Challenges and Issues Within Cloud Computing Technology

Omar Ali
School of Management and Enterprise
Faculty of Business, Education, Law and Arts
University of Southern Queensland
Toowoomba-Australia
Omar.Ali@usq.edu.au

Jeffrey Soar
School of Management and Enterprise
Faculty of Business, Education, Law and Arts
University of Southern Queensland
Toowoomba-Australia
Jeffrey.Soar@usq.edu.au

Abstract-Cloud computing refers to an emerging computing model where machines in large data centres can be used to deliver services in a scalable manner. It has become popular for corporations in need of inexpensive, large scale computing. Organizations and government agencies increasingly utilise cloud computing architectures, platforms and applications to deliver services and meet the needs of their clients. There are many challenges and issues such as privacy, security and trust that can have major impacts on the information and services supported by this technology. This paper summarises the technology background and discusses challenges and issues that can arise by the use of cloud computing in organizations and government agencies.

Keywords-privacy; security; trust; issues; cloud computing.

I. INTRODUCTION

Information Technology (IT) has been adding significant benefits to various aspects of people's life, either in terms of convenience or comfort or entertainment. One of the latest developments in the IT industry is cloud computing, also known as on-demand computing. This new technology provides higher performance at relatively low cost compared to the existing dedicated infrastructures. Moreover, it can be applied to larger scale with greater reliability. Cloud computing offers a shift in the way organizations invest in their IT resources. The new model removes the need for organization to invest a substantial sum of money for the purchase of limited IT resources that are internally managed. Instead, the organization can outsource its IT resource requirements to a cloud computing service provider and pay per use.

Cloud computing is a computing model that provides a pool of computing resources which users can access through the internet. The basic principle of cloud computing is to shift the computing from a local computer to the network. It offers the capacity to utilize a common collection of resources on request. It proves extremely attractive to cash-strapped IT departments that want to deliver better services under pressure. It can offer access to greater infrastructure resources which include network, server, storage, application, services and other components, as required, without huge investment in purchase, implementation, and maintenance. Cloud computing can be deployed either as: private cloud (where organizations develop their own applications and run their own internal infrastructure), community cloud (where the cloud infrastructure is shared by several organizations and supports a specific community), public cloud (where the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services), or hybrid cloud (where the cloud infrastructure is an integration and consolidation of two or more clouds which are private, community, or public) [1]. Cloud computing offers many advantages for IT organizations. There are, however issues and challenges that still exist and which must be dealt with. A key concern in adopting cloud computing is data security, privacy and trust.

This paper presented the state-of-the-art of research into cloud computing technology and its characteristics. It highlighted the main important challenges, barriers and risks related to the cloud computing. Also, the paper presented some mitigation steps to overcome the challenges and issues that discussed.

II. CLOUD BACKGROUND

A. Definitions

Formal definitions have been proposed in both academia and industry; however, the one provided by U.S. National Institute of Standards and Technology (NIST) [2] appears to include key common elements widely used in the cloud computing environment:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction [2].

In order to provide the users with better services, cloud computing maintains proper cloud architecture, offers various deployment strategies depending on the organization structure and provisioning location, and most importantly, takes care of the security issues over a network. The four deployment models along with their characteristics are depicted in the following flow-chart Figure 1.

 ISBN: 978-1-61208-338-4

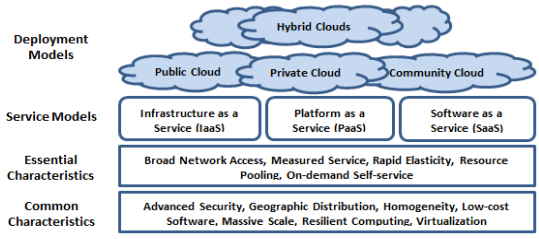

Figure 1.The NIST Cloud Definition Framework [2]

- *On-Demand Self-Service*

A consumer with an instantaneous need in a particular timeslot can avail itself of computing resources (e.g., network storage and software use) in an automatic (self-serve) fashion without resorting to human interactions with the providers of these resources.

- *Broad Network Access*

These computing resources are delivered over the network and used by various client applications with heterogeneous platforms (e.g., mobile phones and laptops) situated at a consumer's site.

- *Resource Pooling*

In an effort to serve multiple consumers, a cloud service-provider pools together the computing resources using either the multi-tenancy or the virtualisation model "with different physical and virtual resources dynamically assigned and reassigned according to consumer demand" [2]. The motivation for setting up such a pool-based computing paradigm lies in two important factors: economies of scale and specialisation. The result of a pool-based model is that physical computing resources become 'invisible' to consumers, who, in general, do not have control over or knowledge about the location, formation, and origins of these resources (Database).

- *Rapid Elasticity*

For consumers, computing resources become immediate rather than persistent: there are no up-front commitments and contracts as they can use them to scale up whenever they want and release them once they finish scaling down. As there is provision for infinite computing resources on the cloud, there is no limitation in meeting their peak requirement of increased consumption any time.

- *Measured Service*

Even though the resources are pooled and shared by multiple consumers through a multi-tenancy model, the cloud infrastructure is equipped with an appropriate mechanism to monitor the usage of computing resources by individual consumers.

The European Network and Information Security Agency (ENISA) has defined cloud computing as an "on-demand service model for IT provision, often based on virtualisation and distributed computing technologies" [3]. The first academic definition of cloud computing offered by [4] is a bit different from the definition provided by the ENISA. According to Chellappa [4], cloud computing is "A computing paradigm where the boundaries of computing will be determined rationale rather than technical". According to Buyyaa et al. [5], cloud computing is "A type of parallel and distributed system consisting of a collection of interconnected and virtualised computers that are dynamically provisioned and present as one or more unified computing resources based on the service-level agreements established through negotiation between the service provider and the customer". While Vaquero et al. [6] proposes the following definition "Cloud is a large pool of easily usable and accessible virtualised resources" (e.g., hardware, development platforms and services). One can reconfigure these resources dynamically to allow the optimum utilisation of resources, which can be exploited by a pay per use model where the infrastructure provider offers a guarantee by means of customised Service Level Agreements (SLAs). These different definitions show the varied understanding of what cloud computing is from the perspectives of different stakeholders such as academics, architects, consumers, developers, engineers and managers.

B. Service/Delivery Models

The following three service models are used to categorize cloud services:

- *Software as a Service*

The SaaS service model enables consumers to use the service provider's applications running on a cloud infrastructure [7]. Consumers can access the applications using various client devices through a thin client interface such as a Web browser (example include, Web-based email) [7]. They do not have the access to manage or control the underlying cloud infrastructure, that is, network, servers, operating systems, storage or even individual application capabilities. Consumers do have access to limited user-specific application configuration settings [2][7][38][39][40] [41]. Examples of SaaS include, Salesforce, Netsuite and Google Apps.

- *Platform as a Service*

The PaaS service model enables the consumer to deploy consumer-created or acquired applications onto the cloud infrastructure with the help of programming languages and tools the provider supports [7]. As in the SaaS model, the consumer does not manage or control the underlying cloud infrastructure, but can control the deployed applications and possibly the application-hosting environment configurations [7][41][42][43]. Examples of PaaS include, Microsoft Azure service platform, Salesforce-Force.com, Google App engine Amazon relational database services and rack space cloud sites.

 ISBN: 978-1-61208-338-4

- *Infrastructure as a Service*

The IaaS service model provides the consumers with processing, storage, network and other fundamental computing resources. The consumer can deploy and run arbitrary software, including operating systems and applications. As with the other two models, the consumer cannot manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications and possibly has limited control over select networking components, such as host firewalls [2][44][45]. Examples of IaaS include, Amazon S3 (simple storage service) - EC2 (elastic cloud computing) and rack-space cloud servers.

C. Deployment Models

More recently, four cloud deployment models have been defined in the cloud community: [2][3][7][8][9].

- *Public Cloud*

This model enables the cloud infrastructure to be made available to the general public or to a large industry group. The cloud service providers have the full ownership of the public cloud with its own policy, value, and profit, costing, and charging model [8]. Many popular cloud services are public clouds, such as Amazon EC2, Google App Engine and Force.com. In this model, clients can choose the security level they need, and negotiate for SLA [2][8].

- *Private Cloud*

In this model, the cloud infrastructure is deployed solely for a single organization. The organization may itself manage the infrastructure or outsource it to a third party, and the cloud infrastructure may exist in the organization's premises or be based off-premise [8]. The motivation to setup a private cloud within an organization has several aspects. Firstly, in order to optimize the utilization of existing internal resources. Secondly, for security concerns including data privacy and trust which makes private cloud an option for many firms. Thirdly, data transfer cost from local IT infrastructure to a public cloud is even more considerable [10]. Fourthly, organizations always require full control over mission-critical activities that exists behind their firewalls. Lastly, academics often build private cloud for research and teaching purposes [2][7][8].

- *Hybrid Cloud*

In this model, the cloud infrastructure is composed of two or more clouds (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (example include, cloud bursting for load-balancing between clouds) [2][7]. Organizations use the hybrid cloud model in order to optimize their resources, to increase their core competencies by margining out peripheral business functions onto the cloud, while controlling core activities on premise through private cloud. The concept of the hybrid cloud aims to address the issues of standardization and cloud interoperability [7].

- *Community Cloud*

This model deploys the cloud infrastructure to several organizations at the same time and supports a specific community that shares similar concerns (example include, mission, security requirements, policies and compliance considerations). The cloud community forms into a degree of economic scalability and democratic equilibrium. The cloud infrastructure may be managed by the organizations or by a third party and may exist in the organizations' premise or be based off-premise [8]. Cloud services in government are generally utilized to reach the citizen using various tools such as Internet, Phone, IVR, etc. In particular, the citizen, can access information from various department including centre, state, and local governments such as Tax, Railway, Passport, Immigration and Visa, Central Excise, Company Affairs, National ID [8].

III. CHALLENGES AND ISSUES

A. Cloud Privacy Issues

One of the fundamental human rights is that of 'privacy'. From the customer point-of-view in commerce, privacy demands complete protection and the appropriate use of customers' personal information [30]. The practice of privacy in an organization includes abiding by laws, policies, standards and processes in managing the personally identifiable information (PII) of individuals.

'Privacy', in the context of the cloud, is not straight forward and depends on the type of cloud situation. The threat to privacy is minimal in some cloud application areas and services for example, services used for processing public information. However, the threat is more in services that deal with different aspects of data (e.g., collecting, transferring, processing, sharing or storing) relating to personal information. This warrants adequate measures be taken to protect privacy with regard to those services dealing with highly sensitive information, especially, information relating to location, preferences, social networks of individuals and personal health data [30] [47][48][49].

To minimize threat where the potential risk is high, customization of such services by including embedded tracking and profiling with inter-device communication can be implemented [30].

Although the public cloud is the preferred economically viable architecture, it also poses a threat to privacy because customers' data are handled and managed by the Cloud Service Provider (CSP) [30]. In this section researchers consider a number of aspects that illustrate the most important privacy issues in the public cloud: lack of user

 ISBN: 978-1-61208-338-4

control, unauthorized secondary usage, trans-border data flow and data proliferation and dynamic provisioning [2][7].

- *Lack of User Control*

In general, cloud computing can be used as three delivery models. As mentioned before: IaaS; PaaS and SaaS [1]. When using SaaS as a delivery module, the responsibility for controlling data belongs entirely to the service-provider [30][50]. Hence, the biggest concern for the customer is: how can it retain its control on the data when information is processed or stored? With this new technology, misuse, theft or illegal use always remain matters of grave concern because a cloud computing system involves the processing of user- sensitive information. Moreover, since the technology has not been secured through a patent initially, CSP can neither impose 'no accessibility' to all PII by a third party nor can it conform to a request to delete an individual's personal data. It can be difficult to get data back from the cloud and avoid vendor lock-in [11][30][47][50]. The problem is even worse when many tenants are hosted on the same physical hardware. Thus, cloud service providers must ensure the customers that their data and applications are secured and the risks are mitigated to an acceptable level. Hence, a legal requirement that becomes important is that both the cloud provider and the customer establish information security systems and trustworthiness for each other [12][30].

- *Unauthorized Secondary Usage*

A threat can occur when information is used illegally but the standard cloud computing business model states that service providers can profit from the authorised secondary use of users' data; In particular, these data are often used to target advertisements [13][30][51].

- *Trans-Border Data Flow and Data Proliferation*

One attribute of cloud computing is data proliferation, which is a process that involves several companies and is not controlled or managed by the data owner. The vendor guarantees the ease of use by facilitating data availability in several data centres. Hence, it is very difficult for the vendor to ensure that duplication of the data or its backups is not stored or processed in a certain authority, and that all these copies of data are deleted if such a request is made [30]. Due to the dynamic nature of this technology and the movement of data, Central Processor (CP) exacerbates the trans-border data flow because it can be extremely difficult to ascertain which specific server or storage device will be used [14][30][52].

- *Dynamic Provision*

Although many of the problems faced by cloud computing are similar to those faced by traditional IT outsourcing, because of the dynamic nature of the cloud, the existing provisions for addressing the problems in more static environments are rendered obsolete or impractical to set up and implement in such a short timescale [30]. It is not clear which party is responsible (statutorily or contractually) for ensuring legal requirements for the protection of personal information, and whether appropriate data handling standards are set and followed [7][30], or if the third-party compliance can be audited effectively with such laws and standards. It is also still unclear if the cloud sub-contractors involved in processing can be properly identified, checked and ascertained as trustworthy, particularly in the dynamic environment of cloud computing. It is also unclear what rights concerning the data will be acquired by data processors and their subcontractors, and whether these are transferable to other third parties upon bankruptcy, takeover or merger [15].

B. Cloud Security Issues

In a traditional security model, such as a corporate firewall, for example, there is self-control over computing resources and storing and processing information within a set security perimeter. The network provides transit to other trusted end hosts, which operate in a similar manner. This model has been proven adequate for the original Internet, but not for public and hybrid clouds [30]. Since the confidential information in the cloud may be processed outside the known trusted areas as these computing environments often have unsure boundaries with regard to the location of storing and processing data, the security perimeter becomes blurred. The consumers, on the other hand, need to extend their trust to the cloud service provider, in order to obtain the service, which in turn can give rise to difficulties [30].

In addition to the privacy issues discussed previously, the public cloud has its share of security concerns. A recent user survey [16], indeed rated security as the top challenge of the cloud model. Private clouds can, to a certain extent, guarantee security, but the cost associated with this approach is quite high [50]. In this section, we present problems that are very important for cloud architectures.

The security challenges associated with cloud computing are exacerbated at the network, host and application levels [30]. The main issues relate to defining which parties are responsible for which aspects of security. Such division of responsibility is hampered by the lack of standardization of the cloud Application Program Interface (API). The risk of data loss, the unauthorized collection and usage of data and the CSP not adequately protecting data [52], are some of the security concerns facing customers. The security risks fit into a broader model of cloud-related risks. According to CSA [17], the top threats to cloud computing are abuse and nefarious use of cloud computing, insecure interfaces and APIs, malicious insiders, shared technology issues, data loss or leakage, account or service hijacking and unknown risk profile. There is no consensus on ranking the degree of severity of these risks.

 ISBN: 978-1-61208-338-4

It may be noted that there is scope for outsourcing security to security experts. Therefore, security need not necessarily suffer in moving to the cloud model. In fact, in many cases, greater protection than those available previously, can be obtained. Some security concerns regarding the public cloud are described below:

- *Access*

Access to confidential information by a governments' surveillance over data stored in that country in the cloud can increase the risks. Governments in the countries where the data is processed or stored may even have legal rights to view the data under some circumstances [18][53], and this may not be known by the consumers. Furthermore, as with other computing models, unauthorized access by entities involved in the provider chain with inadequate security mechanisms in place, can exacerbate the risk. There can be the risk of data theft by rogue employees of CSPs or by data thieves breaking into service providers' machines, or even by other customers of the same service if there is inadequate separation of customers' data in a machine that they share in the cloud [52].

The risk to data stored in the cloud for long periods of time is more from malicious behavior than processing in the cloud, because of higher exposure time. However, the problem can be potentially solved using encryption in the cloud storage [30].

- *Control Over Data Lifecycle*

Another important issue for the cloud is to ensure the customer that they have control over their data. In particular, the cloud should ensure that data be deleted and unrecoverable by a cloud service provider. Presently, there is no way to prove this as it relies on trust. The problem is exacerbated in the cloud because there can be many copies of the data, potentially held by different entities [30].

This risk depends more specifically on the cloud service model being used. When using IaaS or PaaS, one or more virtual machines are created in order to run a program. When the task is finished, the virtual machines and the disk spaces are released. However, it may be possible for the next user to recover the previous user's data as the media may not be wiped completely. Users generally do not know what happens to the physical volume supporting their virtual storage. When using the SaaS approach, the customer is one of the users of a multi-tenant application developed by the CSP. The customers' data is stored in the cloud and made accessible to him on his subsequent log in. The data is deleted only at the end of the lifecycle of the data, if the customer wishes to change service provider.

- *Multi-Tenancy*

It is a feature of SaaS that one program can run to multiple machines. CSP uses a multi-tenant application of the cloud to reduce cost by using a virtual machine, but it increases vulnerability [19].

- *Audit*

Internal control can be achieved through an external audit mechanism which permits CSP to monitor data [30]. The cloud computing environment presents new challenges from an audit and compliance perspective, but the existing solutions for outsourcing and audit can be leveraged. For ensuring data integrity and winning the trust of the data owner in the cloud environment, data transaction needs to be appropriate so as to prevent the occurrence of any untraceable action. This provision is still lacking, especially in public models. Additionally, there remains the issue of unclear ownership regarding the transactional data and this makes it hard to anticipate which data need protection [20].

C. Cloud Trust Issues

One of the major concerns, particularly with regard to financial and health data is the higher risk to data privacy and security attached to the vendor offerings which actually aim to assist business and encourage the use of cloud computing [30]. Both the financial and health sectors deal with confidential and sensitive information. Therefore, the associated vulnerability of the cloud computing system is the key business inhibitor in such sectors. These domains need control against unauthorized or secondary access or any kind of misuse, and cloud computing systems do not allow such customer control. Sectors, like finance and health, have to rely on mechanisms, such as insurance, court action, or penalties, which provide compensation in case of breach of SLAs.

There is no universally accepted scholarly definition of 'trust', as it is a complex concept; however, according to a number of contemporary cross-disciplinary scholarly writings, the following definition is widely held [21]: "Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another". Yet this definition does not fully capture the dynamic and varied subtleties involved: trust is a complex notion and a multi-level analysis is important in order to try to understand it. There are many different ways in which online trust can be established: security may be one of these, although security, on its own, does not necessarily imply trust [22]. Some would argue that security is not even a component of trust: [23] argues that the level of security does not affect trust. Although some would argue that security is not even a component of trust, it has been found that sometimes increasing security enhances the level of trust among customers. One example of this might be that the assurance of cryptogenic protection of credit cards and personal data may encourage people to participate in e-commerce [24].

Some may consider reputation, another component of online trust, as the most valuable asset of any organization

[23], although the reputation of a CSP may not be justified. In the event of any breach of trust, the brand image suffers the most.

In a relationship, trust goes through different phases. In the beginning, trust is built up until it finally becomes a stable trust relationship. However, another phase may follow after achieving a stable relationship, a phase of declining trust, and trust can easily be lost as Nielsen states [25], "It is hard to build and easy to lose: a single violation of trust can destroy years of slowly accumulated credibility".

Now, while assessing trust with regard to cloud computing systems, it is important to differentiate between social and technological aspects of providing diligent and dynamic trust as both aspects are necessary [26].

Persistent Trust: Characterized by properties or infrastructure emerging out of a relatively static socio-technological mechanism, persistent trust is established over the long term.

Dynamic Trust: In a context-based socio-technological mechanism, dynamic trust is associated with a specific state or context and specific, short term or variable information.

In a hardware or software component/system, persistent social-based trust is interlinked with technological-based trust, because the former can only be established if confidence in the operation and implementation of the system is gained [30]. A vouching mechanism underlies this connection - it is equally important to know who is vouching and what are they vouching for. Similarly, in a cloud computing system, persistent trust is established when dynamic-technological-based trust is grown in combination with both social and technological mechanisms. In a cloud resource, information can only be trusted if there is trusted vouch for the method that provides and assesses the information. Depending on the context, vouching on a method should come from different entities such as consumer groups, auditors, security experts, regulators, companies with a proven reputation, and established CSPs.

- *Lack of Customer Trust*

Lack of transparency is one of the major reasons for distrust in any system [30]. The same is true for a cloud system where individuals have no clue why, how and by whom their personal information is managed and this result in skepticism which finally leads to mistrust [27]. Customers may not show confidence in using cloud services, especially when personally identifiable information is involved, due to security related concerns as to whether the cloud can adequately protect data [7], and this is particularly related to sectors like finance and health which involve confidential and sensitive information. Before taking any decision regarding a cloud system, customers should also take into account the obligation and compliance assurance from the prospective suppliers promising to address such risks. Therefore, trust is the key element in the adoption of SaaS by the customer. A mechanism that brings transparency into different service provisions might encourage customers to adopt such a system, because when adopting the cloud, there is always trade-offs between factors like security, privacy, compliance, costs, and benefits [27].

- *Weak Trust Relationships*

Trust relationships may be weak at any point in the cloud service delivery chain, but they exist in order that a service can be provided quickly. When a cloud transaction is initiated there is always a risk of loss of control in the transaction of sensitive data to other organizations because of the globalized nature of cloud infrastructure [30]. This may cause significant loss in business due to the lack of data control on the part of the customer who is using the cloud. For example, the parent organization may not know whether the contractors are sub-contracting the key business processes to others. The contract requirements regarding data protection measures may not be propagated down the contracting chain and this further increases the risk.

Ensuring trust at all level of the chain to customer may not be transitive for cloud providers, and particularly, the customer may not trust some of the subcontractors (XaaS providers). Lack of transparency may not even allow the customer to know about the cloud providers in the chain. Particularly, models, like 'on-demand' and 'pay as you go', based on weak trust relationships, allow third parties in data security practices to, expose data and even delete data which are hard to find. Moreover, addition of new cloud service providers at short notice or in real time does not provide any chance to scrutinize their background.

Trust issues in cloud computing environments can be divided into four sub-categories [28][29][30][31], which include:

- How to define and evaluate trust according to the unique attribute of cloud computing environments?
- How to handle malicious recommend information, which is very important in cloud computing environments, as the trust relationship in the cloud is temporary and dynamic?
- How to consider and provide different security levels of service according to the trust degree?
- How to adjust and really reflect trust relationship dynamic change over time and space?

D. Cloud Interoperability Issues

Currently, each cloud offering has its own way that cloud clients/applications/users interact with the cloud, leading to the 'hazy cloud' phenomenon [32][57], the development of the cloud ecosystem is severely hindered because of enforced vendor lock in which prevents users from choosing alternative service providers for optimizing their resources at different levels within an organization. More importantly, proprietary cloud APIs makes it very difficult to integrate cloud services with an organization's

own existing systems (e.g., an on-premise data center for highly interactive modelling applications in a pharmaceutical company) [49][57]. The scope of interoperability here refers both to the links among different clouds and the connection between a cloud and an organization's local systems. The primary goal of interoperability is to realize seamless fluid data communication across clouds and between the cloud and local applications [54][57].

There are a number of levels at which interoperability is essential for cloud computing. First, to optimize the IT asset and computing resources, an organization often needs to keep in-house IT assets and capabilities associated with their core competencies while outsourcing marginal functions and activities (e.g., the human resource system) on to the cloud. In this case, frequent communication between cloud services (Human Resources **(**HR) system) and on premise systems (e.g., an Enterprise Resource Planning (ERP) system) becomes crucial and indispensable for running a business. Poor interoperability such as proprietary APIs and overly complex or ambiguous data structures used by an HR cloud SaaS will dramatically increase the integration difficulties, putting the IT department into a difficult situation. Second, more often than not, for the purpose of optimization, an organization may need to outsource a number of marginal functions to cloud services offered by different vendors. For example, it is highly likely that a Small and Medium Enterprises (SME) may use Gmail for the email services and SalesForce.com for the HR service. This means that the many features (e.g., address book, calendar) in the email system must connect to the HR employee directory residing in the HR system [57].

- *Intermediary Layer*

The interoperability issues have been addressed in a number of recent works by providing an intermediary layer between cloud consumers and resources (e.g., VM). For example,[33][57] proposed the notion of virtual infrastructure (open nebula) management to replace native VM API interactions in order to accommodate multiple clouds, private or hybrid for an organization. Open nebula works at the virtualization level, thus providing cloud consumers with a unified view and operation interfaces towards the underlying virtualization implementations of various types. Unlike open nebula, [34][57] developed an abstraction layer at a higher level. This provides a single resource usage model, user authentication model and an API to shield the cloud providers' heterogeneity which can hinder the development of cloud-provider independent applications.

- *Standard*

Standardization appears to be a good solution to address the interoperability issue [57]. However, as cloud computing has only now started to take off, the interoperability problem has not appeared on the agenda of major industry cloud vendors. For example, neither Microsoft nor Amazon supports the Unified Cloud Interface (UCI) project proposed by the Cloud Computing Interoperability Forum (CCIF) [35][57]. The standardization process will be very difficult to progress when these big players do not come forward to reach consensus. A widely used cloud API within academia is the Eucalyptus project [36][57], which mirrors the well-known proprietary Amazon EC2 API for cloud operation. Although an Eucalyptus IaaS cloud consumer can easily connect to the EC2 cloud without substantial redevelopment, it cannot solve the general interoperability issue that requires an open API to be complied with by different types of cloud providers.

IV. MITIGATION STEPS

One observer has correctly admonished IT executives, noting that when it comes to shifting to cloud computing, "Standing pat means being left behind" [55]. Linda Cureton, NASA's CIO, stated the matter thus:

"I'd like to say it a little more bluntly. If CIOs don't get ready, manage fears and manage their risk, they will get run over by this disruptive technology. Your organization is doing it anyway – without you! So do something! You don't have to move your entire enterprise into the cloud, just take the first step and look at some appropriate data sets.This does not have to be an all / none decision" [56].

Some mitigation steps and some solutions to overcome the issues discussed in the previous section are discussed here. In addition, this section also outlines a few recommendations for cloud service providers to develop good strategies which may help in reducing security, trust and privacy issues in a cloud environment. Adopting these issues again raises several issues related to performance as well as the security of the system, issues such as the user's privilege to control data causing low transaction performance and internet speed affecting performance [37].

Some actions as listed below must take place to mitigate the above problems:

- In order to relocate a cloud environment from its traditional environment, a new policy must be put forward.
- Finding a new solution to avoid or fix a problem is not enough. One has to check the effect of the solution on the system.
- Any new changes made should be scrutinised by providers along with making the customers' access privileges limited.
- Finding the linked service providers to a particular cloud service provider is necessary for knowing about their right to use data.
- Monitoring system should be excluded.

 ISBN: 978-1-61208-338-4

- Within the duration of services, a customer should be informed by its service provider about managing security policies apart from the provider's own policy.
- Data transfer should be protected and secured by standard security techniques and it must be ensured that data are managed by skilled professionals.

V. CONCLUSIONS

High security is one of the most important problems for opening up the new era of the long dreamed vision of cloud computing as utility services. As the sensitive applications and data are moved into the cloud data centres, run on virtual computing resources in the form of a virtual machine. This unique attribute however, poses many new security challenges, such as: access, control over data lifecycle, availability and back-up, multi-tenancy and audit. With the rapid improvement of cloud computing and the increasing number of cloud users, security, privacy and trust issues will continue to increase. To protect private and sensitive data that are processed in data centres, the cloud user needs to verify the following:

- The real existence of the cloud computing environment in the world.
- The security of information in the cloud.
- The trustworthiness of the systems in the cloud computing environment.

In this paper, researchers primarily aim to highlight the major issues and challenges (security, privacy and trust) on the way towards adopting cloud computing. The interoperability issue was highlighted as well.

REFERENCES

[1] D. Hilley, "Cloud computing: Taxonomy of platform and infrastructure-level offerings", *CERCS Technical Report*, Georgia Institute of Technology, 2009, accessed on September. 2013, available at: http://www.csrc.nist.gov/groups/SNS/cloudcomputing/index.html.

[2] P. Mell and T. Grance, "Draft NIST working definition of cloud computing", vol. 15, 2009, pp. 1-7.

[3] D. Catteddu and G. Hogben, "Cloud computing: Benefits, risks and recommendations for information security", *European Network and Information Security Agency* (ENISA), 2009, pp. 17-25.

[4] R. K. Chellappa, "Intermediaries in Cloud-Computing: A New Computing Paradigm", *INFORMS Annual Meeting*, Dallas, TX, October 26-29, 1997, accessed on December. 2013, available at: http://www.bus.emory.edu/ram/.

[5] R. Buyyaa, C. S. Yeoa, S. Venugopala, J. Broberg, and I. Ivona Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", *Future Generation Computer Systems*, vol. 25, 2009, pp. 599-616.

[6] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition", *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, 2009, pp. 1-6.

[7] CSA, "*Security Guidance for Critical Areas of Focus in Cloud Computing"*, 2009, Cloud Security Alliance.

[8] P. A. Dustin Amrhein, A. De Andrade, E. A. B. Armstrong, J. Bartlett, R. Bruklis, and K. Cameron, "Cloud computing use cases", *White Paper*. Version 3.0 ed., 2010, pp. 1-7.

[9] T. Grance, "The NIST Cloud Definition Framework" 2010, National Institute of Standards and Technology (NIST).

[10] M. Armbrust et al. "Above the clouds: A Berkeley view of cloud computing", *EECS Department, University of California*, Berkeley, Tech. Rep. UCB/EECS, 2009.

[11] S. Pearson, "Taking account of privacy when designing cloud computing services", *ICSE Workshop on Software Engineering Challenges of Cloud Computing*, 2009, p. 44.

[12] Z. Gansen, R. Chunming, L. Jin, Z. Feng, and T. Yong, "Trusted data sharing over untrusted cloud storage providers", *Second International Conference on Cloud Computing Technology and Science*, 2010, p. 97.

[13] P. Kresimir and H. Zeljko, "Cloud computing security issues and challenges", *MIPRO*, 2010, Opatija, Croatia.

[14] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenge", *Proceedings of the 33rd International Convention*, 2010, p. 344.

[15] R. Gellman, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing", *World Privacy Forum*, 2009, accessed on June. 2013, available at: http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

[16] IDC, "Enterprise panel", 2009, accessed on July. 2013, available at: http://www.slideshare.net/JorFigOr/cloud-computing-2010-an-idcupdate.

[17] CSA, "Top threats to cloud computing", 2010, Cloud Security Alliance (CSA).

[18] Regulation of Investigatory Powers Act (RIPA), Part II, 2000, UK.

[19] M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "Technical security issues in cloud computing", *IEEE International Conference on Cloud Computing*, 2010, p. 109.

[20] J. A. Hall and S. L. Liedtka, "The sarbanes-oxley act: Implications for large-scale IT outsourcing", *Communications of the ACM*, vol. 50, no. 3, 2007, pp. 95-100.

[21] D. Rousseau, S. Sitkin, R. Burt, and C. Camerer, C. "Not so different after all: A cross-discipline view of trust", *Academy of Management Review*, vol. 23, no. 3, 1998, pp. 393-404.

[22] D. Osterwalder, "Trust through evaluation and certification?", *Social Science Computer Review*, vol. 19, no. 1, 2001, pp. 32-46.

[23] H. Nissenbaum, "Can trust be secured online? A theoretical perspective", *Etica e-Political*, no. 2, 1999.

[24] S. Giff, "*The Influence of Metaphor, Smart Cards and Interface Dialogue on Trust in e-Commerce"*, 2000, University College London.

[25] J. Nielsen, "Trust or bust: Communicating trustworthiness in web design", *Jacob Nielsen's Alert Box*, 1999, accessed on July. 2013, available at: http://www.useit.com/alertbox/990307.html.

[26] S. Pearson, M. Casassa Mont, and S. Crane, "Persistent and dynamic trust: Analysis and the related impact of trusted platforms", *Trust Management*, LNCS 3477, ed: P. Herrmann, V. Issarny, and S. Shiu, 2005, pp. 355-363.

[27] A. Tweney and S. Crane, "Trust guide 2: An exploration of privacy preferences in an online world", *Expanding the Knowledge Economy*, 2007, IOS Press.

[28] S. Paquette, P. T. Jaeger, and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing", *Government Information Quarterly*, vol. 27, no 3, 2010, pp. 245-253.

[29] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", *Journal of Network and Computer Applications*, vol. 34, no. 1, 2010, pp. 1-11.

 ISBN: 978-1-61208-338-4

[30] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing", *Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science*, IEEE Press, Nov. 2010, pp. 693-702.

[31] A. Sangroya, S. Kumar, J. Dhok, and V. Varma, "Towards analyzing data security risks in cloud computing environments", *Communications in Computer and Information Science*, vol. 54, 2010, pp. 255-265.

[32] M. Nelson, "Building an open cloud", *Science*, vol. 324, 2009, p. 1656.

[33] B. Sotomayor, R. Montero, I. Lorente, and I. Foster, "Virtual infrastructure management in private and hybrid clouds", *IEEE Internet Computing*, vol. 13, 2009, pp. 14-22.

[34] T. Harmer, P. Wright, C. Cunningham, and R. Perrott, "Provider-independent use of the cloud", *The 15th International European Conference on Parallel and Distributed Computing*, 2009, p. 465.

[35] Unified Cloud Interface (UCI) 2010, accessed on August. 2013, available at: http://code.google.com/p/unifiedcloud/.

[36] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The eucalyptus open-source cloud computing system", *Proceedings of Cloud Computing and Its Applications, 2008.*

[37] P. Mathur and N. Nishchal, "Cloud computing: New challenge to the entire computer industry", *The1st International Conference on Parallel, Distributed and Grid Computing (PDGC*), 2010, p. 223.

[38] L. Wang, J. Tao, and M. Kunze, "Scientific cloud computing: Early definition and experience", *Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications*, 2008, Dalian, China.

[39] L. Wang, G. Von Laszewski, A. Younge, X. He, M. Kunze, J. Tao, and C. Fu, "Cloud computing: A perspective study", *New generation Computing*, vol. 28, 2010, pp. 137-146.

[40] E. Clemons and Y. Chen, "Making the decision to contract for cloud services: Managing the risk of an extreme form of it outsourcing", *Proceedings of 44th Hawaii International Conference on System Sciences*, Hawaii, 2011, pp. 1-10.

[41] A. Velte, T. Velte, and R. Elsenpeter, R. "Cloud Computing a Practical Approach', McGraw-Hill, USA, 2010.

[42] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and Grid computing 360-degree compared", *Proceedings of Grid Computing Environments Workshop*, Austin, TX, 2008.

[43] T. Dillion, C. Wu, and E. Chang, "Cloud computing: Issues and challenges", *Proceedings of 24th International Conference on Information Networking and Applications*, 2010, Perth, WA.

[44] Y. Sohan and H. Zeng, "Cloud: A computing infrastructure on demand", *Proceedings of 2nd International Conference on Computer Engineering and Technology*, 2010, Chengdu, China.

[45] S. Bhardwaj, L. Jain, and S. Jain, "Cloud computing: A study of infrastructure as a service (IaaS)", *International Journal of Engineering and Information Technology*, vol. 2, no. 1, 2010, pp. 60-63.

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

[47] S. Alshomrani and S. Qamar, "Cloud based e-government: benefits and challenges", International Journal of Multidisciplinary Sciences and Engineering, vol. 4, no. 6, 2013, pp. 1-7.

[48] F. A. Alvi, B. S. Choudary, N. Jaffery, and E. A. Pathan, "Review on cloud computing security issues and challenges", Department of Electronic Engineering, QUEST Nawabshah, Sindh, Pakistan, 2011.

[49] N. Yadav and V. B. Singh, "E-governance: past, present and future in India", *International Journal of Computer Applications*, vol. 53, no. 7, 2012, pp.36-48.

[50] D. Karunanithi and B. Kiruthika, "Efficient framework for ensuring the effectiveness of information security in cloud computing, *International Conference on Signal, Image Processing and Applications*, workshop of ICEEA, 2011.

[51] D. Catteddu and G. Hogben, "Cloud computing: Benefits, risks and recommendations for information security', *European Network and Information Security Agency* (ENISA), 2009.

[52] B. Zwattendorfer, K. Stranacher, A. Tauber, and P. Reichstädter, "Electronic government and the information system perspective", *International Conference on Network and System Security*, 2011, pp.1-6.

[53] T. Hariguna, "Prototype cloud computing for e-government in Indonesia", *International Journal of Engineering & Technology*, vol. 11, no. 6, 2011.

[54] K. Irion, "Government cloud computing and the policies of data Sovereignty", *22nd European Regional Conference of the International Telecommunications Society*, Budapest, Economic and Policy Issues, 2011.

[55] H. M. Nezhad, B. Stephenson, and S. Singhal, "Outsourcing business to cloud computing services: Opportunities and challenges", *IEEE Internet Computing, Special Issues on Cloud Computing*, 2009, pp. 1-10.

[56] M. O'Gara, "Washington itching to take the lead on cloud computing", 2009, SOA, accessed on December. 2013, available at: http://govit.sys-con.com/node/1055764.

[57] T. Dillon, C. Wu, and E. Chang (2010). Cloud Computing: Issues and Challenges', 24th IEEE International Conference on Advanced Information Networking and Applications, 2010, pp. 1-7.