A REVIEW ON SURVEY ON CLOUD COMPUTING

Ankush Narkhede[1] and *Asutosh Kumar Pandey[2]
[1]*Oriental University, Indore (India)*
[2]*Rishiraj Institute of Technology, Indore*
*Author for Correspondence

ABSTRACT
To maintain the software based system cost more to setting up the infrastructure, network, technical team and related software, also Associate/ Attorney spend more time to maintain the information and it should be secure. Small, medium and independent Law Practice Firms need a full Law Practice system to be up and running quickly without having to invest time and cost in setting up the infrastructure, network and related software. The Practice League Law Practice Solution is Ready-To-Use cloud based Pay-As-You-Go Law Practice software which will help you greatly improve your effectiveness, efficiency and productivity. The proposal is based on the concepts of cloud computing so the information sharing and high-end processing is available in the cloud.

INTRODUCTION
Law Practice Solution brings you all the tools you need to manage your Law Business with Easy-To-Use world class features like Timesheet / Expense Entry, Resource Management, Task Tracking / Court Date Reminders, Calendaring, Contact / Client Management, Conflict Search & Matter Management, Invoicing and Payment Tracking, Documents and Notes, Dashboards, Reports and Analytics. To manage all above task required Maintenance (Stocker, 2011).Other software as well as hardware cost is very high. If your businesses grow you need to improve your infrastructure like disk space, higher processor, new software's etc. It will cost you economically. If, business slow down the investment you have done would be waste. It will always be better if such firm has Pay-As-You-Go Law Practice software which will help you greatly improve your effectiveness, efficiency and productivity (Pearson, 2009). Cloud computing has been gaining industry momentum lately. Its promise to deliver cost effective solution over cloud is so fascinating that many industries have started investing in cloud computing instead of having to own and manage the IT infrastructure which includes both hardware and software. One industry which is yet to fully understand the implications, both positive as well as negative, of cloud computing is Legal firm (Zeljko, 2010). This paper focuses on how cloud computing can be leveraged upon by the Legal Firm to expand their businesses, to stay competent in a cost effective way, to reach to their customer in shortest possible time, to focus on their niche area of operation instead of focusing on managing IT infrastructure etc. Cloud computing is a term used to refer to the services offered on demand over internet. These services include software, platforms to develop new software/tools, and infrastructure such as servers and data center space (Aoying, 2010). These services are offered by sharing resources among many consumers.

1. Motivation
1.1 A Problem with Traditional System
1.1.1. Lack of Uniform Standards for Data Sharing: To share the information between Associates, Attorney, Client, Contacts information should be in standard format and complete information. Because of lack of data sharing will effect on Billing. One of the greatest challenges faced by many firm is planning and implementing data integration and establishing an appropriate technology infrastructure. It is trouble to accessing and managing multiple information systems. The information they are able to access is often redundant and the high volume overwhelming. At the local level, relevant data is entered into multiple computer systems, which very often cannot share information (Hocenski, 2010).

Review Article

1.1.2. High Cost for Independent Construction: To maintain separate database for each Associates / Attorney will cost more as well as should be uniform. Data integrity, security cost increases and difficult to share information (Iacono, 2010).

1.1.3. Difficult to Management, Upgrades and Maintenance: To manage the independent system or for firm need strong infrastructure like Server, Disk, Network, Security, Database and Software's. These are the few things listed but there are some more direct - indirect component are available. To manage this infrastructure need technically sound manpower. To upgrade the infrastructure like update the new software, hardware require extra cost. Maintenance activities into four classes:

a.   Adaptive dealing with changes and adapting in the software environment
b.   Perfective accommodating with new or changed user requirements which concern functional enhancements to the software
c.   Corrective dealing with errors found and fixing it
d.   Preventive concerns activities aiming on increasing software maintainability and prevent problems in the future

Software maintenance is important because it consumes a large part of the overall lifecycle costs and also the inability to change software quickly and reliably means that business opportunities are lost (LING 2010).

2. Related Works

Cloud computing is going from trend to law firm staple. One of the hottest sectors of information technology is taking the legal community by storm. Cloud computing appears to be making inroads in the legal profession, particularly with solo practitioners and small law firms because they can benefit from a mature IT infrastructure including essential legal applications without a major investment. Concerns surrounding confidentiality, privacy, security, business continuity, disaster recovery and jurisdictional issues continue to be hurdles that make law firms pause before taking the plunge. For many lawyers, an overriding concern is control over the data. Some legal observers contend that when data is placed in the cloud, law practitioners lose or at the very least appear to lose control over client and firm data as it is ensconced in the hands of a third party technology services vendor (Ling, 2010).

2.1. Cloud Computing

Like all IT developments, cloud systems present a new set of risks and concerns. This advice note is intended to highlight important cloud computing issues to help you decide if a cloud system is right for you and your firm. Most of the Law firms have been relying traditionally on mainframe systems and paper based forms. They have invested heavily in complex and outdated legacy systems. Making them adopt new technologies will require huge outlay. Cloud computing can be of great benefit to Legal in this scenario. According to some estimates, around 85% of IT budget of an insurer goes in maintaining the legacy systems. Only a meager portion is left for doing some innovation around product, distribution, and customer service. Cloud computing can be used to outsource entire IT business of an insurer, not just people and machines. This will save Law Firms money that is normally spent on maintaining the legacy systems. This money can be used for product and service innovation. Many cloud computing vendors provide dedicated date centers to their customers. Law Firms can have all their data stored in the data centers across the globe at various locations of the vendor. They don't need to worry about the disaster recovery as it will be handled by the vendor. Cloud computing provides the small Legal Cloud a very cost effective way of entering and surviving the market. All services they need to operate in today's world can be delivered over the cloud. Cloud computing is a paradigm shift from the client server model. Cloud computing allows users in an organization to access shared resources, applications, servers, computers, etc. over the internet on demand from a service provider. The provider can calculate the time bound resource utilization as per the service level agreement and bill the organization based on the usage. This is just like using the electricity from your provider and paying the electric bill based on the usage as captured by the meter. This will help the companies to optimize their utilization of IT assets thereby

Review Article

cutting down on any unnecessary IT costs. So this way organization can leverage on the cloud computing model to reduce the capital expenditure on IT (Nishchal, 2010).

3. A Cloud key Features

1.	Cloud computing technology provides a more flexible and agile infrastructure at a low cost. It is important considering the fact that organizations have to often deal with business re-org, market fluctuations, resource resizing etc.

2.	Companies can significantly reduce their capital expenditure on IT by adapting to the cloud computing model. This can be achieved especially through utility based computing where the computing resources such as hardware, software, network bandwidth and other infrastructure components are rented from a third party service providers. So this way organization will have to only worry about the operational expenses from IT infrastructure standpoint. One other advantage of utility based computing is that IT skills required for maintaining the infrastructure will reduce drastically.

3.	Users can access the systems from anywhere in the world via internet regardless of where the infrastructure is located (third party service provider). All that is needed at the user end is a device that is internet enabled such as a computer, laptop or other handheld devices.

4.	Different companies can share the resources under a single cloud from a third party service provider. The benefit of doing so is as follows:

i)	Setting up a centralized infrastructure in a location where the cost of real estate and electricity is low.

ii)	Huge computing resource pool and a greater network bandwidth will increase peak load capacity.

iii)	Using virtualization technology for setting up the cloud infrastructure will allow new host systems to be added or the existing systems to be upgraded with additional computing resources such as processor, memory, storage etc

iv)	Easily without shutting down the systems thereby making the infrastructure extremely scalable.

v)	Optimized utilization of the systems that are often used only 5-10%.

5.	Cloud based application are easy to support and maintain as they are not installed on client machines. Any changes that are made to the application is available to the users instantly.

6.	Data is more secured due to centralized location of the infrastructure.

7.	Cloud computing resource usage can be measured and should be metered per client and application on a daily, weekly, monthly and yearly basis.

4. Understanding the Risks and Benefit

When moving to a cloud based system you should start by considering what you plan to use your cloud system for. If you plan to use it to provide a service or to store confidential client information you should consider how critical that service is to your business and the importance of access to, and security of, your client information given your duties to your clients and to regulators.Cloud computing is a new way of doing business that takes advantage of building efficiencies into the system that can scale out to provide services for multiple companies (Tang, 2009).

4.1. Cloud Computing Challenges

a.	Below are the few challenges that cloud computing currently faces when deployed on a large enterprise scale.

b.	Self-recovery on failure – When there is an application failure or network failure or data storage failure, the service provider should make sure that there will always be a backup running without major delays so that making the resource switch appear seamless to the user.

c.	Driven by Service Level Agreements– In cloud several instances of one application needs to be replicated on multiple servers if there is a demand and this is managed by service level agreements. So based on priorities, the lower level applications can be shut down or run at low priority/background, which is a challenge.

Review Article

d.   Multi-tenancy – With the cloud what will actually happen is multiple clients can be allowed to use the same hardware at the same time; but the client will not knowing about it and hence there is a possibility of causing conflicts of interest among customers.

e.   Service-oriented - Cloud permits one client to use numerous applications which could also be a challenge in terms of service on storage, information, license etc.

f.   Virtualized - Applications are not hardware specific; various programs may run on one machine using virtualization or many machines may run one program.

g.   Linearly scalable - Cloud should handle an increase in data processing linearly; if "n" times more users need a resource, the time to complete the request with "n" more resources should be roughly the same.

h.   Data management - Distribution, partitioning, security and synchronization of data is not that easy.

4.2. Cloud Computing Security Issues

There are seven identified issues that need to be addressed while switching to Cloud computing model. [10]

i.   Privileged user access - information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications first to test the water

ii.   Regulatory compliance - clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by 3rd party organizations that check levels of security and providers that don't

iii.   Data location - depending on contracts, some clients might never know what country or what jurisdiction their data is located

iv.   Data segregation - encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider.

v.   Recovery - every provider should have a disaster recovery protocol to protect user data

vi.   Investigative support - if a client suspects faulty activity from the provider, it may not have many legal ways pursue an investigation

vii.   Long-term viability - refers to the ability to retract a contract and all data if the current provider is bought out by another firm.

Given that not all of the above need to be improved depending on the application at hand, it is still paramount that consensus is reached on the issues regarding standardization.

4.3. Security Benefits

The following sections looks into addressing concepts such as centralized data, incident response or logging. Centralized Data refers to the approach of placing all eggs in one basket. It might be dangerous to think that if the cloud goes down, so does the service they provide, but at the same time, it is easier to monitor. Storing data in the cloud voids many issues related to losing laptops or flash drives, which has been the most common way of losing data for large enterprises or government organizations. The laptop would only store a small cache to interface with the thin client, but the authentication is done through the network, in the cloud. In addition to this, when a laptop is known to be stolen, administrators can block its attempted access based on its identifier or MAC address. Moreover, it is easier and cheaper to store data encrypted in the cloud that to perform disk encryption on every piece of hardware or backup tape.Password Assurance Testing is a service that can be used to harness the computational power of the cloud in attempts to break into a company's system by guessing passwords. This approach minimizes resources and time spent on the client side. Logging benefits come from the idea that the client need not worry about storage space for log files and enjoys a faster way of searching through them. Moreover, it allows for a convenient way to observe which user accessed certain resources at any given time.Improvement of Secure Software refer to several aspects in the development lifecycle of a product.

Review Article

Initially, a company that is thinking of placing their application in the cloud knows that the cost of running the application are directly proportional with the number of processing cycles, thus creating an incentive for an optimal implementation. Secondly, it becomes easier to monitor the effects of various security policies implemented in the software, without the overhead of traditional switching environments from development to production or to testing. Creating a new environment simply means creating a clone of the extant one. Thirdly, software run behind an architecture that is built for secure transactions at a physical, data link, network and transport layer, making it easier to design the application without the outspoken need of a security software engineer.

5. Cloud Provider

Cloud computing involves moving your data and your client's data into the possession of your provider and its data centre. This raises a number of issues regarding data storage, treatment and control (Ghemawat, 2010).

5.1. Ownership of Data Stored With Your Cloud Provider: It is important that your cloud provider gives assurance that the information will be treated as confidential and not used or disclosed to third parties. You should retain full ownership, in terms of intellectual property, in relation to the data that it is stored on your provider's system. You should have an explicit right to get your data back on demand.You will also want to know your provider's policies and procedures on data deletion on termination of your relationship.

5.2. Security of Data Centre

In addition to ascertaining the location of your data, it is fundamental that your contract with your provider contains appropriate assurances as to the technical specifications and security of the data centre storing your data. The data centre should:

a.   Be in a safe facility with security monitoring;

b.   Have strictly controlled access to personnel that have been security vetted;

c.   Have an effective fire detection and fire suppression system;

d.   Have air conditioning to prevent equipment overheating;

e.   Have backup generators to sustain long power outages; and

f.   Have a backup of everything so there is no single point of failure.

Furthermore, your cloud provider should undertake to audit the facilities of its data centre at least annually.

5.3. Back Up

You should carefully examine the SLA for the frequency the cloud provider will back up your data to a separate site. You should be aware of any period of time where your data will not be backed up and will therefore be lost should the cloud system fail.Your provider may recommend independent backup of data stored in their cloud. This will negate some of the cost benefits associated with cloud computing so it may be preferable for data to be periodically returned to you on disk. If you do hold a backup locally, you should check regularly that it is working correctly by creating a test file, deleting it and restoring it from your backup.

5.4. Portability of Data

You should ensure that your provider offers a practical method of moving your data back to your premises or to another provider on demand. There should be a clear procedure that guarantees that your data will be returned timorously in a usable format. This process should be tested with a dummy set of data on a regular basis as part of your ongoing disaster recovery planning. Data should be portable even in the event of a failure of your cloud provider or their data centre to ensure minimal disruption to your

Review Article

business. A possible safeguard is to obtain the software object code and to require your provider to place a copy of the software source code with a recognized third party escrow provider. This will allow another cloud provider to assist with data recovery and reuse.

5.5. Audit and Independent Certification

You should ascertain your provider's willingness to be subjected to audits by independent security certification authorities. Indeed, some providers advertise certification summaries on their data quality and data security. A number of industry self-certification schemes exist but it is not yet clear which represent a true gold standard so they should be treated with appropriate care when selecting cloud providers who use them to credential their services.It is recommended best practice that the cloud provider complies with: (Kresimir and Zeljko, 2010)

i.   ISO 9001 (quality management) standard.
ii.   ISO 27001:2005 (security management) standard.
iii.   ISAE3402 (assurance reporting) standard.
iv.   BS 27999 (business continuity management) standard.
v.   The requirements of a Tier 3 data centre set out in the Telecommunications Industry Association's TIA 942 standard

CONCLUSION

Without a doubt, cloud computing is truly a revolutionary concept for many business organizations. Because of the technology's ease of adoption, significantly lower maintenance costs, and greater workflow efficiency, there is no doubt that cloud computing will gain widespread popularity going forward. For managers dealing with the growing demand for IT in their respective organizations, cloud computing presents itself as an all-in-one solution, being able to satisfy the growing IT needs while, at the same time, reducing energy usage all at an affordable price. Every platform has a certain lifecycle after which its usability decreases and a new platform emerges to supplant the old one. Mainframe and minicomputers were supplanted by the personal computers and servers. Cloud computing is emerging as a new platform for businesses to operate their IT department with full scalability at a lower cost instead of owning and managing personal computers and servers. Insurance businesses, though uncertain as of now about the cloud vendors' capability to maintain integrity and security of their data, would eventually find it profitable to operate with cloud vendors. Cloud computing is still in its infancy but looking at the trend and prospect of it, it is sure that cloud will be playing a significant role to insurance businesses in future.

REFERENCES

Dean and Ghemawat S (2010). MapRduce: Simplified data processing large clusters, communication of the ACM **51** 107-113.

Grobauer B, Walloschek T and Stocker E (2011). Understanding Cloud Computing Vulnerabilities, IEEE **9**(2) 50.

Jensen M, Schwenk J, Gruschka N and Iacono LL (2010). On technical security issues in cloud computing" IEEE International Conference on Cloud Computing, CLOUD '09 109.

Kresimir P and Zeljko H (2010). Cloud computing security issues and challenges, MIPRO 2010.

Mathur P and Nishchal N (2010). Cloud Computing: New Challenge to the Entire Computer Industry, Conference on Parallel, Distributed and Grid Computing **2**(1) 223.

Minqi Z, Rong Z, Wei X, Weining Q and Aoying Z (2010). Security and Privacy in Cloud Computing: A Survey Sixth international conference on Semantics Knowledge and Grid (SKG) **105** 1-3.

Pearson S (2009). Taking Account of Pri- vacy When Designing Cloud Comput- ing Services ICSE Workshop on Software Engineering Challenges of Cloud Computing 44.

Review Article

Popovic K and Hocenski Z (2010). Cloud computing security issues and challenge, Proceedings of the 33rd International Convention 344.

Tian LQ, NI Y and LING (2010). Evolution of user Behavior Trust in Cloud Computing International Conference on Computer Application and System Modeling **7** 567.

Yuefa D, Wu B, Yaqiang G, Zhang Q and Tang C (2009). Data Security Model for Cloud Computing, International Workshop on Information security and Applications (IWISA 2009).