# BYOD network enhancing security / BYOD trend

Nwebonyi, F., & Daniel Ani, U. (2015). BYOD network: Enhancing security through trust--aided access control mechanisms. *International Journal of Cyber-Security and Digital Forensics,* *4*(1), 272-289.

* BYOD expected to grow to 88% patronage among organisations (Scarfo, A. (2012). New Security Perspectives around BYOD. *2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications,* 446-451.)
* More on Bring Your Own Device (BYOD) to Work (Hayes, B., & Kotwica, Kathleen. (2013). *Bring your own device (BYOD) to work trend report* (Risk management portfolio). Oxford: Elsevier.)
* The popularity of it is driven by reduced cost, improved productivity of using familiar devices
* Brings new security challenge

Downer, K., & Bhattacharya, M. (2015). BYOD Security: A New Business Challenge. 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), 1128-1133.

* Deployment challenge: how data is accessed and cotrolled, how to avoid data duplication
* Technical challenges:

**Access control:** Companies need to determine permission levels for each employee when accessing certain company resources with personal devices and external network connections [2][7]. (Astani, M., Ready, K., Tessema, M. (2013) BYOD Issues and Strategies

in Organisations. Issues in Information Systems. Vol: 14, Issue 2. pp.

195-201.)

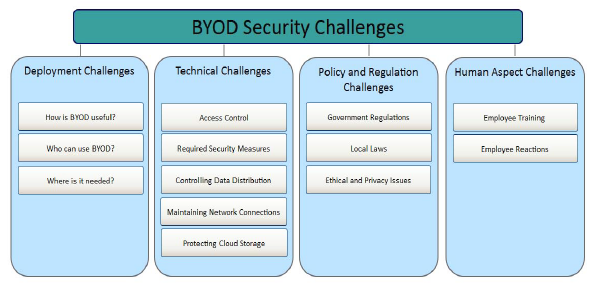
**Ongoing support**: extra resource to maintain the desired level of security (ibid.)

**Distribution of data:** maintaining confidentiality and integrity of data

* Policy and regulation challenges: local law and privacy issues: consent for employee/student to install /access data in their devices (Absalom, R. (2012) International Data Privacy Legislation Review: A guide for BYOD policies. Ovum. Vol. 1. pp. 1-23.)
* Human aspect of challenges: training needed for handling more sensitive data

Security frameworks

1. VPNs (virtual private machine): facilitates exclusive network connection with devices and allows access to resources in a controlled environment (Disterer G and Kleiner C (2013) BYOD Bring Your Own Device. Procedia Technology Vol. 9, 43-53.), reduces the need for storing data on devices, whilst keep flexible work patterns
2. Mobile Information Management: ensure documents synchronization, while administrating security procedures (Scarfo A (2012) New Security perspectives around BYOD. 2012 Seventh International Conference on Broadband, Wireless computing, Communication and Applications. Vol. pp. 446- 451, IEEE Press.)
3. Desktop virtualization models enable desktop computers, virtual machines and servers to host sessions for remotely located devices. Mobile devices operate like remote controls when interacting with applications contained on hosting hardware, and communicate via VPN connections. Desktop virtualisation models are low cost, centralise resources, data and security management and reduces or eliminates the need to transmit data onto mobile devices, thus reduces the possibility of data leakage occurring.



# Virtualization

## VMware

* Virtualization software solves the problem by enabling multiple operating systems and applications to run on one physical server or “host.”
* Because each virtual machine is completely separate and independent, many of them can run simultaneously on a single computer. A thin layer of software called a hypervisor decouples the virtual machines from the host.
* Cost savings is a leading benefit of virtualization, and it can free a business to redirect their resources into value-add opportunities. Organizations can significantly reduce their expenses and make the most of resources through effective pooling, increased automation of operational processes, and the appropriate use of available public cloud services.

## Network virtualization

-gary lee book (also is the source of other 3 chapter

Server virtualization, and data center history)

Lee, G., Green, Todd, editor, & Purdy, Russell, designer. (2014). Cloud networking : Understanding cloud-based data center networks (1st ed.).

## Data centre

Bari, M., Boutaba, Esteves, Granville, Podlesny, Rabbani, . . . Zhani. (2013). Data Center Network Virtualization: A Survey. IEEE Communications Surveys & Tutorials, 15(2), 909-928.

* Data centers provides an infrastructure for storing large volumes of data and **Hosting large scale service applications (IaaS)**
* Traditional data centers which dedicated servers to run applications resulting in poor server utilization and high operational cost
* Data center networking still largely relies on traditional TCP/IP protocol stack

Limitations of traditional data center – **no good for BYOD**

* No performance isolation
* Increased security risk
* Poor application deployability: migrate enterprise applications to data center environment requires cumbersome modifications
* Low flexibility to control their data fabric (in the purpose of load balancing, fault control and security)

Solution: virtualisation of data center

* Creating multiple virtualized network of a shared physical network, thus each VN can be implemented and managed independently. (M. Chowdhury and R. Boutaba, “A Survey of Network Virtualization,” *Computer Networks*, vol. 54, no. 5, pp. 862–876, 2010.)
* Provides performance isolation, facilitated deployment of new application

Data center network

*A data center network is the communication infrastructure used in a data center, and is described by the network topology, routing/switching equipment, and the used protocols (e.g., Ethernet and IP).*

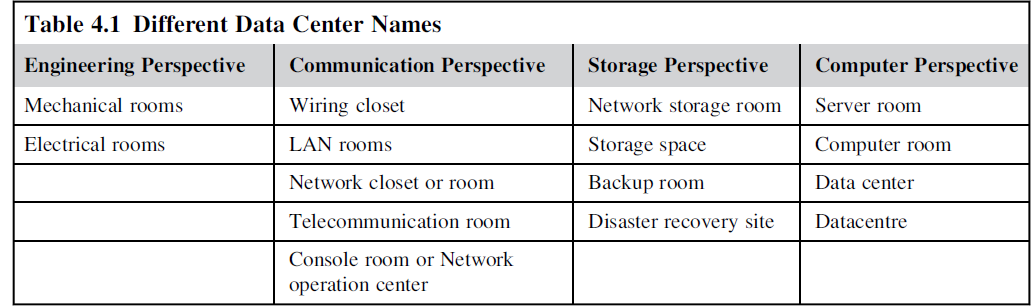
* A Virtualized Data Center is a data center where some or all of the hardware (e.g., servers, routers, switches, and links) are virtualized. Typically, a physical hardware is virtualized using software or firmware called **hypervisor** that divides the equipment into multiple isolated and independent virtual instances.
* Hypervisor can create several virtual machines with different capacity on a single physical server
* Virtual data center: a collection of virtual resources connected via virtual links, subset of deployed resource of physical data center
* Virtual network: a set of virtual networking resources and virtual links
* In summary, data center network virtualization is different

from ISP network virtualization, because one has to consider

different constraints and resources, specific topologies, and degrees

of scalabity

### The facilities of a physical data center



# Wireless virtualization

Wen, H. K., Tiwary, P., & Le-Ngoc, T. (2013). Wireless Virtualization. In SpringerBriefs in Computer Science (pp. 41-81). Springer.

## Advantage of wireless virtualization

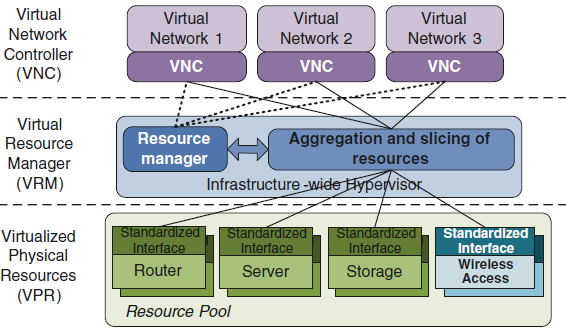
* In general, wireless virtualization can be interpreted as the sharing and abstraction of wireless access devices among multiple users or user groups with a certain degree of isolation between them.
* Resource can refer to the wireless equipment such as the basestation as well as low-level physical resources such as space-time-frequency slots
* Wireless virtualization can be applied to a larger variety of wireless architectures
* Due to the nature of wireless transmission, the penetration of virtualization into the MAC and PHY layer protocols might be necessary
* Thus, 802.11 WLAN technologies and cellular technologies, which satisfy the requirements of high data rate and high number of users, are the main focus of most active research in wireless virtualization.
* Wireless virtualization can also be referred to as wireless access virtualization

or the virtualization of the access and distribution of data through the wireless

medium

* Multiple access, multiplexing and spectrumslicing (refer to Sect. 5.8) techniques are used to allocate these fundamental resources.

## Virtualization architecture



* the virtualized physical resources (VPR), the virtual resource manager (VRM) and the virtual network controller (VNC). This classification fits the network virtualization meta-architectures presented in Chap. 3. The types of VPR considered in [8] include wireless access points and basestations. Each type of VPR has its own standardized interface since they can offer different types of services and functionalities. The VRM is the equivalent of the hypervisorlayer or the virtual machine monitor (VMM) in computer virtualization.

## Final model for network virtualization: Cloud-Centric Architecture for Rich Mobile Networking (from wireless virtualisation)

Wen, H. K., Tiwary, P., & Le-Ngoc, T. (2013). Wireless Virtualization. In SpringerBriefs in Computer Science (pp. 41-81). Springer.

* cloud-centric architecture proposed in is aimed at the support of multidimensionalmobility on a virtualized end-to-end service distribution network.
* One of the goals of this architecture is to maintain a personal cloud that seamlessly

accompanies the user. The emphasis is on the multi-dimensionality of the mobility.

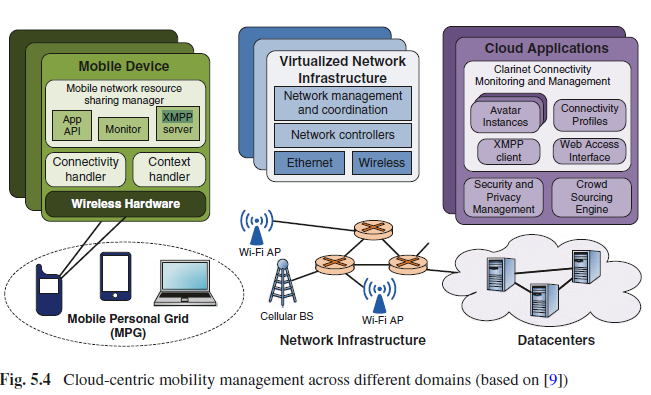
* The user can switch between different devices such as smart phones and laptops. Which is important for university students and staffs
* Ultimately, the user can be mobile across different network infrastructures such as the enterprise WLAN network, the public cellular network and the local area network at home.
* the user mobile devices, the virtualized wireless network infrastructure and the cloud service data centers.
* cloud-based personal connectivity manager application called “Avatar”. This personal assistant gathers resource usage statistics across all devices of the MPG and performs provisioning of handovers across different dimensions.

K.-H. Kim, S.-J. Lee, P. Congdon, in Proceedings of ACM SIGCOMM Mobile Cloud

Computing (MCC) Workshop, “On Cloud-Centric Network Architecture for Multi-

Dimensional Mobility,” (2012)

* Since this manager resides in the cloud, it has centralized visibility and access of user devices, which is necessary to maintain the MPG.



* Comparing the price from Public virtual network like Azure

# Cloud computing

## Cloud computing article

Dixon,Herbert B.,,Jr. (2012). Cloud computing.*The Judges' Journal, 51*(2), 36-38. Retrieved from <https://search-proquest-com.ezproxy.lib.monash.edu.au/docview/1032524464?accountid=12528>

* Cloud computing is the process by which a user can remotely access data and program applications-usually by use of a web browser over the Internet. Today, most users have several devices by which they need to access their data and applications, namely, office and home computers, a laptop, a tablet computing device, and a smartphone. **Related to BYOD**
* Cloud computing will allow the user to access the program over the Internet to view and edit the file as needed. Similarly, if a user needs a computer file he does not physically have with him, cloud computing allows him to access the file over the Internet, wherever the file happens to be stored.
* Often-cited advantages of cloud computing are (1) lack of need to purchase special software (other than an Internet browser) for the device that connects the user to the cloud, (2) no need for significant file storage space on that device, and (3) ease of collaboration among multiple users on documents stored in the cloud. The first two reasons are most often cited to support the conclusion that **cloud computing is often cheaper.**
* The reasons that cloud computing has increased are easy to understand. Businesses and individuals typically need to access files from their multiple computing devices. Also, the availability of faster Internet connections makes accessing files from each of these devices easier and more convenient. Finally, the cost of cloud computing is now within everyone's economic reach, with basic services being free in many instances.
* Businesses have gravitated to cloud computing for several reasons. First, there is often a **lower cost for using cloud services as needed compared to capital and personnel expenses incurred for storage, program applications, and computing capability on site.** Also, **computing tasks might run more quickly and be more efficient using cloud computing**, depending on the speed of the Internet connection if the business itself possesses less capable computing equipment on site, as compared with the computing equipment running the cloud. Lastly, the option to use and thus pay for cloud software services only as needed eliminates **the expense of purchasing and maintaining the software**.

## Cloud computing cost

## Virtualisation in cloud computing

Granville, L. Z., Esteves, R. P. and Wickboldt, J. A. (2015). Virtualization in the Cloud. In Cloud Services, Networking, and Management (eds N. L. da Fonseca and R. Boutaba). doi:[10.1002/9781119042655.ch2](https://doi-org.ezproxy.lib.monash.edu.au/10.1002/9781119042655.ch2)

* Clouds can be public, private, or hybrid. Public clouds offer resources to any interested tenant (e.g., Amazon EC2 and Windows Azure).
* Cloud services are organized according to three basic business models. In infrastructure as a service (IaaS), cloud providers offer logical instances of physical resources, such as VMs, virtual storage, and virtual links to interested tenants. In platform as a service (PaaS), tenants can request a computing platform including an operating system and a development environment.
* Virtualization is the key technology to enable **cloud computing**. Virtualization abstracts the internal details of physical resources and **enables resource sharing. Using virtualization, a physical resource (e.g., server, router, link) can be shared among different users or applications.**
* **Storage** virtualization consists of grouping multiple (possibly heterogeneous) storage devices that are seen as a single virtual storage space. There are two main abstractions to represent storage virtualization in clouds: virtual volumes and virtual data objects.
* Cloud infrastructures rely **on local and wide area networks** to connect the physical

resources (i.e., servers, switches, and routers) of their data centers. Such networks are still based on the current IP architecture that has a number of problems. These problems are mainly related to the lack of isolation, which can allow that one VI or application interferes with another, resulting in poor performance or, even worse, in security problems. Another issue is the limited support for innovation, which hinders the development of new architectures that could suit better cloud applications. To overcome the limitations of current network architectures, virtualization can also

be extend to the cloud networks. ISP network virtualization has been a hot topic of investigation in virtualized cloud networks, multiple virtual networks (VNs) share a physical network and run isolated protocol stacks. A VN is part of a VI that comprises VN nodes (i.e., switches and routers) and virtual links.

# An overview of virtual and cloud computing

H. Frank Cervone, (2010) "An overview of virtual and cloud computing", OCLC Systems

& Services: International digital library perspectives, Vol. 26 Issue: 3, pp.162-165, https://

doi.org/10.1108/1065075101107360

## Cons of traditional environment:

* In many cases, multiple servers may be used when an application services a high transaction volume or when there needs to be a high level of assurance that the failure of a single server will not cause an application to completely fail.
* Although it is simpler to deploy, low scalability occurs
* with *physical server clusters environment, increasing scalability requires additional hardware that exactly duplicates the current physical hardware. When a server is not busy, it is impossible to use the extra capacity of the server.*
* Not all applications will be suitable for this environment.
* It is harder to recover with physical server if natural disaster happens

## Virtual servers:

In a virtual server model, a different type of operating system runs on the physical

hardware. Known as a hypervisor or a virtual machine manager, this operating system

is specialized and designed to run other operating systems as applications. By doing

this, the traditional server environment can be encapsulated in an environment which

provides a layer of isolation from the underlying hardware. A hypervisor can run

multiple operating system environments and their associated applications in individual

virtual machines, each of which runs on a single physical machine. Each virtual machine

is presented with an environmental context that makes it appear as if they were running

natively as the only machine on the physical hardware. It is the job of the hypervisor to

simulate, emulate, or enable all of the functionality necessary for the virtual machine to

operate normally and with all of its functionality.

* Flexibility and scalability:

*Because of this flexibility in being able to move the virtual servers around the cluster,*

*scaling resources to meet the needs of virtual machines is also simplified. In most virtual*

*server implementations, several virtual machines are assigned to a single physical*

*server based on the assumption that none of the virtual machines will need the entire*

*computing power of the physical server. When a particular virtual machine does*

*consume all the processing cycles of the physical server, the hypervisor could migrate*

*the other less busy virtual machines to other physical servers to ensure no virtual*

*machine’s performance is significantly degraded.*

## Cloud computing:

Cloud computing provides an organization with appreciably more flexibility and scalability to satisfy computing needs. An organization can start out running an application on a single virtual server and ramp up as necessary because the cloud

provider hosts the applications on virtual servers. New virtual servers can be created in a

matter of minutes and, depending on demand, a server can be deactivated in a similarly

short amount of time.

* Advantages: cost saving, little capital investment (don’t need to buy so many servers)

*One of the significant advantages of cloud computing is the potential cost savings that can be gained. Usually cloud computing has little or no upfront capital costs.*

*Because of this ability to shift resources, additional hardware purchases can be deferred until the entire cloud cluster’s overall application load requires more computing power, rather than just a single application*.

* Concerns: security

*One of the ways cloud providers keep expenses down is to place data center in locations where the cost of real estate, utilities, and labor are low. Given this scenario, many clouds may be hosted in foreign countries.*

# Aggregated idea: cloud data center

* cloud data centers that can provide a wide variety of data and services to your handheld devices wherever and whenever you need it.
* Cloud data centers can contain tens of thousands of servers that must be connectedto each other, to storage, and to the outside world.
* When enterprise system administrators started to develop their own high-density data centers, they had no choice but to use the same networking gear as used in the

LAN.

* First, packets need to take multiple hops when traveling between servers. This increases latency and latency variation between servers, especially when using enterprise networking gear that has relatively high latency, as latency is not a concern in the LAN.
* In some cases, the service providers operating these large cloud data centers

have specified custom built networking gear from major ODMs and have written

their own networking software to reduce cost even further.

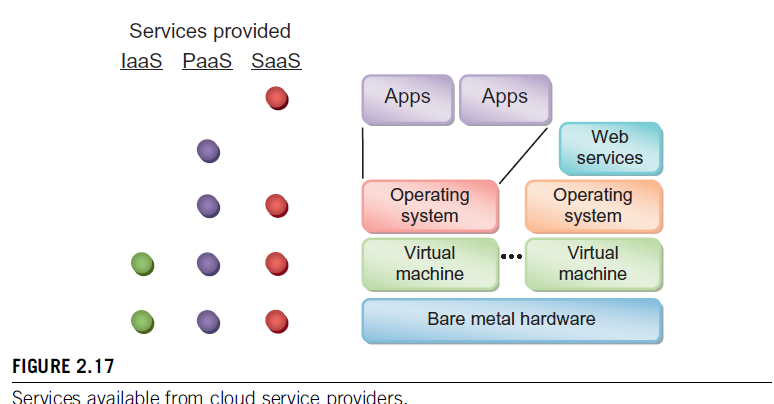
* By providing 10GbE links to the rack servers, the network can support the convergenceof storage and data traffic into one network, reducing costs. As shown in the figure, ToR switches are used with high-bandwidth links to the core and the core routers have been replaced with simpler core switches with a larger number of ports

allowing them to absorb the aggregation function, making this a “flatter” network.

* Driving forces

Designing, building, and maintaining a large corporate data center is a costly affair.

Expensive floor space, special cooling equipment, and high power demands are some of the challenges that data center administrators must face. Even with the advent of virtualized servers, low server utilization is a common problem as the system administrator must design for periods of peak demand. (before and after school)

* 
* Infrastructure as a Service (IaaS) includes hardware resources such as servers,

storage, and networking along with low-level software features such as hypervisors

for virtual machines and load balancers.

* Platform as a Service (PaaS) includes higher layer functions such as operating systems and/or web server applications including databases and development tools. Software as a Service (SaaS) provides web-based software tools to both individuals and corporations.

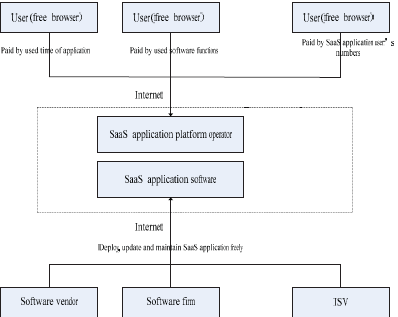
# SaaS

Hancheng Liao. (2010). SaaS business model for software enterprise. 2010 2nd IEEE International Conference on Information Management and Engineering, 2, 604-607.

* “Software as a Service is time and location independent online access to a remotely managed server application” [5].

Markku Sääksjärvi.et al, Evaluating the Software as a Service Business Model: from CPU Time-Sharing to Online Innovation Sharing, IADIS International Conference e-Society 2005

* Generally, SaaS adopted Multi-tenancy architecture, namely, a set of standard hardware equipment and software system could provide services for many different customers at the same time Software suppliers provide Internet applications and the software's offline operations and local data storage, customers leased certain software services to manage their business activities without an amount of investment for hardware, custom software, personals except personal computer and Internet connection software (mostly free).
* SaaS software applications are paid according to the number of rented software functions or the used length of time by customers (important for university - peak time and off-peak time)
* SaaS model can reduce the purchasing and maintain infrastructure and application costs. and expands the ASP application scope.



* SaaS software has some main features: centralized management; Single Multi-tenancy,; isolation data among the different customers for the security and the privacy of each data, which has personalized surface, business logic, data structure and so on
* Data transferred by network would likely make all data not to use unsafe if SaaS operators’ system or network failure; Trojans, viruses, and unexpected disasters and other factors, would make the data lost and sabotage.
* Low cost delivery and applying SaaS application greatly reduce the enterprise informatization cost, so SaaS model could be a simple way to the current deep end of enterprise informatization.