Security Issues and Countermeasures in Cloud Computing

Conference Paper · December 2015

4 authors:

Mahantesh Birje
Visvesvaraya Technological University
58 PUBLICATIONS **702** CITATIONS
SEE PROFILE

Praveen Challagidad
Basaveshwar Engineering College, Bagalkot
19 PUBLICATIONS **265** CITATIONS
SEE PROFILE

Manisha T. Tapale
K L E Society's College of Engineering and Technology
10 PUBLICATIONS **187** CITATIONS
SEE PROFILE

R.H. Goudar
Visvesvaraya Technological University
90 PUBLICATIONS **1,936** CITATIONS
SEE PROFILE

Cloud computing review: concepts, technology, challenges and security

Mahantesh N. Birje*

Center for Post Graduate Studies,
VTU, Belagavi, Karnataka, India
Email: mnbirje@yahoo.com
*Corresponding author

Praveen S. Challagidad

Department of CSE,
Basaveshwar Engineering College,
Bagalkot, Karnataka, India
Email: praveensc07@gmail.com

R.H. Goudar

Center for Post Graduate Studies,
VTU, Belagavi, Karnataka, India
Email: rhgoudar@gmail.com

Manisha T. Tapale

Department of CSE,
KLE Dr. MSSCET,
Belagavi, India
Email: manishabirje@gmail.com

Abstract: Cloud computing delivers IT-related capabilities as a service through internet to multiple customers and these services are charged based on consumption. Many cloud computing providers such as Google, Microsoft, Yahoo, IBM and Amazon are moving towards adoption of cloud technology leading to considerable escalation in the usage of various cloud services. Amazon is the pioneer in this field because of its more number of architectural features compared to others. To meet the needs of cloud service providers and customers various open source tools and commercial tools are being developed. Though many more developments have been taken place in cloud computing area, many challenges such as security, interoperability, resource scheduling, virtualisation etc. are yet to be fine tuned. This paper reviews cloud computing paradigm in terms of its historical evolution, concepts, technology, tools and various challenges. Systematic literature review (SLR) of 77 selected papers, published from 2000 to 2015 is done to properly understand the nuances of the cloud computing paradigm. Since security is the major challenge in cloud computing, it is discussed separately in detail. This review paper helps researchers who would like to begin their research career in cloud computing area.

Keywords: cloud computing; tools; challenges; security; issues; review.

Reference to this paper should be made as follows: Birje, M.N., Challagidad, P.S., Goudar, R.H. and Tapale, M.T. (2017) 'Cloud computing review: concepts, technology, challenges and security', *Int. J. Cloud Computing*, Vol. 6, No. 1, pp.32–57.

Biographical notes: Mahantesh N. Birje received his BE and MTech degree in Computer Science and Engineering in 1997 and 2005 respectively. He obtained his PhD degree from Visvesvaraya Technological University (VTU), Belagavi, India, in 2012. His current research areas include cloud computing, data mining and security. He has published many papers in reputed international journals and conferences. He is a reviewer for few reputed journals. He has given many invited lectures and has conducted several workshops and seminars for faculty and students. He has executed various academic and administrative responsibilities. Currently, he is working as Professor in the Centre for Post Graduate Studies, VTU, Belagavi.

Praveen S. Challagidad received his BE and MTech degree in Computer Science and Engineering in 2007 and 2009 respectively. His areas of interest include cloud computing, computer networks and security. He has published few papers in conferences and journals. Currently, he is working as an Assistant Professor in the Department of Computer Science, Basaveshwar Engineering College, Bagalkot.

R.H. Goudar is currently working as an Associate Professor in Center for Post Graduate Studies, Visvesvaraya Technological University, Belagavi. He has 12 years of teaching experience at professional institutes across India. He worked as a faculty at International Institute of Information Technology, Pune for four years and at Indian National Satellite Master Control Facility, Hassan, India. He has published over 100 papers in international journals, book chapters and conferences of high repute. His subjects of interest include Semantic Web, network security and wireless sensor networks.

Manisha T. Tapale received her BE and MTech degree in Computer Science and Engineering in 2003 and 2010 respectively. Her areas of interest include cloud computing, database systems and operating systems. She has published few papers in conferences and journals. Currently, she is working as an Assistant Professor in the Department of Computer Science, KLES's College of Engineeing and Technology, Belagavi.

1 Introduction

The term 'cloud' was coined from the computer network diagrams which use it to hide the complexity of infrastructure involved. Cloud computing is gaining a great scope towards IT industries, academics and individual users because of its ease of use, on-demand access to network resources, minimal management effort and reduced cost (Rajnish, 2011). The National Institute of Standards and Technology (NIST, 2014) defines cloud computing as "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".

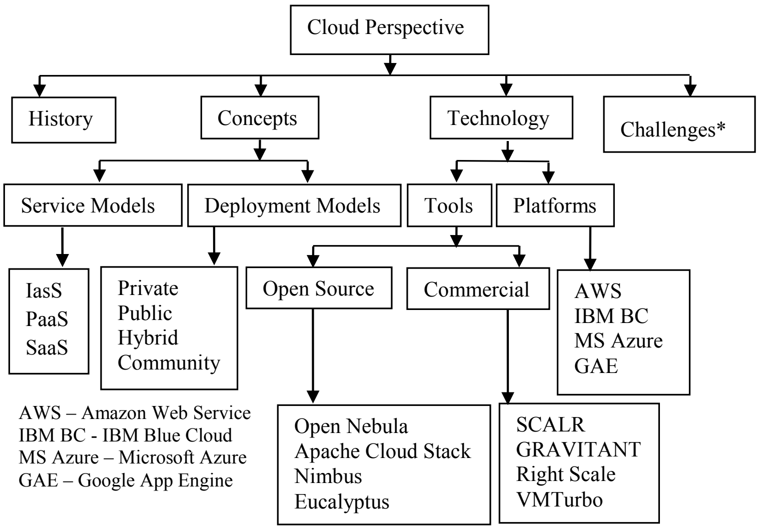
This new cloud computing technology has widely spread in the market and there is an increase in the number of enterprises. It is fascinating the cloud customers by providing services at low price, pay-for-use strategy, distributed nature, rapid delivery of computing resources and provides data storage centre with infinite space and powerful computing capacity for storing and managing data.

The cloud model consists of *five essential characteristics* – broad network access, rapid elasticity, resource pooling, on-demand self-service, and measured service; *three service models* – software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS); and *four deployment models* – public cloud, private cloud, hybrid cloud and community cloud. There are many *advantages of cloud computing* – easy management, cost reduction, uninterrupted services, disaster management and green computing (NIST, 2014).

In spite of the potential gains accomplished from the cloud computing, the organisations are slow in adopting it due to the following limitations: data loss, data cleaning, account hijacking, less control over the process, insider attacks by cloud service providers (CSPs), lack of legal aspects, lack of portability/migration from one service provider to another, less reliable, lack of auditability, less quality of service (QoS) (Joel et al., 2012; Yashpalsinh and Kirit, 2012). These limitations lead to various challenges in adoption of cloud computing such as virtualisation, interoperability, resource scheduling, multi-tenancy, load balancing, security etc. still exist; these challenges are to be fine tuned.

The paper tries to focus on the cloud computing technology considering multiple perspectives. It reviews cloud technology in terms of its historical evolution, concepts, technology and challenges as shown in Figure 1.

Figure 1 Cloud perspective



Note: *Detailed in Section 2.4.

With all of the potential gains and limitations, security is considered as one of the major critical challenges in cloud computing because of shared nature of cloud ecosystem. For example, data in cloud is stored remotely, totally out of the control of the data owner. Actually, security can be an obstacle towards implementation of cloud computing in enterprises, because of the great deal of uncertainty about how security at all levels can be achieved (Ma, 2012). In cloud ecosystem, users lose the control over physical security (Rittinghouse and Ransome, 2010), because users may have to share and store computing resources on cloud servers. Unfortunately these servers are controlled and owned by CSPs. It could be possible that CSPs may themselves modify the user's data. It is also possible for a user's data to be exposed to another user without their knowledge and control. The cloud computing system is based on the trust, what makes security and confidentiality the major issue. Hence security becomes critical issue in cloud computing. This challenge is affecting the widespread adoption of cloud computing. Therefore it is discussed separately in detail.

The remainder of this paper is organised as follows: Section 2 presents cloud perspective in terms of history, concepts, technology and challenges. Sub-section 2.1 describes how cloud is entered into the market; Sub-section 2.2 describes cloud concepts; Sub-section 2.3 describes the technology in terms of architectural features and tools; and Sub-section 2.4 discusses various challenges in cloud. Section 3 describes security in cloud computing paradigm. Sub-section 3.1 describes security objectives; Sub-section 3.2 describes security issue and its countermeasures. Conclusions and future directions are presented at the end.

2 Cloud perspective

The cloud paradigm can be viewed in different perspectives depending on how the user wants to perceive cloud technology. The paper perceives and describes the cloud technology in terms of its history, concepts, technology and challenges of a cloud computing.

2.1 History

Table 1 describes how cloud is entered into the market from the past (Bashe, 1986; Tim, 1989; Bennett et al., 2000; Freiberger and Michael, 2000; Finch, 2006). Though it took some time to agree and start using the cloud technology, many IT companies have come forward to offer various types of cloud services.

Table 1 Cloud retrospective

Year	*Description*
2000–2005	Dot.com bubble burst leads to introduction of cloud.
2006	Amazon enters the cloud market.
2007–2008	The market disagree on the understanding of cloud.
2008	Cloud market expands as more vendors join.
2008–2009	IT attention shift to emerging private cloud.

Table 1 Cloud retrospective (continued)

Year	*Description*
2009–2010	The open source cloud movement takes hold, example Openstack.
2009–2011 and 2012	Cloud computing finds its way, become popular, every organisation started implementing cloud platform. In the year 2011, a new deployment model called hybrid cloud born.
2012–2013 and 2014	The Australian Bureau of Statistics (ABS) 2013–14 Business Characteristics Survey (BCS) showed that one in five businesses had been using some form of paid cloud computing service. The overall results showed that between 2012–13 and 2013–14, businesses using information technology increased. When examining the areas where businesses used IT to a high extent, 60% used it for accounting, and 55% used it for invoicing business processes (http://www.zdnet website, ABS article, online, 24 September 2015).
2014–2015	Many IT companies moving towards adoption of cloud technology because of its effectiveness and fast growth.

2.2 Concepts

Cloud computing is a delivery of extremely scalable IT related facilities as a service through the internet to multiple clients. Clients can have a choice of different cloud service models based on his/her requirements (Edwards, 2012). It involves many services to clients generally called as XaaS, where X stands for any kind of service like hardware, software, platform, infrastructure, data and business etc. that the cloud offers to clients. Basically, X involves three kinds of services which are widely used such as SaaS, PaaS and IaaS.

This section describes cloud constituents such as three service models and four deployment models. The three service models are briefly explained below:

2.2.1 Software as a service

SaaS is a collection of software or services or applications available on cloud that can be accessed by end users based on subscription. End users consume the software application services through this service delivery model directly over network according to on-demand basis. Examples: Whats app, Facebook, Twitter, Google Docs and spreadsheets, salesforce.com, NETSUITE, and IBM LotusLive.

2.2.2 Platform as a service

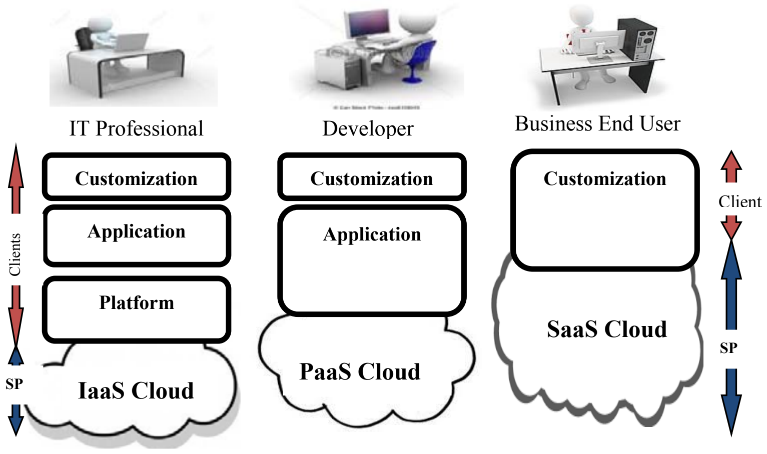
PaaS is a collection of runtime environments such as software and development tools hosted on the provider's servers. It acts as background that provides runtime environment, software deployment framework and component on pay to facilitate the direct deployment of application level assets or web applications. Application developers, implementers, testers, and administrators can go for developing, testing and deploying their software in this platform and here entire software life cycle is operated (Suruchee and Raut, 2014). Examples: Amazon AWS, Rollbase, jelastic.com, force.com, Google App Engine (GAE), Microsoft Azure, and LONG JUMP.

2.2.3 Infrastructure as a service

IaaS is a collection of servers, storage, and networks. Virtualisation is the backbone behind this model where resources like network, storage, virtualised servers, routers and so are consumed by user through virtual desktop, provided by CSP. Based upon usage of per CPU hour, data GB stored per hour, value added services used (e.g., monitoring, auto-scaling etc.), network bandwidth consumed, network infrastructure used per hour, users are charged. Examples: rackspace, VMWare, Joyent, Storage services provided by Amazon S3, and Computation services provided by Amazon EC2.

Figure 2 depicts how customers have a choice of different cloud service models.

Figure 2 Cloud service models (see online version for colours)



SP: Service Provider

The four deployment models of cloud computing are almost the same except their scope and accessibility given to the cloud users. Figure 3 depicts cloud deployment models and their features. These models are briefly explained below:

1 *Public cloud/external cloud*

This cloud allows cloud environment as openly accessible to all users. Public cloud is off premise in which various enterprises can be used to deliver the services to users by taking it from the third party. Examples: Sun Cloud, Google AppEngine, IBM's Blue Cloud, Amazon Elastic Compute Cloud (EC2), and Windows Azure Service Platform.

2 Private cloud/internal cloud

This cloud referred to on-premise cloud used to provide the high level control over cloud services and infrastructure which is controlled or owned by an organisation. It is built specifically to provide the services within an organisation for maintaining the security and privacy. Examples: Seagate and RedHat.com etc.

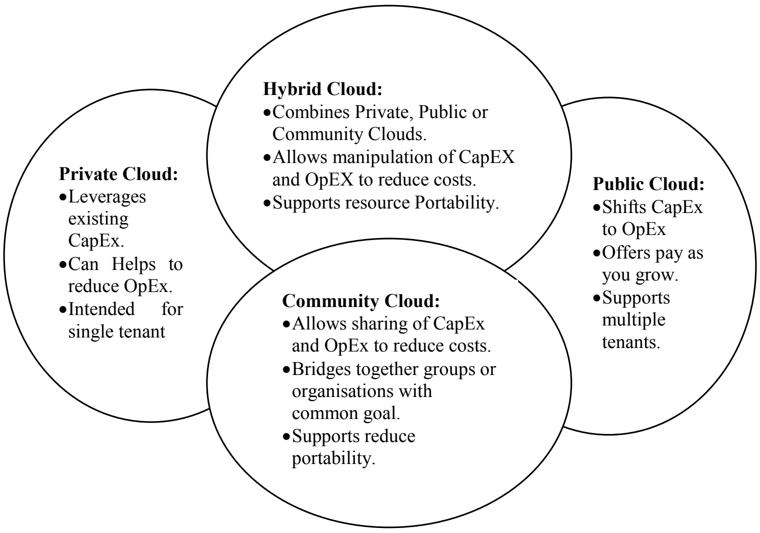
3 *Hybrid cloud/virtual private cloud (*VPC*)*

This cloud combines both public cloud and private models where cloud computing ecosystem is hosted and managed by third party (off-premise) but only an organisation can privately use some dedicated resources. Examples: Cybercon.com (US Microsoft Hybrid Cloud), and Bluemix.net (IBM Cloud App Development), etc.

4 *Community cloud*

This cloud allows the cloud computing environment can be shared or managed by a number of related organisations. Example: soourcingfocus.com.

Figure 3 Cloud deployment models


Hybrid Cloud:
•Combines Private, Public or Community Clouds.
•Allows manipulation of CapEX and OpEX to reduce costs.
•Supports resource Portability.
Private Cloud:
•Leverages existing CapEx.
•Can Helps to reduce OpEx.
•Intended for single tenant
Public Cloud:
•Shifts CapEx to OpEx
•Offers pay as you grow.
•Supports multiple tenants.
Community Cloud:
•Allows sharing of CapEx and OpEx to reduce costs.
•Bridges together groups or organisations with common goal.
•Supports reduce portability.

2.3 Technology

This section describes various cloud platforms based on their features, and also various tools that are available in the market.

2.3.1 Cloud platforms

Table 2 describes various features of four different cloud platforms (Amazon, IBM Blue Cloud, Microsoft Azure and Google App Engine). Though many CSPs like Amazon, IBM, Microsoft and Google are adopting cloud technology, Amazon is a pioneer. Amazon Web Service platform has many features imbibed within it. It is still growing faster compared to other CSPs.

Table 2 Features of different platform

Features	*Platforms*			
	AWS	*IBM Blue Cloud*	*Microsoft Azure*	*GAE*
SLA (Alexander 2009)	AWS as service interface	SOA-based web service	SOA-based web service	Yes
Reliability (Pol, 2009; IBM Introduces Ready-to-Use Cloud Computing, 2014; Charlie and Ramanathan, 2010; Rajkumar et al., 2011)	Highly reliable	Reliable	Azure Fabric	Sandbox
Auto-scaling	Cloud Watch	Maximum	Azure fabric	Memcache
Elasticity (Martijn, 2012)	Elastic Load Balancing Service	No	Yes, as per service usage	AppLoad Balancer
Virtualisation (Bala and Girish, 2012)	VPC	Xen and Power VM	VM role runs an image VHD	Guest VMs
Availability zone (Jinesh, 2011)	Yes, separate zone is present	Yes, separate zone is not present	Yes, separate zone is not present	Yes, separate zone is not present
Privacy	VPC uses IPSec Tunnel mode	Yes	AppFabric and Geneva framework	App controller
Storage (David et al., 2010; Dong and Hui, 2010)	Elastic Block Storage (EBS) and Simple Storage Service (S3)	SVC cluster (IBM Total Storage San Volume Controller) and XIV Nextra	Sql Azure Storage databases, data sync	Google APIs connect open store
Security	AWS Identity and Access Management	Blue Gene Supercomputer, System Z Parallel Sysplex	Yes	App controller

2.3.2 *Tools*

Tools provide environment and platform for developing various cloud services, implementing their own algorithms and mechanisms. Various tools that are available in the market for implementing cloud computing technology are discussed here. Cloud tools are categorised into open source tools and commercial tools.

2.3.2.1 Open source tools

Open source tools can be used/accessed with free of cost such as Open Nebula, Apache Cloud Stack, Nimbus and Eucalyptus. Table 3 describes all aforementioned tools. Though many open source tools are available in the market, Apache Cloud Stack would be the good open source tool to deploy cloud techniques because it is used for public cloud, part of it is a hybrid cloud, has good features and secure AJAX console.

Table 3 Open source tools

Tool name	*Features*	*Security*	*API*	*Cloud type*
Open Nebula: It adopts computing, storage, security, monitoring, virtualisation and networking in their data centres (Open Nebula, 2015).	Cloud bursting, on-demand provision of virtual data centres, multiple zones, multi-VM application management.	Fine-grained ACLs and user quotas. Integration with LDAP, Active Directory.	AWS EC2 and EBS APIs. OGF OCCI APIs.	Private
Apache Cloud Stack: Easy integration with existing portal and it is fully AJAX-based solution compatible with most of the latest internet browsers (Apache Cloud Stack, 2015).	Powerful API. Multi-role support. On-demand virtual data centre hosting. Dynamic workload management. Broad network virtualisation capabilities.	Secure AJAX console access. Secure single sign on. Secure cloud deployments. MPLS support in the cloud.	CloudStack provides an API that's compatible with AWS EC2 and S3 for organisations that wish to deploy hybrid clouds.	Public, hybrid
Nimbus: Power and versatility of infrastructure clouds to scientific users. It allows combining Nimbus, OpenStack, Amazon, etc. (Nimbus, 2015).	Support for proxy credentials for scientific community, batch schedulers, best-effort allocations and others are special targeting features.	-------	EC2/S3 an API as a compatible IaaS.	Private, public
Eucalyptus: It helps customers to design and deploys cloud solutions more quickly (Eucalyptus, 2015).	Multi-cluster tunnelling and LDAP integration.	----------	----------	Private, hybrid

Note: ----------: not applicable.

2.3.2.2 Commercial tools

Commercial tools such as RightScale, Gravitant, VMTurbo and Scalr etc. are briefly described in this section. Though many commercial tools are available in the market, Scalr is a best fit for those looking to implement and/or design their own algorithms or projects.

- *RightScale:* Automated management of workflow of messages and jobs as they move through the computational, storage, and retrieval processes is achieved by RightScale grid framework. Mechanism to implement the elasticity of the grid processing solution is also provided by this tool. Monitoring of the input queue(s) of the system is done continuously, when certain criteria are met; additional worker instances are launched to handle the increased processing load. When the number of items in the input queue comes down, these servers are automatically terminated, thus it takes full advantage of utility computing (Brian, 2013).

- *Gravitant:* Gravitant's cloudMatrix CSB platform is a market leading cloud services brokerage and management platform that integrates multiple cloud provider services (internal or external) into a catalogue and provisioning portal, so enterprises can optimise the consumption of cloud services. The core services and features enabled by Gravitant's cloudMatrix CSB platform and are delivered as packages through a single user interface on myGravitant.com and through a white labelled internal broker platform. Enterprises can deploy these capabilities independently or as an integrated suite based on their cloud services needs. The cloudMatrix CSB platform is technology agnostic and will work and leverage current cloud platforms and business systems deployed by the enterprise (Gravitant, 2014).

- *VMTurbo:* It provides a demand-driven cloud and virtualisation control platform for enterprise businesses (VMTurbo, 2015).

- *Scalr:* Scalr is the best fit for those looking to explore the platform and to build and test their projects on their own. It delivers self-service access to cloud infrastructure and acts as an intermediary management layer between cloud infrastructure and engineering, and provides the ownership of information security back to IT department hands. Scalr enforces cloud infrastructure security such as governance and compliance to create and enforce policies on the basis of budgets, configurations, and user access across entire cloud portfolio. Network policy enforcement allows securing cloud infrastructure by regulating the use of networks. Enabling to deliver single sign-on (SSO) across private and public clouds is achieved through authentication and authorisation techniques (Scalr, 2012).

2.4 Challenges of cloud computing

Despite the potential gains achieved from the cloud computing, the organisations are slow in accepting it due to the following limitations: data loss, data cleaning, account hijacking, less control over the process, insider attacks by the CSP's, lack of legal aspects, lack of portability/migration from one service provider to another, less reliable, lack of auditability, less QoS (Joel et al., 2012; Rajnish, 2011; Yashpalsinh and Kirit, 2012). These limitations lead to the issues or challenges such as – security, interoperability, virtualisation, data leakage, resource sharing, load balancing, multi-tenancy, and Service Level Agreement (SLA) (Daniel and Rich, 2009; Gurudatt et al., 2012). Figure 4 depicts various challenges of cloud computing. Description of challenges, their difficulties and possible solutions are given in Table 4.

Figure 4 General challenges (see online version for colours)

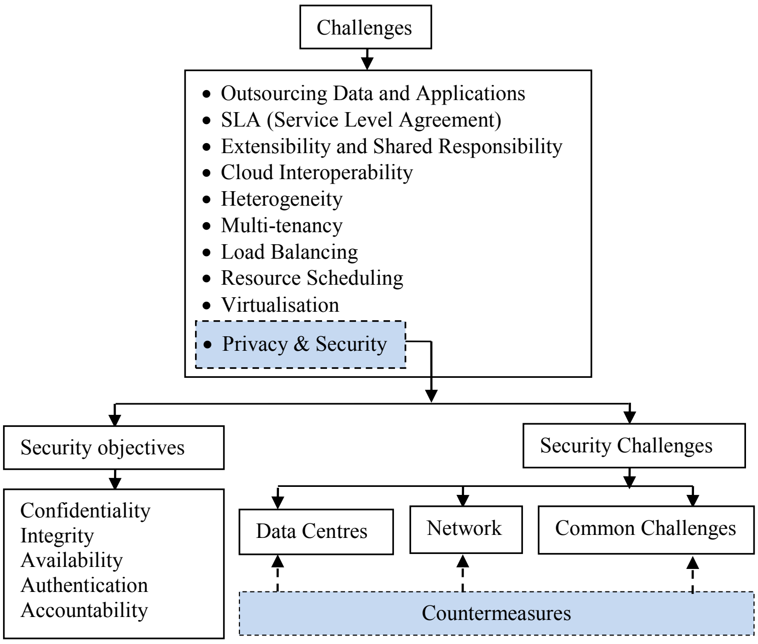


Table 4 General challenges

Challenges/issues	*Difficulties*	*Possible solutions*
Outsourcing data and applications Cloud user host data and applications on cloud servers by relying on third parties to make decisions about user data and platforms. Cloud Computing provides access to data, but the challenge is to ensure that only authorised user can gain access to it (Takabi et al., 2010).	It is very difficult to have appropriate mechanisms to prevent cloud providers from using customers' data in a way that has not been agreed upon.	Any technical means could not completely prevent cloud providers from abusing customer data in all cases, so a combination of techni and non-technical can be used to achieve this. Clients need to have significant trust in their provider's technical competence and economic stability.
SLA It is essential for customers to get assurances from providers on service delivery. Typically, these are provided during SLAs negotiated between the providers and customers (John et al., 2009).	1 Definition of SLA specification. 2 Different cloud offerings will need to classify different meta specifications.	Advanced SLA methods need to regularly integrate user advice and customisation features into the SLA assessment framework.

Table 4 General challenges (continued)

Challenges/issues	*Difficulties*	*Possible solutions*
Extensibility and shared responsibility Cloud providers and customers must share the responsibility for security and privacy in cloud computing environments, but sharing levels will differ for different delivery models, which in turn affect cloud extensibility (Takabi et al., 2010).	1 Providing privacy and security to all deployment models is difficult. 2 Private clouds could also demand more extensibility to accommodate customised requirements so providing security in that stage is difficult.	Provide the security to each level of resource sharing and make use of available, advanced and new protection mechanisms to provide privacy and security to each level. the hardware
Cloud interoperability Which provide the freedom to customer to switch from alternative vendors/offerings/ providers simultaneously to optimise resources at various stages in an organisation (Gundeep et al., 2012).	1 Cloud APIs makes it very difficult to merge cloud services with an organisation's own existing legacy systems. 2 Aim of interoperability is to detect the faultless fluid data across local applications, across clouds and among clouds and it is difficult to detect.	Standardisation approach would be a good solution to deal with this issue. For example optimising in outsourcing a number of insignificant functions to cloud services offered by different vendors.
Heterogeneity Cloud providers use various hardware and software resources to build cloud environments. To some extent, resource virtualisation achieves high-level system homogeneity, but the same infrastructure being used to support different tenants with different protection and system requirements can generate difficulties (Takabi et al., 2010).	A potential issue are: 1 If a client subscribes to different cloud providers for different services then the assumptions that each of these cloud providers make in building the services can severely affect the emergent trust and security properties. 2 Generates integration challenges. 3 In a multi-tenant environment, the protection requirements for each tenant might differ, which can make a multi-tenant cloud a single point of compromise.	Designing of more efficient privacy and security mechanisms could overcome the said difficulties.
Multi-tenancy This means that the cloud platform is shared and exploited by number of clients (Bhaskar et al., 2009; Xiao and Xiao, 2012).	1 Opponents who may also be legal cloud clients may utilise the co-residence issue. 2 Many security issues such as data breach, computation breach, flooding attack, etc., are incurred. 3 It supplies new vulnerabilities to the cloud platform.	There are three kinds of multi-tenancy enablement approaches such as sharing, arbitration and virtualisation. To achieve the full potential of multi-tenancy three issues continue to be solved such as resource sharing, security isolation, customisation.

Table 4 General challenges (continued)

Challenges/issues	*Difficulties*	*Possible solutions*
Load balancing Load balancing can be defined as assigning a part of job to another or idle computer to improve the efficiency and optimise the use of resources (Tsai et al., 2010).	Continuous monitoring of the components becomes overhead and when one becomes non-responsive, the load balancer needs to inform that stop sending traffic to overloaded system.	Effectively implementing load balancer by using new mechanism.
Resource scheduling Means assigning the resources such as hardware, software, process time, communication bandwidth and applications to the processes.	Implementing multitasking and multiplexing techniques in scheduler is somewhat tedious task.	Implement scheduler to have advanced algorithm and mechanism which concern about the throughput, latency, specifically: turnaround time, response time and fairness/waiting time.
Virtualisation IT virtualisation is the abstraction of physical infrastructures such as servers, data centres, networks capabilities and storage resources (Tsai et al., 2010).	1 Rise of high density. 2 Reduced IT load affects power usage effectiveness (PUE). 3 Dynamic IT loads. 4 Lower redundancy requirements are possible.	Physical infrastructure efficiency measured as PUE will increase if the power and cooling infrastructure is right-sized to the new lesser overall load, then necessity for idleness in the physical infrastructure may be reduced by using highly virtualised data centre design and IT fault-tolerance functioned with a high level.
Privacy and security A third party causes the security and privacy issues more critical when outsourcing the data and business applications (Bhaskar et al., 2009).	Finding the solutions for the attacks: Malware-injection, flooding, accountability check problem, browser security, securing data in transmission, identity and access management is difficult.	Requires novel techniques to tackle with. Some of the countermeasures are described in Table 5.

3 Security

In a cloud, responsibility for employing and preserving efficient security mechanisms are in the hands of the providers. To reduce their customer's panic of the cloud, these providers want to convince them that their data and applications will be accurately secured (Bernsmed et al., 2012). Security is considered to be a dangerous obstacle for cloud computing in its lane to success (Bhaskar et al., 2009), and hence it is a major challenge. This section discusses security objectives and issues.

3.1 Security objectives

Five key objectives such as confidentiality, integrity, availability, authenticity and accountability are most important for computer security.

These five objectives represent the basic security objectives for data, information and computing services (William, 2010).

- *Confidentiality:* It is used to preserve authorised limitations on accessing information and disclosure, including means for protecting personal privacy and proprietary information. It has two types:
  1. data confidentiality: it assures that private or sensitive information is made unavailable or disclosed to illegal persons
  2. privacy: it assures that persons control or influence what information feel right to them is collected and stored and by whom and to whom that information is disclosed.
- *Integrity:* Protecting against inappropriate information destruction or modification, including ensuring information non-repudiation and authenticity. It has two types:
  1. data integrity: it assures that information and programs are altered only a specified and authorised manner
  2. system integrity: it assures that a system makes its intended function in superior way, free from inadvertent or deliberate illegal handling of the system.
- *Availability:* Ensuring reliable and timely access to and use of information.
- *Authenticity:* Assurance that a message, transaction, or additional exchange of information is from the source it claims to be from. It entails evidence of identity.
- *Accountability:* The security goal is that creates the requisite for actions of an entity to be traced uniquely to that entity.

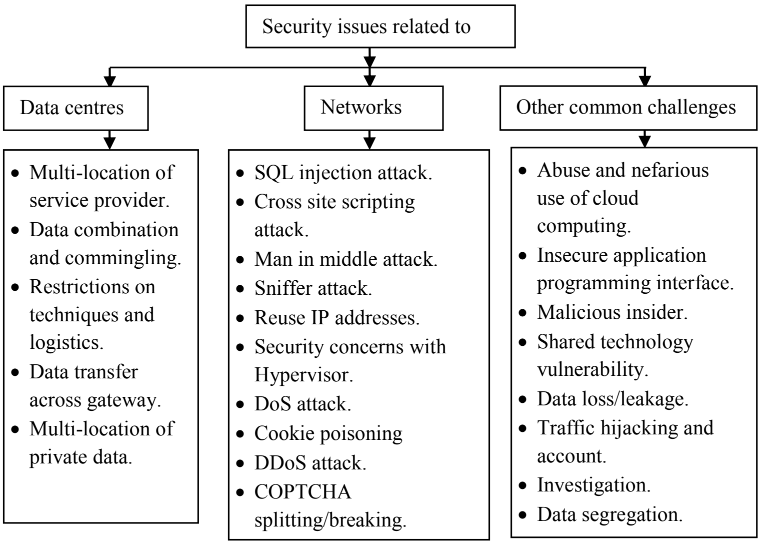
3.2 Security issues

Security is a critical issue in cloud computing paradigm that affects the widespread adoption of cloud computing technology (Ennajjar et al., 2014). Amazon network host service, S3 (Simple Storage Service was broken down for four hours in 2010; this incident made people aware of the risks that may be encountered in users data stored in cloud (Zhang et al., 2012). Other incidents related to traditional web application and data storage security concerns are still occurring in high profile companies like Google, Microsoft, Twitter and Amazon such as data phishing, downtime, data loss, password weakness and compromised hosts running botnet and other threats associated to network and applications (Chen et al., 2010; Subashini and Kavita, 2011).

Another side of security issue that breaches is related to surveillance. In 2013, it has been exposed that the National Security Agency (NSA) and other US law enforcement and national security agencies have access to information from telecommunications and internet providers via secret court orders as specified by USA Patriot Act and the Foreign Intelligence Surveillance Act (FISA) to obtain electronic data from third parties. As this news become accepted widely, it led to a number of questions about appropriate access to an individual's digital information within the USA and other countries, which affects attitudes about using public cloud providers (Castro, 2013).

These technical and legal plan related security issues lead to decrease in the confidence of cloud technology adoption. Similarly security issues related to the location of data centre, network and other common issues also hinder the growth of cloud technology adoption. These issues are depicted in Figure 5. Description of various issues related to the location of data centre, network and other common issues are described in Table 5, Table 6 and Table 7 respectively.

Figure 5 Security issues


Security issues related to
Data centres
Networks
Other common challenges
• Multi-location of service provider.
• Data combination and commingling.
• Restrictions on techniques and logistics.
• Data transfer across gateway.
• Multi-location of private data.
• SQL injection attack.
• Cross site scripting attack.
• Man in middle attack.
• Sniffer attack.
• Reuse IP addresses.
• Security concerns with Hypervisor.
• DoS attack.
• Cookie poisoning
• DDoS attack.
• COPTCHA splitting/breaking.
• Abuse and nefarious use of cloud computing.
• Insecure application programming interface.
• Malicious insider.
• Shared technology vulnerability.
• Data loss/leakage.
• Traffic hijacking and account.
• Investigation.
• Data segregation.

3.2.1 Data centre

Table 5 discusses security issues related to data centre along with their possible countermeasures. In this table, the countermeasure for the issue data transfer across gateway has not been discussed; this need to be fine tuned. This could be a one of the research objectives to find out an efficient mechanism which overcomes this issue.

3.2.2 Networks

Table 6 discusses the security issues related to networks along with their possible countermeasures. In this table, the countermeasures for the every issue has been discussed but there is need for more efficient algorithms and techniques in issues such as SQL injection attacks, Google hacking, sniffer attacks, cookie poisoning and CAPTCHA splitting.

3.2.3 Other challenges

Table 7 discusses the security issues related to networks along with their possible countermeasures. In this table, the countermeasures for the every issue has been discussed but there is a need for an efficient techniques for the issue insecure applications programming interface, traffic hijacking and account service, data loss/leakage, investigation and data segregation.

Table 5 Security issues related to data centre

Data centres security issues (Jensen et al., 2009; Rameshwari, 2013)	*Countermeasures*
Multi-location of the service provider: The cloud clients for example private user or business user also have to ensure that how the cloud service provider performs their affirmed services. Hence, this makes possible for cloud client to make a straight relationship with the provider, and control over their private data (Jensen et al., 2009).	*Protection from attacks at various levels:* Fundamental technical security issues which cover security of web service using XML and SOAP messages, and SSL with transport layer security are provided (Arshad et al., 2009). A technique to guarantee quality of service for compute intensive workloads in term of security attack, encryption algorithm and authentication has been proposed. Haizea is used as an open source resource manager for giving an estimation to achieve security and to perform experimentations. Guest operating system integrity, VM specific attack, backdoor protection, etc., are considered as security requirements.
Data combination and commingling: The cloud client should ensure that its confidential data is stored separately from others or not. If private data are combined with those of other client's data, then it is very vulnerable to attack. For example, viruses might be broadcasted from one client to other clients. The attack might influence the integrity and data availability of other companies existing in the same environment, if another client is the victim of a hack attack.	*Data security:* Rules and regulations for privacy enhancement methods and tools are discussed (Macquarir University, 2008). Privacy in terms of lawful compliance, user trust and data leakage for confidential data are provided. A standard to secure data-in-transit in the cloud has been proposed (Ji, 2009). Large scale search system for the function of information switch over between internet communities leads to creation of covert channels (Rizwana and Sasikumar, 2012). To control data from covert channel an agent-based security model is presented. This could resolve the problem of data leakage in the cloud ecosystem. The privacy issue by retaining data control to user to increase self-assurance is discussed (Descher et al., 2009). Some requirements and means to overcome from the cloud computing attacks are proposed.
Restrictions on techniques and logistics: To assure storage locations of cloud computing client's data might be very difficult or even impossible for cloud service provider. For example, Amazon has data centres everywhere; the client's data is stored automatically across them unless Amazon uses particular servers for dedicated client therefore the cloud service provider should address logistics (Vahid and Seyed, 2012).	*Architecture security:* Challenges of cloud computing security can be handled practically by performing security assessment is discussed (Sonali, 2014). Definition of an architecture ontology approach for secure cloud computing discussed (Kevin, 2009). The architecture of cloud comprises a variety of security mechanisms such as storage security, access management, network security, and security API. These mechanisms implanted in the cloud architecture to endow with secure cloud computing.

Note: ----------: not applicable.

Table 5 Security issues related to data centre (continued)

Data centres security issues (Jensen et al., 2009; Rameshwari, 2013)	*Countermeasures*
Data transfer across the gateway: It is prerequisite to know where the cloud service provider will store the data for transferring data across the country gateway. Because of multi-locations of the XaaS user, the cloud service provider and the cloud owner in the cloud computing ecosystem. Requesting, processing and storing of data usually done in different places of inside or outside countries (Vahid and Seyed, 2012).	--------------------------
Multi-location of the private data: If business stores private data or confidential data in the third party's device, then it is vulnerable, because the business's private data are present in someone else's computer, and in someone else's facility. Then, much stuff goes wrong. 1 CSPs may force to go away from business 2 CSPs may decide to block the data if there is a dispute 3 It is rather difficult for a company to know where its data will be hosted.	*Using mirage image management system:* The issues related to secure virtual-machine images management that encapsulate each application of the cloud are addressed by this system. This system has three major components, such as image maintenance, access control, and image transformation by running filters has been proposed (Vahid and Seyed, 2012).

Note: ----------: not applicable.

Table 6 Security issues related to networks

Network security issues (Khan et al., 2012)	*Countermeasures*
SQL injection attacks: A standard SQL code is made malicious by injecting malicious code. Consequently the attackers are able to access sensitive information and gain unauthorised access to a database.	*SQL injection attacks:* To check the SQL injection attacks filtering techniques etc. can be used to sanitise the user input. A proxy-based architecture can be used to prevent SQL injection attacks which dynamically detects and extracts user's inputs for suspected SQL control sequences has been proposed (Liu et al., 2009).
Cross site scripting (XSS) attacks: Injecting malicious scripts into web is done through these attacks. This is achieved through two methods such as stored XSS and reflected XSS. In case of stored XSS, resources managed by the web application stores the attack script permanently. In case of a Reflected XSS, the attack is reflected back to the user immediately and it is not permanently stored (Vahid and Seyed, 2012a).	*Cross site scripting (XSS) attacks:* Various techniques such as web application vulnerability detection technology, active content filtering, content-based data leakage prevention technology, has been proposed to prevent XSS attacks (Kevin, 2009). These techniques implement a variety of methodologies to identify and fix security flaws. A blueprint-based approach reduces the dependency on web browsers towards identifying not trusted content over the network (Ter and Venkatakrishnan, 2009).

Table 6 Security issues related to networks (continued)

Network security issues	*Countermeasures*
Man in middle attacks (MITM): Here an attacker/entity tries to interrupt by injecting fake information and to have awareness of the significant data transferred in an enduring conversation between a sender and a receiver.	*Man in the middle attacks:* Various tools implementing strong encryption technologies such as Airjack, Ettercap, Dsniff, Cain, Wsniff, etc. has been developed to provide protect against them. A few of them are separate endpoint and server security processes, evaluating software as a service security; evaluating virtualisation at the end-point has been proposed to tackle with this attack (Neha and Chetan, 2015). In all cases, the security practices employed in the organisation's private network and private cloud. However, in case of a public cloud implementation, network topology need to be modified to implement the security features (Pearson, 2009).
Google hacking: Google App engine is one of the well-known solution providers in the scope of cloud computing. Google geo-distributed architecture is used here as a distributed architecture. In Google hacking attack, loophole of all the possible systems are searched by the hacker, once he finds out those systems having loopholes then he wishes to hack those systems.	To avoid these threats, an application security should be evaluated at the various levels of the three service delivery models in cloud such as IaaS, PaaS and SaaS. In an IaaS, security policies applied by the customer and the application's management are mostly not concerned by cloud providers. The following measures should be taken care of while designing the application in PaaS and SaaS: Common vulnerabilities associated with the web must be safeguarded by implementing standard security measures. Traditional implementation of authorisation and authentication techniques should be tested properly before implementation. To avoid data recovery issues in case of a sudden attack back up policies such as continuous data protection (CDP) should be implemented (Zhou et al., 2010).
Sniffer attacks: Applications initiate this which can capture packets streaming in a transmission media of the network. Recording of the traffic/data linked to other systems on the network through the network interface card (NIC) can be done with the help of sniffer program.	*Sniffer attacks:* Address resolution protocol (ARP) and round trip time (RTT) can be implemented in malicious sniffing detection platform to discover a sniffing system running on a network has been proposed (Zouheir et al., 2004).
Cookie poisoning: An unauthorised access to a webpage or to an application modifications are made to the contents of cookie. Cookies basically contain the user's identity related credentials and once these cookies are accessible, the content of these cookies can be forged to imitate an authorised user.	*Cookie poisoning:* Avoidance of cookie poisoning has described in Vieira et al. (2010). This can be avoided by cleaning cookie regularly or implementing an encryption method for the cookie data.

Table 6 Security issues related to networks (continued)

Network security issues	*Countermeasures*
Reused IP addresses: In this case, when a meticulous user/customer moves away from network coverage, then the IP-address assigned earlier to him is allocated to a new user/customer. Occasionally even though the old IP address is being assigned to a new user still there are possibilities of fetching the data by some other user is significant because the address still present in the DNS cache and the data belonging to a particular user may become accessible to some other user breaching the privacy of the earlier user.	*Using client-based privacy manager:* This helps have more privacy of the sensitive data and to reduce the risk of data leakage and provides additional privacy related benefits processing in the cloud. The important features of the privacy manager are: 1 Obfuscation, which automatically complicates some or all of the fields in a data structure before it is sent off. 2 Preference setting this is a method for permitting users to set their preferences about the switching of personal data. 3 Data access this is a module that permits users to access personal information in the cloud, in order to see what is being held about them, and to check its accuracy. 4 Feedback module is used for managing and displaying feedback to the user regarding usage of his personal information, personae that allow the user to choose between multiple personae when interacting with cloud services has been proposed (Abdul et al., 2012).
Security concerns with the hypervisor: Virtualisation is main backbone of cloud computing. In a virtualised environment, hypervisor is a controller known as virtual machine manager (VMM) which allows running of multiple operating systems simultaneously on a system. Since number of operating systems would be running on a solitary hardware platform thus it is impossible to monitor all such systems and hence it is difficult to maintain the security of the operating systems (Liu et al., 2009).	*Security concerns with the hypervisor:* Hacker can do changes to any of the guest operating systems and get a hold on all the data passing through the hypervisor if a hacker is able to get hold on the hypervisor then it harms cloud ecosystem which is discussed in Cloud Security Alliance (2013). Based on the understanding of behaviour of different devices in the hypervisor architecture, an advanced cloud protections system can be developed to monitor the activities of the guest virtual machines (VMs) and inter-communication between the various infrastructure components (Flavio and Roberto, 2011; Wu et al., 2010).
Denial of service attacks: A DoS attack is an effort to make unavailability of services assigned to the authorised users. In this attack, a large number of requests are flooded to service which is been provided by the server hence the service turn out to be unavailable to the authorised user.	*Denial of service attacks:* Use of an intrusion detection system (IDS) is popular method of protection against these attacks (Vieira et al., 2010). A defence federation is used for guarding against such attacks (Ruiping and Kin, 2011). Every cloud is loaded with separate IDS. Information exchange is the basis for working different intrusion detection systems. The whole system is made alerted in case a particular cloud attacked by the cooperative IDS. A decision on trustworthiness of a cloud is taken by voting, and sees to it that the overall system performance is not hindered.

Table 6 Security issues related to networks (continued)

Network security issues	*Countermeasures*
Distributed denial of service attacks: DDoS is an advanced adaptation of DoS, this attack is achieved by flooding the destination severs with huge numbers of packets such that the target server is not able to handle it. This is done to deny the important services running on a server. In this attack it is spread from different dynamic networks which have already been compromised unlike the DoS attack.	A group-based logic for protecting against the DDoS attack (Gellman, 2009). IDS in the virtual machine is used to protect the cloud from DDoS attacks (Aman and Yogesh, 2010). A SNORT like intrusion detection mechanism is implemented onto the virtual machine for sniffing all traffics, either incoming, or outgoing. Another method used to guard against DDoS is to implement intrusion detection systems on all the physical machines which have the user's virtual machines (Claudio et al., 2010). This technique had been illustrated in Nurmi et al. (2009) to perform reasonably well in a Eucalyptus cloud.
CAPTCHA splitting/breaking: Recently, it has been noticed that the spammers are able to split the CAPTCHA, according to information provided by the Hotmail and Gmail service providers (Jenni, 2007). By making use of the audio system spammers are able to read the CAPTCHA characters.	*CAPTCHA breaking:* By integrating various authentication techniques along with CAPTCHA identification which are adopted by companies such as Facebook, Google etc., would be a suitable option against CAPTCHA splitting. Various techniques such as expanding the string length and using a variation in the background implementing letter overlap, variable fonts of the letters used to design a CAPTCHA, can be used to avoid CAPTCHA breaking (John, 2009). Single frame zero knowledge CAPTCHA design principles are able to resist any attack method of static optical character recognition (OCR).

Table 7 Security issues related to other challenges

Other common issues (Gordon and Richard, 2012; Padhy et al., 2011)	*Countermeasures*
Abuse and nefarious use of cloud computing: For example, use of botnets to spread malware and spam. A public cloud can be infiltrated by attackers. Attackers discover a way to insert malware to thousands of computers and use the cloud infrastructure to attack other machines.	To confront this threat, one should strict initial registration and validation processes. Another effective measure is to use enhanced credit card, fraud monitoring system, and comprehensive introspection of customer network traffic. Another useful step to take is to monitor public blacklists for one's own network blocks.
Insecure application programming interface: APIs or software interfaces must have extremely secure access control, authentication, encryption and activity monitoring mechanisms – especially when third parties begin to fabricate on them.	*Confronting insecure application programming interfaces:* To deal this threat, one should analyse the security model of cloud provider interfaces. Another effective measure is to guarantee standard authentication and access controls are implemented in concert with encrypted transmission, and identify the dependency chain associated with the API.

Table 7 Security issues related to other challenges (continued)

Other common issues (Gordon and Richard, 2012; Padhy et al., 2011)	*Countermeasures*
Malicious insiders: People or group of people wish to insert some unwanted, garbage data across the network.	*Confronting malicious insiders:* To confront this threat, one should implement strict supply chain management and conduct a supplier assessment completely. Another effective measure is to make out necessity of human resource as part of legal contracts, and required transparency into overall information security and management practices, as well as agreement reporting. Another step is to determine security breach notification processes.
Traffic hijacking and account service: Traffic hijacking and account service two issues that cloud users need to be aware. These threats range from spam campaigns, to denial-of service attacks and man-in-the-middle attacks, to phishing.	*DNS attacks:* Although using DNS security measures such as Domain Name System Security Extensions (DNSSEC) minimises the effects of DNS threats but still there are cases when these security measures are proves to be insufficient then the lane between a sender and a recipient gets redirected through some malicious link.
Shared technology vulnerability: IaaS provides sharing of infrastructure. Unfortunately, this is not designed for the devices on which this infrastructure is based. Strong compartmentalisation and monitoring are required to ensure that customers do not line on each other's 'territory'.	*Confronting shared technology vulnerabilities:* To confront this threat, one should implement security best practices for installation/ configuration. Another effective measure is to monitor environment for unauthorised changes/activity, and promote strong authentication and access control for administrative access and operations. Other useful steps are to enforce SLAs for patching and vulnerability remediation, and to perform vulnerability scanning and configuration audits.
Data loss/leakage: Data is always in danger of being lost or stolen; it may be by deletion without a backup, by illegal access or by loss of the encoding key. This is important concerns for businesses, because they not only stand to lose their reputation in the market, but are also forced by law to keep it safe.	*Confronting data loss/leakage:* To confront this threat, one should implement strong API access control. Another effective measure is to encrypt and protects data integrity in transit and analyse data protection at both run time and design. Other good steps are to implement generation of strong key, storage and management, and destruction practices, and contractually before it are released into the pool demand providers to clean persistent media. The manager can also contractually specify provider backup and preservation strategies.
Regulatory compliance: Traditional service providers are concerned to external audits and security certifications. Customer trust diminishes if CSPs does not stick to these security audits.	CSPs must ensure the data security in natural and man-made disasters. Generally, data is replicated across multiple sites. However, in the case of any such surplus event, provider must do an immediate and complete restoration.

4 Conclusions and future directions

This paper reviewed cloud computing paradigm in terms of various perspectives such as concepts, cloud platforms, tools, and challenges. The history of cloud computing evolution is presented in Sub-section 2.1. Three service models (SaaS, PaaS and IaaS) and four deployment models (private, public, hybrid and community cloud) are described in Sub-section 2.2. Description of cloud platforms by different CSPs (Amazon, IBM, Microsoft, Google) are discussed in Sub-section 2.3; it also discussed open source tools (Open Nebula, Apache CloudStack, Nimbus and Eucalyptus) and commercial tools (RightScale, Gravitant, VMTurbo and Scalr). Various general challenges of cloud computing and the number of difficulties involved in those challenges are identified and the possible solutions are presented in Sub-section 2.4. These solutions would help the researchers to have proper directions for future research and to get into the efficient implementation of the techniques. Security objectives and security issues related to the location of data centres, network and other common issues are discussed in Sub-sections 3.1 and 3.2 respectively. There is a need of designing efficient solutions to address security issues such as data transfer across gateway, long-term viability, compromised services, regulatory compliance, virtualisation in cloud computing paradigm.

We believe this paper helps researchers who would like to begin their research career in the area of cloud computing.

References

Abdul, W.K. et al. (2012) 'A literature survey on data privacy/protection issues and challenges in cloud computing', *IOSR Journal of Computer Engineering (IOSRJCE)*, Vol. 1, No. 3, pp.28–36.

Alexander, Z. (2009) *'Google App Engine', Seminar on Internetworking, from Google website,* [online] http://www.cse.hut.fi/en/publications/B/5/papers/1Zahariev_final.pdf (accessed 21 January 2014).

Aman, B. and Yogesh, B.D. (2010) 'Securing cloud from DDoS attacks using intrusion detection system in virtual machine', *Proceeding of the Second International Conference on Communication Software and Networks (ICCSN'10)*, pp.260–264.

Apache Cloud Stack (2015) *World Wide Web Consortium* [online] https://www.cloudstack.apache.org/docs/ (accessed 23 January 2014).

Arshad, J., Townend, P. and Xu, J. (2009) 'Quantification of security for compute intensive workloads in clouds', *15th International Conference on Parallel and Distributed Systems*, School of Computation, pp.478–486.

Bala, P.P. and Girish, P. (2012) *Windows Azure – The Cloud Computing Platform*, White Paper, Tata Consultancy Services.

Bashe, C.J. (1986) *IBM's Early Computers*, MIT Press Series in the History of Computing, MIT Press, Cambridge, Mass [online] http://mitprss.mit.edu/books/ibms-early-c (accessed November 19 2014).

Bennett, K., Layzell, P., Budgen, D. et al. (2000) 'Service-based software: the future for flexible software', *Seventh Asia-Pacific Software Engineering Conference (APSEC)*, Singapore.

Bernsmed, K. et al. (2012) 'Thunder in the clouds: security challenges and solutions for federated clouds', *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings.*

Bhaskar, P., Rimal, E.C. and Ian, L. (2009) 'A taxonomy and survey of cloud computing systems', *Fifth International Joint Conference on INC, IMS and IDC*, 978-0-7695-3769-6/.

Brian, A. (2013) *RightScale Grid: Grid Computing Applications in the Cloud*, Technical White Paper, RightScale, Inc.

Castro, D. (2013) *How Much Will PRISM Cost the U.S Cloud Computing Industry?*, August 2013 [online] http://www2.itif.org/2013-cloud-computing-costs.pdf (accessed 21 January 2015).

Charlie, K. and Ramanathan, V. (2010) *Windows Azure™ Security Overview*, White technical paper [online] http://www.research.ijcaonline.org/volume98/number1/pxc3897184.pdf (accessed 12 March 2015).

Chen, Y., Paxson, V. and Katz, R.H. (2010) *What's New About Cloud Computing Security* [online] http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html (accessed 14 March 2015).

Claudio, M., Roberto, B. and Roberto, C. (2010) 'Integrating a network IDS into an open source cloud computing environment', *Sixth International Conference on Information Assurance and Security*, USA, pp.265–270.

Cloud Security Alliance (2013) *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0* [online] https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf (accessed 15 August 2014).

Daniel, N. and Rich, W. (2009) 'Eucalyptus: an open source cloud computing infrastructure', *9th IEEE/ACM International symposium on Cluster Computing and the Grid*.

David, C. et al. (2010) *Introducing the Azure Services Platform*, Sponsored by Microsoft Corporation [online] http://www.ijcsit.com/docs/Volume%202/vol2issue2/ijcsit2011020205.pdf (accessed 15 March 2015).

Descher, M., Masser, P., Feilhauer, T., Tjoa, A.M. and Huemer, D. (2009) 'Retaining data control to the client in infrastructure cloud', *International Conference on Availability, Reliability and Security*, pp.9–16, Dornbirn.

Dong, X. and Hui, L. (2010) 'Reviewing some cloud computing platforms', *Proc. of Second International Symposium on Networking and Network Security (ISNNS '10)*, Jinggangshan, China.

Edwards, J.D. (2012) *Choosing a Deployment Strategy that Fits*, Oracle White Paper, Oracle JD Edwards Cloud Computing.

Ennajjar, I., Tabbi, Y. and Benkadour, A. (2014) 'Security in cloud computing approaches and solutions', *2014 Third IEEE International Colloquium in Information Science and Technology (CIST)*, Tetouan.

Eucalyptus (2015) *World Wide Web Consortium* [online] http://www.eucalyptus.com/reference-architecture/ (accessed 23 January 2015).

Finch, C. (2006) *The Benefits of the Software-as-a-Service Model*, Computer World Management [online] http://www.computerworld.com/s/article/107276/The_Benefits_of_the_Software_as_a_Service_Model (accessed 17 March 2015).

Flavio, L. and Roberto, D.P. (2011) 'Secure virtualization for cloud computing', *Journal of Network and Computer Applications*, Vol. 34, No. 4, pp.1113–1122, Academic Press Ltd., London, UK.

Freiberger, P. and Michael, S. (2000) *Fire in the Valley: The Making of the Personal Computer*, 2nd ed., McGraw-Hill, New York.

Gellman, R. (2009) *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing* [online] http://www.worldprivacyforum.org/.../wprivacyforum/.../WPF_Cloud_Privacy (accessed 12 April 2015).

Gordon, R. and Richard, M. (2012) 'Security issues of a publicly accessible cloud computing infrastructure', *2012 IEEE 11th International Conference on Trust, Security and Privacy in Cloud Computing and Communications*, Liverpool.

Gravitant (2014) 'The power to transform', *Transformational Cloud Services Brokage and Management Empowering Enterprises to Optimize Cloud Consumption* [online] http://www.gravitant.com/hybrid-it-cloud-service-broker/.

Gundeep, S.B., Prashantkumar, S., Krishen, K.K. and Seema, K. (2012) 'Cloud security: analysis and risk management of VM images', *Proceeding of the IEEE International Conference on Information and Automation Shenyang*, China.

Gurudatt, K., Nikita, C., Ruchitra, C., Rani, W. and Rajnikant, P. (2012) 'Cloud security challenges', *7th International Conference on Telecommunication Systems, Services, and Applications [TSSA]*, 978-1-4673-4550-7/12/2012 IEEE.

IBM Introduces Ready-to-Use Cloud Computing (2014) [online] http://phys.org/news114365558.html (accessed 23 November 2014).

Jenni, S.R. (2009) 'A survey on virtual machine security', *Seminar of Network Security*, Helsinki University of Technology.

Jensen, M., Schwenk, J. and Gruschka, N.I. (2009) 'On technical security issues in cloud', *IEEE International Conference on Cloud Computing*, Germany, pp.109–116.

Ji, H.K. (2009) 'A Benchmark of transparent data encryption for migration of web application in cloud', *Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, Chengdu, pp.735–740.

Jinesh, V. (2011) *Architecting for the Cloud: Best Practices*, White paper, Amazon Web Service [online] https://aws.amazon.com/blogs/aws/new-whitepaper-architecture-for-the-cloud-best-practices/.

Joel, G., Darren, E., Robin, R. and Qing, T. (2012) 'Benefits and challenges of three cloud computing service models', *2012 Fourth International Conference on Computational Aspects of Social Networks [CASoN]*, 978-1-4673-4794-5/12/2012 IEEE.

John, E.D. (2009) *Spammers Break Hotmail's CAPTCHA Yet Again*, Tech-world.

John, H., Lorti, M.K. and Bruce, P. (2009) *Data Security in the World of Cloud Computing*, IEEE Security & Privacy, Co-published by the IEEE Computer and Reliability Societies, Vol. 7, No. 4, pp.61–64.

Kevin, J. (2009) *Secure Cloud Computing: An Architecture Ontology Approach* [online] http://sunset.usc.edu/gsaw/gsaw2009/s12b/jackson.pdf (accessed 12 February 2015).

Khan, A.W. et al. (2012) 'A literature survey on data privacy protection issues and challenges in cloud computing', *IOSR Journal of Computer Engineering (IOSRJCE)*, Vol. 1, No. 5, ISSN: 2278-0661.

Liu, A., Yuan, T. and Stavrou, A. (2009) *SQLProb: A Proxybased Architecture towards Preventing SQL Injection Attacks*, 8–12 March, SAC, Honolulu, Hawaii, USA.

Ma, X. (2012) 'Security concerns in cloud computing', *Fourth International Conference on Computational and Information Science*.

Macquarir University (2008) *Guide to Implementation of Assessment Policies*, September [online] https://staff.mq.edu.au/public/download/?id=40234 (accessed 10 April 2015).

Martijn, Z. (2012) *How to Optimize the Usability of Cloud Computing, Without Losing Control?*, Dutch Cloud B.V., Netherlands.

National Institute of Standards and Technology (NIST) (2014) Computer Security Resource Center [online] http://www.csrc.nist.gov [online] (accessed 15 July 2014).

Neha, K. and Kumar, C. (2015) 'Security in cloud: attacks & prevention techniques', *International Journal of Latest Trends in Engineering and Technology (IJLTET)*, Vol. 5, No. 1, pp.85–88.

Nimbus (2015) *World Wide Web Consortium* [online] http://www.nimbusproject.org/ (accessed 23 January 2015).

Nurmi, D., Wolski, R., Grzegorczyk, C., Obertelli, G., Soman, S., Youseff, L. and Zagorodnov, D. (2009) 'The Eucalyptus open-source cloud-computing system', *Proceedings of the 9th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID '09)*, pp.124–131.

Open Nebula (2015) *World Wide Web Consortium* [online] https://www.opennebula.org/about/ (accessed 23 January 2015).

Padhy, R.P., Patra, M.R. and Satapathy, S.C. (2011) 'Cloud computing: security issues and research challenges', *IRACST – International Journal of Computer Science and Information Technology & Security (IJCSITS)*, Vol. 1, No. 2, pp.136–146.

Pearson, S. (2009) 'Taking account of privacy when designing cloud computing services', *Software Engineering Challenges of Cloud Computing*, pp.44–52, Vancouver, BC.

Pol, M.A. (2009) *Terena – IBM Cloud Computing*, IBM Emerging Business Incubation Center Dublin, Ireland.

Rajkumar, B., James, B. and Andrzej, G. (2011) *Cloud Computing Principles and Paradigms*, John Wiley & Sons, Inc. Publications, Indian edition.

Rajnish, C. (2011) 'A survey on cloud computing security, challenges and threats', *International Journal on Computer Science and Engineering [IJCSE]*, Vol. 3, No. 3, pp.1227–1231, ISSN: 0975-3397.

Rameshwari, M. (2013) 'Security on cloud computing: a review', *International Journal of Science and Research (IJSR)*, Vol. 4, No. 4, pp.1722–1729.

Rittinghouse, J. and Ransome, J. (2010) *Cloud Computing: Implementation, Management and Security*, CRC Press, Taylor & Francis Group, Boca Raton.

Rizwana, S. and Sasikumar, M. (2012) 'Security issues in cloud computing: a survey', *International Journal of Computer Applications*, Vol. 44, No. 19, pp.4–10.

Ruiping, L. and Kin, C.Y. (2011) 'Mitigating DDoS attacks with transparent and intelligent fast-flux swarm network', *IEEE Network*, Vol. 25, No. 4, pp.28–33.

Scalr (2012) *Reconciling Cloud and Security*, White Paper [online] http://www.scalr.com/lp2/white-paper/reconciling_cloud_and_security (accessed 15 January 2015).

Sonali, R.C. (2014) 'Network security issues in cloud computing', *International Journal of Pure and Applied Research in Engineering and Technology*, Vol. 2, No. 9, pp.761–768.

Subashini, S. and Kavita, J. (2011) 'A survey on security issues in service delivery models of cloud computing', *Journal of Network and Computer Applications*, Vol. 34, No. 1, pp.268–274.

Suruchee, V.N. and Raut, A.B. (2014) 'A comprehensive study on cloud computing', *International Journal of Computer Science and Mobile Computing*, Vol. 3, No. 4, pp.733–738.

Takabi, H., Joshi, J.B.D. and Ahn, G-J. (2010) *Security and Privacy Challenges in Cloud Computing Environment*, IEEE Computer and Reliability Societies, Vol. 8, No. 6, pp.24–31.

Ter, L. and Venkatakrishnan, V.N. (2009) 'BluePrint: robust prevention of cross-site scripting attacks for existing browsers', *30th IEEE Symposium on Security and Privacy*, pp.331–346.

Tim, B.L. (1989) 'Information management: a proposal', *World Wide Web Consortium* [online] http://www.w3.org/History/1989/proposal.html (accessed 12 January 2015).

Tsai, W.T., Sun, X. and Balasooriya, J. (2010) 'Service-oriented cloud computing architecture', *Seventh International Conference on Information Technology*, 978-0-7695-3984-3/10/2010 IEEE.

Vahid, A. and Seyed, R.T. (2012) 'Security threats and countermeasures in cloud computing', *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, Vol. 1, No. 2, pp.206–215.

Vieira, K., Schulter, A., Westphall, C.B. and Westphall, C.M. (2010) 'Intrusion detection techniques for grid and cloud computing environment', *IT Professional*, Vol. 12, No. 4, pp.38–43, IEEE Computer Society.

VMTurbo (2015) [online] https://ww.vmturbo.com (accessed 26 March 2015).

William, S. (2010) 'Cryptography and network security', *Principles and Practice*, 5th ed., Pearson Publication, Indian edition.

Wu, H., Ding, Y., Winer, C. and Yao, L. (2010) 'Network security for virtual machines in cloud computing', *5th Intel Conference on Computer Sciences and Convergence Information Technology,* pp.18–21, Seoul.

Xiao, Z. and Xiao, Y. (2012) 'Security and privacy in cloud computing', *IEEE Communications Surveys & Tutorials*, accepted for publication.

Yashpalsinh, J. and Kirit, M. (2012) 'Cloud computing – concepts, architecture and challenges', *2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET]*, 978-1-4673-0210-4/12/2012.

Zhang, S., Chen, X., Zhang, S. and Huo, X. (2010) 'Cloud computing research and development trend', *Second International Conference on Future Networks, (ICFN 2010)*.

Zhou, M., Zhang, R., Xie, W., Qian, W. and Zhou, A. (2010) 'Security and privacy in cloud computing: a survey', *Sixth International Conference on Semantics Knowledge and Grid (SKG)*, p.105.

Zouheir, T., Hamza, R., Kamel, K. and Mounir, F. (2004) 'Malicious sniffing system detection platform', *Proceedings of the International Symposium on Applications and the Internet (SAINT'04)*, pp.201–207.