Evaluating Cloud Computing for Futuristic Development

Sarah Shafqat
ShaheedZulfiqar Ali Bhutto Institute of Science and Technology (SZABIST), Islamabad, Pakistan

Muhammad Daud Awan, PhD.
Dean Computer Science, Preston University, Islamabad

QaisarJavaid
International Islamic University (IIU), Islamabad, Pakistan

ABSTRACT

Purpose of this research is to evaluate cloud computing to put the foundation of an Architectural Framework for Trusted Cloud Computing (AFTCC) that would enable businesses to cut their costs by outsourcing their processes on-demand by verifying the confidentiality and integrity of their data and computation. On going research will clearly outline the enhanced execution environment that guarantees confidential execution of guest virtual machines. Further more, current research would allow users of the cloud to attest and determine whether or not the service provided is secure before their virtual machines are launched into the system knowing the identity of every personnel involved in this environment. The architecture would provide virtual view of the processes in the network interface enabling user level access to high-speed communication devices; like, bio-metric devices to enable user level forensic identification system. Also, it would provide architecture for implementation of a system that would do meaningful interpretation of raw data, and informing rightly to the right people at the right time.

Current study mainly focuses on devising the Software Architecture for Trusted Cloud Computing. This research will outline the strengths and weaknesses identified in the literal work that has been done till now in Architectural Framework for Trusted Cloud Computing and its components and how they fit in. And will also identify the latest research and systems that are following it to some extent.

Key words

Cloud Computing, Identity Management, Architectural Framework, Trusted Cloud

1. INTRODUCTION

TO get an understanding of Trusted Cloud Computing and its Architecture there is a need to identify Cloud Computing and its subdivisions.

Cloud computing is the buzz of this era (Knorr & Gruman, infoworld.com). "It's become the phrase du jour," says Gartner, being a collective voice of his peers. In the recent years, cloud computing has gained attention of different stakeholders from IT and Computer Science; academicians, business organizations, institutions, etc. According to some selected vendors and analysts cloud computing is a latest form of utility computing: in actual a spread of unlimited *virtual servers* over the Internet. With the realization of IT needs and what it has to offer, cloud computing emerges as; a virtual infrastructure increasing space or capabilities on the fly with minimum investment for utilizing capacity, licensing new software or training new talent. Today, it is understood that IT has to plug into cloud-based services individually, and emerging are the cloud computing aggregators and integrators.

MSN, Google, Amazon etc. are the trends to follow.

Distinguishing cloud computing, Microsoft's Steve Balmer introduced it as the next frontier, to the group of CEOs gathered in his company's headquarters near Seattle (Ragnet, Xerox.com).

Similarly, Dr. Ajei Gopal (Ragnet, Xerox.com, p. 3), confirmed as cloud is there to change everything. He was heard saying at a company conference in Las Vegas, as a top executive with CA Technologies where there were thousands of people. "Instead of being a gigantic supplier of technology services to the business, the IT department becomes the manager of a dynamic supply chain of internal and external resources that deliversservices to the business and its internal and external clients."

Joe Tucci (Ragnet, Xerox.com, p. 3), the CEO of EMC Corp.,termed the impact of cloud computing as: "We're now going through what I believe is pretty much going to be the biggest wave in the history of information technology."

According to IDC's (Ragnet, Xerox.com, p. 3) forecast, they are expecting to raise $27 billion as net IT revenue by 2013 and 27 percent of it will be from cloud services.

"Cloud computing is a model for enabling 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 definition is given by National Institute of Standards and Technology (NIST) (Ragnet, Xerox.com, p. 3).

A more streamlined definition is offered by Wikipedia: "Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams…Cloud computing is Internet-based computing, whereby shared resources, software and information are provided to computers and other devices on-demand, like the electricity grid."(Wikipedia)

Power of Cloud is well understood by resulting new eBusiness model to be implemented in the Information Technology (IT) era (Shimba, 2010). It promises to shift limited internally managed resources of the organization to the space bought in the cloud and managed by cloud provider on the basis of pay per use. Organizations with huge parallel processing tasks would be handled speedily and their programs would scale to a virtual spread of unlimited servers, for example; using unlimited servers for an hour costs same as using single server for unlimited hours with over loading it. Cloud computing offers scalability plus on-demand supply of resources to the organization. The ability of elastic use of resources with minimum cost is a huge breakthrough in history. As there are many benefits portrayed by the adoption of cloud computing, sensing the need of different dynamics and attaining expertise in various domains is important for an organization. *Currently, there are no adequate guidelines of building trust over the cloud. Trust is a critical factor in cloud computing adoption. Security being the most significant challenge of cloud computing receives more mention.*

Large IT organizations have concerns like (Shields, searchcloudcomputing.com):

- "We can't ensure data security in a cloud service."
- "We can't ensure that we're meeting regulatory compliance in a cloud service."
- "We can't ensure inappropriate accesses are prevented in a cloud service."

Cloud Computing Domains realized as utility computingare:

1. Software-as-a-Service (SaaS)
2. Platform-as-a-Service (PaaS)
3. Infrastructure-as-a-Service (IaaS)
4. Web Services
5. Service Commerce Platforms
6. Internet Integration
7. Managed Service Providers (MSP)

Vision of Cloudis arealization of virtualization and automation as advances in computing architecture and technologies. As economy crawls, cloud computing is the most important technological trend of current time to speed it up as can be seen (Yachin, 2010).Being part of cloud computing, (i) the services are offered as applications over the Internet, and (ii) system software and hardware are available in the datacenters at the provider’s end (Armbrust et al.). The services offered over the internet are referred as *Software as a Service (SaaS),* like;gmail, hotmail, etc. The datacenters with variable space comprising of software and hardware is to be understood as*Cloud*.*PublicCloud* is when the general public uses cloud services (*UtilityComputing*) on some cost per use.When a business or an organization has its own internal datacenter and uses it as an Intranet then it is *PrivateCloud*. It is then understood that Private Clouds do not become part of Cloud Computing. To understand the infrastructure within cloud the focus should be on SaaS and Cloud Providers (Cloud users) and not onSaaS users.

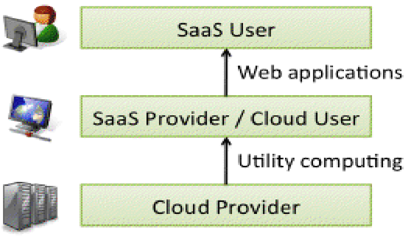

Figure 1: Simple flow of Cloud Computing Infrastructure (Source: RAD Lab, n.d.)

Companies moving in Cloud

Every major technology company tried putting themselves in Cloudsphere and 2010 was certainly an exciting year (Depena). Now, in 2011,Dell, CA, AT & T, CSC, Cisco, Microsoft, HP, IBM, Verizon, and Oracle amongst other strive to win the title –“Who Will Be the Future King of The Cloud?”

Here are some public and private Service and Platform Infrastructure clouds (Jennings, searchcloudcomputing.com):

Name	Source	Description
Azure CmdLets	MSDN Archive	Windows Azure Service Management CmdLets (API wrapper)
AzureWatch	Paraleap	Dynamic scalability and monitoring tool for Windows Azure
Chef	Opscode	Systems integration framework
CloudFormation	Amazon Web Services	Template-based provisioning tool for Amazon Web Services
CloudTest Pro	Soasta	Real-time Web performance monitoring and load testing
CloudWatch	Amazon Web Services	Monitoring and auto-scaling service for Amazon EC2
Fabric	C.V. Hansen & J.E. Forcier	Python library/command-line tool for deployment/sysadmin tasks
Ganglia	Ganglia	Scalable distributed monitoring system for clusters and grids
Kaavo IMOD	Kaavo	App/workload management for EC2, IBM, Rackspace, Terremark
ManageAxis	Cumulux	Dynamic scalability and monitoring tool for Windows Azure
Mcollective	Puppet Labs	Server orchestration/parallel job execution system framework
Nagios 2.0	Nagios Enterprises	Monitoring/alerting for servers, switches, applications and services
SCOM 2007	Microsoft	Windows Azure Management Pack for monitoring cloud resources
Puppet	Puppet Labs	Automated administrative engine for *nix systems
RightScale	RightScale	One of the first

		commercial cloud management platforms
RunDeck	DTOLabs/RunDeck	Automates ad-hoc and routine procedures in data centers/clouds
Skytap Cloud	Skytap	Cloud automation solutions for enterprises and software vendors

There are three new aspects in cloud computing, from resources point of view:

1. Fooling ourselves by believing in having infinite computing resources available on internet.

2. The cloud users are not committed for being up-front. Thus, encouraging small businesses to grow and hardware resources are utilized as per need.

3. Using computing resources for short time period on per payment basis.

2. BACKGROUND STUDY

Obstacles and Opportunities for Cloud Computing:

No.	Barriers	Prospects
1	Reaching everyone over the internet	Use Cloud Providers to infinity
2	Difficult to move data	Compatible Software with Standardized APIs; to enable surge or Hybrid Cloud Computing
3	Bottlenecks in data transferability	Higher Band width switches, FedExing disks
4	Security of Data and its ownership	Deploying Firewalls, encryption, VLANs
5	Virtual I/Os scalability	Enhanced Gang schedule VMs, VM support, and flash memory
6	Scaling Quickly	Inventing snapshots for conversations; auto-scaler that relies on ML
7	Scalable Storage	Inventing scalable store
8	Occurrence of threats in Large Distributed Systems	Distributed VMs supporting debugger
9	Licensed Software	Pay-as-per-use licenses
9	Taking responsibility of fraudulent activities	Providing reputation-guarding services like those for email

Trusted Cloud Computing gives emphasis on security, privacy, and authenticity of the data as well as user who is accessing particular service or information over the cloud.

Thus focus is on; Data confidentiality and Auditability, Performance Unpredictability, Data lock-in, Reputation Fate Sharing.

2.1 Securing the Cloud:

A new field being introduced is Information Protection and Control (IPC), in the security market, is focusing on complying with privacy law enforcement policies and protecting sensitive data. Security companies that pioneered the concept of Data Loss Prevention (DLP) took over the IPC market in the second half of this decade. Thus, for the prevention of unauthorized delivery of sensitive corporate information, there are solutions that are being designed.

Due to the growing complexity of IT environments, a centralized approach to IPC becomes less and less effective, and still there is need for more protection around multiple corners from where the sensitive information may leak.

Headed towards cloud computing,there is increasedcomplexity. Research reflects that security is cited as one of the most significant barriers to adopting the cloud. To a large extent, organizations fear to trust cloud providers for handling their sensitive information.

Encryption is the solution posed by IPC to take over this challenge,thus enabling data security at the root, rather securing unauthorized access at the exit points (e.g., email and Web channels, USB drives, and mobile storage devices).

Another trend in emerging cloud-related security is virtualization security. With such fast growth in Internet even basic security practices, like monitoring network activity; inspecting and filtering traffic and maintaining strictly separated security domains – gotneglected in the virtual environment.Traditional security solutions were slow enough to address security issues created by virtualization. As the virtual traffic does not touch the physical layer, it is unseen by physical network monitoring tools and is left unprotected by physical network security. There is an increased growth in the number of companies that are working on developing error-free virtualization security solutions.

Cloud services are rarely available for industry-specific requirements due to limitations of functionality and security. In industries like healthcare or in public sector strict regulations inhibit the broad adoption of cloud computing (Siemens, 2010).

Siemens IT Solutions and Services proposed a solution aiming at providing ‘community clouds’ to overcome these limitations. Community clouds are tailored with respect to shared needs of specific business community. The business processes are fully realized and at the same time keep security in focus by means of hybrid deployment models. For business-critical information and services the private cloud environment is made with a trusted outsourcing partner.

Different deployment models such as public and private clouds combine to form *Hybrid Cloud*. This model lets users deploy non business-critical services to the public cloud while keeping sensitive processes and data in their control.

Siemens IT Solutions and Services cooperate with leading platform vendors like Microsoft, Oracle, and VM-ware.

Managing the complexity in Sourcing (Siemens, 2010):

a) Complexity of choice

b) Complexity of management

c) Complexity of integration

a. Complexity of Choice:

Currently, cloud market is immature with ongoing acquisitions and mergers. Where there are new players coming in some startups are already backing out. It is not easy for customers to choose right provider from many potential ones. The database is being kept, by Siemens together with the Technische Universitat Munich, to provide an overview of the supplier market in cloud. Till March 2010, it was in beta version and already includes almost 2000 cloud services and over 800 service providers.

b. Complexity of management:

Cloud computing has introduced new ecosystem for IT deployment and service delivery. The SaaS providers engage subcontractors that deliver hosting services, infrastructure, or a cloud platform such as Microsoft Azure. Customers operate within different role of infrastructure provider, platform provider, or software provider. As the selective services are outsourced, high number of different cloud providers may have to be managed. This results in overhead cost for managing different processes like; finance, performance monitoring, controlling, and contract management.

c. Complexity of integration:

Diverse applications and services residing with different providers over the cloud have to be integrated with availability of good technical and system integration skills. Integration becomes complicated due to lack of agreed standards in cloud computing. There are different platforms each specifically programmed using different data access layers and development tools.

Hybrid models are preferred for regulating security, even though it is still a challenge. Security policies need to be enforced at central government level, for identity and access management.

Cloud computing offers higher scalability and lower cost to service providers, infrastructure hosting companies, and large enterprises. With experience and teaming up with leading vendors, Intel helps customers design, deploy, and manage a cloud infrastructure through Intel Cloud Builder (Intel).

Cloud Computing is a solution for Starbucks and Citigroup for analyzing data, providing applications to employees, and running special projects (Mojica et al., Accenture). To deliver dynamic content in multiple formats through variety of devices, and considering public taste, media giants are reported to be working on cloud-like services, i.e.; Facebook, Twitter, etc.

As more IT and telecom providers like; Accenture, Microsoft, Fujitsu, KDDI, China mobile, and SingTel join with cloud pioneers like; Google, Amazon, and SalesForce.com, it will give way to introduce more cloud services and more depth into the area(Mojica et al., Accenture).

Cloud will highly affect present computing dimensions. In futuristic perspective, there are many questions facing retailers regarding adoption of cloud (Mojica et al., Accenture) – concerns remain about security of customer data, feared loss of control of business-critical applications, and the reliability of cloud technology for retailers' critical customer facing systems. Where cloud computing has great promises and capabilities it is hard to evaluate long term costs and risks associated with it. It is still early to determine its exceptionally broad potential uses.

Accenture (Mojica et al., Accenture)identifies six key questions that retailers should ask about cloud computing:

1. How is cloud computing defined and work?
2. How cloud benefits my company?
3. How cloud computing can help address the specific challenge any company faces?
4. Is it economical to be on cloud?
5. How will a company operate in cloud in the future?
6. How cloud assures security and data privacy?

As the accelerated adoption of cloud computing being confirmed, the most surprising element is the adoption of cloud by financial services sector (Pandit, 2010). Also, the assumption that cloud is cheaper is being tested.

Walk-in scenario Use Case for utilizing this framework:

1. Consumer logs in to the cloud portal by verifying his credentials
2. Based on consumer service entitlement type the matching set of services are identified and presented for use
3. The end user confirms the service for consumption and triggers a service request
4. Resources get reserved for service specified.
5. The relevant domains for computation, network, and storage are configured, with security request and service delivery under service-level agreements (SLAs).

Hence, this is a framework for a working structure of cloud (Cisco).

2.2 Trust in Cloud Data Center:

Trust in cloud data center is based on several core concepts:

- Security: Factors include; data theft, eves dropping, user authentication, and resource access control, encryption, and incident detection.
- Control: Control comes when enterprise knows how to directly manage, where, and by whom data and applications are deployed and used.
- Compliance and Service-Level Management: The concept refers to contracting and enforcement of Service-Level Agreements(SLA)between variety of parties, and conformance with regulatory, legal, and general industry standards.

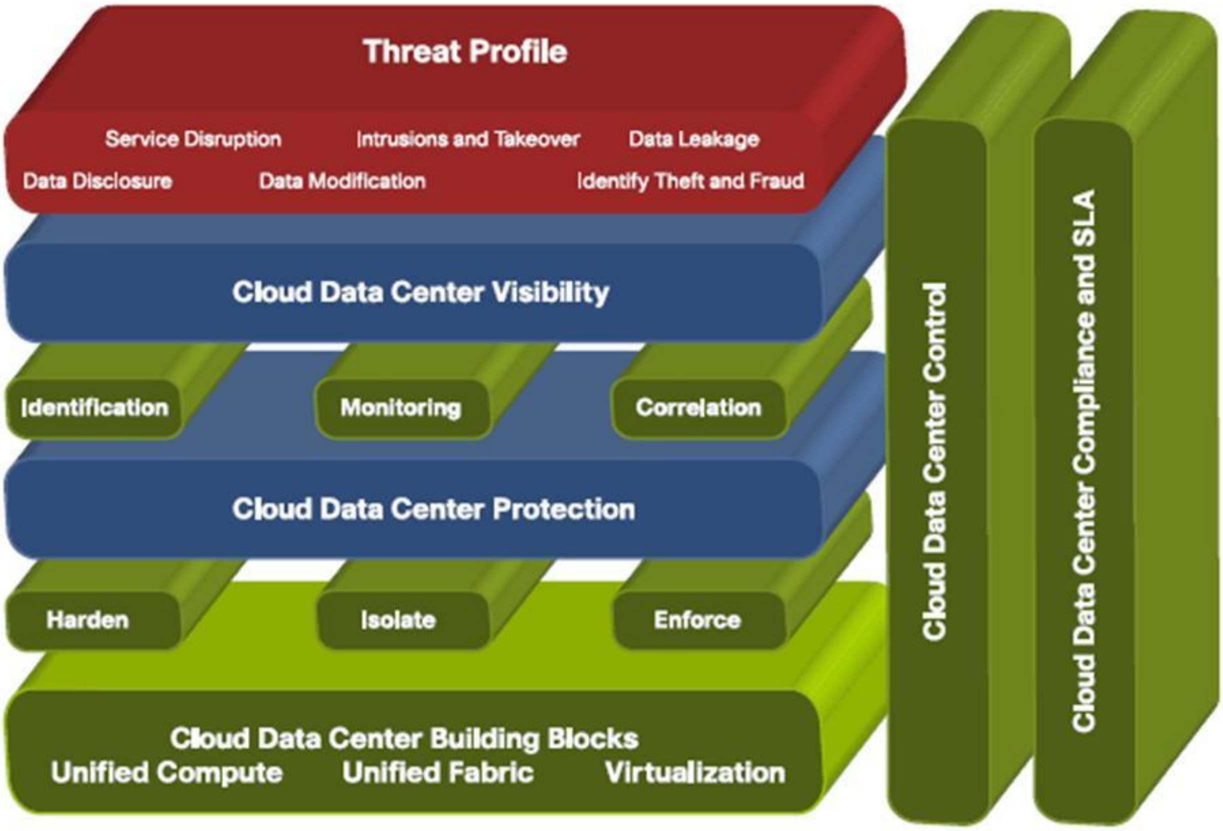

Figure2: Cisco Secure Cloud Data Center Framework (source: www.cisco.com, n.d.)

This framework depicts threats and measures to mitigate security risks. Security should be implemented on layers of architecture and never be an afterthought.

Threats that can be highlighted here are:service interruption, invasion, data leak, data disclosure,data modification, and finally, identity theft and fraud. Visibility and protection should be implemented on all blocks of trusted cloud architecture.

The control aspect in cloud data center security architecture is given due importance. The data centralization leads to greater insider threat, hence, a compartmentalization strategy is made key component of data control. Unencrypted data in the cloud is considered as a risk factor and is under a control policy.

3. LITERATURE REVIEW

Cloud Computing is a big change in computing (Mirashe & Kalyankar, 2010). It moves our applications and documents from desktop into the cloud. Cloud consists of thousands of computers and servers where all the files and applications are linked together and accessible via the internet.

Cloud computing changes the way we work. Users are no more tied to single computer; their work goes wherever they go via web. Also, cloud computing lets them interact in groups. All group members can access same programs and documents from wherever they are located. Cloud computing seems to be farfetched but clients are still using some cloud computing applications. Email programs like; Gmail and Hotmail are computing applications in the cloud. If users are using Google calendar or Apple Mobile Me, then they are computing in the cloud. When people use file-or-photo sharing application such as, flicker or Picasa Web Album, again they are computing in the cloud. It is a future technology which is available for use today as a test bed.

Understanding the Cloud Architecture:

In Cloud architecture, the systems architecture, involved in the delivery of cloud computing, comprises hardware and software that works for a cloud integrator. It involves multiple cloud components communicating through application programming interfaces, usually web services. Complexity is controlled and managed in the Cloud architecture that is being finally extended to the client, where web browsers and/or software applications access cloud applications.

Cloud storage architecture is loosely coupled, often persistently avoiding the use of centralized metadata servers which can become bottlenecks. Loosely coupled architecture enables the data nodes to scale into the hundreds, each independently delivering data to applications or users.

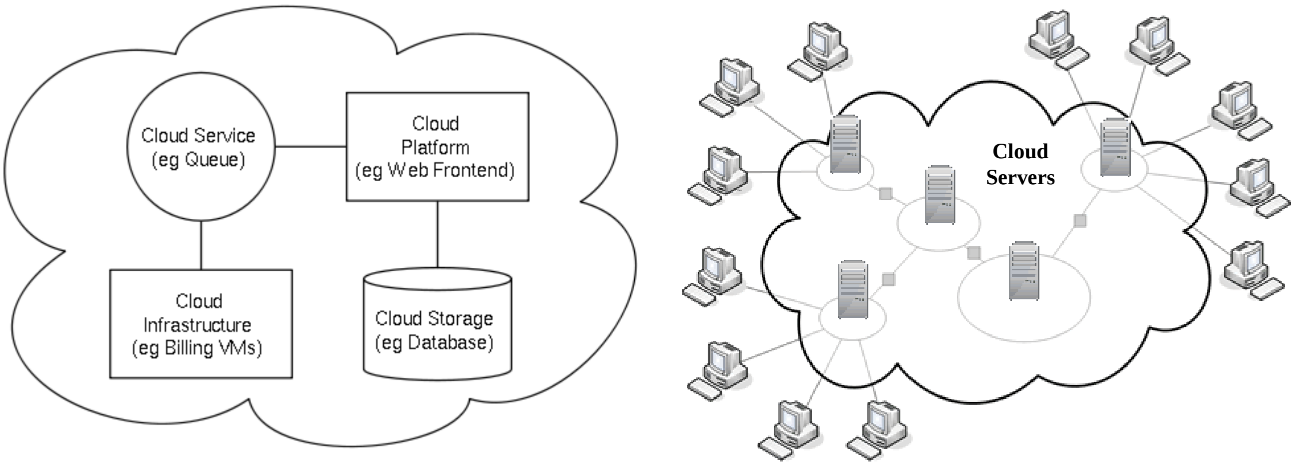

Figure 3: Cloud Computing sample architecture to understand cloud architecture (Source: cloud computing, Journal of Computing, n.d.)

The authenticity of information is judged by analyzing the opinions of many users. On web this approach of building trust and sharing trusted information fails because of users adopting different personas or identity and thus propagate biased opinions. Our mission is to make web network as trustworthy as the users interact in real world scenario, thus believing more on a trusted acquaintance or a friend of friend rather a stranger (Guha et al., 2004). Social networks are propagating an approach centered on relationships of trust providing two primary benefits. A user assessing opinions on a certain idea uses large number of reviews, judgments, or other pieces of information made available through a channel of trust on web presenting views of the data by the individual user, and also opinioned through the sources trusted by the user. And secondly, well-trusted users who globally command greater influence can demand higher prices for goods and services.

Security is greatly focused by the considerable work done concerning trust in computer science. Formal logical models used in the context of cryptography and authentication are; PGP – that is one of the first popular systems to explicitly use the term "Web of Trust" (Guha et al., 2004), even if it was not in the context of search or information flows. The same kind of trust relations between agents can be build for a much wider range of applications than just working on authenticating identities.

For business communities on web trust is the backbone. The importance of gathering information regarding the quality of a product (or service) is greatly emphasized by Ackerlof (Guha et al., 2004). Itshowed how the trustworthiness of a seller is vital for the functioning of a market. Trust is understood to be an important aspect of on-line communities and researchers have started looking at the problem of propagating trust through networks.

Businesses are reluctant to accept cloud computing platforms for their businesses as trust and security isn't fully assured yet. Providers must ensure and work out suitable solutions to secure virtualized data center resources, keep user privacy, and data integrity like crucial issues (Hwang & Li). The researchers opt a solution like implementing a trust-overlay network over multiple datacenters keeping within a reputation system built between service providers and data owners. Data coloring and software watermarking techniques are introduced to protect shared data objects in massive distributed software modules. Multi-way authentications are safeguarded, single sign-on in the cloud is enabled, and tighten access control for sensitive data, is achieved through these techniques implemented in both public and private clouds.

Cloud Computing is a resolution in IT today (Habib et al., 2010). With the emergence of cloud computing there are many research challenges introduced as well. The landscape of Cloud Computing and its research challenges discussed especially the areas of service selection, quality assurance of Cloud services, and trust establishment in Cloud environments are considered and highlighted. Latter is known to be one of the major challenges of Cloud Computing, thus an overview of the important aspects is given which are to be considered when integrating trust and reputation concepts into Cloud Computing.

Online Peer-to-peer (P2P) communities, like, orkut, facebook, etc. offer both opportunities and threats. To counter threats is to use community-based reputations to help estimate the trustworthiness of peers. PeerTrust—a proposed framework to support reputation-based trust, it includes articulate trust model for quantifying and generating the trustworthiness of peers based on a transaction-based feedback system, and a decentralized implementation of such a model over a structured P2P network. PeerTrust model features: three basic trust parameters and two adaptive factors in computing trustworthiness of peers, namely, a trusted channel a peer makes with other peers, the context of transactions a peer performs, the credibility of the feedback sources, transactions made, and the community context factor; then a general trust metric is there to combine these parameters. Strategies are introduced for following the trust model in a decentralized P2P environment, evaluation mechanisms are formulated to validate the effectiveness and cost of PeerTrust model, and set of experiments show the feasibility and benefit of this approach (Xiong & Liu).

It is strived to frame full set of security issues facing cloud-computing. With the best economic picture portrayed by cloud computing, the security challenges it faces are also enormous (Chen et al., 2010). Contemporary and historical perspectives are examined to separate justified concerns from possible over-reactions. It's being argued that some cloud-computing security issues are new or untraceable and fundamental; the complexities of multi-party trust considerations and the ensuing need for mutual auditability.

Where it is known that economic perspective of cloud computing has won the large acceptance – Cloud computing providers can build large datacenters at low cost due to their expertise in organizing and provisioning computational resources, the economies of scale increase revenue for cloud providers and lower costs for cloud users. Thus, resulting on-demand model of computing allows providers to achieve better resource utilization through statistical multiplexing, and enables users to avoid the costs of resource over-provisioning through dynamic scaling. At the same time, security has emerged as the most significant barrier to the adoption of cloud computing. For many business-critical scenarios, cloud computing appears inadvisable due to issues like; service unavailability, data confidentiality, reputation fate sharing, etc.

Here the high level view of the problem is given keeping in mind that cloud computing is the future. The combined contemporary and historical viewpoints open up new dimensions for research.

First point that can be considered is to introduce additional feature supporting 'plug and play' services that is readily in compliance with common standards as HIPAA (Chen et al., 2010) or payment card industry.

Second area of research can be determining suitable granularities for isolation. Possible solution considered can be; isolating virtual or physical machines, LANs, clouds, or datacenters.

Another new area that has yet to receive attention is mutual auditability (Chen et al., 2010). In cloud computing, providers and users will have to prove their trustworthiness. They will have to demonstrate law enforcement put on user's data that's being exchanged over the cloud. For auditing it should be understood that third party is also involved. Thus achieving mutual auditability robustly it would constitute an important security feature.

The ecosystem of combined threats should be understood. Future work on cloud computing should bridge all boundaries on cloud security.

ROCCA (Roadmap for Cloud Computing Adoption), provides organizations with number of steps for adopting Cloud Computing and building trust. It also proposes a Framework called ROCCA Achievement Framework (RAF) (Shimba, 2010). RAF measures adherence level to the ROCCA by the organizations. It presents in detail the technological factors underlying the cloud computing, and defines different delivery and deployment models of Cloud Computing. It clearly emphasizes the need for client and vendor interaction over the cloud and it is possible if organization feels free, confident, and secure over the cloud. The guidelines outlined here guarantee that if followed properly organizations can ensure their adoption of cloud computing as effective, efficient, and providing high degree of satisfaction. It also reflects the business perspective of cloud computing and ensures that projects are well budgeted, and risks are properly understood.

There are no security breaches reported but the instances of cloud computing has resulted in loss of service and this has created reluctance and fear towards using the cloud. March 13, 2009 Microsoft (Shimba, 2010)sidekick that lasted for 6 days reported that there was customer data losses and attributed the loss to system failure. Then on October 16, 2008, the outage affected Google apps customers resulting in failure to access services like emails. The most recent example reported is of salesforce.com, in this case service to 68000 customers got disrupted but no data loss was reported.

To build trust on cloud, trust models being developed need to address different challenges raised by cloud computing.

Currently, the models that try addressing challenges faced by cloud computing are; the trusted computing platform (TCCP) (Santos et al., 2009), Private virtual infrastructure (Krautheim, 2009), Cloud cube model (Jericho, 2009) among others.

Questions raised are:

1. What are the key barriers to cloud computing adoption?
2. Is it possible for client and vendor to collaborate for successful cloud adoption project?
3. Can a roadmap to address the challenges facing cloud computing adoption successfully adopt cloud computing to be developed?

Security and privacy being the prime barriers to adoption of the cloud computing are addressed focusing on Infrastructure-as-a-Service model. A trusted cloud computing platform model has been proposed providing an environment that enables closed box execution guaranteeing to execute guest virtual machines confidentially. But the drawbacks are there; that it reliesa lot on the trusted third party outside of the cloud circumstance. The paper shows how this issue is addressed based on the neutral feature of the Trusted Platform Module (Han-zhang& Liu-sheng, 2010). The responsibility of managing trusted platforms is moved from the trusted third party to the trusted platforms of Infrastructure-as-a-Service model, thus TCCP model is improved achieving higher availability, reliability and safety.

As cloud computing offers a concentration of resources, it poses risks for data privacy through breach into the network. In cloud computing, the heterogeneity of "users" represents entities having multiple accounts associated with a single or multiple service providers (SPs), thus introducing a danger of multiple, collaborative threats. Also, sharing sensitive identity information (that is, Personally Identifiable information or PII) along with associated attributes of the same entity across services can lead to mapping of the identities to the entity, heading to privacy loss. Identity management (IDM) is one of the core components in cloud privacy that demands attention. For identifying entities to Service Providers, available solutions use trusted third party (TTP). Untrusted hosts are not recommended for use by the solution providers. Here it proposes an approach for IDM, which is independent of TTP, and untrusted hosts have the ability to route identity data. Encryption and multi-party computing are the proposed solution for negotiating a use of a cloud service (Ranchal et al.). A middleware agent is used as an active bundle that includes PII data, privacy policies, a virtual machine on which policies are enforced, and has a set of protection mechanisms for its protection. A user interacts through active bundle authenticating him to cloud services using user's privacy policies.

In this paper, there is an analysis of some security requirements in cloud computing environment. Since the security problems both in software and hardware, integrating the trusted computing platform (TCP) into cloud computing system, would be a good method to build a trusted computing environment for cloud computing. A new prototype system is proposed, in which cloud computing system is combined with Trusted Platform Support Service (TSS) and TSS is based on Trusted Platform Module (TPM).This design demonstrates a system from which a better effect can be obtained in authentication, role based access and data protection in cloud computing environment (Shen et al., 2010).

Difference between cloud computing and traditional enterprise internal IT services is that the owner and the user of cloud IT infrastructures are separated in cloud that would require a security duty separation in cloud computing. Customers are the authority in cloud so Cloud service providers (CSP) should secure the services they offer. Currently, no such requirement is met in today's traditional information security products. A multi-tenancy trusted computing environment model (MTCEM) is there to assure a trusted cloud infrastructure to customers and is designed for IaaS delivery model. MTCEM presents transitive trust mechanism and supports a security duty separation function simultaneously on a dual level (Li et al., 2010). MTCEM can be used to improve customers' confidence on cloud computing and CSP. The prototype of MTCEM is successful technically and practically feasible but it has low impact on system performance.

To bring new opportunities for the alertness, reuse, and the adaptive capability of IT, SOA and cloud computing is now introduced for the ever changing business requirements and environments. As the rapidly emerging technologies are still immature, especially in the areas of security, service or information integrity, privacy, quality of service, many enterprises have been hesitating to make the shift due to possible injurious consequences associated. This paper revolves around the concept of insurance and establishes a framework and the supporting reference model for cloud computing. Utilized here is the value-at-risk (VAR) approach to establish several appropriate mechanisms, and use a set of measurable metrics (Luo et al., 2010). For the business value and risk assessment, those quantitative or qualitative metrics can be applied as the basis and eventually for insurance premium and compensation calculation for the failures of the services offered in Cloud environment. This is assumed to be a potential new innovative market branch for the insurance industry.

As discussed earlier Cloud computing with exciting market prospects, has a number of potential risks and safety issues to the cloud services users. The latest research progress is in the field of cloud security (Wu et al., 2011). Finally, trusted cloud computing as another research field is pointed out and is there to integrate with cloud computing.

As Cloud computing is a hot topic in the IT industry for this era. With all the research going on, there are few researches about the impact of cloud computing over individual users. It is important to focus on how to provide personalized services for individual users in the cloud environment. Argument is given that a personalized cloud service shall compose of two parts; the client side program records user activities on personal devices such as PC – besides that, the user model is also computed on the client side to avoid server overhead and the cloud side program fetches the user model periodically and adjusts its results accordingly. A personalized cloud data search engine prototype is built to prove the idea (Guo et al., 2009).

For the large-scale management of distributed resources, cloud and GRID are computing paradigms that are being considered. There is a lot of interest in their integration when cloud is usually oriented for transaction-based applications, and GRID is associated to High Performance Computation. Infrastructure-as-a-Service cloud model gives the opportunity for this integration, as it is exploited in the GRID context to offer machine with full administration rights to users (Casola et al., 2010). The focus is given on the security problems linked to the integration of cloud and GRID computing. Identity federation is proposed to be used between different security domains to manage the relationship between the user machines and the standard GRID infrastructure. PerfCloud is its experimented solution – a cloud implementation that exploits an underlying GRID platform.

4. CRITICAL EVALUATION

Cloud Architecture involves multiple cloud components communicating through application programming interfaces, usually web services(Mirashe & Kalyankar, 2010). Complexity is controlled and managed in the Cloud architecture that is being finally extended to the client, where web browsers and/or software applications access cloud applications.

Cloud storage architecture is loosely coupled, often persistently avoiding the use of centralized metadata servers which can become bottlenecks. Looselycoupled architecture enables the data nodes to scale into the hundreds, each independently delivering data to applications or users – *needs to be authentic*.

The authenticity of information is judged by analyzing the opinions of many users (Guha et al., 2004). On web this approach of building trust and sharing trusted information fails because of users adopting different personas or identity and thus propagate biased opinions.

Security is greatly focused by the considerable work done concerning trust in computer science. Formal logical models used in the context of cryptography and authentication are; PGP – that is one of the first popular systems to explicitly use the term “Web of Trust”.

For business communities on web trust is the backbone. Businesses are reluctant to accept cloud computing platforms for their businesses as trust and security isn't fully implemented yet (Hwang & Li). A Framework called ROCCA Achievement Framework (RAF) is proposed by ROCCA (Roadmap for Cloud Computing Adoption) (Shimba, 2010). RAF measures adherence level to the ROCCA by the organizations.It presents in detail the technological factors underlying the cloud computing, and describes different delivery and deployment models of Cloud Computing. It clearly emphasizes the need for client and vendor interaction over the cloud and it is possible if organization feels free, confident, and secure over the cloud. The guidelines outlined here guarantee that if followed organizations can ensure their adoption of cloud computing as effective, efficient, and providing high degree of satisfaction. It also reflects the business perspective of cloud computing and ensures that projects are well budgeted, and risks are properly understood.

There are no security breaches reported but the instances of cloud computing have resulted in loss of service and this has created reluctance and fear towards using the cloud.

Online Peer-to-peer (P2P)communities offer both opportunities and threats. To minimize threats is to use community-based reputations to help estimate the trustworthiness of peers (Xiong & Liu). PeerTrust—a reputation-based trust supporting framework is proposed, which includes articulate adaptive trust model for quantifying and comparing the trustworthiness of peers based on a transaction-based feedback system, and a decentralized implementation of such a model over a structured P2P network.

It's being argued that some cloud-computing security issues are new or intractable and fundamental; the complexities of multi-party trust considerations and the ensuing need for mutual auditability(Chen et al., 2010).

As cloud computing offers a concentration of resources, it poses risks for data privacy through breach into the network. In cloud computing, the heterogeneity of "users" represents entities having multiple accounts associated with a single or multiple service providers (SPs), thus introducing a danger of multiple, collaborative threats. Also, sharing sensitive identity information (that is, Personally Identifiable Information or PII) along with associated attributes of the same entity across services can lead to mapping of the identities to the entity, heading to privacy loss. Identity management (IDM) is one of the core components in cloud privacy that demands attention (Ranchal et al.). For identifying entities to Service Providers, available solutions use trusted third party (TTP). Untrusted hosts are not recommended for use by the solution providers. Here it proposes an approach for IDM, which is independent of TTP, and untrusted hosts have the ability to route identity data. Encryption and multi-party computing are the proposed solution for negotiating a use of a cloud service. A middleware agent is used as an active bundle that includes PII data, privacy policies, a virtual machine on which policies are enforced and has a set of protection mechanisms for its protection. A user interacts through active bundle authenticating him to cloud services using user's privacy policies.

Questions raised are (Shimba, 2010)**:**

1. What are the key barriers to cloud computing adoption?

2. Is it possible for client and vendor to collaborate for successful cloud adoption project?

3. Can a roadmap to address the challenges facing cloud computing adoption and successfully adopt cloud computing be developed?

Proposed Solutions are many:

Consideration can be given to introduce additional feature that supports 'plug and play' services readily compliant with common standards as HIPAA or payment card industry(Chen et al., 2010).

Possible solution considered can be; isolating virtual or physical machines, LANs, clouds, or datacenters.

Another new area that has yet to receive attention is mutual auditability. In cloud computing, providers and users will have to prove their trustworthiness.

Currently, the models that try addressing challenges faced by cloud computing are; the trusted computing platform (TCCP) (Santos et al., 2009), Private virtual infrastructure (Krautheim, 2009), Cloud cube model (JERICHO, 2009) among others(Shimba, 2010).

A new prototype system is proposed, in which cloud computing system is combined with Trusted Platform Support Service (TSS) and TSS is based on Trusted Platform Module (TPM).This design demonstrates a system from which a better effect can be obtained in authentication, role based access and data protection in cloud computing environment (Shen et al., 2010).

A Multi-Tenancy Trusted Computing Environment Model (MTCEM) is there to assure a trusted cloud infrastructure to customers and is designed for IaaS delivery model. MTCEM presents transitive trust mechanism and supports a security duty separation function simultaneously on a dual level(Li et al., 2010). MTCEM can be used to improve customers' confidence on cloud computing and CSP. The prototype of MTCEM is successful technically and practically feasible but it has low impact on system performance.

The latest research progress is in the field of cloud security. Finally, trusted cloud computing as another research field is pointed out and is there to integrate with cloud computing.

For the large-scale management of distributed resources, cloud and GRID are computing paradigms that are being considered.

5. CONCLUSION

In the light of critical evaluation done on the past research, this research would like to propose an Identity Matrix (IMx) solution enhancing the present Architectural Framework for Trusted Cloud Computing (AFTCC). It suggests adding a module in the present architecture of cloud computing for biometric identification at user level. Any user who is logging into cloud has to verify his identity through biometric check – thumb impression would be the best option for the time being. Then the details user enters against his impression should be verified by online Identity Card (IC) issuing authorities on international level with respect to the respective country the individual belongs. Biometric device would be built-in in any future electronic device that can be connected to internet.

Future work would be incorporating this module in the Architectural Frameworkfor Trusted Cloud Computing (AFTCC), and what ever more work is done regarding incorporating security in founding layers of architecture; taking it forward to implement it.

REFERENCES

[1] Armbrust M., Fox A., Griffith R., Joseph A. D., Katz R., Konwinski A., Lee G., Patterson D., Rabkin A., Stoica I., &Zaharia M., *Above the Clouds: A view of cloud computing*, [UC Berkeley Reliable Adaptive Distributed systems Laboratory (RAD Lab)]

[2] *Cloud computing* - Wikipedia, the free encyclopedia.mht

[3] Chen Y., Paxson V. & Katz R. H., *What's new about cloud computing security?*, [CS Division, EECS Dept. UC Berkeley], 2010

[4] Casola V., Rak M. & Villano U., *Identity federation in cloud computing*, [Dipt. di Inf. e Sist., Univ. degliStudi di Napoli Federico II, Naples, Italy], IEEE, 2010

[5] Depena R, *Cloud Computing Companies to Watch in 2011 (2010 was certainly an exciting year in the Cloudsphere)*.

[6] Figure 1: Simple flow of Cloud Computing Infrastructure (Source: RAD Lab)

[7] Figure 2: Cisco Secure Cloud Data Center Framework [source: www.cisco.com], *Cisco Cloud Computing - Data Center Strategy, Architecture, and Solutions Point of View White Paper* [for U.S. Public Sector], 1st Edition.

[8] Figure 3: Cloud Computing sample architecture to understand cloud architecture [Source: cloud computing, Journal of Computing]

[9] Guha R., Kumar R., Raghavan P. & Tomkins A., *Propagation of Trust and Distrust*, [IBM Almaden Research Center], 2004

[10] Guo H., Wu W., Wang W. & Chen J., *Personalization as a service: the architecture and a case study*, [EMC Research China, Fudan Univerisity], 2009

[11] Han-zhang W. & Liu-sheng H., *An improved trusted cloud computing platform model based on DAA and privacy CA scheme*, [Dept. of Comput. Sci. & Technol., Univ. of Sci. & Technol. of China, Hefei, China], 2010

[12] Hwang K. & Li D., *Trusted Cloud Computing with Secure Resources and Data Coloring*, [Univ. of Southern California, Los Angeles, CA, USA]

[13] Habib S. M., Ries S. & Mühlhäuser M., *Cloud Computing Landscape and Research Challenges Regarding Trust and Reputation*, [Xi'an, China], 2010

[14] *Intel Cloud Builder Guide to Cloud Design and Deployment on Intel Xeon Processor-Based Platforms, Enomaly Elastic Computing Platform*, [Service Provider Edition]

[15] Jennings *R., How DevOps brings order to a cloud-oriented world*, [searchCloudComputing.com]

[16] JERICHO, *Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration*, V1.0 (Position Paper). Jericho Forum, 2009

[17] Knorr E. & Gruman G., *What cloud computing really means*,[InfoWorld],link: http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031

[18] Krautheim, F. J. *Private Virtual Infrastructure for Cloud Computing*. 2009

[19] Li X.; Zhou L.; Shi Y. & Guo Y., *A trusted computing environment model in cloud architecture*, [Beijing Jiaotong Univ., Beijing, China], 2010

[20] Luo M.; Zhang L. & Lei F., *AnInsuanrance Model for Guranteeing Service Assurance, Integrity and QoS in Cloud Computing*, [IEEE], 2010

[21] Mojica M., Stephenson J. & Healey A., *Six questions every retail executive should ask about cloud computing*, [Accenture]

[22] Mirashe S. P.& Dr. Kalyankar N.V., *Cloud Computing*, Journal of computing, volume 2, issue 3, March 2010

[23] Pandit M., *Scalable Computing Programme Newsletter*, [Digital Systems KTN], 3rd Edition, June 2010Ragnet F., Can You Trust the *Cloud? A Practical Guide to the Opportunities and Challenges Involved in Cloud Computing*, [Xerox]

[24] Ranchal R., Bhargava B., Othmane L.B., Lilien L., Kim A., Kang M. &Linderman M.; *Protection of Identity Information in Cloud Computing without Trusted Third Party*, [Purdue University], [Western Michigan University], [Naval Research Laboratory], [Air Force Research Laboratory], USA

[25] Shimba F., *Cloud Computing: Strategies for Cloud Computing Adoption*, Dublin Institute of Technology, 2010

[26] Shields G., *Can you trust your public cloud provider?* searchCloudComputing.com

[27] Siemens IT Solutions and Services, *Community Clouds – supporting business ecosystems with cloud computing*

[28] Santos, N., Gummadi, K. P., et al. *Towards Trusted Cloud Computing*. Planc Institute for Software Systems, 2009

[29] Shen Z., Li L., Yan F. & Wu X., *Cloud Computing System Based on Trusted Computing Platform*, [State Key Lab. of Software Eng., Wuhan Univ., Wuhan, China], 2010

[30] Website: www.salesforce.com, copyright 2000-2012

[31] Wu J. Y., Shen Q. L., Zhang J. L.& Xie Q., *Cloud Computing: Cloud Security to Trusted Cloud*, [2011, Advanced Materials Research, 186, 596]

[32] Xiong L. & Liu L., *PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities*, IEEE Computer Society

[33] Yachin D., *Israel Software Industry Review: Addressing Cloud Computing Challenges*, February 2010