Cloud computing is an emerging technology. This new paradigm eases physical limitations of traditional data centers and brings extensive and powerful computational, storage and software resources to users who previously could not afford them. Cloud providers offer information and technology utility services with similar functionalities in various configurations and different pricing plans. Often the differentiating factor might be a non-functional property of the system called trust. Trust may be the basis for both predicting behavior of the provided services and selecting the provider of the services. But trust is based on information. There is a need to have sufficient information about providers and their services to establish trust. Since trust is a human perception, its not just the identified facts about a cloud environment that impact decision making and trust, but also perceptions of users about these facts. The key question being examined in this work is “How much and what information can a potential cloud user obtain directly from provider web-sites, and how can that information impact trust towards that provider?”.

To discuss metrics, perceptions and components of trust in the context of cloud computing, we first identify elements we believe are needed to build trust. We present a framework that identifies elements, such as services, components, capabilities and resources, of a “good” cloud. Some of these elements are reliability, availability, security, privacy, fault-tolerance, virtualization, networking capability, appropriate APIs, data, authentication, authorization, accounting, various levels of support, provenance, policy management, etc. Given the framework, we then examined literature - popular press, aca-
ademic and industry papers and documents etc., to understand what users might perceive as principal components of trust in the context of cloud computing. Identified trust building metrics were then correlated with the framework components and analyzed. We find that the principal trust components appear to be reliability, availability, security, data management, cost (potential gains and losses) and competence of the provider. The order of preference changes with user and the context. We then construct a user-perspective trust model and use it to compare five major cloud providers against identified trust metrics with inputs derived solely from information available to users first-hand from vendor web-sites. Second hand information (such as third-party reports) is used to discuss the model and the results. Some metrics are on interval and ratio scale, but more are on ordinal scale. For example, most of the cloud providers assure security to their customers or potential customers through certifications or by describing their security processes in white papers. None appear to provide direct information about security (e.g., number of security breaches). Some offer auxiliary information regarding their security controls, for example, by answering Cloud Security Alliance’s Consensus Assessment Initiative Questionnaire. Results indicate that all major cloud providers seem to have some surprising gaps either in how they actually operate, or in what information and how much they provide to potential users first-hand. For example, four out of five providers appear to lack in their openness about security and in their data management practices. For two out of five interoperability appears to be an issue. On the other hand, all appear to be willing to sign SLAs that promise at least 99.9% uptime. Cost of similar services vary by a factor of two or more among the providers. It is not surprising that surveys of potential customers (such as those conducted by IDC) and state-of-cloud-security assessments, such as those done by CSA, confirm that security and data management remain top concerns regarding that industry.
Trust Metrics for Cloud Computing

by
Sai Rajesh Tallamraju

A thesis submitted to the Graduate Faculty of
North Carolina State University
in partial fulfillment of the
requirements for the Degree of
Master of Science

Computer Science
Raleigh, North Carolina
2013

APPROVED BY:

--------------------------
Dr. Laurie Williams

--------------------------
Dr. Ting yu

--------------------------
Dr. Mladen A. Vouk
Chair of Advisory Committee
DEDICATION

To my beloved parents and brother; without their love, support and encouragement none of this would be possible.
BIOGRAPHY

Tallamraju Sai Rajesh was born in Hyderabad, Andhra Pradesh in India. He received his Bachelor’s degree in Computer Science and Engineering from Vasavi College of Engineering which is affiliated to Osmania University, Hyderabad in May 2008. Upon completion of Bachelors, he joined a linux mobile start-up Azzo Soft Systems as Software Engineer in Cloud Services team and worked for almost 3 years. Later, he went forward to pursue his Masters in Computer Science at North Carolina State University from August 2011 to May 2013.

Besides professional life, he likes to read live blogs from industry experts on various topics related to cloud, mobile. Also enjoys swimming and watching movies. He is expected to work for NetApp Inc, starting June 2013.
ACKNOWLEDGEMENTS

I would like to thank my parents and my brother for their constant love, faith and support in me. Without my brother steady encouragement, this would not have happened.

I am immensely grateful to my advisor Dr. Mladen A. Vouk for spending time during initial days in understanding my interests and helping me to focus my attention onto a particular topic. I am thankful for all the insightful discussions, guidance, feedback and the trust he had in me all through the research work. Thank you for being patient in correcting my writing. I would like to thank Dr. Ting Yu for making his course valuable and knowledgeable and Dr. Laurie Williams for her valuable help and graciously agreeing to be in the thesis committee.

This work was supported in part by NSF grant 0910767, the U.S. Army Research Office (ARO) grant W911NF-08-1-0105 managed by NCSU Science of Security Initiative and Science of Security Lablet, and IBM Share University Research and Fellowships program funding.
# TABLE OF CONTENTS

**LIST OF TABLES** .......................... vii

**LIST OF FIGURES** .......................... viii

**Chapter 1 Introduction** .......................... 1
   1.1 Motivation .................................... 1
   1.2 Cloud Computing .................................. 2
      1.2.1 Cloud Computing Characteristics ......................... 2
      1.2.2 Service Models .................................. 3
      1.2.3 Deployment Models ................................ 6
   1.3 Trust ......................................... 7
   1.4 Related Work .................................... 8

**Chapter 2 Trust and its principles** .......................... 10
   2.1 Definition ...................................... 10
   2.2 Principles of Trust ................................. 14
      2.2.1 Trust is based on information, beliefs and metrics .......... 14
      2.2.2 First hand information ................................ 15
      2.2.3 Third party ratings .................................. 15
      2.2.4 Provider’s identity .................................. 15
      2.2.5 User preferences .................................... 16
      2.2.6 Relationship properties ................................. 16
      2.2.7 Global and Local score .............................. 17
      2.2.8 Dynamic nature ..................................... 17
      2.2.9 Deepens over time and with increased reciprocity ........... 17
      2.2.10 Risk ........................................... 18
      2.2.11 Error rate ....................................... 18
      2.2.12 Approaches ...................................... 19

**Chapter 3 Trust Metrics for Cloud Computing** .......................... 20
   3.1 Approach ........................................ 21
   3.2 Components/Capabilities ............................. 22
      3.2.1 Reliability ...................................... 23
      3.2.2 Availability ...................................... 25
      3.2.3 Scalability ....................................... 26
      3.2.4 24/7 Support ..................................... 27
      3.2.5 Performance ...................................... 27
      3.2.6 Pay per Use ...................................... 28
      3.2.7 Time to Market .................................... 28
<table>
<thead>
<tr>
<th>Table</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Control between provider and clients [42]</td>
<td>32</td>
</tr>
<tr>
<td>3.2</td>
<td>Industry standards [97]</td>
<td>35</td>
</tr>
<tr>
<td>3.3</td>
<td>Service trust components - how we measure them in this study</td>
<td>40</td>
</tr>
<tr>
<td>3.4</td>
<td>Privacy regulations [97]</td>
<td>44</td>
</tr>
<tr>
<td>3.5</td>
<td>Cloud Provider trust components</td>
<td>47</td>
</tr>
<tr>
<td>4.1</td>
<td>Trust evaluation parameters for five cloud providers</td>
<td>58</td>
</tr>
<tr>
<td>4.2</td>
<td>Trust evaluation parameters for five cloud providers (Service age in years, Support, Security, Scaling, API, Tools, Interoperability, Data Management - 0 is least satisfactory, 2 is most satisfactory)</td>
<td>66</td>
</tr>
<tr>
<td>4.3</td>
<td>Trust evaluation for cloud providers - normalized</td>
<td>68</td>
</tr>
<tr>
<td>A.1</td>
<td>Cost</td>
<td>92</td>
</tr>
<tr>
<td>A.2</td>
<td>Vendor experience</td>
<td>92</td>
</tr>
<tr>
<td>A.3</td>
<td>Support</td>
<td>93</td>
</tr>
<tr>
<td>A.4</td>
<td>Certifications</td>
<td>94</td>
</tr>
<tr>
<td>A.5</td>
<td>Protection</td>
<td>95</td>
</tr>
<tr>
<td>A.6</td>
<td>Scalability</td>
<td>96</td>
</tr>
<tr>
<td>A.7</td>
<td>API</td>
<td>96</td>
</tr>
<tr>
<td>A.8</td>
<td>Monitoring Tools</td>
<td>97</td>
</tr>
<tr>
<td>A.9</td>
<td>Monitoring Tools</td>
<td>98</td>
</tr>
<tr>
<td>A.10</td>
<td>Data Management</td>
<td>98</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1.1</td>
<td>Cloud service architecture [10]</td>
<td>5</td>
</tr>
<tr>
<td>Figure 3.1</td>
<td>Bubble Framework [48]</td>
<td>22</td>
</tr>
<tr>
<td>Figure 4.1</td>
<td>Reliability &amp; availability comparison</td>
<td>69</td>
</tr>
<tr>
<td>Figure 4.2</td>
<td>Security comparison</td>
<td>71</td>
</tr>
<tr>
<td>Figure 4.3</td>
<td>Scaling, API, Cost and Credit comparison</td>
<td>72</td>
</tr>
<tr>
<td>Figure 4.4</td>
<td>Data management, Tools and Interoperability comparison</td>
<td>73</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

1.1 Motivation

Increasing demand for new and more cost-effective information technology (IT) utility services is creating a constant pressure to expand IT infrastructure and meet the demand. To address this challenge, a new architecture called cloud computing was developed. Cloud computing is a service oriented paradigm and architecture that optimizes user overhead, costs and other benefits by offering services at different levels via different service models, provisions services and its parts from diverse providers. The problem with this kind of provisioning is that by necessity service oriented architecture may require hiding of complexity, and thus a certain level of opacity from the end-user experience. Lack of transparency is not conducive of trust. It may mask the very information needed to generate the evidence based confidence that leads to trust. At the same time, presence of many players with different motives and providers with similar services in the market complicates the issue. On the other hand, new consumers who wish to adopt cloud computing may be reluctant to do so because of trust deficits. Unfortunately what
comprises trust and how much of that is measurable in a repeatable way remains elusive. Trust very often has a very large human component.

Under cloud computing paradigm, an organization confers a high level of trust onto the cloud provider. The challenge is to identify and reliably assess characteristics, parameters, metrics etc., that are important to a user or an organization and map it onto the cloud provider and its cloud. The overall goal of this study is to survey and identify trust metrics that appear to be relevant to cloud computing from consumer perspective.

1.2 Cloud Computing

US National Institute of Standards and Technology (NIST) defines cloud computing as “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. The NIST model is composed of five essential characteristics, three service models and four deployment models [99].

1.2.1 Cloud Computing Characteristics

Cloud computing has five fundamental characteristics [99]:

**On-demand self service** “A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service’s provider” [99].

**Broad network access** “Capabilities are available over network and accessed through standard mechanisms” [99].

**Resource pooling** “The provider’s computing resources are pooled to serve multiple
consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and re-assigned according to consumer demand” [99].

**Rapid elasticity** “Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in” [99].

**Measured service** “Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usage can be monitored, controlled and reported, providing transparency for both the provider and consumer of utilized service” [99].

### 1.2.2 Service Models

Service model to which a cloud conforms dictates an organization’s scope and control over the computational environment and characterizes the level of abstraction for its use. Three well-known and often used service models are briefly described below [84]. An illustration of cloud services architecture is presented in Figure 1.1

- **Software as a Service:** “Software as a Service is a model of service delivery whereby one or more applications and the computational resources to run them are provided for use on demand. Its main purpose is to reduce the total cost of hardware and software development, maintenance and operations. The cloud consumer does not manage or control underlying cloud infrastructure or individual applications, except for preference selections and application settings” [84].
  
  Examples: Google Docs [71], Salesforce CRM [125]

- **Platform as a Service:** “Platform as a Service is a model of service delivery whereby computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost
and complexity of buying, housing and managing the underlying hardware and software components of the platform, including any needed program and database development tools. The development environment is typically special purpose, determined by the cloud provider and tailored to the design and architecture of its platform” [84].

Examples: Windows Azure [139], Google App Engine [72], Virtual Computing Laboratory (VCL) Desktop Services [80]

- **Infrastructure as a Service:** “Infrastructure as a Service is a model of service delivery whereby the basic computing infrastructure of server, software and network equipment provided as an on-demand service upon which a platform to develop and execute applications can be established. Its main purpose is to avoid purchasing, housing and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualized objects controllable via a service interface. The cloud consumer has broad freedom to choose the operating system and development environment to be hosted” [84].

Examples: Amazon EC2 [14], Rackspace Cloud Servers [113], Virtual Computing Laboratory (VCL) [80]

Overall, cloud computing is not restricted to Infrastructure/Platform/Software as a Service, it can be further extended to provide variety of service models. Armbrust et al. [21] coin the phrase “X as a Service (XaaS)”; values of X can be any possible service that can be provided to consumer as a service.
Figure 1.1: Cloud service architecture [10]
1.2.3 Deployment Models

Similar to type of service models cloud may be hosted and deployed in different fashions depending on use cases. Below are four deployment models for cloud services, with derivate variations that address specific requirements [10].

- **Public Cloud**: “The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services” [10].

- **Private Cloud**: “The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off-premises” [10].

- **Community Cloud**: “The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy or compliance considerations). It may be managed by the organizations or third-party and may exist on on-premises or off-premises” [10].

- **Hybrid Cloud**: “The cloud infrastructure is a composition of two or more clouds (private, public or community) that remains unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds)” [10].

“With customer demand and mature market offerings, we have other derivative cloud deployment models emerging like virtual private cloud - a way of utilizing a public cloud infrastructure in a private or semi-private manner and interconnecting these resources to internal resources of a consumers’ datacenter, usually via virtual private network (VPN) connectivity” [10].
1.3 Trust

Trust is a very broad concept that has been investigated for centuries in fields as diverse as sociology, psychology, economics, politics, philosophy and now computer science. There is no consensus in literature on what trust is and what constitutes trust decision. Hussain et al.[76] enumerate various definitions of trust and every definition is accepted and contested. Trust escapes clear definition despite having many definitions. Yet everybody recognizes it immediately. “Trust is recognized as an essential element of every social transaction but it can be hardly found in any written contract and is even less likely to be enforced. Trust escapes rational judgment yet everybody seems to be expert in judging trust. Trust is what happens between people or communities, is not easily quantifiable, takes time and effort to build and can be easily lost. It’s a belief in competence or expertise of other’s such that you feel you can rely on others to care for your assets” [39].

From technology perspective, trust has always been associated with reliability and security. In distributed computing systems, trust was effectively managed through constructs like trusted domains (several computers trusting each other’s authentication capabilities), trusted credentials (other’s identities accepted without any proof), trusted zones (privileged Internet address space) etc. More recently, the recognition of the fundamental nature of trust has been addressed in initiatives such as Trusted Computing, where individual devices are given assurance in their own configuration on the basis of a highly-protected, hardware-based root of trust [74].

But why is trust very important in research world? With trust, more people and enterprises enter on-line world and will interact with others. If we establish trust on-line, attitude towards on-line transactions changes. Trust makes interactions and transactions lively and invites further new investment, transactions and so on. Without trust, every
one becomes suspicious of their transactions. The same applies to cloud, if a trusted environment is set up, it attracts more enterprises to adopt cloud which invites new players into market, healthy competition and enforcement of strong mechanisms that ensures a healthy cloud.

1.4 Related Work

This work supplements with other industry efforts in ensuring trust among customers towards cloud computing. Industry works include Cloud Trust Protocol (CTP) 2.0 [44] is a question and answer protocol that enables clients to ask provider about configuration, vulnerability, access, authorization, policies, accountability, reliability and operating status they are interested in depending on the context and allows provider to prepare and deliver information in response to requests in best way possible to them. The next version of this protocol 3.0 with explicit request and response format is still under expert review and is scheduled to be released for public review in second half of 2013 [8]. Another trust initiative include, Cloud Security Alliance’s (CSA) Cloud Controls Matrix [12], this matrix provides fundamental security principles to guide providers and assists customers in assessing the overall risk of a cloud provider. It includes 100 questions related to 13 domains CSA identified related to security concepts and principles. For providers and customers interested in yes/no answers, CSA’s Consensus Assessment Initiative Questionnaire [11] includes 140 questions related to security risks and principles that can help both provider and customer assess the controls in place. Apart from industry efforts, FedRAMP [5] is a federal government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud services. Through this ongoing security assessments, the program makes sure that deployed
security controls remains effective with new changes in system, environment and against new exploits and attacks. Apart from US efforts, Asia Cloud Computing Association (ACCA) [4] has prepared a Cloud Assessment Tool (CAT) [134] to enable prospective users of cloud computing to objectively access the operational performance and other critical capabilities offered by different providers based on eight operational categories like security, performance, long-term support, connectivity, certification, interoperability, data center basics and access (connectivity). European Commission with help of DMTF [47], ETSI [57], SNIA [131], ITU [83], IEEE and major industry players like Microsoft, VMware etc., started an initiative called SIENA (Standards and Interoperability for eInfrastructure implemeNTation initiAtive) [129] for co-ordinating the effort of developing inter-operable and standardized cloud standards. Such an initiative enable a competitive, open and secure environment in public cloud market and provide a common criteria to assess operational characteristics of different cloud providers. However, EU initiative is still in road-map phase till end of 2013. All these efforts including this work, is a step towards ensuring transparency into cloud operations, measuring operational characteristics and assuring trust.

The rest of this work is organized as follows: In chapter 2, we understand trust by discussing the concept of trust and its principles. In chapter 3, based on understanding of trust, we identify trust components in the context of cloud computing with help of an evaluation framework [48]. In chapter 4, we develop a user-perceivable trust assessment model based on identified trust components and compare five major cloud providers to see how much information does a potential customer get from their websites and how does that information impact the trust decision. And finally in chapter 5, we end this study with conclusion and discussion of future work.
Chapter 2

Trust and its principles

As more providers offer information utility services with similar functionalities, the task of which provider and which services to use becomes more interesting and challenging. The key factor is trust. Trust facilitates interaction in uncertain and risky environments. Trust makes the uncertainty and complexity tolerable. “Trust also reduces the complexity in a given scenario because user will have less number of options to consider. Humans, if faced with a full range of alternatives, if forced to acknowledge and calculate all possible outcomes of all possible decision nodes, would freeze in uncertainty and indecision. In this state, we might never be able to act in situations that call for action and decisiveness” [107]. To identify trust metrics for cloud, we must first understand trust concept and its components.

2.1 Definition

There does not appear to be consensus in the literature on what trust is. There is extensive research on trust in the fields of philosophy, psychology, management, business,
marketing, e-commerce, etc. There is no common agreement across all disciplines regarding definition of trust. Each of these disciplines produced their own definition and concepts. For example, Hussain et al. in [76] list various definitions of trust from the literature. All definitions have both supporters and detractors. Corritore et al in [41] clarifies ‘what trust is not’ in order to understand trust. Trust is not cooperation, trustworthiness, competence, and faith. “Trust is an act of a trustor(who trusts other entity).” In contrast,

- Cooperation is either a cause or a manifestation of trust rather than trust itself.

- Trustworthiness is a characteristic of someone or something that is the object of trust.

- Competence is only one of many cognitive cues for trust but trust goes beyond a belief in the competence of the object.

- Faith involves taking a leap that is not fully supported by reason whereas trust encompasses a reason.” [41]

On the other hand, for some entities these characteristics may be the key ingredients of trust and may in fact be a deciding factor in their decisions about trust. We adopted trust definition from [87] that we believe fits cloud scenario. “Trust means act of confidence and reliance in something that’s expected to behave or deliver as promised”. However, it is important to say that in the context of cyber-security and safety, trust definition needs to be expanded to include not only expected behavior but also avoidance and prevention of unexpected behavior. For example, when trust is expressed in terms of reliability, the definition might also include what should not happen like data loss or data
compromise in addition to mentioning of desired features like fault tolerance, redundancy etc. Establishing trust on-line is important but so is maintaining that on-line trust.

To obtain and maintain trust, one must have an overview of how trust is induced by understanding different entities (players) involved and different types of interactions: human-human, human-organization, human-machine, machine-machine. For human-human trust [94] [104], an entity in general shall try to choose the most reliable partner from a pool of potential partners and devise a strategy to achieve their utility. There are number of ways of doing this. Firstly, they could interact with each of the partner and learn about their behavior. Secondly, when direct reach is not possible, entity could ask others about their perception of the partner. The opinion from a source who possess similar capabilities as trustor is more important than opinion of the party who does not have those characteristics. Thirdly, entity could characterize the motivations of other partners, and form beliefs about their characteristics and reasoning behind the motivations in order to decide how much to trust them. For example, partner might act as expected because partner believes that such act would gain him/her business benefits and reputation which further invites good business. Eventually, this should lead to selection of most reliable and honest partner.

For human-organization trust, disciplines such as law, economics and finance ensure trust through formal mechanisms like written contracts, legislations and the like. For example, in credit card purchasing we unknowingly trust the transaction partner because we are assured that laws and procedures from credit report bureaus, justice system etc., will act against defectors who break the laws.

For human-machine and machine-machine trust, there is a vast research to formalize trust into computational methods through different trust models like learning based and reputation based. Through a learning strategy, entity with multiple interactions learn
about behavior of the partner and their tendency to fail in an interaction. From this, entity can assume sufficient information (strategies, payoffs) and can strategically respond by assessing the best possible move of their opponent. In case of reputation based trust model, trust is mainly derived from aggregation of opinions and experiences. The main task in this method, remains in retrieving and propagating the ratings. Singh et al. [140], [141] proposed methods to disseminate and gather required information through the network. They show how agents explore the network by contacting the neighbor and use referrals gathered to gradually build up a social network. However, these models are computationally expensive when considering all factors affecting trust at component level. So, set of mechanisms and protocols were developed at system level that force interaction partners to behave in trustworthy manner. These mechanisms eliminate the need of developing trust mechanisms at individual component level. One such mechanism include security. Trust is ensured by the fact that a user has to prove their identity through authentication mechanisms(username and password, digital certificates etc.) before accessing a service of entity. Ramchurn et al. [122] which internally refers to [111] proposes a number of security requirements that are necessary to induce trust. The requirements include identity, access permissions, content integrity and content privacy. These basic requirements can be implemented through public key models (like PGP, X.509) and certification infrastructure.

To understand how a trust model instills trust among users and motivates them to click/open a website/email, we conducted a literature survey on “how phishing works”. Rachna et al [46] summarize malicious strategies and empirically proves that visual deceptions like deceptive text, animated images, trusted third-party logos from entities like Verisign, TRUST-e, lack of knowledge about security indicators like padlocks, https and lack of computer knowledge about domains, cousin domains, ip addresses etc., deceive
users to believe phishing websites as legitimate ones. To understand nature of trust, we shall below list principles of trust relevant to this study summarized from [45], [107] and [41].

2.2 Principles of Trust

2.2.1 Trust is based on information, beliefs and metrics

There must be sufficient information about other entity to establish trust in the context of beliefs, opinions and metrics of atleast one party. But what information should we use to build trust? Every entity has many dimensions and depending on trustor requirements he/she must consider relevant information as each requirement seek different properties. Also, trust has many dimensions and the challenge remains in mapping trust model of a trustor(who trusts other entity) to the trust model of a trustee(object of trust). For example: a customer wants to subscribe to a simple database service. Later customer may need to scale-up and scale-out and might require a database service that is distributed, fault-tolerant and highly available. If the customer is aware of his needs ahead of time, it may affect the trust decision with respect to service provider who has limited scaling capabilities. If the customer does not know that ahead of time, trust may be warranted at the time, but perhaps a misplaced one. On other hand, the provider may want the business of the customer, and may not inform the user of all limitations or may imply capabilities that may not coincide with the user profile. This may result in miscalculation of trust towards trustee and in an eventual trustee disappointment [45].
2.2.2 First hand information

Information that service providers provide themselves is critical to development of trust. For example, information about performance, security, privacy and few QoS parameters (response time, throughput, latency) are being considered by many sites to establish trust. If this information is directly provided by service provider, trust develops [7].

2.2.3 Third party ratings

Trust is greatly influenced by opinions of the people who had interaction with provider earlier. Experiences of the person who had similar transaction are highly valued. In off-line world, we have friends and acquaintances who give personal opinions based on their experience, whereas in on-line world community forums and trusted third parties consolidate all user experiences and opinions. These trusted third parties allows an entity to gather ratings of other entities even without having direct experience. Seals from trusted third-party organizations like TRUSTe, Verisign, ISO induce trust about site or transaction. These seals certify that organization or sites conform to the standards laid [24].

2.2.4 Provider’s identity

Trust depends on identity. Because identity acts as a hash tag that helps in categorizing all history transactions user(customer) have with the subject (provider). From this history, we can refer to past experiences that hint trust or betrayal. In off-line world, identity can be established by visual recognition or authoritative tokens like driver license’s and passports. But in on-line world, providers may have virtual identities whose mapping to their identities in off-line world are masked and few providers remain anonymous. But as
long as identifying tokens remain constant, they can be used to group all past experiences [45]. In on-line world, identifying tokens include user names, digital tokens etc.

### 2.2.5 User preferences

Trust changes with change in user and their preferences. Because every user have their own preference over other system properties. So, a provider might be assigned a different trust value depending on user and his/her preference. For example, a financial services customer might prefer a provider who promises 100% availability against the provider who offers highly exceptional security controls and comparatively low availability percentage. But the choice differs with the change in customer who prefers security over availability.[7].

### 2.2.6 Relationship properties

Trust is established between a trustor and a trustee. Trustor trusts trustee with respect to its ability to perform a specific action within a specific context. In some interactions, trustor and trustee can be either a single entity or multiple entities, forming different combinations of relationship (one-to-one, one-to-many, many-to-one, many-to-many). Trust may be symmetric or transitive but not always. For example, if user trusts his/her doctor and doctor trusts a specialist, then user may trust specialist. Degree of trust changes with change in context. For example, a higher level of trust is needed for executing code in system owned by other than just writing a new file and writing a new file requires a higher level of trust than for reading a file [7].
2.2.7 Global and Local score

Massa et al. [96] mentions about two different kind of trust metrics: global and local trust score to measure trustworthiness of trustee. “Global trust metrics assign to a given user a unique trust score, the same independently of the user that is evaluating other user’s trustworthiness. On the other hand, a local trust metric provides personalized trust score that depends on the point of view of the evaluating user” [96]. In global trust score, score is based on the opinions or experiences from the general population, which is public and visible to all the members. But global trust score might be calculated based on some falsified information provided by anonymous users. While in personalized/local score, the value is built on the opinions/experiences from a group of members/participants selected by evaluating user. The local trust score is therefore influenced by user’s social network, interests, preferences, priorities etc. For example, user considers global trust score while selecting a weather forecast service, because personalization is not important.

2.2.8 Dynamic nature

Trust is dynamic. Trust increases or decreases with further experiences. Trust also decay with time. New experiences are more important than old ones since old experiences may become obsolete or irrelevant as time pass by. So, one must constantly evaluate trustworthiness of the trustee.

2.2.9 Deepens over time and with increased reciprocity

To establish trust between entities, initial trust formation is very important. A transaction involving two parties do not takes place unless any party involved in transaction moves first and have a certain level of trust that second will fulfill its said promises.”Trust
is associated with risk and when a trustee realizes that a trustor has taken considerable risk in trusting them, they tend to be motivated to behave in a trustworthy manner. Such reciprocity has been found to be key element in trust building” [45]. This is a crucial stage in any trust relationship. In next phase, both entities tries to stabilize trust based on interactions and opinions/recommendations from other parties with similar characteristics.

2.2.10 Risk

Trust is a function of the perception of the risk. Trust only exists in a risky and uncertain environment. If trustor has a higher control, he/she has less need to trust the trustee. “Risk is the core of trust in that trust is the degree to which a trustor holds a positive attitude toward the trustee’s goodwill and reliability in a risky exchange situation” [45]. But Nissenbaum [107] argues that where people are guaranteed safety, where they are protected from harm via assurances, when the other party act under coercion, trust is redundant. Also, penalties and rewards are necessary to support trust intention when something go wrong.

2.2.11 Error rate

Errors have strong effect on trust. Corritore et al. [41] mentions that level of trust fall is proportional to magnitude of error. If error is not repeated, performance can recover immediately but regaining trust to level prior to error takes long time. Recovery of trust can happen if user is able to understand the cause and compensate for the errors but not to the level prior to errors.
2.2.12 Approaches

Different approaches help build and evolve trust. These approaches include direct experience (builds trust after utilizing services), third party (builds trust after gathering information like reputation, recommendations through third parties), automated trust negotiation (builds mutual trust, i.e., through usage of credentials) and hybrid (builds trust by combination of other approaches) [7]. Degree of trust varies with different approaches. Trust established through direct experience approach is much valued than trust formed through other approaches.

Leveraging on different trust interactions between entities, different components of trust in terms of different words related to trust [85] and trust principles, we obtain an overview of trust and what factors to be considered while establishing trust. With this understanding of trust, chapter 3 identifies list of trust components in the context of cloud computing based on literature survey.
Chapter 3

Trust Metrics for Cloud Computing

Customers of cloud service, like all customers in other areas, need a way of differentiating among similarly presented services from different providers. A differentiating factor might be trust. Trust is contextual and is based on information, customer may consider. It is difficult to determine what information should be used. Trust has many dimensions and a service provider is free to choose any dimension towards instilling trust among customers or potential customers. For example, a service provider can focus on reliability as its trust metric. Another provider might use security and compliance to standards as its trust metric. Of course, requestor (or customer) has his/her own preference of service properties. For example, a financial services customer may prefer high availability over exceptionally high security and may consider information appropriate to those aspects to build trust. This chapter discusses trust metrics in context of cloud computing.
3.1 Approach

In this work, it was decided to focus on information available in the literature, popular press and academic and industry white papers, reports and documents to understand what a user and provider might perceive as metrics and components of trust in the context of cloud computing. We conducted a literature search on materials written in English.

In order to assess metrics for cloud computing and how they are related to users and providers, we need an evaluation framework that identifies desirable components/capabilities/characteristics that make a “good” cloud. We have identified eight frameworks of interest. The frameworks are SLA-based framework [26], TrustCloud framework [89], SMICloud [59], Armor framework [90], Control Objectives for Information and Related Technology (COBIT) [22], NIST SP800-55 [133], SANS Security Metrics [109], and Bubble Framework [48].

SLA-based framework evaluates trustworthiness of provider using identified parameters from SLA. TrustCloud framework assures trustworthiness of cloud through the use of detective controls like auditability and accountability. SMICloud proposes a comparison framework which measures quality and prioritize cloud services. Armor framework assures trustworthiness of cloud by constantly monitoring and evaluating the behavior of each component using historical data. The above four frameworks were published in academic papers and lack industry acceptance. SP800-55 framework was specially designed for US government and might not be universally accepted. SANS Security Metrics discusses construction of metrics and is security focused. COBIT framework focuses more on business and aims at ensuring organizations meet business objectives by managing IT risks [22]. While all of the identified frameworks are relevant and have something to
contribute, they did not cover the full range of measures one may need to have in a cloud. We therefore decided to use a framework, called Bubble framework [48] that covers all key characteristics that a “good” cloud needs to have.

3.2 Components/Capabilities

![Bubble Framework](image_url)

Figure 3.1: Bubble Framework [48]
The diagram in Figure 3.1 attempts to encapsulate the most desirable properties of a cloud from both user (customer) and provider perspectives. The degree of each property/capability, scalability of the solutions and the costs are some of the additional insights that both users and providers need.

It is hard to argue that a “good” cloud should not have good reliability properties, good security and privacy properties, good access control and well defined external interfaces, ability to manage compliance well (e.g, with export controls), as well as well defined and maintained resources and services, and an ability to collect and analyze extensive provenance information that can then, in turn be used to achieve desired level of performance and both functional and non-functional quality (such as reliability and security).

Following sub-sections discuss some of the properties and associated metrics in more detail.

3.2.1 Reliability

Reliability is the foundation upon which other aspects of customer satisfaction is built. IEEE Reliability Society defines reliability as “a design engineering discipline which applies scientific knowledge to assure that a system will perform its intended function for the required duration within a given environment, including the ability to test and support the system through its total life cycle” [132]. Vouk [137] defines reliability for software as “probability that a system or a system component, will deliver its intended functionality and quality for a specific period of time and under specified conditions”. When applying these definitions to cloud, a reliable service must achieve the following four goals [102].
• Maximize service availability to customers “Ensure that customers can access the service and perform the tasks that they need to perform to complete their work”.

• Minimize the impact of any failure on customers “Assume that failures will occur but minimize the impact of failure has on any given customer, minimize the number of customers impacted by a failure and reduce the number of minutes that a customer (or customers) cannot use the service in its entirety”.

• Maximize service performance and capacity “Reduce the impact to customers when there is decreased performance, even if there is no detectable failure”.

• Maximize business continuity “Focus on how an organization responds to failures when they happen. As much as possible, software and the associated services should be architected to handle large-scale disaster scenarios so that service will be recovered quickly and protect the integrity of the data where applicable. For services that cannot automate recovery, a disaster recovery plan for service restoration should be developed”.

When it comes to cloud, use of commodity hardware and software latent bugs makes failure inevitable. The main aim of service providers should be rapid recovery from failure. Recent outages of AWS [16], Microsoft Azure[103] have shown that even major cloud vendors can still have glitches that take considerable time to repair. But providers with their experienced staff mitigate the outage in shortest time that fall within the acceptable SLA downtime.
3.2.2 Availability

Availability is one of the core capability of cloud systems and also the main reason for organizations to adopt cloud. Previously, organizations based their operations from internal data center. Servers are set up in designated areas to host the data and applications needed by business. But there can be a situation where large number of customers access applications at a time, thereby causing long waiting time for servers to respond and also requests may fail. So, many organizations tend to adopt cloud for its capability of automation of processing power. The cloud provider depending on the load, can scale the processing power up or down with no large upfront cost. Organization only pays for the amount of computing resources utilized.

On the other hand, availability is also main concern for businesses to remain hesitant adopting cloud. Having applications and data in cloud, businesses expect high availability of these resources. Any slightest mishap will have huge impact on client’s workflow, trust and profits. Recent outages of AWS [16], Microsoft Azure [103] and other cloud failures delay adoption of cloud services by many organizations. Organizations wish to have reliable service if they switch to cloud environment from internal IT data centers. IT outages might occur, let it be cloud environment or internal data center. The goal of cloud provider should be to recover from an outage rapidly. Customers should also expect certain level of downtime and should have procedures in place to encounter outage whenever it happens. To assure high availability of its cloud services for its customers, providers employ various ways. Some of them are

- **Redundancy** With introduction of redundancy for services and data, failures can be masked transparently. Providers should be able to run applications on multiple data centers that are unlikely to be affected by the same disaster [106].
• **Load Balancing** By dividing traffic among servers, data can be sent and received without delay. It maximizes throughput with minimum response time [106].

• **Transparency** Availability can be greatly increased with increase in level of transparency. Let the customers know current performance, where is their data and who controls it, any problems or disruption should they occur. Many cloud providers offer their customers with this kind of information in their trust sites like [100], [126] and service dashboards like [101], [15]. This level of transparency will give customers the necessary information to make better decisions and potentially plan for high availability.

• **Effective SLA** SLA should mention uptime availability that user will receive. This makes customer aware of downtime to expect in a given year and let him/her choose provider that can promise level of availability customer needs. SLA must also mention compensation credits, had the provider not meet the promised SLA.

### 3.2.3 Scalability

Scalability is an essential feature of cloud systems. Organizations who adopted cloud systems can spin up new server without any upfront cost or limitation of fitting in given space. Cloud spins up requested number of virtual machines and customer needs to manage virtual environment. Since there is no bound on number of virtual servers to be launched, a whole new way of scaling infrastructure can be unveiled. Along with traditional methods of horizontal(scale-out) and vertical(scale-up/down) scaling, in cloud we can perform scaling in both ways i.e., apply both horizontal and vertical scaling in single solution.

• **Vertical Scaling** (scale-up/down) This is a method where a server can be beefed
up by adding more CPUs, more memory or add faster disks. More CPUs can help in executing batch jobs faster. More memory can increase size of local cache and can serve results faster. Faster disks can reduce I/O time and random access time. With this kind of scaling, individual applications and single-threaded applications can speed up without worrying about context switching and coordination.

- **Horizontal Scaling (scale-out)** This is a method where another similar instance of server is instantiated and can act as load-balancing by sharing requests directed to main server. This kind of scaling invites complexity as it involves communication, concurrency and careful management of tasks among servers.

Cloud systems can scale infrastructure in a way that fits application. There is no single infrastructure architecture that fits all scenarios. So, customers has to choose a provider with desired scalability feature depending on personality of the application.

### 3.2.4 24/7 Support

Every provider offers 24/7/365 support at various levels. Few providers offers support only in form of on-line forums, while others offer telephone, chat, email, technical guidance or dedicated support teams at base or premium price. Depending on the criticality of applications, level of service needed, customers or potential customers need to choose the provider appropriately.

### 3.2.5 Performance

Quality of Service is essential for the business services where basic QoS like response time, throughput, latency, performance must be guaranteed to be met. Reports like CloudSleuth [60], show that latency has huge impact on the business. For high-speed
applications in the cloud, customer must have an end-to-end view of request-response path to guarantee performance. Issues like how far is application and data from end-user, intra- and inter- network performance in cloud, I/O speed between computational resources and storage will have high impact on performance.

### 3.2.6 Pay per Use

Organizations by moving from usual upfront investment model to a model where you pay to the actual consumption of resources, accelerate their development and adoption of new innovative technologies. Buyya [25] considers cloud computing as a fifth utility which can be commoditized and delivered similar to traditional utilities like telephone, water, gas and electricity. Though the utility pricing most providers offer seem low, lot of little charges can add up to large amount. PlanforCloud.com [123] is a useful resource allowing customers to design complete cloud architecture and compare costs from various providers (currently, this tool supports five providers).

### 3.2.7 Time to Market

This characteristic is utmost important for small and medium scale enterprises who want to offer their service quickly by overcoming delays caused by setting up infrastructure that is comparable to larger enterprises. Even larger enterprises wish to have this characteristic to publish new services with enhanced capabilities to remain competitive in the market. Cloud systems can reduce time to market by providing infrastructure support that have capability of easy provisioning.
3.2.8 Virtualization

Virtualization is a foundational technology platform improving cloud computing. Virtualization refers to the abstraction of compute resources (CPU, storage, network, memory, application stack and database) from applications and end users consuming the service. It hides technological complexity from the user and enhances the flexibility. Following are the benefits of virtualization that are applied to cloud computing [40].

- **Reduction in Infrastructure Costs** With virtualization, users do not have to buy computing hardware and maintain it. It helps in consolidating servers into a single physical server, and reduce usage of hardware and failure points. Server consolidation also reduces energy bill with reduction in usage of processors and their peripherals like cooling systems.

- **Reduce complexity** Virtualization helps in hiding the complexity of underlying infrastructure and promotes interoperability by making code platform independent. It also helps in reducing number of servers to monitor. With its management console users can centrally manage, monitor, load-balance servers to achieve optimum efficiency.

- **Adaptability** With help of virtualization, users have the ability to rapidly create, destroy or recreate a sandbox environment. With use of import/export to a template, users can fastly deploy new instances without having to install basic components like OS. Such a benefit allows users to try and develop new services without any upfront costs.

- **Location Independence** Virtualization enables migration of virtual machines on to other physical server with high availability whenever current server can not
perform efficiently due to load or hardware failure. It also enables all the services to be accessed independent of user location. Critical data can be securely stored on centralized servers without having it saved on user-machines.

Virtualization plays a major role in provider selection because migration of workload from internal data center to cloud or between clouds can only happen if underlying hypervisors match.

### 3.2.9 Security

Security is one of the most significant barrier for adoption of cloud computing. Because cloud computing being a new computing model, there is uncertainty about implementation of security control mechanisms at all components in cloud (like infrastructure, network, host, application, data). Though the security mechanisms for traditional IT and cloud computing are almost same but service, deployment models and various technologies that make up cloud pose different risk than traditional IT. A provider’s security level is characterized by effectiveness and completeness of security controls implemented in one or more layers. Mather et al. [97] discusses about security risks and mechanisms at different layers in cloud. When it comes to cloud, implementation of security mechanisms is duty of both provider and customer depending on the type of service model. If these responsibilities are not properly assigned and understood, wrong and insecure configurations or vulnerabilities would go unnoticed resulting in exploit, data loss and compliance issues. For

- **IaaS** Provider is responsible for physical security, environmental security and virtualization security. The customer is responsible for security controls related to IT, operating systems, applications and data.
• **PaaS** Provider is responsible for security of platform ranging from infrastructure security to operating system security and any extra platform capabilities provided. The customer is responsible for security of applications, solution stack, interfaces and data.

• **SaaS** Provider is responsible for physical, environmental, infrastructure, applications and data. The customer is relieved from operational security responsibility but is responsible for security of data and a limited application configuration settings if any.

Table 3.1 depicts responsibilities of client and provider for service models with respect to cloud layers.

Though customers might be attracted to SaaS or PaaS models due to reduced responsibility for administering environment, they should be aware that these models also greatly reduce control over environment hosting sensitive data. Contractual agreements becomes critical where control is outsourced to ensure that required security measures are being implemented and maintained by provider. Few standards and documents identify critical areas of focus client must consider to confirm security measures maintained by provider. Like, Cloud Security Alliance’s security guide [10] identifies twelve domains which provide users with solid foundation for assessing, managing and governing security in cloud computing environments. Microsoft Azure [98] addresses security by organizing security knowledge into ten key buckets which are actionable. Azure groups threats, attacks, and vulnerabilities into these buckets and implements counter-measures in their cloud solution. These ten buckets include auditing and logging, authentication, authorization, communication, configuration management, cryptography, exception management, sensitive data, session management and validation. These buckets give an
Table 3.1: Control between provider and clients [42]

<table>
<thead>
<tr>
<th>Cloud Layer</th>
<th>Service Models</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IaaS</td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
<tr>
<td>Interface (GUIs &amp; APIs)</td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td></td>
</tr>
<tr>
<td>Solution Stack</td>
<td></td>
</tr>
<tr>
<td>Operating Systems (OS)</td>
<td></td>
</tr>
<tr>
<td>Virtual Machines</td>
<td></td>
</tr>
<tr>
<td>Virtual network Infrastructure</td>
<td></td>
</tr>
<tr>
<td>Hypervisors</td>
<td></td>
</tr>
<tr>
<td>Processors and Memory</td>
<td></td>
</tr>
<tr>
<td>Data Storage (Disks, backups etc.)</td>
<td></td>
</tr>
<tr>
<td>Network (interfaces, communication infrastructure)</td>
<td></td>
</tr>
<tr>
<td>Physical facilities</td>
<td></td>
</tr>
</tbody>
</table>
overview for user what to consider while looking security as a metric. Also NIST [84] issues security guidelines which provide an overview of security and privacy challenges related to public cloud computing and considerations organizations should take prior to outsourcing data, applications and infrastructure to public cloud environment. Gartner [86] has identified seven security areas customer has to consider before selecting provider. All these studies identify components of security that must exist in a cloud solution.

### 3.2.10 Privacy

Privacy is essential in all systems that are potentially dealing with sensitive information and data. Privacy has no standard definition to be used across countries and jurisdictions. Mather [97] defines privacy as rights or obligations that are related to the collection, use, disclosure, storage and destruction of personal data ("any information relating to an identified or identifiable individual"). There are no comprehensive frameworks and standards like NIST security guidelines [84] for organizations to know about privacy and implement the necessary controls. Against standards, we all have conflicting regulations and laws on what privacy is and what it requires from organization to protect it. Most of the cloud providers ensure privacy by participating in safe harbor [58] programs whose seven principles provide more control to customer over their data. And through attestation reports like SSAE 16 SOC1 [1] and SOC2 [2], PCI DSS [110] and certification of ISO 27001, to assure that relevant controls are in place to protect sensitive data. Mechanisms like encryption/decryption, public keys, digital certificates ensure privacy and integrity of the data [84].
3.2.11 Compliance

Compliance refers to organization’s responsibility to operate in agreement to establish laws, regulations, standards and specifications. With dynamic nature of cloud, cloud service providers are finding hard to establish, monitor and demonstrate compliance that meets customers’ requirements. Also, various types of security and privacy laws and regulations exist within different countries at national, state and local levels, making compliance more complex. So providers demonstrate compliance to customer requirements by demonstrating compliance to industry standards. Providers employ two basic methods to demonstrate compliance to customers. One from internal perspective - adopt a programmatic approach by monitoring, and another from external perspective - audit. These approaches can be employed by either provider or customer depending on requirement and deployment. Auditing is a one-time or periodic exercise for evaluation whereas monitoring is an ongoing activity. Continuous monitoring might be considered important to providers because providers can not take risk of waiting for external audit to submit report/feedback of relevant controls. Honoring individual customer audits will be challenging to provider both from resource and confidentiality perspective. So, providers has to build strong internal monitoring function that fits for all clients along with robust external audit process. Mather [97] summarizes various industry standards against the controls which can be followed to build a strong baseline in a table 3.2.
Table 3.2: Industry standards [97]

<table>
<thead>
<tr>
<th>Control environment/Company Level Controls</th>
<th>Information Security</th>
<th>IT service delivery/operation</th>
<th>Systems development</th>
<th>Financial reporting systems</th>
<th>Incremental requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best practice guidance</td>
<td>COBIT</td>
<td>COBIT</td>
<td>ITIL ISO 20000-2</td>
<td>COBIT</td>
<td>ISO various</td>
</tr>
<tr>
<td></td>
<td>COSO</td>
<td>ISO 27002</td>
<td></td>
<td>ITIL CMM/ISO</td>
<td>ANSI various</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ISO 20000-2</td>
<td>NIST various</td>
</tr>
<tr>
<td>Certification</td>
<td>ISO 27001</td>
<td>ISO 20000-1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory/Industry requirements</td>
<td>FFIEC</td>
<td>FFIEC</td>
<td></td>
<td>ISO 2700X</td>
<td>SOX PCAOB</td>
</tr>
<tr>
<td></td>
<td>HIPAA</td>
<td>HIPAA</td>
<td></td>
<td></td>
<td>EV SSL</td>
</tr>
<tr>
<td></td>
<td>PCI</td>
<td>PCI</td>
<td>SOX</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NIST various</td>
<td>NIST various ISO 2700X</td>
<td>PCAOB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Framework</td>
<td>SAS 70</td>
<td>SAS 70</td>
<td>SAS 70</td>
<td>SAS 70</td>
<td>WebTrust</td>
</tr>
<tr>
<td></td>
<td>SysTrust WebTrust</td>
<td>SysTrust WebTrust</td>
<td>SysTrust WebTrust</td>
<td>SysTrust WebTrust</td>
<td>CA WebTrust EV</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

35
3.2.12 Data Management

Cloud computing paradigm usually requires customers to transfer resources to cloud which is controlled by third-party. With this, two main changes occur to customer’s data. One, data is saved on to someone’s device, other data is moved into multi-tenant environment. Once private data is moved to someone’s computer, many things can go wrong. Firstly, location of data is unknown and it is very important for customer to understand data location because law varies with locations. Secondly, provider sustainability, what happens to the data if provider ran out of business or lease company to third party or business competitors. Thirdly, unauthorized usage of saved data when organizations have centralized database which leads to new logistics/views that are not approved. Participating in safe harbor programs, employing encryption techniques both at rest and in transit, using only SSL protected end-points upto certain extent assures customers of their control over data.

Data destruction is another major concern related to data management. Because data deleted is never actually gone, only file system marks corresponding blocks of file as usable but contents still remain. As we know, in cloud computing these virtual storage devices will be reallocated to new users. Personal information or data stored on this device may now be available to new user violating privacy laws and regulations. The same issue occurs when storage device reaches end of its life-time, data must have to be completely destroyed before de-commissioning the device. There are several approved methods of data destruction like media sanitization, multiple disk overwrites with random byte pattern and destruction of key for encrypted data etc [88].
3.2.13 API

Application Programming Interface (APIs) are essential to access cloud features, infrastructure and performing operations like provisioning and de-provisioning servers. Interoperability APIs ease task of migrating applications or load-balancing across different providers as it imposes less changes to the application. If an API is widely accepted by community, it promotes establishment of strong ecosystem with complementary services. For example, AWS has strong ecosystem which include tools from third-parties like RightScale, enStratus. Apart from proprietary API’s, there are open source alternatives like OpenStack [108] and CloudStack [27].

3.2.14 Provenance

Provenance is meta-data that describes history of an object [105]. For example, provenance include history of the data, resource or object ownership and access, any transformation applied. Provenance can be found in many places in the system including logs. Placing lineage information in the logs eases auditors or engineers in finding information in a single place. Care must be taken to restrict access to logs. Such logging mechanism can act as psychological obstacle to go against policies and regulations. This can act as detective control and act as record for any investigations. Provenance of the system is not a new topic but with advent of cloud computing and importance to the data made provenance a must have. At the same time, it offers many new challenges than traditional IT data center. Ko et al. [89] list challenges provenance faces with arrival of cloud computing. Ko et al recommends logging from a file-centric perspective i.e., the need to trace data and files from the time they were created to the time they were destroyed. Such a logging mechanism will give a detailed lineage of data and easy access to review
information to make person or system accountable for any violations if found. There are few tools in the market like HyTrust [77] which provide monitoring capability to lineage of data at virtual machine level and operating system level.

3.2.15 Tools

Tools are important to facilitate development, adoption and usage of cloud services. There are many tools that empower user with real-time monitoring of OS or process or application performance, set-up alerts to notify when service is down or reach safe threshold levels, perform analytics, gain insights, collect and track metrics etc.

3.3 Metrics

Various trust components/metrics were identified from [124] [92] [91] [6] [95] [3] [87] [73] [95] [81] [138] [9]. Thoran Rodrigues article [124] compares cloud providers based on metrics like variety of pricing plans, average monthly cost, storage costs, bandwidth costs, number of data centers, supported operating systems, instance types, APIs, security, reliability, ease of migration and scalability and monitoring capability. Li et al [92] compares cloud providers based on finishing time and cost to complete each benchmark test, scaling latency, cost and response time for each storage operation, and intra- and inter- network latency. Lee et al.[91] and Alhamad et al [6] evaluates cloud applications based on quality attributes like re-usability, availability, efficiency, reliability and scalability. Abawajy [3] feels that resource provider’s competence, honesty, availability, reliability, security, capability, quality of service and reputation will influence the selection of cloud provider to transact with. Khan [87] considers control, ownership, and security are necessary to establish trust in cloud computing. Grandison [73] in his survey of internet applications
mentions that reliability, competence, honesty, timeliness, truthfulness, dependability of
transaction partner influence trust decisions. Manchala et al. [95] considers transaction
cost, transaction history, indemnity, number of intermediaries involved in transaction
towards trust metrics in E-commerce transactions. Apart from above metrics, this study
also considers top concerns/challenges in cloud computing identified in survey reports
like IDC [81], Information Week [138] and CSA [9] towards trust metrics. These survey
reports identifies security, availability, performance, lack of interoperability, data loss and
insecure APIs as few of the top concerns in cloud computing.

These identified components/metrics were then correlated with Bubble framework
[48] to filter out components in the context of cloud computing. Table 4.1 and Table 4.2
show components used to measure trust in this study.

### 3.3.1 Service trust components

Service trust components are divided into metrics that can be measured on interval or
ratio scale and ordinal scale.

- **Response time:** It is the time system takes to react to given input. In cloud
  scenario, it is the time system takes to process and complete the service request.

- **Latency:** It measures delay between sending the request and receiving the re-
  sponse. Both response time and latency measure network performance (intra- and
  inter-) in cloud and I/O speeds. CloudSleuth’s Global Provider View [38] a third
  party monitoring service, measures response time in terms of page delivery time of
  major cloud providers by downloading a simple target application web-pages.

- **Reliability and Availability:** Failures are inevitable in cloud. So, main aim of
Table 3.3: Service trust components - how we measure them in this study

<table>
<thead>
<tr>
<th>Interval or ratio scale</th>
<th>Ordinal scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response time</td>
<td>Security</td>
</tr>
<tr>
<td>Latency</td>
<td>Privacy</td>
</tr>
<tr>
<td>Reliability</td>
<td>Scalability</td>
</tr>
<tr>
<td>Availability</td>
<td>Interoperability</td>
</tr>
<tr>
<td>Cost</td>
<td>Compliance</td>
</tr>
<tr>
<td>Credit upto</td>
<td>Data control</td>
</tr>
<tr>
<td></td>
<td>Monitoring tools</td>
</tr>
<tr>
<td></td>
<td>Provenance</td>
</tr>
<tr>
<td></td>
<td>Dependability</td>
</tr>
</tbody>
</table>

provider is to reduce time to recovery from failure. So, customers are most interested in Mean Time To Recovery (MTTR) than Mean Time To Failure (MTTF). MTTF measures how frequently software and hardware fails whereas MTTR measures amount of time it takes to get service up and running again. So, lower the MTTR value, better is the reliability. Reliability is also measured in terms of “uptime’ which is time the computer has been working and available. Uptime is the opposite of downtime. Vendors mention their uptime percentages in SLA.

Reliability and availability are tightly coupled in industry measurements. Industry experts and IT managers, express readings in terms of downtime per year. Such a measure would include both reliability and availability. Availability is expressed as percentage of uptime in a given year. They express reliability and availability metric in terms of “nines”. For example, two nines is same as 99% which is (100%-
99\% \times 365 \text{ or } 3.65\text{ days of downtime per year. This metric usually do not include any planned downtime (like downtime for upgrades, scheduled hardware repairs, software maintenance). Unplanned downtime is where providers gain or lose.}

User might perceive reliability through three options [124] - SLA uptime, service age and support. Support has become important measure because it is very hard to react to unplanned downtime when instance running your service is not under your control. So, a reliable service requires continuous support that can help fix the issue in shortest time possible. Service age acts as hint towards strength of business, implied good will from customers and customer satisfaction. To a certain extent credit upto, assure customers of any financial losses incurred by unplanned downtime. Customer might perceive credit upto as a trust metric when he/she has alternate backup strategy to encounter unplanned downtime but not when reputation is at stake.

- **Cost:** Cost is a straightforward way to compare different providers. The pricing most vendors offer appear low but there are many other charges that add up to the bill. Such charges include cost of data transfer-out and data transfer-in, storage costs, bandwidth costs etc. Comparison is not so simple as it appears because each vendor has their own measurement unit for configuration. RightScale’s PlanforCloud [123] is a useful ready-made resource for cost planning. It allows customer to build his/her cloud architecture and compare costs among IaaS providers.

Metrics that are measured on ordinal scale represent functional and non-functional properties of the system. Importance and value of these metrics depend on the context and preference of a customer. There are no standard measurement units to quantize them.
• **Security:** Security is one of the most important factors to be considered for trust establishment. There are many ways in literature to quantify security. Few measure security in terms of number of security incidents, number of intrusion attempts etc [75]. But for this study, we measure security from user perceptive by considering first hand information available from vendor’s websites, white papers, documents, questionnaire etc. It is more likely that customers perceive security through certifications, audit reports, technical audits and penetration tests and vulnerability scans they can run on the resources rented from provider.

Standards for Attestation Engagement 16 (SSAE 16) SOC 1 [1] attestation report attest controls at an organization that may be relevant to user’s internal control over financial reporting. The report is on controls related to security monitoring, change management, service delivery, support services, backup and environmental controls, logical and physical access. SOC 2 [2] report attest organization’s information system controls relevant to security, availability, processing integrity, confidentiality, and privacy. Type II reports of SOC 1 and SOC 2 attest both design and operating efficiency of controls. This standard is descriptive, i.e., provider describes the controls he/she choose to attest to.

Payment Card Industry Data Security Standards (PCI DSS) [110] provide a baseline of technical and operational requirements designed to protect card-holder data. This standard defines 12 requirements for protecting card-holder data. PCI DSS offers a self assessment questionnaire (SAQ) to self evaluate compliance with PCI DSS.

ISO 27001 [82] is an information security management system standard that sets out requirements and best practices for a systematic approach to managing cus-
tomer and company information based on periodic risk assessments appropriate to ever-changing threat scenarios. Certification showing compliance to this standard shows that company has systematic and ongoing approach to manage information security risks that affect the confidentiality, integrity and availability of company and customer information. [20]

Cloud Security Alliance (CSA) is a not-to-profit organization with focus on security that describes best practices for cloud providers in variety of areas. CSA has created a new registry called STAR (CSA Security Trust and Assurance Registry) to hold responses from different cloud providers to Cloud Assessment Initiative Questionnaire (CAIQ) [11], which comprises 140 questions regarding security controls which also includes provider’s policies, procedures and controls against malicious insiders. All the responses are publicly accessible.

Apart from documentation, customers can confirm security posture of a provider through vulnerability scans, technical audits and penetrations tests, if provider approves. Security posture of a provider can also be analyzed from protection mechanisms likes firewalls, multi-factor authentication, access controls, VPN, subnets etc., they offer to customers in their solutions.

• **Privacy:** Privacy is assured through various laws and regulations. Table 3.4 list few of many regulations that are important with respect to privacy of information.

• **Scalability:** For applications whose load can not be predicted before hand, scalability becomes one of the foremost concern for the customer. Scaling can happen either horizontally or vertically or both. Cloud providers refer to scaling in terms of scale up/down and scale out to represent vertical and horizontal scaling respectively in their information.
Table 3.4: Privacy regulations [97]

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Act</td>
<td>Governs the collection, maintenance, use and dissemination of information about individuals that is maintained in records by federal agencies</td>
</tr>
<tr>
<td>FISMA(Federal Information Security Management Act)</td>
<td>Requires federal agencies to adequately protect their information and information systems against unauthorized access, use, disclosure, disruption or destruction</td>
</tr>
<tr>
<td>EU Data Protection Directive</td>
<td>Regulates processing(automated or not) of personal data within in European Union. Processing includes operations like collection, recording, storage, alteration, use, retrieval, disclosure, dissemination and destruction</td>
</tr>
<tr>
<td>GLBA(Gramm-Leach-Bliley Act)</td>
<td>Mostly deals with financial issues. Enforces administrative, technical safeguards essential for protecting personal information provided by 1) customer to financial institution, 2) resulting from any transaction with customer, 3) otherwise obtained by financial institution.</td>
</tr>
<tr>
<td>HIPAA(Health Insurance Portability and Accountability Act)</td>
<td>Regulates the use and disclosure of protected health information (PHI) by health care providers and health plans. Also requires health care providers to notify individuals of their information practices.</td>
</tr>
</tbody>
</table>
• **Interoperability:** Interoperability eases customer from the fear of vendor lock-in, business continuity and application changes. If an API is supported across different platforms, it facilitates migration of an application from one platform to other, or eases simultaneous working across different platforms with less or no application changes. Also, to migrate or duplicate virtual machine across different providers, underlying hypervisor needs to be same or virtual machine must be imported/exported in a standard format. Most of the upcoming vendors into market are basing their solutions on VMware hypervisor. With new OVF 3.0 [136] template for import/export VM image, VMware soon appears to be standard. On the other hand, there are also open source alternatives like OpenStack [108] and CloudStack [108] to develop an inter-operable cloud ecosystem.

• **Compliance:** External audits assures customers about effectiveness of controls implemented at provider organization. Some of the audit reports include reports based on standards like SSAE 16, ISO 27001, PCI DSS and industry specific compliance requirements like HIPAA, GLBA etc. SSAE 16 attests prescribed internal (security and technology) controls of service organization necessary for financial reporting and controls relevant to security, availability, confidentiality, processing integrity and privacy. ISO 27001 certifies organization’s information security management system. PCI DSS audits organization controls and design principles involved in protecting payment information and card-holder data.

• **Data control:** With cloud computing, user has to transfer his/her data into cloud thereby losing control over the data. More control user has on the data, more he/she trusts the provider or service. So, provider by participating in safe harbor programs, employing encryption techniques both at rest and in transit, external audits related
to SSAE 16, ISO 27001, PCI DSS assure customers of their control over data. By following above methods and guidelines like sanitization [88], providers assure customers about best practices being followed for data use, collection, recording, storage, alteration, dissemination and destruction.

- **Monitoring tools**: These tools help customer to monitor health or status of the service, gain insights, track metrics and set up alerts whenever service reaches assigned safe threshold levels or stopped. More deeply the tools integrated into the software stack, higher is their monitoring capability. Integrated tools automatically scale with your solution architecture without any manual intervention. How good the third-party monitoring tool be, their penetration into software stack is always limited and might require some manual effort to support scaling. So, a provider with deeply integrated monitoring tools might always be preferred as trusted partner.

- **Provenance**: This act as detective control to identify any out-of-band operations during audit or incident response programs and held those responsible accountable. But providers rarely discuss about provenance controls in the documentation or in the white papers. To a given extent, ISO 27001 certification audits processes and procedures that were in place for provenance.

### 3.3.2 Provider trust components

If there are many services with similar functionalities from different providers, then user might prefer the provider with high trust value.

- **24/7 Support**: Support has become important measure because it is very hard to react to unplanned downtime when instance running your service is not under
Table 3.5: Cloud Provider trust components

| 24/7 Support | Competence | Honesty | Reputation | Website | Usability | Risk Management | Policies | Incident Management |

your control. So, a reliable service requires continuous support that can help fix the issue in shortest time possible. Many options are available for support like forums, chat, telephone, email, ticketing, engineer support and dedicated team support.

- **Reputation**: A provider with brand name reflects his/her good-will and long term history with its customers. This can act as trust bootstrap for a new customer who is looking for a provider. Measuring reputation of provider is subjective to customer. For few customers, global reputation score is sufficient where as for few customers, personalized score and feedback from inner circles value much.

- **Website and Usability**: A website can act of sales person in on-line world and an object of trust. A website with appropriate and useful content, easy access to contact information, ease of searching, professional look, good maintenance with no broken links, seals from trusted third-party organizations like Verisign, TRUST-e etc., can induce some confidence in customer. Corritore et al. [41] details about
influence of websites on trustworthiness.

- **Risk Management:** NIST SP 800-37 [93] defines risk management framework for information systems which provides a disciplined and structured process that integrates security and risk management activities into system development life cycle. With constant introduction of new services and their dependent devices or modules, a trusted provider must have a well-defined risk management framework to encounter any unplanned risks. Such a framework ensures right controls are selected, implemented and monitored continuously.

- **Policies:** There are many compelling reasons for enterprises to move IT functionality into the cloud. Therefore, enterprises need to have defined policies that provide administrative guidance for users on how to use IT services securely, policies that define who is authorized and what level of access will be granted, automation policies that trigger alarms when soft threshold is reached and other policies that define patch and incident management. Lacking physical control on most of processing capabilities, customer has to now evaluate policies required to fill in the gaps that are made by cloud transition. These policies also help customer during their audit for compliance.

- **Incident Management:** Incident management steps would normally include detect, notify, isolate, recover and post-mortem reports. With most of responsibility of managing IT vested in providers depending on service model, customer should consider a provider who is willing to share their controls in place, testing methods, recovery plans, cause of error reports and continuous improvement plans. With such solid understanding between customers and provider, customers are well aware of plans to manage incidents when something go wrong.
One can derive competence and honesty from reputation and past experiences with provider. Chapter 4 uses some of these identified trust components and their metrics to compare major cloud providers.
Chapter 4

A Trust Evaluation

Cloud computing is a complex term encompassing different things from infrastructure to software services. In order to understand what role, and how, trust plays in this domain, one must evaluate providers who offer cloud services (and what their view of trust is), and perceptions users have about trust. In this study, we chose to primarily evaluate providers with Infrastructure as a Service (IaaS) offering. Based on available information, selected were

- Amazon EC2 (aws.amazon.com)
- Rackspace - Cloud Servers (www.rackspace.com/cloud/servers)
- HP Cloud - Compute (www.hpcloud.com/products/cloud-compute)
- IBM SmartCloud Enterprise (www.ibm.com/services/us/en/cloud-enterprise) and
- GoGrid (www.gogrid.com).

Sources of information in this study are public websites, published papers and white papers, and documentation attested by service provider. There are a few third-party
services which compare cloud providers based on some of the previously identified trust metrics [38] [37] [92]. However, because every third party assessment appears to have own way of measuring the cloud characteristics, but without always disclosing all the considerations that went into the results, and thus sometimes introducing a possible bias, we chose to approach our evaluation from a different angle. We tried to rely on as much first hand information as possible, e.g., directly from vendor web-sites, so that we would have the perspective of an end-user attempting to make a decision about the cloud services based only on the publicly web-disclosed provider information. This is one of the reasons, why metrics such as response time, and latency are not being considered in this trust evaluation. We did employ our own mechanism to assess services based on metric we think are very important - metrics that map back onto the “bubble” framework. Some of the metrics are more quantitative in nature, some are more qualitative, and on some information was not available. For qualitative metrics, we developed a Likert scale in order to allow mutual comparison of the measures that may contribute to a trust measure. Presentation is done using tables and Radar charts. Data used in calculations is shown in the tables in following sections.

4.1 Evaluation Metrics

The user-perceivable trust assessment model developed in this study identifies trust metrics by considering all components/capabilities of a “good” cloud (bubbles in “Bubble” [48]framework). However, few components/capabilities like work-flow composition tools, analytics, HPC/HPD support and domain services are not discussed in this model as they are more domain specific and relatively new, lacking necessary first-hand information. This model however, considers necessary components/capabilities like scalability
and monitoring tools in addition to components of “Bubble” framework.

- **Cost:** As the norm, we use calculated monthly cost for a cloud server instance with 1 CPU, minimum of 1GB RAM and a Linux/Unix image. We use 730 hours as representing one month of service. Providers like HP Cloud and Rackspace offer their monthly cost calculated at the rate of 730 hours of service. So, to keep comparison of all providers on same scale, we computed monthly cost for other providers using hourly plan for 730 hours unless a provider already have any discounted monthly price plan. This cost does not include any bandwidth and storage costs. For example, HP Cloud and GoGrid offers a discounted monthly price plan against hourly plan. Details are provided in Appendix A.

- **Reliability and Availability:** Users can perceive these metrics through direct measurement of their own experience, through provider-user SLA guarantees, or through monitoring of explicit data that may be offered by the cloud provider (e.g., VCL [135], AWS [15]) or by third-party (e.g., CloudSleuth [38], CloudHarmony [37]). What SLAs frequently offer is uptime guarantees (a component of availability), but in practice there is little or no information about, for example of cloud mean-time-to-repair (MTTR) (one can argue that clouds never fail, but that is probably a hollow argument judging by what is known about large scale clouds such as AWS [16]).

From the user perspective, another interesting measure may be how long the provider has been in the business. We call it Service Age. Yet another measure is the level and state of customer support offering is - e.g., 24/7 through forums, chat, email, tickets or technical guidance. While most the metrics mentioned so far in this paragraph are directly measurable. It is less obvious how one measures support.
Certainly through experiences of the user satisfaction. Unfortunately that information is not readily available. What is however available is how support is promised and when. Again, we take a very user-centric view. For support, higher value is assigned to the choice that instills more confidence in customer. (See Appendix A for details)

1. Poor - value 0. If company offers support only through support forums.

2. Average - value 1. If company offers any one extra support in addition to support forums.

3. Good - value 2. If company provides multiple support features included in base package.

Finally, an additional insight into the confidence of the provider as to their ability to meet SLA is the “credit” metric - how much are they willing to put on line (e.g., in money) in case they do not meet SLA. This is discussed further in the next section.

- **Security:** Security is a complex metric to quantify. While one can measure security in terms of the number of security incidents, and the number of intrusion attempts [75]. This information is not readily available from providers. It is more likely that customers perceive security through certifications, protection measures employed and to a certain extent through technical audits, and penetration tests and vulnerability scans they can run on the resources they are renting from the provider. But to perform these scans and tests, customers need permission for the tests from providers well in advance. Providers typically approve only after customers sign an “Acceptable Use” policy which makes customer pay compensation if
policy is violated. These tests are very complex and take considerable time. Thus, they are not performed often [127]. Therefore, users are more likely to base their decisions regarding security on certifications and protection mechanisms which are already documented and audited through third-party auditors.

We choose to assess security posture of a provider through certifications and audit reports. Such documents are based on SSAE 16 SOC1 [1] and SOC2 [2], PCI DSS [110], ISO 27001 [82] and other standards. These documents assure presence of information, data and operational security, as well as of technology controls in an organization. In the context of our evaluation, we use the following ratings for quantifying this metric (See Appendix A for details)

1. Poor - value 0. No certifications.
3. Good - value 2. Auxiliary first-hand information in addition to certifications.

Customers may prefer the provider who offers protection behind regular basic firewalls. If yes, value of 2 (which represents good standing) is assigned else value 0 is assigned to “protection” parameter. Value 0 is also assigned to provider who provides protection through some third-party services because sustainability of third-party services plays a major role.

- Scalability: Scale-up/down and scale-out are important factors for customers to consider when application load can not be predicted. As discussed in chapter 3, scalability can happen vertically or horizontally. Vertical scaling refers to things like addition of extra memory or CPU or storage to existing cloud resource instances, where as horizontal scaling refers to deployment of new similar instances.
To quantify, we assign (See Appendix A for details)

1. Value 0 - No obvious or declared scaling
2. Value 1 - One of the scaling options is explicitly available
3. Value 2 - Both options available

Application Programming Interface (API) can also act as measure of scalability. APIs can provide capability to interact with different cloud layers (IaaS, PaaS and SaaS, XaaS) and through that perform operations like provisioning and de-provisioning of new instances on the fly. Interoperability APIs ease task of migrating applications or working together across different providers. To quantify, we assign

1. Poor - value 0. No explicit and user-usable API at appropriate service level.
2. Average - value 1. APIs available
3. Good - value 2. APIs compatible with other service providers like HP Cloud and EC2 Compatibility API.

- **Monitoring tools:** Situation awareness is an extremely important component of any business, and especially so when it is being done in the cloud. This is not a new finding but having monitoring tools integrated into a solution is critical. Monitoring tools provide capability for user to monitor health, performance, and in general states of the system/process/application. Integrated tools gives higher monitoring capability and scales with your solution architecture. To quantify, we assign (See Appendix A for details)
1. *Poor* - value 0. No integrated tools. Requires deployment of third-party tools.

2. *Average* - value 1. If simple API exist whose response include health status of subject.

3. *Good* - value 2. If complete integrated tools exist.

**Interoperability:** Interoperability with other clouds, and facilities, is at the core of the freedom and support clouds offer, in theory. In practice portability of codes, data and services depends on how inter-operable a cloud is often, how well it conforms to standards. For example, underlying hypervisor influences the choice of providers because migration of workloads needs similar hypervisor across providers or standard format to import/export a virtual machine. With extensive use of VMware and standardization of OVF 3.0 [136], VMware is now being considered as possible standard. Open source cloud systems like VCL [80], OpenStack [108] and CloudStack [27] reduces the risk of lock-in associated with proprietary platforms. To quantify, we assign value 2 (represents good standing) to the provider who follow standards like OVF 3.0 [136], or earlier version, or open source alternatives like VCL, OpenStack or CloudStack, and value 0 if not.

**Data management:** Data management activities include use, collection, encryption, storage, recording, dissemination and destruction of data. The seven principles of Safe Harbor program [58] assure customers of control over their data. Decommissioning and destruction of data is a differentiating factor among providers. To quantify, we assign

1. *Poor* - value 0. No standards or principles followed for data management
activities.


### 4.2 Results

The primary goal of current work is to provide model of a user-centric perspective of the trust one may gain by surveying public information for commercial clouds. Table 4.1 summarizes the assessment information we have collected and coded. Coding information is detailed in the Appendix A. Cost, credit, SLA Uptime and Service Age are given on quantitative scale, while the remaining metrics are expressed on a ordinal scale like Likert scale. (All the values are based on information derived from web-sites dated February 27, 2013).
<table>
<thead>
<tr>
<th>Providers</th>
<th>Cost/month in $</th>
<th>Credit</th>
<th>Reliability and Availability</th>
<th>Security</th>
<th>Scaling</th>
<th>Tools</th>
<th>Interoperability</th>
<th>Data management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>43.8</td>
<td>10%</td>
<td>SLA Uptime</td>
<td>Good</td>
<td>Yes</td>
<td>Yes</td>
<td>Average</td>
<td>Good</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Uptime Service Age Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rackspace</td>
<td>43.8</td>
<td>5%</td>
<td>100%</td>
<td>Good</td>
<td>Average</td>
<td>Yes</td>
<td>Good</td>
<td>Open-Stack</td>
</tr>
<tr>
<td>HP</td>
<td>15.33</td>
<td>0%</td>
<td>99.95%</td>
<td>Average</td>
<td>Yes</td>
<td>No</td>
<td>Good</td>
<td>Open-Stack</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Uptime Service Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM</td>
<td>68.4</td>
<td>10%</td>
<td>99.9%</td>
<td>Average</td>
<td>Yes</td>
<td>No</td>
<td>Average</td>
<td>Good</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Uptime Service Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>OVF</td>
</tr>
<tr>
<td>GoGrid</td>
<td>36.25</td>
<td>10000%</td>
<td>100%</td>
<td>Average</td>
<td>Yes</td>
<td>Yes</td>
<td>Average</td>
<td>Poor</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Uptime Service Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4.1: Trust evaluation parameters for five cloud providers
4.2.1 Discussion

A reason we have avoided using third party cloud service evaluations is because we are not sure what the reporting bias of that party. So, our study considers only first-hand information in provider websites, and their white papers, documents etc. That, of course has its own perils. Vendor information is probably biased towards the vendor goals and agendas. But it is natural to have the vendors highlight their strengths. That also is what reality of cloud computing is today. In an ideal situation one would have a trusted third-party evaluator as well as the vendor information. Lacking that, we believe that it may be more informative to cross-compare vendors and draw conclusions that way. This is why we developed the current assessment model.

- **Cost per month in dollars:** It is difficult to compare provider pricing, as each provider offers a different combination of computational resources, computational memory and other resources and services. Depending on what is actually being offered, 6 to 10 cents per CPU hours that we find on vendor websites may not be a bad price. But this cost does not include any bandwidth costs, storage costs etc. The total cost therefore depends on your solution architecture. In order to have reasonably meaningful comparison among providers, we choose to use monthly pricing for basic configuration of 1 CPU, minimum 1GB RAM and a LINUX/UNIX image. Such a minimum configuration is normally associated with small or extra small resource instance. However we understand that every customer’s use-case is unique and there is no one-size-fits-all tool that can assess total monthly cost for customer’s service solution. So, for comparison we opted to use pricing of instances that met our basic criteria excluding any extra costs for storage and bandwidth. We use 730 hours (HP Cloud and GoGrid considers 730 hours as monthly hours of service) for
our calculation if discounted monthly cost isn’t mentioned in the provider’s website. Our values are based on information from Amazon [23], Rackspace [116], HP [33], IBM [52] and GoGrid [65]. For IBM, we configured copper resource instance [56] for monthly cost estimation because it is the only configuration available for IBM with 1CPU and 2GB memory (this is lowest memory configuration available). This cost information is one such information that is found relatively easy when compared to other metrics. All the providers have a dedicated page explaining cost and instance types easily accessible from homepage. While the above comparison is not really an apples-to-apples comparison, it is based on first hand information available to a general user. The lower the value the more relief a customer gets when trying services before committing to a provider.

• Credit: This represents service credit customer is entitled to when vendor fails to meet agreed SLA uptime. For comparison, we calculated the amount the customer is credited for a service downtime of one more hour than agreed. Every provider has their own way of calculating uptime percentage and of offering service credit. For example, HP offers 5% of monthly bill credited if uptime ranges between <99.95% and 99.9%, 10% for <99.9% to 99.5% and so on.

To illustrate credit calculation, consider Amazon EC2. Amazon EC2 SLA promises SLA Uptime of 99.95% i.e., \((100-99.95)\% \times 365 \times 24 = 4.38\) hours of downtime. So, as per SLA 4.38 hours of unplanned downtime is agreeable and does not incur any service credit. EC2 calculates uptime via “Annual Uptime Percentage” which is percentage of 5 minute periods during the service year in which Amazon EC2 was in state of region unavailable subtracted from 100%. This implies in a year we have 105,120 five-minute periods and as per SLA 52.56 five-minute periods of
downtime do not incur service credit. For our calculation, we assumed downtime of 5.38 hours in a service year and that the extra hour of downtime has happened in same service month. With this extra hour, annual uptime percentage drops to 99.94%, thus making us eligible for 10% of service credit added to next month billing cycle. If monthly pricing amounts to $43.8 then customer is credited $4.38. Credit and SLA Uptime are tightly bound together. Higher percentage of SLA Uptime ensures customers of larger time availability. At the same time service credit compensates to a certain level of financial loss customers incur if vendors fail to meet SLA promises.

• **SLA Uptime:** These values represent uptime providers strive to maintain. The values we report are derived from provider’s respective SLAs Amazon EC2 [49], Rackspace [115], HP Cloud [34], IBM SmartCloud Enterprise [53] and GoGrid [67]. When compared to other providers, IBM SmartCloud Enterprise SLA is not easily accessible from homepage, this study has to perform website search to obtain SLA.

• **Service Age:** Service Age values represent the number of years since the services were made available for public use by that provider. A higher number indicates longer presence in the IaaS market, implied good-will from customers, and a greater chance of more information, feedback and solutions to common problems over forums/communities etc. The values are derived from Amazon EC2 [13], Rackspace [112], HP Cloud [28], IBM SmartCloud Enterprise [79] and GoGrid [61]. All the information related to service age is derived from their respective release notes or time-line information. Such information is not directly accessible or found in main web-pages.

• **Support:** Support values indicate level of customer support available to cus-
tomers in the base package. We did not to consider premium packages because every provider offers managed support for an extra but difficult to compare costs. So we compare support features available with no extra charge. “Good” support level implies vendor is offering multiple features like chat, phone, ticket, technical guidance, forums for free (included in base package). The values we report are derived from respective provider websites Amazon EC2 [50], Rackspace [120], HP Cloud [35], IBM SmartCloud Enterprise [54] and GoGrid [68]. All the information related to support is easily accessible across all providers.

- **Certifications:** Security is a complex metric to quantify. One can manage security through metrics such as number of intrusions, number of threats mitigated etc., [75]. But all this information usually is not readily available. Another way to assess security would be to audit a cloud provider regarding controls and countermeasures. But it is not possible for a provider to participate in a detailed technical audit reports for each and every customer. The next best way may be to take advantage of documentation that most providers make available to customers. We chose to assess security posture of a provider through certifications, audit reports published by vendor in their website. Such documents are based on SSAE 16 SOC1 [1] and SOC2 [2], PCI DSS [110] and ISO 27001 [82] and other standards. These standards relate to presence of information, data and operational security, as well as of technology controls in the organization. We attributed additional value to those providers who provide detail information about their security controls such as responses to questionnaire provided by industry-expert like Cloud Security Alliance (cloudsecurityalliance.org). If rating stands at “good” level, then it implies that provider has above mentioned certifications and audit reports along with auxiliary
information like responses to questionnaire (see Appendix A for details). Information regarding certifications and audit reports is retrieved from Amazon EC2 [20], Rackspace [121], HP Cloud [36], IBM SmartCloud Enterprise [130] and GoGrid [64]. Amazon has detailed its security posture in white-papers which are easily accessible under documentation section. Rackspace and IBM mentioned its security related certifications and reports in their web-page which is easily accessible. Where as HP Cloud, although did not have any specific web-page or documentation for its security related information but mentioned about security certifications while describing features of its IaaS offering. GoGrid has no specific information related to security except a press release which confirms its certifications.

- **Protection:** These values represent presence of advanced protection mechanisms in addition to basic firewalls. For example, multi-factor authentication, security groups, VPNs, access control lists, communication security through key management, anti-virus, intrusion prevention and detection systems etc. Relevant information is retrieved from Amazon EC2 [128], Rackspace [118], HP Cloud [30], IBM SmartCloud Enterprise [130] and GoGrid [66]. All the providers detailed about their protection mechanisms in their respective security white-paper or specific web-pages which are directly accessible from their homepage, whereas information related to HP Cloud’s protection mechanisms is in its security white-paper but the paper itself is not easily accessible from the web-site. This study has to perform a normal web-search for its security white paper.

- **Scaling:** These values indicate capability of provider to scale up/down and scale out. Higher value is assigned to provider that have both the scaling capabilities available to its resources. IBM SmartCloud Enterprise [43] and HP Cloud [31] which
were assigned average value, offer only horizontal scaling support by allowing to add and delete as many instances as customer needs. Whereas Amazon EC2 [19], Rackspace [119] and GoGrid [69] offers both vertical and horizontal scaling. All the information related to scaling is either derived from provider blogs or frequently asked questions. Amazon is the only provider who has a dedicated easily accessible web-page related to scaling.

- **API:** API allows customers to operate with different layers of cloud. A higher value is assigned to provider who has API support and also inter-cloud API support like HP Cloud - EC2 Compatibility API. Relevant information is derived from Amazon EC2 [17], Rackspace [117], HP Cloud [29], IBM SmartCloud Enterprise needs user login to look into API [51] and GoGrid [62].

- **Tools:** Higher value is assigned to provider who has deeply integrated monitoring tools that give customers more control and monitoring capacity. However, providers are assigned a mid value with simple API support where responses include only status of system, and poor value is assigned to providers who have no API or have only third-party tools to monitor health/status of system. From website information, GoGrid [70] appears to have third party tools for monitoring. Whereas HP Cloud [32] has its monitoring tools in private beta release and have basic API support, so average value was assigned. Amazon EC2 [18], Rackspace [114] and IBM SmartCloud Enterprise [55] have complete set of integrated tools with automated capacity to handle any safety warnings. Although, IBM SmartCloud Enterprise have integrated tools but its information is only accessible through a web-site search.

- **Data Management:** Customers trust a provider more, if it offers more control
of their data. With providers having multiple data centers across continents and crossing state and/or country boundaries, customers need to be aware of data operations, data location and data destruction practices employed by provider. Safe Harbor initiatives [58] and its seven principles ensure more control to user over their data. Higher value is assigned to provider who follows media sanitization guidelines [88] to decommission storage devices. It is interesting to note that providers Rackspace, IBM and GoGrid confirmed that they properly decommission storage devices through their sales chat, but we did not find any relevant documentation on their website confirming the same (confirmed through site search for words “decommissioning”, “sanitization” or “NIST 800-88”). As this study concentrates on user-perceivable factors, we assigned average value to their data management practices. HP Cloud site search yields zero results for both Safe Harbor program and media sanitization search results, hence it was assigned value poor. Relevant information is derived from Amazon [20], Rackspace [121], IBM SmartCloud Enterprise [130] and GoGrid [63].

Table 4.2 summarizes numerical values assigned to metrics we have collected. For qualitative metrics, we used Likert-scale to quantize values defined in table 4.1. For coding of qualitative metrics, see Appendix A.
Table 4.2: Trust evaluation parameters for five cloud providers (Service age in years, Support, Security, Scaling, API, Tools, Interoperability, Data Management - 0 is least satisfactory, 2 is most satisfactory)

<table>
<thead>
<tr>
<th>Providers</th>
<th>Cost/month in $</th>
<th>Credit</th>
<th>Reliability and Availability</th>
<th>Security</th>
<th>Scaling</th>
<th>API</th>
<th>Tools</th>
<th>Interoperability</th>
<th>Data Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>43.8</td>
<td>4.38</td>
<td>99.95%</td>
<td>7</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Rackspace</td>
<td>43.8</td>
<td>2.19</td>
<td>100%</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>HP</td>
<td>15.33</td>
<td>0</td>
<td>99.95%</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>IBM</td>
<td>68.4</td>
<td>0.93</td>
<td>99.9%</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>GoGrid</td>
<td>36.25</td>
<td>8</td>
<td>100%</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

66
To compare metrics we use standard score to normalize them onto a common scale. These normalized values are shown in table 4.3. For example, “cost per month in $” column value(x) are normalized using standard score formula

\[ z = \frac{x - \mu}{\sigma} \]

where \( \mu \) is the mean of the readings and \( \sigma \) is the standard deviation of the readings. So, for monthly cost, we have \( \mu = 41.52 \) and \( \sigma = 17.01 \). Using these values, standard score for each provider is calculated. For Amazon, \( z = \frac{43.8 - 41.52}{17.01} = 0.13 \). To be consistent with the notation of “high value is most satisfactory and less value is least satisfactory” across table, we use \( z = -\left(\frac{x - \mu}{\sigma}\right) \) for only “cost per month in $” where low cost is most satisfactory for user (customer). Similar calculations were performed for other metrics. With the exception of “protection”, which has no standard deviation. In that case we used real values. It is important to note that the score formula provides a convenient normalization vehicle, but the reader should not assume that it also implies an underlying distribution for x values. We do not have enough information about the distribution(s) of the model parameters to be able to say anything about them. All the calculated values are shown in table 4.3.
Table 4.3: Trust evaluation for cloud providers - normalized

<table>
<thead>
<tr>
<th>Providers</th>
<th>Cost/ month in $</th>
<th>Credit</th>
<th>Reliability and Availability</th>
<th>Security</th>
<th>Scaling</th>
<th>API</th>
<th>Tools</th>
<th>Interoperability</th>
<th>Data management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>SLA Uptime</td>
<td>Service Age</td>
<td>Support</td>
<td>Certifications</td>
<td>Protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon</td>
<td>-0.13</td>
<td>0.45</td>
<td>-0.24</td>
<td>1.49</td>
<td>-1.58</td>
<td>2</td>
<td>2</td>
<td>0.82</td>
<td>-0.82</td>
</tr>
<tr>
<td>Rackspace</td>
<td>-0.13</td>
<td>-0.32</td>
<td>0.95</td>
<td>0.09</td>
<td>1.05</td>
<td>-0.5</td>
<td>2</td>
<td>0.82</td>
<td>1.23</td>
</tr>
<tr>
<td>HP</td>
<td>1.54</td>
<td>-1.08</td>
<td>-0.24</td>
<td>-1.31</td>
<td>1.05</td>
<td>-0.5</td>
<td>2</td>
<td>-1.23</td>
<td>1.23</td>
</tr>
<tr>
<td>IBM</td>
<td>-1.92</td>
<td>-0.76</td>
<td>-1.43</td>
<td>-0.84</td>
<td>-1.58</td>
<td>-0.5</td>
<td>2</td>
<td>-1.23</td>
<td>-0.82</td>
</tr>
<tr>
<td>GoGrid</td>
<td>0.31</td>
<td>1.71</td>
<td>0.95</td>
<td>0.56</td>
<td>1.05</td>
<td>-0.5</td>
<td>2</td>
<td>0.82</td>
<td>-0.82</td>
</tr>
</tbody>
</table>

68
These normalized values are depicted on the radar charts below which show multivariate data in two-dimension. The negative values represent values below the mean and positive values represent values above mean. High value is most satisfactory to user (customer) and least value is less satisfactory. Charts are shown for “Reliability and Availability”, “Security” and “Other” attributes. Latter collect all remaining attributes.

4.2.2 “Reliability” and “Availability”

Figure 4.1: Reliability & availability comparison
From the Figure 4.1, Rackspace, HP Cloud and GoGrid with their multi support options like chat, phone, email, ticket, technical guidance appear to stand ahead when compared to AWS and IBM who offer only on-line forum support. Providers IBM and HP, though they are relatively new to Infrastructure-as-a-Service (IaaS) offering when compared to other providers, but they have many years of experience in designing, constructing and operating computing systems (See Appendix A for details). Trust on their effective management and operating procedures may have some impact on some users while considering reliability and availability of their cloud services.

4.2.3 “Security”

From the Figure 4.2, Amazon with its certifications and auxiliary information like CSA CAIQ [11] regarding its security controls stands top when compared to others. While with protection mechanisms, all providers offer extra protection beyond basic firewalls.

4.2.4 “Other” metrics

In the Figure 4.3, from monthly cost point of view, IBM charges relatively higher when compared to others for same configuration of 1 CPU and minimum 1 GB RAM. The discounted monthly plan considered is highly dependent on promotional offers which are specific for a given duration. GoGrid, through its “credit upto” percentage of “10000%” trying to impart confidence among customers (users) about their quality of service standards. How much of this kind of confidence influence trust decision is highly subjective, depending on the subject (user) and their preferences. IBM and HP loses when it comes to scaling because they only offer scaling up/down.

In the Figure 4.4, Amazon, Rackspace and IBM provides deeply integrated monitoring
Figure 4.2: Security comparison
Figure 4.3: Scaling, API, Cost and Credit comparison
Figure 4.4: Data management, Tools and Interoperability comparison
tools. HP Cloud offers simple API which appears to be better than GoGrid which offers only third-party tools for monitoring status and health of system or application. From data management perspective, Amazon stands top when compared to others with its Safe Harbor initiatives and de-commissioning capability.

The model developed in this study is a user-perspective model rather a comparative model like Rodrigues [124] based on available features with cloud providers. The model in this study considers only readily available first-hand information and is not based on any benchmark tests or experiments based on selected metrics. The model tries to avoid third party bias, but does bring in vendor bias (via the information vendor supplies), and of course any bias the user may have. This model also assigns importance to any auxiliary information a vendor is willing to provide (vendor openness) regarding major concerns such as security. This willingness to share may engender trust in a user.

4.2.5 Limitations

The model developed in this study assumes that information offered by a cloud provider on its websites, in its published papers and in its white papers and documentation is good and generated by following good practices and in good faith. Since, we did not conduct any survey of users directly, we do not have direct field validation of the model (this is expected to be future work). However, the model was developed by considering top concerns found in the surveys done by other parties e.g., IDC [81] [138] [86], by evaluation of relevant published work [92] [91] [6] and through consultation of third party state-of-practices assessment such as the most recent CSA top nine cloud security threats [9]. Based on that (and on what is available on vendor sites) we have proposed the metrics that are part of this trust model. It is, of course, possible that there may be other
motivations and metrics that are more important to a particular class of users than the measure we have proposed. For example, if geopolitical considerations enter the picture, it would not be surprising to have as a major trust element the country or political affiliation of cloud provider. Similarly, business competitors are likely to distrust each other’s services. Unless a vendor offers bare-machine loads or can guarantee single-tenancy in a virtual environment that may also become an issue for more security conscious customers. Customer priorities and situations may emphasize different variables differently, and may bring in new variables. However, we believe that it may be difficult to trust a provider unless one is given an option to assess reliability, availability, security, cost, data management, situation awareness (monitoring tools, provenance), regulation compliance, interoperability, and scalability - essentially the basic components of our model. This model does not consider components/capabilities that were domain specific and relatively new services like work-flows, XaaS, HPC/HPD, and domain specific services. The model also did not consider usability of websites while assessing trust. It is highly likely that broken links, ease of use, website experience and other usability factors influence trust decision because no user (customer) may prefer a provider (vendor) with a poorly maintained website. It is also worth noting that some of the metrics could be expressed differently. For example, instead of, or in addition to, consideration of experience in the IaaS market (Service Age), one could consider the overall business experiences of the vendor, e.g., how long they have been in the business, or their financial status etc. That information may be additional component in the trust equation. Appendix table A3 illustrates this for the vendors discussed in this thesis by showing not only their IaaS “age” but also their overall “age”.

Cloud computing itself is still developing and evolving. We believe various providers (including providers compared for this study) continuously evolve and offer existing or
new services that are more technically competent with enhanced functionality than existing offerings. So, the choices available for each metric in the study may constantly change or new metrics may be added. The choices and the encoded values might change but model’s basic idea for assessing trustworthiness is still valid. With evolution, redundant first-hand information might be available to the users (customers) that help users in making a better trust decision.

**Ease of finding**

The model developed in this study derives its input from provider websites, and its published papers and white papers. The ease of finding the relevant information also influence trust decision among users (customers). If the required information is hidden deep in the websites, it might imply that providers either seem the respective information as less relevant or less important to potential customer. Also, the ease of finding depends on the subject (user) who is performing the search on the first-hand information. For an avid web user, even if some required information is hidden deep in websites, user can obtain such information relatively easy either from website search or press releases or frequently asked questions. But the same can not be expected from all potential customers. On the other hand, if a metric is not important when compared to other metrics, user might spend less effort to find relevant information for less important metric. This limitation of easiness can result in different values against metrics for providers in our model depending on the users and their preferences.
Chapter 5

Conclusion

Cloud computing is an emerging paradigm in IT industry. Many organizations are adopting cloud computing for capital benefits and better performance. Following this demand, many providers are offering information and technology utility services with similar functionalities in various configurations and different pricing plans. In this scenario, trust becomes a significant factor in selection of a provider. Trust is a human perception and is based on information. Sometimes it is difficult to determine what information should be used to build trust.

This study develops a user-perception based trust assessment model for cloud provider services. The model assess trust solely on readily available first-hand information, primarily from provider web pages. For qualitative metrics, the model uses Likert scale (0-2) to encode and order importance of property values. A high value is assigned to the choice that instills more confidence among the users (customers). As this model is based on user-perception, the values assigned against each metric might differ depending on the user and their preferences. Finally, we use a convenient normalized function to compare cloud providers against various identified metrics. Every customer (user) might
consider a given trust metric or metrics or new trust metrics while making a decision.

Providers like Amazon with its larger experience in the IaaS market, has good security mechanisms, monitoring tools, scalability and data management capabilities. Providers like HP Cloud, though relatively new (compared to other providers under consideration) offer its services based on OpenStack with good API and customer support. Rackspace and GoGrid promises 100% uptime with pro-active customer support. IBM with its proven best-in-class security offers various enterprise and monitoring tools that accelerate development and test activities at enterprises. IBM recently announced that all of its cloud services and software will be based on an open cloud architecture OpenStack [78]. Thus making three cloud providers (in our study) Rackspace, HP Cloud and IBM working on industry-wide open standards for cloud computing thereby reducing risk of vendor lock-in and proprietary platforms. This should enable construction of hybrid clouds and higher interoperability of clouds.

In the future work we first expect to assess the model using a wide and diverse range of users (empirical data collection), and then possibly extend this model and develop an automated trust assessment tool that would visit vendor sites and analyze the information they offer about their services for trust elements using advance analytics tools, such as those found in SAS and IBM analytics packages. Tool would also analyze third party information and provide a context and external consistency analysis of the information collected first-hand.
REFERENCES


Amazon-EC2. [Last accessed: February 25, 2013].


com/AWSEC2/latest/APIReference/Welcome.html, December 2012. [Last ac-
cessed: February 25, 2013].


[Last accessed: March 5, 2013].


and emerging it platforms: Vision, hype, and reality for delivering computing as


82


83


Appendix A

Coding metrics

All the values assigned to the metrics were based on the information collected from websites, white papers, documentation that were referred on February 25, 2013.

A.1 Cost

Table A.1 illustrates 730 hours calculated monthly cost and monthly discounted plan if any. The information is based on Amazon [23], Rackspace [116], HP [33], IBM [52] and GoGrid [65].

A.2 Service Age

Table A.2 illustrates age (date of inception of its parent company) and service age (age of provider’s Infrastructure-as-a-Service offering). The information is based on Amazon EC2 [13], Rackspace [112], HP Cloud [28], IBM SmartCloud Enterprise [79] and GoGrid [61].
Table A.1: Cost

<table>
<thead>
<tr>
<th>Providers</th>
<th>Monthly Cost in $</th>
<th>Discounted monthly cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>43.8</td>
<td></td>
</tr>
<tr>
<td>Rackspace</td>
<td>43.8</td>
<td></td>
</tr>
<tr>
<td>HP</td>
<td>25.5</td>
<td>15.33</td>
</tr>
<tr>
<td>IBM</td>
<td>68.4</td>
<td></td>
</tr>
<tr>
<td>GoGrid</td>
<td>58.4</td>
<td>36.25</td>
</tr>
</tbody>
</table>

Table A.2: Vendor experience

<table>
<thead>
<tr>
<th>Providers</th>
<th>Vendor Age</th>
<th>Service (IaaS) Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>19</td>
<td>6</td>
</tr>
<tr>
<td>Rackspace</td>
<td>15</td>
<td>4</td>
</tr>
<tr>
<td>HP</td>
<td>56</td>
<td>1</td>
</tr>
<tr>
<td>IBM</td>
<td>90</td>
<td>2</td>
</tr>
<tr>
<td>GoGrid</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>
Table A.3: Support

<table>
<thead>
<tr>
<th>Choices</th>
<th>Rating</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only online forum support</td>
<td>Poor</td>
<td>0</td>
</tr>
<tr>
<td>Online forum support + any one extra support like chat, e-mail, phone, tickets, technical guidance</td>
<td>Medium</td>
<td>1</td>
</tr>
<tr>
<td>All support features like phone, chat, e-mail, tickets, online forums, API support, technical guidance</td>
<td>Good</td>
<td>2</td>
</tr>
</tbody>
</table>

A.3 Support

Table A.3 illustrates choices for support. The parameters for “good” metric are derived from [120].

A.4 Certifications

Table A.4 illustrates choices for certifications. The parameters for “good” metric are derived from [20].

A.5 Protection

Table A.5 illustrates choices for protection mechanisms. The parameters for “good” metric are derived from [128].
<table>
<thead>
<tr>
<th>Choices</th>
<th>Rating</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No certifications or audit reports based on standards like SSAE 16 SOC1, PCI DSS, ISO 27001</td>
<td>Poor</td>
<td>0</td>
</tr>
<tr>
<td>Certifications or audit reports based on SSAE 16 SOC1, PCI DSS and ISO 27001 are available</td>
<td>Medium</td>
<td>1</td>
</tr>
<tr>
<td>SOC2 attestation report in addition to certifications or audit reports based on standards like SSAE 16 SOC1, PCI DSS and ISO 27001. And auxiliary information like Cloud Security Alliance’s Security Assessment initiative Questionnaire (CAIQ) [11] related to security controls is available</td>
<td>Good</td>
<td>2</td>
</tr>
</tbody>
</table>
Table A.5: Protection

<table>
<thead>
<tr>
<th>Choices</th>
<th>Rating</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only basic firewalls support or protect through some third-party services</td>
<td>Poor</td>
<td>0</td>
</tr>
<tr>
<td>Presence of advance protection mechanisms like multi-factor authentication, security groups, security access control lists, virtual private networks, anti-virus, intrusion prevention and detection systems, encryption/decryption in addition to basic firewalls</td>
<td>Good</td>
<td>1</td>
</tr>
</tbody>
</table>

A.6 Scalability

Table A.6 illustrates choices for scalability. The parameters for “good” metric are derived from [19] and [119].

A.7 Application Programming Interface (API)

Table A.7 illustrates choices for API. The parameters for “good” metric are derived from [29].
Table A.6: Scalability

<table>
<thead>
<tr>
<th>Choices</th>
<th>Rating</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No scaling capability</td>
<td>Poor</td>
<td>0</td>
</tr>
<tr>
<td>Either scale-up/down or scale-out capability is available to resources</td>
<td>Medium</td>
<td>1</td>
</tr>
<tr>
<td>Both scale-up/down and scale-out capability available to resources</td>
<td>Good</td>
<td>2</td>
</tr>
</tbody>
</table>

Table A.7: API

<table>
<thead>
<tr>
<th>Choices</th>
<th>Rating</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No APIs available</td>
<td>Poor</td>
<td>0</td>
</tr>
<tr>
<td>Required APIs are available</td>
<td>Medium</td>
<td>1</td>
</tr>
<tr>
<td>Required APIs + other cloud compatibility APIs available like HP Cloud - EC2 compatible API</td>
<td>Good</td>
<td>2</td>
</tr>
</tbody>
</table>
Table A.8: Monitoring Tools

<table>
<thead>
<tr>
<th>Choices</th>
<th>Rating</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No integrated tools or APIs exist to know health/status of system</td>
<td>Poor</td>
<td>0</td>
</tr>
<tr>
<td>Simple APIs like raw request-response APIs exist to know health/status of system</td>
<td>Medium</td>
<td>1</td>
</tr>
<tr>
<td>Deeply integrated tools to monitor pre-selected metrics, set alarms, generate statistics and graphs</td>
<td>Good</td>
<td>2</td>
</tr>
</tbody>
</table>

A.8 Monitoring Tools

Table A.8 illustrates choices for monitoring tools. The parameters for “good” metric are derived from [18] and [114].

A.9 Inter-operability

Table A.9 illustrates choices for interoperability.

A.10 Data Management

Table A.10 illustrates choices for data management. The parameters for “good” metric are derived from [20].
Table A.9: Monitoring Tools

<table>
<thead>
<tr>
<th>Choices</th>
<th>Rating</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No standard or alternatives for interoperability</td>
<td>Poor</td>
<td>0</td>
</tr>
<tr>
<td>Follows standards like OVF 3.0 [136] or uses open source</td>
<td>Good</td>
<td>1</td>
</tr>
<tr>
<td>alternate operating systems like OpenStack [108] and CloudStack [27]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table A.10: Data Management

<table>
<thead>
<tr>
<th>Choices</th>
<th>Rating</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No standards or principles followed for data operations</td>
<td>Poor</td>
<td>0</td>
</tr>
<tr>
<td>Follows safe harbor [58] principles for data operations like notify</td>
<td>Medium</td>
<td>1</td>
</tr>
<tr>
<td>user, provide user with choice to opt out, request permission from</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user before transferring user information to third-parties, have</td>
<td></td>
<td></td>
</tr>
<tr>
<td>relevant controls to implement access, security, integrity and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Follows safe harbor [58] principles and guidelines for media</td>
<td>Good</td>
<td>2</td>
</tr>
<tr>
<td>sanitization NIST SP800-88 depending on information impact level</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>