I.J. Computer Network and Information Security, 2014, 3, 20-29
Published Online February 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.03.03

Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review

Sumit Goyal
Member, IDA, New Delhi, India
Email: thesumitgoyal@gmail.com

Abstract **—** These days cloud computing is booming like no other technology. Every organization whether it's small, mid-sized or big, wants to adapt this cutting edge technology for its business. As cloud technology becomes immensely popular among these businesses, the question arises: Which cloud model to consider for your business? There are four types of cloud models available in the market: Public, Private, Hybrid and Community. This review paper answers the question, which model would be most beneficial for your business. All the four models are defined, discussed and compared with the benefits and pitfalls, thus giving you a clear idea, which model to adopt for your organization.

Index Terms **—** Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud, Cloud Computing, Cloud Security.

I. INTRODUCTION

Today, we can easily notice how the nature of the Internet is changing from a place used to read web pages to an environment that allows the users to run software applications [1]. One vision of 21st century computing is that users will access Internet services over lightweight portable devices rather than through some descendant of the traditional desktop PC. Because users won't have (or be interested in) powerful machines, who will supply the computing power? The answer to this question lies with cloud computing [2, 3]. Cloud computing is a distributed computing paradigm that focuses on providing a wide range of users with distributed access to scalable, virtualized hardware and/or software infrastructure over the internet [4]. Cloud computing has revolutionized the information technology industry by enabling elastic on-demand provisioning of computing resources [5]. Cloud Computing is hinting at a future in which we won't compute on local computers, but on centralized facilities operated by third-party compute and storage utilities [6]. Cloud computing paradigm has emerged as an energy-efficient, fault-tolerant and on-demand approach, which enables ubiquitous network accesses to a shared pool of flexibly reconfigurable computing resources. Networks, servers, storage, applications and services can be rapidly deployed with minimal management input or service provider interaction [7]. Cloud Computing, the long-held dream of computing as an utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service. The datacenter hardware and software is what we will call a cloud. When a cloud is made available in a pay-as-you-go manner to the general public, we call it a public cloud; the service being sold is utility computing. We use the term private cloud to refer to internal datacenters of a business or other organization, not made available to the general public [8]. Community cloud shares infrastructure between several organizations [9]. Hybrid cloud provides the flexibility of in-house applications with the fault tolerance and scalability of cloud based services [10]. Several machines located around the world, which are connected to a single network can be used for providing cloud computing.

The paper is organized in IX sections. Section I gives the introduction. Section II talks about the significance of this study. Section III provides the overview of cloud computing, followed by section IV, which discusses the three service models of cloud computing in detail. Section V, VI, VII and VIII define, discuss and review the pros & cons of public, private, hybrid and community clouds. The last section is conclusion, which summarizes the key outcomes of this review.

II. SIGNIFICANE OF STUDY

More and more enterprises are adopting the cloud model for their businesses, whether they are small, mid-sized or large organizations, as cloud computing provides low cost business solutions to their organizations. It is a well known fact that every business needs cloud, as the technology has become very popular and accepted world over. Cloud computing has promised tremendous advantages to organizations in terms of cost effectiveness, operational excellence and innovation. The main factor for which enterprises are shifting to cloud is the low cost. Cloud helps to turn substantial investments into operational expenses, reduce man management costs, operational costs and maintenance costs. Start-ups and small & mid businesses (SMBs) take particular interest in public cloud as they have limited investments and resources. Instead, big organizations prefer private cloud. This review paper covers the concerns of enterprises in adopting public, private, hybrid, and community clouds for their respective organizations, and lists the differences among them, thus providing a complete idea which model would be better for their enterprises.

III. OVERVIEW OF CLOUD COMPUTING

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.,* networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models [9]. Cloud computing has three basic abstraction layers, *i.e*, system layer (which is a virtual machine abstraction of a server), the platform layer (a virtualized operating system of a server) and application layer (that includes web applications) [11]. Computing is being transformed to a model consisting of services that are commoditized and delivered in a manner similar to traditional utilities such as water, electricity, gas, and telephony [12]. The cloud computing service model involves the provision, by a service provider, of large pools of high performance computing resources and high-capacity storage devices that are shared among end users as required [13-15]. Cloud computing potentially offers an overall financial benefit, in that end users share a large, centrally managed pool of storage and computing resources, rather than owning and managing their own systems [16]. Cloud service providers invest in the necessary infrastructure and management systems, and in return receive a time-based or usage-based fee from end users [17]. Cloud computing is emerging today as a commercial infrastructure that eliminates the need for maintaining expensive computing hardware. Through the use of virtualization, clouds promise to address with the same shared set of physical resources a large user base with different needs. Thus, clouds promise for scientists to be an alternative to clusters, grids, and supercomputers [18]. Cloud computing systems fundamentally provide access to large pools of data and computational resources through a variety of interfaces [19-24]. However, despite the fact that cloud computing offers huge opportunities to the IT industry, the development of cloud computing technology is currently at its infancy, with many issues still to be addressed [25-28]. Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance [29]. With the technology, users on various types of devices—including PCs, laptops, smart phones, and PDAs—access programs, storage, processing, and even application-development platforms over the Internet, via services offered by cloud-computing providers [30]. The data you can find in a cloud ranges from public source, which has minimal security concerns, to private data containing highly sensitive information (such as social security numbers, medical records, or shipping manifests for hazardous material) [31-44]. Authentication of both users and services is a significant issue for the trust and security of the cloud computing [45-46]. As promising as it is, cloud also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against un-trusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users [47-60]. Cloud data storage is a technology that uses the internet and central remote servers to maintain data and share the applications. It allows consumer to use applications without installation and access their personal files at any computer with internet access. In general data property analysis system, source and destination file content is compared in the form of bytes. In the cloud environment, data verification is needed for every computation in the storage correctness. So every time the data is retrieved from local system and compared with the destination file from the cloud zone [61-63]. In cloud environment, a client device or other processing device comprises a file processing module, with the file processing module being operative to request proof from a file system that a file having a first format is stored by the file system in a second format different than the first format, to receive the proof from the file system, and to verify that the file is stored in the second format using the proof provided by the file system responsive to the request. The proof is based at least in part on application of a function to the file in the second format, and the function imposes a minimum resource requirement on generation of the proof. The file system may comprise one or more servers associated with a cloud storage provider. Advantageously, one or more illustrative embodiments allow a client device to verify that its files are stored by a cloud storage provider in encrypted form or with other appropriate protections [64].

IV. SERVICE MODELS OF CLOUD COMPUTING

A. *Infrastructure-as-a-service (IaaS)*

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (*e.g.,* host firewalls) [9]. Infrastructure services provided by cloud vendors, allow any user to provision a large number of compute instances fairly easily [65]. IaaS is the pillar on which a cloud computing architecture is built. With the advancement of technologies in communications, computing, and storage devices, IaaS has emerged as a highly efficient platform to construct Software-as- a-Service and Platform-as- a-Service layer on top of it. IaaS solutions vary from an organization to another. One single solution does not fit all [66]. IaaS serves as the foundation layer for the other delivery models [67-70]. IaaS [71-72] itself is comprised of the following components:

- Servers (both physical and virtual).
- Storage systems by means of network attached storage (NAS) and storage area network (SAN).
- Network segmentation using different network blocks and virtual local area networks.
- Communication network (including routers, switches, firewalls, load balancer, etc.).
- High speed internet connectivity (often on OC 192 backbones).
- Platform virtualization environment.
- Service-level agreements.
- Utility computing billing.
- Security by means of hardware or virtual machine (VM) based firewall and intrusion detection & prevention system.
- Hardware load balancer.
- Domain name service (DNS), Dynamic host configuration protocol (DHCP) and other management and support services.
- Power, cooling and disaster recovery system.

Amazon EC2 is an example of IaaS, where virtual servers can be set up and configured over a web based interface within minutes [73-74]. The consumer can choose operating system, database and application development environment, which gives the consumer greater control over the hardware in comparison to Platform-as- a-Service. The consumer has the possibility to configure the servers based on their needs, which generally includes more maintenance in comparison to Platform-as- a-Service but also more options [75].

B. *Platform-as- a-Service (PaaS)*

PaaS refers to applications created by a development language that is hosted by the cloud service provider in a cloud infrastructure [76]. In comparison to SaaS where the application already exists, and is usually owned by the cloud provider, PaaS offers the possibility to create and modify applications. It is an outgrowth of the SaaS application delivery model [71]. In the PaaS model, the consumer is allowed to write applications that run on the service provider's specific environment. PaaS environment provide you with an infrastructure as well as complete operational and development environments for the deployment of your applications. You can program using the vendor's specific application development platform. A well-known example is the Google Apps Engine [72, 77-78]. To aid the developer, different tools are provided like programming languages and Application Programming Interfaces (API). In comparison to IaaS, the user does not control the virtualization instance or network configuration of the cloud server [57].

PaaS allows for the secure storage and processing of users' confidential data by leveraging the tamper-proof capabilities of cryptographic co-processors. Using tamper-proof facilities provides a secure execution domain in the computing cloud that is physically and logically protected from un-authorized access. PaaS central design goal is to maximize users' control in managing the various aspects related to the privacy of sensitive data. This is achieved by implementing user-configurable software protection and data privacy mechanisms. Moreover, PaaS provides a privacy feedback process, which informs users of the different privacy operations applied on their data and makes them aware of any potential risks that may jeopardize the confidentiality of their sensitive information [43].

C. *Software-as-a-Service (SaaS)*

SaaS is a term that refers to software in a cloud [72]. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (*e.g.*, web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings [57].

The SaaS [79, 80] model incorporates a number of unique characteristics:

- Although the consumer loses some level of control, the SaaS model shifts the burden of getting and keeping an enterprise application up and running from the consumer to the vendor. It permits users to leverage the software functionality without the burden of deploying and managing the software themselves. The applications are accessed through a web-based interface typically run from a web browser. This delivery mechanism allows for easy scalability as new users are added.
- Generally, rather than licensing, installing and maintaining software on clients' computers or servers, the SaaS model lets users access the vendors software via the internet on a "pay-as-you-use" basis.
- Each consumer can opt either to share access to the software with other consumers (multi-tenancy), thus enabling shared total costs and creating economies of scale, or decide to be a single tenant, thus providing greater control and security.
- The SaaS model includes systematic support of the software, rather than annual maintenance and upload of fixes and patches, to all subscribers.
- The SaaS model enables every consumer to benefit from the vendor's latest technological features

without the disruptions and costs associated with software updates and upgrades.

- The SaaS model eliminates the added costs and complexities of deploying additional hardware and software, or dedicating additional staff resources to support an enterprise application on an ongoing basis.

The traditional method of purchasing software requires the consumer to locally install an application on their computer and use licenses to authorize the usage. With SaaS the consumer pays for the software on a subscription level and does not need to install any software on their computers. The software, application, is instead accessed via the internet through a web browser [75, 78]. An example of this is Google Docs, a word processing application offered online. The user can access the application through a web browser, create documents and use all the features of the application [81]. What differs SaaS from PaaS and IaaS is that the user will not alter the application itself, nor the hardware that the application runs on, or the network configuration. What Google offers with Google Docs is an application that the user can use but not directly alter. It is like a traditional computer program but used through the internet [75].

V. PUBLIC CLOUD

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services [9]. In public clouds, resources are offered as a service, usually over an internet connection, for a pay-per-usage fee. Users can scale their use on demand and do not need to purchase hardware to use the service. Public cloud providers manage the infrastructure and pool resources into the capacity required by its users [4]. Public clouds are available to the general public or large organizations, and are owned by a third party organization that offers the cloud service [57]. A public cloud is hosted on the internet and designed to be used by any user with an internet connection to provide a similar range of capabilities and services [13]. Public cloud users are typically residential users and connect to the public internet through an internet service provider's network [82]. Google, Amazon and Microsoft are examples of public cloud vendors who offer their services to the general public [78]. Data created and submitted by consumers are usually stored on the servers of the third party vendor [75].

The advantages of public cloud include:

- Data availability and continuous uptime
- 24/7 technical expertise
- On demand scalability
- Easy and inexpensive setup
- No wasted resources

Drawbacks of public cloud:

- Data security
- Privacy

Another issue with public cloud is that you may not know where your data is stored or how it is backed up, and whether unauthorized users can get access to it. Reliability is another concern for public cloud networks. A recent two-day Amazon cloud outage, for example, left dozens of major e-commerce websites disabled or completely unavailable [83].

Examples of public cloud include:

- Amazon AWS
- Google Apps
- Salesforce.com
- Microsoft BPOS
- Microsoft Office 365

Public cloud computing represents a significant paradigm shift from the conventional norms of an organizational data center to a deperimeterized infrastructure open to use by potential adversaries. As with any emerging information technology area, cloud computing should be approached carefully with due consideration to the sensitivity of data. Planning helps to ensure that the computing environment is as secure as possible and in compliance with all relevant organizational policies and that privacy is maintained. It also helps to ensure that the agency derives full benefit from information technology spending.

Public cloud providers' default offerings generally do not reflect a specific organization's security and privacy needs. From a risk perspective, determining the suitability of cloud services requires an understanding of the context in which the organization operates and the consequences from the plausible threats it faces. Adjustments to the cloud computing environment may be warranted to meet an organization's requirements. Organizations should require that any selected public cloud computing solution is configured, deployed, and managed to meet their security, privacy, and other requirements.

While one of the biggest obstacles facing public cloud computing is security, the cloud computing paradigm provides opportunities for innovation in provisioning security services that hold the prospect of improving the overall security of some organizations. The biggest beneficiaries are likely to be smaller organizations that have limited numbers of information technology administrators and security personnel, and can gain the economies of scale available to larger organizations with sizeable data centers, by transitioning to a public cloud.

Non-negotiable service agreements in which the terms of service are prescribed completely by the cloud provider are generally the norm in public cloud computing. Negotiated service agreements are also possible. Similar to traditional information technology outsourcing contracts used by agencies, negotiated agreements can address an organization's concerns about security and privacy details, such as the vetting of employees, data ownership and exit rights, breach notification, isolation of tenant applications, data encryption and segregation, tracking and reporting service effectiveness, compliance with laws and regulations, and the use of validated products meeting federal or national standards (*e.g.*, Federal Information Processing Standard 140). A negotiated agreement can also document the assurances the cloud provider must furnish to corroborate that organizational requirements are being met.

Critical data and applications may require an agency to undertake a negotiated service agreement in order to use a public cloud. Points of negotiation can negatively affect the economies of scale that a non-negotiable service agreement brings to public cloud computing, however, making a negotiated agreement less cost effective. As an alternative, the organization may be able to employ compensating controls to work around identified shortcomings in the public cloud service.

With the growing number of cloud providers and range of services from which to choose, organizations must exercise due diligence when selecting and moving functions to the cloud. Decision making about services and service arrangements entails striking a balance between benefits in cost and productivity versus drawbacks in risk and liability. While the sensitivity of data handled by government organizations and the current state of the art make the likelihood of outsourcing all information technology services to a public cloud low, it should be possible for most government organizations to deploy some of their information technology services to a public cloud, provided that all requisite risk mitigations are taken [60].

VI. PRIVATE CLOUD

The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise [9]. The cloud infrastructure is accessed only by the members of the organization and/or by granted third parties. The purpose is not to offer cloud services to the general public, but to use it within the organization. For example an enterprise that wants to make consumer data available to their different stores [75]. A private cloud is hosted in the data centre of a company and provides its services only to users inside that company or its partners. A private cloud provides more security than public clouds, and cost saving in case it utilizes otherwise un-used capacities in an already existing data centre. Making such un-used capacities available through cloud interfaces allows to utilize the same tools as when working with public clouds and to benefit the capabilities inherent in cloud management software, like a self-service interface, automated management of computing resources, and the ability to sell existing over capacities to partner companies. The Aberdeen group published a report, which concludes that organizations operating private clouds typically have about 12% cost advantage over organizations using public clouds [84]. A private cloud has the potential to give the organization greater control over the infrastructure and computational resources [60]. Although all cloud models offer similar advantages as there is not much difference in technology. The only big advantage that private cloud has over public cloud is that of data security and privacy.

Over the last several years, major cloud service breaches have dominated the headlines. Corporations are taking notice and some are deciding that the private cloud proves less risky. Private cloud's ability to virtualized services maximizes hardware usage, ultimately reducing costs and complexity. The most important resources of any organization are arguably its resources and its data. Trusting these resources to outside entities that have been repeatedly proven vulnerable to attack puts an organization in a most precarious situation [85-93].

The major drawback of private cloud is its higher cost. When comparisons are made with public cloud; the cost of purchasing equipment, software and staffing often results in higher costs to an organization having their own private cloud.

VII. HYBRID CLOUD

Hybrid clouds are more complex than the other deployment models, since they involve a composition of two or more clouds (private, community, or public). Each member remains a unique entity, but is bound to others through standardized or proprietary technology that enables application and data portability among them [60]. A hybrid cloud is a composition of at least one private cloud and at least one public cloud. A hybrid cloud is typically offered in one of two ways: a vendor has a private cloud and forms a partnership with a public cloud provider, or a public cloud provider forms a partnership with a vendor that provides private cloud platforms [94]. Hybrid cloud infrastructure is a composition of two or more clouds that are unique entities, but at the same time are bound together by standardized or proprietary technology that enables data and application portability [57]. In hybrid cloud, an organization provides and manages some resources in-house and some out-house. For example, organizations that have their human resource (HR) and customer relationship management (CRM) data in a public cloud like Saleforces.com but have confidential data in their own private cloud [95]. Ideally, the hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without exposing mission-critical applications and data to third-party vulnerabilities. This type of hybrid cloud is also referred to as hybrid IT [96-99].

Hybrid clouds [100] offer the cost and scale benefits of public clouds, while also offering the security and control of private clouds. The advantages of hybrid cloud include:

- Reduces capital expenses as part of the organization’s infrastructure, needs are outsourced to public cloud providers.
- Improves resource allocation for temporary projects at a vastly reduced cost because the use of public cloud removes the need for investments to carry out these projects.
- Helps optimize the infrastructure spending during different stages of the application lifecycle. Public clouds can be tapped for development and testing while private clouds can be used for production. More importantly, public clouds can be used to retire applications, which may be no longer needed because of the move to SaaS, at much lower costs than dedicated on-premise infrastructure.
- Offers both the controls available in a private cloud deployment along with the ability to rapidly scale using public cloud.
- Supplies support for cloud-bursting.
- Provides drastic improvements in the overall organizational agility, because of the ability to leverage public clouds, leading to increased opportunities.

Drawbacks of hybrid cloud are:

- As a hybrid cloud extends the IT perimeter outside the organizational boundaries, it opens up a larger surface area for attacks with a section of the hybrid cloud infrastructure under the control of the service provider.
- An easier approach to solving the identity, needs of hybrid clouds is to extend the existing enterprise identity and access management to the public clouds. This opens up concerns about how this approach will affect the enterprise identity and its impact on the organization’s security.
- When organizations manage complex hybrid cloud environments using a management tool, either as a part of the cloud platform or as a third-party tool, organizations should consider the security implications of using such a tool. For example, the management tool should be able to handle the identity and enforce security uniformly across hybrid cloud environments.
- A hybrid cloud makes the data flow from a private environment to a public cloud much easier. There are privacy and integrity concerns associated with such data movement because the privacy controls in the public cloud environment vary significantly from the private cloud.
- There are risks associated with the security policies spanning the hybrid cloud environment such as issues with how encryption keys are managed in a public cloud compared to a pure private cloud environment.

Hybrid clouds offer a greater flexibility to businesses while offering choice in terms of keeping control and security. Hybrid clouds are usually deployed by organizations willing to push part of their workloads to public clouds either for cloud-bursting purposes or for projects requiring faster implementation. Because hybrid clouds vary based on company needs and structure of implementation, there is no one-size-fits-all solution. Since hybrid environments involve both on-premise and public cloud providers, some additional infrastructure security considerations come into the picture, which are normally associated with public clouds. Any businesses planning to deploy hybrid clouds should understand the different security needs and follow the industry best practices to mitigate any risks. Once secure, a hybrid cloud environment can help businesses transition more applications into public clouds, providing additional cost savings [100-102].

VIII. COMMUNITY CLOUD

A community cloud falls between public and private clouds with respect to the target set of consumers. It is somewhat similar to a private cloud, but the infrastructure and computational resources are exclusive to two or more organizations that have common privacy, security, and regulatory considerations, rather than a single organization [60]. The community cloud aspires to combine distributed resource provision from grid computing, distributed control from digital ecosystems and sustainability from green computing, with the use cases of cloud computing, while making greater use of self-management advances from autonomic computing. Replacing vendor clouds by shaping the under utilized resources of user machines to form a community cloud, with nodes potentially fulfilling all roles, consumer, producer, and most importantly coordinator [105-106]. The advantages [107] of community cloud include:

- Cost of setting up a communal cloud versus individual private cloud can be cheaper due to the division of costs among all participants.
- Management of the community cloud can be outsourced to a cloud provider. The advantage here is that the provider would be an impartial third party that is bound by contract and that has no preference to any of the clients involved other than what is contractually mandated.
- Tools residing in the community cloud can be used to leverage the information stored to serve consumers and the supply chain, such as return tracking and just-in-time production and distribution.

Drawbacks of community cloud:

- Costs higher than public cloud.
- Fixed amount of bandwidth and data storage is shared among all community members.

The concept of community cloud is still in its infancy, but picking up rapidly among start-ups and small and medium term businesses.

IX. CONCLUSION

Organizations willing to adapt cloud model for their enterprise often feel confused, which model will fit best for their business. To help business organizations take this decision, this review was planned. Cloud computing is a new emerging technology, which every organization these days wants to adapt for its business for more profitability and scalability. This communication defined cloud computing, highlighted all the service models of cloud computing and discussed the features of public, private, hybrid and community cloud computing. Also, cloud security issues were raised and discussed. Technology-wise, there is not much significant difference among these four models. They all run on the same technology, one of the pitfalls of adopting a public cloud is data security and privacy. On the other hand private cloud is secure, but costly, so not every organization can afford a private cloud. Hybrid cloud is a mixture of public and private cloud; organizations keep their regular data in the public cloud and use private cloud to keep their sensitive data in hybrid model. Similarly a community cloud falls between public and private cloud, as some organizations get together and form a separate private cloud of their own, called a community cloud.

REFERENCES

[1] T. Surcel and F. Alecu, “Applications of Cloud Computing,” In International Conference of Science and Technology in the Context of the Sustainable Development, pp. 177-180, 2008.

[2] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis and A. Vakali, “Cloud computing: Distributed Internet computing for IT and scientific research,” Internet Computing, IEEE, 13(5), 10-13, 2009.

[3] Sumit Goyal, “Perils of cloud based enterprise resource planning,” Advances in Asian Social Science, 3(4), 880-881, 2013.

[4] G. Lewis, “Basics about cloud computing,” Software Engineering Institute Carniege Mellon University, Pittsburgh, 2010.

[5] A. Beloglazov, “Energy-Efficient Management of Virtual Machines in Data Centers for Cloud Computing,” PhD Thesis, 2013.

[6] I. Foster, Y. Zhao, I. Raicu and S. Lu, “Cloud computing and grid computing 360-degree compared,” In: IEEE Grid Computing Environments Workshop, pp.1-10, November, 2008.

[7] Z. Liu H.S. Lallie and L. Liu L, “A Hash-based Secure Interface on Plain Connection,” In: Proceedings of CHINACOM. ICST.OTG & IEEE Press, Harbin, China, 2011.

[8] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee and I. Stoica, “ Above the clouds: A Berkeley view of cloud computing,” Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Rep. UCB/EECS, 28, 2009.

[9] P. Mell and T. Grance, “The NIST definition of cloud computing (draft),” NIST special publication, 800(145), 7, 2011.

[10] A. Stevens, “When hybrid clouds are a mixed blessing,” The Register, June 29, 2011.

[11] S. Roschke, F. Cheng and C. Meinel, “Intrusion Detection in the Cloud,” In: Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.

[12] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg and I. Brandic, “Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility,” Future Generation computer systems, 25(6), 599-616, 2009.

[13] (2013) Open Cloud Manifesto. [Online]. Available: http://www.opencloudmanifesto.org/.

[14] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “BAbove the clouds: A Berkeley view of cloud computing,”[Electr. Eng. Comput. Sci. Dept., Univ. California, Berkeley, CA, Tech. Rep. UCB/EECS-2009-28, February 2009.

[15] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “BA break in the clouds: Towards a cloud definition,” [SIGCOMM Comput. Commun. Rev., 39(1), 50–55, 2009.

[16] D. Kondo, B. Javadi, P. Malecot, F. Cappello, and D. P. Anderson, “BCost-benefit analysis of cloud computing versus desktop grids,” In: Proceedings of IEEE International Symposium on Parallel and Distributed Processing, Rome, Italy, May 2009.

[17] R. Buyya, C. S. Yeo, and S. Venugopal, “BMarket-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities,” In: Proceedings of 10th IEEE International Conference on High Performance Computing and Communication, Dalian, China, Sep. 2008, pp. 5–13.

[18] S. Ostermann, A. Iosup, N. Yigitbasi, R. Prodan, T. Fahringer and D. Epema, “A performance analysis of EC2 cloud computing services for scientific computing,” In: Cloud Computing (pp. 115-131). Springer Berlin Heidelberg, 2010.

[19] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff and D. Zagorodnov, “The eucalyptus open-source cloud-computing system,” In: Proceedings of 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, (pp. 124-131), May 2009.

[20] T. Velte, A. Velte and R. Elsenpeter, “Cloud computing, a practical approach,” McGraw-Hill, Inc., 2009.

[21] R. Buyya, S. Pandey and C. Vecchiola, “Cloudbus toolkit for market-oriented cloud computing,” In: Cloud Computing (pp. 24-44). Springer Berlin Heidelberg, 2009.

[22] L. Youseff, M. Butrico and D. Da Silva, “Toward a unified ontology of cloud computing,” In: Proceedings of IEEE Grid Computing

Environments Workshop, (pp. 1-10), November 2008.

[23] S. Pearson, Y. Shen and M. Mowbray, "A privacy manager for cloud computing," In: Cloud Computing (pp. 90-106). Springer Berlin Heidelberg, 2009.

[24] M.A. Vouk, "Cloud computing–issues, research and implementations," Journal of Computing and Information Technology, 16(4), 235-246, 2004.

[25] Q. Zhang, L. Cheng and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of Internet Services and Applications, 1(1), 7-18, 2010.

[26] L. Wang, J. Tao, M. Kunze, A.C. Castellanos, D. Kramer and W. Karl, "Scientific cloud computing: Early definition and experience," In: Proceedings of 10th IEEE International Conference on High Performance Computing and Communications, (pp. 825-830), September 2008.

[27] H. Brian, T. Brunschwiler, H. Dill, H. Christ, B. Falsafi, M. Fischer and M. Zollinger, "Cloud computing," Communications of the ACM, 51(7), 9-11, 2008.

[28] R.L. Grossman, "The case for cloud computing," IT professional, 11(2), 23-27, 2009.

[29] N. Leavitt, "Is cloud computing really ready for prime time," Growth, 27(5), 2009.

[30] C. Wang, Q. Wang, K. Ren and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," In: IEEE Proceedings of INFOCOM, (pp. 1-9), March 2010.

[31] L.M. Kaufman, "Data security in the world of cloud computing," IEEE Security & Privacy, 7(4), 61-64, 2009.

[32] B. P. Rimal, E. Choi and I. Lumb, "A taxonomy and survey of cloud computing systems," In: Proceedings of IEEE 5th International Joint Conference on IMS and IDC, (pp. 44-51), August 2009.

[33] L. Yan, C. Rong and C. Zhao, "Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography," In: Cloud Computing (pp. 167-177). Springer Berlin Heidelberg, 2009.

[34] D. Catteddu, "Cloud Computing: Benefits, risks and recommendations for information security," (pp. 17-17). Springer Berlin Heidelberg.

[35] B. Rochwerger, D. Breitgand, E. Levy, A. Galis, K. Nagin, I.M. Llorente and F. Galán, "The reservoir model and architecture for open federated cloud computing," IBM Journal of Research and Development, 53(4), 4-1, 2009.

[36] N. Santos, K.P. Gummadi and R. Rodrigues, "Towards trusted cloud computing," In: Proceedings of the conference on Hot topics in cloud computing (pp. 3-3), June, 2009.

[37] M. Jensen, J. Schwenk, N. Gruschka and L.L. Iacono, "On technical security issues in cloud computing," In: Proceedings of IEEE International Conference on Cloud Computing, (pp. 109-116), September, 2009.

[38] L. Wang, G. Von Laszewski, A. Younge, X. He, M. Kunze, J. Tao and C. Fu, "Cloud computing: a perspective study," New Generation Computing, 28(2), 137-146, 2010.

[39] M. D. Ryan, "Cloud computing privacy concerns on our doorstep," Communications of the ACM, 54(1), 2011.

[40] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, 34(1), 1-11, 2011.

[41] R. Buyya, R. Ranjan and R.N. Calheiros, "Modeling and simulation of scalable Cloud computing environments and the CloudSim toolkit: Challenges and opportunities. In: Proceedings of IEEE International Conference on High Performance Computing & Simulation, (pp. 1-11), June 2009.

[42] J. Brodkin, "Gartner: Seven cloud-computing security risks," 2008.

[43] Q. Wang, C. Wang, J. Li, K. Ren and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," In: Computer Security–ESORICS (pp. 355-370). Springer Berlin Heidelberg, 2009.

[44] L. Qian, Z. Luo, Y. Du and L. Guo, "Cloud computing: an overview," In: Cloud Computing (pp. 626-631). Springer Berlin Heidelberg, 2009.

[45] H. Li, Y. Dai, L. Tian and H. Yang, "Identity-based authentication for cloud computing," In Cloud computing (pp. 157-166). Springer Berlin Heidelberg, 2009.

[46] S. Pearson, "Taking account of privacy when designing cloud computing services," In: IEEE ICSE Workshop on Software Engineering Challenges of Cloud Computing, (pp. 44-52), May 2009.

[47] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," In: Proceedings of IEEE INFOCOM, (pp. 1-9), March 2010.

[48] H. Takabi, J.B. Joshi and G.J. Ahn, "Security and privacy challenges in cloud computing environments," Security & Privacy, IEEE, 8(6), 24-31, 2010.

[49] T. Dillon, C. Wu and E. Chang, "Cloud computing: Issues and challenges," In: Proceedings of IEEE 24th International Conference on Advanced Information Networking and Applications, (pp. 27-33), April, 2010.

[50] G. Boss, P. Malladi, D. Quan, L. Legregni and H. Hall, "Cloud computing," IBM white paper, 321, 224-231, 2007.

[51] J.W. Rittinghouse and J.F. Ransome, "Cloud computing: implementation, management, and security," CRC press, 2009.

[52] W. Kim, "Cloud Computing: Today and

Tomorrow," Journal of Object Technology, 8(1), 65-72, 2009.

[53] Y. Chen, V. Paxson and R.H. Katz, "What's new about cloud computing security," University of California, Berkeley Report No. UCB/EECS-2010-5 January, 20(2010).

[54] D. Durkee, "Why cloud computing will never be free. Queue, 8(4), 20, 2010.

[55] D. G. Feng, M. Zhang, Y. Zhang and Z. Xu, "Study on cloud computing security," Journal of Software, 22(1), 71-83, 2011.

[56] S. Pearson and A. Charlesworth, "Accountability as a way forward for privacy protection in the cloud," In: Cloud computing (pp. 131-144). Springer Berlin Heidelberg, 2009.

[57] P. Mell and T. Grance, "Effectively and securely using the cloud computing paradigm," NIST, Information Technology Lab., 2009.

[58] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, 28(3), 583-592, 2012.

[59] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," In: Proceedings of IEEE 33rd International Convention on MIPRO, (pp. 344-349) May, 2010.

[60] W. Jansen and T. Grance, "Guidelines on security and privacy in public cloud computing," NIST special publication 800-144, 2011.

[61] S. Srinivasan and R.B. Krishnan, "Data property analyzer for information storage in cloud," In: Proceedings of IEEE International Conference on Pattern Recognition, Informatics and Medical Engineering (pp. 443-446), February, 2013.

[62] C. Liu, J. Chen, L. Yang, X. Zhang, C. Yang, R. Ranjan and K. Ramamohanarao, "Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates," 2013.

[63] S. Sawhney, H. Puri and H.V. Rietschote, U.S. Patent No. 8,370,312. Washington, DC: U.S. Patent and Trademark Office, 2013.

[64] A. Juels, M.E. Van Dijk, A. Oprea, R.L. Rivest and E.P. Stefanov, U.S. Patent No. 8,346,742. Washington, DC: U.S. Patent and Trademark Office, 2013.

[65] J. Ekanayake and G. Fox, "High performance parallel computing with clouds and cloud technologies," In: Cloud Computing (pp. 20-38). Springer Berlin Heidelberg, 2010.

[66] S. Hossain, "Infrastructure as a Service," In: A. Bento, and A. Aggarwal (Eds.), Cloud Computing Service and Deployment Models: Layers and Management (pp. 26-49). Hershey, PA: Business Science Reference. doi:10.4018/978-1-4666-2187-9.ch002, 2013.

[67] W. Dawoud, I. Takouna and C. Meinel, "Infrastructure as a service security: Challenges and solutions," In: 7th International Conference on Informatics and Systems, 1(8), pp. 28-30, March 2010.

[68] R. Prodan and S. Ostermann, "A survey and taxonomy of infrastructure as a service and web hosting cloud providers," In: Proceedings of 10th IEEE/ACM International Conference on Grid Computing, 17(25), 13-15, October 2009.

[69] M. Mattess, C. Vecchiola and R. Buyya, "Managing Peak Loads by Leasing Cloud Infrastructure Services from a Spot Market," In: Proceedings of IEEE 12th International Conference on High Performance Computing and Communications, 180(188), 1-3, September 2010.

[70] S. Bhardwaj, J. Jain and S. Jain, "Cloud computing: A study of infrastructure as a service (IAAS)," International Journal of engineering and information Technology, 2(1), 60-63, 2010.

[71] W.J. Rittinghouse and F.J. Ransome, "Cloud Computing Implementation, Management, and Security," Boca Raton, FL, CRC Press, 2010.

[72] G. Reese, "Cloud Application Architectures," O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2009.

[73] (2012) Aws. Amazon website. [Online]. Available: http://aws.amazon.com/ec2/.

[74] J. Hurwitz, R. Bloor, M. Kaufman and F. Halper, "Cloud computing for dummies," Wiley Publishing, Inc., Indianapolis, Indiana, 2010.

[75] O. Hamrén. (2012). M.S. Thesis. "Mobile phones and cloud computing".

[76] J. Peng, X. Zhang, Z. Lei, B. Zhang, W. Zhang and Q. Li, "Comparison of Several Cloud Computing Platforms," In: 2nd IEEE International Symposium on Information Science and Engineering,(pp.23-27), 2009.

[77] L.M. Vaquero, L. Rodero-Merino, J. Caceres and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, 39(1), 50-55, 2008.

[78] T. Mather, S. Kumaraswamy and S. Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance," Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2009.

[79] P. Nema and B.D. Bailey, "Is SaaS the Silver Lining to the Cloud," SVB, September 2, 2009.

[80] G. Newton, "Software as a Service (SaaS) Strategy V1.0, State of Oregon, 2011.

[81] (2012) Drive. Google Website. [Online]. Available: https://drive.google.com/.

[82] J. Baliga, R. Ayre, W. V. Sorin, K. Hinton, and R. S. Tucker, "BEnergy consumption in access networks," In: Proceedings of National Optical Fiber Communication Conference, San Diego, CA, February 2008.

[83] (2013) Veruscorp Website. [Online]. Available: http://www.veruscorp.com/public-cloud-networks.aspx.

[84] (2012) Aberdeen Website. [Online]. Available: http://www.aberdeen.com/Research/Research-Library.aspx?search=private%20could.

[85] (2013) Datamation Website. [Online]. Available:

http://www.datamation.com/cloud-computing/benefits-of-private-cloud-over-public-cloud-2.html.

[86] F. Doelitzscher, A. Sulistio, C. Reich, H. Kuijs and D. Wolf, "Private cloud for collaboration and e-Learning services: from IaaS to SaaS," Computing, 91(1), 23-42, 2011.

[87] Y.W. Ahn and A. M. K. Cheng, "Autonomic computing architecture for real-time medical application running on virtual private cloud infrastructures. ACM SIGBED Review, 10(2), 15-15, 2013.

[88] M. Missbach, J. Stelzel, C. Gardiner, G. Anderson and M. Tempes, "Private Cloud Infrastructures for SAP," In: SAP on the Cloud (pp. 137-166). Springer Berlin Heidelberg, 2013.

[89] A. Flavel, C. Lund, and H.F. Nguyen, "Network connectivity wizard to support automated creation of customized configurations for virtual private cloud computing networks," U.S. Patent Application 13/771,188, 2013.

[90] S. Kumar, J. Ali, A. Bhagat, and P.K. Jinendran, "An Approach of Creating a Private Cloud for Universities and Security Issues in Private Cloud, 2013.

[91] L. Cao, X. Liu, M. Liu and K. Han, "Process-based Security Detection Approach for Virtual Machines on Private Cloud Platforms," Journal of Networks, 8(6), 1380-1386, 2013.

[92] T.S. Soares, M.A.R. Dantas, D. Macedo and M.A. Bauer, "A data management in a private cloud storage environment utilizing high performance distributed file systems," In: Proceedings of the IEEE 22nd International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, (pp. 158-163) June 2013.

[93] H. Ghanbari, B. Simmons, M. Litoiu and G. Iszlai, "Feedback-based optimization of a private cloud," Future Generation Computer Systems, 28(1), 104-111, 2012.

[94] (2013) Search cloud computing Tec target Website. [Online]. Available: http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud.

[95] D.E.Y. Sarna, "Implementing and Developing Cloud Computing Applications," Taylor and Francis Group, Boca Raton, FL: CRC Press, 2011.

[96] D. Garber, J. Malik and A. Fazio, "Windows Azure Hybrid Cloud," John Wiley & Sons, 2013.

[97] Z. Zhou, H. Zhang, X. Du, P. Li and X. Yu, "Prometheus: Privacy-aware data retrieval on hybrid cloud," In: Proceedings of IEEE INFOCOM, (pp. 2643-2651), April 2013.

[98] A. Tripathi and M.S. Jalil, "Data access and integrity with authentication in hybrid cloud," Oriental International Journal of Innovative Engineering Research, 1(1), pp-030, 2013.

[99] R.K. Grewal and P.K. Pateriya, "A rule-based approach for effective resource provisioning in hybrid cloud environment," In: New Paradigms in Internet Computing (pp. 41-57). Springer Berlin Heidelberg, 2013.

[100] (2013) Emma TrendMicro Website. [Online]. Available: http://emea. TrendMicro. com/imperia/md/content/uk/cloud security/wp01 _hybridcloud-krish_110624us. pdf.

[101] R. Palwe, G. Kulkarni and A. Dongare, "A new approach to hybrid cloud," International Journal of Computer Science and Engineering. 2(1), 1-6, 2012.

[102] R. Sujay, "Hybrid cloud: A new era," International Journal of Computer Science and Technology, 2(2), 323-326, 2011.

[103] (2013) Philippheckel Website. [Online]. Available: http://www.philippheckel.com/files /hybrid-cloud-presentation.pdf.

[104] C. Philipp, "Heckel Hybrid Clouds: Comparing Cloud Toolkits," University of Mannheim, 7 May, 2010.

[105] A. Marinos and G. Briscoe, "Community cloud computing," In: Cloud Computing (pp. 472-484). Springer Berlin Heidelberg, 2009.

[106] X. G. Condori, "Community cloud computing," Revista de Informaci ón Teconolog á Y Sociedad, 70-72, 2013.

[107] (2013) Thecaseforcloud Website. [Online]. Available: http://thecaseforcloud.blogspot.in/2011/11/innovation-community-clouds-part-2.html.

Sumit Goyal received his Bachelor and Master's degree from the central university of Government of India. He has published research papers in many international journals throughout the world, which have been cited many times. Besides that, he has also written book chapters, instructional manuals, marketing collaterals, user manuals, product guides, review articles, technical papers, and brought out special issues of international journals, as Guest Editor. He is holding positions in the editorial board of many world renowned international journals. He has great experience in preparing B2B marketing, sales and advertising campaigns for leading IT Software Enterprises. He is expert in Cloud Computing, Business Intelligence and Analytics, Big Data, Market Research, Mobile Computing, E-Commerce, ERP, Social Media Marketing/Advertising, E-Learning, Artificial Intelligence, Artificial Neural Networks, Machine Learning, Soft Computing, Telecommunications, Wireless Technology, Honeynet, and Networking Servers.

How to cite this paper: Sumit Goyal,"Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review", IJCNIS, vol.6, no.3, pp.20-29, 2014. DOI: 10.5815/ijcnis.2014.03.03

These days cloud computing is booming like no other technology. Every organization whether it's small, mid-sized or big, wants to adapt this cutting edge technology for its business. As cloud technology becomes immensely popular among these businesses, the question arises: Which cloud model to consider for your business?Â This review paper answers the question, which model would be most beneficial for your business. All the four models are defined, discussed and compared with the benefits and pitfalls, thus giving you a clear idea, which model to adopt for your organization.Â @inproceedings{Goyal2014PublicVP, title={Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review}, author={Sumit Goyal}, year={2014} }. Sumit Goyal.