The International Journal Of Engineering And Science (IJES)
|| Volume || 5 || Issue || 6 || Pages || PP -86-97 || 2016 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Impacts of Cloud Computing in the Society

Obinnaya Omankwu,
[a] *Department of Computer Science, Michael Okpara University of Agriculture,Umudike,Umuahia,Abia State*
Chizoba Ezeme,
[b] *Department of Computer Science & Information technology, Caritas University,Enugu,Nigeria*
Chioma Ugwa
[c] *Project Development Institute, (PRODA),Enugu, Nigeria*

----------**ABSTRACT**----------
This paper describes that Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications. Cloud computing involves deploying groups of remote servers and software networks that allow centralized data storage and online access to computer services or resources. Clouds can be classified based on service models as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). It can also be classified based on types as public, private or hybrid cloud.

Keywords: *Cloud; Platform as Service (Paas); Software as a Service (Saas); Infrastructure as a Service (IaaS);)*

Date of Submission: 17 May 2016 Date of Accepted: 05 June 2016

I. INTRODUCTION

The terms "cloud computing" and "working in the cloud" refer to performing computer tasks using services delivered entirely over the Internet. Cloud computing is a movement away from applications needing to be installed on an individual's computer towards the applications being hosted online. (The "cloud" refers to the Internet and was inspired by technical flow charts and diagrams, which tend to use a cloud symbol to represent the Internet.) In other words, Cloud computing refers to the use of computing resources, those being hardware and/or software) that reside on a remote machine and are delivered to the end user as a service over a network, with the most prevalent example being the internet. It might be more accurate, however, to define cloud computing as computer services delivered via the Internet, as cloud computing encompasses more than web applications and data storage**.**

Examples of Cloud Computing Services

Over the last few years we've seen tremendous growth in cloud computing, as witnessed by the many popular Web apps used today, including: Web-Based Email: Web-based email services like Gmail and Hotmail deliver a cloud computing service.Users can access their email "in the cloud" from any computer with a browser and Internet connection, regardless of what kind of hardware is on that particular computer. The emails are hosted on Google's and Microsoft's servers, rather than being stored locally on the client computer. VoIP e.g., Skype, Google Voice, Social applications, e.g., Facebook, Twitter, LinkedIn, Media services (e.g., Picassa, YouTube, Flickr), Content distribution (e.g., BitTorrent),Financial apps (e.g., Mint), and many more. Even traditional desktop software, such as Microsoft Office, has moved in part to the Web, starting with its Office 2010 Web Apps.

There are three categories of cloud computing service models.

They are:

1. Infrastructure as a Service (IaaS),
2. Platform as a Service (PaaS) and
3. Software as a Service (SaaS).

Infrastructure as a Service (IaaS)
Infrastructure as a Service (IaaS) provides the user with virtual infrastructure, such as servers and data storage space. This is where virtualization fits into the cloud. The cloud service provider owns the equipment and is responsible for all the server hardware/software infrastructure costs.
In the IaaS model, the IaaS providers supply a virtual server instance and storage, as well as application program interfaces (APIs) that let users migrate workloads to a virtual machine (VM). Users have an allocated storage capacity and start, stop, access and configure the VM and storage as desired. IaaS providers offer small, medium, large, extra-large, and memory- or compute-optimized instances, in addition to customized instances, for various workload needs. In other words, IaaS is a virtual server storage such as Amazon Web Services
For a business, switching to a cloud infrastructure can offload the costs of housing, managing, and maintaining mail/file/database servers. Backups and data security become the responsibility of the cloud provider as do server software/hardware upgrades, which can be very costly for businesses (ask any business that has performed a major Windows Server upgrade).

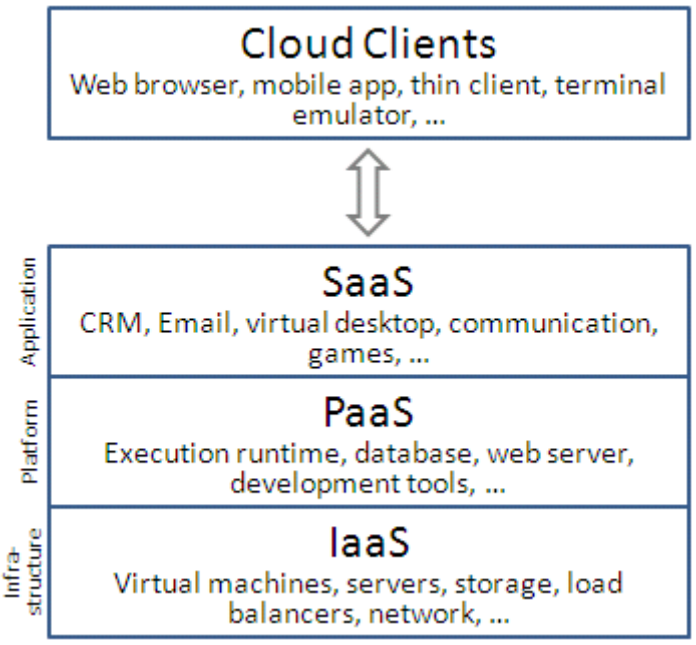
Platform as a Service (PaaS)
Platform as a Service PaaS is a software and product development tools. PaaS provides the user with development environment services where the user can create and run home-grown applications. This allows the software development/support teams to develop and test applications on various hardware/software platforms without having to constantly upgrade, manage, and maintain the platforms in-house. PaaS is used for general software development and many PaaS providers will host the software after it's developed. Common PaaS providers include Salesforce.com's Force.com, Amazon Elastic Beanstalk and Google App Engine. Users access those tools over the Internet using APIs, Web portals or gateway software.

Software as a Service (SaaS)
Software as a Service (SaaS) provides the user with access to already created applications that are operating in the cloud. It is a distribution model that delivers software applications over the Internet; these are often called Web services. Microsoft Office 365 is a SaaS offering for productivity software and email services. Users can access SaaS applications and services from any location using a computer or mobile device that has Internet access.

---

* Corresponding author.
E-mail address: author@institute.xxx .

1.1. Structure



II. LITERATUREVREVIEW

The origin of the term *cloud computing* is unclear. The expression *cloud* is commonly used in science to describe a large agglomeration of objects that visually appear from a distance as a cloud and describes any set of

things whose details are not inspected further in a given context. Another explanation is that the old programs to draw network schematics surrounded the icons for servers with a circle, and a cluster of servers in a network diagram had several overlapping circles, which resembled a cloud.
In analogy to above usage the word *cloud* was used as a metaphor for the Internet and a standardized cloud-like shape was used to denote a network on telephony schematics and later to depict the Internet in computer network diagrams. With this simplification, the implication is that the specifics of how the end points of a network are connected are not relevant for the purposes of understanding the diagram. The cloud symbol was used to represent the Internet as early as 1994, in which servers were then shown connected to, but external to, the cloud. References to cloud computing in its modern sense appeared early as 1996, with the earliest known mention in a Compaq internal document.

History of Cloud Computing
The 1950s
The underlying concept of cloud computing dates to the 1950s, when large-scale mainframe computers were seen as the future of computing, and became available in academia and corporations, accessible via thin clients/terminal computers, often referred to as "dumb terminals", because they were used for communications but had no internal processing capacities. To make more efficient use of costly mainframes, a practice evolved that allowed multiple users to share both the physical access to the computer from multiple terminals as well as the CPU time. This eliminated periods of inactivity on the mainframe and allowed for a greater return on the investment. The practice of sharing CPU time on a mainframe became known in the industry as time-sharing.[
During the mid 70s, time-sharing was popularly known as RJE (Remote Job Entry); this nomenclature was mostly associated with large vendors such as IBM and DEC. IBM developed the VM Operating System to provide time-sharing services.

The 1990s
In the 1990s, telecommunications companies, who previously offered primarily dedicated point-to-point data circuits, began offering virtual private network (VPN) services with comparable quality of service, but at a lower cost. By switching traffic as they saw fit to balance server use, they could use overall network bandwidth more effectively. They began to use the cloud symbol to denote the demarcation point between what the provider was responsible for and what users were responsible for. Cloud computing extends this boundary to cover all servers as well as the network infrastructure.
As computers became more prevalent, scientists and technologists explored ways to make large-scale computing power available to more users through time-sharing. They experimented with algorithms to optimize the infrastructure, platform, and applications to prioritize CPUs and increase efficiency for end users.
Since 2000 cloud computing has come into existence. In early 2008, OpenNebula, enhanced in the RESERVOIR European Commission-funded project, became the first open-source software for deploying private and hybrid clouds, and for the federation of clouds.In the same year, efforts were focused on providing quality of service guarantees (as required by real-time interactive applications) to cloud-based infrastructures, in the framework of the IRMOS European Commission-funded project, resulting in a real-time cloud environment.
By mid-2008, Gartner saw an opportunity for cloud computing "to shape the relationship among consumers of IT services, those who use IT services and those who sell them" and observed that "organizations are switching from company-owned hardware and software assets to per-use service-based models" so that the "projected shift to computing ... will result in dramatic growth in IT products in some areas and significant reductions in other areas."
In July 2010, Rackspace Hosting and NASA jointly launched an open-source cloud-software initiative known as OpenStack. The OpenStack project intended to help organizations offer cloud-computing services running on standard hardware. The early code came from NASA's Nebula platform as well as from Rackspace's Cloud Files platform.
On March 1, 2011, IBM announced the IBM SmartCloud framework to support Smarter Planet. Among the various components of the Smarter Computing foundation, cloud computing is a critical piece.
On June 7, 2012, Oracle announced the Oracle Cloud. While aspects of the Oracle Cloud are still in development, this cloud offering is posed to be the first to provide users with access to an integrated set of IT solutions, including the Applications (SaaS), Platform (PaaS), and Infrastructure (IaaS) layers.

Characteristics of Cloud Computing
Cloud computing exhibits the following key characteristics:
- **Agility** improves with users' ability to re-provision technological infrastructure resources.
- **Application programming interface** (API) accessibility to software that enables machines to interact with cloud software in the same way that a traditional user interface (e.g., a computer desktop) facilitates

interaction between humans and computers. Cloud computing systems typically use Representational State Transfer (REST)-based APIs.

- **Cost** reductions claimed by cloud providers. A public-cloud delivery model converts capital expenditure to operational expenditure. This purportedly lowers barriers to entry, as infrastructure is typically provided by a third party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained, with usage-based options and fewer IT skills are required for implementation (in-house). The e-FISCAL project's state-of-the-art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.
- **Device and location independence** enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.
- **Maintenance** of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.
- **Multitenancy** enables sharing of resources and costs across a large pool of users thus allowing for:
- **Performance** is monitored, and consistent and loosely coupled architectures are constructed using web services as the system interface.
- **Productivity** may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to install application software upgrades to their computer.
- **Reliability** improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
- **Scalability and elasticity** via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis in near real-time[(Note, the VM startup time varies by VM type, location, OS and cloud providers), without users having to engineer for peak loads.
- **Security** can improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford to tackle. However, the complexity of security is greatly increased when data is distributed over a wider area or over a greater number of devices, as well as in multi-tenant systems shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

Cloud computing types

Private cloud

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally.Undertaking a private cloud project requires a significant level and degree of engagement to virtualize the business environment, and requires the organization to reevaluate decisions about existing resources. When done right, it can improve business, but every step in the project raises security issues that must be addressed to prevent serious vulnerabilities. Self-run data centers are generally capital intensive. They have a significant physical footprint, requiring allocations of space, hardware, and environmental controls. These assets have to be refreshed periodically, resulting in additional capital expenditures. They have attracted criticism because users "still have to buy, build, and manage them" and thus do not benefit from less hands-on management, essentially lacking the economic model that makes cloud computing such an intriguing concept.

Public cloud

A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Public cloud services may be free. Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources) that are made available by a service provider for a public audience and when communication is effected over a non-trusted network. Saasu is a large public cloud. Generally, public cloud service providers like Amazon AWS, Microsoft and Google own and operate the infrastructure at their data center and access is generally via the Internet. AWS and Microsoft also offer direct connect services called "AWS Direct Connect" and "Azure ExpressRoute" respectively, such connections require customers to purchase or lease a private connection to a peering point offered by the cloud provider.

Hybrid cloud
Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.
Gartner, Inc. defines a hybrid cloud service as a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers. A hybrid cloud service crosses isolation and provider boundaries so that it can't be simply put in one category of private, public, or community cloud service. It allows one to extend either the capacity or the capability of a cloud service, by aggregation, integration or customization with another cloud service.
Varied use cases for hybrid cloud composition exist. For example, an organization may store sensitive client data in house on a private cloud application, but interconnect that application to a business intelligence application provided on a public cloud as a software service. This example of hybrid cloud extends the capabilities of the enterprise to deliver a specific business service through the addition of externally available public cloud services. Hybrid cloud adoption depends on a number of factors such as data security and compliance requirements, level of control needed over data, and the applications an organization uses.
Another example of hybrid cloud is one where IT organizations use public cloud computing resources to meet temporary capacity needs that cannot be met by the private cloud. This capability enables hybrid clouds to employ cloud bursting for scaling across clouds. Cloud bursting is an application deployment model in which an application runs in a private cloud or data center and "bursts" to a public cloud when the demand for computing capacity increases. A primary advantage of cloud bursting and a hybrid cloud model is that an organization only pays for extra compute resources when they are needed. Cloud bursting enables data centers to create an in-house IT infrastructure that supports average workloads, and use cloud resources from public or private clouds, during spikes in processing demands.

Advantages of Cloud Computing
Cloud computing offers numerous advantages both to end users and businesses of all sizes. The obvious huge advantage is that you no more have to support the infrastructure or have the knowledge necessary to develop and maintain the infrastructure, development environment or application, as were things up until recently. The burden has been lifted and someone else is taking care of all that. Business are now able to focus on their core business by outsourcing all the hassle of IT infrastructure.

1. Cost Efficiency
This is the biggest advantage of cloud computing, achieved by the elimination of the investment in stand-alone software or servers. By leveraging cloud's capabilities, companies can save on licensing fees and at the same time eliminate overhead charges such as the cost of data storage, software updates, management etc.
The cloud is in general available at much cheaper rates than traditional approaches and can significantly lower the overall IT expenses. At the same time, convenient and scalable charging models have emerged (such as one-time-payment and pay-as-you-go), making the cloud even more attractive.
If you want to get more technical and analytical, cloud computing delivers a better cash flow by eliminating the capital expense (CAPEX) associated with developing and maintaining the server infrastructure.

2. Convenience and continuous availability
Public clouds offer services that are available wherever the end user might be located. This approach enables easy access to information and accommodates the needs of users in different time zones and geographic locations. As a side benefit, collaboration booms since it is now easier than ever to access, view and modify shared documents and files.
Moreover, service uptime is in most cases guaranteed, providing in that way continuous availability of resources. The various cloud vendors typically use multiple servers for maximum redundancy. In case of system failure, alternative instances are automatically spawned on other machines.

3. Backup and Recovery
The process of backing up and recovering data is simplified since those now reside on the cloud and not on a physical device. The various cloud providers offer reliable and flexible backup/recovery solutions. In some cases, the cloud itself is used solely as a backup repository of the data located in local computers.

4. Cloud is environmentally friendly
The cloud is in general more efficient than the typical IT infrastructure and It takes fewer resources to compute, thus saving energy. For example, when servers are not used, the infrastructure normally scales down, freeing up resources and consuming less power. At any moment, only the resources that are truly needed are consumed by the system.

5.Resiliency and Redundancy
A cloud deployment is usually built on a robust architecture thus providing resiliency and redundancy to its users. The cloud offers automatic failover between hardware platforms out of the box, while disaster recovery services are also often included.

6. Scalability and Performance
Scalability is a built-in feature for cloud deployments. Cloud instances are deployed automatically only when needed and as a result, you pay only for the applications and data storage you need. Hand in hand, also comes elasticity, since clouds can be scaled to meet your changing IT system demands.
Regarding performance, the systems utilize distributed architectures which offer excellent speed of computations. Again, it is the provider's responsibility to ensure that your services run on cutting edge machinery. Instances can be added instantly for improved performance and customers have access to the total resources of the cloud's core hardware via their dashboards.

7. Quick deployment and ease of integration
A cloud system can be up and running in a very short period, making quick deployment a key benefit. On the same aspect, the introduction of a new user in the system happens instantaneously, eliminating waiting periods.
Furthermore, software integration occurs automatically and organically in cloud installations. A business is allowed to choose the services and applications that best suit their preferences, while there is minimum effort in customizing and integrating those applications.

8. Increased Storage Capacity
The cloud can accommodate and store much more data compared to a personal computer and in a way offers almost unlimited storage capacity. It eliminates worries about running out of storage space and at the same time It spares businesses the need to upgrade their computer hardware, further reducing the overall IT cost.

9. Device Diversity and Location Independence
Cloud computing services can be accessed via a plethora of electronic devices that are able to have access to the internet. These devices include not only the traditional PCs, but also smartphones, tablets etc. With the cloud, the "Bring your own device" (BYOD) policy can be easily adopted, permitting employees to bring personally owned mobile devices to their workplace.
An end-user might decide not only which device to use, but also where to access the service from. There is no limitation of place and medium. We can access our applications and data anywhere in the world, making this method very attractive to people. Cloud computing is in that way especially appealing to international companies as it offers the flexibility for its employees to access company files wherever they are.

10. Smaller Learning Curve
Cloud applications usually entail smaller learning curves since people are quietly used to them. Users find it easier to adopt them and come up to speed much faster. Main examples of this are applications like GMail and Google Docs.

Disadvantages of Cloud Computing
As made clear from the above, cloud computing is a tool that offers enormous benefits to its adopters. However, being a tool, it also comes with its set of problems and inefficiencies. Let's address the most significant ones.

1. Security and privacy in the Cloud
Security is the biggest concern when it comes to cloud computing. By leveraging a remote cloud based infrastructure, a company essentially gives away private data and information, things that might be sensitive and confidential. It is then up to the cloud service provider to manage, protect and retain them, thus the provider's reliability is very critical. A company's existence might be put in jeopardy, so all possible alternatives should be explored before a decision. On the same note, even end users might feel uncomfortable surrendering their data to a third party.
Similarly, privacy in the cloud is another huge issue. Companies and users have to trust their cloud service vendors that they will protect their data from unauthorized users. The various stories of data loss and password leakage in the media does not help to reassure some of the most concerned users.

2. Dependency and vendor lock-in
One of the major disadvantages of cloud computing is the implicit dependency on the provider. This is what the industry calls "vendor lock-in" since it is difficult, and sometimes impossible, to migrate from a provider once you have rolled with him. If a user wishes to switch to some other provider, then it can be really painful and cumbersome to transfer huge data from the old provider to the new one. This is another reason why you should carefully and thoroughly contemplate all options when picking a vendor.

3. Technical Difficulties and Downtime
Certainly the smaller business will enjoy not having to deal with the daily technical issues and will prefer handing those to an established IT company, however you should keep in mind that all systems might face dysfunctions from time to time. Outage and downtime is possible even to the best cloud service providers, as the past has shown.
Additionally, you should remember that the whole setup is dependent on internet access, thus any network or connectivity problems will render the setup useless. As a minor detail, also keep in mind that it might take several minutes for the cloud to detect a server fault and launch a new instance from an image snapshot.

4. Limited control and flexibility
Since the applications and services run on remote, third party virtual environments, companies and users have limited control over the function and execution of the hardware and software. Moreover, since remote software is being used, it usually lacks the features of an application running locally.

5. Increased Vulnerability
Related to the security and privacy mentioned before, note that cloud based solutions are exposed on the public internet and are thus a more vulnerable target for malicious users and hackers. Nothing on the Internet is completely secure and even the biggest players suffer from serious attacks and security breaches. Due to the interdependency of the system, If there is a compromise one one of the machines that data is stored, there might be a leakage of personal information to the world.

III. CLOUD COMPUTING SECURITY

Cloud computing security or, more simply, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Security issues associated with the cloud
There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the on the cloud). The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures.When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially business sensitive and confidential data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the third biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity.In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. As a result there is a chance that one user's private data can by viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.

Cloud Security Controls
Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:

Deterrent controls
These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed.

Preventive controls
Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

Detective controls
Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue. System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.

Corrective controls
Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

Dimensions of cloud security
It is generally recommended that information security controls be selected and implemented according and in proportion to the risks, typically by assessing the threats, vulnerabilities and impacts. While cloud security concerns can be grouped into any number of dimensions (e.g. Gartner named seven[8] while the Cloud Security Alliance identified fourteen areas of concern[9]), three are outlined below.[10]

Security and Privacy
Cloud computing poses privacy concerns because the service provider can access the data that is on the cloud at any time. It could accidentally or deliberately alter or even delete information. Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. That is permitted in their privacy policies which users have to agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end users' choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access.

Identity management
Every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, using federation or SSO technology, or provide an identity management solution of their own.[11]

Physical Security
Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers.

Personnel security
Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive security monitoring and supervision, disciplinary procedures and contractual obligations embedded in employment contracts, service level agreements, codes of conduct, policies etc.

Availability
Cloud providers help ensure that customers can rely on access to their data and applications, at least in part (failures at any point - not just within the cloud service providers' domains - may disrupt the communications chains between users and applications).

Application security
Cloud providers ensure that applications available as a service via the cloud (SaaS) are secure by specifying, designing, implementing, testing and maintaining appropriate application security measures in the production environment. Note that - as with any commercial software - the controls they implement may not necessarily fully mitigate all the risks they have identified, and that they may not necessarily have identified all the risks that are of concern to customers. Consequently, customers may also need to assure themselves that cloud applications are adequately secured for their specific purposes, including their compliance obligations.

Privacy
Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted (even better) and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

Compliance
Numerous laws and regulations pertain to the storage and use of data. In the US these include privacy or data protection laws.
Similar laws may apply in different legal jurisdictions and may differ quite markedly from those enforced in the US. Cloud service users may often need to be aware of the legal and regulatory differences between the jurisdictions. For example data stored by a Cloud Service Provider may be located in, say, Singapore and mirrored in the US. ../Mrs Chizoba Ezeme/Documents/Cloud_computing_security.htm - cite_note-12
Many of these regulations mandate particular controls (such as strong access controls and audit trails) and require regular reporting. Cloud customers must ensure that their cloud providers adequately fulfil such requirements as appropriate, enabling them to comply with their obligations since, to a large extent, they remain accountable.

Business Continuity and Data recovery
Cloud providers have business continuity and data recovery plans in place to ensure that service can be maintained in case of a disaster or an emergency and that any data loss will be recovered.[These plans may be shared with and reviewed by their customers, ideally dovetailing with the customers' own continuity arrangements. Joint continuity exercises may be appropriate, simulating a major Internet or electricity supply failure for instance.

Logs and audit trails
In addition to producing logs and audit trails, cloud providers work with their customers to ensure that these logs and audit trails are properly secured, maintained for as long as the customer requires, and are accessible for the purposes of forensic investigation.

Unique compliance requirements
In addition to the requirements to which customers are subject, the data centers used by cloud providers may also be subject to compliance requirements. Using a cloud service provider (CSP) can lead to additional security concerns around data jurisdiction since customer or tenant data may not remain on the same system, or in the same data center or even within the same provider's cloud.

Legal and Contractual Issues
Aside from the security and compliance issues enumerated above, cloud providers and their customers will negotiate terms around liability (stipulating how incidents involving data loss or compromise will be resolved, for example), intellectual property, and end-of-service (when data and applications are ultimately returned to the customer). In addition, there are considerations for acquiring data from the cloud that may be involved in litigation. Conclusion

REFERENCES

[1]. Adams, Richard (2013). "'The emergence of cloud storage
[2]. "Gartner: Seven cloud-computing security risks". InfoWorld. 2008-07-02. Retrieved 2010-01-25.
[3]. Hassan, Qusay (2011). "Demystifying Cloud Computing". *The Journal of Defense Software Engineering* (CrossTalk) **2011** (Jan/Feb): 16–21. Retrieved 11 December2014.
[4]. Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80. Print.
[5]. Srinavasin, Madhan (2012). "'State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment". ACM ICACCI'.
[6]. "Swamp Computing a.k.a. Cloud Computing". Web Security Journal. 2009-12-28. Retrieved 2010-01-25.
[7]. "Top Threats to Cloud Computing v1.0". Cloud Security Alliance. Retrieved 2014-10-20.

[8]. Winkler, Vic. "Cloud Computing: Virtual Cloud Security Concerns". Technet Magazine, Microsoft. Retrieved 12 February 2012.
[9]. Winkler, Vic (2011). *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Waltham, MA USA: Elsevier. p. 59. ISBN 978-1-59749-592-9.
[10]. Winkler, Vic (2011). *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Waltham, MA USA: Elsevier. pp. 65, 68, 72, 81, 218–219, 231, 240. ISBN 978-1-59749-592-9.
[11]. "Security Guidance for Critical Areas of Focus in Cloud Computing". Cloud Security Alliance. 2011. Retrieved 2011-05-04.

Files should be in MS Word format only and should be formatted for direct printing. **Figures and tables should be embedded and not supplied separately**.
Please make sure that you use as much as possible normal fonts in your documents. Special fonts, such as fonts used in the Far East (Japanese, Chinese, Korean, etc.) may cause problems during processing. To avoid unnecessary errors you are strongly advised to use the 'spellchecker' function of MS Word.
Follow this order when typing manuscripts: Title, Authors, Affiliations, Abstract, Keywords, introduction, materials and methods, results, conclusion, Acknowledgements, References, Appendix. Collate acknowledgements in a separate section at the end of the article and do not include them on the title page.
Bulleted lists may be included and should look like this:

- First point
- Second point
- And so on

Please do not alter the formatting and style layouts which have been set up in this template document. As indicated in the template, papers should be prepared in single column format suitable for direct printing onto A4 paper (8.3in x 11.7in/210mm x 297mm). Leave a line clear between paragraphs.

1.2. Tables(tables should start and end within the same page unless the table is longer than one page)

All tables should be numbered with Arabic numerals. Headings should be placed above tables, center justified. 10pt font size. Leave one line space between the heading and the table. Tables must be **embedded into the text and not supplied separately**. Below is an example which authors may find useful.

Table 1: An example of a table

An example of a column heading	Column A (*t*)	Column B (*T*)
And an entry	1	2
And another entry	3	4
And another entry	5	6

1.3. Construction of references

References should be listed at the end of the paper, and numbered in the order of their appearance in the text. Authors should ensure that every reference in the text appears in the list of references and vice versa. Indicate references by numbers in the text. In the text the number of the reference should be given in square brackets [3]. The actual authors can be referred to, but the reference number(s) must always be given.
Some examples of how your references should be listed are given at the end of this template in the 'References' section which will allow you to assemble your reference list according to the correct format and font size. There is a shortened form for last page number. e.g., 51–9, and that for more than 6 authors the first 6 should be listed followed by "et al."

1.4. Section headings

Section headings should be left justified, with the first letter capitalized and numbered consecutively, starting with the Introduction. Sub-section headings should be in capital and lower-case italic letters, numbered 1.1, 1.2, etc, and left justified, with second and subsequent lines indented.

1.5. General guidelines for the preparation of your text

Weights and measures should be expressed in either SI (MKS) or CGS as primary units. (SI units are encouraged.).

2. Figures and equations (do not use write figure as Fig.)

All figures should be numbered with Arabic numerals (1,2,...n). All photographs, schemas, graphs and diagrams are to be referred to as figures. Figures must be embedded into the text and not supplied separately. Lettering and symbols should be clearly defined either in the caption or in a legend provided as part of the figure.
The figure number and caption should be typed below the illustration in 10pt and center justified.

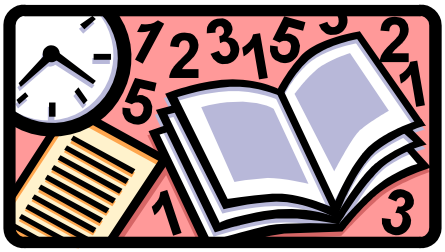


Figure 1: first picture

Equations and formulae should be typed and numbered consecutively with Arabic numerals in parentheses on the right hand side of the page (if referred to explicitly in the text).

$$Rt = K\,EP = 93.02\ (\pm 9.62) - 13.45 \qquad (1)$$

We suggest that you use a text box to insert a graphic, because this method is somewhat more stable than directly inserting a picture.

To have non-visible rules on your frame, use the MSWord "Format" pull-down menu, select Text Box > Colors and Lines to choose No Fill and No Line.

Acknowledgements

These and the Reference headings are in bold. Text below continues as normal.

References (use 10 point font, times new roman**)**

IEEE Citation Style Guide to prepare your references

Anycitationstyleissetuptogivethereaderimmediateinformationaboutsourcescitedinthetext.InIEEEcitations,therefe rencesshouldbenumberedandappearintheordertheyappearinthetext.Whenreferringtoareferenceinthetextofthedocu ment,putthenumberofthereferenceinsquarebrackets.Eg:[1]

The references are numbered at the end of the paper, then the reference number from the reference list at the end of the author paper (the references at the end of the paper should be numbered) should be used instead of author name and year. Example on the correct citation "The authors in [2,3] noted that crushed aggregates having angular to sub-angular shaped". Example on the wrong citation " (nassar,2013) and (Fokianos et al., 2007) noted that crushed aggregates having angular to sub-angular shaped" (nassar,2013).

TheIEEEcitationstylehas3mainfeatures:

- Theauthornameisfirstname(orinitial)andlast.ThisdiffersfromMLAstylewhereauthor'slastnameisfirst.
- Thetitleofanarticle(orchapter,conferencepaper,patentetc.)isinquotationmarks.
- Thetitleofthejournalorbookisinitalics.

Theseconventionsallowthereadertodistinguishbetweentypesofreferenceataglance.Thecorrectplacementofperiods, commasandcolonsandofdateandpagenumbers dependsonthetypeofreferencecited.Checktheexamplesbelow.Followthedetailsexactly.Eg.:putperiodsafterauthora ndbooktitle,citepagenumbersaspp.,abbreviateallmonthstothefirstthreeletters(eg.Jun.)

Checkthedistinctionsbetweenprintandelectronicsources(especiallyforjournals)carefully.

PrintReferences

Book:

Author(s).*Booktitle*.Location:Publishingcompany,year,pp Example: W.K.Chen .*Linear Networks and Systems*. Belmont,CA: Wadsworth,1993,pp.123-35.

Book Chapters

Author(s)."Chaptertitle"in*Booktitle*,edition,volume.Editorsname,Ed.Publishinglocation:Publishingcompany,year ,pp. Example: J.E. Bourne ."Synthe ticstructu reofindustrial plastics,"in*Plastics*,2nd ed.,vol.3.J. Peters,Ed.New York: Mc Graw-Hill,1964,pp.15-67.

ArticleinaJournal
Author(s).“Articletitle*”.Journaltitle*,vol.,pp,date.Example:G.Pevere.“InfraredNation.”*TheInternationalJournalofInfraredDesign*,vol.33,pp. 56-99,Jan.1979.
ArticlesfromConferenceProceedings(published) Author(s).“Articletitle.”*Conferenceproceedings*,year,pp.
Example: D.B.PayneandH.G.Gunhold.“Digitalsundialsandbroadbandtechnology,”in*Proc.IOOC-ECOC*, 1986, pp. 557-998.

PapersPresentedatConferences(unpublished) Author(s).“Paper’stitle,”Conferencename,Location,year.
Example:

B.BrandliandM.Dick.“Engineeringnamesandconcepts,”presentedatthe2nd Int.Conf.EngineeringEducation,Frankfurt,Germany,1999.

Standards/Patents
Author(s)/Inventor(s).“Name/Title.”Countrywherepatentisregistered.Patentnumber,date.
Example:
E.E.Rebecca.“Alternatingcurrentfedpowersupply.”U.S.Patent7897777,Nov.3, 1987.

ElectronicReferences
Books
Author.(year,Monthday).*Booktitle*.(edition).[Typeofmedium].Vol.(issue). Available:site/path/file[dateaccessed].
Example:

S.Calmer.(1999,June1).*EngineeringandArt*.(2nd edition).[On-line].27(3).Available:
www.enggart.com/examples/students.html[May21,2003].

Journal
Author.(year,month).“Articletitle.”*Journaltitle*.[Typeofmedium].Vol.(issue),pages.Available:site/path/file[dateaccessed].Example:
A.Paul.(1987,Oct.).“Electricalpropertiesofflyingmachines.”*FlyingMachines*.[On- line].38(1),pp.778-998.Available:www.flyingmachjourn/properties/fly.edu[Dec.1,
2003].

WorldWideWeb
Author(s)*.“Title.”Internet:completeURL,dateupdated*[dateaccessed].Example:M.Duncan.“EngineeringConceptsonIce.Internet:www.iceengg.edu/staff.html,Oct.25, 2000 [Nov. 29, 2003].

OddSources
Newspaper
Author(s)*.“Articletitle.”*Newspaper*(month,year),section,pages.Examples:B.Bart.“GoingFaster.”*GlobeandMail*(Oct.14,2002),sec.Ap.1.“TelehealthinAlberta.”*TorontoStar*(Nov.12,2003),sec.Gpp.1-3.

DissertationsandTheses
Author.“Title.”Degreelevel,school,location,year.Example:S.Mack.“DesperateOptimism.”M.A.thesis,UniversityofCalgary,Canada,2000.

Lecture
Lecturer(s).Occasion,Topic:“Lecturetitle.”Location,date.Example:S.Maw.Engg251.ClassLecture,Topic:“Speedskating.”ICT224,Facultyof Engineering,UniversityofCalgary,Calgary,Alberta,Oct.31,2003.

E-mail
Author.Subjectlineofposting.PersonalE-mail(date).Example:J.Aston.“RE:newlocation,okay?”Personale-mail(Jul.3,2003).

Internet-Newsgroup
AuthororTopic*,“Title,”Completenetworkaddress,datewhenitwasupdated[dateaccessed].Example:G.G.Gavin.“Climbingandlimbtorsion#3387,”USENET:sci.climb.torsion,Apr.19, 2000[Oct.4,2002].
*ifyoucan’tfindthisinformation,excludeit.

ExactpagenumberReferences
To referrea ders to specific page numbers in atext, uset henu mbe rof the reference follow edbyaco lon(:)and the pagenumbers.Example: Johnsonsuggeststhatcitingwillleadtoadecreaseinbeingcitedforplagiarism[1:28-29].
The [1]refers to then umbere dreference And the 28-29 refers to the pages beingcited.