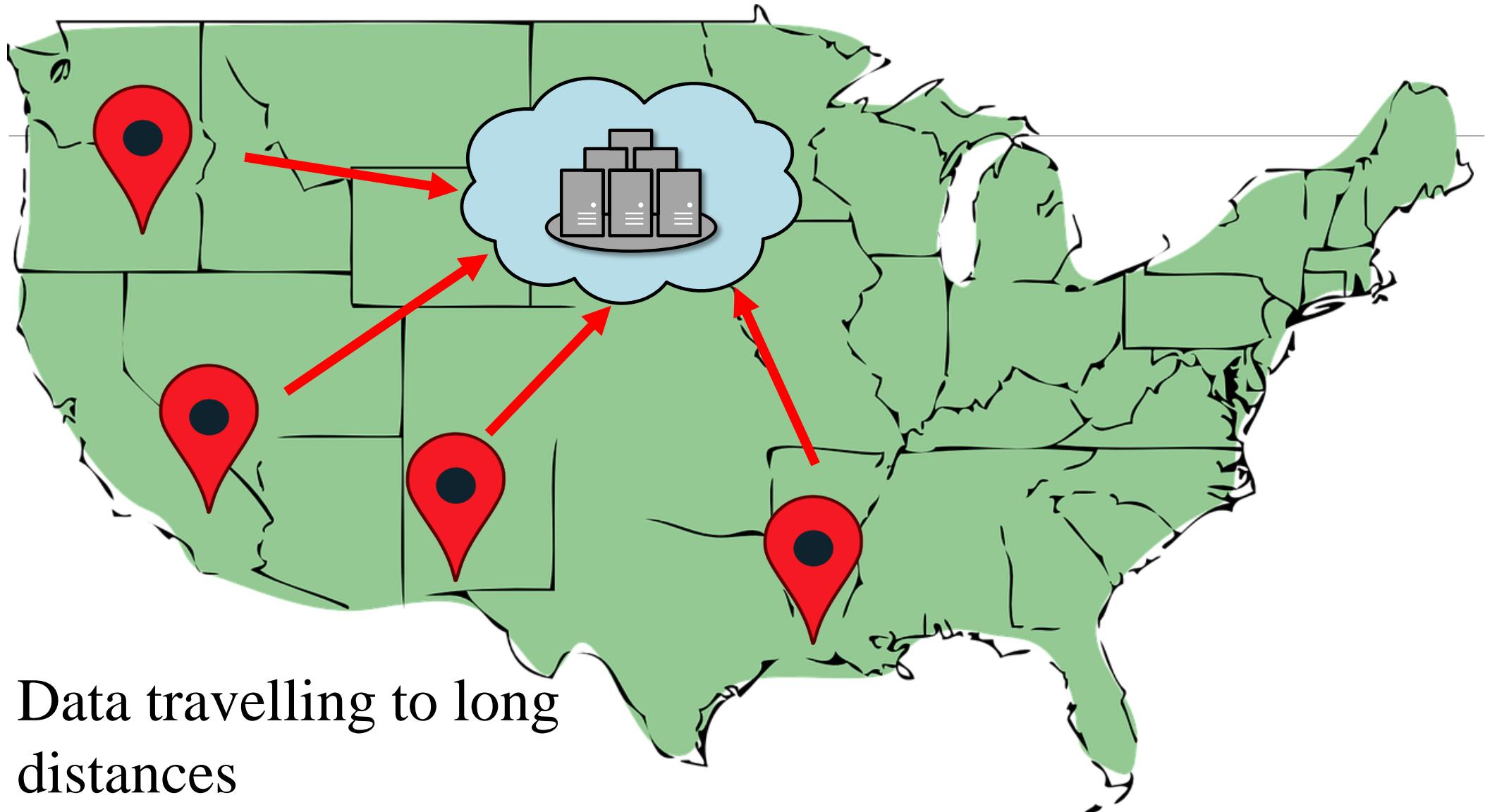
Fog allows local processing

Data does not need to travel far

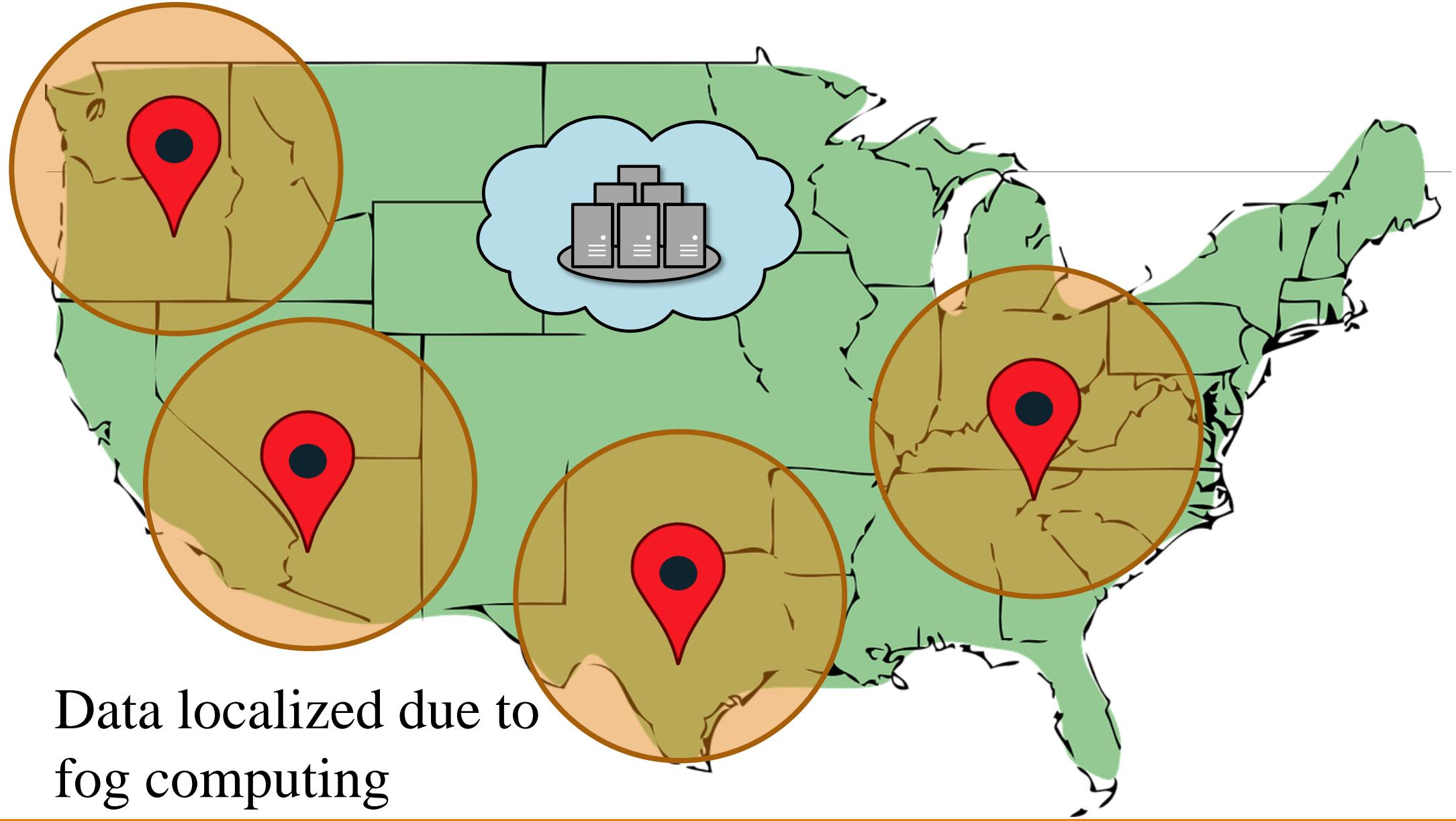
Remains closer to data generating sensor modules

Reduces the possibility of attacks

Limited to local network



Data travelling to long
distances



Data localized due to
fog computing

Other Advantages..

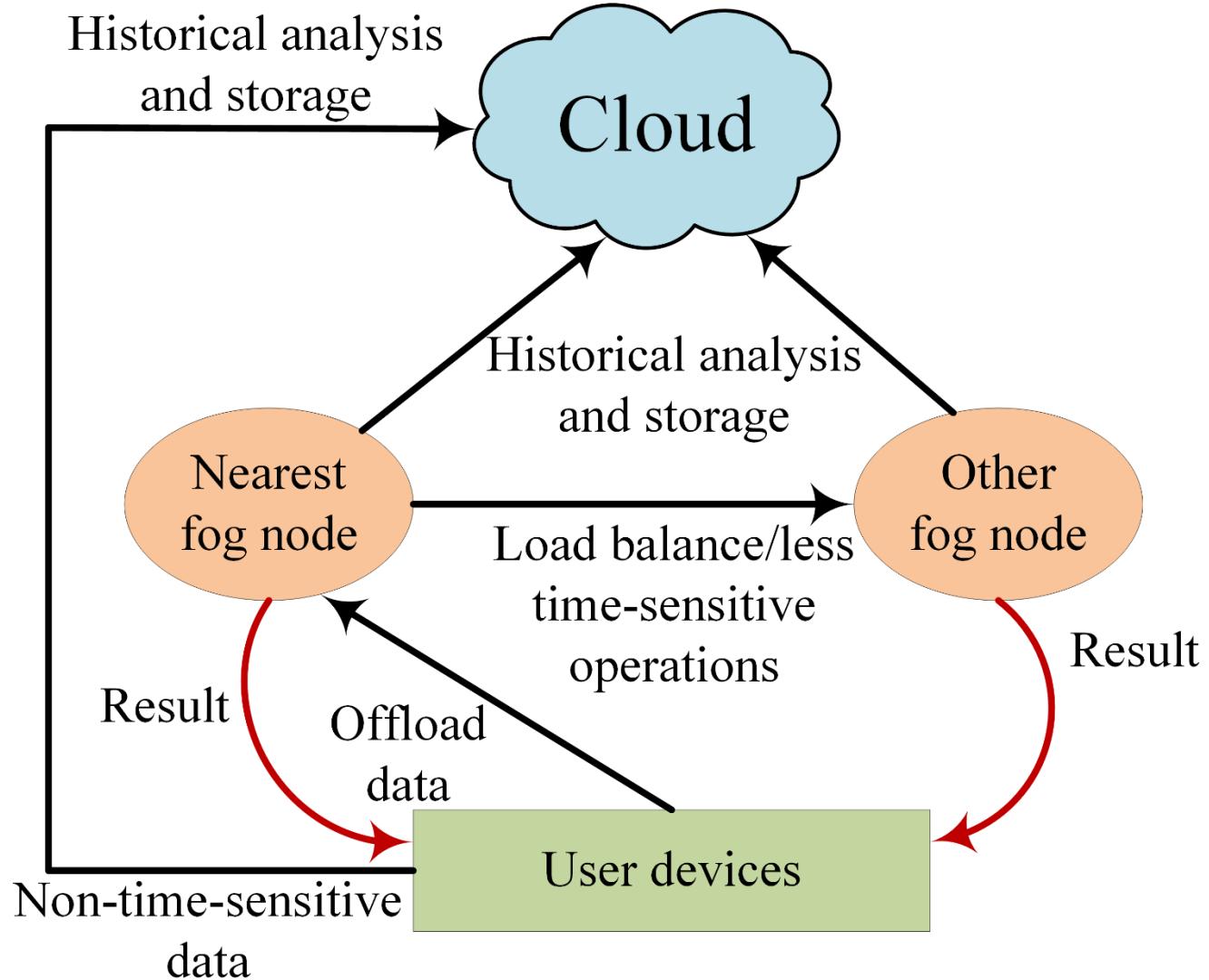
Reliable operations

Spatially aware data

Optimized movement of data

Reduce load from the cloud

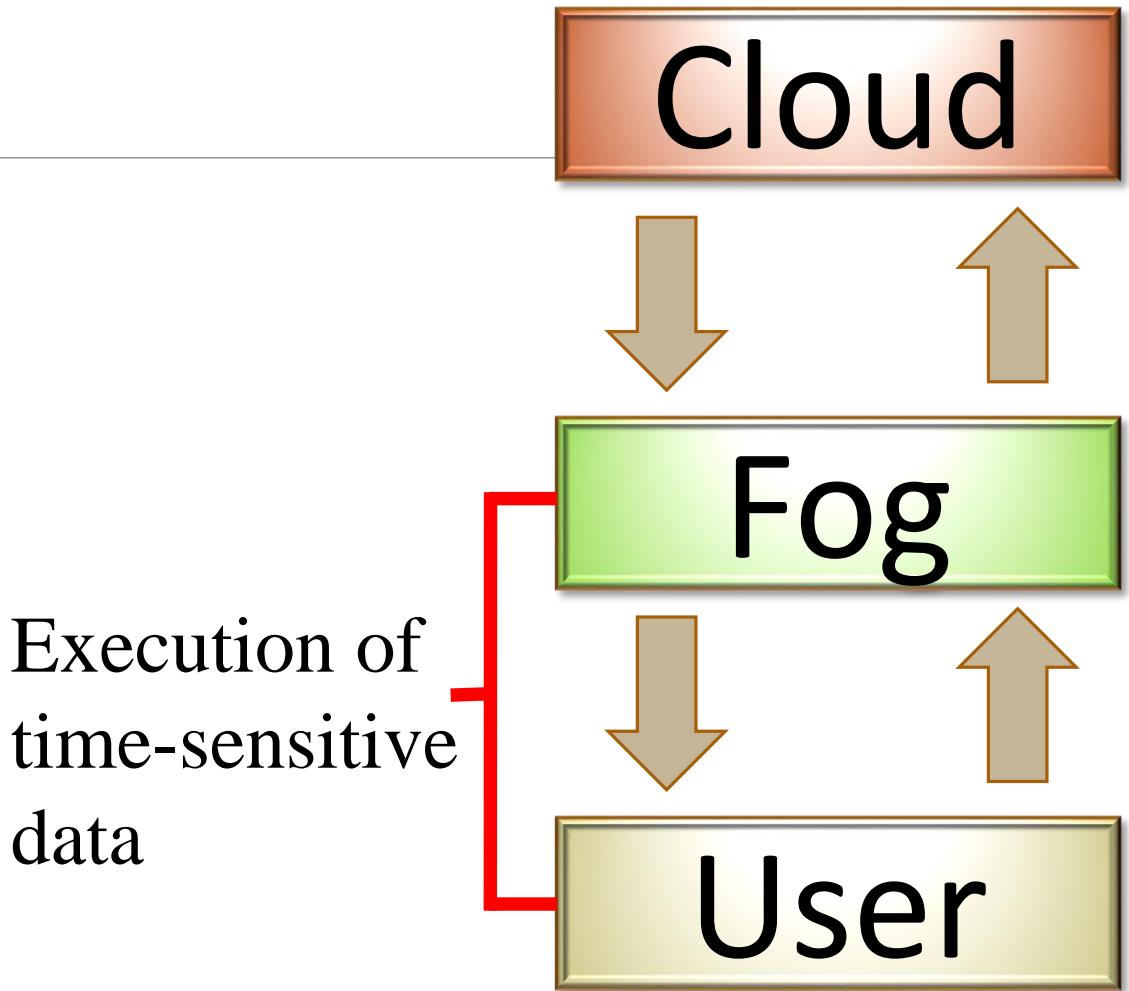
Support mobility



Applications

Real-time health analysis
Intelligent power efficient system
Real-time rail monitoring
Pipeline optimization

Real-time monitoring
Reduced network latency
Close proximity
Reduced operational cost
And others...



Challenges

Power consumption

Data security

Reliability

Fault tolerance

Real-time analysis

Architecture

Upcoming 5G technology

Millimeter waves

Small cells

Massive MIMO

Beamforming

Full Duplex

Upcoming 5G technology

Millimeter waves

Small cells

Massive MIMO

Beamforming

Full Duplex

- Wavelength decreases as the frequency increases
- narrow wavelengths
- Vulnerable against gases, rain and humidity
- Absorption
- Range limited to few kilometers

Upcoming 5G technology

Millimeter waves

Small cells

Massive MIMO

Beamforming

Full Duplex

- Reliable coverage
- Spectral efficiency
- Improved capacity
- Improved overall performance
- High speed

Upcoming 5G technology

Millimeter waves

Small cells

Massive MIMO

Beamforming

Full Duplex

- Increase in number of devices/users
- Diverse services
- Need for efficient task scheduling
- Processing near the data generating devices
- Need for preventing bottlenecks

Upcoming 5G technology

Millimeter waves

Small cells

Massive MIMO

Beamforming

Full Duplex

- Directional signal transmission
- Enhance LoS transmission
- Avoid blockage due to buildings/trees
- Faster
- Reliable

Upcoming 5G technology

Millimeter waves

Small cells

Massive MIMO

Beamforming

Full Duplex

- Typically, MAC schemes used
- TDMA/FDMA/CDMA
- 2-way communication in same channel
- Increased capacity
- Spectral efficiency

Conclusion

Reduces load from the cloud

Brings processing closer to the users/sensors

Increases security

Real-time analysis and monitoring

Complements the services of the cloud

Perfect for upcoming technologies

Thank You



Cloud Computing (CS60118)

(Spring 2020-2021)

Introduction

Dr. Sudip Misra

Professor

Department of Computer Science and Engineering

Indian Institute of Technology Kharagpur

Email: smisra@sit.iitkgp.ernet.in

Website: <http://cse.iitkgp.ac.in/~smisra/>

Research Lab: cse.iitkgp.ac.in/~smisra/swan/

Outline

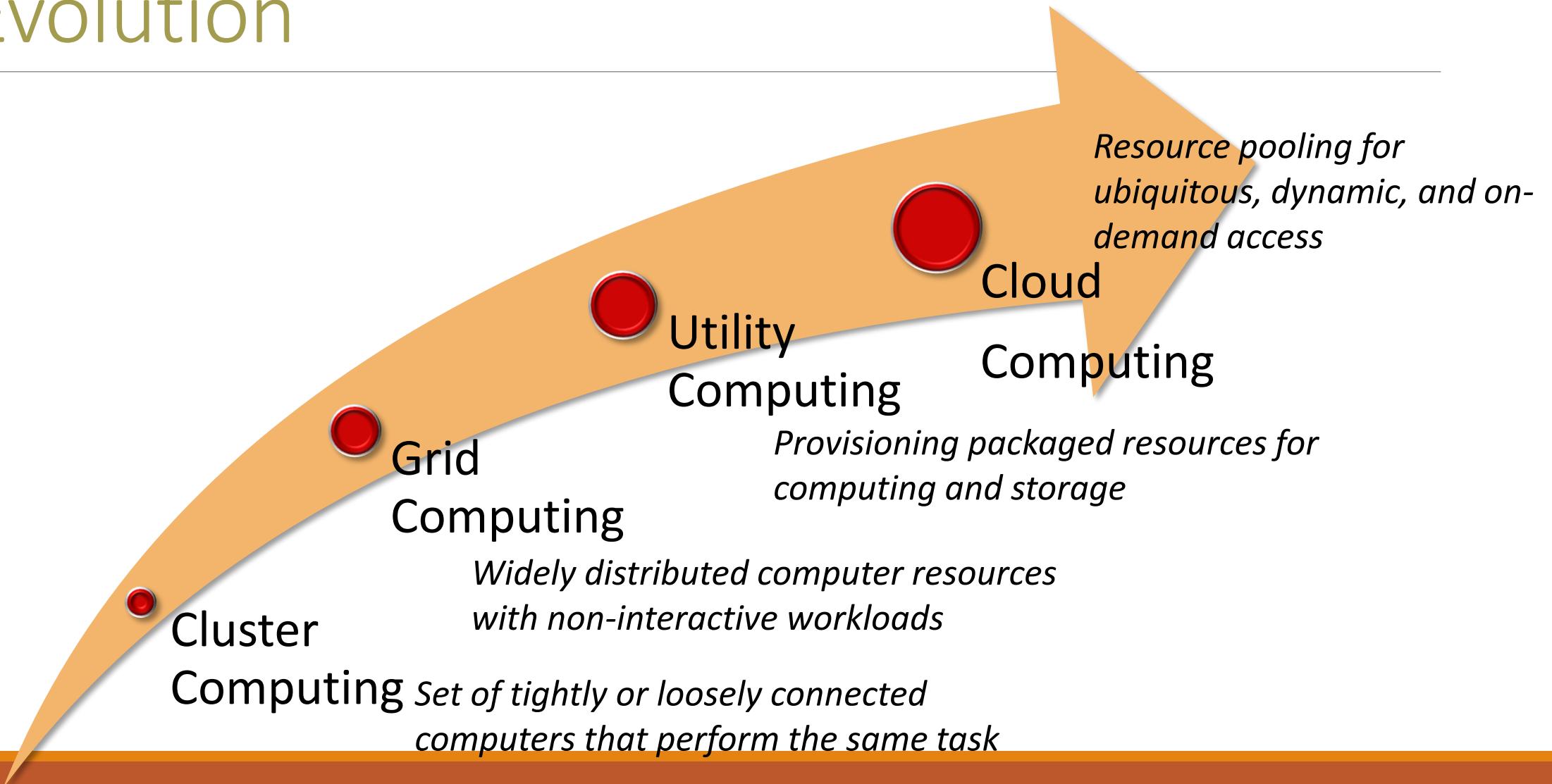
- Introduction to Cloud computing
- Cloud computing architecture and its components
- Service and data management in the cloud
- Federation, Presence, Identity, and Privacy in the Cloud
- Case Studies
- Future directions: Where are we heading?
- Demos

What is Cloud Computing?

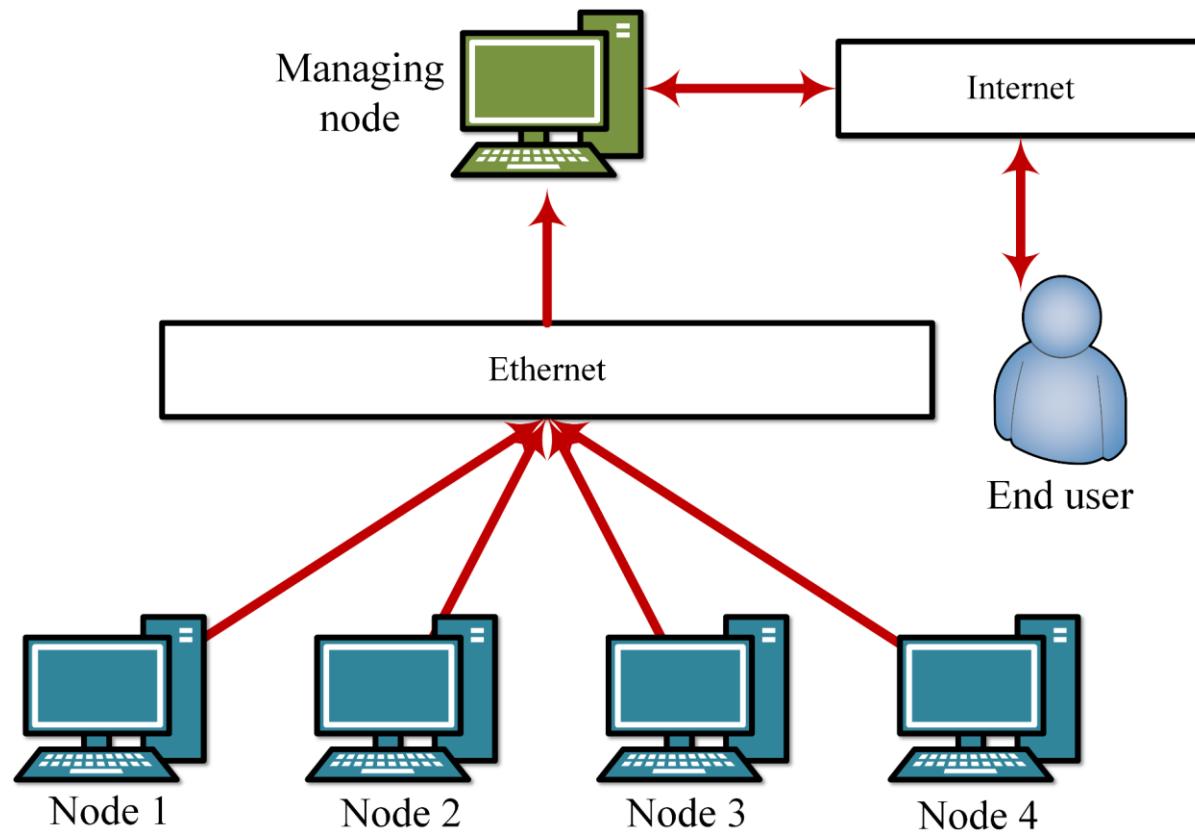
*Cloud computing is a model for enabling **ubiquitous, convenient, on-demand network access** to a **shared pool of configurable computing resources** (e.g., networks, servers, storage, applications, and services) that can be rapidly **provisioned** and **released** with **minimal management effort** or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.*

-NIST

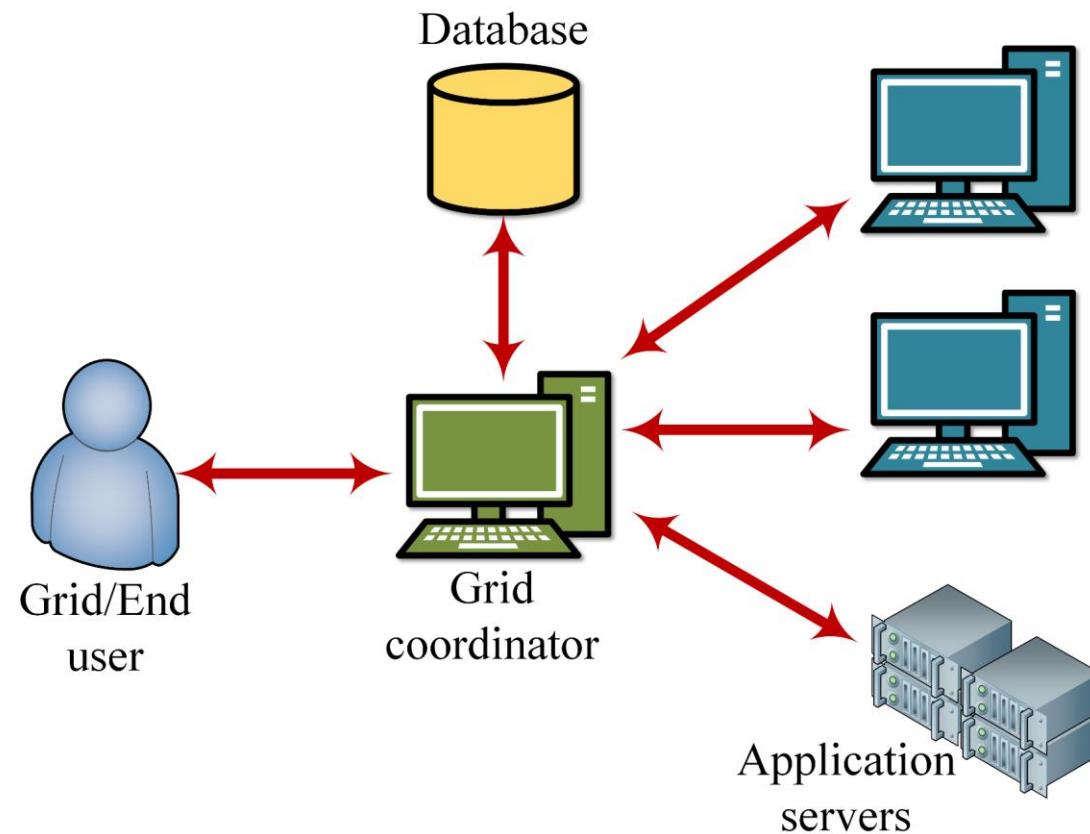
Evolution



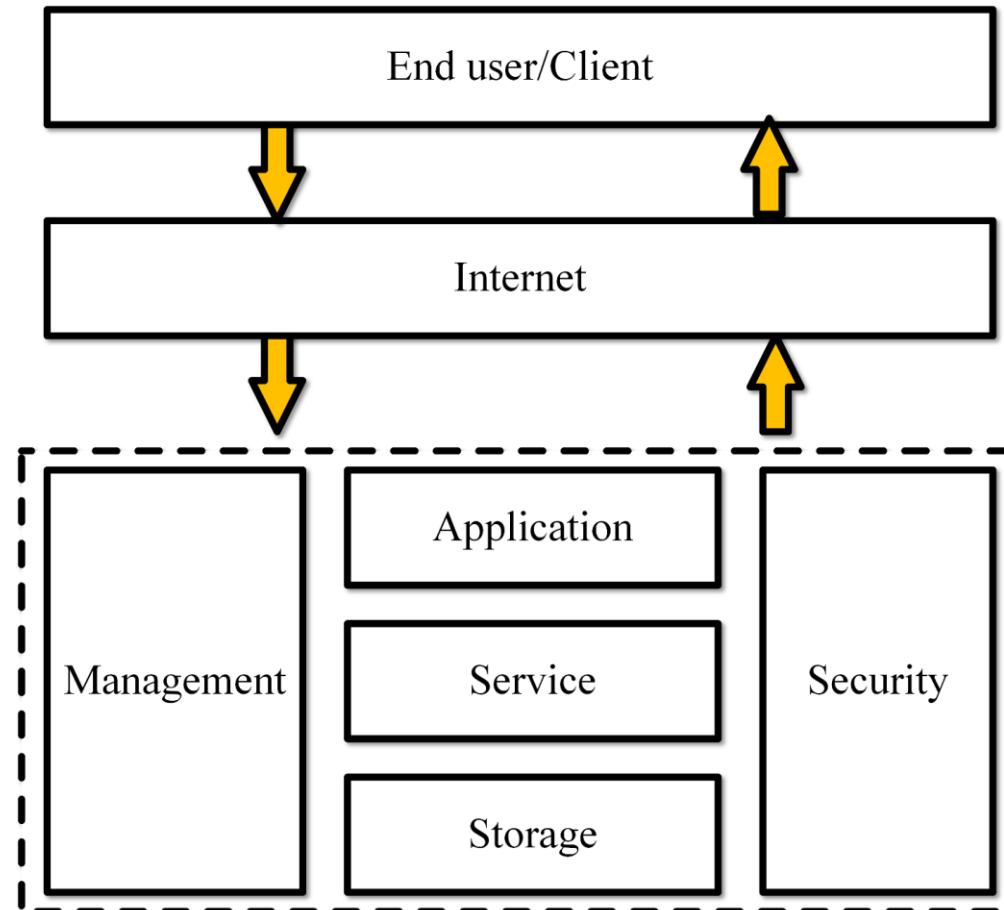
Cluster Computing



Grid Computing



Cloud Computing



Participants

Consumers

- End-users that use the cloud services for personal/business activities.

Service providers

- Cloud providers offering a variety of functions such as infrastructure, applications, tools, and others.

Designers

- Applications and tools builders in the cloud.

General Characteristics

On-demand self-service

- Consumers can provision resources without interacting with service providers.

Broad network access

- Independent (with respect to thin and thick clients) provisioning of resources.

Resource pooling

- grouping together resources for maximizing advantage and minimizing risk to the users.

Rapid elasticity

- Real-time scaling of resources commensurate with demand.

Measured service

- Metering the resource usage for billing.

Essential Characteristics

Broad network access

- Cloud resources should be available over the network
- Should support standard mechanisms for information retrieval using traditional interfaces
- Supported clients: Heterogeneous Thin and Thick clients

Thin Client

Features

- Stateless
- Fanless desktop terminal
- No hard drive

Example: Virtual desktops

Highly dependent on central server (due to lack of localized hard drive)

Reliable connections are important

Advantages:

- Reduced cost
- Increased security
- Scalable and easily manageable

Thick Client

Opposite of thin clients

Full-featured computers connected to a network

They are functional whether connected to the network or not

Servers provide program/codes which are not present in the memory

Example: Personal computers, laptops, etc

Disadvantages in comparison to thin clients:

- Difficult to secure and manage
- Costlier to deploy
- High energy consumption

Essential Characteristics Contd.

Rapid Elasticity

- Rapid, elastic, and automated allocation of cloud resources
- Dynamic allocation/release for scale-out and scale-in
- Customers should feel infinite resources

Measured service

- Resource usage should be recorded and monitored
- Facility to dynamically control and optimize the resource usage
- Transparency between the service provider and consumer

Essential Characteristics Contd.

On-demand self-service

- Automatic provision of server time and network storage
- Self-service

Resource pooling

- Automated pooling of all available resources
- Serve multiple end users using a multi-tenant model
- Allocation of resources according to user demand

Difference between Cloud and Cluster Computing

Cloud Computing	Cluster Computing
Heterogeneous resources	Homogeneous resources
Support for virtualization	No support for virtualization
Very low capex	Very high capex
Low security requirement	High security requirement
Low maintenance	Relatively high maintenance
Support for multiple OS simultaneously	Support for singular OS
Centralized and decentralized management	Centralized management
High scalability	Low scalability
Dynamic resource allotment	Tightly coupled resources
Application domain independent software provisioning	Application domain dependent software provisioning

Difference between Cloud and Grid Computing

Cloud Computing	Grid Computing
Client-server architecture	Distributed architecture
Centralized resource usage	Distributed resource usage
Highly flexible	Flexibility is low
Payment according to usage	Does not support pay-per-use
High accessibility	Low accessibility
Support for multiple OS simultaneously	Support for singular OS
Centralized and decentralized management	Centralized management
High scalability	Low scalability
Middleware independent	Requires grid computing middleware

Mainframe Computing

First came into existence in 1951

Highly powerful and reliable computing machines

Massive input-output operations

High fault tolerance

Cluster computing is a replacement for mainframe computing

Components of the Cloud

Clients/end-users: Thin and thick clients (mobile and stationary)

Services: Products and solutions

Applications: Web Apps, SaaS, etc

Platform: Apps/Web hosting using PaaS

Storage: Database, Data Storage-as-a-Service (DSaaS)

Infrastructure: Virtualization, IaaS, EC2

Clients/end-users

Services

Applications

Platform

Storage

Infrastructure

Everyone Uses Cloud

For instance, ***Google's Gmail service***, we are all using a cloud email service.

Anything that can be served as a service-

- Compute power to computing infrastructure
- Applications and business processes

Only two constraints:

- Common standardization
- Automation.

Standardization

Consistent service delivery using consistent interfaces

Necessary both before and after deployment

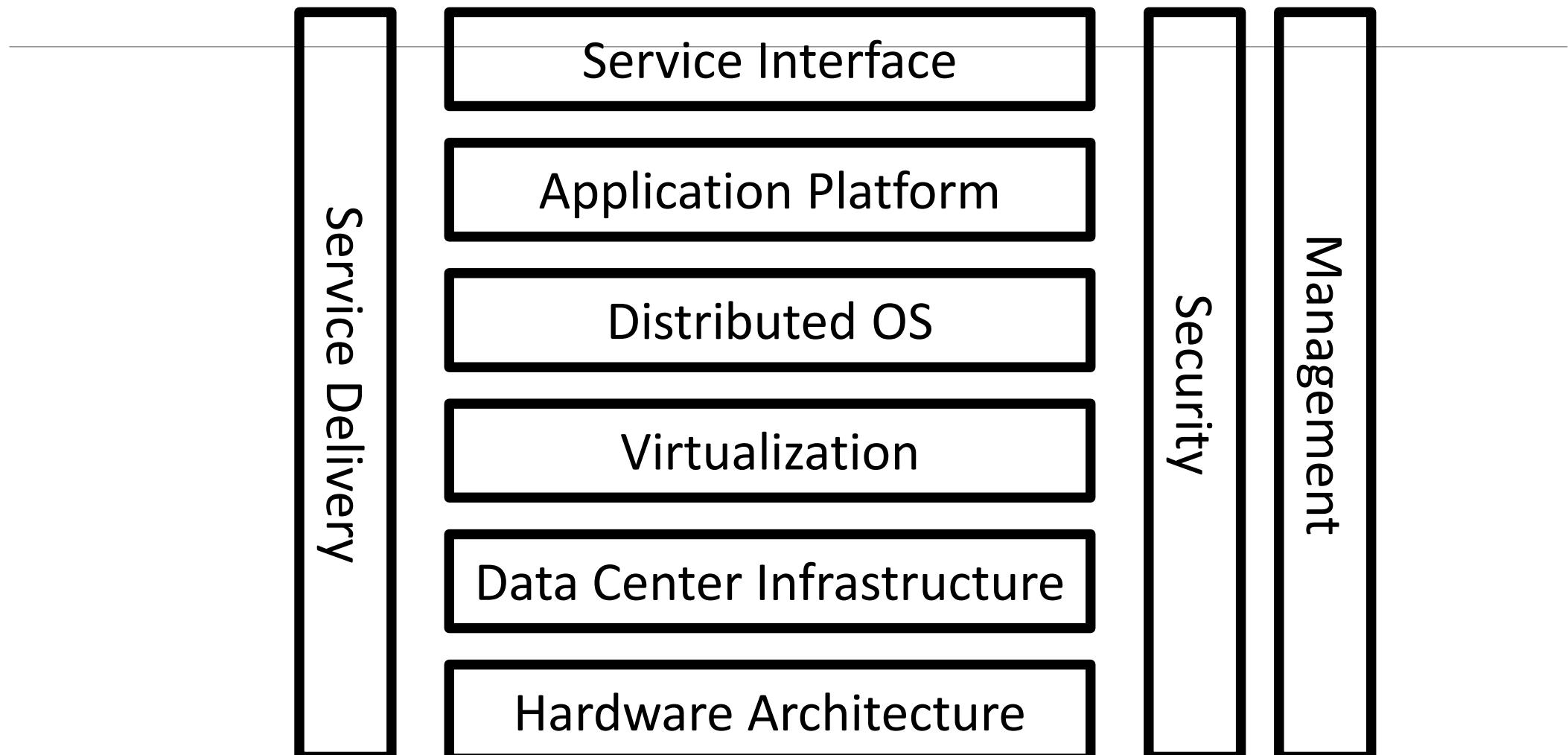
Main areas for standardization:

- Service calling
- Service interfaces
- Resource and network management

Typically, 6 layers need standardization

Motive: Scalability, interoperability, and security in the cloud

Standardization Layers



Automation

Self-service provisioning model

Reduce manual intervention for:

- Provisioning
- Configuring
- Managing cloud environments

For instance, automation ensures returning the resources to the resource pool after a provisioned service is exhausted

Facilitates capacity planning and overall workload management

Advantages of Automation

Improved security and resilience

- Reduction of human errors and malicious insiders

Improved backup processes

- Improves an organization's resilience to disaster

Improved governance

- Improved control over infrastructure

*Note: Automation and orchestration are different concepts. **Orchestration** deals with the scheduling and integration of automated tasks across heterogeneous systems. It is the step after achieving automation.*

Deployment Models

Public cloud

- Resources owned and operated by third parties.
- Allow usage other companies/customers.

Private cloud

- Resources owned and operated by the company/organization.
- Used behind a firewall.

Hybrid

- Combination of private and public clouds.

Multi-cloud

- Organization using two or more public clouds.

Public Cloud

Resources owned and operated by third parties

Usage by organizations/customers

Customers unaware of underlying infrastructure

Third parties offer rich set of services in addition to the resources

- Security
- Specialized infrastructures such as GPU

On-demand delivery of services and resources

Support multi-tenancy

Multi-Tenancy

Multiple applications operate in a shared environment

Logical isolation

A single instance of a software application serves multiple tenants

Tenants = Customers

Tenants have the option of customizing the user interface and operating rules (cannot manipulate application code)

Applicable for both private and public clouds

Improves scalability

Cheaper than single-tenancy

Disadvantages of Multi-Tenancy

Less flexible

Complex architecture compared to single-tenancy

Strict authentication rules (high physical integration among tenants)

May lead to slow response time (if some tenant consumes all resources)

Note: Some public cloud services offer single-tenancy at higher costs. However, networking services may need to be shared.

Private Cloud

Resources owned and operated by an organization

Explicit use by its employees, partners, and customers

Can be owned and operated by third parties too

Private cloud hosted behind firewalls

Automation higher than public clouds

Public cloud vendors often install data centers in the organization's premises

Third parties may own the on premise resources and bill clients

Public Cloud vs Private Cloud

	Public Cloud	Private Cloud
Virtualized Resources	Publicly shared	Privately Shared
Customer Types	Multiple	Limited
Connectivity	Over Internet	Over Internet/private network
Security	Low	High

Hybrid Cloud

Combination of private and public cloud models

Collaborative use of the cloud models to achieve common goals

Combine services

- Computing environment with the following features:
 - Unified
 - Automated
 - Well-managed
 - Transparent to end users

Superior orchestration methods required for operations and deployment

Multicloud

Two or more public clouds are involved

Multicloud may or may not involve private clouds

- Hybrid cloud must have both private and public cloud models

Multicloud helps in better abstraction of activities and services

Corporate Computing: Combination of multiple public services with private clouds and data centers

Note: Not all combinations of public and private clouds mean hybrid cloud computing.

Common Misconceptions

The following does not mean hybrid computing:

- Architectures with public cloud service disconnected with the private cloud and data center
- No movement of data from a company's deployed software to its data center
- Each division/activity is run on mutually exclusive public clouds

The following qualifies as hybrid computing:

- The public deployments sends data to a private cloud or data center
- Each division/activity is run on public clouds and can collaborate among each other
- An organization can move workloads from one public cloud to another on requirement

Other Types of Cloud

Community Cloud

- Shared set-up between several organizations having common concerns (security, compliance, jurisdiction, etc)
- Managed internally or by third party

Distributed Cloud

- Collection of scattered set of computing devices in different locations, however, connected to a single network
- Two types: Public-resource computing and Volunteer cloud

Other Types of Cloud Contd.

Multi-cloud

- Multiple cloud computing services offered via single heterogeneous architecture
- Increases fault-tolerance and flexibility

Inter-cloud

- Unified global ‘cloud of clouds’ based on the Internet
- Supports interoperability between cloud service providers

Comparison of the Deployment Models

	On-premise	Off-premise
Dedicated Access	Private cloud	Hosted private cloud
Shared Access	Community cloud	Public cloud

Business Advantages

Nearly zero cost for upfront infrastructure investment

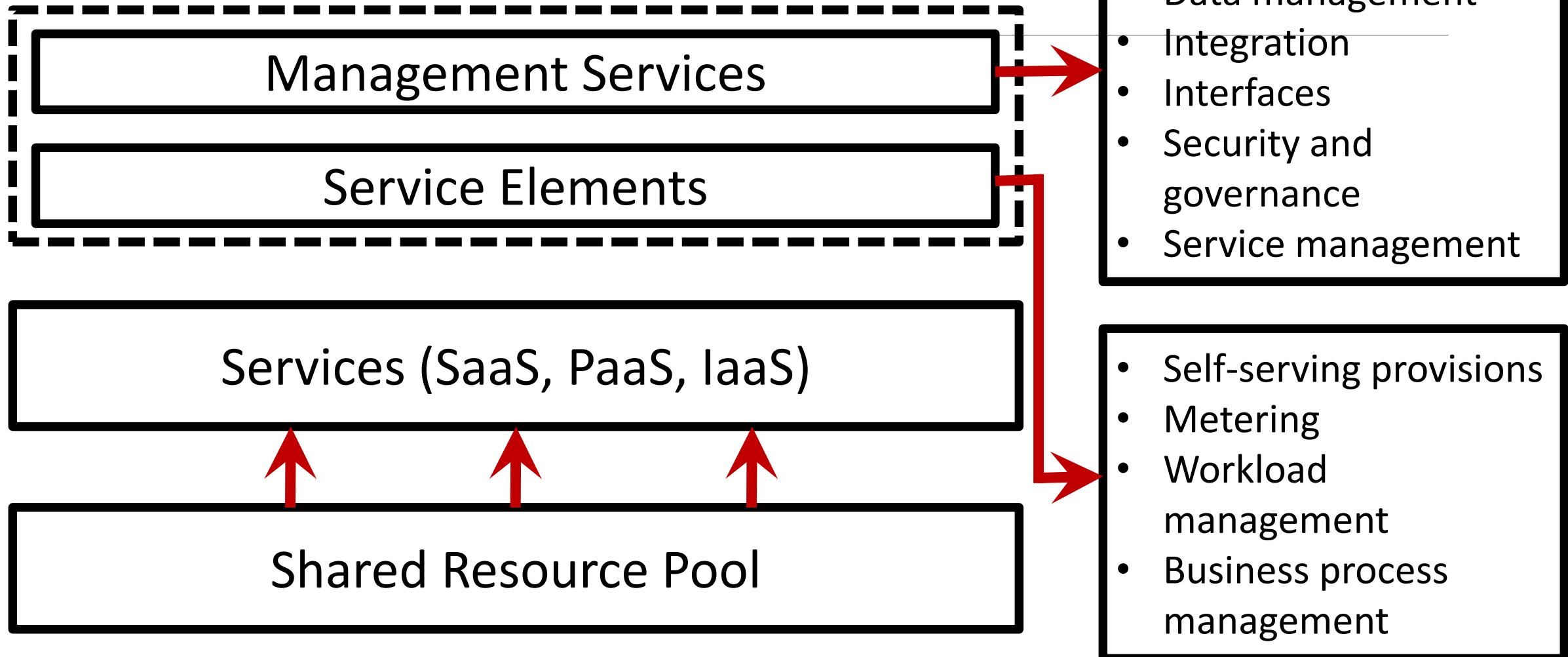
Real-time infrastructure availability

More efficient resource utilization

Usage-based costing

Reduced time to market

Cloud Elements



Service Models

Software-as-a-Service (SaaS)

Platform-as-a-Service (PaaS)

Infrastructure-as-a-Service (IaaS)

Software-as-a-Service (SaaS)

Facility to execute service provider's applications at user's end

Applications are available as 'services'

Services can be accessed via different types of client devices (e.g. web browser, app)

End-users do not possess the control of the cloud infrastructure

Examples: Google Apps, Salesforce, Learn.com.

Platform-as-a-Service (PaaS)

Facility for the consumer to execute consumer-created or acquired applications onto cloud infrastructure

Support for deployment of such applications

The user does not control the cloud infrastructure

User can control the deployed applications using given configurations

Examples: Windows Azure, Google App Engine

Infrastructure-as-a-Service (IaaS)

Facility to access computing resources such as network, storage, and operating system

User can deploy, execute and control any software (Operating systems and other applications)

In some case, the user can control selected networking components (e.g., host firewalls).

Examples: Amazon EC2, GoGrid, iLand, Rackspace Cloud Servers.

Difference Between the Service Models

IaaS	PaaS	SaaS
Resources/Infrastructure for storage and development	Platforms and tools to create, test, and deploy applications and software.	Web applications
Virtual machines, virtual storage, etc.	Integrated Development Environments (IDEs)	Developed Softwares
It is used by network architects.	It is used by developers.	It is used by end users.

Resource Life Cycle in the Cloud

Intuition: Customers/end users consume resources only when needed

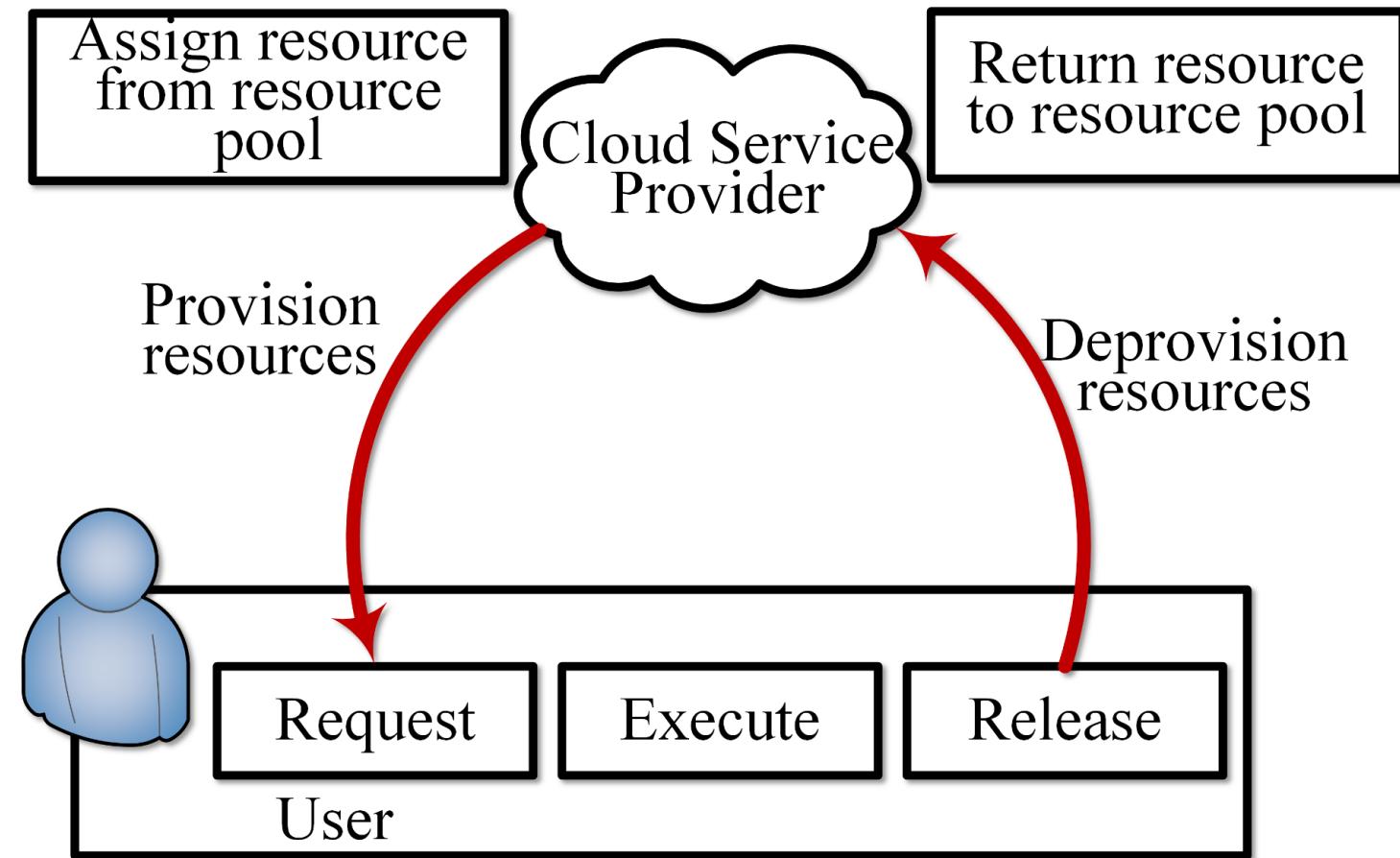
They are charged only when they are using the resources (measured)

Analogous to *renting*

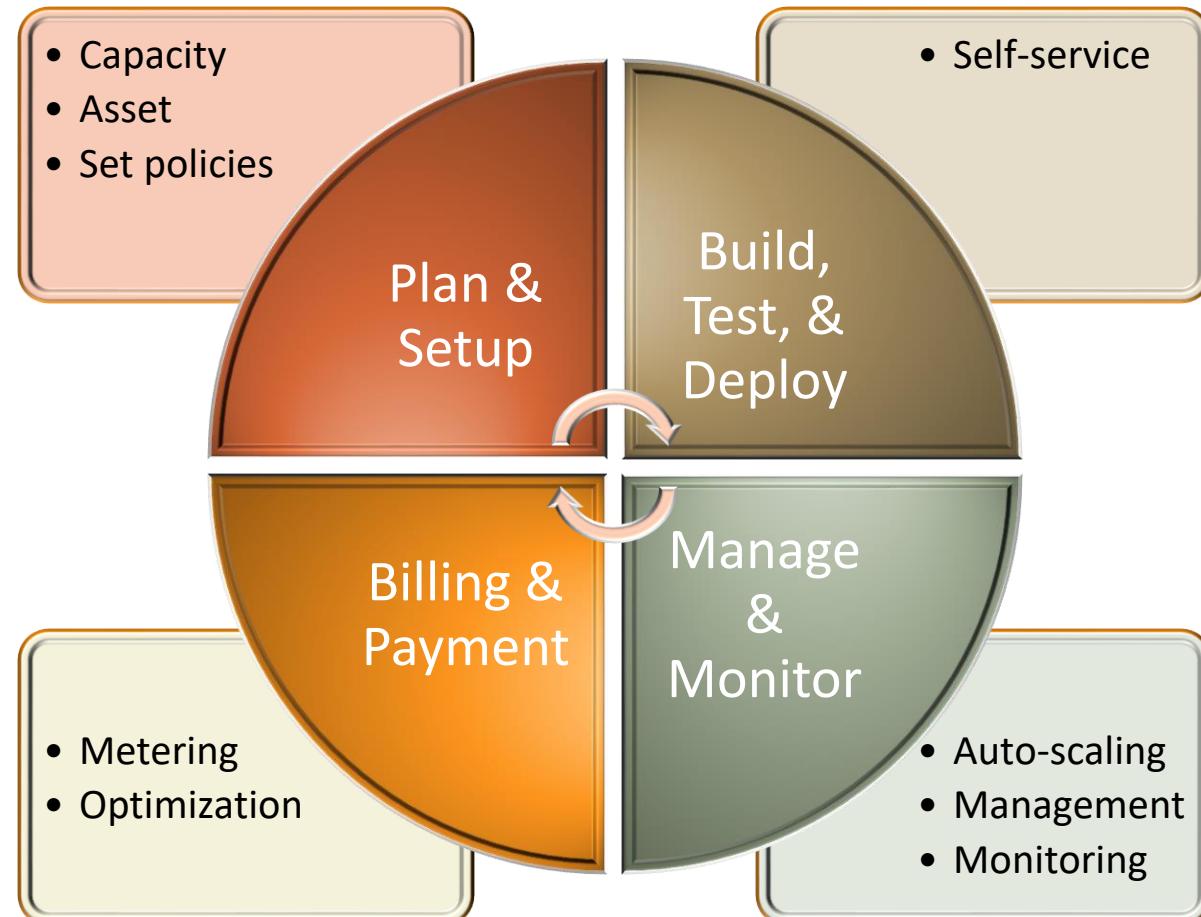
Cloud design considerations:

- Respond immediately on receiving customer requests
- Ensure resource availability at all times
- Return assigned resources back to the resource pool after usage by the customers

Resource Life Cycle Management



Cloud Life Cycle Management



Self-Service

Important feature of cloud computing

Website acts as an interface for the customers for:

- Select and purchase cloud services
- Modify service configurations
- Launch the service

Start using the purchased resource and service within seconds of deployment

No Self-Service in Traditional Data Centers

Customer needs to:

- File an application for the resources
- Concerned personnel verify and approve the application
- Concerned personnel install and launch the requested configurations
- No elasticity
- Handover of the deployed system to the customer
- Customer waits until approval (days/weeks)

Elasticity

Cloud resources change their original/provisioned configurations

Automatic increase and decrease in resource allotment

Example:

- Storage service
- Customer may start with low space
- Increase capacity on reaching limit
- Shrink capacity on deleting files
- Pay-per-use

Elasticity benefits both customers and service providers

Workload

Atomic service/program routine

Executable

Cloud is a collection of workloads

Organization between the workloads is important

Issues:

- Localizing workloads and data near each other
- Optimize performance
- Cloud strategy

Management Services

Maintain consistent quality of service

Irrespective of cloud deployment and service models

Resistance to outages and slow networks

Ensure overall security (to all participants)

Data management in hybrid and multicloud environments

THANK YOU



Cloud Computing (CS60118)

(Spring 2020-2021)

Cloud Architecture & Components

Dr. Sudip Misra

Professor

Department of Computer Science and Engineering

Indian Institute of Technology Kharagpur

Email: smisra@sit.iitkgp.ernet.in

Website: <http://cse.iitkgp.ac.in/~smisra/>

Research Lab: cse.iitkgp.ac.in/~smisra/swan/

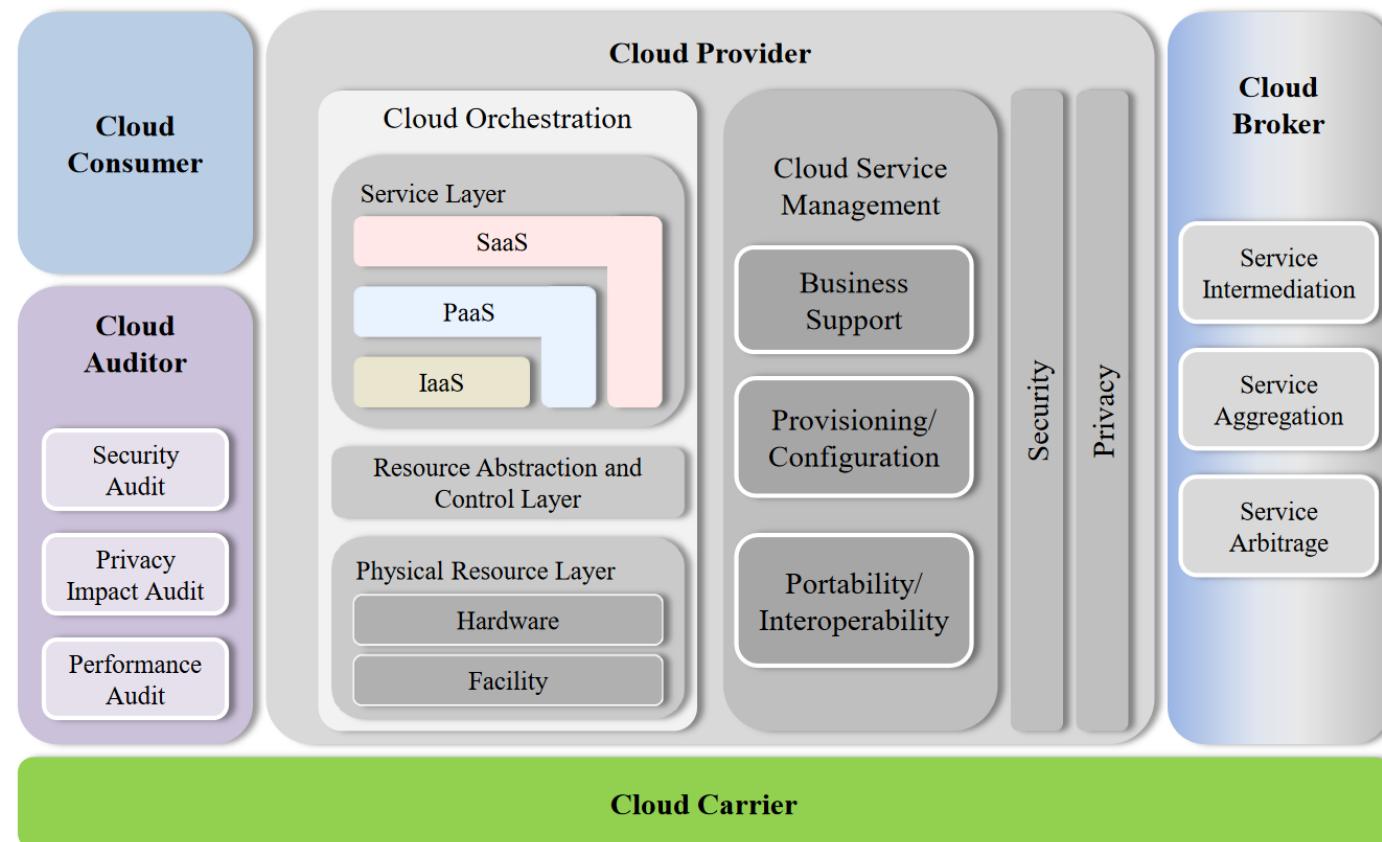
Contents

- The NIST cloud reference architecture
- Components of Cloud Architecture
- Anything/Everything as a Service (XaaS)
 - IaaS
 - PaaS
 - SaaS
- Microservices

Cloud Computing: The Architecture

- Multiple components
- Broad classification
 - Front end
 - Back end
- Front end takes care of the connection with the end-user or the clients
- Back end is used by the service provider for managing the services and infrastructure.

NIST Architecture



Source: R. B. Bohn, J. Messina, F. Liu, J. Tong and J. Mao, "NIST Cloud Computing Reference Architecture," 2011 IEEE World Congress on Services, Washington, DC, 2011, pp. 594-596, doi: 10.1109/SERVICES.2011.105.

NIST Architecture

The **National Institute of Standards and Technology's** definition of cloud computing identifies "five essential characteristics":

➤ ***On-demand self-service***

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

➤ ***Broad network access***

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Source: R. B. Bohn, J. Messina, F. Liu, J. Tong and J. Mao, "NIST Cloud Computing Reference Architecture," 2011 IEEE World Congress on Services, Washington, DC, 2011, pp. 594-596, doi: 10.1109/SERVICES.2011.105.

NIST Architecture

➤ ***Resource pooling***

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

➤ ***Rapid elasticity***

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

Source: R. B. Bohn, J. Messina, F. Liu, J. Tong and J. Mao, "NIST Cloud Computing Reference Architecture," 2011 IEEE World Congress on Services, Washington, DC, 2011, pp. 594-596, doi: 10.1109/SERVICES.2011.105.

NIST Architecture

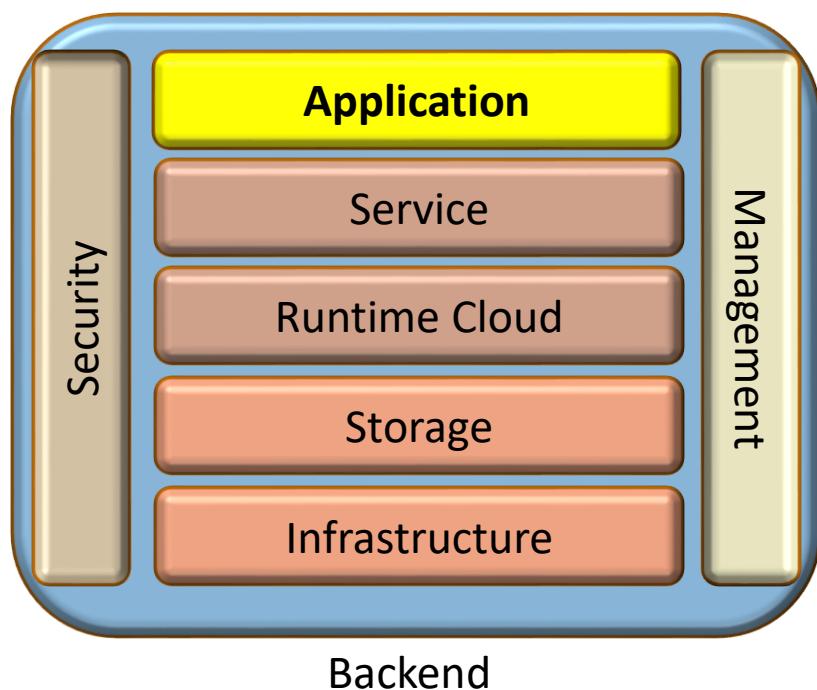
➤ ***Measured service***

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

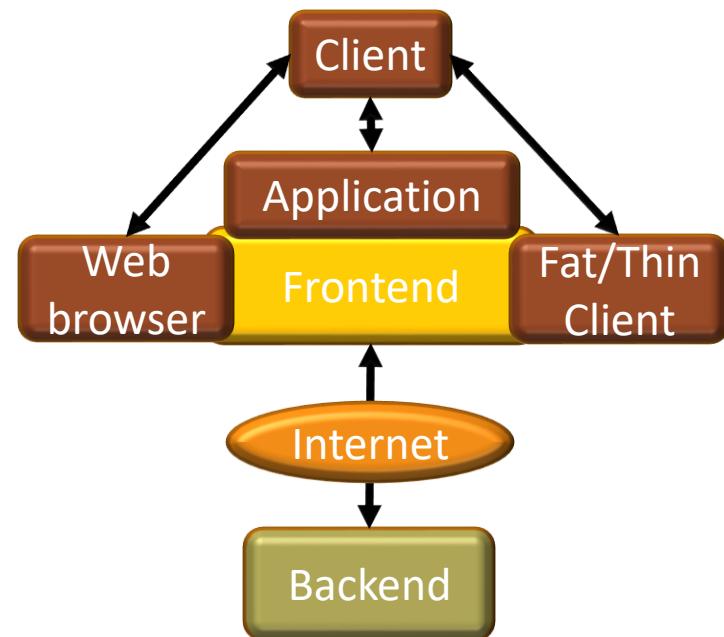
Source: R. B. Bohn, J. Messina, F. Liu, J. Tong and J. Mao, "NIST Cloud Computing Reference Architecture," 2011 IEEE World Congress on Services, Washington, DC, 2011, pp. 594-596, doi: 10.1109/SERVICES.2011.105.

Components

➤ Backend

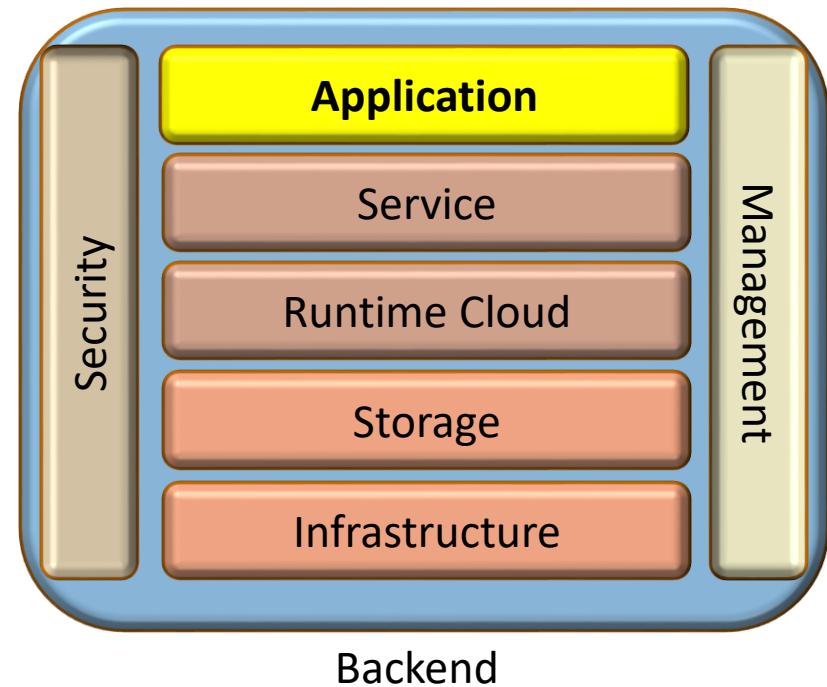


➤ Frontend



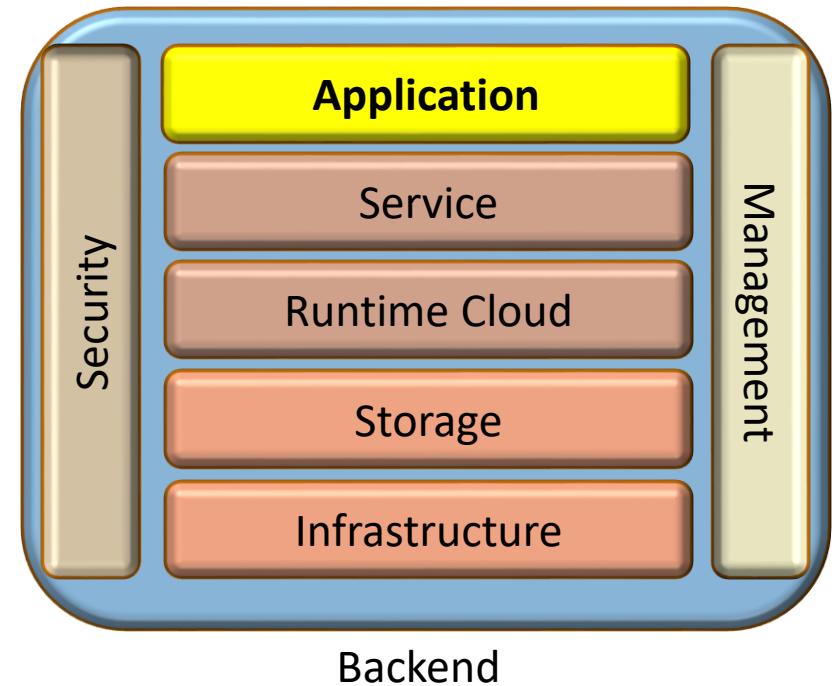
Backend: Components

- Application
- Storage
- Service
- Runtime Cloud
- Management
- Security
- Infrastructure



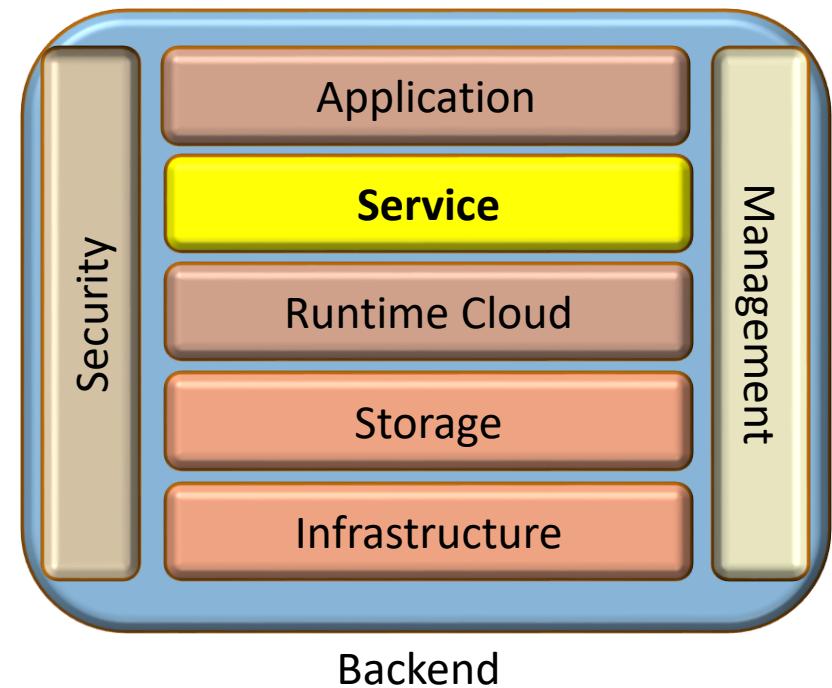
Application

- User Interface for the backend
- Used by the client to interact with the backend services, databases, and manage the client's requests.
- It may be any kind of software that the client wants to access.



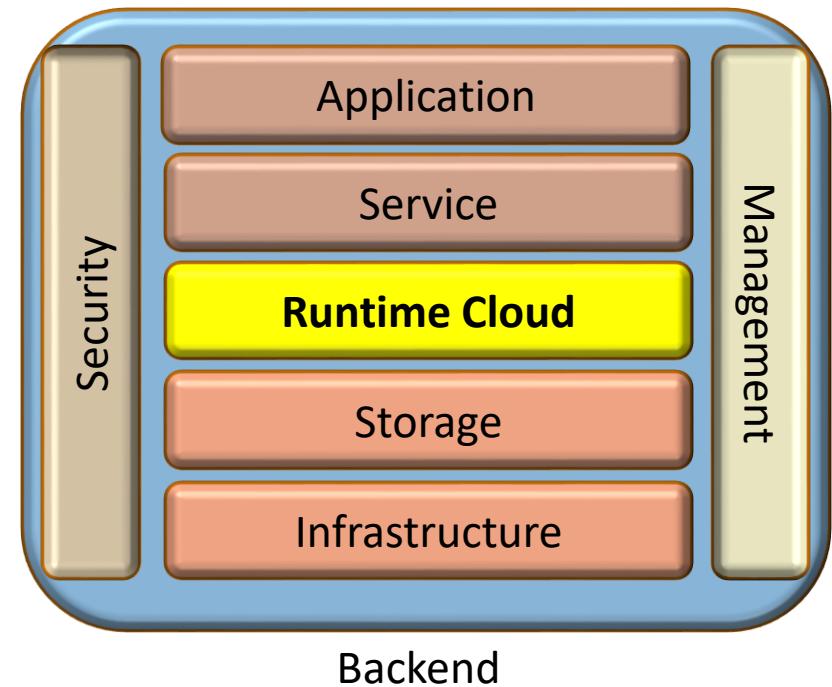
Service

- Services consists of different type of service that has to accessed as per the requirement of the client.
- The services are primarily classified as-
 - Platform as a Service
 - Software as a Service
 - Infrastructure as a Service



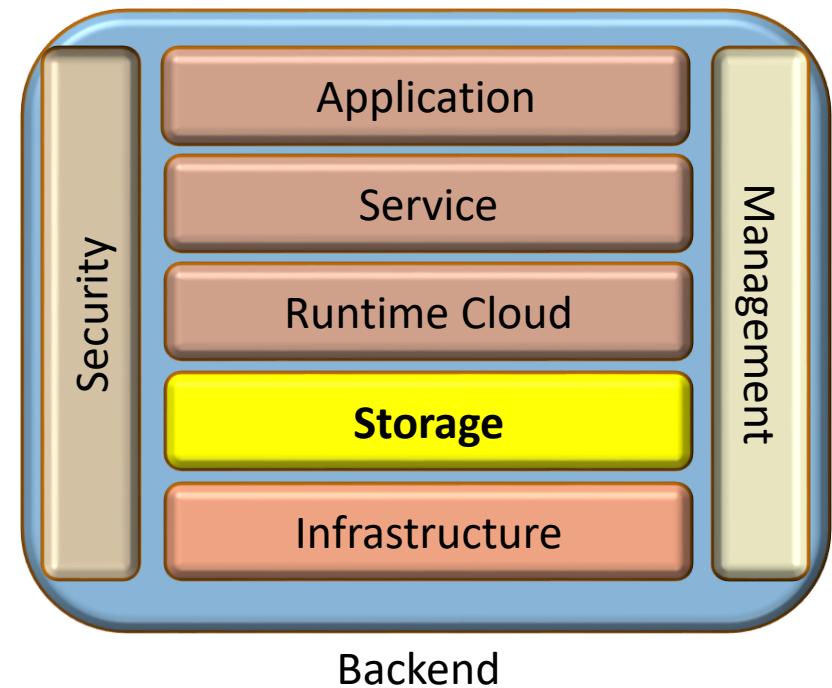
Runtime Cloud

- Manages the execution of programs in virtual machines
- Manages runtime environment and instances of virtual machines



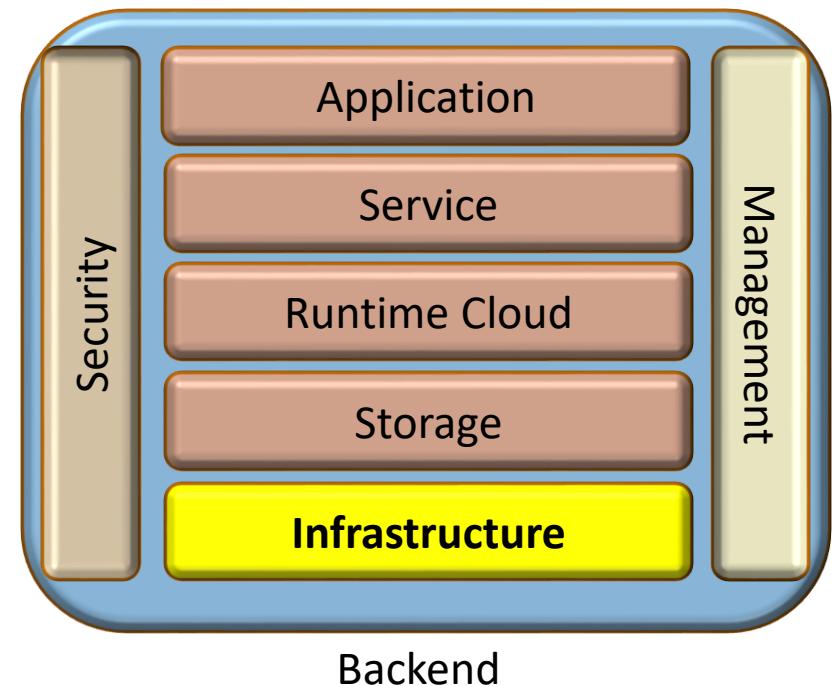
Storage

- Provides large storage capacity for client data
- Enables complex data analytics
- Supports computationally intensive tasks



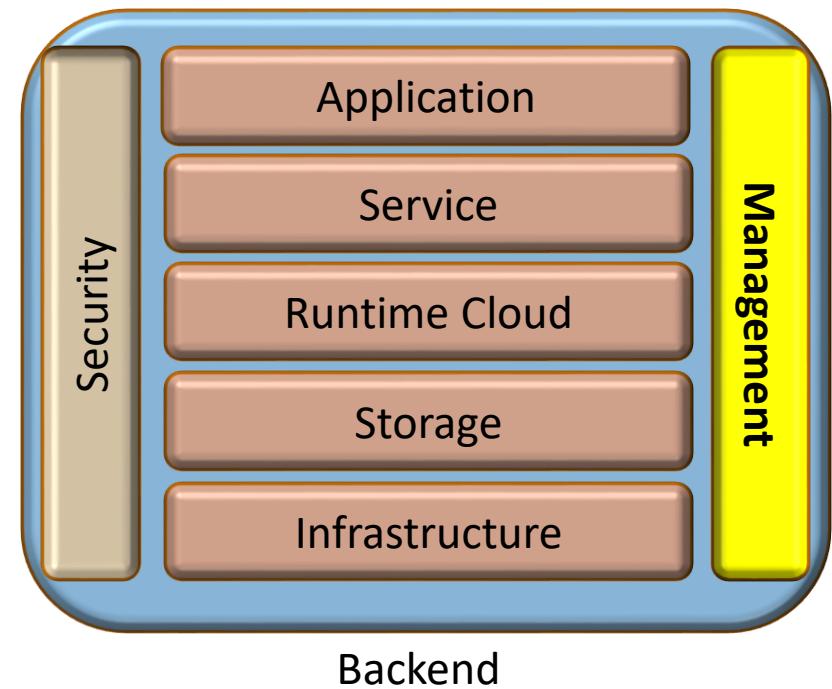
Infrastructure

- Responsible for providing services at 3 different levels-
 - Host level
 - Application level
 - Network level
- Infrastructure consists of-
 - Software components such as virtualization software
 - Hardware components such as network devices, servers, and storage facilities



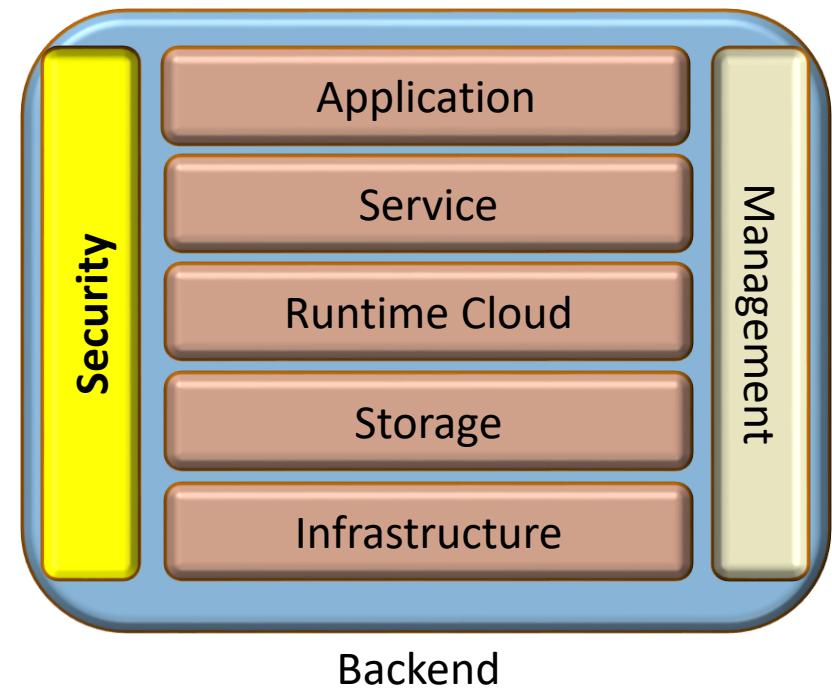
Management

- Coordinates between different components of the backend
- Manages the cloud environment
- Manages the resources in the backend and orchestrate the workflow
- Manages workload distribution
- Implement security



Security

- This is a dedicated inbuilt component of the cloud backend
- Set of policies, rules, applications, and control mechanisms to enhance the privacy and security of the cloud infrastructure and services.

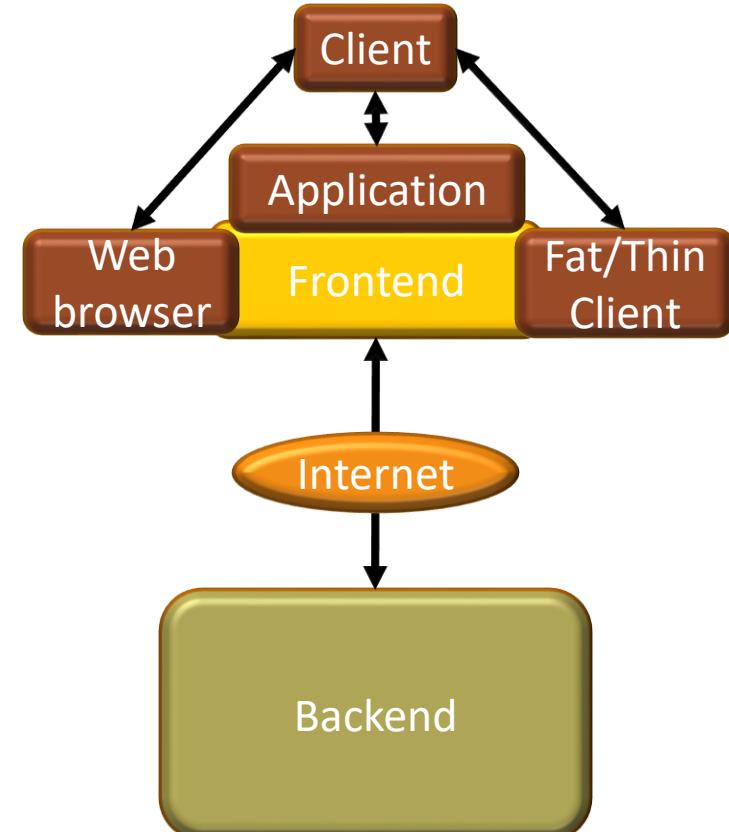


Front end: Components

- User Application
- User Interface
- Web Servers
- Thin Client
- Fat Client

Front end

- User interface
- Client side web applications
- Web browsers
- Web servers



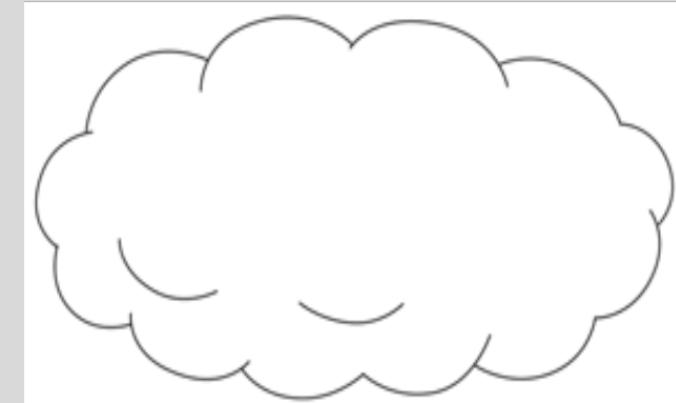
Cloud Actors

- Cloud Consumer
- Cloud Auditor
- Cloud Provider
- Cloud Broker
- Cloud Carrier

Cloud Consumer
Person or organization
that maintains a
business relationship
with, and uses service
from *Cloud Providers*.

Cloud Auditor
A party that can conduct
independent assessment
of cloud services,
information system
operations, performance
and security of the cloud
implementation.

Cloud Provider
Person, organization or entity responsible for making a service
available to *Cloud Consumers*.



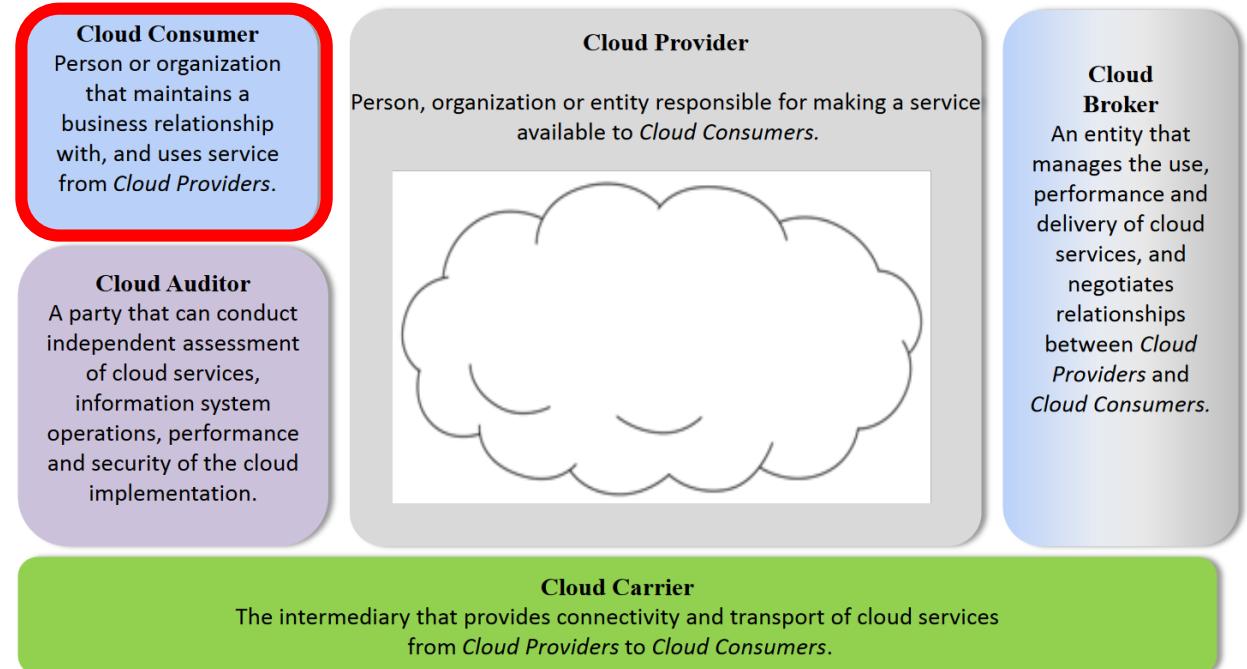
Cloud Broker
An entity that
manages the use,
performance and
delivery of cloud
services, and
negotiates
relationships
between *Cloud
Providers* and
Cloud Consumers.

Cloud Carrier
The intermediary that provides connectivity and transport of cloud services
from *Cloud Providers* to *Cloud Consumers*.

Source:

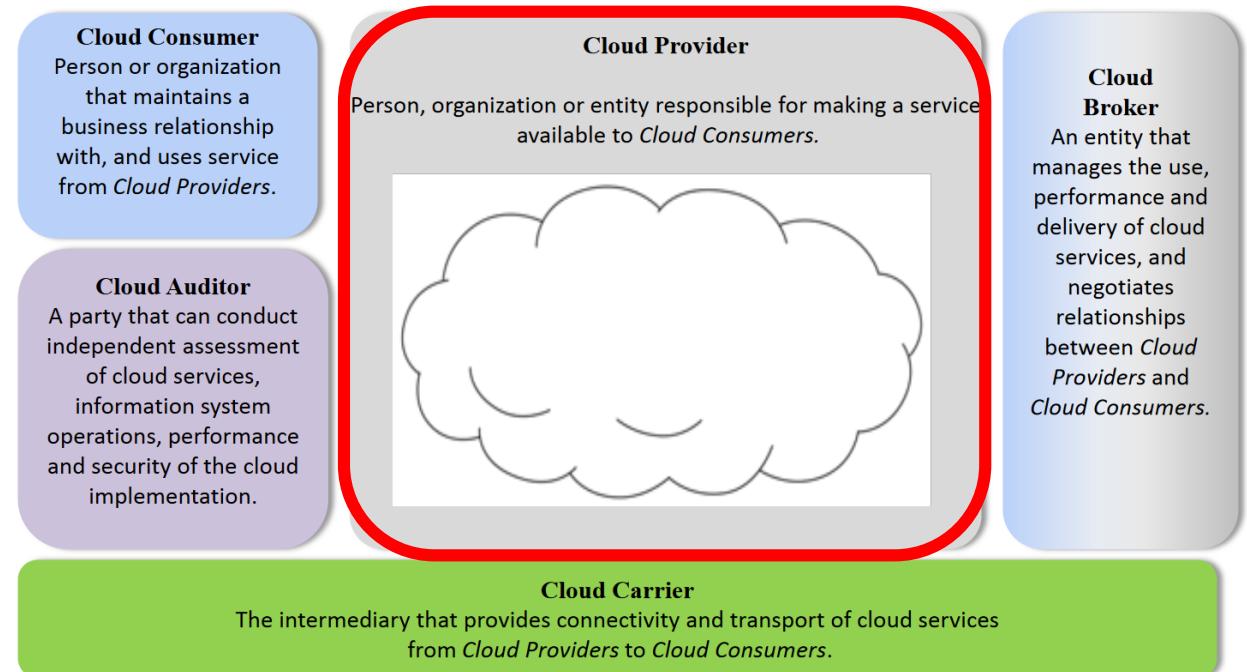
Cloud Consumer

- Primary stakeholder in the cloud computing services
- It may represent a person or an organization
- A cloud consumer uses the services of the cloud



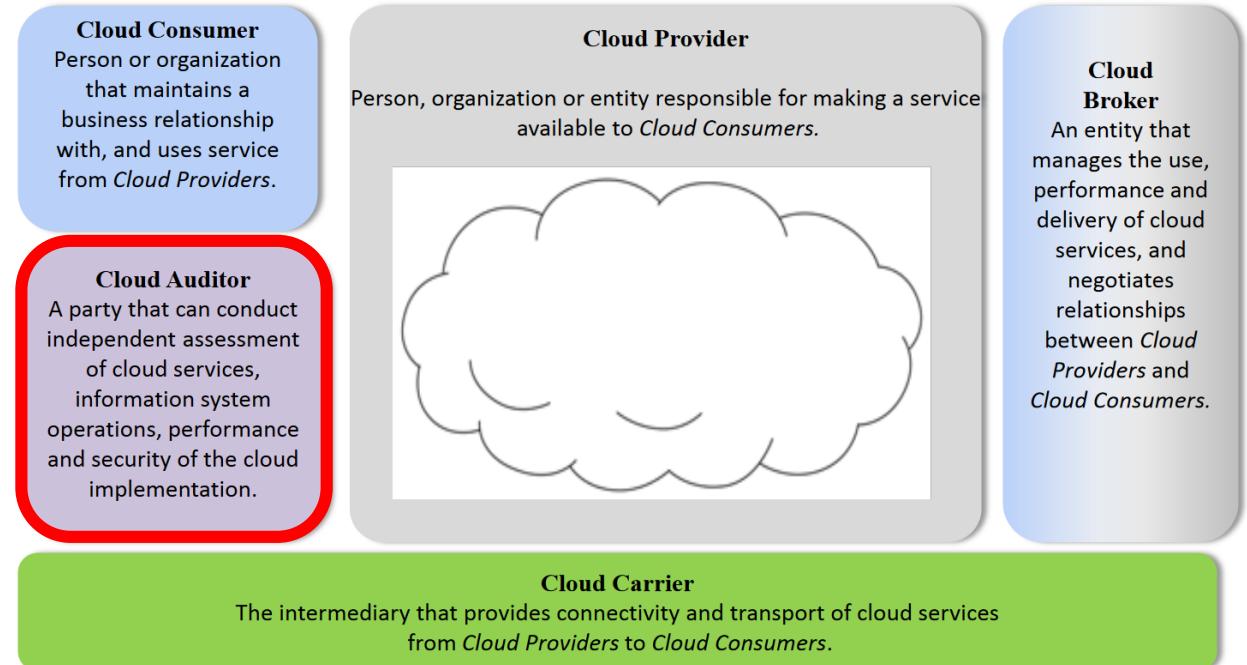
Cloud provider

- Provides cloud services to individuals or organizations
- Provides provide rented and provider-managed virtual hardware, software, infrastructure and other related services



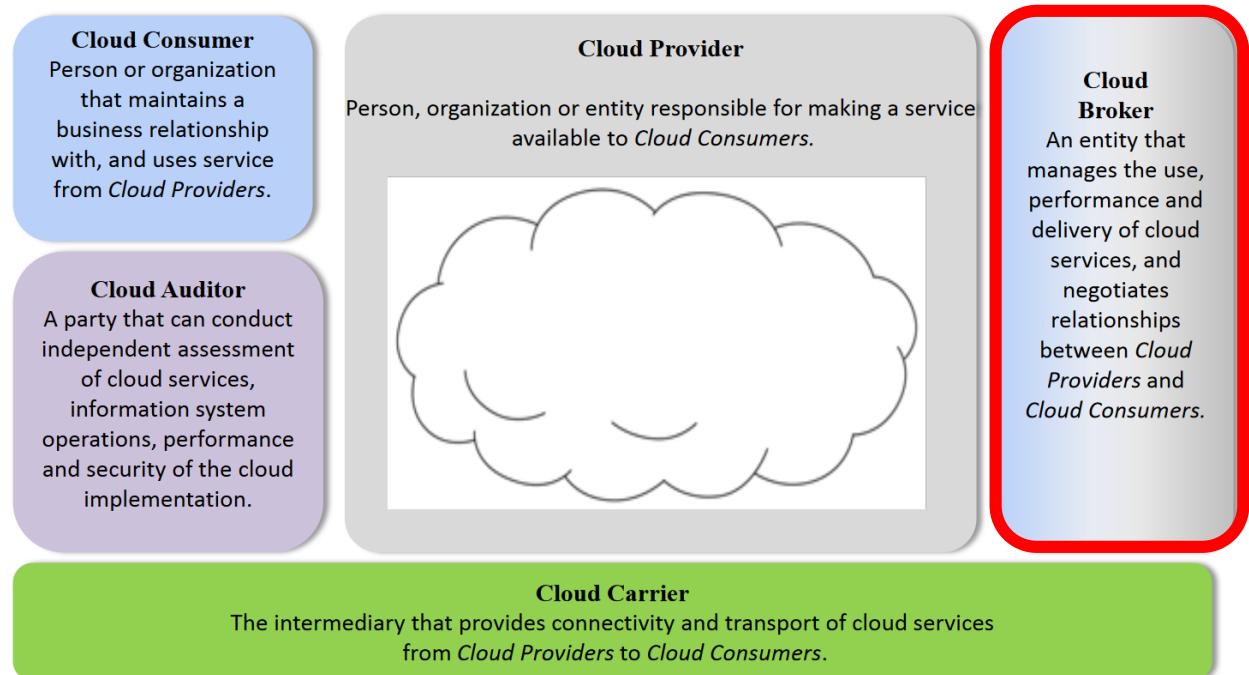
Cloud Auditor

- Examines the services provided by the Cloud provider
- Provides an independent opinion about the services and verify conformance with the standards
- Evaluate services such as security, performance, and privacy



Cloud Broker

- Manages the use, performance and delivery of cloud services
- Negotiates relationships between cloud providers and cloud consumers
- Three categories of services provided by the cloud broker-
 - Aggregation
 - Arbitrage
 - Intermediation



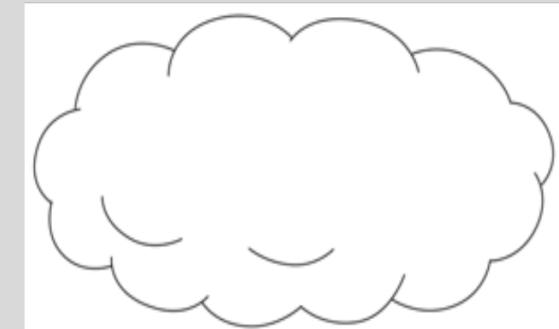
Cloud Carrier

- Connects cloud services to the telecommunication provider
- Carrier clouds integrate some of the components and features found in telecom networks such as wide area networks ([WAN](#)), virtual private networks ([VPN](#)), open [APIs](#) and dynamic resource allocation.

Cloud Consumer
Person or organization that maintains a business relationship with, and uses service from *Cloud Providers*.

Cloud Auditor
A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.

Cloud Provider
Person, organization or entity responsible for making a service available to *Cloud Consumers*.



Cloud Broker
An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.

Cloud Carrier

The intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

Cloud Service Models (XaaS)

- XaaS stands for “Anything-as-a-Service” or “Everything-as-a-Service”
- Combination of Service Oriented Architecture and Cloud computing
- XaaS refers to different services provided over the Internet instead of performing it on the local machine or on-site.

Primary Cloud Service Models

- Infrastructure as a Service
- Platform as a Service
- Software as a Service

Provider Type	Major Activities
SaaS	Installs, manages, maintains and supports the software application on a cloud infrastructure.
PaaS	Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment and administration tools to platform consumers.
IaaS	Provisions and manages the physical processing, storage, networking and the hosting environment and cloud infrastructure for IaaS consumers.

Source:

Infrastructure as a Service

- Services that provide high-level APIs used to abstract various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup
- According to NIST's definition of IaaS is
where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Infrastructure as a Service

Business aspects of IaaS:

- Economical web hosting services
- Supports application and web servers and manage networking resources
- Increased performance on computing
- Assists in big data analysis
- Maintains huge storage, backup, and recovery

Infrastructure as a Service

Example of IaaS:

- Google Cloud Platform
- Amazon's AWS
- Microsoft Azure

Platform as a Service

- NIST defines PaaS as

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

- Gives customers the ability to use a provider's physical hardware remotely
- Clients may utilize a provider's virtual servers, storage databases and networks on pay-per-use basis.

Platform as a Service

Business aspects of PaaS:

- Stands as a platform for the development and customization of cloud-based applications.
- PaaS tools allow you to investigate and mine their information thus finding deeper insights to deliver better outcomes.
- Offers services for enhanced protection, workflow, directory, and scheduling.

Platform as a Service

Examples of PaaS:

- Google App Engine
- Heroku

Software as a Service

- Provides on-demand access and use of cloud-based software without the need for physical, on-site equipment, platforms or installed software applications.
- As per the definition of SaaS by NIST-

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Software as a Service

Business aspects of SaaS:

- Shows simple accessibility for complex applications
- Allows using client software in a free manner
- Mobilize workforce
- Accessibility for application information from any location

Software as a Service

Examples of SaaS:

- OneDrive
- DropBox
- Office 365

Other Cloud Service Models

- Security as a Service (SECaaaS)
- Database as a Service (DaaS)
- Business Process as a Service (BPaaS)
- Identity as a Service (IDaaS)
- Backup as a Service (BaaS)
- Communications, content, and computing as a Service (CaaS)
- Storage as a Service (another SaaS)

Requirements

➤ Requirements of Cloud Service Provider:

➤ Increase productivity

➤ Increase end-user satisfaction

➤ Increase innovation

➤ Increase agility

Microservices

- It is a variant of the Service-oriented Architecture
- It arranges an application as a collection of loosely coupled services
- Microservices use lightweight protocols

Microservices

Characteristics:

- Services in a microservice architecture (MSA) are often processes that communicate over a network to fulfil a goal using technology-agnostic protocols such as HTTP
- Services are organized around business capabilities
- Services can be implemented using different programming languages, databases, hardware and software environment, depending on what fits best

Microservices

Characteristics:

- Services are small in size, messaging-enabled, bounded by contexts, autonomously developed, independently deployable, decentralized and built and released with automated processes
- Lends itself to a continuous delivery software development process. A change to a small part of the application only requires rebuilding and redeploying only one or a small number of services
- Adheres to principles such as fine-grained interfaces (to independently deployable services), business-driven development (e.g. domain-driven design)

Microservices

Benefits:

➤ **Scalability:**

Since microservices are implemented and deployed independently of each other, i.e. they run within independent processes, they can be monitored and scaled independently

➤ **Distributed development:**

It parallelizes development by enabling small autonomous teams to develop, deploy and scale their respective services independently. It also allows the architecture of an individual service to emerge through continuous refactoring. Microservice-based architectures facilitate continuous integration, continuous delivery and deployment.

Microservices

Benefits:

➤ **Modularity:**

This makes the application easier to understand, develop, test, and become more resilient to architecture erosion. This benefit is often argued in comparison to the complexity of monolithic architectures

➤ **Integration of heterogeneous and legacy systems:**

Microservices is considered as a viable mean for modernizing existing monolithic software application. There are experience reports of several companies who have successfully replaced (parts of) their existing software by microservices, or are in the process of doing so. The process for Software modernization of legacy applications is done using an incremental approach.

References

- R. B. Bohn, J. Messina, F. Liu, J. Tong and J. Mao, "NIST Cloud Computing Reference Architecture," 2011 IEEE World Congress on Services, Washington, DC, 2011, pp. 594-596, doi: 10.1109/SERVICES.2011.105.
- <https://www.javatpoint.com/cloud-computing-vs-grid-computing>
- <https://www.cloudcruiser.com/cloud-computing-architecture/>
- <https://www.elprocus.com/cloud-computing-technology/>
- <https://www.netapp.com/knowledge-center/what-are-microservices/>

Thank You!



Cloud Computing (CS60118)

(Spring 2020-2021)

Communication and Networking Technologies

Dr. Sudip Misra

Professor

Department of Computer Science and Engineering

Indian Institute of Technology Kharagpur

Email: smisra@sit.iitkgp.ernet.in

Website: <http://cse.iitkgp.ac.in/~smisra/>

Research Lab: cse.iitkgp.ac.in/~smisra/swan/

Contents

- Communication Technologies

- IEEE 802.15.4
- 6LoWPAN
- RFID
- Zigbee
- Wireless HART
- Bluetooth

- Networking Technologies

- MQTT
- CoAP
- XMPP

Introduction

- The most important and commonly used communication protocols in IoTs and cloud computing are:
 - 6LoWPAN, Zigbee, IEEE 802.15.4, Wireless HART, Z-Wave, ISA 100, NFC, RFID, and Bluetooth

IEEE 802.15.4

Features of IEEE 802.15.4

- IEEE 802.15.4 is the technical standard for low-rate wireless personal area networks
- Developed primarily for low-data-rate applications and extended-life low-power-consumption uses.
- IEEE 802.15.4 employs only the first two layers (PHY, MAC) in addition with the logical link control (LLC) and service-specific convergence sublayer (SSCS) to communicate with all upper layers.
- Operates in the ISM radio band.
- The goal of IEEE 802.15.4 is to render a base format to which the upper layers (layers 3 through 7) could add other protocols and features.

Source: L.Fenzel, “[What’s The Difference Between IEEE 802.15.4 And ZigBee Wireless?](#)”, Electronic Design (Online), Mar. 2013

Features of IEEE 802.15.4

- IEEE 802.15.4 utilizes direct sequence spread spectrum (DSSS) modulation.
- High tolerance to noise and interference and offers link reliability improvement mechanisms.
- The low-speed versions of IEEE 802.15.4 use Binary Phase Shift Keying (BPSK), whereas the high data-rate versions use offset-quadrature phase-shift keying (O-QPSK). Uses CSMA-CA for channel access.
- Multiplexing feature enables multiple devices to access the same channel without interference at different times.

Source: L.Fenzel, “What’s The Difference Between IEEE 802.15.4 And ZigBee Wireless?”, Electronic Design (Online), Mar. 2013

Features of IEEE 802.15.4

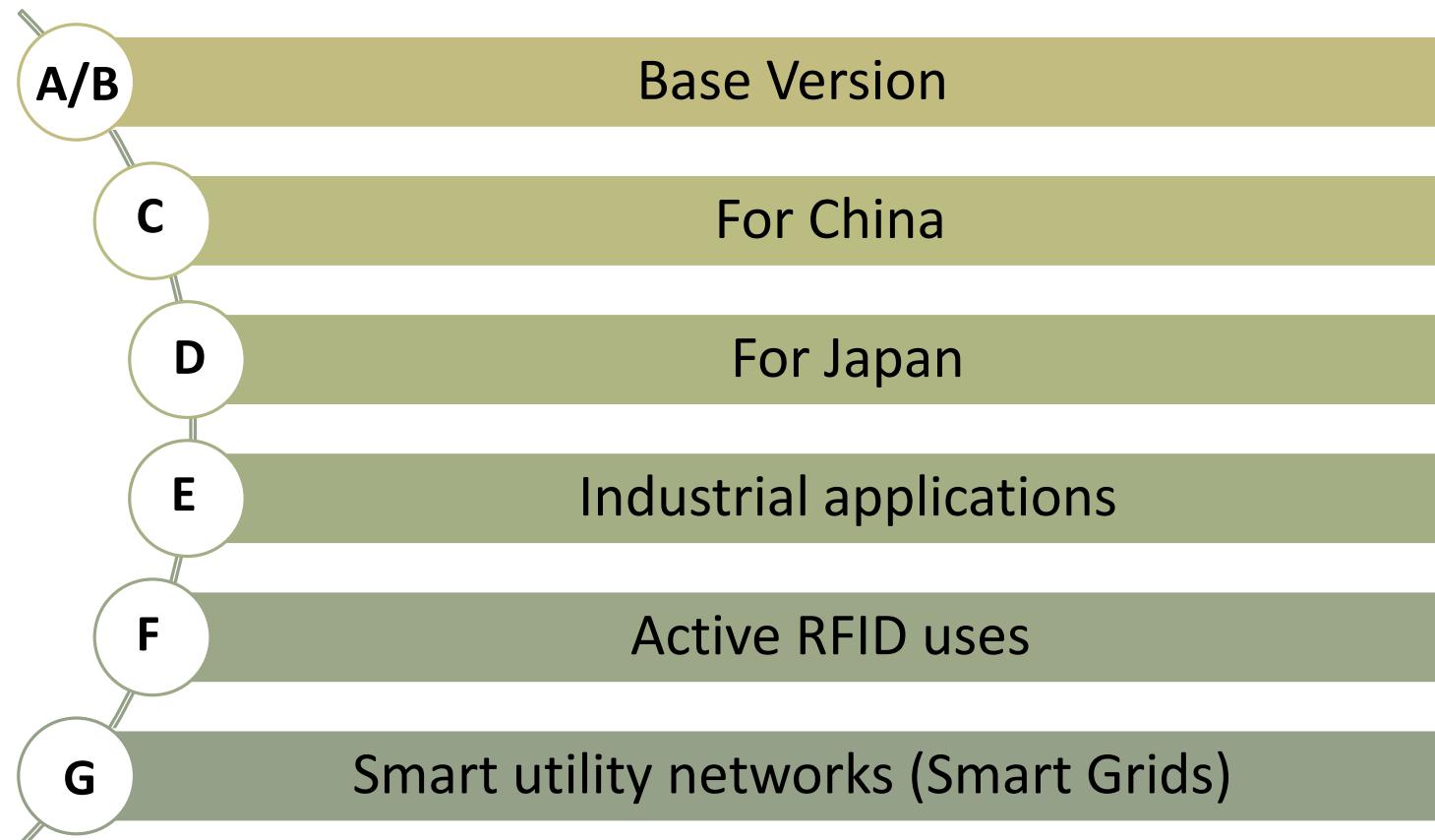
- Short packets are transmitted infrequently for a very low duty cycle (<1%) to minimize power consumption.
- The minimum power level defined is –3 dBm or 0.5 mW.
- Under the best conditions the transmission range can reach up to 1000 meters.
- Standard transmission range is 10 to 75 meters.
- The nature of the transmission path is mostly line of sight (LOS).
- 802.15.4 defines two topologies:
 - a basic star
 - a basic peer-to-peer (P2P)

Source: L.Fenzel, “What’s The Difference Between IEEE 802.15.4 And ZigBee Wireless?”, Electronic Design (Online), Mar. 2013

IEEE 802.15.4 Layered diagram

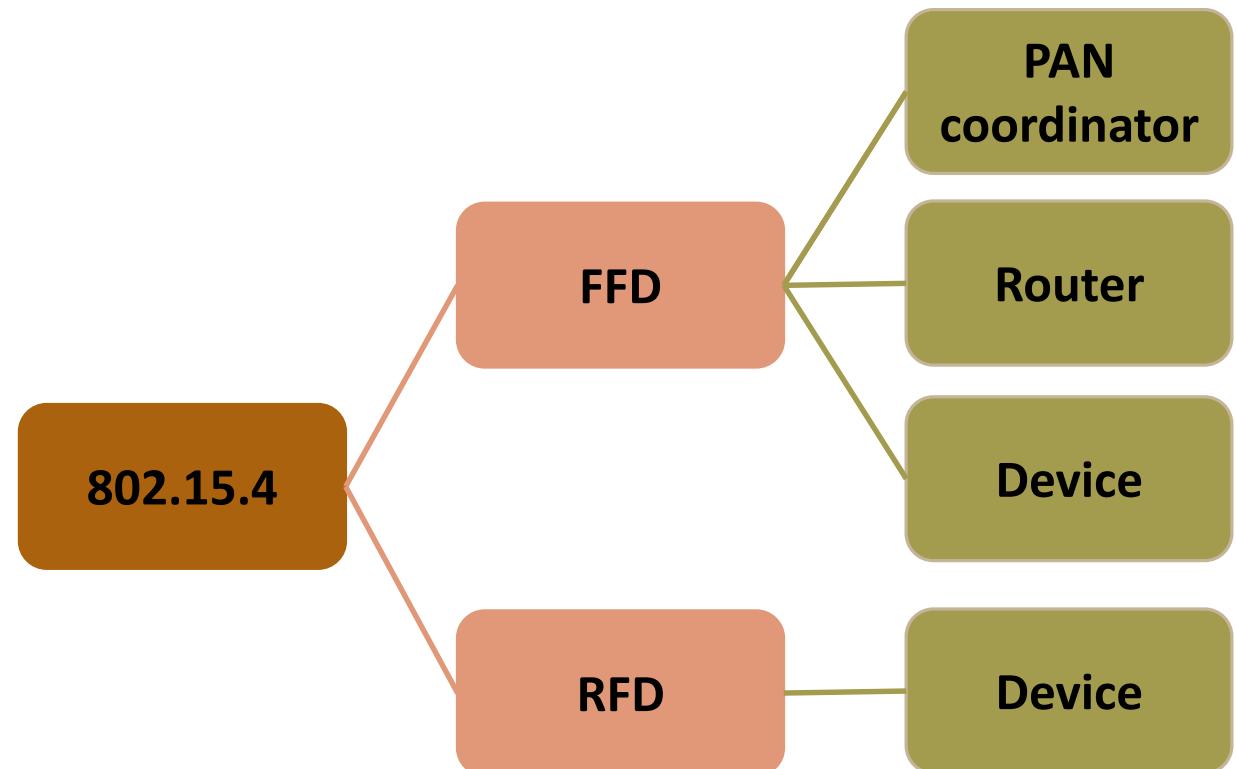


IEEE 802.15.4 Variants

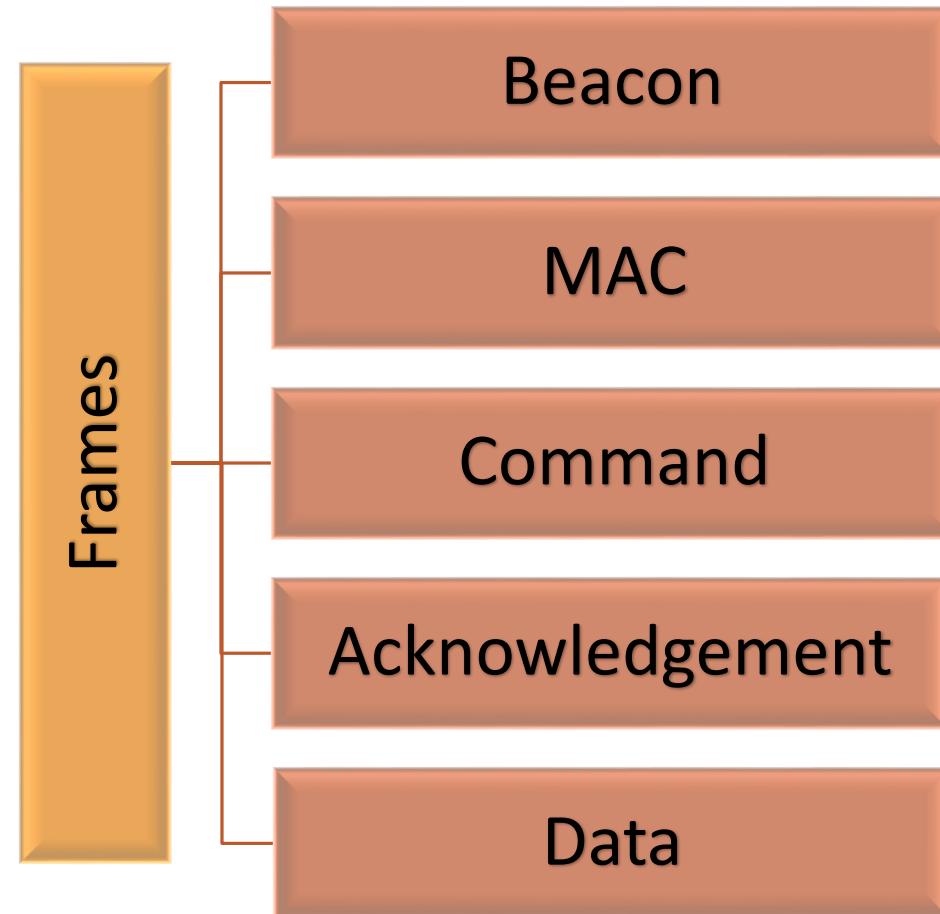


IEEE 802.15.4 Types

- Full Function Device (FFD)
 - Can communicate with all types of devices
 - Supports full protocol
- Reduced Function Device (RFD)
 - Can only communicate with an FFD
 - Reduces power consumption
 - Minimum CPU/RAM required

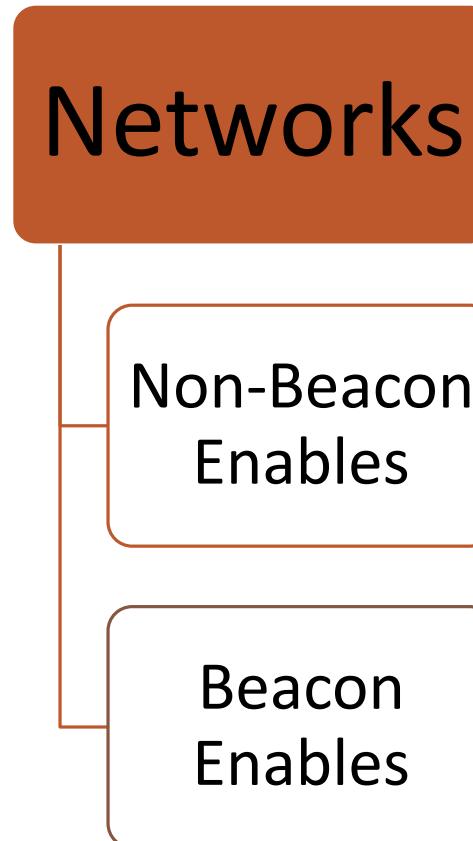


IEEE 802.15.4 Frames



Beacon Enabled Networks

- Beacon messages are transmitted periodically.
- Data-frames are transmitted through Slotted CSMA/CA with a superframe structure which the PAN coordinator manages.
- Beacons are used to synchronize & associate nodes with the coordinator.
- Operational scope crosses the whole network.



Non-Beacon Enabled Networks

- Data-frames are transmitted through un-slotted CSMA/CA (ContentionBased)
- Beacons are used for only link-layer discovery.
- Both source and destination IDs are required.
- All protocol addressing must stick to mesh configurations as IEEE 802.15.4 is primarily a mesh protocol.
- Communications amongst nodes are de-centralized.

6LoWPAN

Introduction

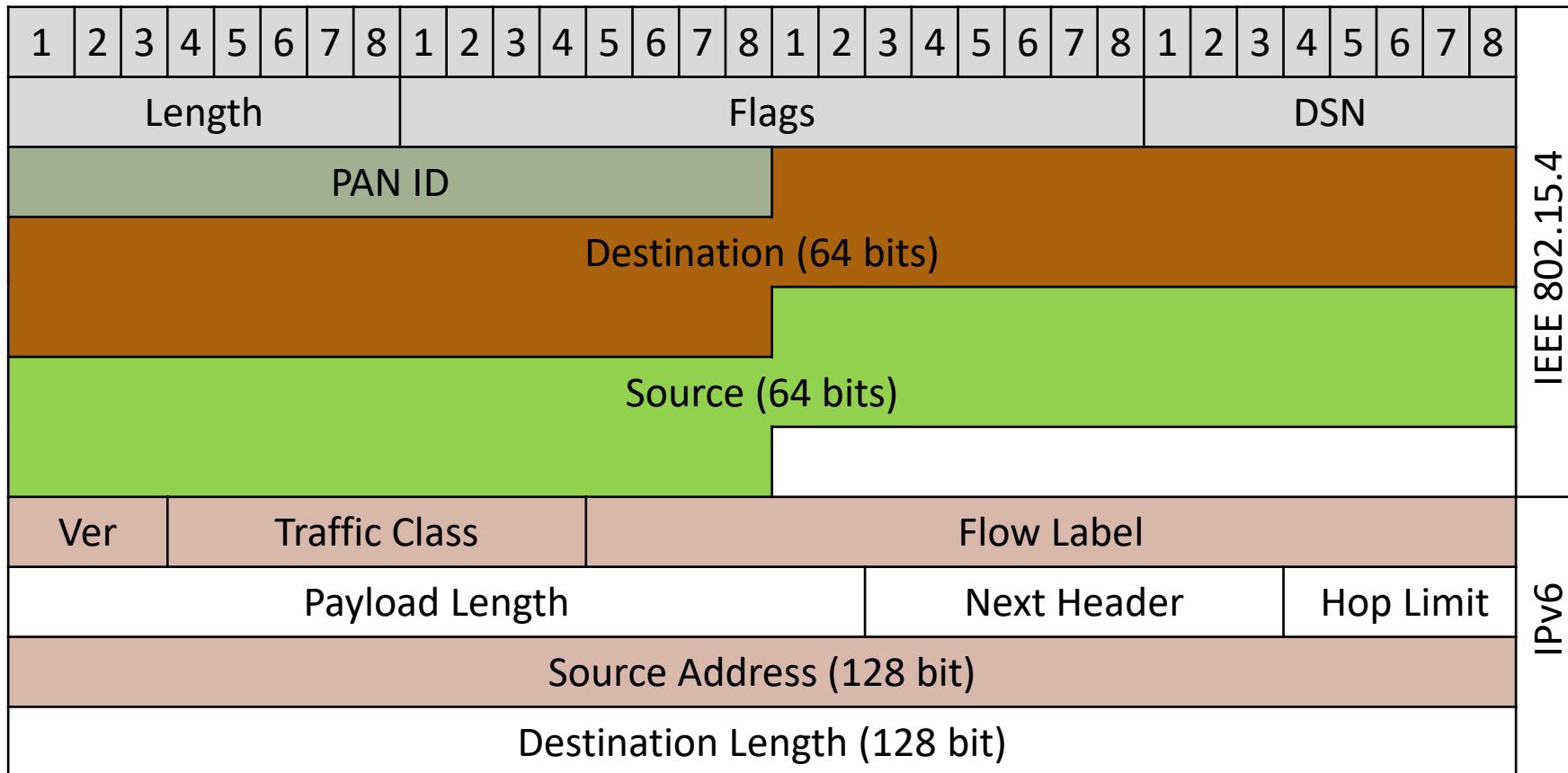
- Acronym for Low-power Wireless Personal Area Networks (LoWPAN) over IPv6.
- Especially designed for low-power devices by adopting a compressed IPv6 protocol to minimize resource consumption
- Allows small low-power devices with limited processing capability to communicate wirelessly through an Internet protocol.
- It was created by the Internet Engineering Task Force (IETF) - RFC 5933 and RFC 4919.

Source: T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik , JP. Vasseur, R. Alexander,
“RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks”, IETF, Standards Track, Mar. 2012

Features of 6LoWPAN

- Small packet size with low bandwidth (250/40/20 kbps) and low power (battery operated)
- Addressing:
 - 64-bit extended
 - 16-bit short addressing: unique within the PAN [IEEE802.15.4].
- Supports star and mesh topology
- Relatively low cost

6LowPAN Packet Format



Header Type: Dispatch Header

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	
0,1	Dispatch								Type specific header															

- 0,1:
 - Dispatch Type Identifier
- Dispatch:
 - 6-bit
 - Identifies the type of the subsequent header.
- Type-specific header
 - A header determined by the Dispatch Header.

Header Type: Mesh Addressing Header

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
0,1	O	F	Hops Left	originator address						Final address													

➤ O:

- 0 if the Originator Address is an IEEE extended 64 bit address
- 1 if it is a short 16-bit addresses.

➤ F:

- 0 if the Final Destination Address is an IEEE extended 64 bit
- 1 if it is a short 16-bit addresses.

➤ Hops Left:

- Decrement by each forwarding node before forwarding the packet to its next hop
- The packet is not forwarded any further if Hops Left becomes 0.

Header Type: Fragmentation Header

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1	1	0	Datagram tag								Datagram size												

Figure: First Fragment

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1	1	1	Datagram tag						Datagram size						Datagram offset								

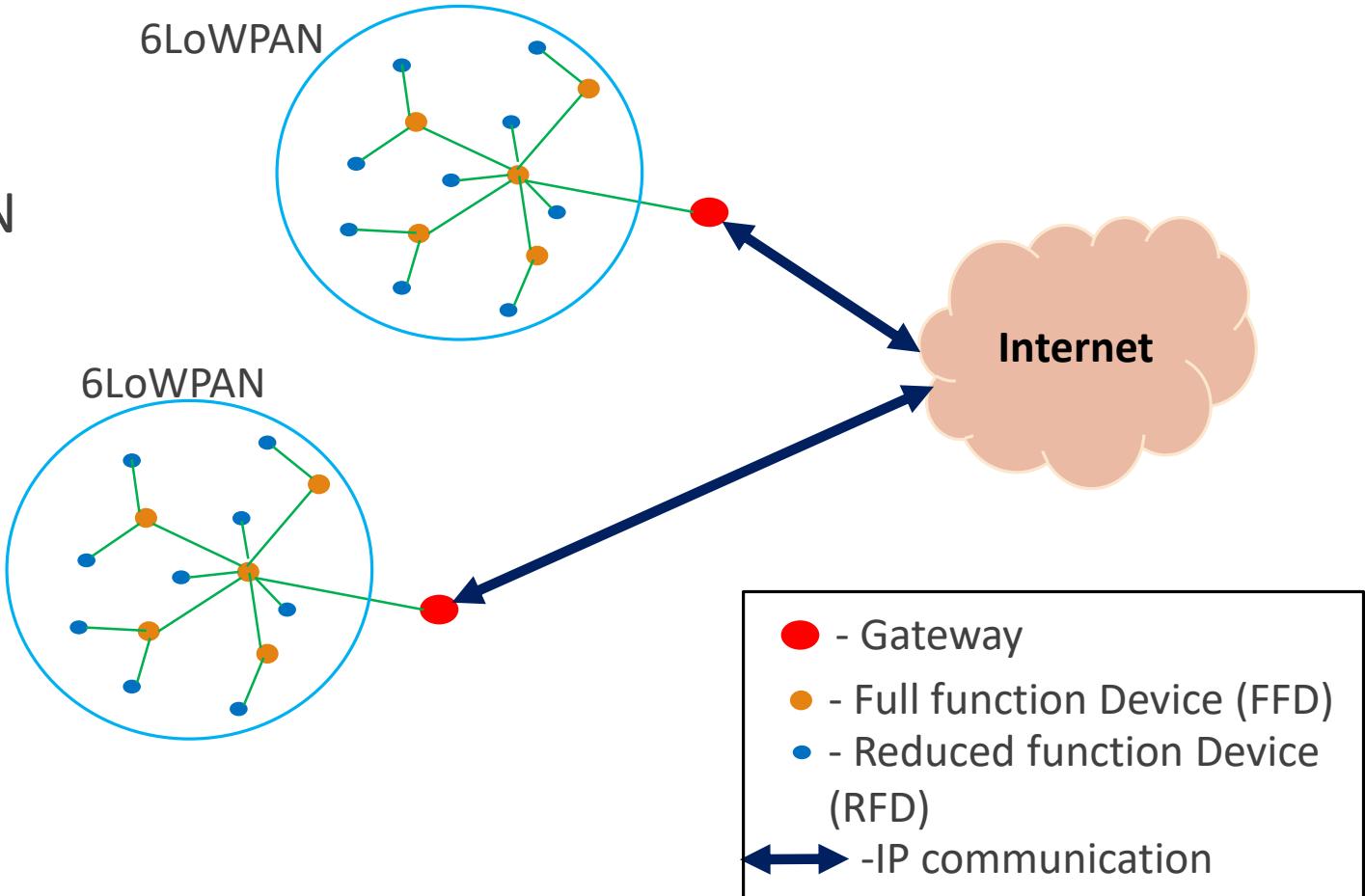
Figure: Subsequent Fragment

Header Type: Fragmentation Header

- Datagram tag:
 - Same value for all link fragments of a payload.
 - The sender increments datagram tag for successive, fragmented datagrams.
 - 10 bits long.
- Datagram size:
 - 11 bit long
 - Same value for all link fragments of an IP payload datagram.
- Datagram offset:
 - present only in the second and subsequent link fragments
 - 8 bits long.

6LoWPAN Routing

- Mesh routing within the PAN.
- Routing between IP and the PAN domain
- Routing protocols in use:
 - LOADng
 - RPL
 - HiLow



LOADng Routing

- Simplified on-demand routing protocol based on Ad-hoc On-demand Distance Vector (AODV), which is extended for use in IoT.
- Basic operations of LOADng are:
 - **Generation of Route Requests (RREQs)** by originator to discover a route to a destination
 - **Forwarding of RREQs** until they reach the destination LOADng Router
 - **Generation of Route Replies (RREP)**s after receiving RREQ from the destination to the originator

Source: Clausen, T.; Colin de Verdiere, A.; Yi, J.; Niktash, A.; Igarashi, Y.; Satoh, H.; Herberg, U.; Lavenu, C. et al. (January 2016). [*The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation \(LOADng\)*](#). IETF. I-D draft-clausen-lln-loadng-14

LOADng Routing

- If a route is broken, a **Route Error (RERR)** message will be sent back to the originator to inform the originator about the route breakage.
- **Optimized flooding** is supported to reduce the overhead created by RREQ generation and flooding.
- Only the destination is authorized to respond to an RREQ.
- Intermediate LOADng Routers are strictly forbidden from replying to any RREQs, even if they have any active routes to the destination.
- RREQ/RREP messages created by a LOADng Router has a unique, monotonically increasing sequence number.

RPL Routing

- Routing protocol for lossy and low power networks.
- Handles routing topology employing low rate beaconing.
- Detection inconsistencies increase beaconing rate (if a node or link in a route is broken).
- The datagram itself constitutes Routing information.
- Proactive: Maintaining routing topology.
- Reactive: Resolving routing inconsistencies.
- RPL separates packet processing and forwarding from the routing optimization objective, which helps in Low power Lossy Networks (LLN).

Source: T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik , JP. Vasseur, R. Alexander,
“RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks”, IETF, Standards Track, Mar. 2012

RPL Routing

- RPL supports confidentiality and integrity of a message, Data-Path Validation, and Loop Detection.
- Routing optimization objectives of RPL comprise:
 - minimizing energy
 - minimizing latency
 - satisfying constraints (w.r.t node power, bandwidth.)
- RPL operations need bidirectional links, and in some LLN cases, those links may show asymmetric nature.
- It is necessary to substantiate the reachability of a router before it is used as a parent.

Source: T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik , JP. Vasseur, R. Alexander,
[“RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks”](#), IETF, Standards Track, Mar. 2012

RFID

Introduction

- Radio-frequency identification
- An RFID system comprises a radio transponder, a radio receiver and a transmitter.
- Slightly similar to barcodes.
- Digitally encoded data in RFID tags can be read by a reader. The reader read data from tags and store in a database.
- Unlike barcodes and QR codes, RFID tag data can be read outside the line-of-sight

Source: “How does RFID work?” AB&R (Online)

Features RFID

- Each RFID tag comprises an integrated circuit and an antenna.
- RFID tags are often covered with a protective material to act as a shield against various environmental effects.
- Tags can be passive or active.
- Passive RFID tags are more widely used.
- Passive tags are powered by the RFID reader's interrogating radio waves before they can transmit information
- Active tags have their own power supply, and therefore, the reader can read them from hundreds of meters apart

Source: “How does RFID work?” AB&R (Online)

RFID Types

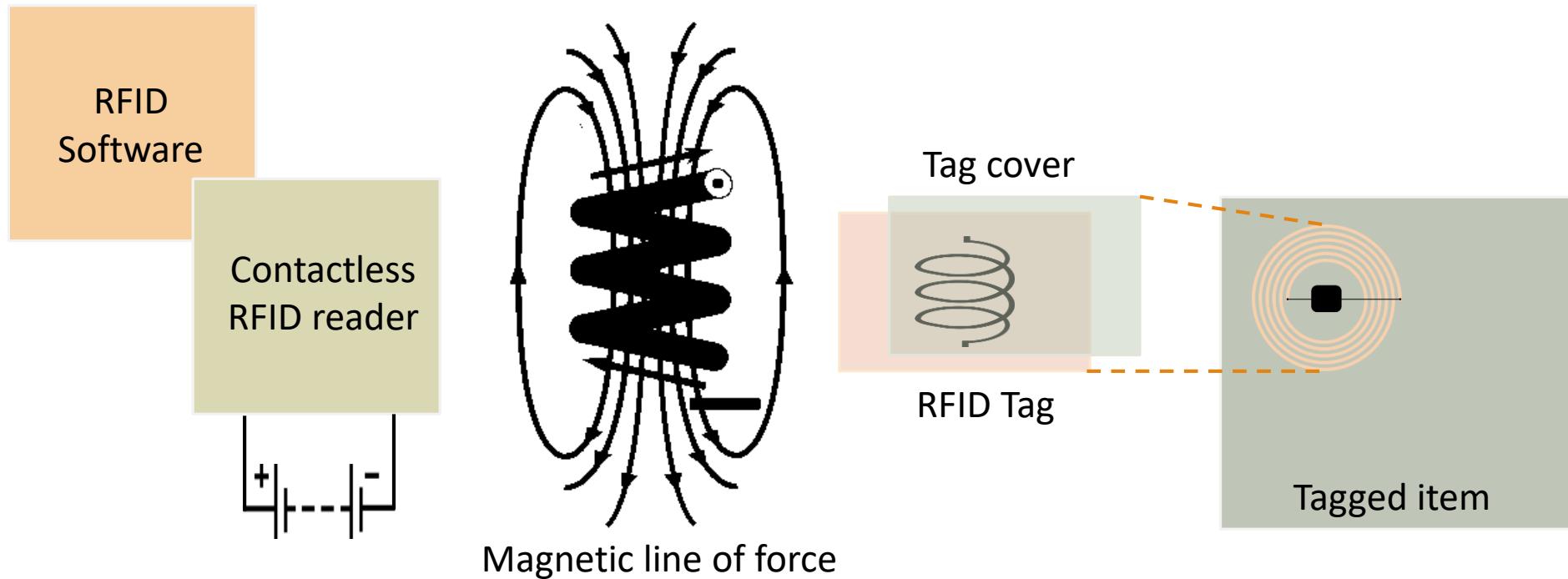
- Passive Reader Active Tag (PRAT)
- Active Reader Passive Tag (ARPT)
- Active Reader Active Tag (ARAT)

Working Principle

- Derived from Automatic Identification and Data Capture (AIDC) technology.
- AIDC is the method that automatically identifies objects, collects data about the objects, and stores them directly into computer systems with little or no human intervention.
- QR codes, bar codes, RFID, biometrics, magnetic stripes, optical character recognition (OCR), smart cards, and voice recognition are considered as part of AIDC.
- RFID uses radio waves to perform AIDC functions.
- An RFID system's main components are:-- an RFID tag or smart label, an RFID reader, and an antenna.

Source: “How does RFID work?” AB&R (Online)

Working Diagram



Applications

- Inventory management
- Asset tracking
- Controlling access to restricted areas
- Locating lost airport baggage
- Timing sporting events
- Supply chain management
- Counterfeit prevention
- Tracking of persons and animals
- Toll collection and contactless payment

Source: “How does RFID work?” AB&R (Online)



Cloud Computing (CS60118)
(Spring 2020-2021)

Service and Data Management in Cloud

Dr. Sudip Misra

Professor

Department of Computer Science and Engineering

Indian Institute of Technology Kharagpur

Email: smisra@sit.iitkgp.ernet.in

Website: <http://cse.iitkgp.ac.in/~smisra/>

Research Lab: cse.iitkgp.ac.in/~smisra/swan/

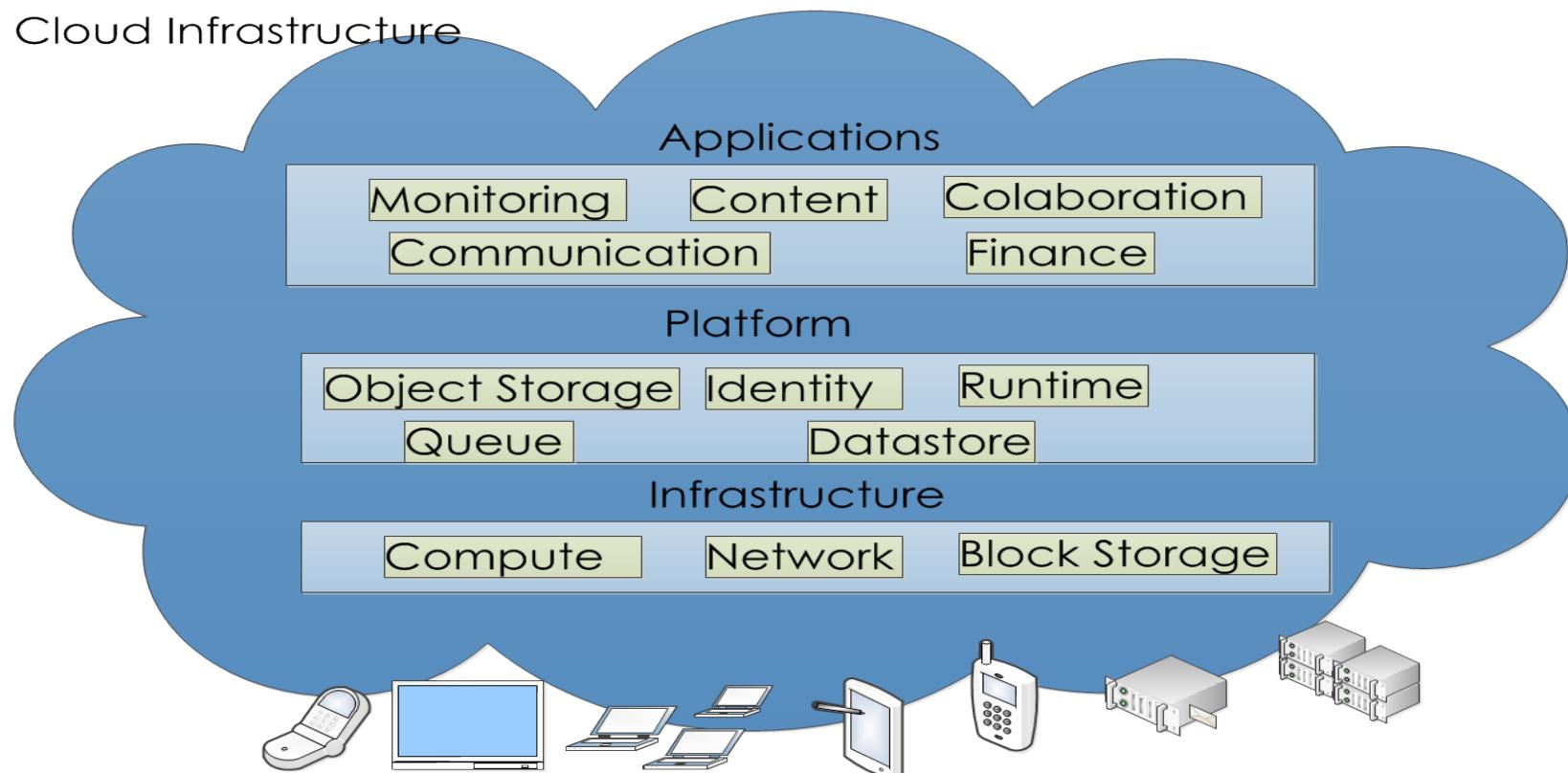
Contents

- Resource Abstraction and Workloads
- Load Management
- Storage Access Protocols
- Functions and Benefits of the Services and Storage

Resource View of Cloud

- Consumer View -
 - Metered scalable service consists of infinite resource pool, capable to provide any amount of resource .
- Cloud Service Provider View
 - Serve as many as consumers with finite amount of resource pool.
 - Optimal management of resources.
 - Provision of minimal service accessing overhead of consumers through resource abstraction

Different Types of Resource in Cloud



Source: [cloud computing-wikipedia](#)

Need of Resource Management

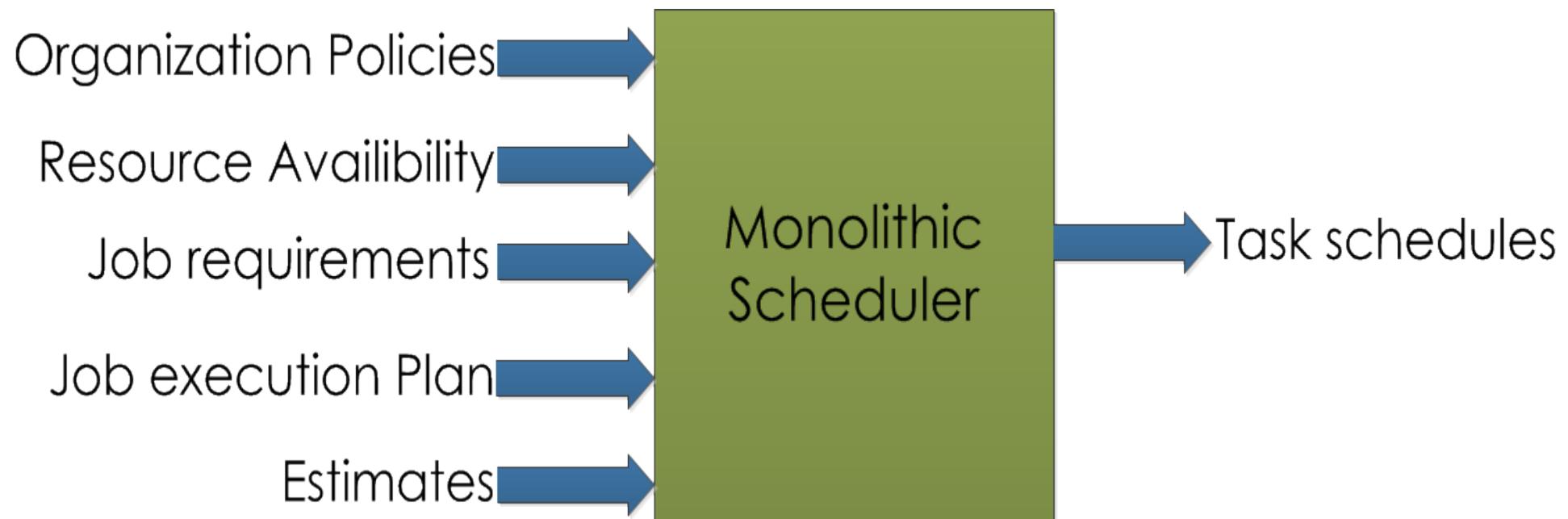
- Integration of heterogeneous resources in cloud enhances the adoption of cloud computing by service consumer. The advantages of heterogeneous resource integrations are
 - Wide range of application support.
 - Mapping between application requirements and resource features or characteristics.
 - Maximization of cloud service provider (CSP) profit
 - Maximization of Cloud Service Consumer satisfaction.

Cloud Resource Scheduler

- Cloud Resource scheduler is grouped into three types –
 - Monolithic scheduler
 - Two-Level scheduler
 - Shared State scheduler

Monolithic Scheduler

- Monolithic Scheduler -- A Monolithic Scheduler has a single instance, is sequential, and must implement all policy choices in a single code base. e.g. Google Borg scheduler.

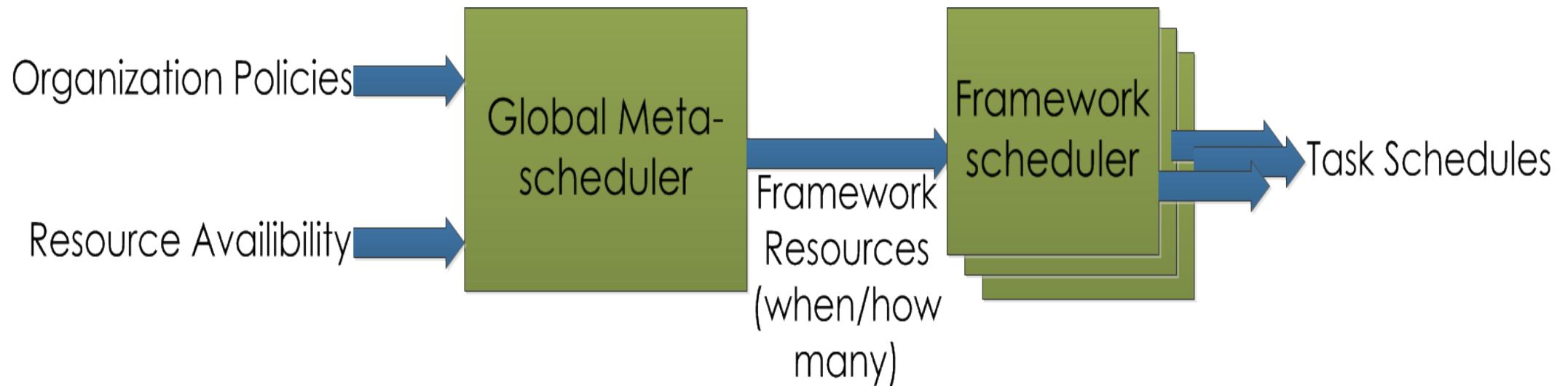


Source: <https://bit.ly/3kC8agV>

Two-level Scheduler

- It is an infrastructure management framework and separates application schedulers from resource schedulers.
- Master scheduler decides the number of resources from the available pool can be assigned to a framework.
- Application scheduler allocates resources to each application within a framework.
- Mesos is an example of two-level scheduler.

Two-level Scheduler

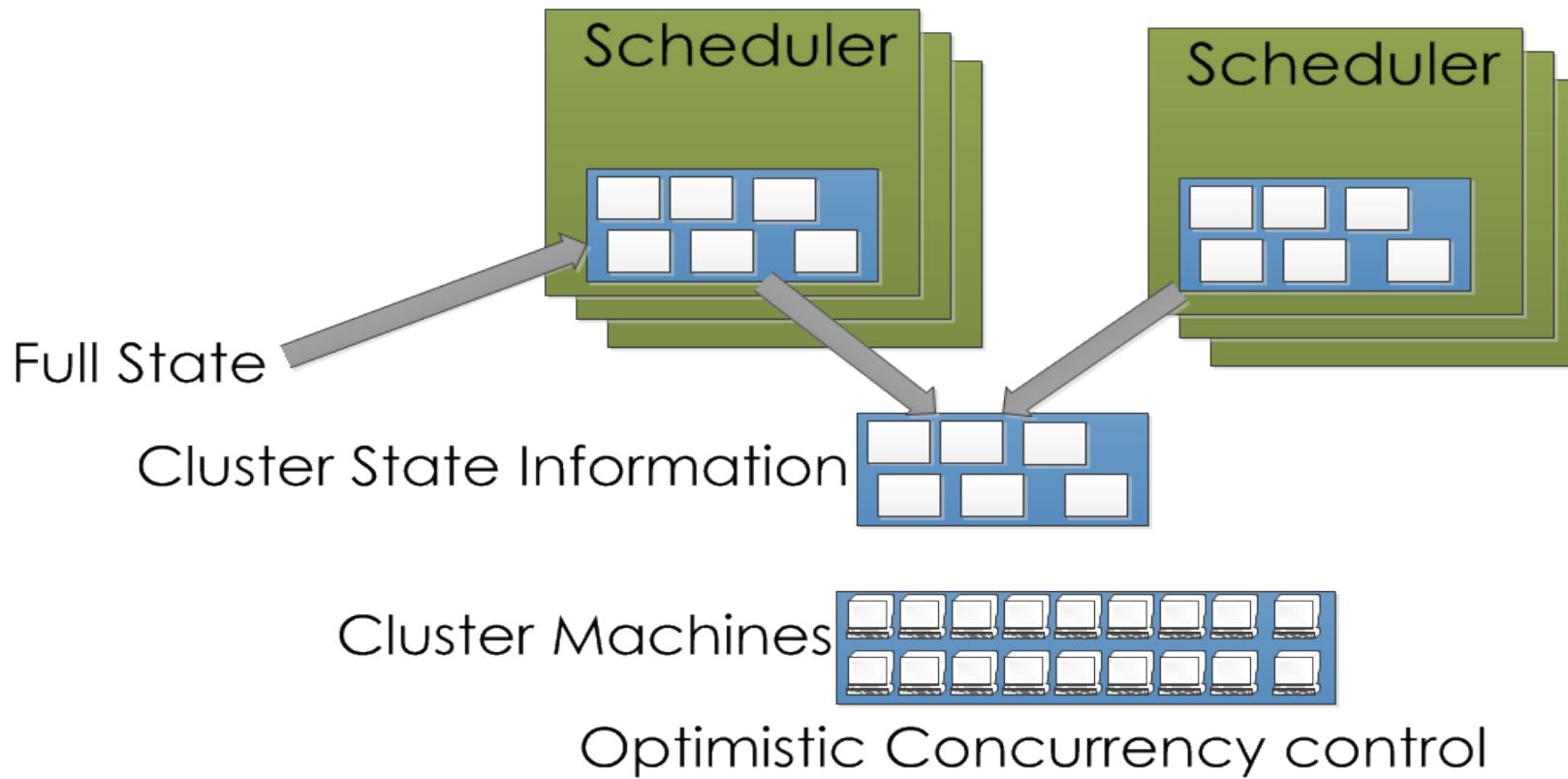


Source: <https://bit.ly/3kC8agV>

Shared State Scheduler

- Supports multiple parallel scheduler.
- Each scheduler maintains a local copy of the global state for local decision making.
- After each local decision the shared copy of the global state is also updated. The state synchronization is done through atomic commit.
- Google omega is a shared state scheduler.

Shared State Scheduler



Source: <https://bit.ly/3kC8agV>

Cloud Resource Scheduling Decision Parameters

- Parameters to map the applications to cloud resources are --
 - Resource requirement of applications.
 - Number of available CPU cores.
 - Free memory space.
 - Available storage space.
 - System state Information.

Resource Abstraction

- Abstraction enables shared, ubiquitous access to cloud resources.
- Virtualization or containerization is the key to resource abstraction in cloud.
- Virtualization uses a set of technologies to create virtual machine, virtual server, virtual storage and virtual network.
- Virtualization assigns a logical name to physical resources and provides a pointer when a request is made.
- The mapping in virtualization is dynamic.

Types of Virtualization

- Access – Consumer can access cloud resources from any location.
- Application – Cloud has multiple application instances and directs request to one of instances based on predefined criteria.
- CPU – Computers are partitioned into set of virtual machines and each machine is assigned a workload.
- Storage – Data is stored in storage and virtual storage is assigned by exhibiting the redundancy via replication.

Virtual Machine

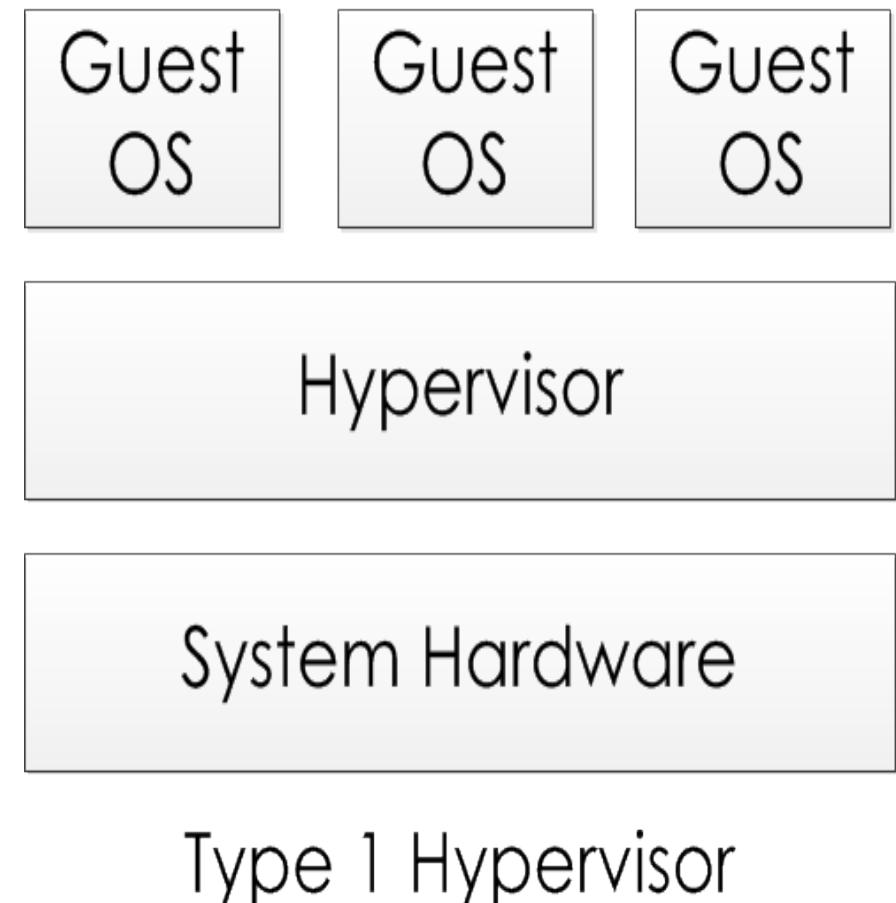
- A virtual machine has all the features of a physical machine, but is a software which emulates a physical machine.
- A system virtual machine or hardware virtual machine has own resource allocation, I/O with virtual driver and address space in memory.
- Process virtual machine runs as a single application or process.
- A virtual machine is logically separated from the host physical machine.
- Host machine can run multiple virtual machine at the same time, each with separate operating system and applications.

Hypervisor or Virtual Machine Monitor

- A low level program which helps to create and manage virtual machines.
- The operating system running on the physical machine is known as host operating system.
- The operating system installed on virtual machine is known as guest operating system.
- There are two types of virtual machine –
 - Type 1 Hypervisor
 - Type 2 Hypervisor

Type 1 Hypervisor

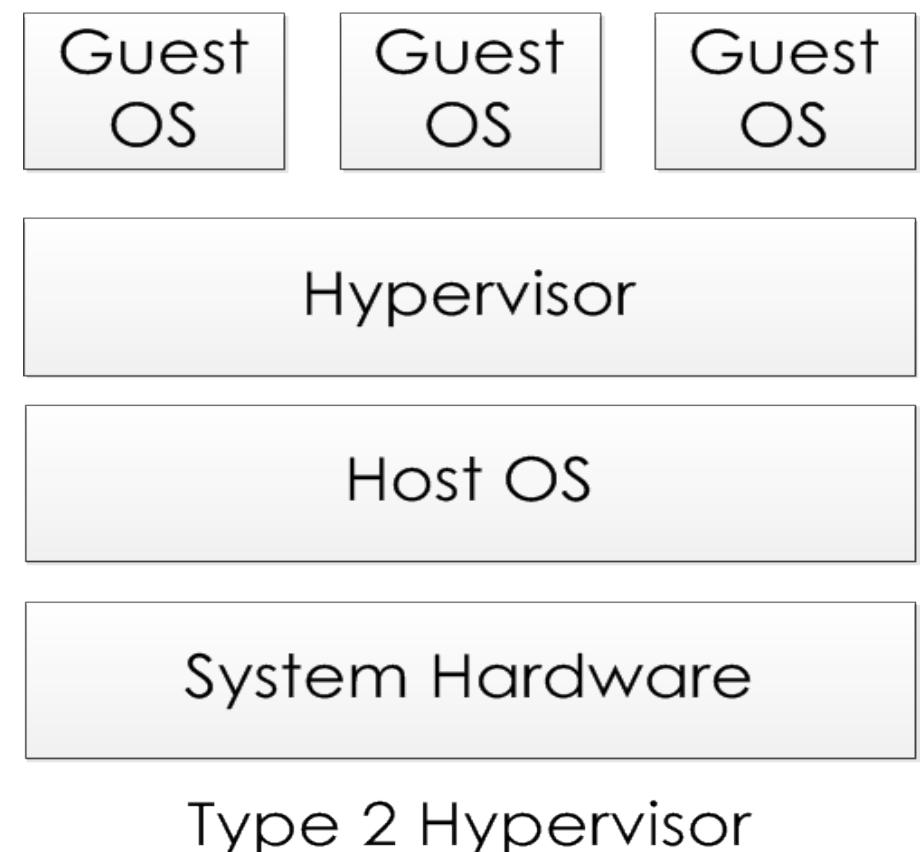
- A hypervisor running on a bare metal is called type 1 hypervisor or native VM.
- Type 1 hypervisor has no host operating system.
- LynxSecure, RTS Hypervisor, Oracle VM, Sun xVM Server, VirtualLogix VLX, VMware ESX and ESXi are example of type 1 hypervisor.



Source: Cloud Computing Bible.

Type 2 Hypervisor

- Type 2 hypervisor installed over host operating system and runs as a single application.
- KVM, Microsoft Hyper V, Parallels Desktop for Mac, Wind River Simics, VMWare Fusion, Virtual Server 2005 R2, Xen, Windows Virtual PC, and VMware Workstation 6.0 and Server are example of type 2 hypervisor.



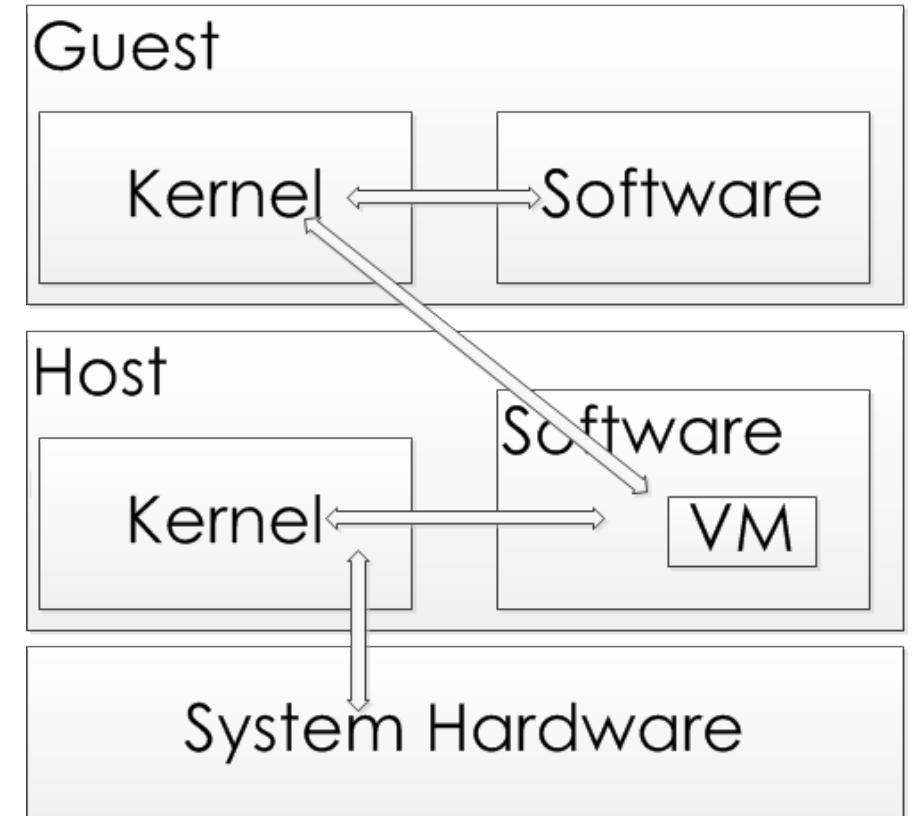
Source: Cloud Computing Bible.

Types of Virtualization

- Emulation
- Para virtualization
- Full Virtualization

Emulation

- In emulation, virtual machine simulates hardware.
- It is independent of the underlying host system hardware.
- Guest operating system is not modified.

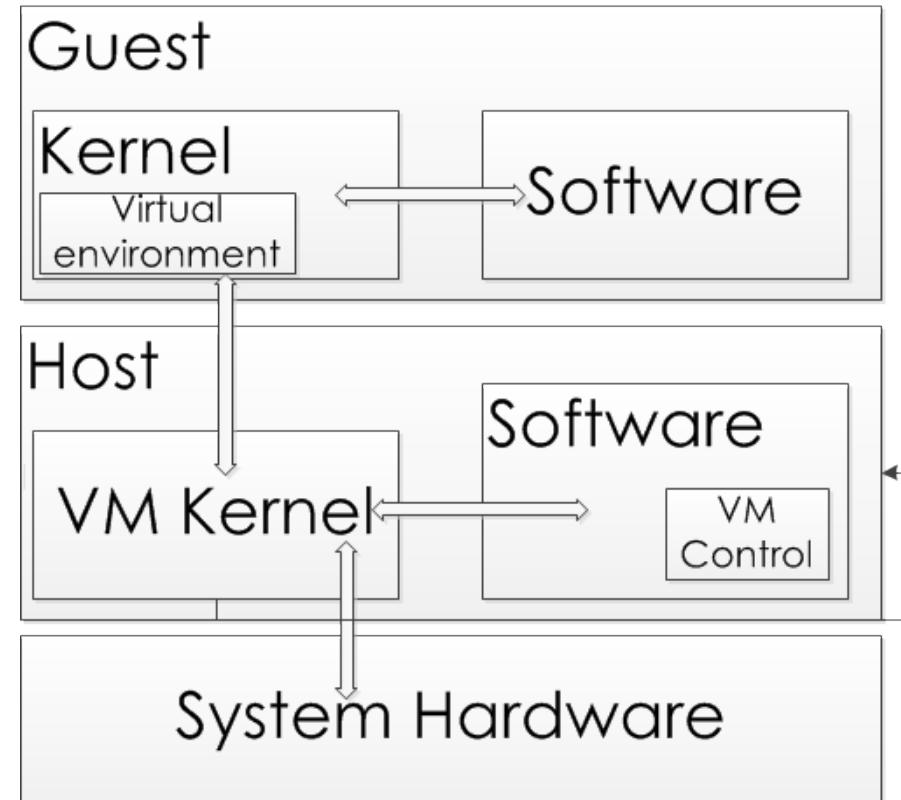


Emulation

Source: Cloud Computing Bible.

Para Virtualization

- Host operating system provides a virtual machine interface through which guest OS interacts with the host machine hardware.
- Guest operating system is modified to interact with the host machine hardware.

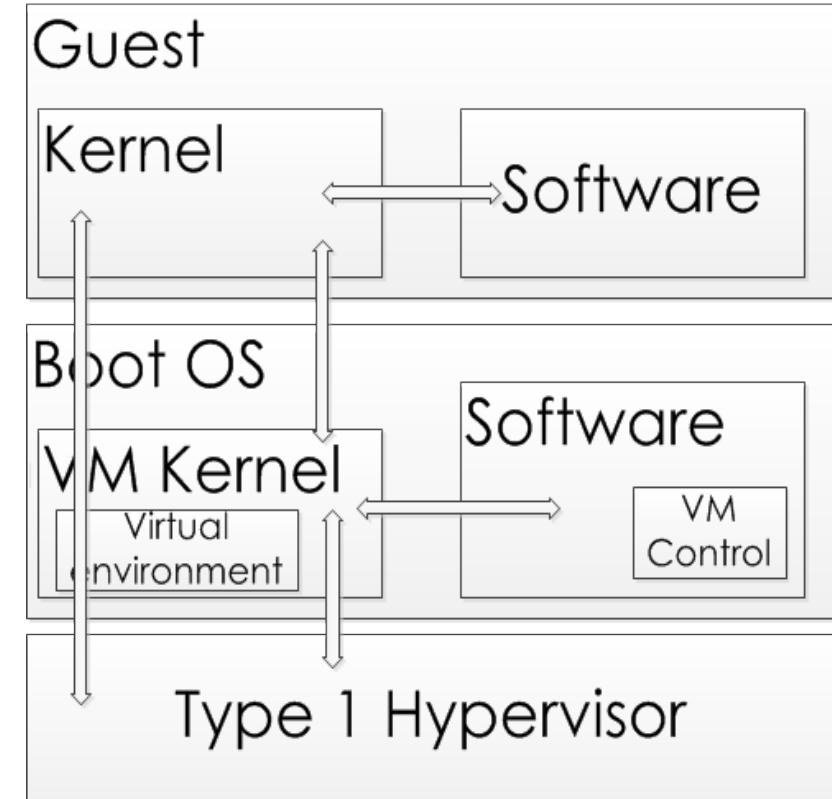


Para Virtualization

Source: Cloud Computing Bible.

Full Virtualization

- VM is installed as type 1 hypervisor directly on top of hardware.
- All operating systems communicates directly with the hypervisor.
- Guest operating system is not modified.
- Guest operating system is faster than other virtualization.



Full Virtualization

Source: Cloud Computing Bible.

Virtual Machine Lifecycle

- Let us assume that a request for creating a new server for a particular service has come from consumer .
- The request is delivered to the IT department.
- The IT department do the following--
 - Check the resource pool of the server's pool.
 - Match the resource specifications with the requirements.
 - Start provisioning the needed the virtual machines.
- After provisioning, it is delivered to the consumer.

Virtual Machine Lifecycle (contd)

Release Machine End of Service Compute resource deallocated to other VMs	IT Service Request Infrastructure Requirement Analysis IT Request
VM in Operation Serving web Request Migration Service Scale on demand compute resource	VM Provision Load OS Customize and Configure Start the server

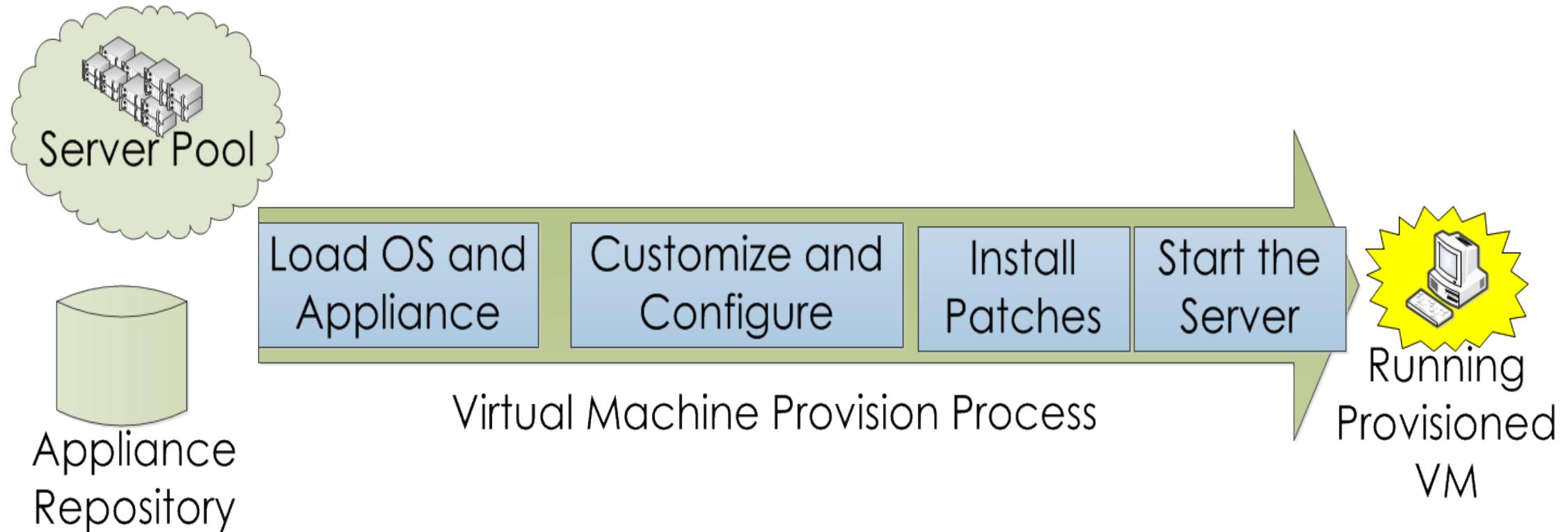
Virtual Machine Life Cycle

Source: Cloud Computing: Principles and Paradigms.

VM Provisioning Process

- VM provisioning the process of making ready the VM according to requirements.
- The provisioning steps are ---
 - Select a server from a pool of available servers with required OS template.
 - Load the appropriate software (device drivers, middleware and required application software) in selected server.
 - Customize and configure the machine.
 - Configure the associated network and storage.

VM Provisioning Process (contd)



Source: Cloud Computing: Principles and Paradigms.

CloudLightning Approach

- This architecture is constructed to address the challenges associated with heterogeneous cloud.
- It is composed of components and services with self-organization and self-management support.
- This approach describes how specialized hardware can be seamlessly integrated and complexity of resource management can be handled considering heterogeneity in cloud computing.

Infrastructure Organization of CloudLightning

- The architecture of CloudLightning is similar to warehouse scale computer.
- It is composed of cells.
- Each cell composed of different racks.
- Each rack composed of different computational resources.

Hardware Organization of CloudLightning

- Physical server is partitioned into different group based on geographical locations or regions called cells.
- Each cell is composed of heterogeneous computational resources, known as Compute Resource Fabric.
- There are five primary computational hardware are considered .
 - Commodity servers (CPUs)
 - Servers with GPU accelerators.
 - Servers with MIC accelerators
 - Servers with FPGA accelerators
 - Non-uniform Memory Access Scale high-performance computer

Hardware Organization of CloudLightning (contd)

- In conventional data centre, physical racks are used to hold the computational resources.
- The physical racks in conventional data centre has no explicit identity.
- CloudLightning introduces a virtual component called vRacks.
- Each vRacks contains a group of physical servers that share common properties such as hardware types, hardware compatibility and network connection.

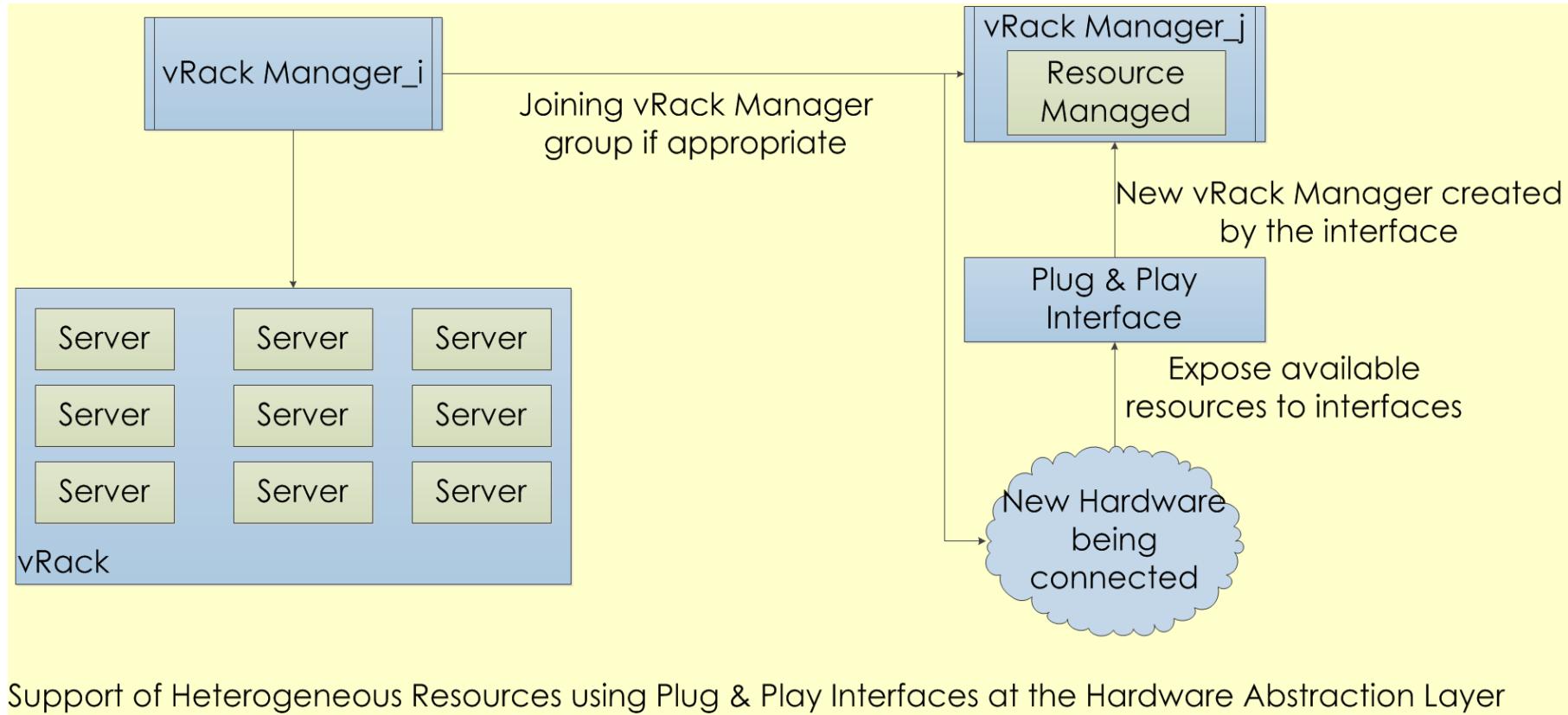
Resource Abstraction in CloudLightning

- The hardware abstraction layer (HAL) provides a logical view of the underlying hardware to the cloud management layer.
- The resources are placed into vRacks by the HAL.
- The initial size of a vRack is determined by the type of the resources to be managed.
- A vRack can also communicate with other vRacks to transfer or pull resources.

Resource Abstraction in CloudLightning (contd)

- A dedicated Plug & Play interface adds new resources to the CloudLightning system.
- The newly added hardware provides its specification to the Plug & Play interface.
- The interface creates CloudLightning specific resource instance (CL-Resources) from the specification of newly added hardware.
- The newly created CL-Resources is attached with a suitable vRack and managed by a designated vRack Manager.

Resource Abstraction in CloudLightning (contd)



Source: Heterogeneity, High Performance Computing, Self-Organization and the Cloud.

Cloud Management Layer of CloudLightning

- In this layer, a cell manager is associated with each cell.
- The cell manager performs the following functions ---
 - Receives Application Requirement documents
 - Acquires CL-Resources
 - User can select resources found by Resource Discovery phase (resource reservation is required).
 - System can also assign appropriate resources according to requirement (resource reservation not required).

Cloud Management Layer of CloudLightning (contd)

- The operations of cloud management layer are divided into following stages --
 - CL-Resource Discovery.
 - The CL-Resource Selection.
 - Resource Acquisition.
 - Coalition Lifecycle Management.

CL-Resource Discovery of Cloud Management Layer

- The CL-Resource discovery is initiated by the cell manager after receiving Application Requirements Document from gateway.
- The Application Requirements Document contains blueprint of service requirements.
- The discovery process ---
 - locate all of the possible CL-Resources that can satisfy specified requirements.
 - Determine the information about the dynamically changing capabilities and capacities of vRack managers.
 - Instructs vRack managers to reserve the resources.
 - Forward the resource discovery information to the resource selection stage.

CL-Resource Selection of Cloud Management Layer

- Determine the resource sets required for fulfilling consumer specified criteria.
- Selects one of resource set which minimizes the overhead of cloud service provider.
- A vRack Manager manages all of the CL-Resources associated its own vRack.
- Each vRack Manager has three functional components ---
 - Resource Acquisition component
 - Coalition Lifecycle Management component
 - Self-Organization Agent .

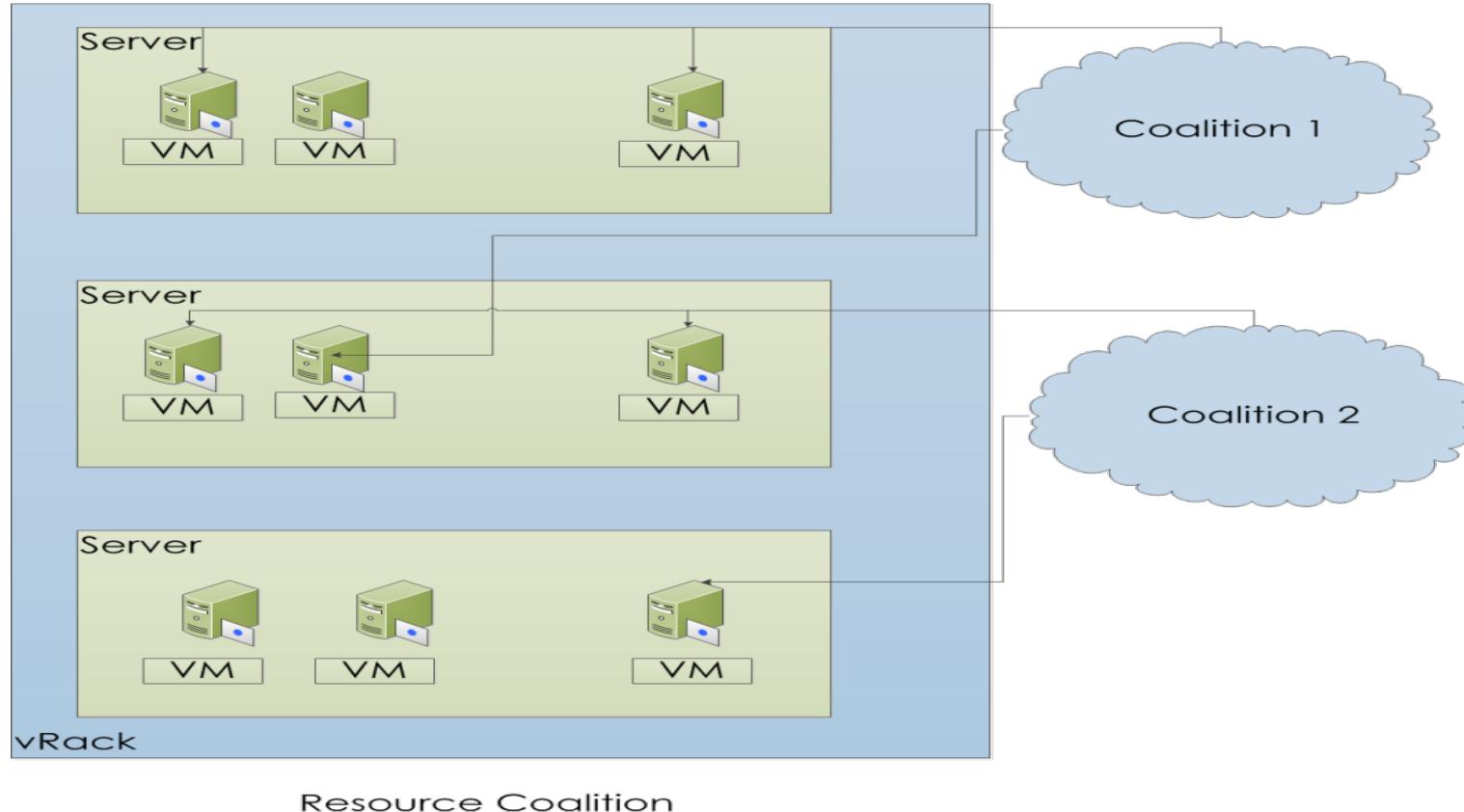
CL-Resource Selection of Cloud Management Layer (contd)

- Resource Acquisition Component— This component is activated by Cell Manager and acquires CL-Resources selected in the CL-Resource Selection stage .
- Coalition Lifecycle Management Component—
- A coalition is a special type of CL-Resource and represents a set of homogeneous set of resources within a single vRack .
- There are two types of Coalition ---
 - Static Coalitions
 - Dynamic Coalitions

CL-Resource Selection of Cloud Management Layer (contd)

- Static Coalitions — The coalition formed by vRack Manager from fixed set of CL-Resource is persistent and called static coalitions.
- Dynamic Coalitions — The vRack Manager constructs dynamic coalitions by dynamically creating some or all CL-Resources.
- A coalitions may exist within a single server or it can span multiple servers.
- If the coalitions spans multiple vRack, then different vRack Manager communicates with adjacent vRack Managers.

CL-Resource Selection of Cloud Management Layer (contd)



Source: Heterogeneity, High Performance Computing, Self-Organization and the Cloud.

CL-Resource Selection of Cloud Management Layer (contd)

- Self-Organization Agent—
 - vRack Managers organize themselves into groups and determine local optimum strategy for CL-Resource management.
 - Self-Organisation Agent maintains data about vRack Managers within a group and exchange local state information within vRack Managers.
 - Exchange power management decision among the servers within a vRack.
 - Helps to migrate servers from one vRack to another vRack.

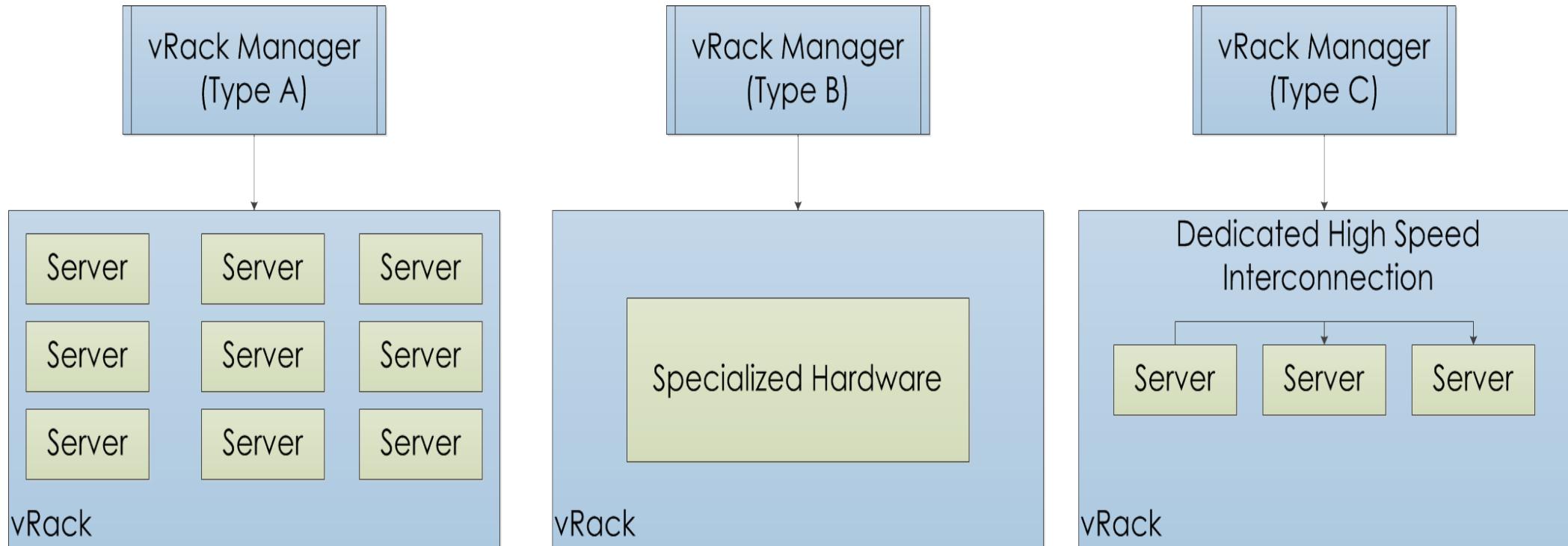
Classification of vRack Managers

- There are three types of vRack Managers —
 - Type-A vRack Managers
 - Type-B vRack Managers
 - Type-C vRack Managers
- Type-A vRack Managers ---
 - Manage a set of homogeneous resources.
 - These managers can be commodity hardware or CPU-GPU pairs or CPU-Data Flow Engine pairs or CPU-MIC pairs.

Classification of vRack Managers (contd)

- Type-B vRack Managers ---
 - are more specialised.
 - Manages a set of HPC machine considered as single CL-Resource.
- Type-C vRack Managers ---
 - Manages a set of hardware resources collocated on a high speed interconnect.

Classification of vRack Managers (contd)



Source: Heterogeneity, High Performance Computing, Self-Organization and the Cloud.

Load Management

Cloud Load Balancing

- The overloaded and underloaded situation in the cloud can cause different system failure and affects the power consumption, execution time.
- The different types of load in cloud are ---
 - Memory load
 - Computation (CPU) load
 - Network load
- The load balancing in cloud may be among physical hosts or VMs.
- The load balancer distributes the dynamic workload among different host or virtual machine.

Performance metrics that effects load balancing

- Expected Time to Compute (ETC) matrix: The distribution of tasks into a set of VM is expressed as ETC matrix. The each entry ETC_{ij} is the ratio between the length of the task i in MIPS to processing speed of VM j .
- Throughput (TP): It denotes the number of user requests or tasks are executed per unit time by a virtual machine. System performance is proportional to throughput of the system.
- Thrashing (TH): In a cloud environment thrashing occurs when a number of VMs are spending more time in migration than executing.

Performance metrics that effects load balancing

- Accuracy: It determines the perfection of task execution.
- Predictability: It is the degree used for the prediction of task allocation, task execution, and task completion according to the available cloud resources (virtual machines). The better prediction improves the load balancing performance of the cloud computing.
- Scalability: It is the capability of the system to perform under unexpected circumstances and a measure of load balancing performance of the cloud when system load increases. In a scalable cloud system, rescaling is done at regular intervals.
- Makespan: It is the total time required to complete all tasks submitted to the system. Makespan of the system is the maximum time taken by the host running over the data center.

Performance metrics that effects load balancing

- Migration time: It is the time to migrate a task from one VM to another. The migration can be from one VM to another within a single host or different hosts.
- Associated Cost: The associated cost depends on the resource utilization. The cloud user tries to depreciate the cost of resource provisioning by degrading the on-demand resource cost and over-subscribed resource cost of over-provisioning and under-provisioning.
- Energy Consumption: It is the amount of energy consumption to execute load balancing algorithms on different resources.

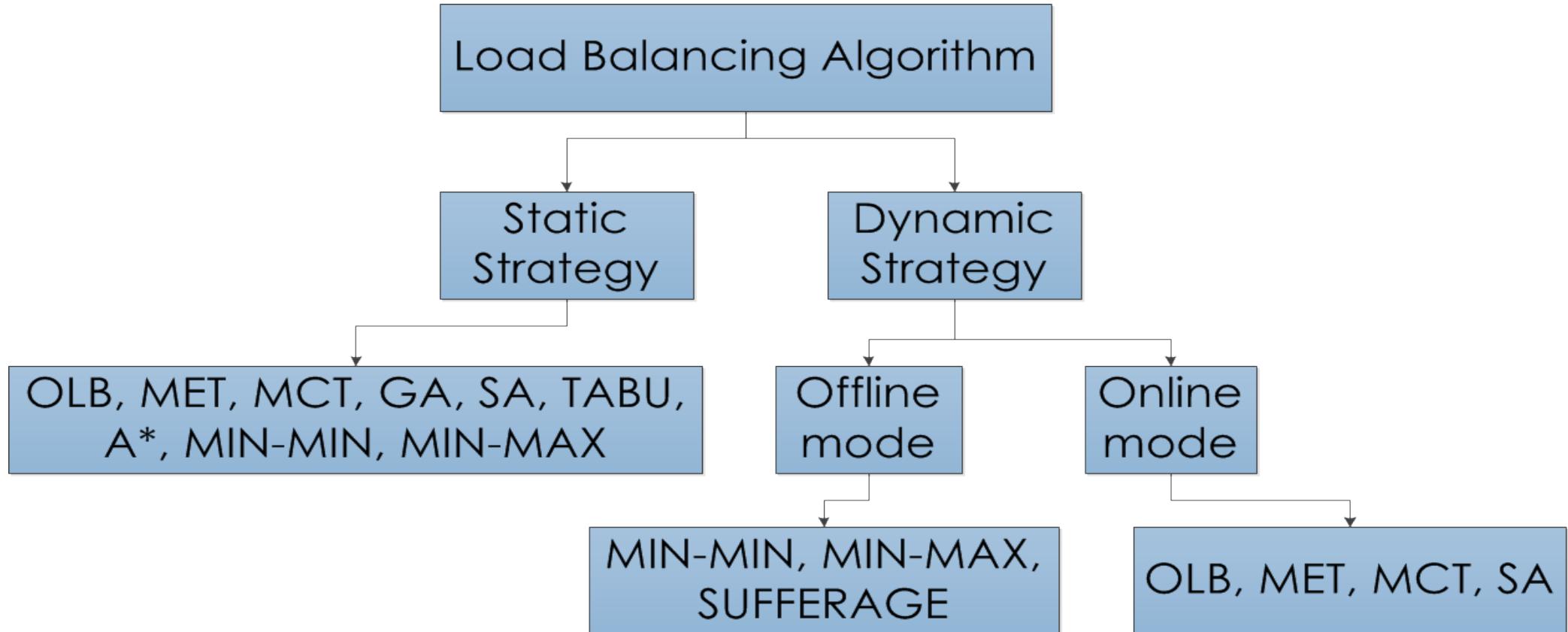
Classification of Load Balancing Algorithm

- The task allocation algorithm in cloud depends on the current state of the VM.
- The load balancing algorithms make a fair allocation of resources.
- The objectives of the load balancing are twofold—
 - achieve a high user satisfaction.
 - improve the stability of the system.
- Resource management plays a major role in the cloud load balancing algorithm.

Classification of Load Balancing Algorithm

- The multi-objective load balancing in cloud is NP-complete problem.
- The objectives of the load balancing algorithms are ---
 - Energy saving
 - Makespan minimization
 - Throughput maximization
- Load balancers are used for load balancing in cloud.
- Researchers use different types of heuristic for load balancing in cloud.

Heuristic Strategies of Load Balancing in Cloud



Source: Load balancing in cloud computing: A big picture

Heuristic Strategies of Load Balancing in Cloud (contd)

- Static Strategies: The static strategies in cloud uses two assumptions—
 - Initial task arrival.
 - Availability of physical machines at the beginning.
- The resource updates in these strategies are done after the task allocations.
- Examples of static strategies are OLB, MET, MCT, GA, Switching Algorithm, TABU, A algorithm, Min-Min, Min-Max.

Heuristic Strategies of Load Balancing in Cloud (contd)

- Dynamic Strategies: In these strategies, load distribution is done at runtime. Dynamic strategies are classified into two types ---
 - Off-line mode (Batch mode)
 - On-line mode.
- Batch Mode Dynamic Strategies --- In these strategies,
 - task is allocated only at predefined time.
 - It is used to measure the execution time of a set of tasks.
 - Examples are --- Max–min, Min-min, Sufferage algorithm.

Heuristic Strategies of Load Balancing in Cloud (contd)

- Online or Immediate mode Dynamic Strategies --- In this strategies,
 - task is allocated to a computing node as soon as it arrives at the scheduler.
 - Each task is scheduled only once.
 - Examples are --- OLB, MET, MCT, SA.
- OLB (Opportunistic load balancing): OLB heuristic used in both static and dynamic strategies.
 - This heuristic initially selects a machine randomly, allocates the task and then finds next available machine.
 - In online mode, a task is allocated to a VM based on different parameters such as execution time.

Heuristic Strategies of Load Balancing in Cloud (contd)

- OLB (Opportunistic load balancing):
 - The task execution is done at VM level.
 - In online mode, a task is allocated to a VM based on different parameters such as execution time.
 - The advantage of OLB is to increase host machine utilization for better efficiency and proper load balancing.
 - The disadvantage of OLB is poor make-span when multiple objectives are considered simultaneously.

Heuristic Strategies of Load Balancing in Cloud (contd)

- MET (Minimum Execution Time):
 - This heuristic technique used in both static and dynamic (Online mode) strategy.
 - This strategy maps each task to VM.
 - The scheduler allocates each task according to lowest execution time.
 - It tries to enhance the make-span of the system through balancing of cloud resources.
 - The disadvantage of this algorithm is not to consider machine ready time. It also shows load variations in machines.

Heuristic Strategies of Load Balancing in Cloud (contd)

- MCT (Minimum Completion Time):
 - It is used in both static and dynamic (Online mode) strategy.
 - This strategy maps each task to VM.
 - It uses ready-to-execute time and the expected execution time of the tasks for load balancing.
 - It allocates the task in the machine which has least completion time.

Heuristic Strategies of Load Balancing in Cloud (contd)

- Min-Min:
 - The basic Min-Min selects minimum size task and chooses a cloud resource (VM) that has the minimum capacity.
 - This algorithm uses a queue for task allocation. After allocating a task from queue it is removed from queue and next task is allocated.
 - It is suitable for small scale distributed system.
 - The improved Min-Min algorithm not only optimizes the load, but also optimizes the make-span and resource utilization.

Heuristic Strategies of Load Balancing in Cloud (contd)

- Load Balanced Improved Min-Min:
 - In Load Balanced Improved Min-Min (LBIMM) algorithm, tasks are first partitioned into two groups—group A and B.
 - Group A tasks are of higher priority.
 - Group B tasks are of lower priority.
 - Scheduler first schedules group A tasks and then group B tasks.
 - The load balancing algorithms balance the load of different machines after tasks allocation.

Heuristic Strategies of Load Balancing in Cloud (contd)

- Min-Max:
 - The basic Min-Max algorithm selects the task with larger size and chooses a cloud resource (VM) that has the minimum processing capacity.
 - This algorithm uses a queue for task allocation. After allocating a task from the queue it is removed from queue and the next task is allocated.
 - It is suitable for small scale distributed system.
 - The augmented Max–Min algorithm keeps a task status table and expected completion time of tasks.

Heuristic Strategies of Load Balancing in Cloud (contd)

- Genetic Algorithm (GA):
 - GA algorithm is population and chromosome based.
 - The fitness value of the chromosome are energy consumption, make-span and throughput.
 - The basic steps are selection, crossover and mutation.
 - In load balancing the total number of tasks arrived at the system are considered as chromosome.

Heuristic Strategies of Load Balancing in Cloud (contd)

- Simulated annealing (SA):
 - This type of algorithm is used to solve unconstrained and bound-constrained optimization problems.
 - At each iteration, a new point is generated based on some probability distribution.
 - It avoids local minima and finds the global optimized solution.
 - In load balancing, this algorithm is used to map the jobs with resources.

Heuristic Strategies of Load Balancing in Cloud (contd)

- Tabu Search (TS):
 - It is a meta-heuristic based solution.
 - This method uses adaptive memory that performs a more elastic search behavior.
 - The algorithm effectively handles 500 nodes and 1000 data center locations.

Heuristic Strategies of Load Balancing in Cloud (contd)

- A-star Search:
 - A-star search algorithm is extensively applied as a graphic searching algorithm.
 - This heuristic algorithm combines the benefits of both depth-first search and breadth-first search algorithm.
 - It supports two lists, the first list act as a priority queue of the tasks and the second list has the processing capacity of all VMs.
- Switching Algorithm:
 - This algorithm is used in the cloud environment for the migration of tasks or VMs.
 - Using this method, we can achieve the fault tolerant property.

Storage Access Protocols

Types of Cloud Storage

- Cloud Storage type is classified into two types—
 - Unstructured storage types
 - Structured key-value store
- Message Queues are temporary storage structure to store the messages passed among multiple cloud applications. E.g. Microsoft MSMQs, IBMs MQ series etc.
- Block devices are like traditional storage type and store bytes in sequential order.
- Cloud Applications can format block devices according to their requirements.

Types of Cloud Storage (contd)

- RDBMS store is a cloud storage, similar to traditional RDBMS storage.
- In RDBMS store, cloud applications can use SQL server instances hosted in the cloud infrastructure.

Storage Type	AWS	Windows Azure	Google AppEngine
Unstructured	yes	yes	yes
Structured	yes	yes	yes
Message queues	yes	yes	yes
Block Devices	yes	yes	No
RDBMS	yes	yes	No

Unstructured Storage Types

- It is similar to traditional file system but the logical view is different from simple sequence of bytes.
- Cloud storage service providers offer read/write based unstructured storage types.
- This storage type can include files up to size 1 TB.
- It provides different interfaces for doing IO.
- Examples are Amazon Web Services (AWS), Windows Azure, and Google Blobstore.

Amazon Simple Storage Service

- Simple Storage Service (S3) is one of the earliest storage service providers in the cloud.
- S3 consists of buckets and objects and under one storage account buckets and objects are created.
- Buckets are like directories, and each of them may have one or more objects.
- The maximum size of each S3 object is 5GB and access is sequential in nature.

Amazon Simple Storage Service (contd)

- Buckets in S3 can not be nested and only provides two level of hierarchy.
- The naming of a bucket is unique within a storage account.
- The naming of an object is unique with respect to a bucket or the account where the object is created.
- Moving or renaming an object is supported via copying.
- Objects are write once, means that once written, they cannot be updated in place.
- The objects can have multiple versions and redo and undo operation is permitted on the objects.

Amazon Simple Storage Service (contd)

- The high availability of Objects are done by replication.
- S3 does not have locking for multiple writes, which results in lack of synchronization.
- S3 provides resume-able downloads and integration with the Bit-torrent protocol.
- It also does not encrypt data stored in objects.
- Consumer is responsible for encryption and decryption of data.
- S3 provides Bucket Grant policies and specialized signed URI for the consumers.

List of Operations Support in Amazon S3

Operation	Description
Create Bucket	Create a new bucket.
Delete Bucket	Delete a bucket. Only an empty Bucket can be deleted.
List Buckets	List the buckets that are defined in a single storage account.
Get Bucket Policy	Retrieve the policy associated with the Bucket.
Set Bucket Policies	Set user defined bucket policies.

List of Operations Support in Amazon S3

Operation	Description
Get Bucket ACL	Get the bucket Access Control List as defined.
Set Bucket ACL	Set the bucket Access Control List.
List Objects	List the objects in a given bucket.
Put Object	Create or update an object with a new version.
Post Object	Create or update an object with a specific version.

Windows Azure Blob Storage

- Windows Azure blob store is provided through Windows blob account.
- A user can create one or more account and within each account one or more container can be created to store data.
- Containers are like directories and under one container one or more blob storage can be created.
- There are two different types of blob storage --- block blobs and page blobs.
- In a block blob, each blob is composed of a finite number of blocks and maximum size of a block is 4 MB.

Windows Azure Blob Storage

- The maximum size of a block blob can be 200 GB and the blocks of a blob may have different sizes.
- The access of a block blob is sequential and immutable.
- A page blob consists of a sequence of pages each of which has a fixed size of 512 KB.
- The maximum size of a page blob can be 1 TB and supports random access read and write.
- The communication to the storage system can be secured using HTTPS instead of HTTP.

List of Operations Support in Windows Azure Blob Storage

Operation	Description
List Container	List the containers that are defined in a single storage account.
Create Container	Create a new container. A container can only be created underneath a storage account. Nesting of containers is not supported.
Delete Container	Delete a container and the blobs.
Get Container ACL	Get the container Access Control List as defined.

List of Operations Support in Windows Azure Blob Storage

Operation	Description
Set Container ACL	Set the container Access Control List.
List Blobs	List the blobs in a given container.
Put Blob	Create a new blob (block or page).
Put Block	Create a new block.
Put Block List	Create a new block list or replace the old block list of a block blob.
Get Block List	Get block list of a particular blob.
Put Page	Create a new set of page ranges or delete a range.

List of Operations Support in Windows Azure Blob Storage

Operation	Description
Copy Blob	Copy a blob to a new blob in the same account.
Delete Blob	Delete a blob.
Lease Blob	Request for an exclusive one minute lease lock for the blob.
Snapshot Blob	Create a new read only snapshot copy of the blob.

Google BlobStore

- Google's BlobStore stores unstructured data.
- HTTP Post request is used to generate a blob and it supports flat namespace.
- Under a single account, a blob is unique.
- Each blob has binary data and a metadata and after successful completion of storing a blob, AppEngine returns an opaque key to access the blob.
- The metadata of a blob, accessible using the blob key, is stored in Google DataStore from where different properties of the blob can be retrieved.

Google BlobStore

- Each blob stored in the blob storage is immutable.
- Java and python libraries are provided to create and access a blob.
- The maximum size of a blob can be 2 GB.

List of Operations Support in Google BlobStore

Operation	Description
Create Blob	Create a blob in the user App- Engine account.
Delete Blob	Delete a blob.
Fetch Data	Retrieve a range of bytes from a blob.
Fetch Blob Key	Fetch Blob Key.

Structured Key-Value Pair

- In this storage an object is a collection of pair <key, value>, where key is used to access the value.
- This storage does not support any schema.
- The set of objects are grouped to create a complex objects.
- Examples are Amazon's SimpleDB and Microsoft Azure's Table.

Amazon SimpleDB

- The data model of SimpleDB consists of domain which represents collection of objects known as items.
- Each item consists of set of attributes.
- In every item within a domain, a key is defined which is unique across all the items in the same domain.
- In SimpleDB, the maximum size of each domain is 10 GB.
- Each item is replicated across a set of nodes in an Amazon data centre.
- SimpleDB provides REST and SOAP interfaces.

Windows Azure Table

- It has three levels --- tables, entities and properties.
- Properties are represented by key, value pair.
- The maximum size of an entity can be up to 1 MB and the maximum number of properties are 256.
- The first two mandatory properties are partition key and row key.
- Partition key is used to partition the entities within the same table.
- Within a single partition, row key is used to identify a single entity.
- System generates timestamp when a new entity is created.

Functions and Benefits of the Services and Storage

Benefits of Cloud Storage

- Usability and accessibility --- User can drag and drop the files in cloud storage similar to local storage and stored file can be accessed from anywhere with internet connection.
- Disaster Recovery --- In cloud storage, a backup is maintained for the stored data which helps to recover the data in case of failure of local storage.
- Security --- Cloud Service provider implements different types of security policy to protect the privacy of the data.

Benefits of Cloud Storage

- Cost Savings --- Business owners can save money by storing data into cloud storage instead of investing to acquire data store.
- Easy Sharing --- Data stored in cloud can be shared easily.
- Automation --- Consumer can store and maintain data with minimal human intervention.
- Synchronization --- Data stored in cloud can be automatically synchronized with the data stored in local storage.

References

- Cloud Computing: Principles and Paradigms, Editors: Rajkumar Buyya, James Broberg, Andrzej M. Goscinski, Wiley, 2011.
- Cloud Computing Bible, Barrie Sosinsky, Wiley-India, 2010.
- Heterogeneity, High Performance Computing, Self-Organization and the Cloud, Editors: Theo Lynn, John P. Morrison, David Kenny, Springer, 2018.
- H. Dewan and R. C. Hansdah, "A Survey of Cloud Storage Facilities," *2011 IEEE World Congress on Services*, Washington, DC, 2011, pp. 224-231, doi: 10.1109/SERVICES.2011.43.
- S. K. Mishra, B. Sahoo, and P. P. Parida, "Load balancing in cloud computing: A big picture," *Journal of King Saud University – Computer and Information Sciences*, vol. 32, no. 2, pp. 149–158, 2020.
- https://en.wikipedia.org/wiki/Cloud_computing
- <http://www.cs.cmu.edu/~garth/15719/lectures/15719-S17-multilevel-scheduling-comb.pdf>
- <https://www.milesweb.in/blog/hosting/cloud/10-benefits-data-storage-cloud>

Thank You!!!