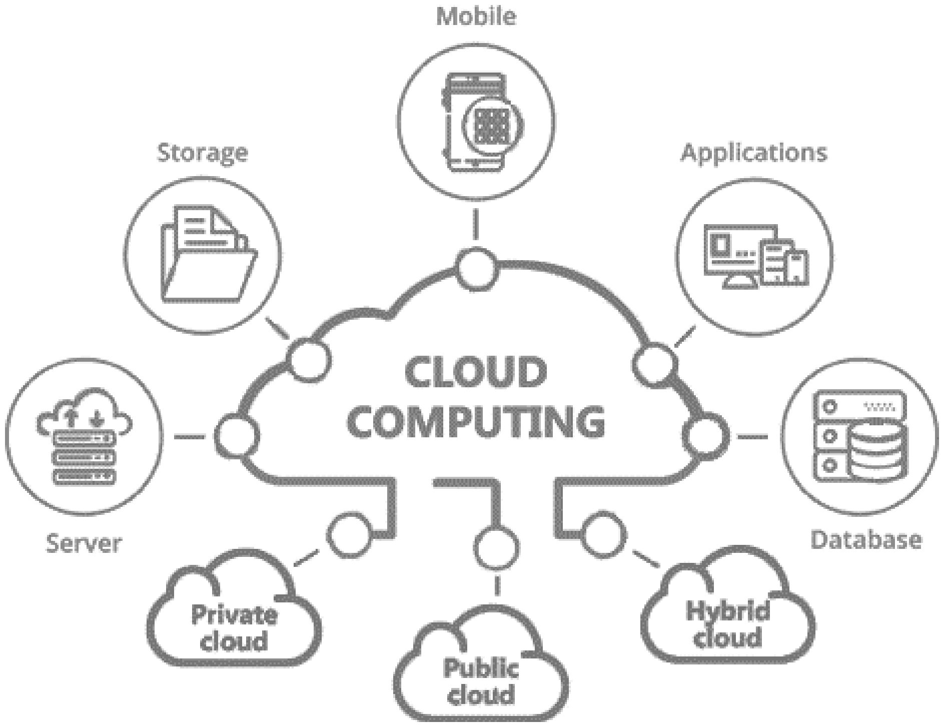
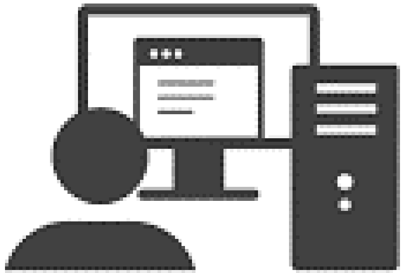
Unit-4

Cloud for IoT

Introduction to Cloud Computing

- Cloud computing is the delivery of computing services over the internet, by providing flexible, affordable, effective and efficient resources for development.
- That includes servers, storage, databases, networking, software, analytics, and intelligence.
- Cloud computing provide economical freedom along with technical strength to the application.
- In other word, it is about outsourcing of IT services and infrastructure to make them available anywhere via the Internet.

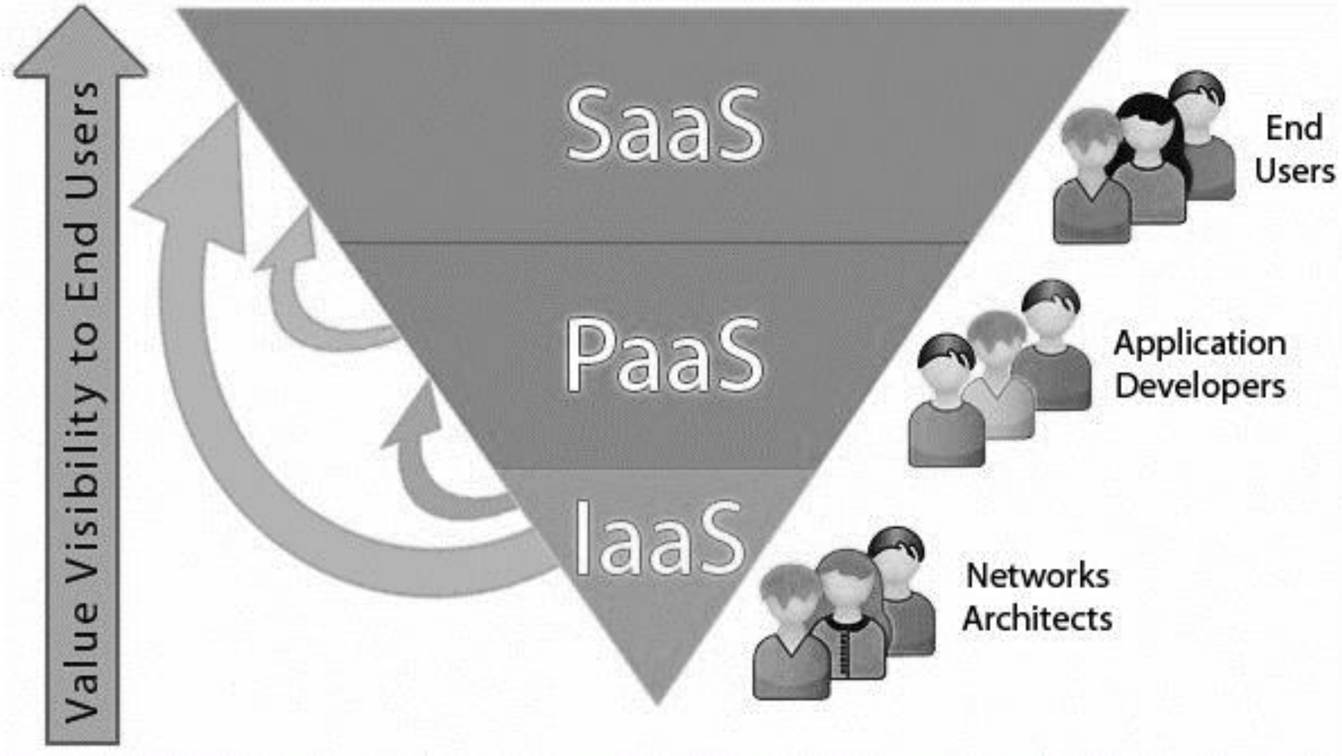




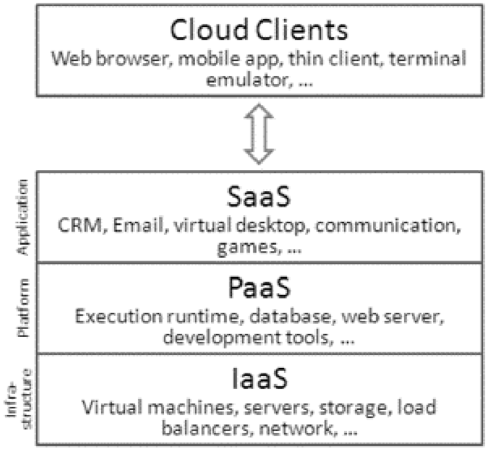
Application logic runs on user’s computer

Application logic runs in the cloud

Service Models of Cloud Computing



- There are **three** main service models of **cloud computing** – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).
- Each model represents a different part of the cloud computing stack.
- Each type of cloud service provides you with different levels of control, flexibility, and management.



Cloud Clients

Web browser, mobile app, thin client, terminal emulator, ...

Application

SaaS

CRM, Email, virtual desktop, communication, games, ...

Platform

PaaS

Execution runtime, database, web server, development tools, ...

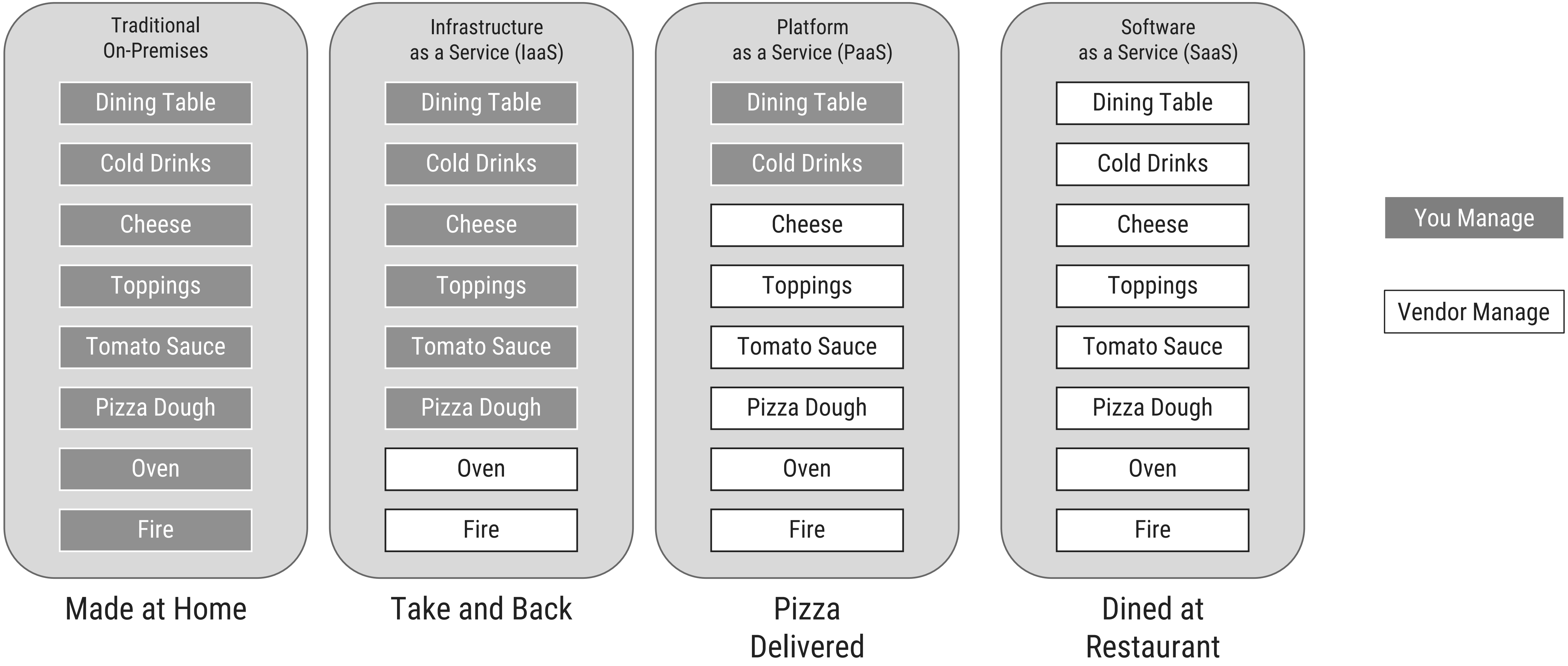
Infra-structure

IaaS

Virtual machines, servers, storage, load balancers, network, ...

Example of “as a Service”

Pizza as a Service

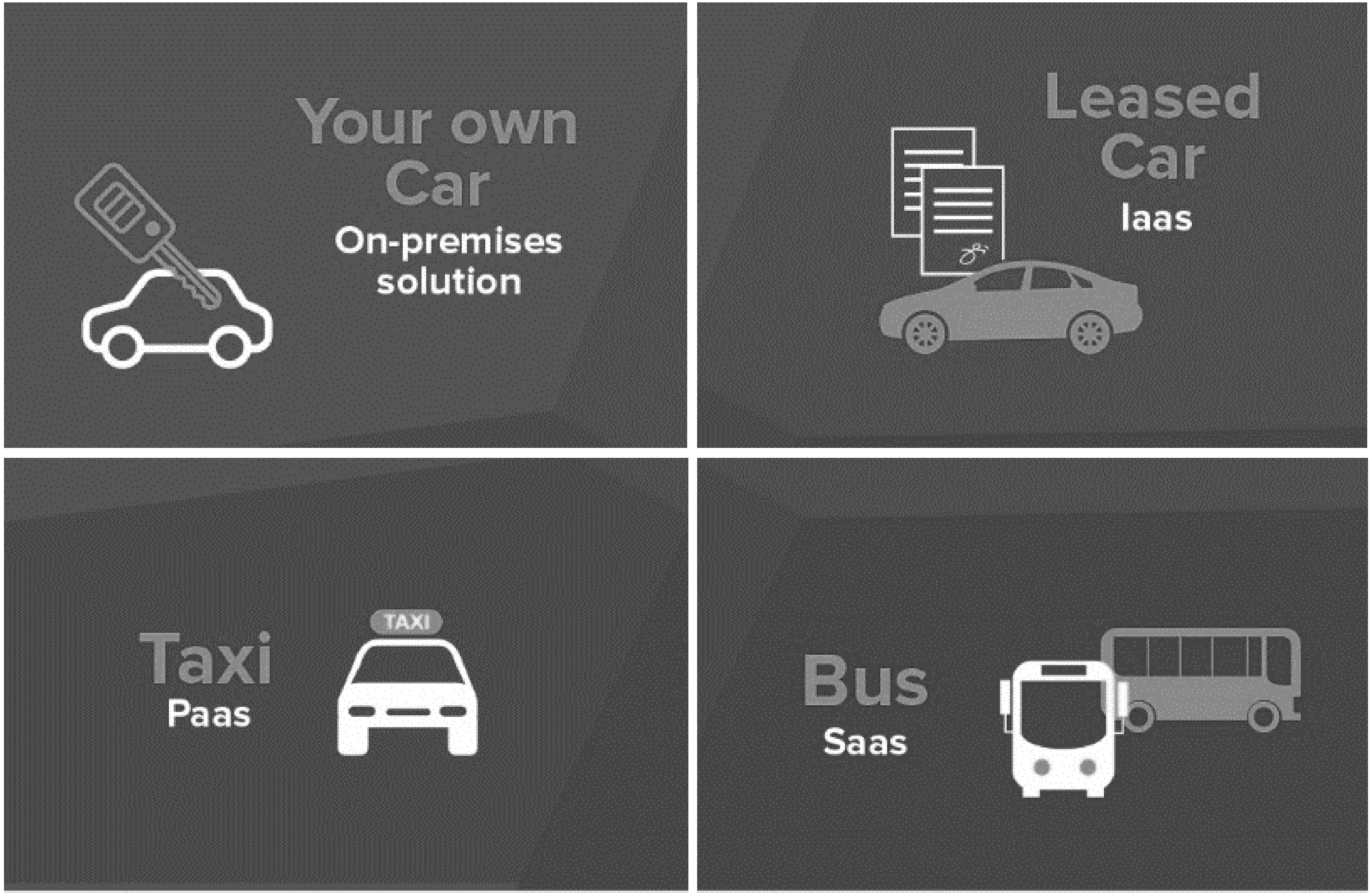


Traditional On-Premises	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
▨ Dining Table	▨ Dining Table	▨ Dining Table	□ Dining Table
▨ Cold Drinks	▨ Cold Drinks	▨ Cold Drinks	□ Cold Drinks
▨ Cheese	▨ Cheese	□ Cheese	□ Cheese
▨ Toppings	▨ Toppings	□ Toppings	□ Toppings
▨ Tomato Sauce	▨ Tomato Sauce	□ Tomato Sauce	□ Tomato Sauce
▨ Pizza Dough	▨ Pizza Dough	□ Pizza Dough	□ Pizza Dough
▨ Oven	□ Oven	□ Oven	□ Oven
▨ Fire	□ Fire	□ Fire	□ Fire
Made at Home	Take and Back	Pizza Delivered	Dined at Restaurant

▨ You Manage

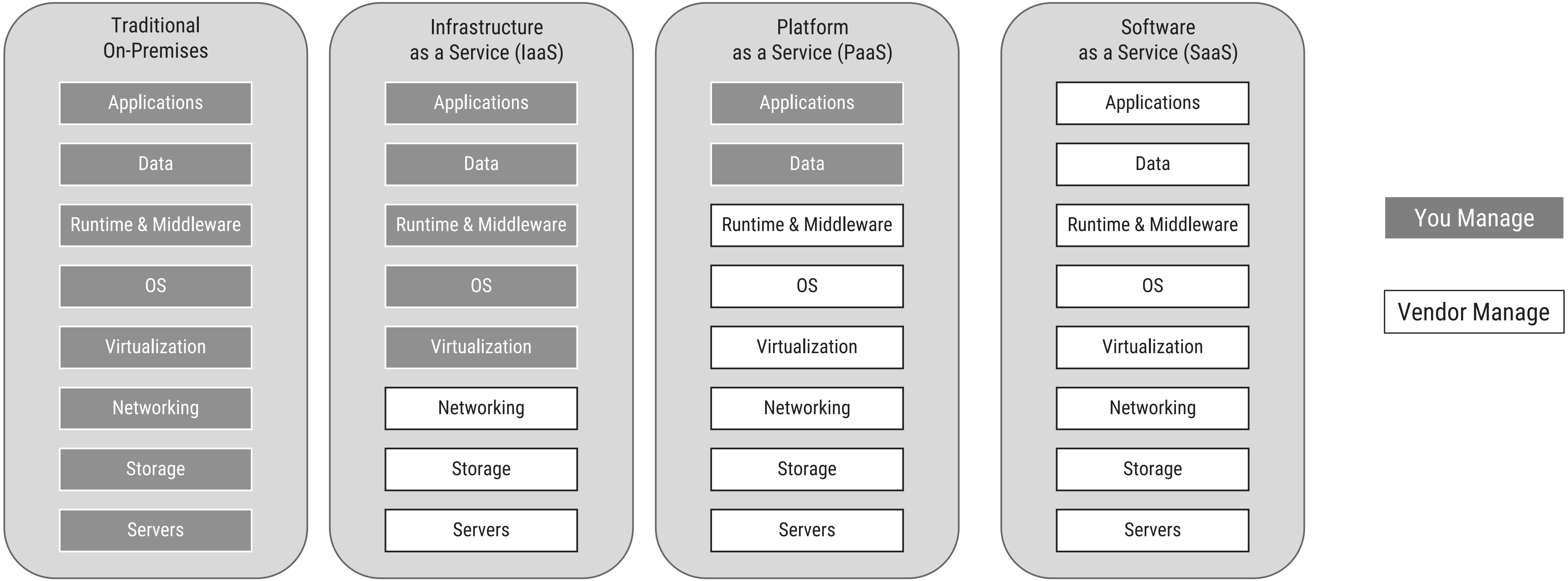
□ Vendor Manage

Example of “as a Service”



Vehicle as a Service

Cloud Services



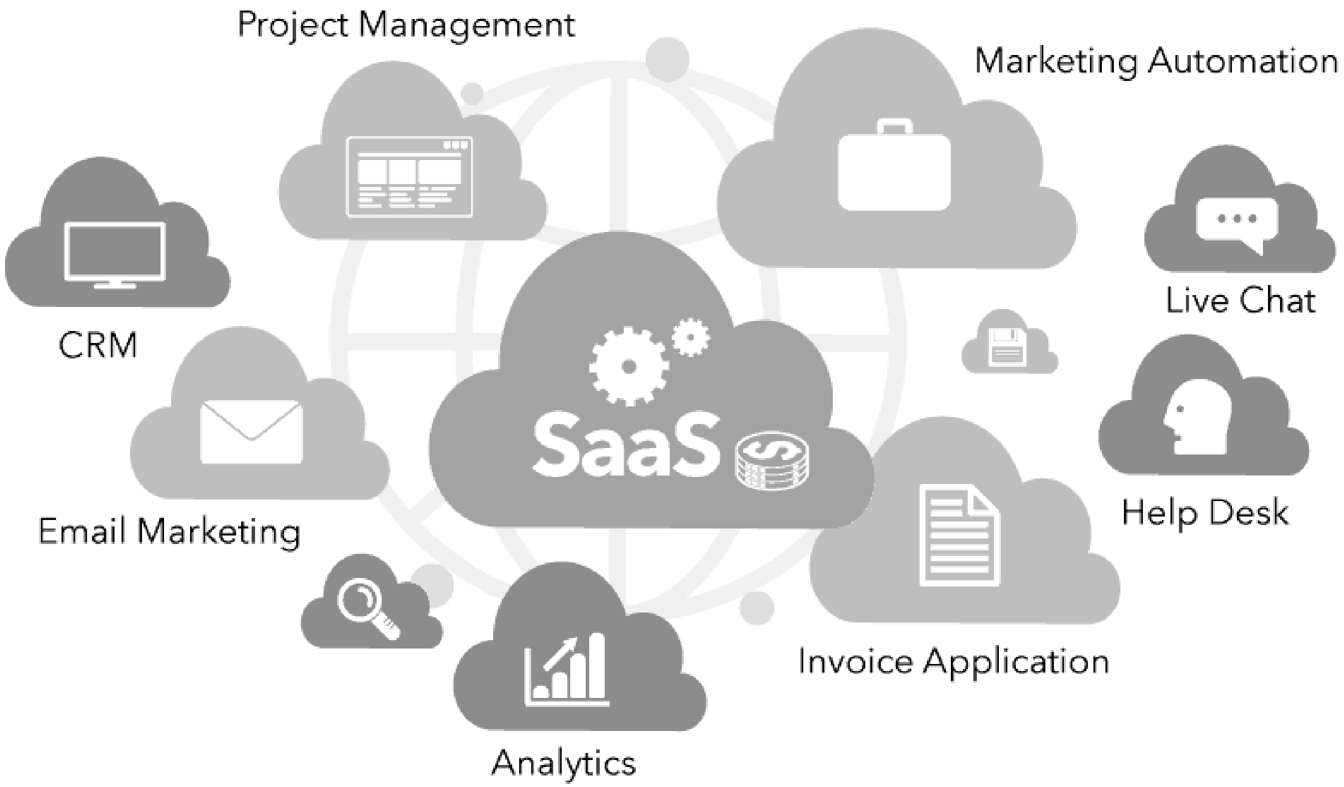
	Traditional On-Premises	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Applications	▨	▨	▨	□
Data	▨	▨	▨	□
Runtime & Middleware	▨	▨	□	□
OS	▨	▨	□	□
Virtualization	▨	▨	□	□
Networking	▨	□	□	□
Storage	▨	□	□	□
Servers	▨	□	□	□

▨ You Manage

□ Vendor Manage

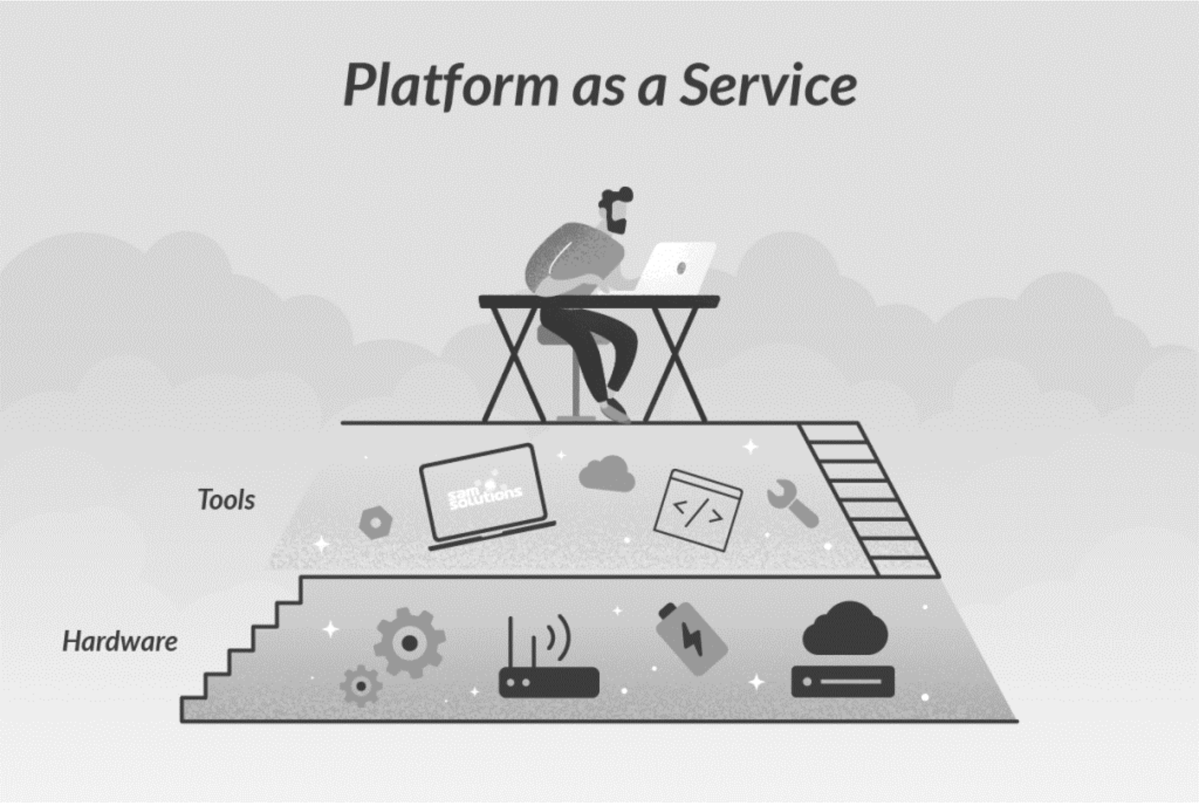
Software-as-a-Service (SaaS)

- Complete software application as a service is provided to the user that is run and managed by the service provider.
- It can also be called application as a service as a pay monthly, yearly etc. subscription.
- In SaaS, user don't need to worry about software upgradation and management.
- A common example of a SaaS application is web-based email where you can send and receive email without having to manage the server that the email program is running.



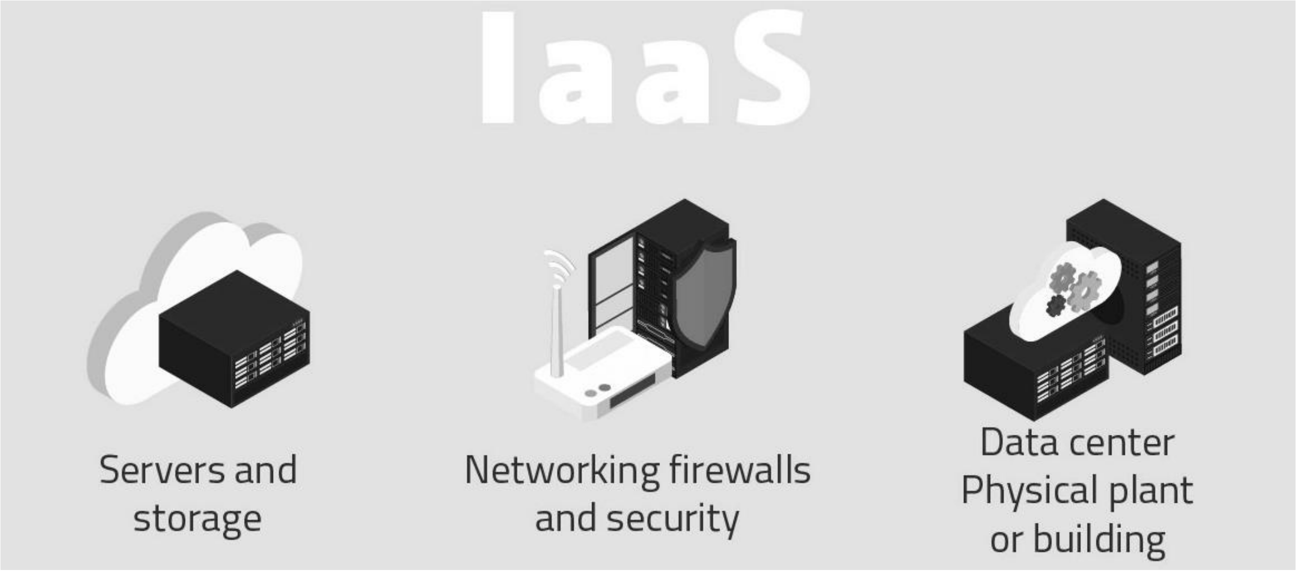
Platform-as-a-Service (PaaS)

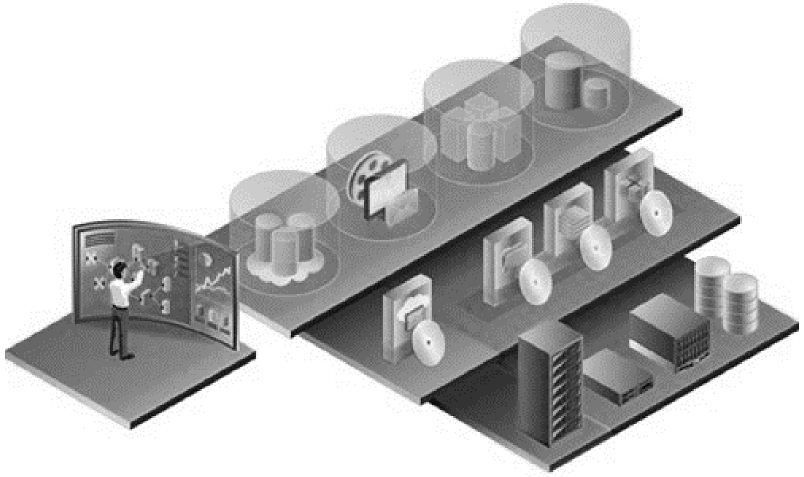
- It provides a development environment to application developers.
- Operating system, programming-language execution environment, database, web server, development tools, APIs, libraries, etc., will be provided by the cloud service provider.
- Users have to build, manage and maintain the applications.
- Application developers develop and run their software on a cloud platform instead of directly buying and managing the essential hardware and software layers.
- AWS Lambda, Google App Engine, IBM Cloud Foundry, Oracle Cloud Platform, Red Hat OpenShift, Zoho Creator.



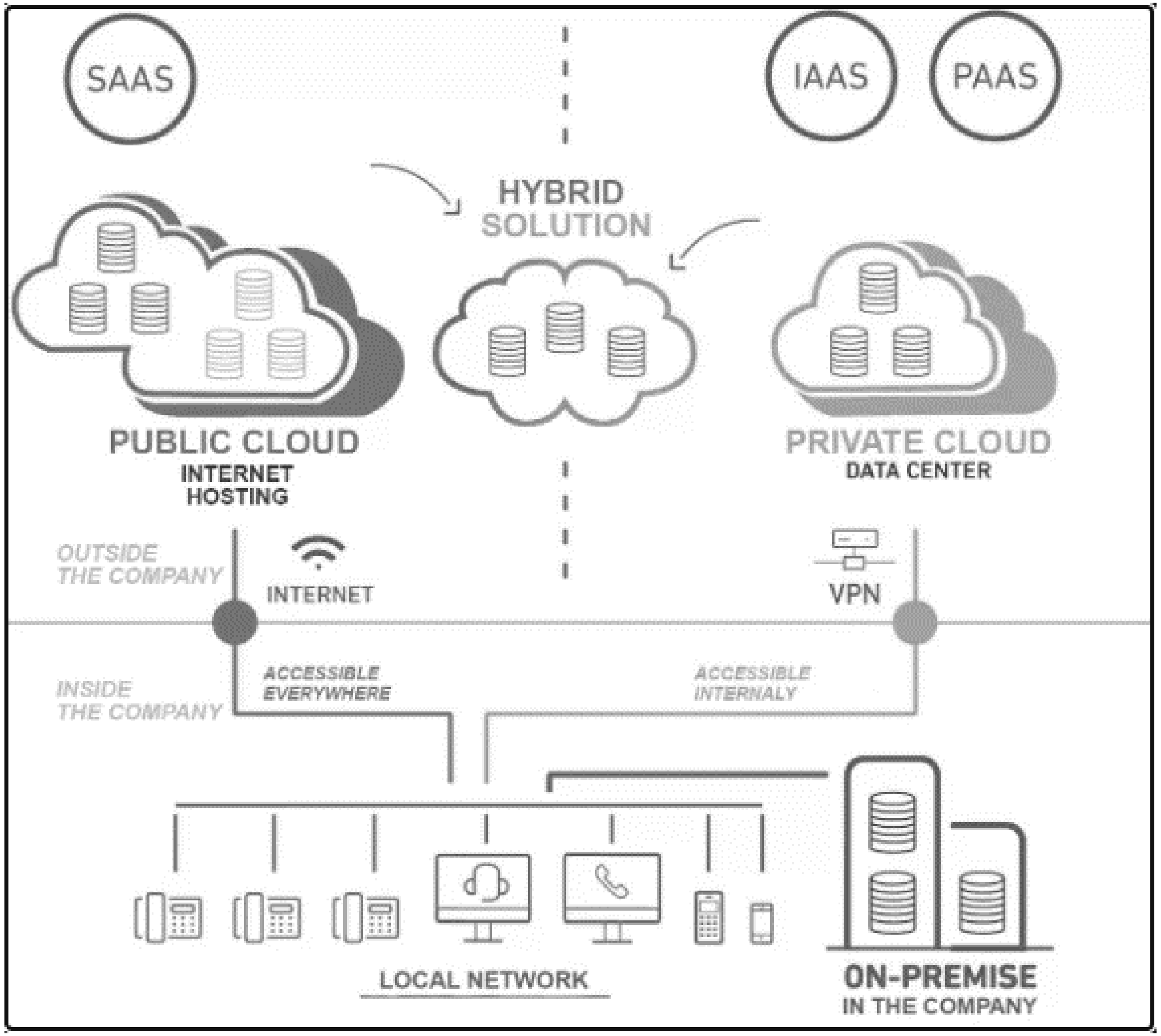
Infrastructure-as-a-Service (IaaS)

- IaaS provides access to computing hardware, networking features, and data storage space.
- Where the consumer is able to deploy and run 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
- This service provides you with the highest level of flexibility.


IaaS
Servers and storage
Networking firewalls and security
Data center Physical plant or building



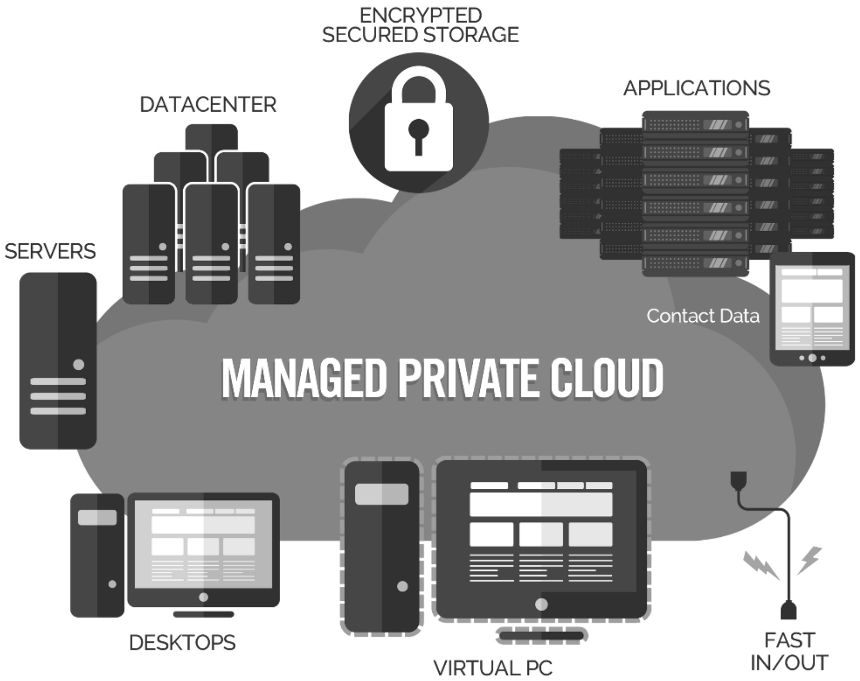
Deployment Models of Cloud Computing



- Deployment models of cloud computing are categorized based on their location as public, private or hybrid cloud
- It is often possible to choose a geographic area to put the data “closer” to users.
- More the money you pay, better in comfort and service

Private Cloud

- Private cloud provides computing services within the organization’s private network and selected other users.
- In this cloud model all the hardware, software, datacenter, employees, infrastructure, etc., are maintained, monitored, and installed by the organization.
- This particular deployment model can be chosen wherever confidentiality matters the most.
- Advantages
  - High level of security and privacy
  - More control flexible in terms of deciding and managing the resources
- Disadvantages
  - Very Expensive
  - Need technical skill for maintaining and difficult to management
  - Policies and other related things are to be framed carefully to make sure that the data is safe

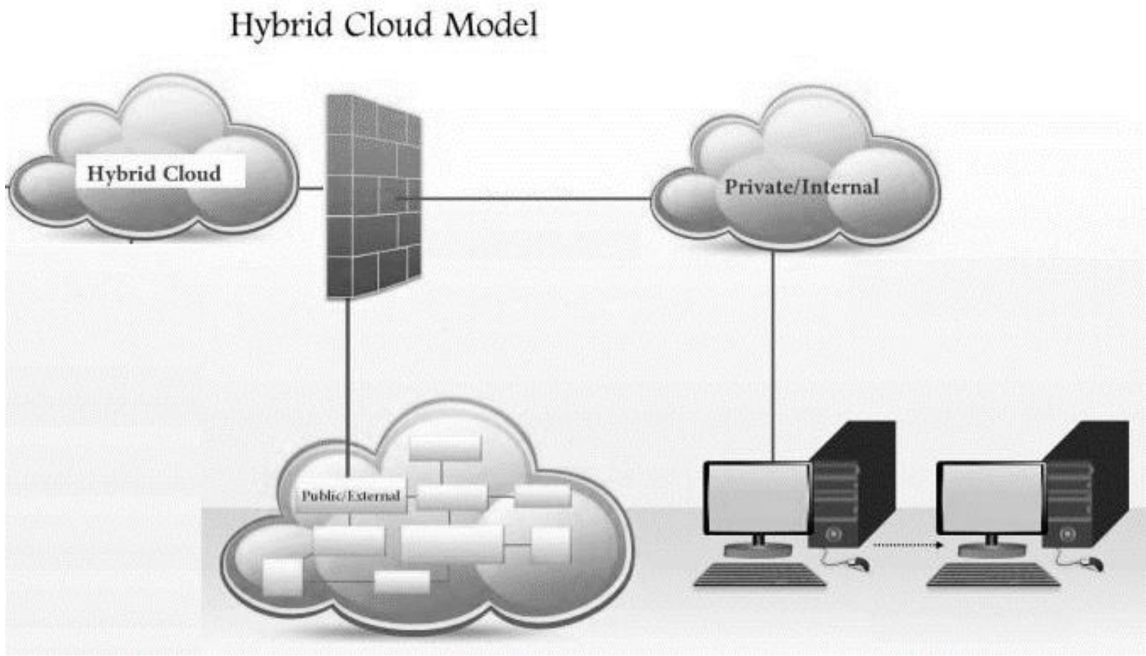


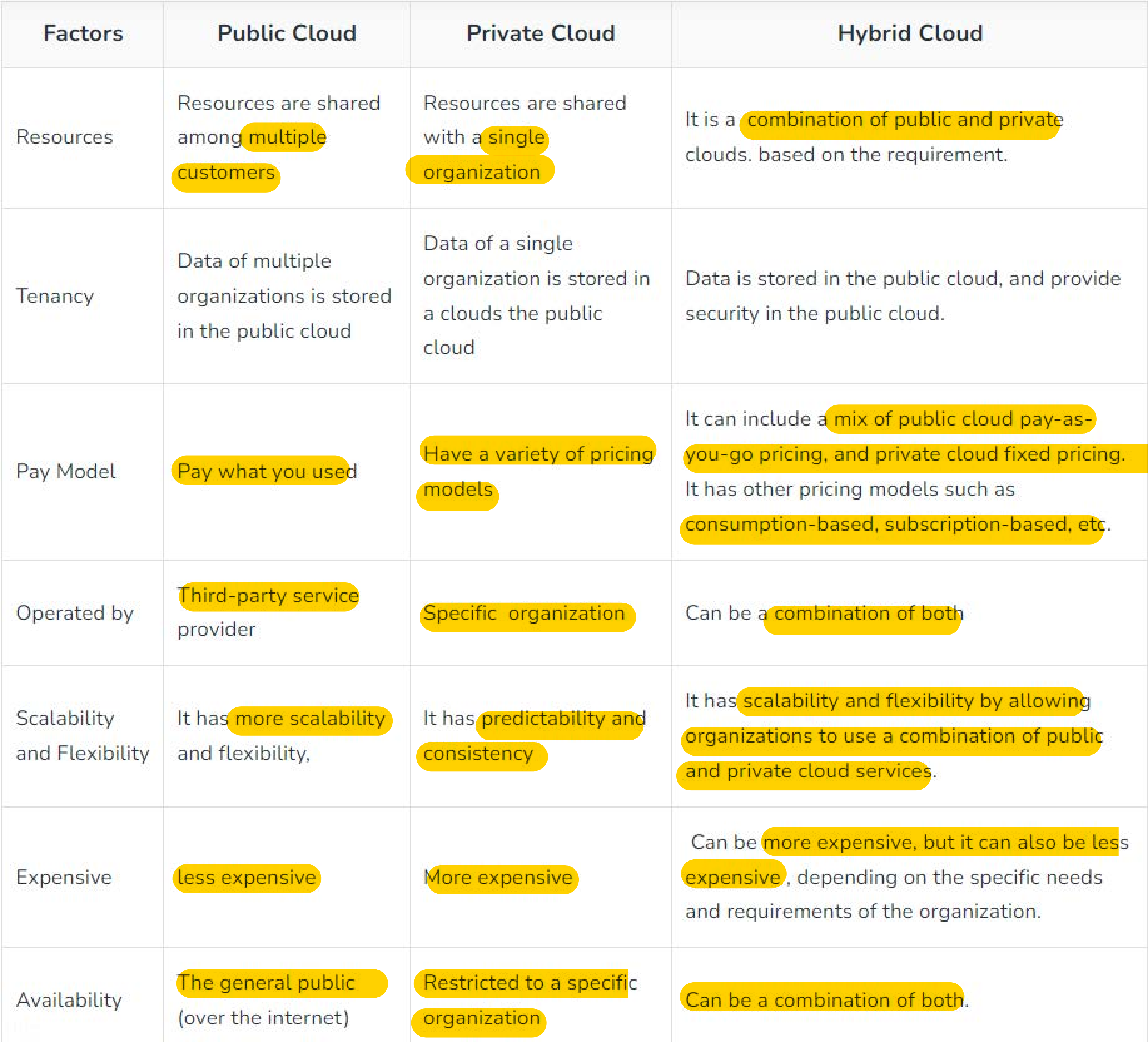
Public Cloud

- The cloud resources are owned and managed by a third-party cloud service provider.
- Pay as per usage approach makes it most cost effective model.
- Advantages
  - Inexpensive model, no need to invest in setting up the infrastructure and maintenance
  - Less technical skill required
  - Customer support team can be reached on demand
  - Easily scaled up or scaled down based on requirements
  - High reliability—a vast network of servers ensures against failure.
- Disadvantages
  - Security and privacy issues are the major challenges
  - Less flexibility and controls

Hybrid Cloud

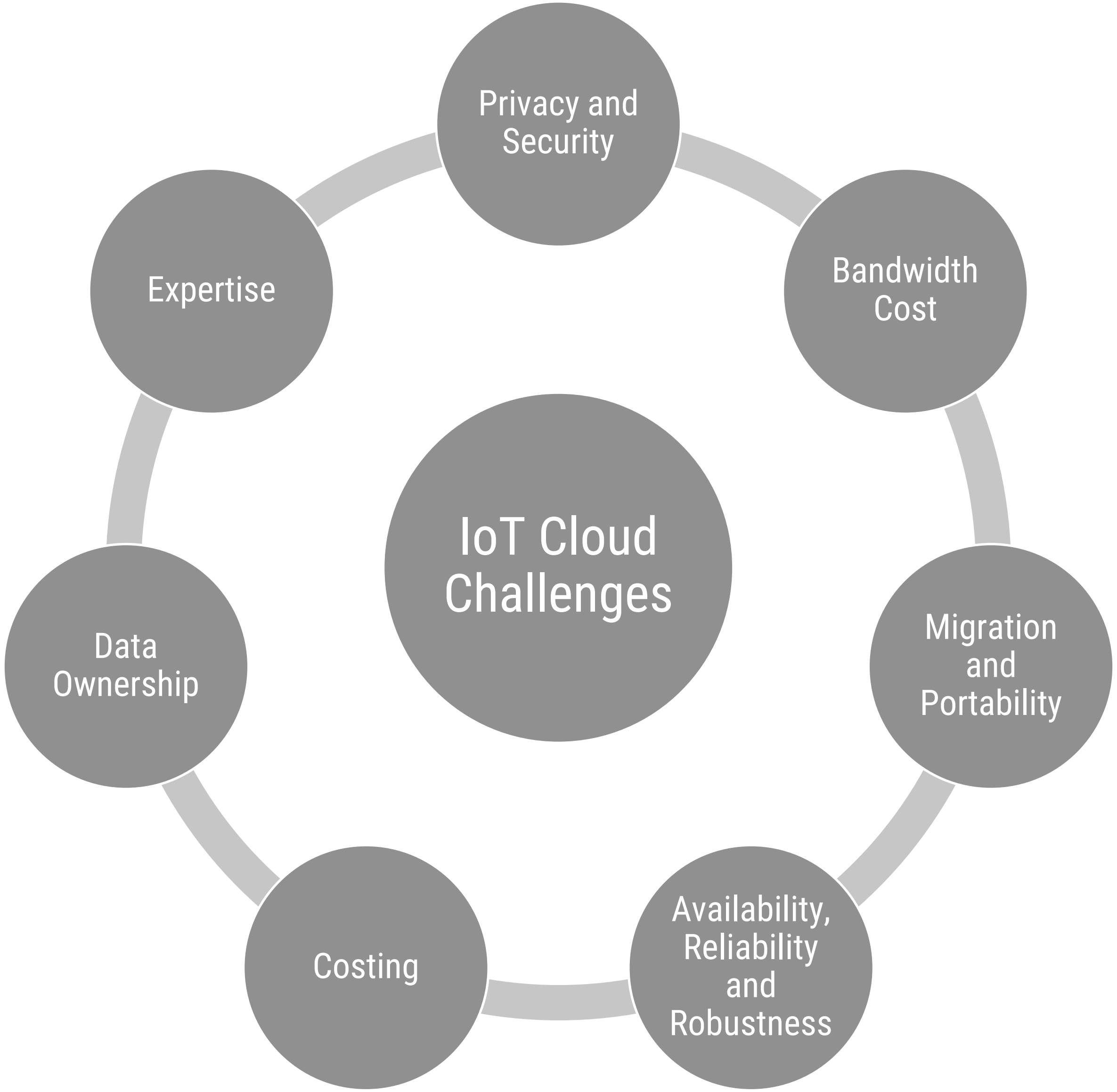
- This deployment is a mix of both private and public cloud deployment
- The resources offered and managed are both in-house and third party based
- Advantages
  - Less investment needed to setup the infrastructure
  - Less technical skill required to manage and maintain the cloud
  - Customer support team can be reached on demand
  - Easily scaled up or scaled down based on requirements
- Disadvantages
  - Security and privacy issues are the major challenges
  - Less flexibility and controls compare to public cloud





Factors	Public Cloud	Private Cloud	Hybrid Cloud
Resources	Resources are shared among multiple customers	Resources are shared with a single organization	It is a combination of public and private clouds. based on the requirement.
Tenancy	Data of multiple organizations is stored in the public cloud	Data of a single organization is stored in a clouds the public cloud	Data is stored in the public cloud, and provide security in the public cloud.
Pay Model	Pay what you used	Have a variety of pricing models	It can include a mix of public cloud pay-as-you-go pricing, and private cloud fixed pricing. It has other pricing models such as consumption-based, subscription-based, etc.
Operated by	Third-party service provider	Specific organization	Can be a combination of both
Scalability and Flexibility	It has more scalability and flexibility,	It has predictability and consistency	It has scalability and flexibility by allowing organizations to use a combination of public and private cloud services.
Expensive	less expensive	More expensive	Can be more expensive, but it can also be less expensive, depending on the specific needs and requirements of the organization.
Availability	The general public (over the internet)	Restricted to a specific organization	Can be a combination of both.

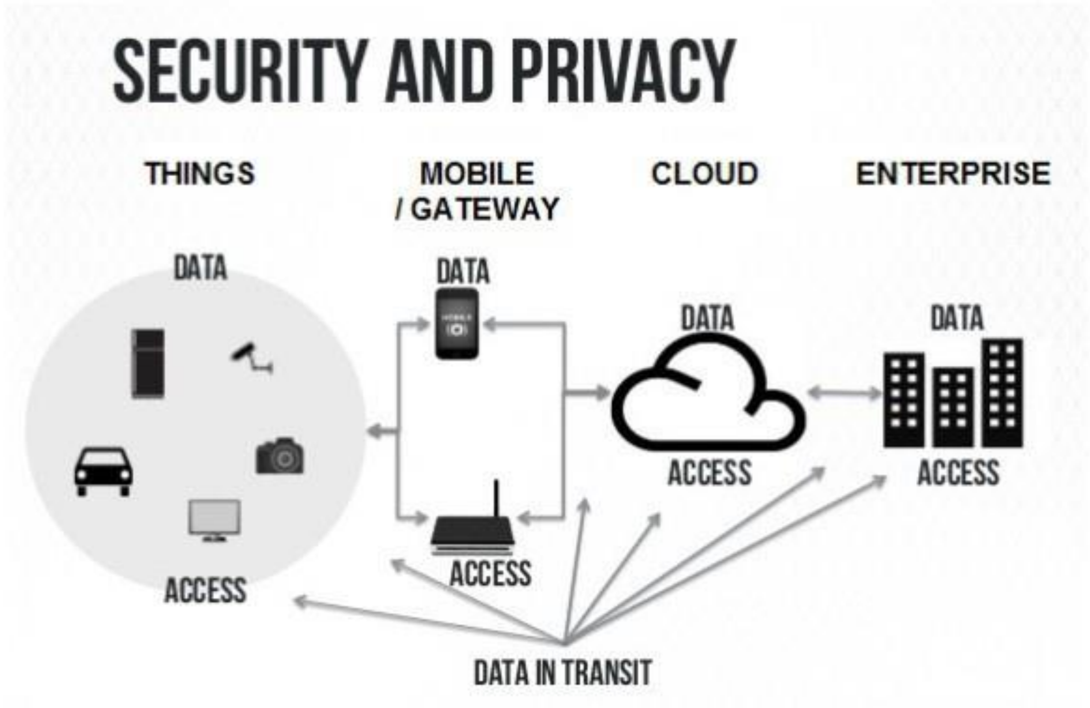
IoT with Cloud - Challenges



- We have already discussed the challenges of IoT and cloud.
- These challenges can be increased when the IoT and cloud are integrated.
- Here we will discuss seven such challenges
  - Privacy and Security
  - Bandwidth Cost
  - Migration and Portability
  - Availability, Reliability and Robustness
  - Costing
  - Data Ownership
  - Expertise

Privacy and Security

- Security is a major concern in the field of IoT.
- Valuable data goes into the cloud, outside the firewall this data becomes hackable.

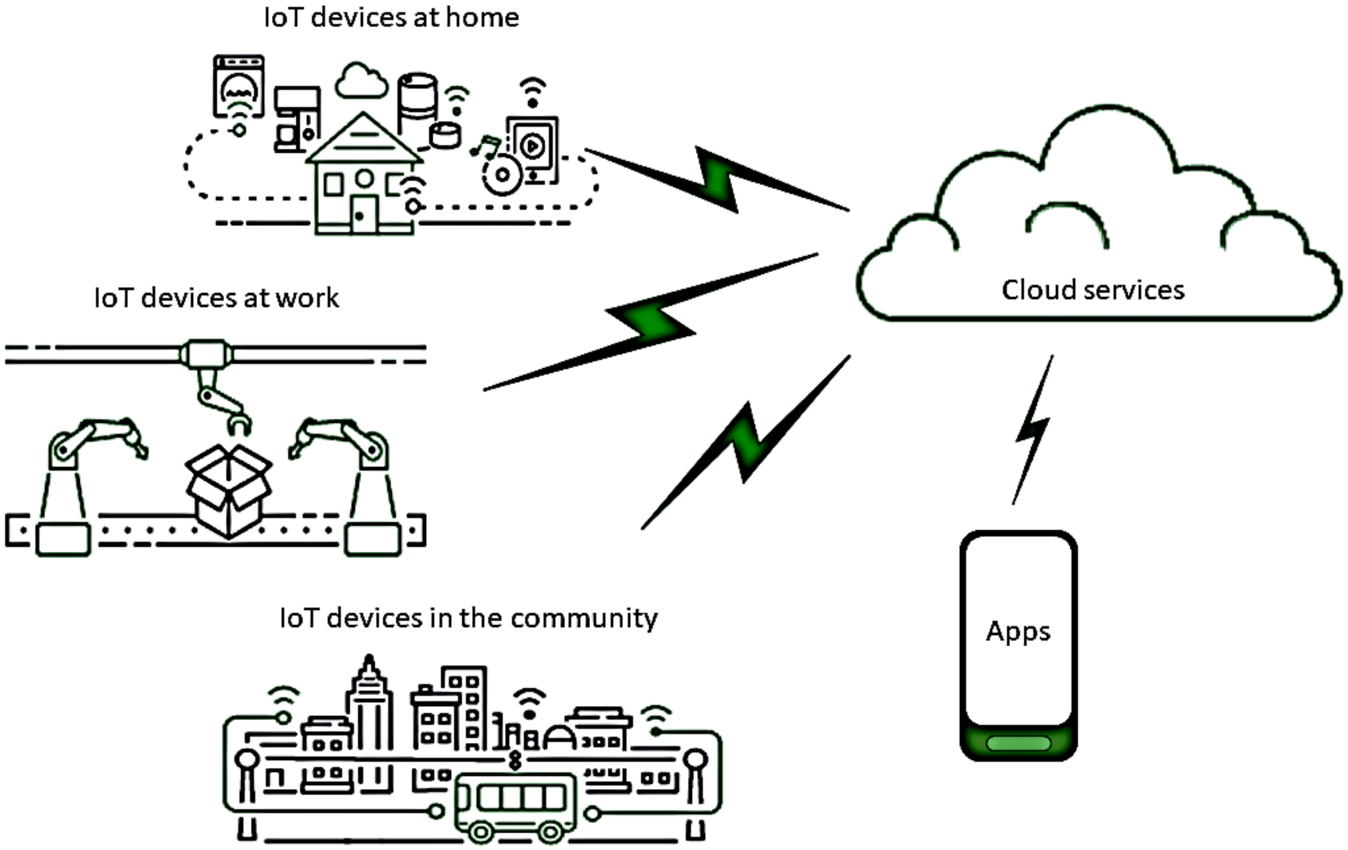


The following are solutions to this privacy and security challenge.

- Periodic monitoring of the network activities
- Select private cloud if the data is confidential
- To reduce the risk of being exposed, use recognized antivirus solutions.
- Before signing the contract with a cloud service provider, it is necessary to read and understand the regulations involved in the service being provided.

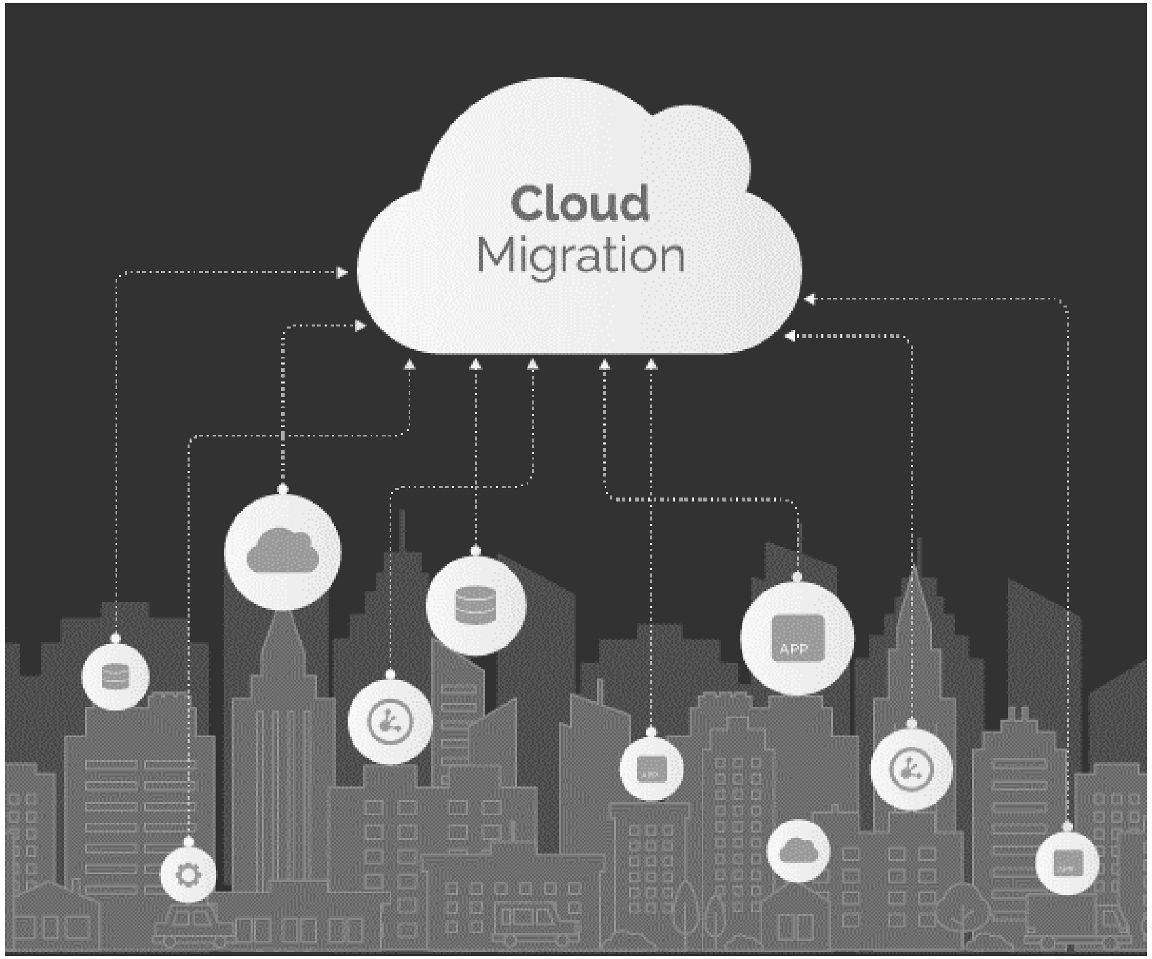
Bandwidth Cost

- Bandwidth is one of the challenges because of continues data transferring from the IoT devices.
- IoT is all about data, and in most cases, this would be big data. Hence, huge investment in storage is needed.
- Cloud computing is preferred for storage and processing in IoT.
- Small-scale IoT application demanding lesser resources.
- But if the application is data concentrated, then the investment in bandwidth would be considerable.



Migration and Portability

- When data is to be moved to or migrate from the cloud, we have to take care of the followings.
  - How easy and safe is it to move the data?
  - How much downtime would this process require?
  - What is the strategy to migrate data to the cloud?
  - Will it be easy to select out of the cloud and take data back to the infrastructure?
  - How much would it cost?
  - Would there be support offered to migrate smoothly to another cloud service provider?
- All these challenges are doubled with IoT as the data comes from the various sensory nodes at a very high speed.

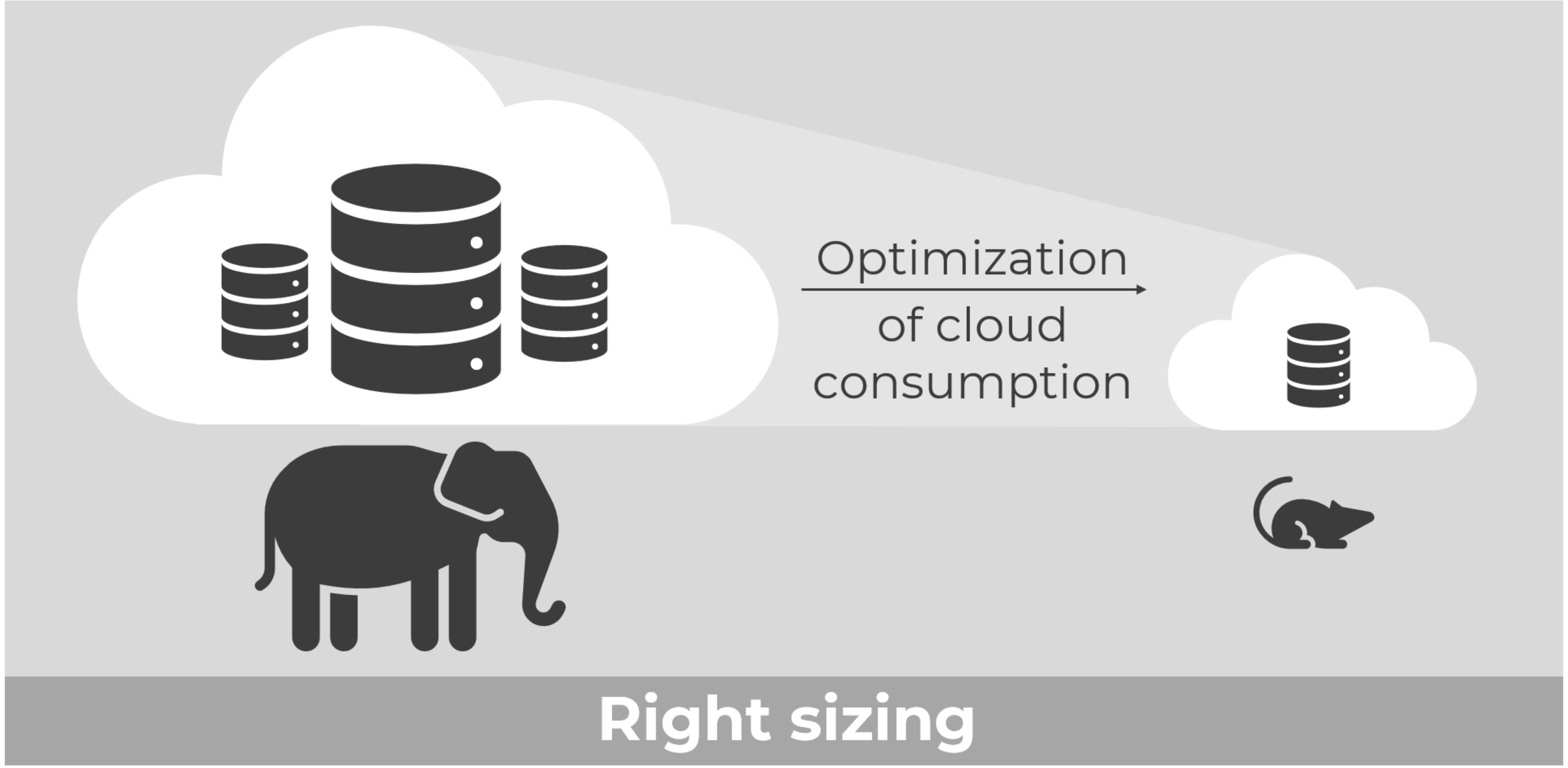


Availability, Reliability and Robustness

- Continuous monitoring and reading of the data need to have continuous cloud service availability in IoT.
- In downtime, it would miss critical data so reliability of the process has to be monitored.
- The process should be robust towards handling data at different rates.
- Data could be flooded or slowed at anytime, in the both situations it should be handled effortlessly.

Costing

- One of the main advantages of cloud is that it can scale up with rising demand.
- While it is scalable and flexible, an organization should plan its budget carefully.
- Wrong selection for subscription without having clear vision and planning, it may lead to unnecessary cost.



Data Ownership

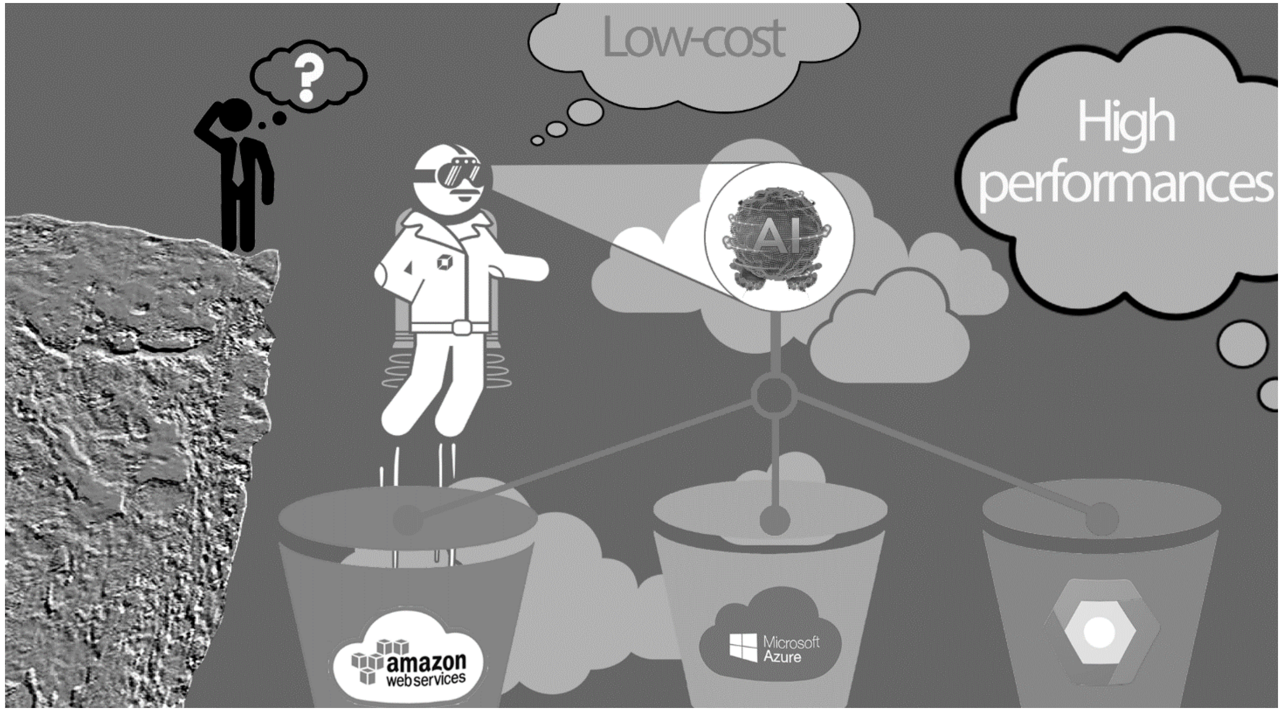
- The data stored by the user on the cloud is owned by the user.
- This means that the data is under the ownership of the person who generates it.
- However, when opting for cloud storage, the data is under the custody of the cloud service provider.
- Then, it appears that the service provider owns the data.
- When it comes to IoT, the data is generated at multiple points and ownership could lie with multiple participating parties.
- Hence, in IoT the ownership-related challenges are multiplied.

Expertise

- To use the cloud with IoT requires a specific skill set.
- The cloud platform gets updated every now and then and so experts have to constantly upgrade themselves.
- Expertise is a definite challenge.
- When IoT and cloud comes together then it will be more challenging,
- To understand the sensors and at the same time, to be updated on cloud development is a challenging task.

Selection of Cloud Service Provider: An Overview

- There are many parameters to select cloud service providers from the numerous service providers.
- It is advisable to consider following parameters while selecting the cloud service provider.
    - Certification and Standards Compliance
    - Financial Health of the Service Provider
    - Business and Technology Strength
    - Compliance Audit
    - Service Level Agreements
    - Reporting/Tracking
    - Costing and Billing
    - Maintenance Monitoring and Upgrade
    - Support
    - Security



Criteria 1: Certification and Standards Compliance

- When a product adheres to the standards that are accepted widely, it is considered as a reliable product. Similarly,
- Cloud service providers (CSPs) are expected to comply with standards. Because product with standards are accepted widely, it is considered as a reliable product
- Industry accepted standards is the first criteria to select the CSP.
- Though there are many standards framed and followed by the industry, some of the main standards for cloud are ISO, Open Cloud Consortium (OCC), IEEE, SNIA (Cloud Storage Initiative).

Criteria 2: Financial Health of the Service Provider

- The service provider should hold sufficient funding to operate business for a long period.
- If the service provider has healthy financial status and history of sustenance, then it is most unlikely to shut down.

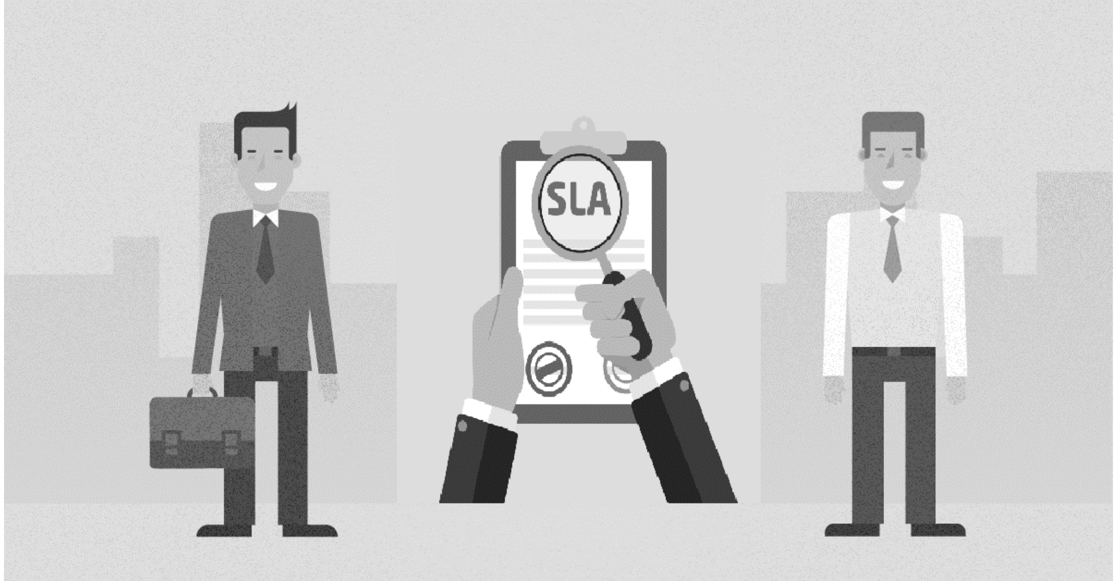
Criteria 3: Business and Technology Strength

- Having the technical expertise to sustain and adapt to a client's requirements is a key factor in selecting a CSP.
- Having just the technical skill and strength does not help; the CSP needs business skills as well to sustain.
- Business skills include growth planning, financial planning, and other factors that are required to sustain in the market.
- Sustenance = Technology + Business Skills

Criteria 4: Compliance Audit

- The CSP must validate compliance with the client's requirement.
- Which should be done through a proper third party audit.
- This will enable transparency and perfect validation.

Criteria 5: Service Level Agreements



- Service Level Agreements (SLAs) provides detail information about the services being provided.
- SLAs also indicates the real value that a customer gets out of them.
- SLAs serve as a legal contract, define the terms & conditions and the relationship between the two parties.

Criteria 6: Reporting/Tracking

- The service provider should be capable for issuing a complete performance report, which also highlights the problems.
- This will enable the customer to understand the complete situation.

Criteria 7: Costing and Billing

- The costing and billing should be transparent and should provide the complete details of the usage.
- It is expected to be automated with details of the complete resource utilization.
- It should with having clarity along with the breakup.
- This means the billing should be transparent and for the usage only.
- This is a major factor in selecting the CSP.

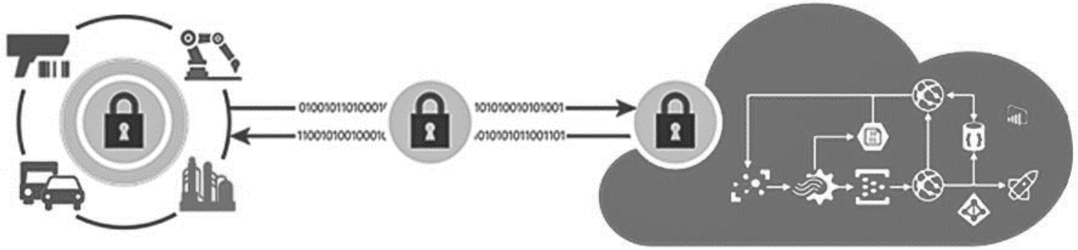
Criteria 8: Maintenance Monitoring and Upgrade

- It should be easy and less expensive to migrate to the CSP's environment.
- When there is an upgrade, it should be done with ease.
- Any maintenance should be easy and affordable.
- In short, it should be easier to install, manage, maintain, and upgrade.
- This upgrade includes migration from private to public to hybrid cloud, if needed.

Criteria 9: Support

- Help and assistance should be provided when required.
- Support should be available based on the agreements and a dedicated resource.
- Support levels based on complexity of problem.
- Onsite support may be needed when clarifications cannot be offered over phone or online.
- Thus, support is a major deciding factor for selection of a service provider.

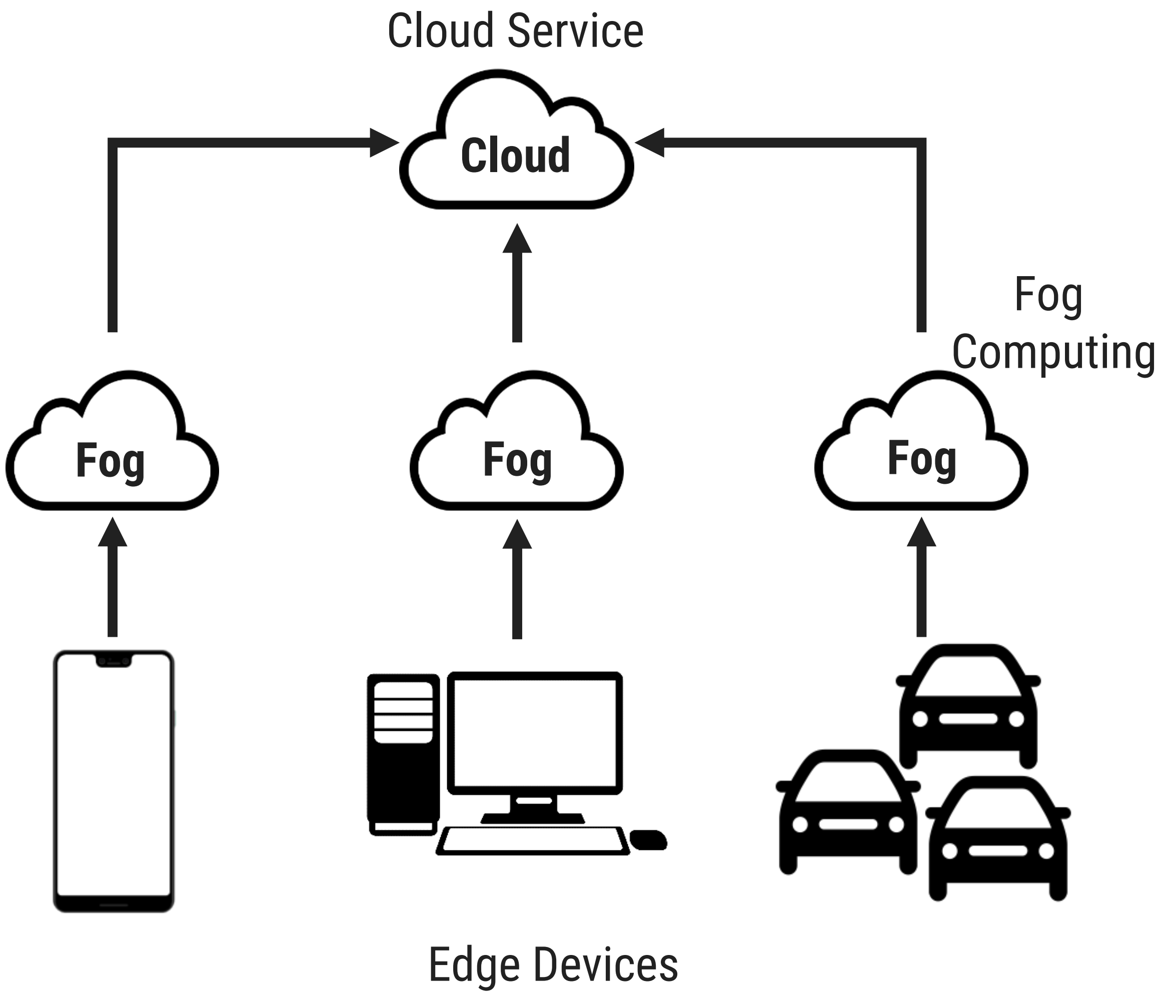
Criteria 10: Security



- The infrastructure, both hardware and software should be secured.
- There should be defined policies about the security that should also be shared with a customer.
- This includes everything, from access restrictions to customer data.
- The data should be safe in case of a breakdown/failure.
- The recovery and backup options should be sound.
- The physical infrastructure has to be safeguarded as well.
- All these factors would require audit, which should be carried out by a third party.
- Security is the prime concern and cannot be ignored.
- Evaluation should start from this point.

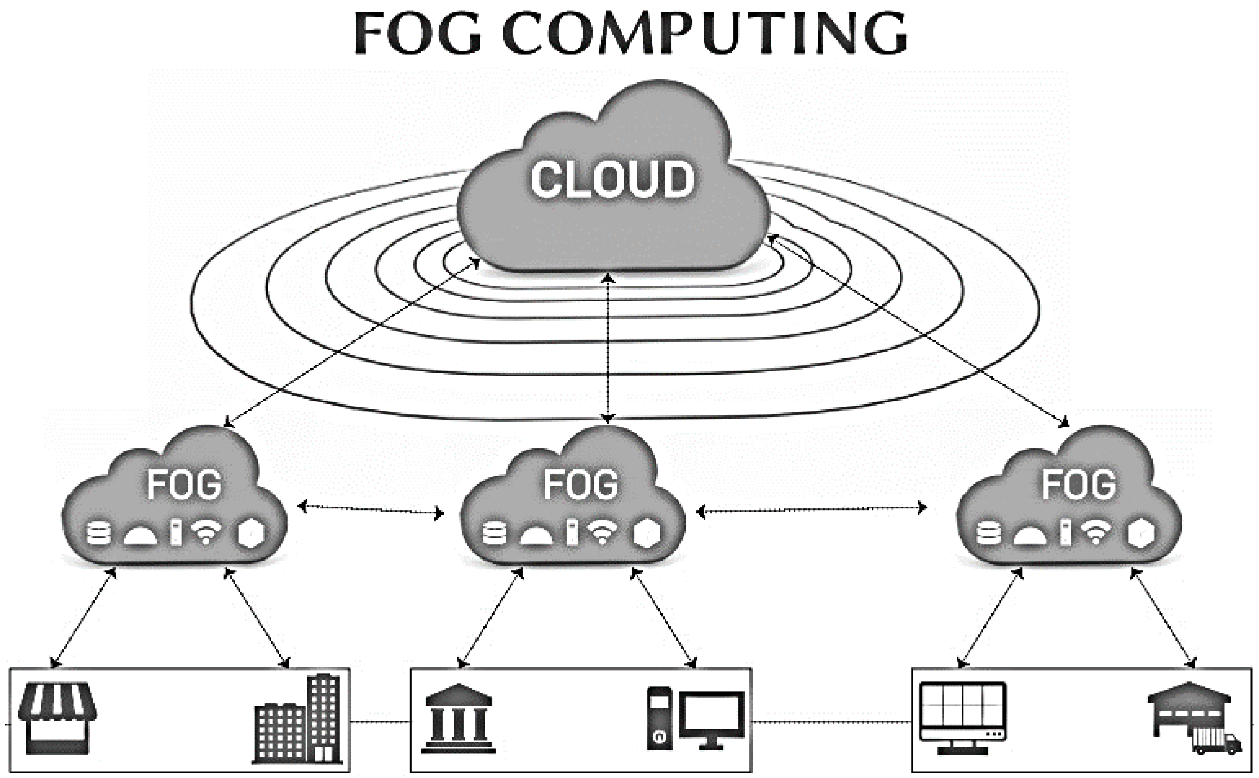
Introduction to Fog Computing

- IoT is all about the data. The factors that affect data are the four Vs - variety, velocity, veracity and volume.
- All IoT applications require instant analysis and action.
- Most of the time, the action would be corrective in nature, it would be business critical.
- In case the data volume is high and it reaches the cloud after some delay.
- So we may lost the opportunity to use the data appropriately.
- In such cases, fog computing serves the solution.



Introduction to Fog Computing

- The most sensitive data should be analyzed in the area closer to the place where it is generated.
- With fog computing, it is possible.
- Using fog computing we can process the data locally and to avoid the trouble by not sending the data to the cloud.
- Respond much faster because of data is moving locally so data travel is reduced considerably.
- It thus process the data in milliseconds.

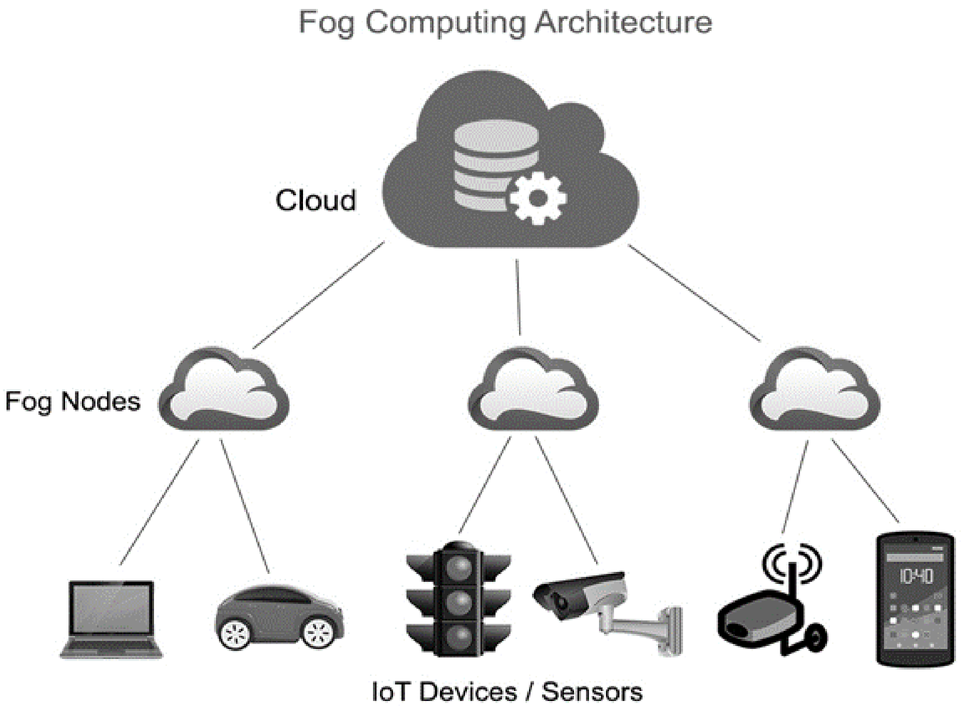


Introduction to Fog Computing

- Only the required data will be sent to the cloud.
- This will be based on storage requirements and guidelines.
- Predictive analytics can also be carried out with the data stored in the cloud.
- The fog is below cloud, which means it is closer to the elements that generate data.
- After analysis, the data stored is pushed on to the cloud.
- Results in increased efficiency and safety both physical and asset safety.
- Some examples where faster response time is extremely important are factory or manufacturing line, oil and gas tube lines fault analysis, on-flight diagnosis, and healthcare.

Working of Fog Computing

- Sensors/devices generate data transmit it to the middle layer, which is very close the data source.
- These nodes in the middle layer are capable of handling the data.
- This requires minimum power and lesser resources.
- All the data need not go to the cloud at the instant.
- Also, sensitive data gets processed very fast, which results in an instant response.
- Fog is not meant for hefty storage. It is still the cloud that does the task of storing big data.
- Fog is just an intermediary layer for faster data processing, and the faster response time.



Summarize the concepts

Concept of fog nodes

- It receives the data feed from the sensors, in real-time.
- Response time is minimal, ideally in milliseconds.
- Fog computing is transit, where data is stored for a limited time only.
- Data is then sent to cloud as a summary.
- It is important to note that not all data goes to the cloud.

Concept of cloud computing platform

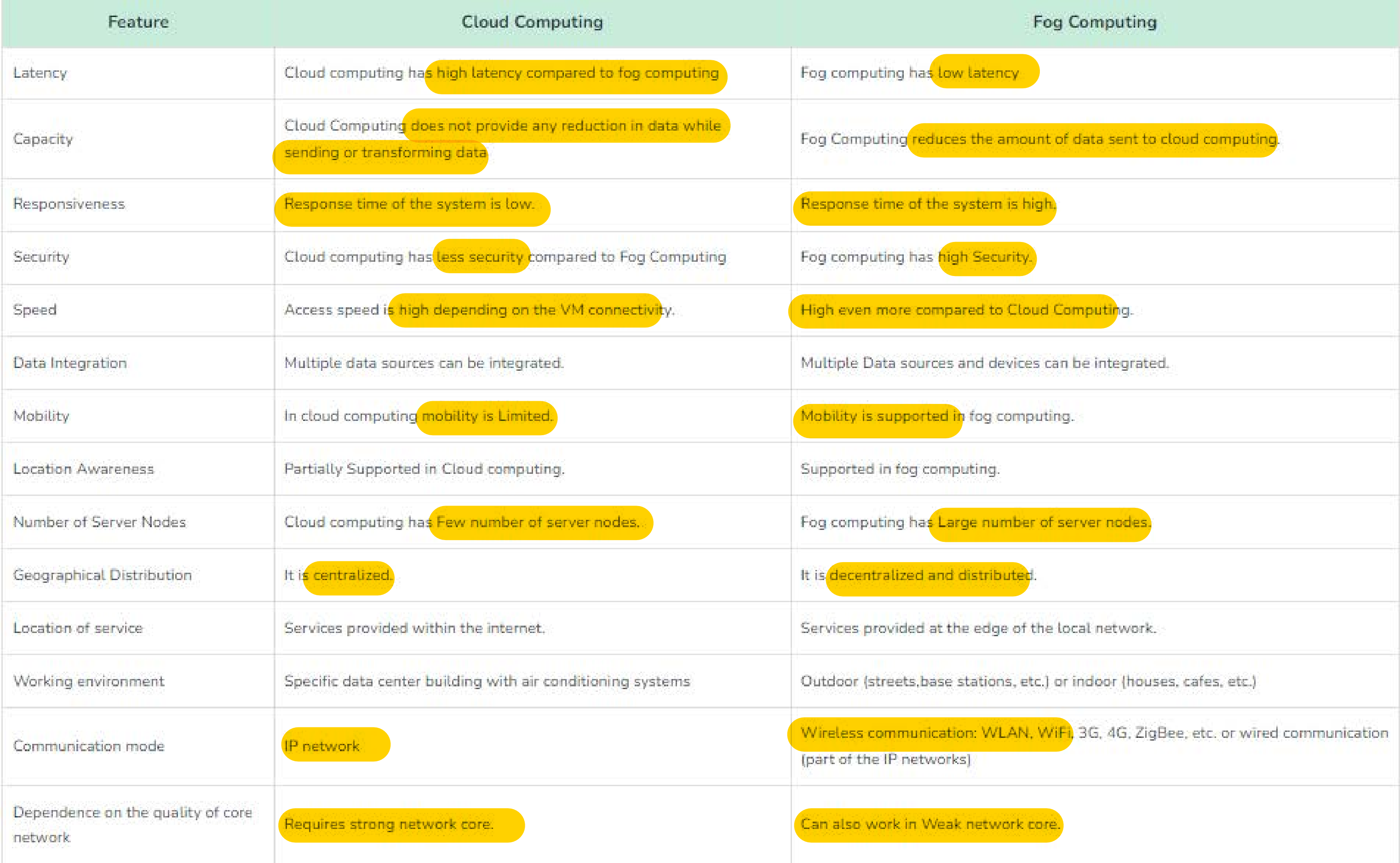
- It receives the data summary from the fog.
- Data prediction, data analytics, data storage, etc. takes place here.

Benefits of fog computing model

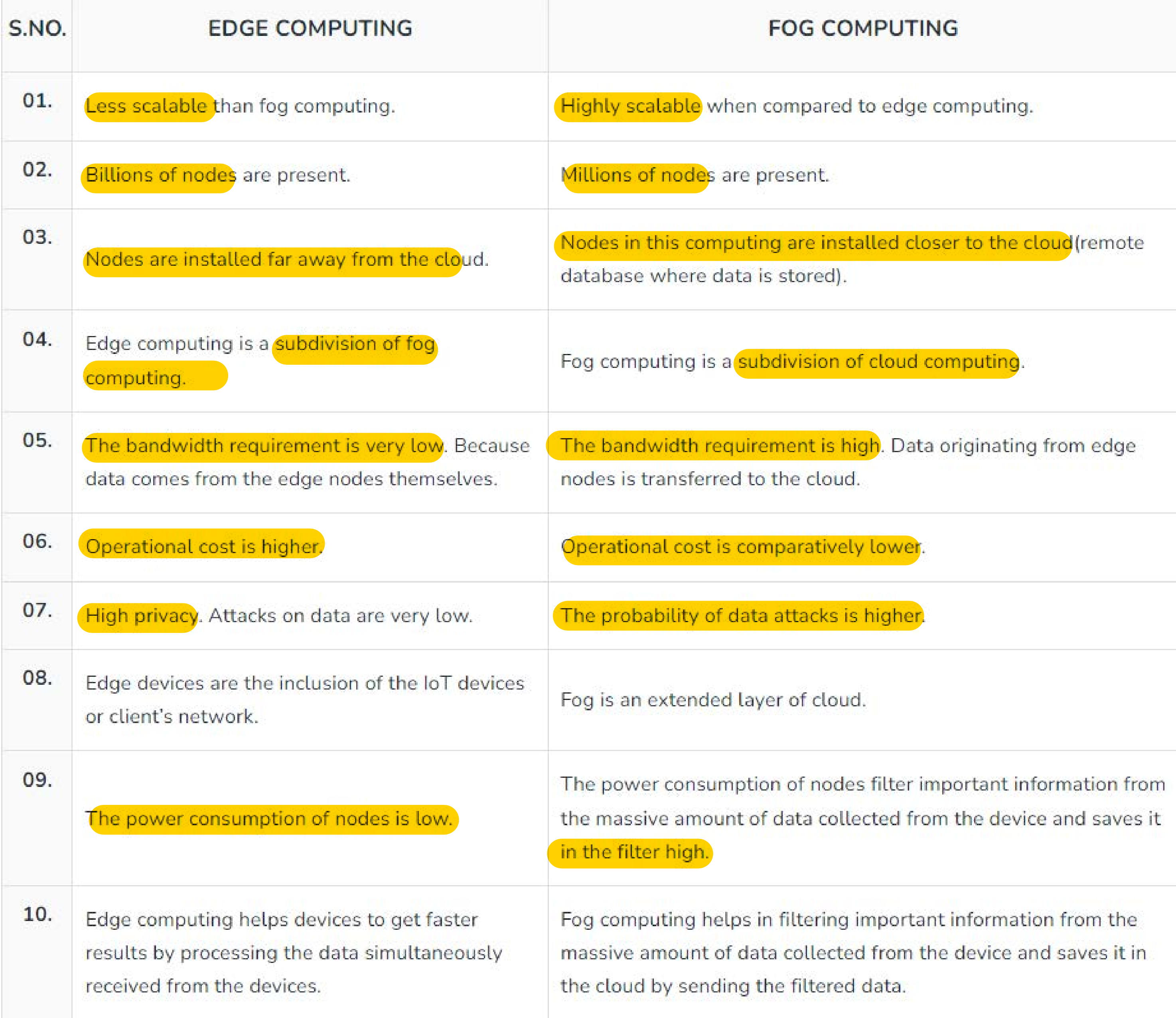
- Minimal amount of data sent to the cloud.
- Reduced bandwidth consumption.
- Reduced data latency.
- Improved data security. When limited data goes to cloud, it is easier to protect it.
- Immediate processing of data in real time (this is very much needed in industrial applications).

Difference between Edge and Fog Computing

- Both fog and edge are concerned with the computing capabilities to be executed locally, before passing it to the cloud.
- Both aim at reducing complete dependency on the cloud to perform computation.
- Analyzing data and processing it at the cloud is to be avoided.
- Both these reduce the time delay for making faster decision for real-time applications.
- The main difference between edge and fog computing is where data processing takes place.
- Edge computing is the computing carried out at the device itself, where all the sensors are-connected.
- In fog computing, data processing is moved to the processors that are connected to the local area network (LAN), making it a little farther from the sensors and actuators.
- Thus, the main difference between edge and fog computing is the distance.



Feature	Cloud Computing	Fog Computing
Latency	Cloud computing has high latency compared to fog computing	Fog computing has low latency
Capacity	Cloud Computing does not provide any reduction in data while sending or transforming data	Fog Computing reduces the amount of data sent to cloud computing.
Responsiveness	Response time of the system is low.	Response time of the system is high.
Security	Cloud computing has less security compared to Fog Computing	Fog computing has high Security.
Speed	Access speed is high depending on the VM connectivity.	High even more compared to Cloud Computing.
Data Integration	Multiple data sources can be integrated.	Multiple Data sources and devices can be integrated.
Mobility	In cloud computing mobility is Limited.	Mobility is supported in fog computing.
Location Awareness	Partially Supported in Cloud computing.	Supported in fog computing.
Number of Server Nodes	Cloud computing has Few number of server nodes.	Fog computing has Large number of server nodes.
Geographical Distribution	It is centralized.	It is decentralized and distributed.
Location of service	Services provided within the internet.	Services provided at the edge of the local network.
Working environment	Specific data center building with air conditioning systems	Outdoor (streets,base stations, etc.) or indoor (houses, cafes, etc.)
Communication mode	IP network	Wireless communication: WLAN, WiFi, 3G, 4G, ZigBee, etc. or wired communication (part of the IP networks)
Dependence on the quality of core network	Requires strong network core.	Can also work in Weak network core.



S.NO.	EDGE COMPUTING	FOG COMPUTING
01.	Less scalable than fog computing.	Highly scalable when compared to edge computing.
02.	Billions of nodes are present.	Millions of nodes are present.
03.	Nodes are installed far away from the cloud.	Nodes in this computing are installed closer to the cloud(remote database where data is stored).
04.	Edge computing is a subdivision of fog computing.	Fog computing is a subdivision of cloud computing.
05.	The bandwidth requirement is very low. Because data comes from the edge nodes themselves.	The bandwidth requirement is high. Data originating from edge nodes is transferred to the cloud.
06.	Operational cost is higher.	Operational cost is comparatively lower.
07.	High privacy. Attacks on data are very low.	The probability of data attacks is higher.
08.	Edge devices are the inclusion of the IoT devices or client's network.	Fog is an extended layer of cloud.
09.	The power consumption of nodes is low.	The power consumption of nodes filter important information from the massive amount of data collected from the device and saves it in the filter high.
10.	Edge computing helps devices to get faster results by processing the data simultaneously received from the devices.	Fog computing helps in filtering important information from the massive amount of data collected from the device and saves it in the cloud by sending the filtered data.

Cloud Computing: Security Aspects

- The security of any computing platform including cloud computing depends on
  - ↪ Software security,
  - ↪ Infrastructure security,
  - ↪ Storage security, and
  - ↪ Network security,
- If any of these is compromised, it would result in security violation and could cause damages.
- Let us discuss these security aspects briefly.

Cloud Computing: Security Aspects

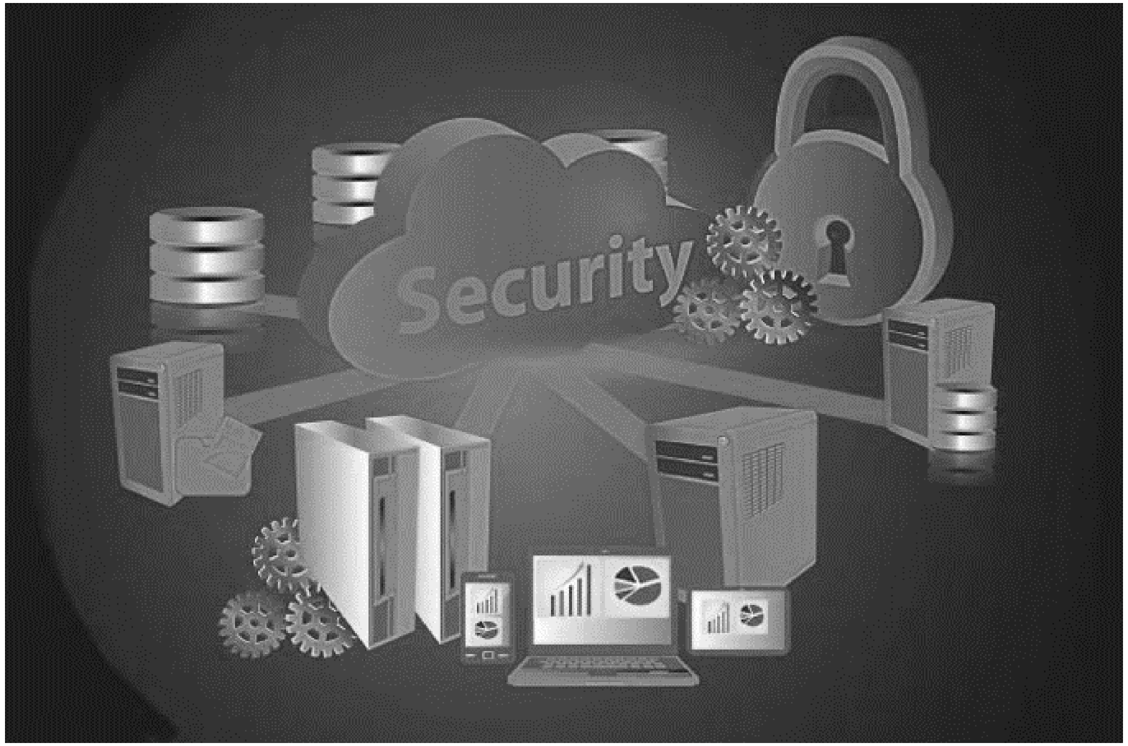
1. Software Security:

- Software is the core component and plays a vital role in presenting and ensuring a secure environment.
- If there are defects created/generated during the development phase, it is a software security threat.
- Defects such as simple software implementation defects, memory allocation, design issues, and exception handling all contribute to security issues.
- This can be ensured by complete and comprehensive testing carried out at all-stages.

Cloud Computing: Security Aspects

2. Infrastructure Security:

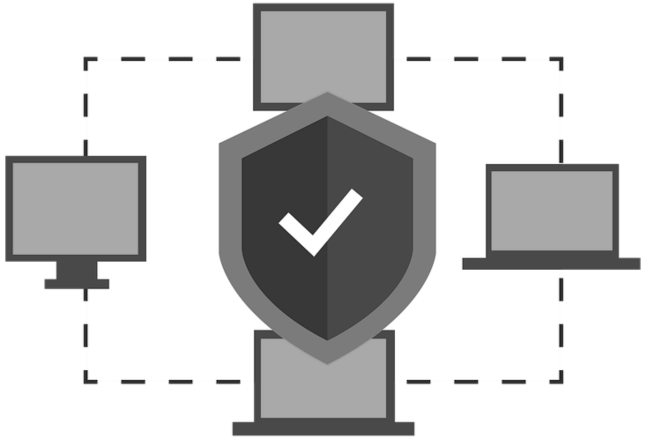
- Making sure that the infrastructure provided by the CSP is safe is a must.
- Third party could also contribute to the infrastructure.
- It is extremely important to check the security vulnerabilities with the infrastructure.
- All infrastructure related guidelines should be mentioned clearly in the agreements and should be made transparent to the customer.
- If data is damaged, everything is damaged and lost.
- Hence, care should be taken to protect the infrastructure.

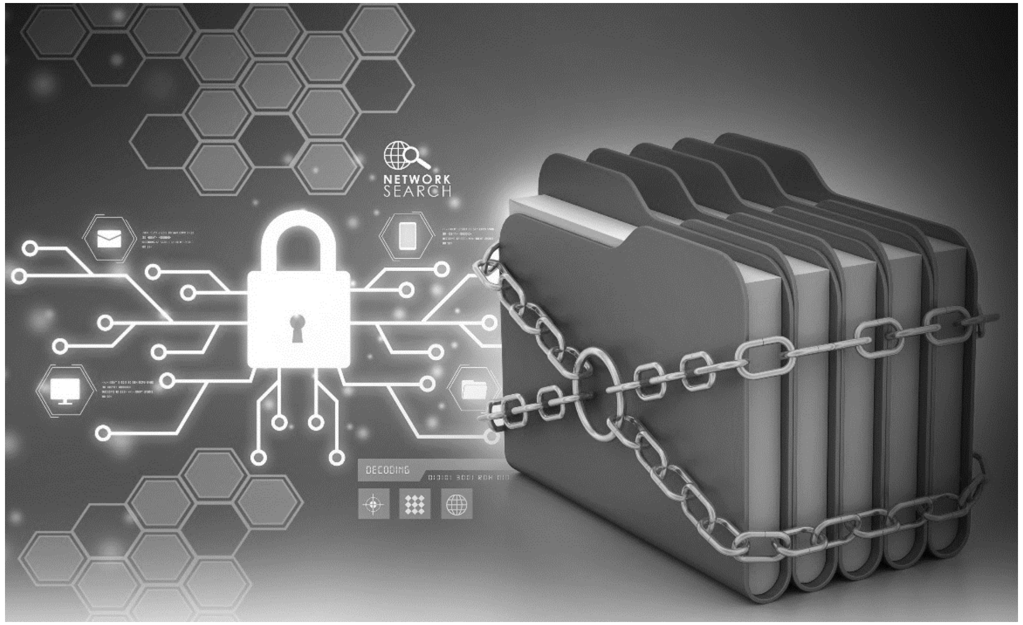


Cloud Computing: Security Aspects

3. Storage Security:

- It is important to be informed of who owns the data and the location where it is stored.
- Data leak, snooping, malware attacks, etc. are all threats to the stored data and can be listed under storage security.
- Appropriate antivirus software and periodic monitoring, should help protect the data.





4. Network Security:

- Data is stored in the cloud via the Internet, and hence all network threats become a possibility.

Summary

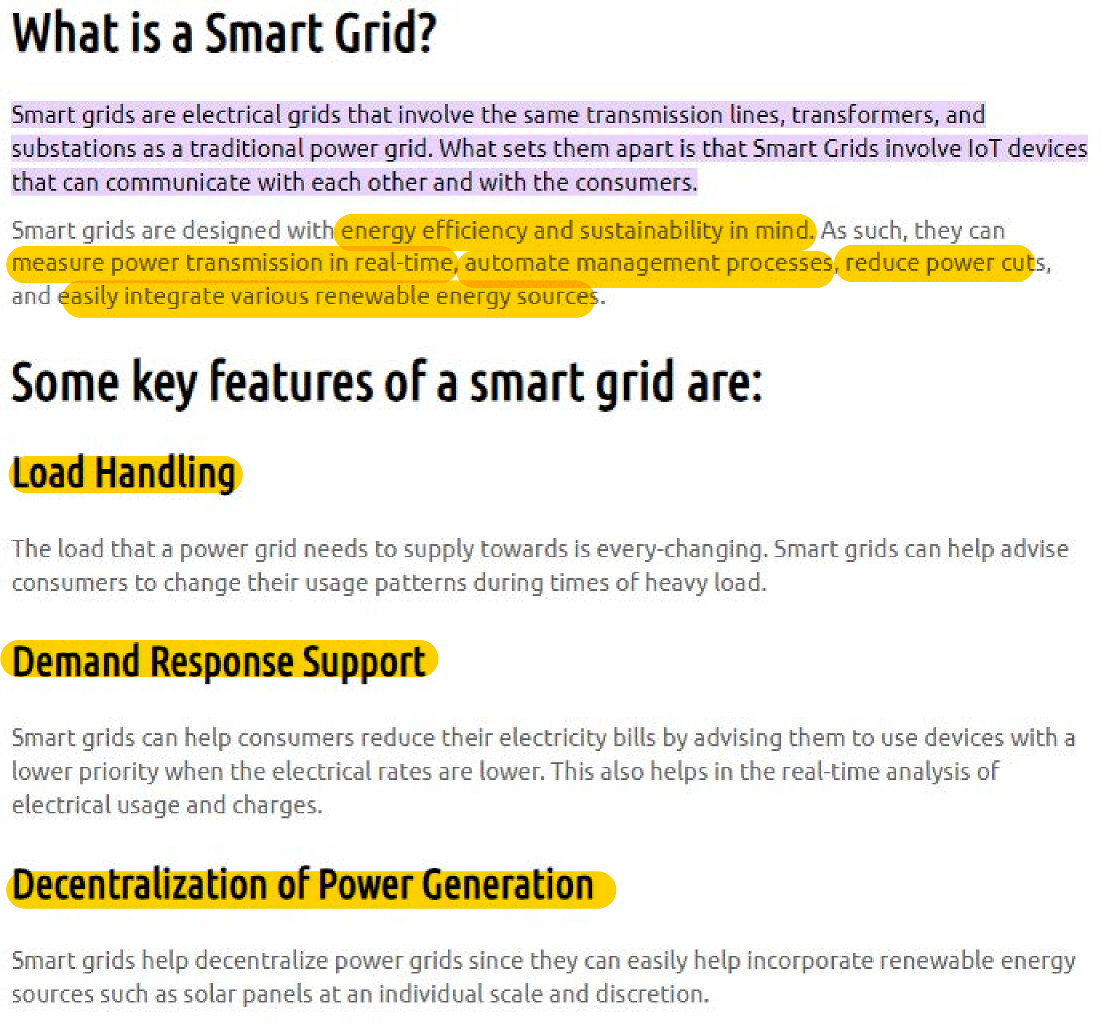
- Cloud computing has become one of the most used technology components in modern day applications, which not only provides storage but also supports data analytics.
- Cloud services could be any one of the following:
  - **Software as a Service (SaaS):** Complete software application as a service is provided to the user.
  - **Platform as a Service (PaaS):** Development tools, APIs, libraries, etc. will be divided by the cloud service provider. User have to build, manage and maintain the applications.
  - **Infrastructure as a Service (IaaS):** User should be provided with virtual machine support, where the user does not need to know and worry about the infrastructure. Everything should be taken care by the service provider. User will manage the machines, select the OS and underlying applications.
- The three deployment models generally used for public, private and hybrid
- Private cloud deployment model can be opted wherever confidentiality matters the most.
- When its come to public cloud deployment model, the cloud service provider owns all the resource which include hardware/infrastructure and software. Cloud service provider will take care of all resource management.

Summary

- Hybrid development is a mix of both public and private deployment model. In this approach the resource offered and manage are both in-house and third party based.
- There are many challenges one could face while opting for cloud storage with IoT applications some of these are as follows:
  - Privacy and security
  - Bandwidth cost
  - Migration and portability
  - Reliability and availability
  - Costing
  - Data ownership
  - Expertise
- Selecting a CSP is not easy. Many parameters are to be considered before choosing the best option.
- With fog computing, it become possible to analyze the data at a place closer to where it is generated.

Summary

- Fog computing provides the following advantages:
  - Minimal amount of data send to cloud
  - Reduce bandwidth consumption
  - Reduce data latency
  - Improve data security
  - Immediate processing of data



What is a Smart Grid?

Smart grids are electrical grids that involve the same transmission lines, transformers, and substations as a traditional power grid. What sets them apart is that Smart Grids involve IoT devices that can communicate with each other and with the consumers.

Smart grids are designed with energy efficiency and sustainability in mind. As such, they can measure power transmission in real-time, automate management processes, reduce power cuts, and easily integrate various renewable energy sources.

Some key features of a smart grid are:

Load Handling

The load that a power grid needs to supply towards is every-changing. Smart grids can help advise consumers to change their usage patterns during times of heavy load.

Demand Response Support

Smart grids can help consumers reduce their electricity bills by advising them to use devices with a lower priority when the electrical rates are lower. This also helps in the real-time analysis of electrical usage and charges.

Decentralization of Power Generation

Smart grids help decentralize power grids since they can easily help incorporate renewable energy sources such as solar panels at an individual scale and discretion.

How Do Smart Grids Work?

You've already seen how smart grids can help with modern energy requirements. Let's look at how smart grids impact the power cycle at each stage:

Generate

Smart grids can combine the power generation from various energy sources, including nuclear, coal, hydro, and solar. This allows for increased energy production at a grid level that can handle the growing need for power of a modern city.

Distribute

Smart grids use smart transmission lines that transmit power in a specified voltage range. This allows for reduced power loss from heat generation in the power lines.

Use

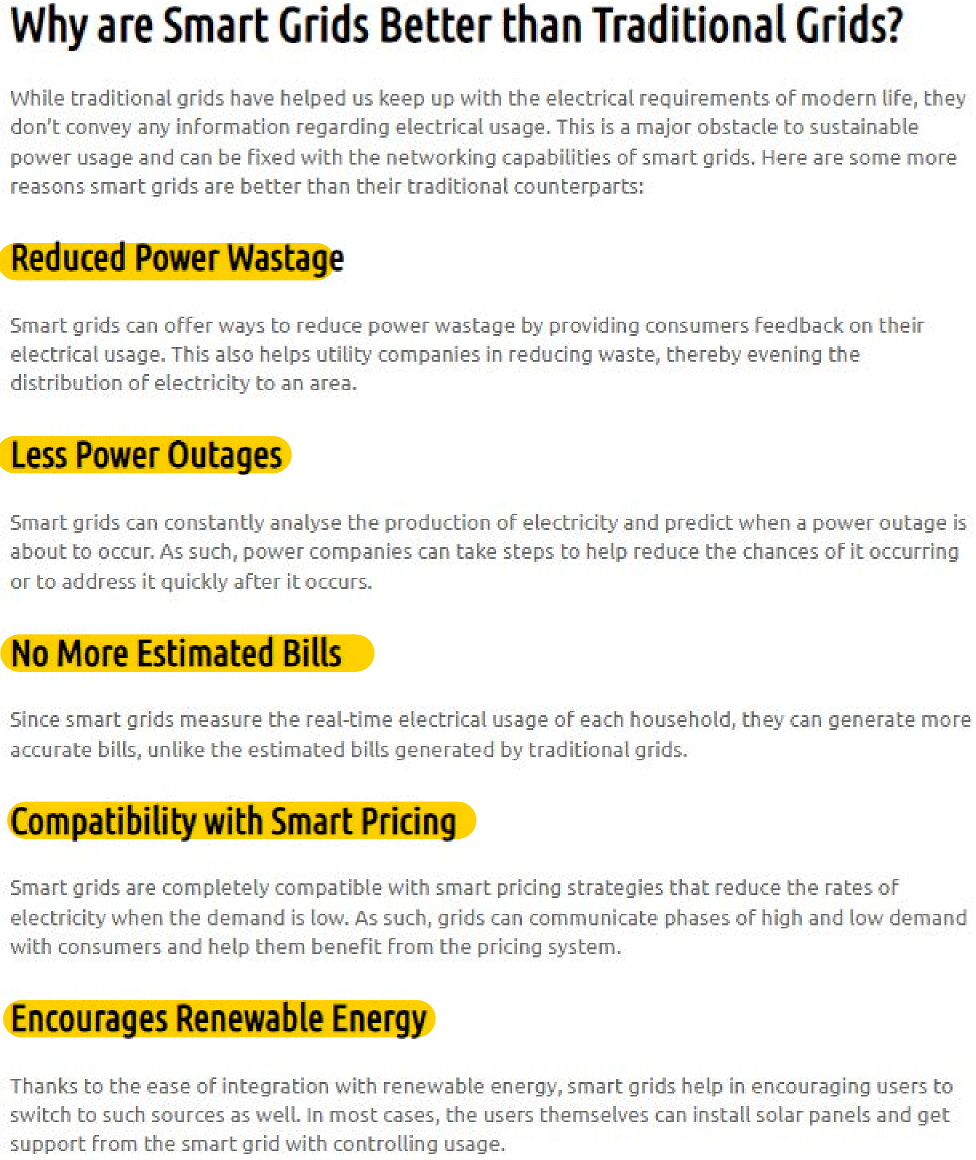
Consumers can view their power usage at any time and further integrate the smart grid into their homes with smart sockets and meters. This helps make them gain control over their power consumption and make better decisions for reducing usage.

Control

People working in utility companies can expand their control with smart grids. They can view energy usage across the region and perform various preventive maintenance checks to ensure that the grid keeps running at its best.

Store

Smart grids also allow homes to store extra power in the case of a forecasted blackout. This also works for various power backup systems in modern buildings.



Why are Smart Grids Better than Traditional Grids?

While traditional grids have helped us keep up with the electrical requirements of modern life, they don't convey any information regarding electrical usage. This is a major obstacle to sustainable power usage and can be fixed with the networking capabilities of smart grids. Here are some more reasons smart grids are better than their traditional counterparts:

Reduced Power Wastage

Smart grids can offer ways to reduce power wastage by providing consumers feedback on their electrical usage. This also helps utility companies in reducing waste, thereby evening the distribution of electricity to an area.

Less Power Outages

Smart grids can constantly analyse the production of electricity and predict when a power outage is about to occur. As such, power companies can take steps to help reduce the chances of it occurring or to address it quickly after it occurs.

No More Estimated Bills

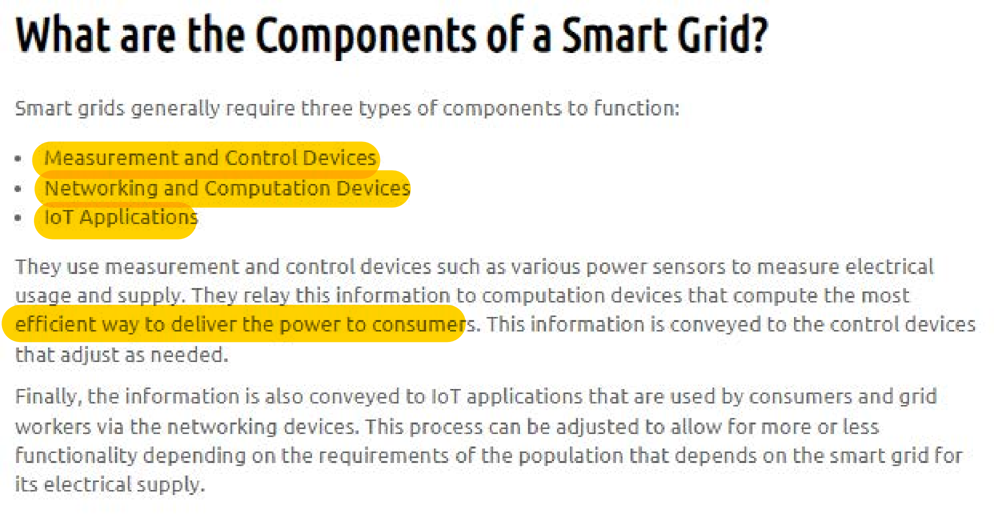
Since smart grids measure the real-time electrical usage of each household, they can generate more accurate bills, unlike the estimated bills generated by traditional grids.

Compatibility with Smart Pricing

Smart grids are completely compatible with smart pricing strategies that reduce the rates of electricity when the demand is low. As such, grids can communicate phases of high and low demand with consumers and help them benefit from the pricing system.

Encourages Renewable Energy

Thanks to the ease of integration with renewable energy, smart grids help in encouraging users to switch to such sources as well. In most cases, the users themselves can install solar panels and get support from the smart grid with controlling usage.



What are the Components of a Smart Grid?

Smart grids generally require three types of components to function:

- Measurement and Control Devices
- Networking and Computation Devices
- IoT Applications

They use measurement and control devices such as various power sensors to measure electrical usage and supply. They relay this information to computation devices that compute the most efficient way to deliver the power to consumers. This information is conveyed to the control devices that adjust as needed.

Finally, the information is also conveyed to IoT applications that are used by consumers and grid workers via the networking devices. This process can be adjusted to allow for more or less functionality depending on the requirements of the population that depends on the smart grid for its electrical supply.