Cloud Computing Assignment- Software, Systems and Applications

mdsw22
School of Engineering and Computer Science,
Durham University,
Durham, UK
christian.johnston@durham.ac.uk

*For section (1d) I analyse product offering from different providers **throughout** the essay.*

Company

The business is in the healthcare industry; providing a health-monitoring product.

Characteristics of the company include:

- Large bandwidth of confidential data
- 24/7 operation
- Custom software stack
- Infinitely scalable product
- Variable demand load

The company *currently* stores Electronic Medical Records (EMR) on a database held on local infrastructure.

The company's business critical infrastructure includes:

- Web server
- Sales server
- Servers storing EMR (confidential patient data)

Aim

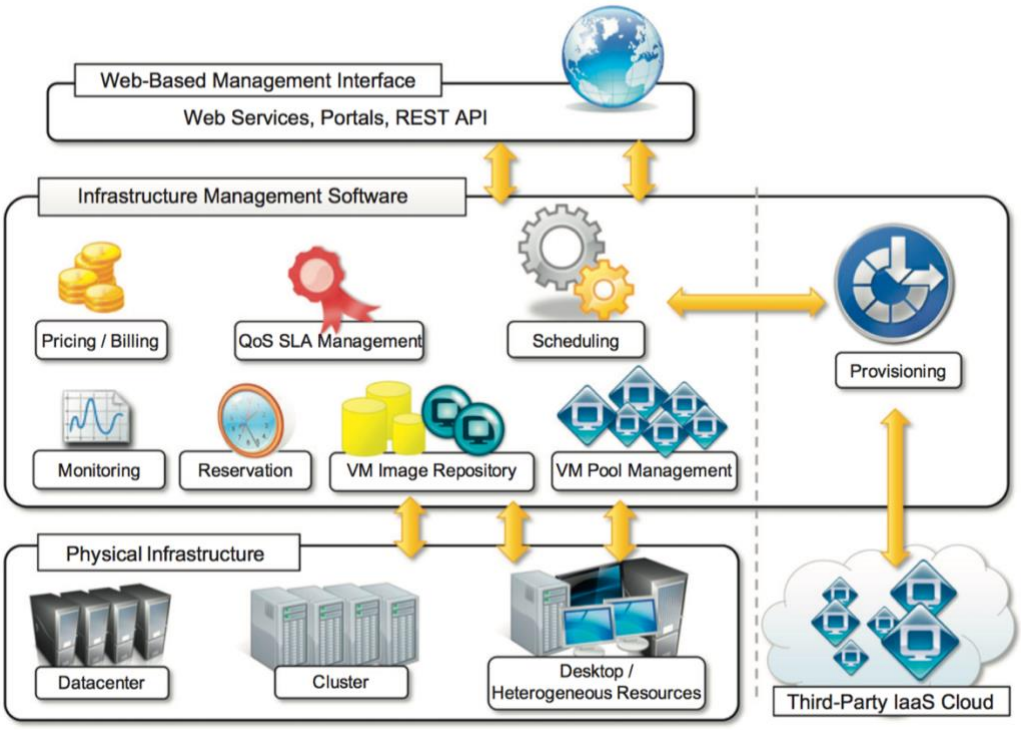
This brief will advise your company on how to manage a deployment of your business-critical infrastructure to the cloud in terms of infrastructure and security whilst also looking at future trends which may have implications on how you manage your cloud deployment.

Introduction

When your company considers migrating its business-critical infrastructure to the cloud, you must take into consideration factors including: behaviour of the application in a multi-tenant environment, deployment method, QoS offered, costs, security and scalability.

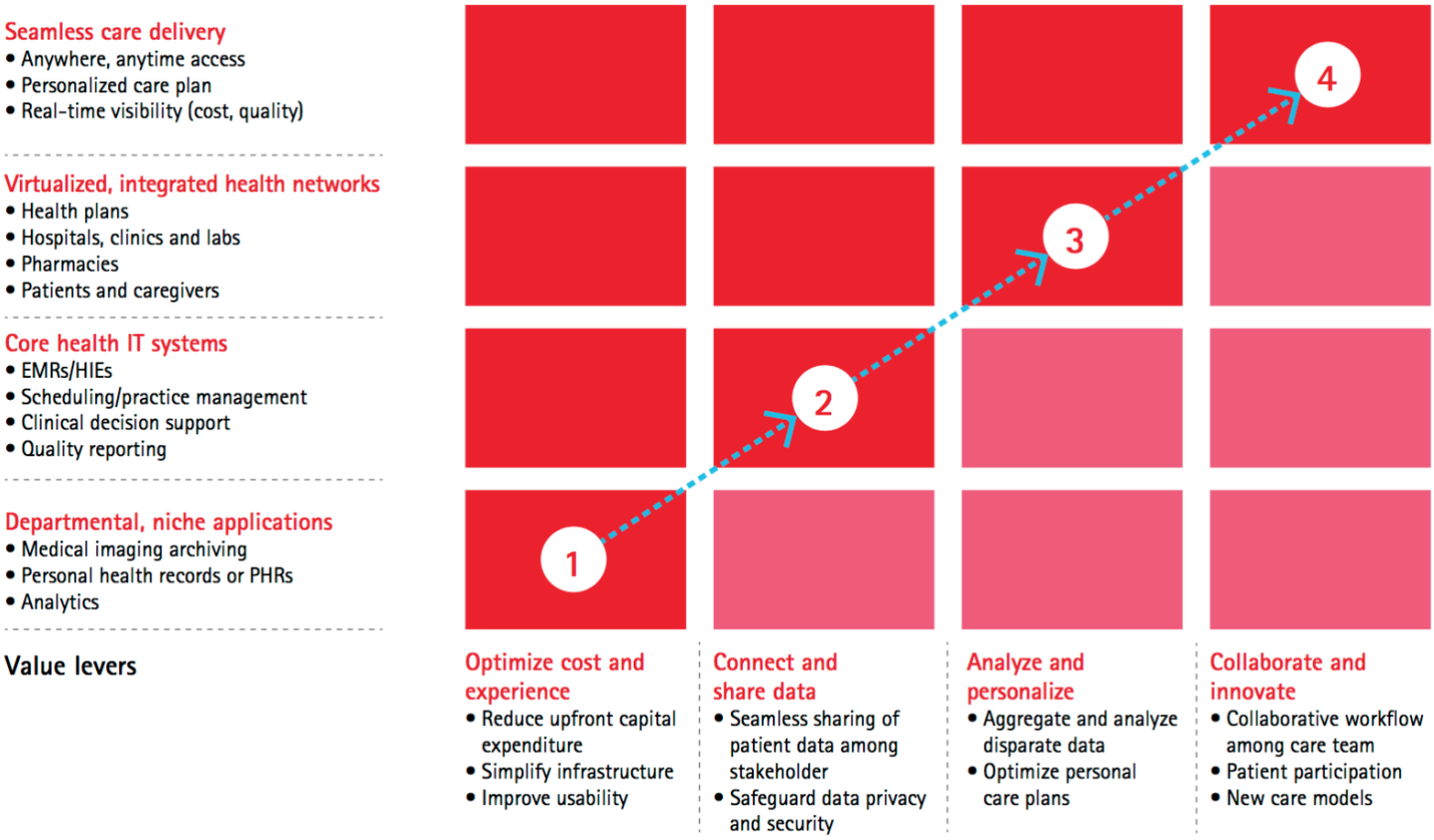
As your company implements a custom software stack, you are looking to utilise the Infrastructure as a service (IaaS) cloud delivery model. This will reduce both capital and administration costs and allow you to take advantage of the customisation offered by virtualization while the cloud service provider (CSP) manages physical processing, storage and networking.

Diagram below showing IaaS reference implementation. [1]



Analytic capabilities utilised through cloud services can support healthcare staff's cognitive capabilities; mitigating medical mistakes and minimising patient adverse events. Clouds can enable your company to access a body of medical knowledge to improve differential diagnosis and treatment planning, leading to more personalized care. [2]

Diagram below illustrates the cloud maturity model for the healthcare industry. [3]



1. Infrastructure Management

a) Deployment techniques

In the case of public clouds, the CSP is in control of the infrastructure and thus of the customers' data. This lack of control could be perceived as a risk due to the confidential nature of patient data.

There are monetary benefits to moving infrastructure to a public cloud as it reduces long term TCO, improves cash flow and helps shift from CAPEX to OPEX. These costs can be controlled according to business needs.

A problem that comes with migrating business-critical infrastructure to a public cloud is that this core infrastructure becomes isolated from the operational site creating a problem of sending data between them, often across country boundaries with different data laws. If your organisation is subject to third-party compliance standards, specific

procedures will have to be used when deploying applications, which may not be possible in a public cloud.

An alternative is private clouds where the business application is implemented on top of private infrastructure, keeping all operations in-house. Security concerns are reduced since information does not flow out of the private infrastructure. A major drawback is the inability to scale on demand to address peak loads.

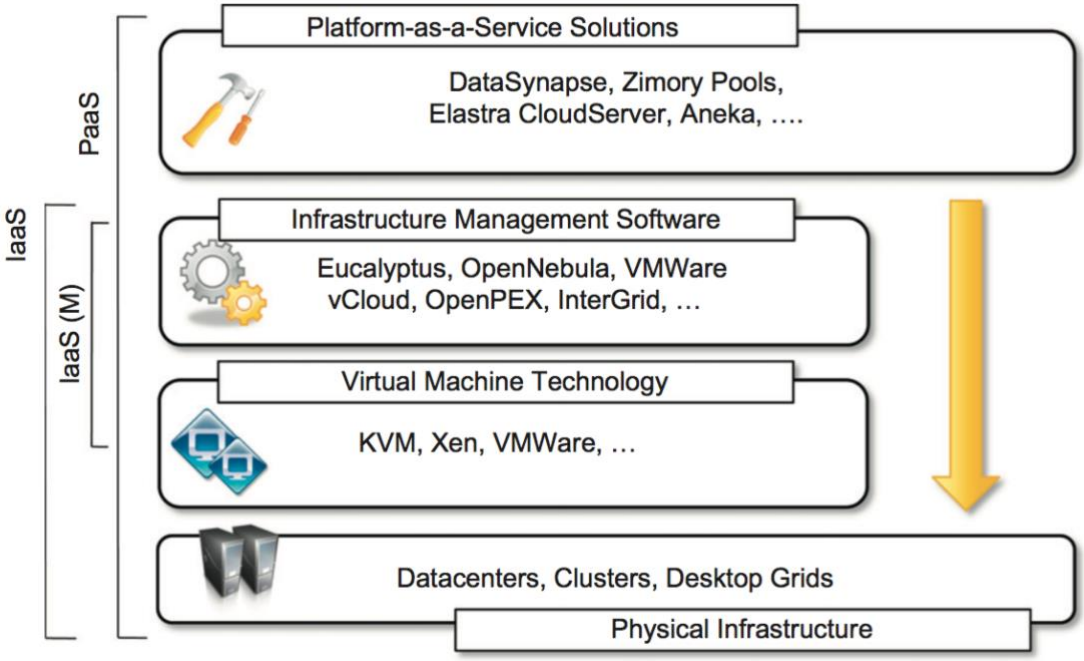
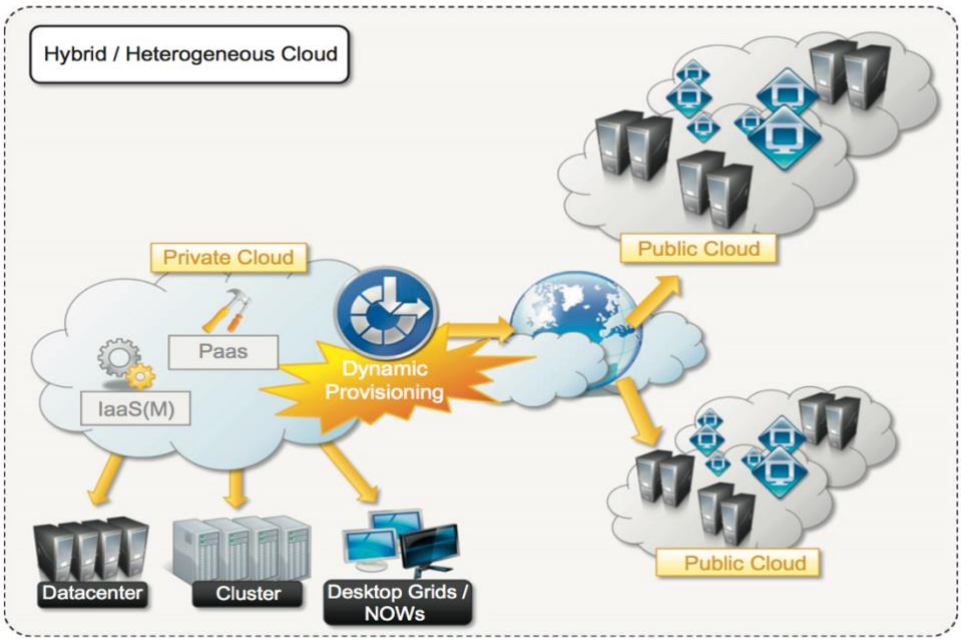


Diagram showing private clouds hardware and software stack. [1]

A balance is hybrid clouds, maintaining sensitive information within the premises. Security concerns are limited to the public portion of the cloud used to perform operations with less stringent constraints. Scalability issues are addressed by leveraging external resources. This concept is known as ‘cloudbursting as in the event of a spike in demand, the application can be deployed to the public cloud. [4]



Another solution suggested by Dillon et al is a Virtual Private Cloud (VPC); a platform running on top of a public cloud leveraging virtual private network (VPN) technology, allowing CSPs to design their own security policies such as firewall rules. [5]

The business could also utilise community clouds; infrastructure shared by several organizations, implemented over multiple administrative domains. The naturally hybrid deployment model of community clouds supports storing patient-related data in a private cloud while using the shared infrastructure for non-critical services and automating processes within hospitals. [1]

	Infrastructure management	Infratructure ownership	Infrastructure location	Access and consumption
Public cloud	Third-party provider	Third-party provider	Off-premise	Untrusted
Private/community cloud	Organization or third-party provider	Organization or third-party provider	On-premise or off-premise	Trusted
Hybrid cloud	Both organization and third-party provider	Both organization and third-party provider	Both on-premise and off-premise	Trusted and untrusted

Table above illustrating the various deployment models. [6]

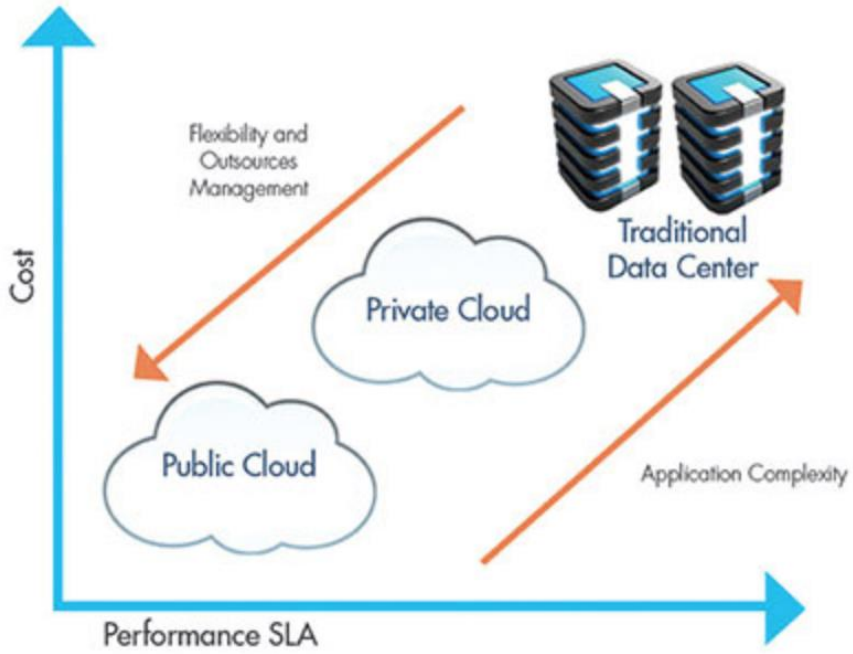


Figure above illustrating business strategy driving cloud selection. [7]

b) Autonomic Management

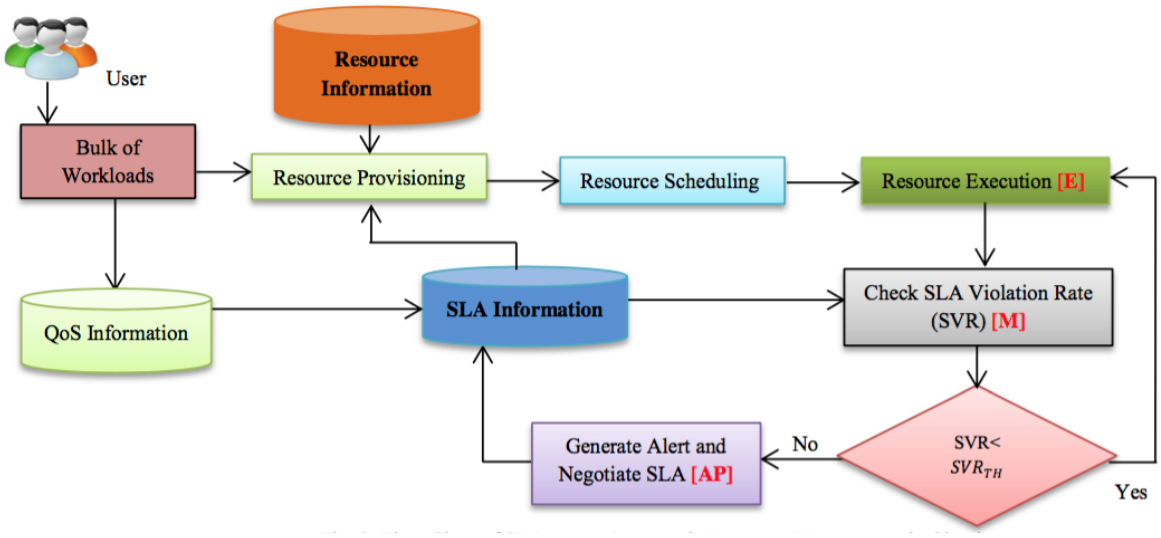
In an autonomic system, instead of controlling the system directly, the cloud consumer defines rules that guide the self-management process.

IBM defines the following four properties [8]:

1. Self-configuration.
2. Self-healing.
3. Self-optimisation.
4. Self-protection.

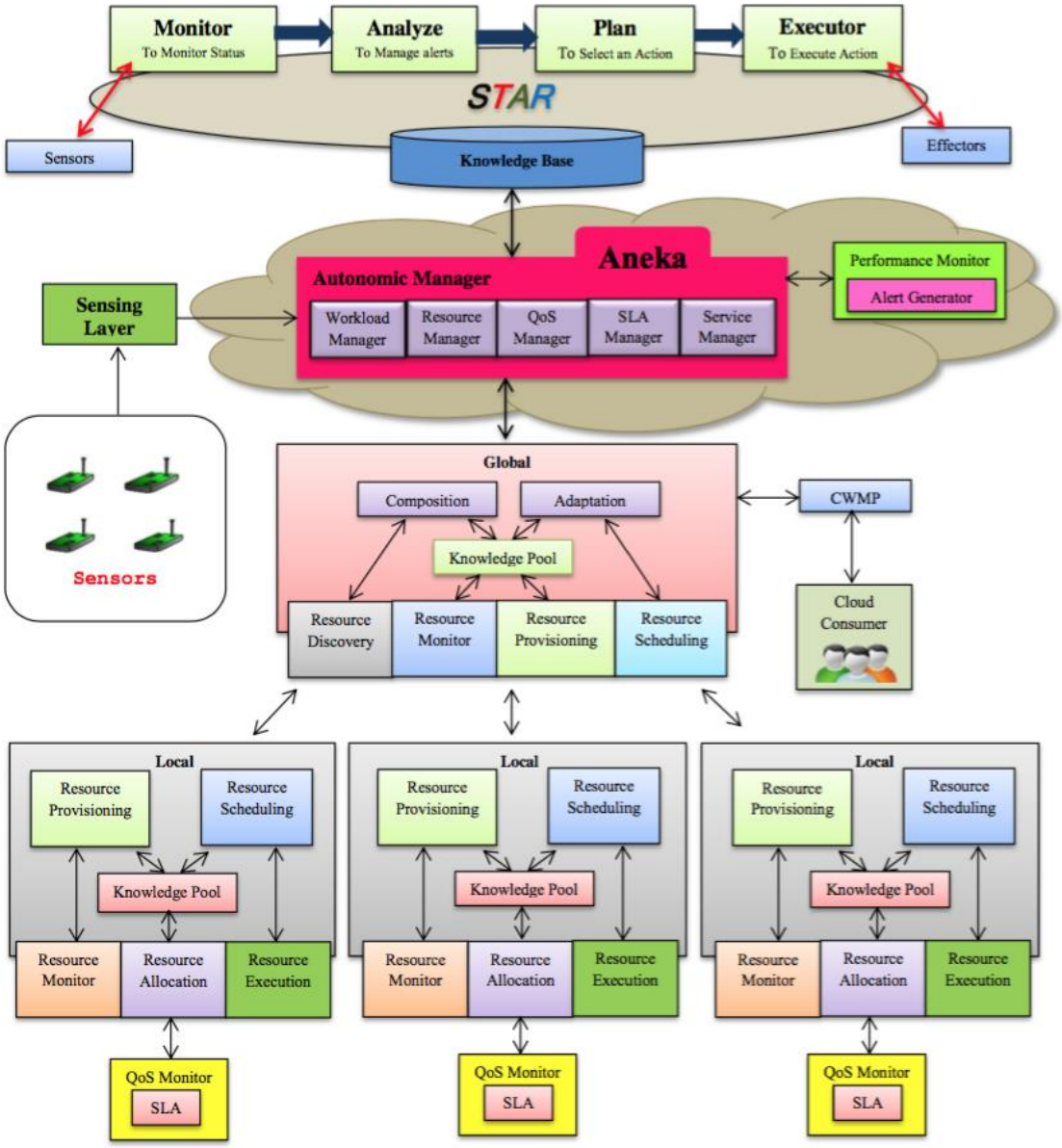
I suggest using a Control Loops concept which monitors a resource autonomously, keeping parameters within a desired range. The challenge is to optimise a server cluster to provide a desired response time whilst minimising the number of virtual machines (VMs) deployed. [9]

One solution is Amazon's 'Elastic MapReduce' which allows its customers to dynamically modify the size of their running job queues and to modify resource utilisation. [9] Moreover, Amazon's Elastic Compute Cloud offers a system that auto-scales groups of instances based on alert mechanisms that trigger the deployment of new instances when some condition is met. These mechanisms are based on infrastructure metrics such as load and bandwidth consumption. [10]



Flow chart above illustrating a Service Level Agreement (SLA) aware Autonomic Resource Management in Cloud. [10]

Singh et al suggest a series of sensors and QoS monitors to measure the impact of QoS parameters on SLA violation rate. (illustrated in diagram below) [10]



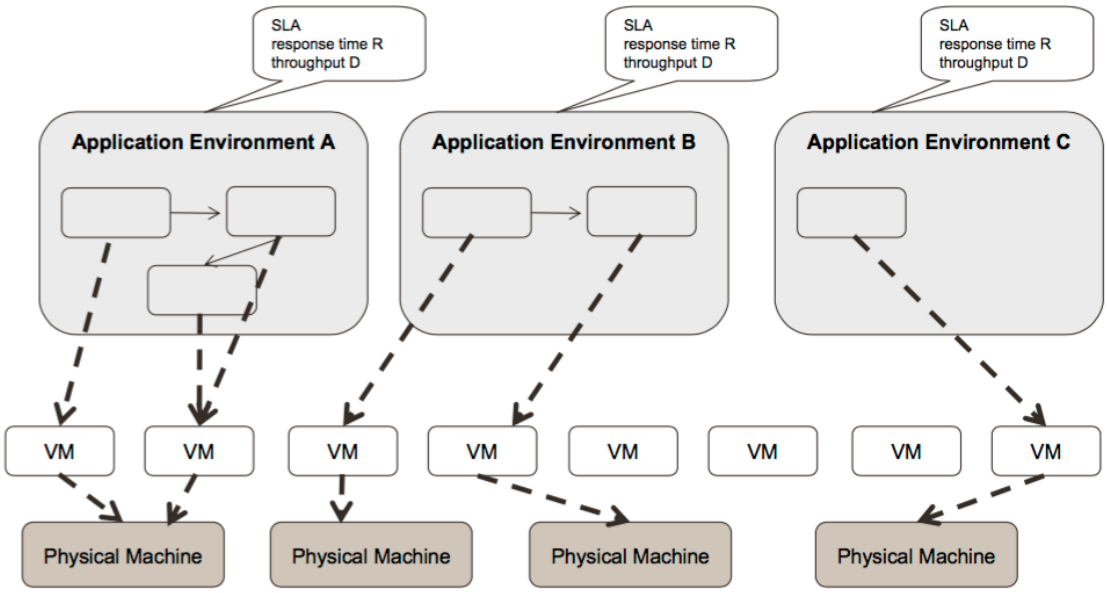
Solomon and Ionescu suggest building an autonomic system via object composition. The system obtains functionality dynamically by choosing appropriate components and composing them into an autonomic system. Each of the components performs only one role, thus providing high cohesion and low coupling. [11]

Lui et al suggest a different approach; 'worker agents' are attached to physical resources as well as VMs and their role is: monitoring events, interacting with other agents, making resource management decisions according to their local rules under the supervision of network management processes ensuring that the behaviour of worker agents conforms to global objectives. [12]

Leite et al suggest using a goal-oriented autonomic system which exhibits context

aware properties and implements a hierarchical P2P overlay to manage the VMs and to deal with inter-cloud communication. [13]

Finally, Van et al propose an autonomic resource manager to control the virtualised environment, decoupling the provisioning of resources from the dynamic placement of VMs. This aims to optimise a global utility function, integrating both SLA fulfilment and operating costs. The system relies on a two-level architecture with a separation between application functions and a global decision level, illustrated in the diagram below. [14]



c) Scalability under constraints

The IaaS model provides scalability due to virtualisation that can rapidly respond to a variable demand load. Despite this, there are a number of constraining issues to take into account including: scalable data storage, network issues and conventional data-centre architecture.

Scalable data storage is not yet feasible and so the choice is between proprietary storage and challenges for interoperability. Amazon and Google each rely on key-value store, which is scalable but doesn't allow storage of complex table structures and so these solutions most likely lack the power required for your business application.

There are considerations around network limitations, especially if your company plans to send large volumes of data over large distances. A study in 2010 calculated that

shipping 10 terabytes of data from California to Seattle would take 45 days and cost $1000 in network transfer fees. [15]

Hao and Lakshman propose a design based on network virtualization utilising forwarding Elements (FEs) and a Central Controller (CC). Packet handling actions are handled by FEs and the CC stores control information such as addresses, location, and policy. This offers effective isolation between customers whilst allowing physical resource sharing, increasing the potential for scalability. [16]

In conventional data centres, a layered multi-root tree architecture is commonly used, however this architecture cannot support a large-scale data centre with tens of thousands of servers in one site. The main problem is the shortage of bandwidth in higher layers and thus it becomes a bottleneck for the entire network.

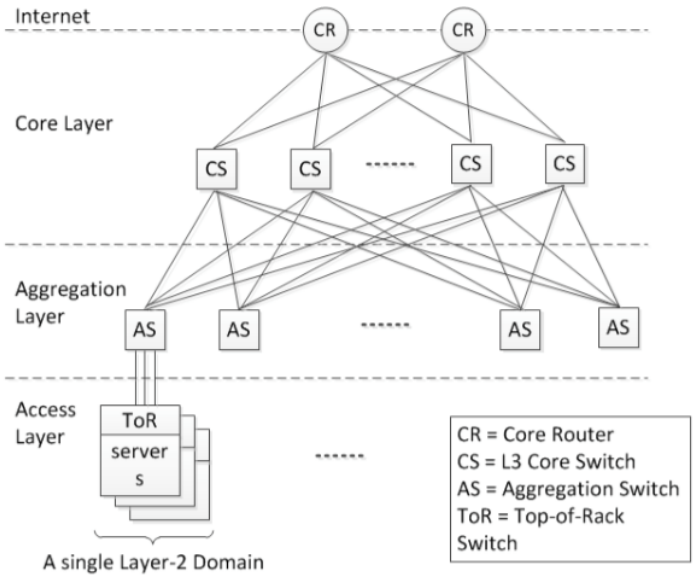


Fig. 1. A conventional network for data centers

Sun et al suggest a new architecture; using switches and servers arranged in rows and columns that compose a matrix structure. A network based on this architecture can accommodate up to hundreds of thousands of servers with improved scalability. [17] Moreover, I suggest integrating elastic load balancers into your system, distributing traffic across multiple instance and utilising network-side scripting.

One further issue with scalability is identifying when a request for increased resources is due to a DoS attack. Solutions to this are proposed in a later section.

d) Product offerings from different providers

There are numerous cloud service providers, each with their own product offerings including Microsoft Azure and Google Cloud Platform however Amazon Web Service (AWS) leads the pack with 40% market share.

For compute, AWS' offering is its EC2 instances and also provides services such as Beanstalk for app deployment, the EC2 Container service and AWS Lambda. Azure's compute offering is centred around VMs with other tools such as Cloud Services and Resource Manager to help deploy applications to the cloud. All three cloud providers support relational databases as well as NoSQL databases with Azure' DocumentDB, Amazon DynamoDB and Google Bigtable. AWS storage includes its Simple Storage (S3), Elastic Block Storage (EBS) and Elastic File System (EFS). Microsoft's offerings include its core Azure Storage service as well as Table, Queue and File storage.

service		provider	GB/month
Block Storage	w	Rackspace Cloud	$0.12
Cloud Files	w	Rackspace Cloud	$0.1
Cloud Storage	w	Google Cloud Platform	$0.026 (standard) / $0.02 (DRA[1])
Data Lake Store	w	Microsoft Azure	$0.04
Simple Storage Service (S3)	w	Amazon Web Services	$0.03 (standard) / $0.0125 (infrequent)
Storage	w	Microsoft Azure	$0.024 (LRS[2]) / $0.048 (GRS[3]) / $0.061 (RA-GRS[4])

Table to right displays the pricing of a Linux VM per month.

Provider	Pricing
OVH	$4
Internap	$8
1&1	$10
DigtialOcean	$10
AliCloud	$12
CloudSigma	$17
Google	$24
Rackspace	$27
CenturyLink	$27
ProfitBricks	$28
IBM SoftLayer	$35
Cogeco Peer1	$37
Microsoft	$37
Interoute	$37
Joyent	$48
AWS	$49
Dimension Data	$58

AWS is the most popular and trusted HIPAA-compliant provider for hosting healthcare applications. AWS has utility-based cloud services to process, store, and transmit Protected Health Information (PHI). They sign a business associate addendum (BAA), clarifying how your HIPAA obligations will be shared with AWS. Azure is certified according to HIPAA and ISO 27001, providing a compliant foundation for healthcare customers

Lock-in refers to the challenges faced by a cloud customer attempting to migrate between CSPs. Currently, each cloud offering has its own way on how cloud clients interact with the cloud, leading to the "Hazy Cloud" phenomenon. [18]

Using open standards such as SAML (Security Assertion Markup Language) helps to ensure portability and developing an Identity Access Management (IAM) system to support SAML assertions will aid future portability of systems to the cloud. [19] The Open Virtualization Format (OVF) is an attempt to provide a common format for storing the information describing a VM image as the use of proprietary formats is a major reason for vendor lock-in. [20]

Sotomayor proposed the notion of Virtual Infrastructure Management system to replace VM API interactions in order to accommodate multiple clouds for an organisation. This provides a single resource usage model, user authentication model and API to shield cloud providers heterogeneity. [21] Similarly, Dillon and Wu suggest the use of an intermediary layer between the cloud consumers and the cloud-specific resources. [5]

Cloud Infrastructure Management Interface (CIMI) is an API specification for managing cloud infrastructure. CIMI's goal is to enable users to manage cloud infrastructure way by standardising interactions between cloud environments to achieve interoperable cloud infrastructure management between CSP and consumers.

In some cases, different CSP’s have to interact with each other for completing a particular task. All data has to be encrypted for security purposes and management becomes a difficult task in such situations. A proposed solution to consider for interoperable security is the use of WS-Security for authentications so the controls can be interoperable with other standards-based systems. [19]

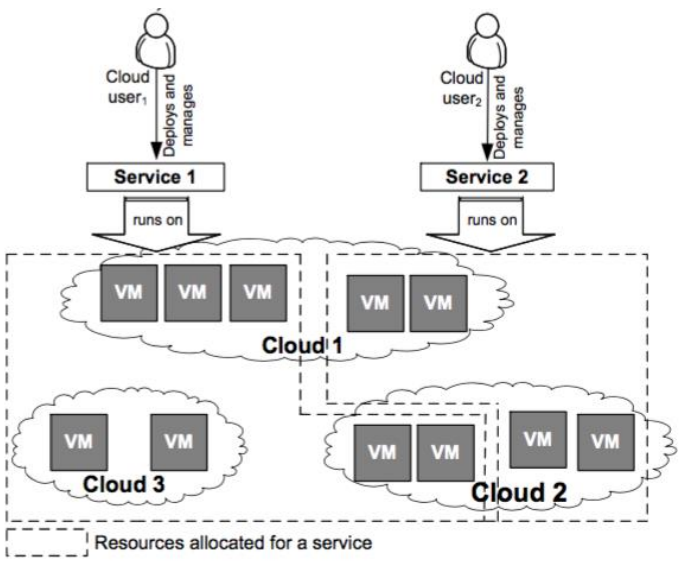


Diagram above is an example of an inter-cloud scenario, where two different services run on resources distributed across multiple clouds [13].

You could also utilise a cloud-brokering architecture, using a broker to serve as an intermediary between users and providers. This would help to choose the most suitable cloud on which to deploy the application and even lets you deploy different service components across multiple clouds.

2. Security

There are three IaaS domains:

1. Machine virtualization- deals with concerns in a multitenant environment
2. Network virtualization- an effect of infrastructure sharing
3. Physical Domain- infrastructure such as the CSP's datacentre holds customer's data and thus need securing.

In the cloud, responsibility over security is divided among parties including the cloud user, the CSP and any third-party vendors that users rely on for security software.

The cloud user (your business) is responsible for application-level security and the CSP is responsible for physical security, enforcing external firewall policies and securing VM images repository.

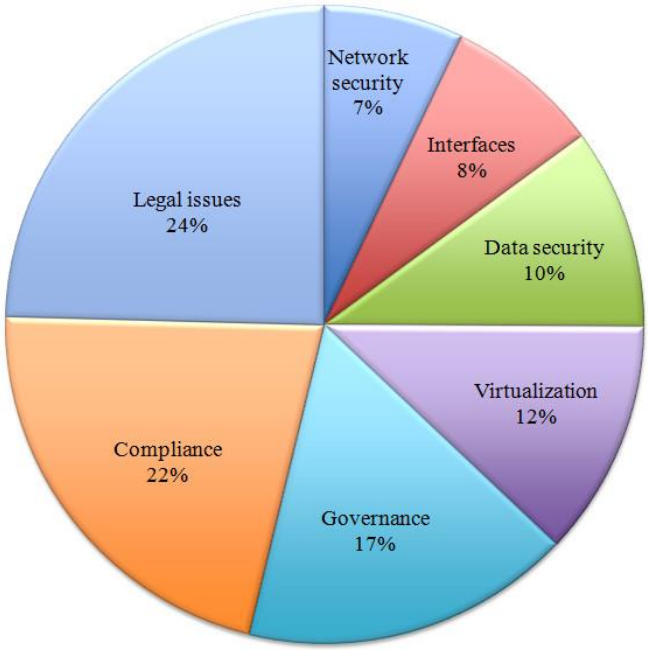
A hypervisor is the main controller of any access to the physical server resources by VMs and hypervisor security is the responsibility of cloud provider and the service provider (SP). In this case, the SP is the company that delivers the hypervisor software such as VMware. [22]

The VM's security is the responsibility of cloud consumers as each consumer can use their own security controls based on their needs, expected risk level and their own security management process.

Properties of a *secure* information system:

1. Confidentiality
2. Integrity
3. Availability

A secure cloud should also protect data storage and ensure proper access control.



Nelson Gonzalez broke down security issues into 7 main categories. [51]

Some security management processes will be required regardless of the nature of the organization's business:

- Security Policy implementation
- Intrusion detection
- Virtualisation security management

a) Data Management and Protection

In regard to data storage, you must consider who manages and has access to the data and where is it stored and so what data-laws apply. In healthcare applications, use and disclosure of protected health information (PHI) should meet the requirements of Health Insurance Portability and Accountability Act (HIPAA). [23] Moreover, without knowing the specific location of data storage, the provision of data protection acts for some region might be violated - the USA Patriot Act provides its government and other agencies with limitless powers to access information. [24]

One solution to data *availability* is Google File System (GFS) which is a distributed-file-systems. Compared with traditional file systems, GFS is optimized to run on data centres providing high data throughputs and low latency. It achieves availability by replicating the data across servers stored on geo-diverse nodes. [25]

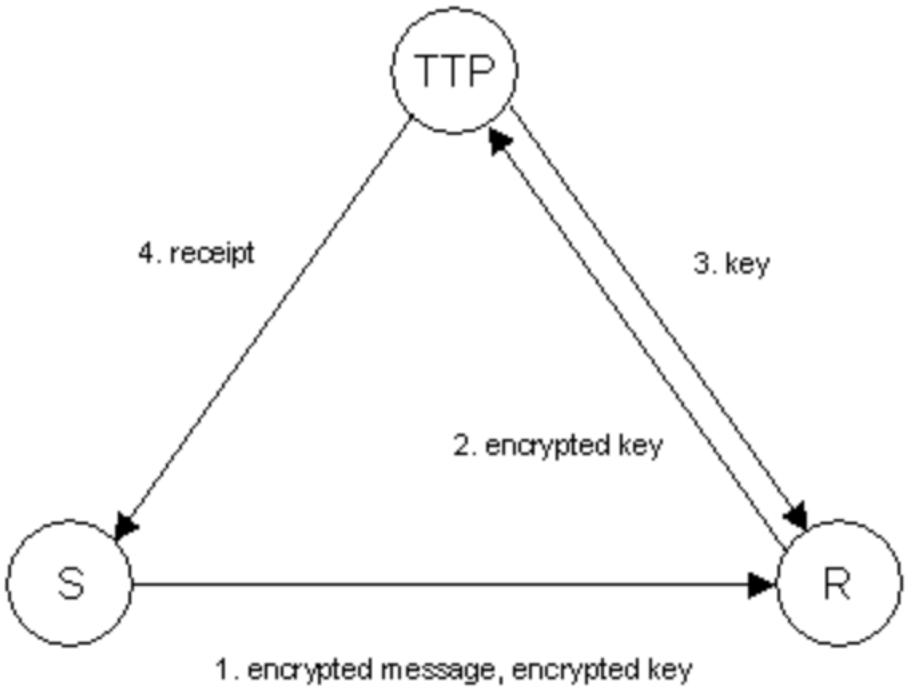
One solution for *confidentiality* is to apply cryptographic methods, disclosing data decryption keys only to authorized users. [26] Such solutions introduce a computational overhead when fine-grained data access control is desired and thus do

not scale well. Encryption can come in different forms; application encryption, network encryption such as SSH and TLS or proxy based encryption [19]. A proxy encrypting approach was successfully used by TC3; a company with sensitive patient records, when moving their HIPAA-compliant application to AWS. [27] I suggest conforming to a practice called crypto-shredding, deleting encryption keys when there is no more use of the data.

IPSec, an IP layer protocol that enables the sending of cryptographically protected packets, can provide data *confidentiality* and users are able to authenticate themselves using Public Key Infrastructure (PKI) certificates in a way that enhances scalability, as only the trusted CA (Certification Authority) need to be transmitted beforehand. [28]

Since a cloud application is hosted in a virtual environment it becomes accessible to the VM manager. The lack of control over data poses problems for the trust we give to CSP and the level of privacy we want to have for our data. One solution to this is tokenization, suggested by Dubey, where data is replaced by a unique id symbol that carries the essential information without compromising the security of sensitive data. [29]

In a public cloud, control is migrated to the infrastructure owner to enforce a sufficient security policy. Zissis and Lekkas propose a solution to this which is to use a Trusted Third Party within a cloud, which can address the loss of the traditional security boundary by producing trusted security domains. [29] See diagram below illustrating use of a TPP.



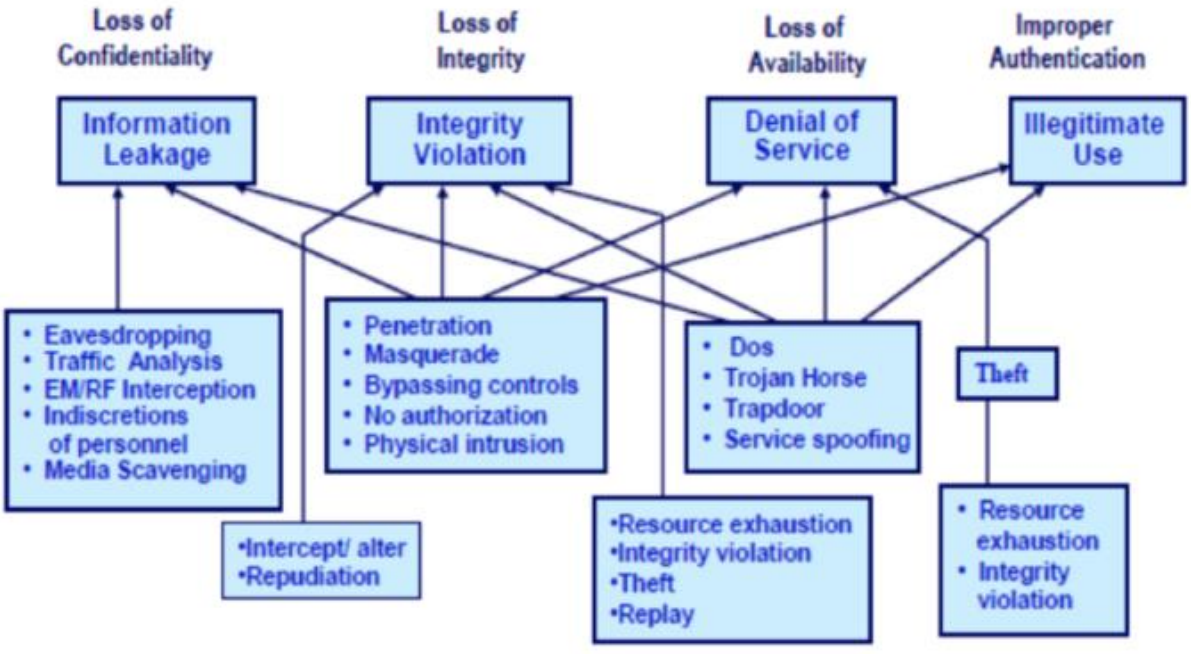
Sensitive data can be made ‘self-protecting’ by having security and authorization access built into the metadata itself. This enables the security to flow with data ensuring it is only readable by authorized individuals. Moreover, you could also employ a watermarking technique to protect shared data objects which will tighten the data access-control in public clouds.

Finally, data dispersion is a technique that improves data security through fragmentation. A file is split into n fragments where they are all signed and sent to *n* remote servers. The user can then reconstruct the file by accessing m arbitrarily chosen fragments. Splitting data adds extra cost and affects the system performance. [5]

In the healthcare industry, Li et al suggest a mechanism for data access control to Patient Health Records (PHR) on untrusted servers. To achieve fine-grained and scalable data access controls, the system utilises attribute-based encryption (ABE) techniques. This framework divides users in the PHR system into multiple security domains, reducing the key management complexity and allowing dynamic modification of access policies and file attributes. [30]

b) Potential Threat Vectors

There are various threat vectors in a cloud environment including network, infrastructure and datacentre which will lead to a breakdown of one of the properties of security, illustrated in the diagram below.



Virtualisation and a multi-tenant environment

Multitenancy issues arise as both the attacker and the victim are sharing the same server, introducing side channels. AlJahdali et al notes that risks can be mitigated using specific resource isolation techniques [31]. Salesforce.com employs a query rewriter at the database level whereas Amazon uses hypervisors at the hardware level. [32]

Virtualization in general increases the security of a cloud environment as a single machine can be divided into many VMs; providing data isolation and safety against attacks. Although CSP's such as Amazon have VM monitors in place to detect malicious or illegal activity; this security measure cannot fully prevent compromised VMs from extracting confidential information. [33]

Key management is a critical issue in cloud infrastructures, as the virtualisation of services obscures the identification of the physical key storage location, disabling traditional protection mechanisms. One solution is to deploy tamperproof devices for key protection such as user smarts cards coupled with Hardware Security Module as proposed by Zissis. [29]

Physical threats

DoS attacks against a virtualized system are as prevalent as against non-virtualized systems but because the VMs share the host's resources, the threat of an attack against another is greatly increased. Krutz suggests deploying perimeter defences on the VMs such as intrusion detection systems. [4]

Mitigation techniques are available against SQL injection attacks such as avoiding usage of dynamically generated SQL queries and filtering techniques on user input. Bhadauria and Sanyal suggest a proxy-based architecture which dynamically detects and extracts users' inputs for suspected SQL control sequences. [34]

Attackers can strike by creating their own module within the cloud and tricking the system to treat that malicious instance as valid. In solution to this, you could setup a Database Activity Monitoring (DAM) system which alerts based on policy violations. [19]

Network level security

All data flow over the network needs to be secured in order to prevent leakage of sensitive information. This involves the use of network traffic encryption techniques such as Secure Socket Layer (SSL) and Transport Layer Security (TLS). In the case of AWS, the network layer provides protection against traditional network security

issues such as Man-In-The-Middle attacks, IP spoofing and port scanning. For maximum security, Amazon S3 is accessible via SSL encrypted endpoints. [36]

One potential threat vector is the CSP as they control the "bottom layer" of the software stack, circumventing most security techniques. Businesses can monitor for internal data migrations using DAM which can be combined with URL filtering and Data Loss Prevention tools to help monitor network traffic. [19]

VMs of different customers often reside on the same physical machine and data packets share the same LAN. Hao and Lackshman explore a "middle ground", where users share physical hardware resources but user networks are isolated and accesses are controlled. [36]

Identity Management, Authentication and Access Controls

Due to the multi-tenant environment, cloud platforms should deliver a robust identity management system which should cover cloud users with corresponding identity information. Such system should adopt existing standards, such as SPML, SAML, OAuth, and XACML to securely combine identities among interacting entities within different domains and cloud platforms.

Diagram below from [36].

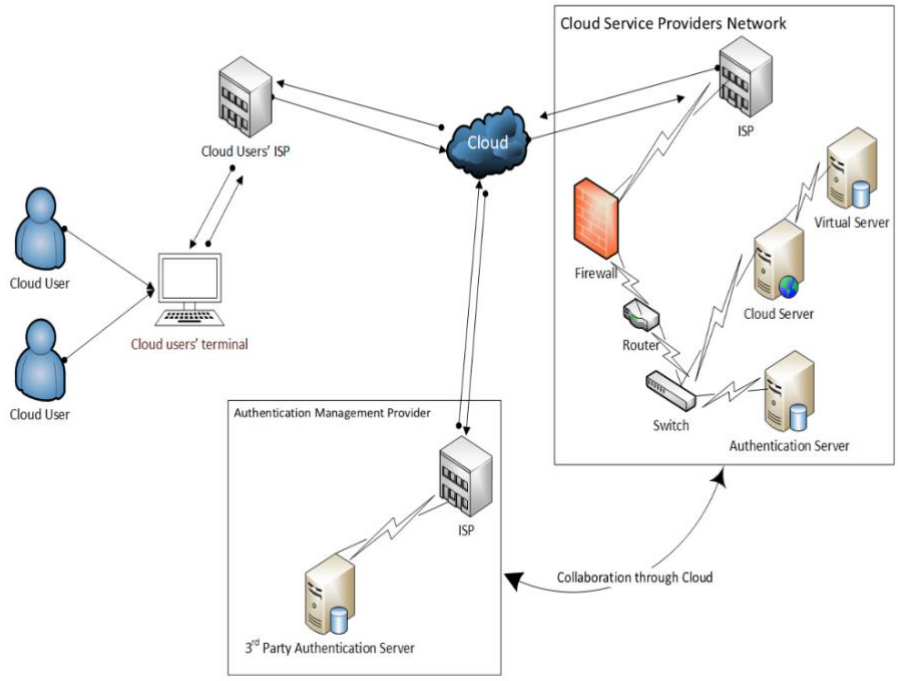


Figure 3: Authentication in the Cloud

CSPs and users are often not in the same security domain and thus traditional identity-based access control models are not effective. Takabi et al suggest using identifiers and attributes to help define a user which takes away the complexity of identity management. [37] Moreover, many cloud providers use weak, password-based authentication which could be improved using trusted authentication mechanisms based on public keys such as X.509 certificates or the Lightweight Directory Access Protocol. [15]

Single sign-on (SSO) addresses the problem of authentication across multiple clouds-enabling providers to define federated identities that they can share securely across different sites. [15]

Diagram below illustrates the use of a CA, validating who sent a query.

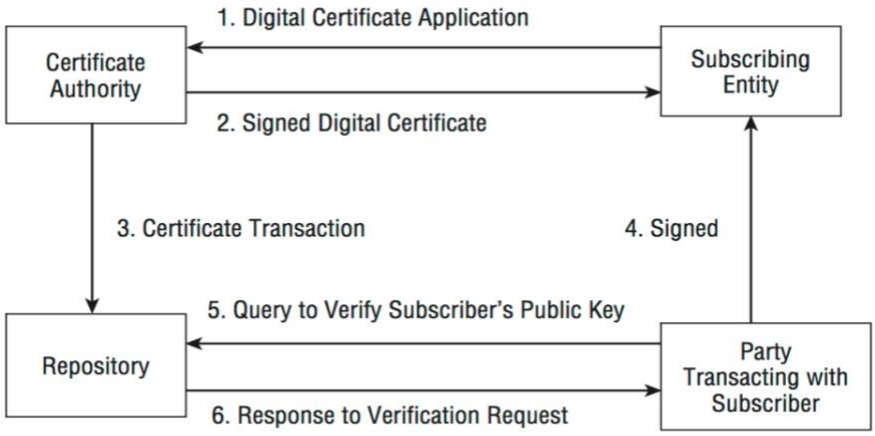


Figure 6-5: A transaction with digital certificates

Security SLA

Casola et all suggest a system to automatically acquire and configure cloud resources to deploy security-related software components for the enforcement of a Security SLAs. The proposed approach is based on:

(i) Matching customers' security requirements with security mechanisms.

(ii) Automatic deployment of software components providing the desired security mechanisms. [38]

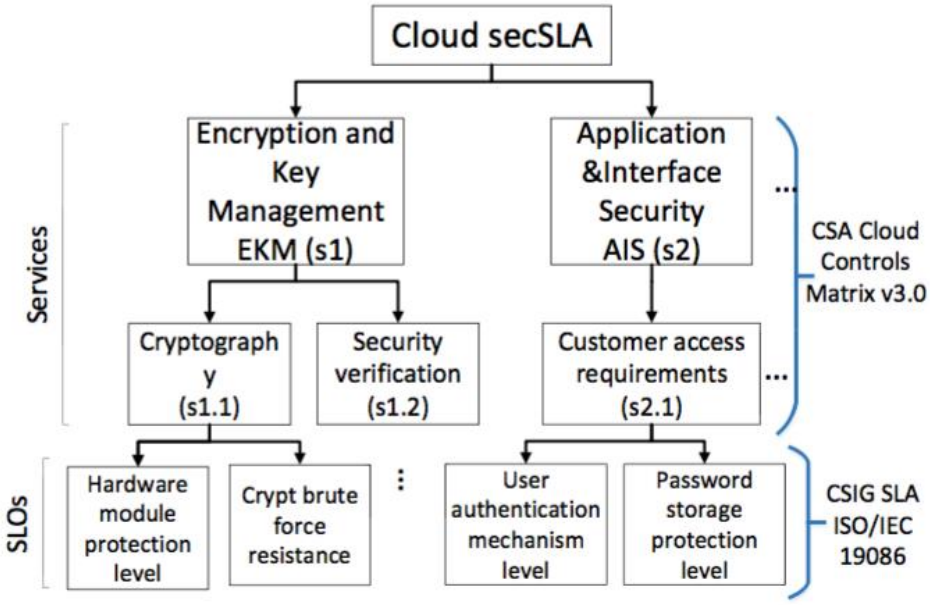


Diagram above illustrating cloud security SLA hierarchy. [39]

3. New trends within Cloud Computing (Focus on IaaS)

IoT and Big Data

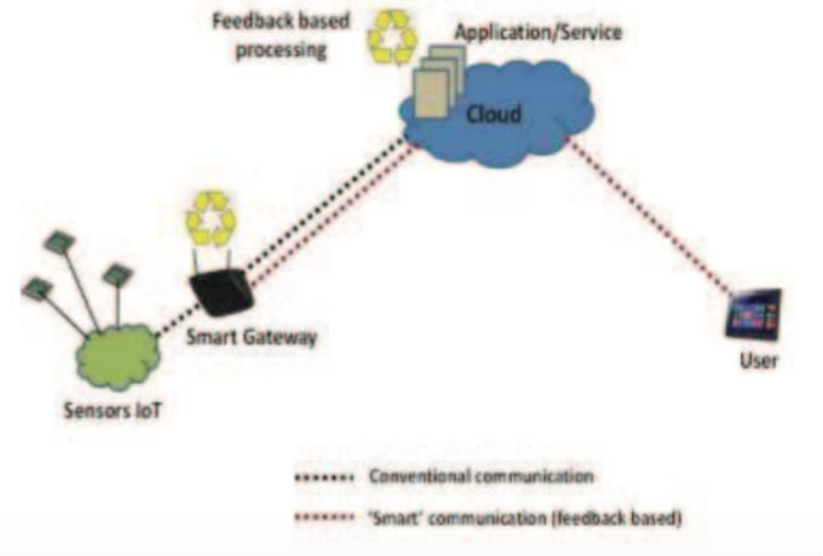
The network of internet connected devices and their integration with the cloud is known as CoT (cloud of things). This integration is a good fit due their complementary properties (*see table below*).

TABLE I: Complementarity and Integration of Cloud and IoT.

IoT	Cloud
pervasive (things placed everywhere)	ubiquitous (resources usable from everywhere)
real world things	virtual resources
limited computational capabilities	virtually unlimited computational capabilities
limited storage or no storage capabilities	virtually unlimited storage capabilities
Internet as a point of convergence	Internet for service delivery
big data source	means to manage big data

Data often consists of structured and unstructured data and thus data storage components must have the ability to deal with heterogeneous data sources. Jian at al suggest a platform with the ability of storing and managing structured and unstructured IoT data through the use of Hadoop distributed file system as well as NoSQL and relational databases. [40]

Due to the large amounts of data produced, data must be 'trimmed' so as to not put unnecessary pressure on the network. Aazman et al suggest implementing a feedback based gateway device which pre-processes and trims the data before sending it to the cloud. (see figure below). [41]



In healthcare, cloud IoT provides the ability to: collect patients' vital data via a network of connected medical devices, deliver the data to a medical centre's cloud for storage and processing and guarantee access to Electronic Healthcare Records (EHR). With Big Data Analytics platforms like Apache Hadoop, structured and unstructured data can be processed and analysed.

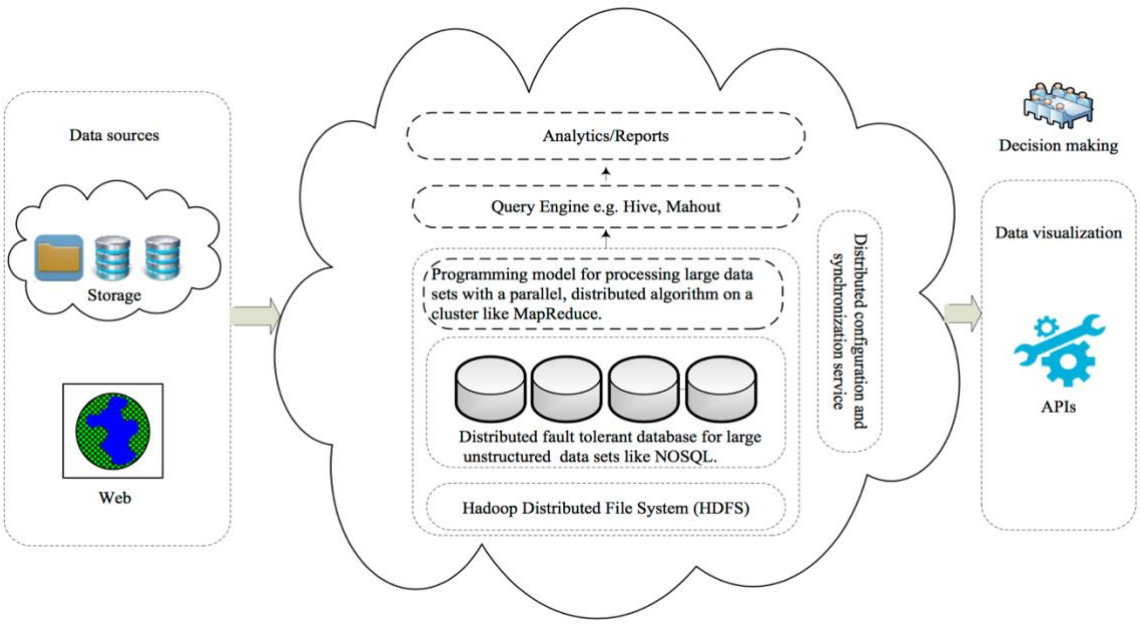


Fig. 3. Cloud computing usage in big data.

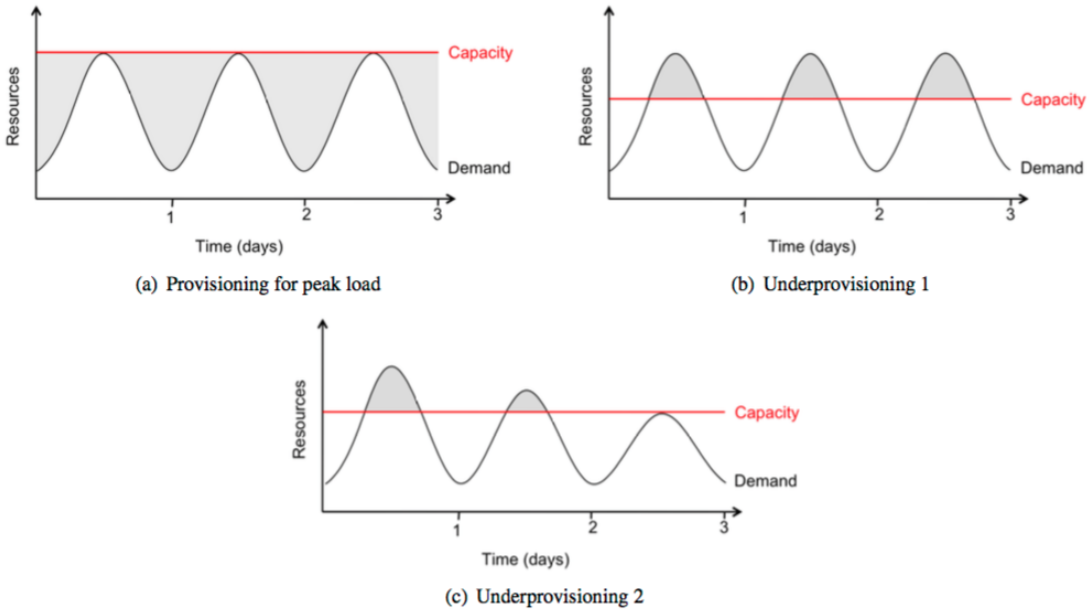
Diagram above illustrating the role the cloud plays with Big Data [42] and the diagram below compares various big data cloud platforms.

	Google	Microsoft	Amazon	Cloudera
Big data storage	Google cloud services	Azure	S3	
MapReduce	AppEngine	Hadoop on Azure	Elastic MapReduce (Hadoop)	MapReduce YARN
Big data analytics	BigQuery	Hadoop on Azure	Elastic MapReduce (Hadoop)	Elastic MapReduce (Hadoop)
Relational database	Cloud SQL	SQL Azure	MySQL or Oracle	MySQL, Oracle, PostgreSQL
NoSQL database	AppEngine Datastore	Table storage	DynamoDB	Apache Accumulo
Streaming processing	Search API	Streaminsight	Nothing prepackaged	Apache Spark
Machine learning	Prediction API	Hadoop+Mahout	Hadoop+Mahout	Hadoop+Oryx
Data import	Network	Network	Network	Network
Data sources	A few sample datasets	Windows Azure marketplace	Public Datasets	Public Datasets
Availability	Some services in private beta	Some services in private beta	Public production	Industries

Machine Learning

Previous autonomic management attempts have failed to show robustness to changes in the application and its environment over time including changes in usage patterns.

This can be mitigated by implementing analysis techniques derived from statistics and machine learning. Peter Bodik et al suggest applying statistical models of the application's performance, simulation-based methods for finding an optimal control policy and change-point methods to find abrupt changes in performance. [43] This will help to eliminate the wasted resources as shown in the diagram below and the ultimate goal is for resources to follow demand exactly. [44]



Habib and Khan suggest a reinforcement learning mechanism to automate decision making process in the case of the maintenance of the VMs. This is based on a reinforcement learning technique called Q-learning. [45] In terms of industry offerings, IBM have an AI-powered cloud-based whilst Microsoft's Azure provides over 20 cognitive cloud services.

Serverless Computing

Serverless computing such as AWS Lambda adds another layer of abstraction atop cloud infrastructure so developers no longer need to worry about servers. Users load the code they want to run and Lambda takes care of resource provisioning, monitoring and management.

Cloud Containers

Containers, such as those provided by Docker, provide an easy-to-deploy and secure method of implementing infrastructure requirements and are designed to provide a virtual instance of a single application. Containers create an isolation boundary at the application level rather than at the server level meaning that if anything goes wrong in that container it only affects that individual container and not the whole server. Containers can operate with a minimum amount of resources to perform the task they were designed for which results in two or three times as many containers being able to be deployed on a server than VMs. Cloud containers are also portable - once the container has been created, it can be deployed to different servers very easily [46]

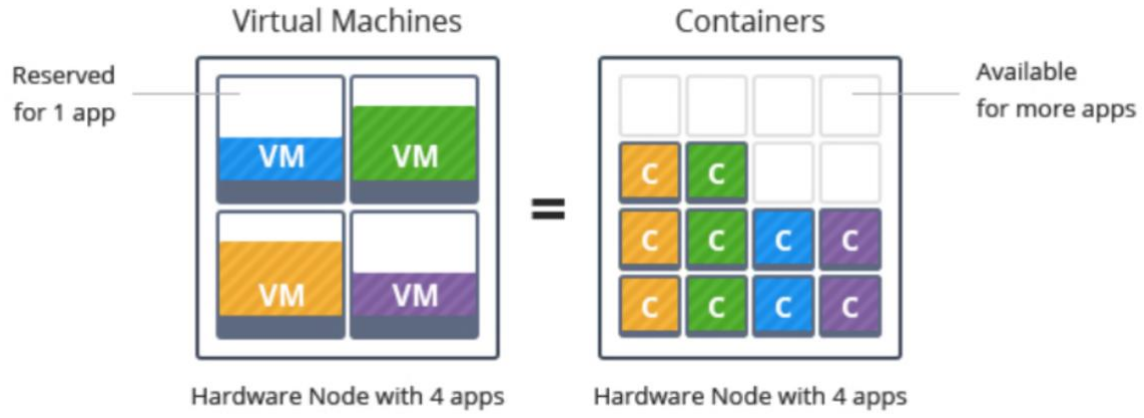


Diagram above illustrates the difference between VMs and containers. [47]

Edge Computing

Edge computing is a method of optimising cloud systems by performing data processing at the edge of the network, near the source of the data. This reduces the bandwidth needed between sensors and the datacentre by performing analytics and knowledge generation near the source of the data. This approach streamlines the flow of traffic from IoT devices and provides real-time local data analysis and analytics, particularly relevant to your business needs. [48]

Blockchain

Blockchain technology can be used to solve the problem of accountability by providing a verifiable data supply chain. Blockchain allows users of the platform to verify that the platform is in the correct state in real-time. Such a system would give traceability for the cloud; entities who are either using or administrating the cloud can be held responsible for their actions, regulators get to audit processes and everyone involved can verify what happened when. This has been adopted by Oracle and Microsoft in their respective cloud solutions. [49]

In conclusion

This brief aimed to advise your company on how to manage a deployment to the cloud in terms of infrastructure management and security. I recommend that your business utilises the hybrid cloud deployment method, maintaining sensitive information within the premises, using a public cloud to address scalability issues by leveraging external resources. I suggest implementing an autonomic management system that automatically monitors QoS parameters as well as adopting open standards such as SAML to aid cloud interoperability. I have recommended multiple security mechanism and I recommend having a security-SLA so that the CSP is contractually required to provide a given level of security. In the coming few years, the use of CoT, machine learning and containers could dramatically affect the performance of your cloud system and I recommend utilising them fully.

Bibliography

[1] C. V. S. T. S. Rajkumar Buyya, Mastering Cloud Computing- Foundations and Application Programing, Morgan Kaufman.

[2] J. Barton, "Impact of Cloud Computing on Healthcare," *Cloud standards customer council* .

[3] Accenture, "A new era for the healthcare industry Cloud computing changes the game".

[4] R. L. K. a. R. D. Vines, Cloud Security: A comprehensive Guide to Secure Cloud Computing.

[5] C. W. a. E. C. Tharam Dillon, "Cloud Computing: Issues and Challenges," *Advanced Information Networking and Applications.*

[6] V. K. S. Subashini, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications.*

[7] T. Hobika, "Migrating To Infrastructure As A Service (IaaS): A Practical Guide," [Online]. Available: https://www.cloudstrategymag.com/articles/84951-migrating-to-infrastructure-as-a-service-iaas-a-practical-guide.

[8] S. Poslad, "Autonomous systems and Artificial Life, In: Ubiquitous Computing Smart Devices, Smart Environments and Smart Interaction".

[9] R. C. a. X. L. Rajkumar Buyya, "Autonomic Cloud Computing: Open Challeneges and Architectural Elements," *IEEE.*

[10] I. C. a. R. B. F. Sukhpal Singh, "STAR: SLA-aware Autonomic Management of Cloud Resources," *Transactions on Cloud Computing IEEE.*

[11] D. I. M. L. G. I. Bogdan Solomon, "Designing Autonomic Management Systems for Cloud Computing," *IEEE.*

[12] E. S. L. G. K. T. D. D. S. Qi Liu, " TOWARDS AN AGENT-BASED SYMBIOTIC ARCHITECTURE FOR AUTONOMIC MANAGEMENT OF VIRTUALIZED DATA CENTERS," *Winter Simulation Conference.*

[13] V. A. G.´. N. R. e. a. Alessandro Ferreira Leite, "Autonomic Provisioning, Configuration, and Management of Inter-Cloud Environments based on a Software Product Line Engineering Method," *2016 International Conference on Cloud and Autonomic Computing.*

[14] F.´.´. D. T. Hien Nguyen Van, "Autonomic virtual resource management for service hosting platforms∗," *Orange Labs.*

[15] P. H. a. D. Woods, "Cloud Computing: The limits of Public Clouds for Business Applications".

[16] T. L. S. M. H. S. Fang Hao, "Secure Cloud Computing with a Virtualized Network Infrastructure," *Bell Labs.*

[17] A. H. P. N. A. f. L.-s. C. M. D. Centers, "Yantao Sun, Min Chen, Qiang Liu, Jing Cheng".

[18] I. F. &. A. O. Kuyoro S. O., "Cloud Computing Security Issues and Challenges," *ResearchGate.*

[19] C. S. Alliance, "SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0".

[20] D. M. T. Force, "Open virtualization format specification".

[21] R. M. I. L. a. I. F. B. Sotomayor, “Virtual Infrastructure Management in Private and Hybrid Clouds,” *IEEE Internet Computing.*

[22] J. G. a. I. M. Mohamed Al Morsy, “An Analysis of the Cloud Computing Security Problem,” *Computer Science & Software Engineering, Faculty of Information & Communication Technologies.*

[23] S. a. F.-g. D. A. C. i. C. C. Achieving Secure, “Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou,” *IEEE.*

[24] S. Overby, “The Patriot Act and Your Data: Should You Ask Cloud Providers About Protection?,” [Online].

[25] Q. Z. ·. L. C. ·. R. Boutaba, “Cloud computing: state-of-the-art and research challenges,” *The Brazilian Computer Society.*

[26] S. Yu, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,” *IEEE.*

[27] A. f. R. G. A. D. J. R. K. A. K. G. L. D. P. A. R. i. S. A. m. z. miChAEL ARmBRuSt, “A View of Cloud Computing: Clearing the clouds away from the true potential and obstacles posed by this computing capability.”.

[28] D. L. Dimitrios Zissis, “Addressing cloud computing security issues,” *Future Generation Computer Systems.*

[29] P. A. Vigya Dubey, “http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7570892&tag=1,” *Collosal Data Analysis and Networking.*

[30] S. Y. Y. Z. K. R. a. W. L. Ming Li, “In the healthcare industry, Li et al suggest a mechanism for data access control to Patient Health Records (PHR) in untrusted servers. To achieve fine-grained and scalable data access controls, it utilises attribute-based encryption (ABE) techniques. This framework dividers users in the PHR system into multiple security domains, greatly reducing the key management complexity and allows dynamic modification of access policies or file attributes.,” *IEEE Transactions on Parallel and Distributed Systems.*

[31] A. A. P. G. P. T. L. L. J. X. Hussain AlJahdali, “Multi-tenancy in cloud computing,” *IEEE.*

[32] J. J. Hassan Takabi, “Security and Privacy Challenges in Cloud Computing Environments,” *Cloud Computing IEEE.*

[33] M. D. O. Yasir Ahmed Hamza1, “Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing,” *nternational Journal of Computational Engineering Research.*

[34] S. S. a. R. Bhadauria, “Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques”.

[35] T. L. S. M. H. S. Fang Hao, “Secure Cloud Computing with a Virtualized Network Infrastructure,” *Bell Labs.*

[36] M. A. a. M. A. Hossain, “CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD,” *International Journal of Network Security & Its Applications* .

[37] J. B. J. G.-J. A. Hassan Takabi, “Security and Privacy Challenges in Cloud Computing Environments”.

[38] A. D. B. M. E. , c. J. M. a. M. R. Valentina Casola, “Automatically Enforcing Security SLAs in the Cloud,” *IEEE TRANSACTIONS ON SERVICES COMPUTING.*

[39] R. T. J. L. a. N. S. Ahmed Taha, “A Framework for Ranking Cloud Security Services,” *IEEE 14th International Conference on Services Computing,* 2017.

[40] A. I.-O. D. S. F. i. C. C. Platform, " Lihong Jiang ; Li Da Xu ; Hongming Cai ; Zuhai Jiang ; Fenglin Bu ; Boyi Xu," *IEEE Transactions on Industrial Informatics.*

[41] I. K. A. A. Mohammad Aazam, "Cloud of Things: Integrating IoT and Cloud Computing and the issues involved".

[42] I. Y. N. B. A. S. M. A. G. S. U. K. Ibrahim Abaker Targio Hashem, "The rise of "big data" on cloud computing: Review and open research issues," *Information Systems ,* 2015.

[43] R. G. C. S. A. F. M. J. D. P. Peter Bod´ık, "Statistical Machine Learning Makes Automatic Control Practical for Internet Datacenters," *RAD Lab, EECS Department, UC Berkeley.*

[44] M. A. A. F. R. G. A. D. J. R. H. K. A. K. G. L. D. A. P. A. R. I. S. M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," *Electrical Engineering and Computer Sciences University of California at Berkeley .*

[45] M. I. K. Arafat Habib, "Reinforcement Learning based Autonomic Virtual Machine Management in Clouds," *Informatics, Electronics and Vision (ICIEV) .*

[46] R. Shapland, "Cloud containers -- what they are and how they work," [Online]. Available: http://searchcloudsecurity.techtarget.com/feature/Cloud-containers-what-they-are-and-how-they-work.

[47] D. O. Reilly, "Mastering the Art of Container Management," [Online]. Available: https://morpheusdata.com/blog/2017-05-10-mastering-the-art-of-container-management.

[48] H. Yamanaka, E. Kawai, Y. Teranishi and H. Harai, "Proximity-Aware IaaS for Edge Computing Environment," *Computer Communication and Networks .*

[49] C. Hall, "Oracle Brings Blockchain-as-a-Service to Its Cloud," [Online]. Available: http://www.datacenterknowledge.com/oracle/oracle-brings-blockchain-service-its-cloud.

[50] D. J. Abadi, "Data Management in the Cloud: Limitations and Opportunities," *Yale University.*

[51] C. M. Nelson Gonzalez, "A quantitative analysis of current security concerns and solutions for cloud computing," *Journal of Cloud Computing: Advances, Systems and Applications .*

[52] R. B. a. S. Sanyal, "Cloud Computing and Associated Mitigation Techniques," *arxiv.*

[53] D. J. Abadi, "Data Management in the Cloud: Limitations and Opportunities," *Yale.*

[54] W. d. D. V. P. a. A. P. Alessio Botta, "On the Integration of Cloud Computing and Internet of Things," *Future Internet of Things and Cloud.*

[55] M. A. A. F. R. G. A. D. J. R. H. K. A. K. G. L. D. A. P. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," *Electrical Engineering and Computer Sciences University of California at Berkeley.*

[56] G. F. a. J. D. K. Hwang, Distributed and Cloud Computing,, Morgan Kaufmann , 2012.