Comparing Cloud Computing & Big Data Risk Management

Marquita Snow
Department of Computer Science
Hampton University
marquita.snow@my.hamptonu.edu

Jean Muhammad
Department of Computer Science
Hampton University
jeana.muhammad@hamptonu.edu

ABSTRACT

This paper will inspect the issues revolved around cloud computing and big data so that even a consumer can understand its purposes, risks, and benefits. This paper will also highlight three companies' world cutting-edge evolutionary inventions that are complimentary projects that will help quantify the human existence and quality of life just from the use of big data alone and how big data will continue to explode and transform many different industries. Hopefully, after someone reads this paper, they will gain a profound appreciation for the cloud and the details of risk management and data processing in cloud computing environment.

CCS CONCEPTS

• **Software and its engineering** → Risk management; Cloud computing

KEYWORDS

Cloud Computing, Risk Management, Big Data Analysis

ACM Reference format:

M. Snow, J. Muhammad. 2017. Comparing Cloud Computing & Big Data Risk Management. In *Proceedings of 2017 ADMI Symposium,* Virginia Beach, Virginia USA, March 23-26, 2017.

1 INTRODUCTION

If you think that you are exempt from the new wave of the revolution of big data, then you are sadly mistaken. Big data is the new wave to the world around us and is changing every aspect to the way we conduct business. Big data has grown past just a general concept into its very own era of revolutionary purposes for the use of big data. Time Magazine made an 80-second video simplifying the principle and concepts of the cloud by demystifying its functions. They went into detail about the time share features of today's technological devices (e.g., computers, mobile devices) and how the benefits of using cloud computing outweigh the risks marginally. They bring up a valid point with their highlighting of the risks alongside the cloud models. Overall, they agree with the consensus agreement across the various research outlets, that cloud computing is here to stay and it will continue to evolve. As the world changes, the industries of big data and cloud computing will gain momentum for developments in understanding the processing big data as a whole with its uses, analysis challenges, and deployment measures across different companies despite the many different platforms provided by the concept of cloud computing.

2 OVERVIEW: CLOUD COMPUTING & BIG DATA

2.1 Cloud Computing & Big Data: Brief History

Cloud computing has a vast history which dates back to the 1950s when John McCarthy created the terminology and concept of artificial intelligence paralleling closely to the functionality of cloud computing1. Cloud computing can be defined with a very complex technological definition because it is always changing in its features, capabilities, and vulnerabilities.

Big data's historical origins are not completely clear because it has a conglomerate of characteristics that spread across a spectrum of industries such as: business, technology, statistics, economics, mathematics, intelligence, and etc. The conundrum that we cannot definitively give the foundational credit or merit to one particular entity goes to show why it is not easy to define big data simplistically.

2.2 Definitions

2.2.1 Cloud computing. The National Institute of Standards and Technology (NIST) developed a general definition that will be used as a benchmark to give a better understanding of its industrial relation to computing. They define cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" that are "rapidly provisioned and released with minimal management effort or service provider interaction which is composed of five essential characteristics, three service models, and four deployment models" (The NIST 800-145 Definition of Cloud Computing, 2). This definition has many technical terminologies

that may make the concept of cloud computing complex to the average person.

2.2.2 Big Data. Merriam-Webster categorizes the term big data as a noun with the definition as "an accumulation of data that is too large and complex for processing by traditional database management tools" which is only a basic understanding of the what big data truly is to the world around us. The simple definition given by Merriam-Webster is very different from the ambiguous definition that big data has in the data processing industry. The ambiguity comes from the actuality that big data is an inclusive business that everyone in the world plays a part in every day.

2.3 Cloud Computing

Big data is a big business that revolves around revolutionary ways to make the ways we use big data and collect big data easier. There are various companies that use, collect, and analyze big data which highlights the versatile nature of being used in different circumstances. However, add the concept of cloud computing to the equation of processing big data on an opportunity for scalable data management. Just like it is important to know that every cloud platform is not a one size fit all model with the various deployment modes, the same concept applies when using a cloud database to process big data.

Before anyone can understand the issues of cloud computing, the characteristics of cloud computing must be comprehended. There are five different essential aspects that this paper will cover. The definitions were provided directly by The National Institute of Standards and Technology (NIST) publications on The Definition of Cloud Computing. This document also includes their recommendations for cloud computing which are "the precedential frameworks in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347." This disclaimer goes to prove the importance of the responsibilities of this agency in publicizing and informing to the technological forum for agencies, organizations, and the general public.
In Figure 1, this lists the various automation characteristics that could occur in any particular cloud service also known as characteristics of a cloud service.

The essential characteristics of cloud computing services which are: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. NIST defines the key features as followed below as characteristics that every cloud service must have:

1. Cloud services must be an on-demand self-service in which a customer can provision on its own devoid of communication with the cloud service provider.
2. Cloud services must have broad network access with reachability and platform options.
3. Cloud services must be a multi-tenant atmosphere promoting location-independence with various resources virtually and physically.
4. Cloud services must support rapid elasticity with the flexibility for expansion and minimization on demand of policy, with zero impact to applications or users.
5. Cloud services must be a measured service with controllability of their performance or metered by the performance with a variation of the service models.

The next key concept to understand are the different types of service models available with cloud computing which are: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). The different service models can work either independently of be co-dependent on one another to function in a hybrid type atmosphere. The importance of understanding the difference between the three service models is due to they affect the cloud services are accessible by those using the cloud services. The reason it is important to understand what type of service model the cloud computing service is using because a user wants a cloud service that will meet their needs of accessibility to their information.

2.3.1 Terminology, Definitions, and Figures In Figure 2, Figure 3, and Figure 4 it shows a depiction of the three different models of cloud computing by telling what the cloud service provider offers to the client and what the client will have based on that type of model of cloud service. Any of these models could be combined into a package to create a customized experience for the customer if they needed that particular type of model for their computing needs.

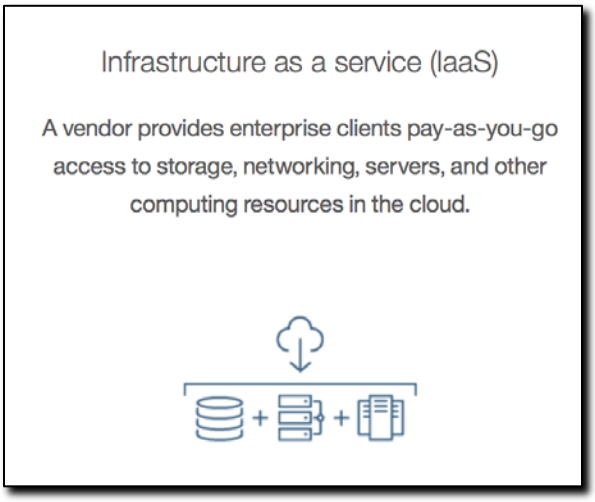

Figure 2: Infrastructure as a Service (IaaS) (Barbara, J)

2.3.2 Infrastructure as a Service (IaaS) model is where the cloud computing vendor gives the consumer access to use the provider's applications running on a cloud infrastructure using an on-demand basis. The client can access the applications through a web browser or a program interface causing flexibility and cost efficiency.

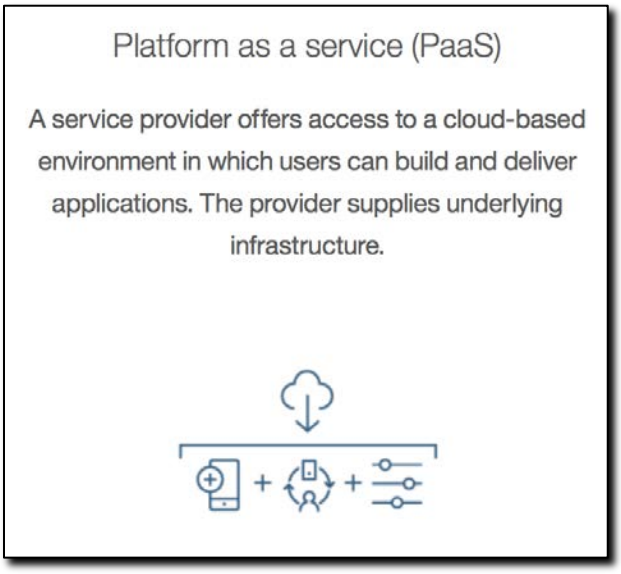

Figure 3: Platform as a Service (PaaS) (Barbara, J)

2.3.3 Platform as a Service (PaaS) model presents the consumer with the capability to have accessibility where they can construct, maintain, store or deliver applications onto a consumer-created the cloud infrastructure or acquire applications created using programming languages, libraries, services, and tools supported by the provider.

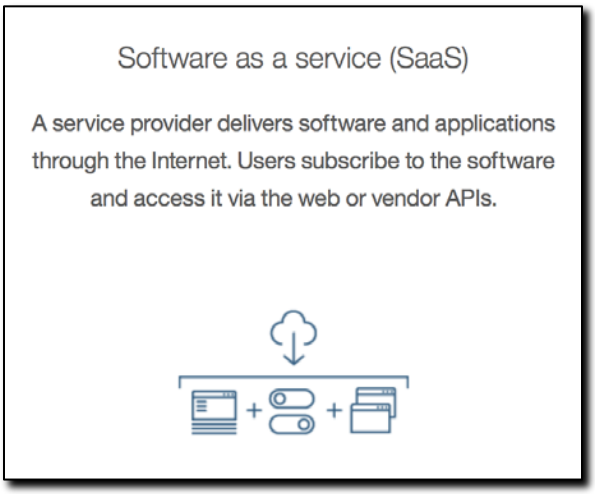

Figure 4: Software as a Service (SaaS) (Barbara, J)

2.3.4 Software as a Service (SaaS) The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to install and run software, which is provided by the SaaS vendor to the client. The installation of updates, software, and management of this model is all controlled by the vendor. Applications are remote accessible making it portable across the cloud making this model the most collaborative and versatile for users.

The next terminology to understand is the various deployment models that a cloud computing service can have for a user which are: private, community, public, and hybrid. These different deployment cloud models work in conjunction with the service model to provide the user with their cloud interface or the architectural makeup of their cloud. The variations of how these two aspects can be combined are to make the infrastructure more integral into their needs for a cloud computing service.

No single deployment model is a sure fit for a specific need of an organization's needs. As cloud computing evolves, a company may change their cloud deployment model to meet the needs of their business at that time. Although cloud computing can be a difficult topic for most people to grasp, the understanding of the different cloud deployment models is quite easy to understand.

2.3.5 Public Cloud The public cloud deployment model can be described as the model where of the physical properties are maintained and activated by a third party cloud computing provider through the public Internet. This deployment model is a pay-as-you-go model because services can be arranged and charged on the basis of usage alone. This model provides the peak grade of rate of cost through savings while demanding the least amount of overhead.

2.3.6 Private Cloud The private cloud presents a cloud deployment model where computer services are supplied to a business. This model has multiple of the same components of two-tier architecture, while incorporating structures connected with other deployment cloud computing models. Similar to other cloud deployment models, services are provided on demand from a dispersed substructure. In comparison to the client-server computing model, consumers do not access a particular resource in a disclosed location and there are hardware and software requirements. The cloud computing resources may be at a stationary on or at an off-site location. In addition to location capabilities, they can be maintained in-house or by a third party agency. This model emphasizes on the aspect of security and privacy that are deep-rooted in other cloud computing models.

2.3.7 Community Cloud A community cloud encompasses shared characteristics of the public and private cloud models. Like a public cloud, the community cloud might have software, data storage, and computing resources that are used by numerous groups. The difference in this model from the public model is that the infrastructure can only be used by groups that are known to each other in the community. It is also comparable to a private cloud because these groups are accountable for the operation of their own infrastructure meaning they are self-contained. The community cloud model can afford an organization a greater cost savings margin than the private cloud while offering some of the same security options. This model works best with organizations that have some of the same requirements with components such as security or legal agreements. The operational management of this

type of cloud model is like a private cloud model because it can be managed by the organizations or a third party provider.

2.3.8 Hybrid Cloud The hybrid cloud computing model has features of all of the other cloud models. This model is the most used method of cloud deployment within a sizable organization. A company may use in-house resources in a private cloud to have total control over its proprietary data. It can then use a public cloud storage provider for creating backups of lower levels of sensitive data. The hybrid cloud model is the most flexible because of the combinational feature which are an advantageous ability that allow companies to have more controls over their abilities and information.

There are many different variations of cloud computing setups for companies. There is not just one right and wrong way for a company to have their cloud system set up because it is based on their needs. A company's performance needs may change over time which means that they may also change their cloud computing model. Not only may the company's needs change but also the field of cloud computing may change to meet the needs of the age of technology which means that a business may need to change their cloud computing model to meet their specific performance abilities and the technological changes. The technological changes occur to aide in the control of the risks that the use of cloud computing can present.

3 Risk Management/Risk Assessment

In order to understand risk analysis and risk management, the term risk must be defined as an aspect that can cause harm, danger, contamination, or even an exposure of negligence on behalf of specified unforeseen details. Risk management is very important to cloud computing because it is a continuous task that needs to be handled by the cloud agency towards the benefits of their client. The difficult task is that due to cloud computing's continual advancements there are always new risks presenting themselves. It is often difficult for agencies to stay ahead of the development of new risks before they present themselves as a problematic issue that may jeopardize the integrity of the cloud system.

In order to understand risk management as an aspect of cloud computing, organizations must understand the different types of probable risks that may present in form while using a cloud system. They must also understand the risk assessment associated with these various risks.

Risk assessment is key importance when a company is deciding whether to use cloud computing or not to use cloud computing. "Properly assessing your organizational risk tolerance is essential before adopting a cloud computing platform" (Microsoft). Risk assessment is different from risk management but it falls into the categorization with risk management because it is the analysis on the basis of the findings under the risk management task. The findings are how we prevent or the probable solutions that could prohibit the risks from occurring or to reduce the heightened risk. There are so many different types of risk that can present or make the cloud system vulnerable.

There are also many different ways to compute that risk level through risk analysis or risk assessment. I will be using a ranking system ranging from 1 to10 on points covering the tiers of low (1 to 4 points), medium (5 to 6 points), and high (7 to 10 points) which are defined in Figure 5. This risk table was devised off the basis of research from MITRE and Microsoft. I built the concept diagram myself to display the differences between the different risk levels and the designated point systems that they receive between one another. The three levels have subcategories of:

Low (1 to 4 points)
- minor
- insignificant

Medium (5 to 6 points)
- moderate
- major
- significant
- damaging

High (7 to 10 points)
- major
- extreme
- serious
- critical

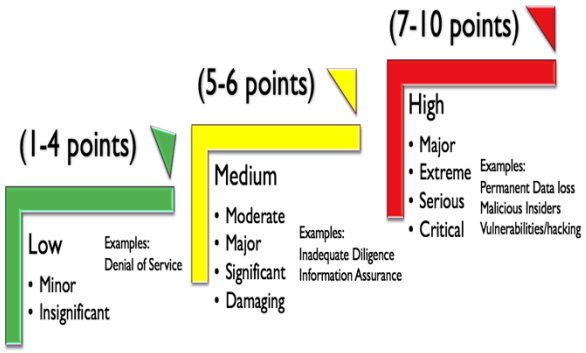

Figure 5: Risk Analysis (MITRE/Microsoft)

However, the main risks are: privacy concerns, security, accessibility, data ownership, assurance, and compliance. These are not all the risks that may present but these are six of the top risks with cloud computing.

3.1 Types of Risk, Risk Analysis, and Probable Solutions

3.1.1 Security One "of the top concerns of cloud computing due to data storage" is security (El-Booz 1). There are already measures in place to protect the security of data that may be stored in a cloud such as an application that may determine if information may be tampered with in a cloud. However, this may not be enough to ensure that it does not get tampered. This presents a high risk which is serious according to the risk analysis table in Figure 5.

Booz recommends stronger encryption methods pass the initial password authenticity such as a double encryption key such as two-step verification. Two-step verification could allow for the less likeliness for hack-ability because there would have to get past the two wall tiered protection system to have open access to the cloud.

3.1.2 Data Integrity and Privacy Concerns The integrity of data and privacy is another high concerned risk that companies take into consideration when using cloud computing. Since the cloud is a service that is built by a third party vendor, the data that is being stored on the cloud is accessible by these third party vendors. A company may be selective over the data that they disclose because of the sensitivity of classification tier of accessibility of this data may be a high classification. This type of risk is a high risk in according with Figure 5. This is a high risk on the risk analysis because it could potentially allow for malicious acts of intrusion on a cloud system. The other reason for this being such a high risk is due to the amount of measures that may need to be taken to prevent this from occurring which I cover in the next paragraph with a probable solution.

A probable solution could be to use more than one agency for handling high sensitive classified data. An agency could use an in-between software or agency to proof that information before uploading that information to the cloud. They could also grant clearance to the cloud service to give a single individual accessibility to their classified information by granting them a high tier level security clearance to handle sensitive information. Although this still presents an issue of maintaining that information, the only way to ensure their data is not compromised is to not upload high sensitive data to an outsourced cloud.

3.1.2 Accessibility With cloud computing becoming more popular with usage, an important feature but also yet still a risk is accessibility. Accessibility can be defined as the ease of access to a cloud service or the information on the cloud service. Accessibility is a feature of cloud computing services but it is also a risk. The risks that present with using a cloud service for storage of data or the running of applications could present an issue if the cloud service underwent a failure in the system meaning that the cloud service had technical difficulties which could present a blackout. If there was a blackout on a cloud service, a company would not have access to their data. Although this is highly unlikely to happen because the cloud service has a designated team of individuals monitoring the cloud's performance, it is always the risk of this happening and a company would have to have a contingency plan in place to access or recover their data. This type of risk is a low ended risk because of the less likelihood of this occurring as well as it is minor.

In regards to the loss of data, if a consumer decided to leave a cloud computing service, they will not have access to their data that they have stored on the cloud service unless they have this information stored in another location which would defeat the purpose of the usage of the cloud. The loss of data would cause a huge disadvantage to the user of the cloud service and maybe even present a larger battle over ownership of the data being stored on the cloud service.

Accessibility can be both a low risk and a high risk. The reason is can be defined between two risk levels is because of the denial of service and the loss of data aspect. The denial of service means a person is locked out of their cloud service which could have multiple reasons such a forgotten password or not having the specific clearance levels to gain access to the cloud which is low risk because it is not at the fault of the cloud service provider that the person did not have the diligence to remember their password nor to give them the specific clearance level because that is at the responsibility of the client. However, the loss of data is definitely a high risk because that is the sole responsibility of the cloud service provider on different cloud service deployments and models. If the heightened risk does happen, the cloud service provider should have some type of plan in place to protect their clients which I provide a probable solution in the next paragraph which could potentially lower the risk level of this occurring.

A probable solution would be to have a contingency plan in place to store this information in an alter location besides just a cloud service. They could also use a hybrid cloud system which would reduce the likelihood of downtown when a blackout occurs. Another solution to the risk of accessibility to data if a company decided to discontinue their use of a particular cloud service would be to draft up a user agreement policy which would cover the distribution of data at the end of the agreement. They would be legally bound to return the information that they were storing for a company but not responsible for the format for which the data is delivered.

3.1.4 Assurance Cloud computing has security and privacy plans in place to help minimize the risk of losing the integrity of their data. However, the assurance that a cloud service cannot be hacked, compromised, or the risk of data loss is where the terminology assurance comes into place. Assurance is the responsibility of the cloud service by the use of auditors.

Assurance brings a medium risk analysis in accordance to Figure 5 on the dealings of risk analysis. The reason that this is a medium risk instead of a low risk analysis is because the responsibility of assurance rests on the auditors but the risk could be exposed by the clients of the cloud. The organizations or consumers using the cloud should not have to worry about the types of information that they put out into the cloud but if they put sensitive or classified data into their cloud and it is hacked; that would potentially expose them to a medium level of risk. The reason that this is a medium instead of a high risk is because the team of auditors continuously monitor this risk and their information which means that they can potentially catch an incident before it occurs and becomes a high level risk problem.

As more data is stored on a cloud service, the cloud will become more susceptible to the risks of hackers, data loss, and even crashing the cloud. The auditors have the responsibility to ensure that these risks do not heighten the risk of a low level assurance plan. The assurance plan of a specific cloud should encompass that "data [is] being correctly stored and maintained, that is, the user should be equipped with security means so that he

can make continuous correctness assurance (to enforce cloud storage service-level agreement) of his stored data even without the existence of local copies" (El-Booz 5-6). This is important to protect the data that the user is storing on the cloud. In addition to the user and the cloud service has a service-level agreement which sets the expectation of what performance should be provided from the cloud service provider.

Since auditors that have the task of cloud auditing do not have an easy task to accomplish due to the concept that innovation of cloud computing is so fairly new which makes the risk greater for security and assurance. David Chou reports that "[I]n order to conduct a complete audit process, these technological drawbacks need to be discovered and published" so that it "allows Information auditors to find the right areas to examine; therefore, cloud computing's audit effectiveness can be achieved rapidly" (Chou, 76). He could not be more correct on his information because this would be a great solution to the problem that auditors have at hand with the task of assurance the security of data that his stored in the cloud. The changes with attempting to put more plans in place at the level of the cloud service presents a great solution but yet another problem which is data ownership, governance, and controls of the information that they are assuring is safe within the cloud service that they provide to a consumer.

3.1.5 Data Ownership/Governance/Control Data that is stored on a cloud service is input by a company but managed by a cloud service. The originality of the data cannot be disputed but yet the true ownership, governance, and controllability can be argued over with retrospect to data management which is a low but yet high risk topic in cloud computing. It is such a complex risk because as cloud computing continues to evolve, so do the rules and regulations that govern ownership of data. Data ownership can be broken down into copyright, confidentiality, and contract.

Copyright is a term that means "is a form of protection provided by the laws of the United States (title 17, U.S.Code) to the authors of "original works of authorship," including literary, dramatic, musical, artistic, and certain other intellectual works" which is "to both published and unpublished works". Most would think that any documents or applications that were drafted for a cloud service would be copyrighted to the author but this assumption is not always truthful in the case because the cloud service has accessible rights to store that information onto their cloud service. The way to determine who owns the rights to the information is to determine the type of information that it is being contested for copyright ownership then to determine the authenticity of where that was originally published.

Confidentiality can partner with contract when determining ownership. Confidentiality is a tier of access or privacy tier for classification of who can have access to certain information. The reason why this can be partnered with an agreement is because the agreement can legally declare ownership and determine if the data is confidential or bound by a contractual agreement as to the client's ownership or the cloud service's ownership.

The downfall to all three of these ownership categories is misclassification, ambiguity in the laws that are continuously changing for technical law, or for the lack thereof laws that set precedence over ownership of the data that is in the cloud. Copyrights have special technical levels and patents that have to be applied for before sole ownership can be declared. There are so many laws that governs the various aspects of the legal and regulatory status of cloud computing but yet the laws do not seem to be able to stay ahead of the pre-destined future of cloud computing. Cloud computing is evolving way faster than the laws can even be established for governing the platforms.

The three of these issues are all level tiered for the medium level with 5 to 6 points. The reason that this is a medium level risk on the risk analysis table is because "cloud computing is like the Wild West of the computing industry" meaning that the laws are being introduced as we discover the areas of weakened governances or that the risks are being exposed every day and also changing so rapidly. There is not one specific agency that actually governs the area of cloud computing which could be attested to the uniqueness and newness of this industry. In the next paragraph, I introduce a far fetch idea that could be a futuristic probable solution to the risk at hand when dealing with the retrospect of data ownership, governance, and control in cloud computing.

A probable solution to the issue would be to declare a specialty for cyber law that takes a special interest in cloud computing. Also, because cloud computing law is so rare and seems to be a scarce topic, it should be taught in the field of computer science so that they may take an interest in defending their rights as developing the vast field of cloud computing.

3.1.6 Compliance Compliance deals with legal abilities which is a high "importance of risk management in cloud computing is a consequence of the need to support various parties involved in making informed decisions regarding contractual agreements" (Djemame 265). Briefly earlier there was an introduction to issue of legal issues when dealing with cloud computing, the greatest issue is one of the highest operating risk of using cloud computing. Compliance is not just relevant to the actual implementation of cloud computing dealing with risks but also the unforeseen legal risks when using cloud computing.

There is not a legal document that can cover every aspect of legal responsibility with cloud computing. The rules and regulations are different in every country, continent, and even within various companies. A compliance agreement must be carefully reviewed when dealing with cloud computing because the data that is being stored on the cloud service could potentially be stored anywhere since in many cases it is stored in more than just one location meaning the physical location of the server could be in any region of the world.

Compliance regulators are not always considered when drafting agreements and many times companies do not read the fine print putting themselves into jeopardy of being incompliant to their own agreements or needing to withdraw from a cloud service due to the technological changes that the cloud service has had to make in an attempt to stay ahead of the curb with protecting their data.

Compliance agreements should be drafted with the user's needs taken into strong consideration. The compliance agreement is in place to protect the cloud computing service as well as the consumer of the cloud service. Arbitrarily, this agreement needs

to be reviewed multiple times and may even need to be revised through many meetings with lawyers or legal advisors which is a probable solution to ensuring that the legal community is exposed to the needs of cloud computing in a legal sense.

Cloud Computing Risks
Security
Service attacks by hackers Systematic Encryption too weak Authentication failures Vulnerable platforms
Data Integrity & Privacy Concerns
More robust disaster recovery plans reduce risk Hackers gaining cloud access Releasing copied/stolen data Cross-pollination of data Failure to coordinate cloud and local applications
Accessibility
Violating government or industry privacy regulations Inaccessibility access to the cloud Denial of service attacks Increased access risk for mission critical systems Leaving portals open
Assurance/Compliance **Data Ownership/Governance/Control**
Intellectual Property Issues Unfamiliar of compliances or regulations for data Multitudes amount of information or applications Arbitrary agreements outdated contractually
Big Data Risks
Fail to meet user requirements due to inability to process data Inappropriate use of analytical methods Applications that adversely affect interested parties Uncertainty regarding who owns customer information Addressing the wrong problem Focusing on the near domain and ignoring the real problem Mischaracterizing data resulting in privacy violations Mischaracterizing data resulting poor decisions Disenfranchising groups by ignoring theory and over-relying on data

Figure 6: Summarizes cloud computing & big data risks

In Figure 6, it shows that many of the risks in cloud computing are also risks of big data as well but the use of big data can lower the vast amount of risks that cloud computing alone presents.

4 Cloud Preservative

There are many different cloud service agencies that offer different types of clouds. Each of these cloud models have different aspects that may entice a company to use their services more than any other competitor cloud service. Companies must outweigh their options that they are presented with from a specific cloud service before deciding that this particular cloud service is the best fit service for them.

4.1 Examples of Risk Management Models in Realistic Companies/Consumers

4.1.1 Azure is a Microsoft based public cloud platform that has many different that is a pay-as-you go services available for companies to choose from to build an infrastructure for a cloud service that best fits the needs of their company. Azure is used by many companies such as The Hershey Company, March of Dimes, UBER, and many other companies who have entrusted their information to the Azure services. Azure has changed the model makeup for cloud computing services because it is so versatile in the corporate industries. However, there are some risks that have been uncovered with the use of Azure.

In the medical field or the field of dealing with patient information, there are standards that must be followed such as Health Insurance Portability and Accountability Act (HIPPA) which means that this information must be secure and meet the compliance standards that are set forth by HIPPA. According to Azure's released publication information, it is possible to meet the set standards that HIPPA has even while using their cloud services. However, it is the responsibility of the client to "have their own compliance mechanisms, policies, and procedures in place to ensure they do not use Azure in a way that violates HIPAA and HITECH Act requirements" meaning that the customer "should independently verify with their own legal counsel that their implementation meets all HIPAA and HITECH Act" (Microsoft Azure HIPAA/HITECH Act Implementation Guidance 3). The compliance capability is great but it presents great risks to companies such a March of Dimes who must consult their own legal counsels before ensuring that the data that they want to share with the cloud service is safe and in compliance with another federal mandate to protect their patients.

Azure also has a great hybrid network which meets the abilities to having a risk of blackout time on their services. "Azure offers a number of features intended to minimize downtime and loss of data" by offering a service called "Azure Storage" which "stores multiple copies of data on different fault domains, and, by default, will replicate data to a backup data center (the geographic replication feature can be turned off if desired)" (Microsoft Azure HIPAA/HITECH Act Implementation Guidance 4). Although this conquers a potential risk of downtime or loss of data the downfall to this risk management model that it is the responsibility of the customer to assess the information and to complete the additionally needed "backups of Customer Data, storing backups of Customer Data off the platform, deploying redundant compute instances within and across data centers, or backing up state within a virtual portal" (Microsoft Azure

HIPAA/HITECH Act Implementation Guidance 4). This could still present a shortfall in their risk management model because if a company like The Hershey Company or UBER forgets to make the backup of information then they have lost all the data that they have created if the system has a faulty glitch.

4.1.2 Apple has never been far behind the curb with their development of a cloud service for consumers called iCloud. The iCloud service is a paid subscription service that allows customers using iOS, OS, or PC devices to save information such as photographs, music, documents, contacts, calendars, and so much more. Just recently with the iOS 10 and Mac Sierra updates, Apple gave the ability of collaboration across document creation which highlights the importance of this service transforming from a consumer only service to a more business oriented approach. The future for iCloud is endless because it could be used by individuals, businesses, and even in the world of education. There is a slight risk at hand when using the iCloud service because no one truly knows where their data is being stored. Apple has over 782 million cloud users as of earlier this year which was revealed by Eddy Cue and Craig Federighi during a podcast interview with John Gruber on The Talk Show on Episode 146. Their release of their numbers came on the release of public beta testing for iOS 10 which changed the functions of iCloud and word processing through their platform of Pages and Keynote with a collaborative feature allowing for changes to documents that are saved in iCloud Drive which is application that allows the access of data, photos, documents, and so forth for the purpose of storing or editing.

The benefit to iCloud is that the documents that you edit are changed in live time on the iCloud Drive if you save them on the iCloud Drive. The downfall to this is that if you make any changes on the iCloud Drive then the changes are made across every device that you are using that accesses that particular iCloud account or iCloud Drive. The accessibility feature can be advantage or a disadvantage depending on the user's purpose for using the particular cloud system. The advantages are that you do not have to make the changes in multiple different interfaces but the disadvantage could be that you want to have multiple different versions of the information that you are editing. The collaborative feature could also be a downfall and cause the risk of the loss of data because it is accessible by multiple people and they have the ability to make changes based on the restrictions that the creator allots them with.

4.1.3 Google is ahead of Apple with their cloud service that they offer. They have the same interface for the ability for their consumers but they have a special service to offer for Google cloud services at work. They also have a feature with their ability to conference on their Hangouts application to have video conferencing for collaborations on projects where they can physically see the project that they are working on actively and connect with those that are given access to the hangout session and to the project that they are working on.

Their security levels are beyond safe with their guarantee of 99 percent of zero shutdowns. Google publicizes on their website that "Google Drive for work includes dozens of critical security features specifically designed to keep your data safe, secure and in your control" because Google believes that "your data belongs to you, and our tools enable you to control it, including who you share it with and how you share it" (Google at Work). The encryption model has many security features that protects a user's data online and on their devices which is similar to Apple's interface but yet even more additive with their support teams. They also offer phone and email support 24 hours, 7 days a week with is more than Apple and Azure's services which cost more than Google's cloud services. Google is able to offer more services at a low end cost but offer more features that deal with security and the assurance of the safety of the client's information.

5 Conclusion

Cloud computing has changed the way of computing with its affordability, flexibility, and accessibility. Although there are risks that present with cloud computing, they can be managed with the proper planning in place. Companies are researching and gaining an understanding of cloud computing. With the emphasis to integrate cloud computing in the age of technology, cloud computing is only going to continue to advance in its abilities and features. The advancements in cloud computing will continue to transform the age of technology. The advancements are limitless to the innovations that are to come in the future of cloud computing because the cloud is here to stay. Companies are partaking in the advancements in cloud computing because they all know that it is the way of the future of technology and the high demand of the industry because of its ease, flexibility, and yet even though there are risks in using cloud computing they can be managed with the proper risk management models in place by companies and the cloud service company.

Risks will always be an issue however by the implementation of risk management we can minimalize the heighten risk or the impact that the companies may endure in the use of cloud computing. As cloud computing evolves, the risk will arise faster than we can detect the risk. A solution to the future of cloud computing and risk management is the implementation of big data as a methodology to improve their predictive ability to catch the risks in real-time motion to make better evidentiary decisions and to save a significant amount of money with risk management.

References

[1] Alosaimi, R., & Alnuem, M. (2016). Risk management framework for cloud computing: A critical review. International Journal of Computer Science and Information Technology, 8(4), 1-11. doi:10.5121/ijcsit.2016.8401

[2] Barabas, J. (n.d.). IaaS PaaS SaaS - Cloud Service Models. Retrieved October 15, 2016, from https://www.ibm.com/cloud-computing/iaas-paas-saas

[3] Chou, D. C. (2015). Cloud computing: A value creation model. *Computer Standards & Interfaces, 38*, 72-77. doi:10.1016/j.csi.2014.10.001

[4] Dixon, M. (2013). Demystifying 'the cloud'. Ottawa: The Summit Group.

[5] Djemame, K., Armstrong, D., Guitart, J., & Macias, M. (2016). A risk assessment framework for cloud computing. IEEE Transactions

on Cloud Computing, 4(3), 265-278. doi:10.1109/TCC.2014.2344653

[6] El-Booz, S. A., Attiya, G., & El-Fishawy, N. (2016). A secure cloud storage system combining time-based one-time password and automatic blocker protocol. EURASIP Journal on Information Security, 2016(1), 1-13. doi:10.1186/s13635-016-0037-0

[7] Take Google Drive to Work. (n.d.). Retrieved from https://gsuite.google.com/driveforwork/?utm_medium=et&utm_source=aboutdrive&utm_campaign=en&utm_content=consnav

[8] Re: '"They Might Be Giants" With a Spanish Accent', With Special Guests Eddy Cue and Craig Federighi [Audio blog comment]. (2016, February 12). Retrieved October 18, 2016, from http://daringfireball.net/thetalkshow/2016/02/12/ep-146

[9] Mell, P., & Grance, T. (2010). The NIST definition of cloud computing. New York: Association for Computing Machinery.

[10] Neumann, P. (2014). Risks and myths of cloud computing and cloud storage ACM. doi:10.1145/2661049