Secure Cloud Computing

Benefits, Risks and Controls

Mariana Carroll, Alta van der Merwe
CSIR Meraka Institute
School of Computing, University of South Africa
Pretoria, South Africa
MCarroll@csir.co.za, alta@meraka.org.

Paula Kotzé
CSIR Meraka Institute
Institute for ICT Advancement, Nelson Mandela Metropolitan University
South Africa
paula.kotze@meraka.org.za

***Abstract*—Cloud computing presents a new model for IT service delivery and it typically involves over-a-network, on-demand, self-service access, which is dynamically scalable and elastic, utilising pools of often virtualized resources. Through these features, cloud computing has the potential to improve the way businesses and IT operate by offering fast start-up, flexibility, scalability and cost efficiency. Even though cloud computing provides compelling benefits and cost-effective options for IT hosting and expansion, new risks and opportunities for security exploits are introduced. Standards, policies and controls are therefore of the essence to assist management in protecting and safeguarding systems and data. Management should understand and analyse cloud computing risks in order to protect systems and data from security exploits. The focus of this paper is on mitigation for cloud computing security risks as a fundamental step towards ensuring secure cloud computing environments.**

Keywords: cloud computing; benefits; controls; risks.

I. INTRODUCTION

During the 1990s, data centre floor space, power, cooling and operating expenses increased and lead to the adoption of grid computing and virtualization. Through grid computing users could plug in and use a metered utility service. By allowing the infrastructure to be virtualized and shared across consumers, service providers needed to change their business model to provide for remotely managed services and lower costs. As services became more and more distributed, a need for integration and management of these services became important and lead to the emergence of service-oriented architecture (SOA). Cloud computing developed out of this need to provide IT resources 'as-a-service'.

Cloud computing is characterised by consumers who use cloud services as needed, who consume shared resources as a service that can rapidly and elastically scale up or down as needed, who pay only for what is used and who access services over a networked infrastructure. Cloud computing is changing the current IT delivery model for services. Benefits for business and IT include reduced costs, scalability, flexibility, capacity utilisation, higher efficiencies and mobility. Predictions for growth indicate massive developments for and implementations of cloud computing services, including that the cloud computing services market is likely to reach between $150 billion in 2014 [1-2] and $222.5 billion in 2015 [3].

As with any technology, though, cloud computing raises many concerns including security, management and control, disaster recovery and business continuity, supplier management, regulations and legislations, and the lack of standards and guidelines. In order to minimise the impact of these concerns, risk mitigation is imperative if organisations want to take advantage of the many benefits of cloud computing while protecting and safeguarding systems and data. Management is under pressure to ensure adequate mitigation of risks to reduce the impact on business. Risk mitigation strategies and the implementation of controls are further complicated since standards and guidelines dealing with cloud computing security do not exist [4-6].

The focus of this paper is to provide recommendations for the mitigation of cloud computing security risks as a fundamental step towards the development of guidelines and standards for secure cloud computing environments.

Section II provides an overview of cloud computing. The research process followed in identifying the benefits, risks and mitigating controls is described in section III. Cloud computing benefits are discussed in section IV and the cloud computing risks, with specific focus on security risks, are described in section V. Security risks and considerations for mitigation are discussed in section VI, followed by the conclusion in section VII.

II. BACKGROUND

A. What is cloud computing

The IT environment evolved from mainframes to client servers, the Internet, virtualization and cloud computing. Cloud computing provides a shared pool of configurable IT resources (e.g. processing, network, software, information and storage) on demand, as a scalable and elastic service, through a networked infrastructure, on a measured (pay-per-use or subscription) basis, which needs minimal management effort, is based on service level agreements between the service provider and consumers, and often utilises virtualization resources. This frequently takes the form of web-based tools or applications that users can access and use through a web browser as if it was a program installed locally on their own computer. Cloud computing can include software (software-as-a-service), hardware (infrastructure-as-a-service), or

technology tools (platform-as-a-service) that are available on demand, as opposed to licensed software and tools, or purchased hardware. The type and quality of service and cloud computing requirements are, in most cases, agreed upon in a service level agreement (SLA) between the service provider and consumers.

B. Cloud architecture and role players

In a traditional IT environment, applications and other IT infrastructure are maintained in-house. Cloud computing offers software, IT platforms, storage or other infrastructure in the cloud, somewhere in the infinite reaches of the Internet. Services are delivered by a third party supplier, which masks the complexities of the underlying infrastructure from the end user. The building blocks of cloud computing are hardware and software architectures that enable infrastructure scaling and virtualization. Cloud computing architecture therefore comprises cloud services (measured services) delivered by cloud service providers (third parties, suppliers or brokers) to cloud consumers (end users, enterprises, or IT staff) over a networked infrastructure (i.e. the Internet or a virtual private network). Such cloud computing services are governed by contractual agreements (SLA) that specify consumer requirements and the provider's commitment to them.

Cloud services and products are based on an infrastructure of four core layers, namely hardware (physical parts, i.e. servers and the network components), software (i.e. operating systems), virtualization resources (enabling pooling and sharing of computing resources) and applications (i.e. Salesforce.com and Google Apps). The service developer creates, publishes and monitors the cloud based applications and services for use by both the cloud consumer and cloud provider. Management and monitoring represent one of the most important layers in the cloud stack and are mostly provided by the cloud service providers. Management and monitoring include metering, provisioning, monitoring, billing, capacity planning, providing security to customers, SLA management, and reporting to provide transparency for both the provider and consumer of the utilised service.

C. Cloud computing characteristics

A level of consensus is emerging over cloud computing characteristics. In the literature, most authors refer to the five characteristics defined by The US National Institute of Standards and Technology (NIST). These five key cloud computing characteristics as described by Mell and Grance [7], are *on-demand self-service* (automatic provisioning of computing capabilities), *broad network access* (capabilities are available over a networked infrastructure), *resource pooling* (resources are pooled together to serve multiple consumers using a multi-tenant model), *rapid elasticity* (rapid and elastic provisioning of capabilities to quickly scale up or down as required) and *measured service* (automatic control and optimisation of resources utilising a pay-per-use model).

D. Cloud computing deployment models

Cloud computing services and technology are deployed over different types of delivery models based on their characteristics and purpose. The deployment models include public (external), private (internal), community, hybrid, and virtual private clouds.

A *public cloud* is where resources, such as storage and applications, are made available to multiple consumers by a service provider, via a web application or web service over the Internet. The resources are therefore located at an off-site location that is controlled and managed by the service provider. These are typically low-cost or pay-on-demand and highly scalable services [6-12]. A *private cloud* infrastructure is operated for a single organisation. It may be managed by the organisation or a third party and may exist at an on-site or off-site location. Private cloud services offer the provider and the user greater control over the cloud infrastructure, improving security, compliance, resiliency and transparency. Private clouds, however, require capital expenditure, operational expenditure and a highly skilled IT team [6-12]. *Community clouds* are controlled and shared by several organisations and support a specific community that has shared interests, such as mission, policy, security requirements and compliance considerations. It may be managed by the organisations or a third party and may exist at on-site or off-site locations, and the members of the community share access to the data and applications in the community cloud. Community cloud users therefore seek to exploit economies of scale while minimizing the costs associated with private clouds and the risks associated with public clouds [6-12]. A *hybrid cloud* is a combination of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability. Applications with less stringent security, legal, compliance and service level requirements can be outsourced to the public cloud, while keeping business-critical services and data in a secured and controlled private cloud [6-12]. Another deployment model, described by fewer sources, is one in which service providers utilise public cloud resources and infrastructure to create a private or semi-private *virtual cloud* (interconnecting to internal resources), usually via virtual private network (VPN) connectivity [13].

E. Cloud computing service models

Cloud computing is any hosted service that is delivered over a network, typically the Internet. Cloud services are broadly divided into three categories, namely Infrastructure-as-a-Service (IaaS) (includes the entire infrastructure stack), Platform-as-a-Service (PaaS) (sits on top of IaaS and adds an additional layer with application development capabilities and programming languages and tools) and Software-as-a-Service (SaaS) (builds upon IaaS and PaaS and provides a self-contained operating environment delivering presentation, application and management capabilities).

SaaS is the delivery of applications that are licensed for use, and which are provided to consumers on demand over a public (Internet) or private network. SaaS is most often implemented to provide business software functionality at a low cost while allowing the consumers to obtain the same benefits of commercially licensed, internally operated software without the complexity of installation, management, support, licensing and high initial costs [6-7, 9, 12, 14-22].

PaaS is the delivery of facilities that are required to support the complete lifecycle of building and delivering applications and services over a cloud infrastructure, and therefore is a set of programming languages and software and product development tools. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems or storage, but has control over the deployed applications and possibly the configuration set-up. PaaS services include application design, development, testing, deployment, hosting, team collaborations, web service integration, database integration, security, scalability, storage, state management and versioning [6-7, 9, 12, 14-22].

IaaS is the delivery of computer infrastructure (resources) as a fully outsourced service over a public or private network, including servers, software, data centre space, virtualization platforms and network equipment. IaaS therefore offers advantages such as near instantaneous scalability, cost-effectiveness and flexibility [6-7, 9, 12, 14-22].

Apart from the SaaS, PaaS and IaaS service models, the following alternatives or extensions to these services exist: Communication-as-a-Service (CaaS); Security-as-a-Service (SECaaS); Monitoring-as-a-Service (MaaS); Storage-as-a-Service (STaaS); Desktop-as-a-Service (DTaaS); Compute Capacity-as-a-Service (CCaaS); Database-as-a-Service (DBaaS); Hardware-as-a-Service (HaaS); IT-as-a-Service (ITaaS); and Business Process-as-a-Service (BPaaS).

F. Security in cloud computing

Even though these cloud computing components and characteristic provide compelling solutions to IT problems and many advantages, cloud computing is not risk-free or completely secure. Management is responsible for taking care of security risks to protect systems and data. Governance, risk and control of cloud computing are therefore critical in the performance of any assurance management process. Governance is enforced through the implementation of policies and procedures. These policies and procedures should be based on best practices and should be aligned between business and IT objectives. Risk identification and analysis is important to prioritise the implementation (extent and time frame) of governance and controls, as well as to establish scope for reviewing or auditing cloud computing environments. Based on the identification and analysis of risks, controls should be designed and implemented to ensure that necessary actions are taken to address risks and to achieve business and IT objectives.

This paper aims to provide some guidelines to assist management with the identification of risks and recommendations for the mitigation of cloud computing security risks. The process we followed in conducting this research is described in section III, followed by cloud computing benefits (section IV), cloud computing risks (section V) and recommendations for the mitigation of security risks (section VI) arising from our research.

III. RESEARCH PROCESS

To identify cloud computing security risks and make recommendations for the mitigation of the risks identified, we employed a qualitative research approach in an extensive study of existing resources that refer to cloud computing benefits, risks and/or consideration or mitigation of cloud computing risks. We used representative primary and secondary resources (selecting a sample of work or texts in order to understand and conceptualise the necessary information). The literature review included available subject databases, online library catalogues, published articles, relevant textbooks, industry-specific information and trusted resources from the Internet. The benefits and risks identified from the extensive literature review were also tested against primary data collected through interviews. Interviews were conducted with 15 participants, representing various South African organisations and a variety of different industries. The criteria for participation in the interviews included a cloud computing and/or virtualization interest, current or planned implementation of cloud computing and/or virtualization, and current placement in senior management or higher positions. The interviews were conducted during July 2010 and October 2010. The construction research method was followed to derive, analyse and present a summary of the research findings obtained from both the literature review and the interviews. Sections IV to V discuss the outcome of this research.

IV. CLOUD COMPUTING BENEFITS

Major growth in cloud computing adoption is expected. Predictions for growth in the cloud services market range between $46.3 billion reported in 2008 to $148.8 billion and $150 billion by 2014 and $222.5 billion market by 2015 [1-3]. Cloud computing spending is predicted to grow from $16 billion in 2008 to around $55 billion in 2014 [23-24]. These predictions for growth are based on the realization of the many benefits of cloud computing.

Cloud computing provides compelling savings in IT related costs including lower implementation and maintenance costs; less hardware to purchase and support; the elimination of the cost of power, cooling, floor space and storage as resources are moved to a service provider; a reduction in operational costs; and paying only for what is used (measured service). Cloud computing also enables organisations to become more competitive due to flexible and agile computing platforms, providing for scalability and high-performance resources and highly reliable and available applications and data. Through cloud computing, IT departments save on application development, deployments, security, and maintenance time and costs, while benefiting from economies of scale. ‘Going green’ and saving costs are a key focus point for organisations. Cloud computing helps organisations to reduce power, cooling, storage and space usage and thereby facilitates more sustainable, environmentally responsible data centres. Moving to the cloud further frees up existing infrastructure and resources that can be allocated to more strategic tasks.

Cloud computing benefits are listed in Fig. 1, arranged from the highest occurrence (therefore cited most in literature) to the lowest.

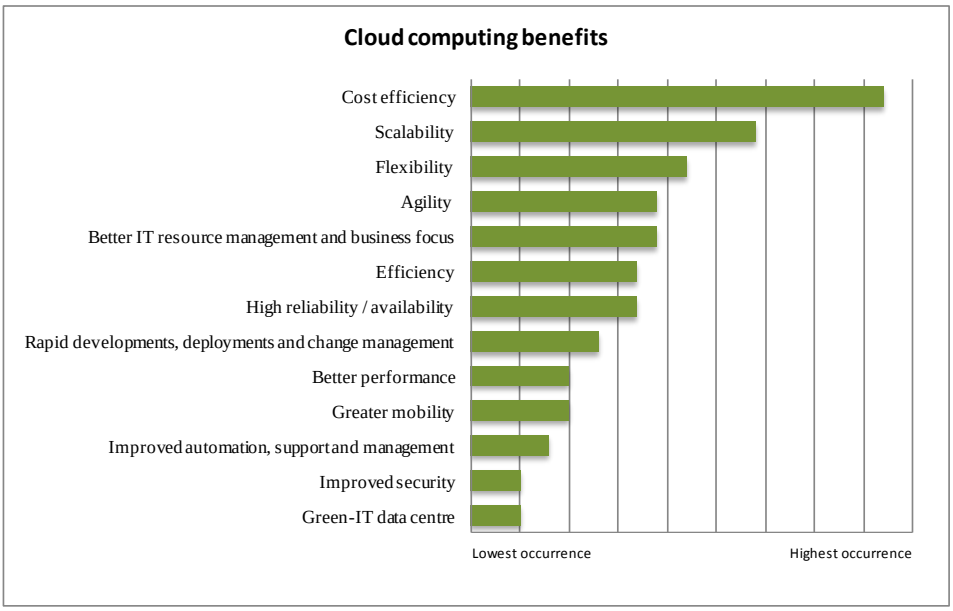

Figure 1. Cloud computing benefits.

Cost efficiency is the main driver for cloud computing adoption. Other primary benefits include scalability, flexibility, agility, better IT resource management and business focus, efficiency, higher reliability and availability, rapid development, deployment and change management, better performance and greater mobility. Improved automation, support and management, improved security, and green-IT data centres were also cited as valuable drivers for moving to the cloud.

V. CLOUD COMPUTING RISKS

Even though there are many drivers for moving to a cloud based solution, cloud computing is not without risks or completely secure. A thorough understanding and the mitigation of security risks represent an important step towards securing cloud environments and harnessing the benefits of cloud computing.

Fig. 2 presents the list of identified risks. As described in section III, the first step in our research was to review the published literature and to conduct an analysis to identify the risks. This was followed by 15 interviews to verify and/or enhance the data obtained from the literature review (Table I).

According to the literature review, the biggest cloud computing concern is security (Fig.2). With applications and data being hosted by a service provider, data is no longer under the control of management and prone to vulnerabilities. Hosting application and data in shared infrastructures increase the potential of unauthorised access and raise concerns such as privacy, identity management, authentication, compliance, confidentiality, integrity, availability of data, encryption, network security and physical security. Apart from the security risks, other concerns include SLA and third-party (service provider) management, vendor lock-in, quality of service, vendor viability, data and application management and control, workload management, performance, change control, availability of service, the lack of monitoring and management tools, transparency, compliance with laws and regulations, portability and interpretability, disaster recovery, virtualization risks, the lack of standards and auditing, the unproven nature of cloud computing and uncontrolled viable costs.

Similar results were obtained from the interviews, as shown in Table I. Information security was rated by 91.7 percent of the respondents to be the most critical risk area for the implementation of cloud computing and virtualization standards, policies and controls. Disaster recovery / business continuity planning was rated the second most critical risk area, with a score of 66.7 percent. Standards, policies and controls for operations management, change management, third party / service level management, interface management, and regulations and legislation were rated as being 'somewhat important' for the mitigation of risks.

The findings from both the literature review and the interviews corroborate the importance of ensuring that the cloud environment is adequately protected and secure. Establishing controls to overcome the security issues are hence an important step towards securing the cloud environment. We therefore focus primarily on security risks when we discuss risk mitigation strategies in the remainder of the paper.

TABLE I. CLOUD COMPUTING AND VIRTUALIZATION CRITICAL RISK AREAS

Risk Area	Critical	Somewhat important	Not so important
Information security	**91.7%**	8.3%	0.0%
Operations management	41.7%	**58.3%**	0.0%
Change management	41.7%	**50.0%**	8.3%
Disaster recovery/ business continuity planning	**66.7%**	33.3%	0.0%
Third-party/ service level management	41.7%	41.7%	16.7%
Interface management	8.3%	**50.0%**	41.7%
Regulations and legislation	33.3%	**41.7%**	25.0%

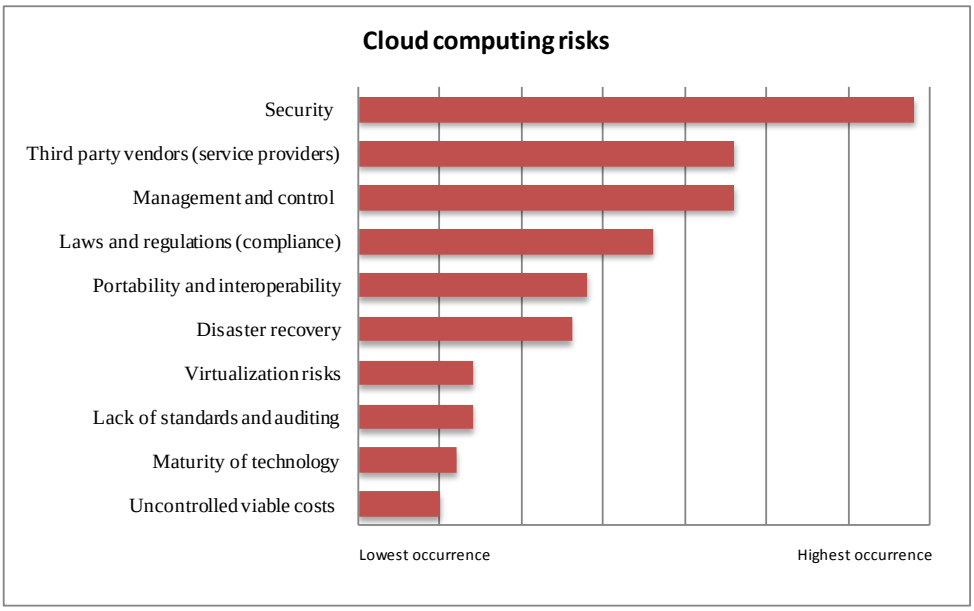

Figure 2. Cloud computing risks.

VI. MITIGATION OF SECURITY RISKS

An adequate risk mitigation strategy needs to be developed and followed to ensure mitigation of security risks and subsequent protection of data and applications in the cloud. Proper safeguarding and protection of valuable business data and systems remains the responsibility of management, regardless of whether or not the data and systems are hosted in the cloud.

Through the extensive literature review, the following control objectives were identified as important for the mitigation of cloud computing security risks: data security, administration and control; logical access; network security; physical access; compliance; and virtualization. Each of these objectives is discussed in more detail in the following sections. The discussion of each control objective is accompanied by a table (Tables II to VI) containing a summary of the risks and recommendations for possible mitigation of the risk as determined from the literature review. These recommendations form the first steps in setting up a complete framework for mitigating security risks in cloud computing environments.

Most of the security risks and subsequent controls, described in the remainder of this paper, constitute resources being hosted by a service provider at an off-site location, regardless whether it is a public cloud, private cloud, community cloud or a combination of two or more clouds

A. *Data security, administration and control*

Data security risks constitute the biggest barrier for cloud computing. Some businesses are still reluctant to move data and applications to the cloud, especially if critical to the business, due to the risk of data leakage leading to confidentially and privacy risks (A1), the lack of control over hosted data and applications (A2), availability concerns of cloud services and data (A3), the risk of data integrity impairment (A4), and ineffective protection of data in transit, in rest or in back-up due to inadequate encryption (A5). These *data security, administration and control* risks and the recommendations for mitigation of these risks are detailed in Table II.

B. *Logical access*

The risks of unauthorised access to data and applications in the cloud and the recommendations for mitigation of these risks are detailed in Table III. Access via a public network and hosted services means increased exposure and subsequently more risks. Privileged access rights (B1) should be assigned carefully to authorised users only, and reviewed for adequacy on a frequent basis. The implementation of security tools and techniques are required to ensure authorised user access to data and applications (B2).

C. *Network security*

Network security risks include the increased risk of hacking and intrusion (C1), enterprise perimeter evaporation (C2) and mobile device attacks (C3). These network security risks and the recommendations for mitigation of these risks are detailed in Table IV.

D. *Physical security*

With the disappearance of physical data centre perimeters, attackers could gain access to data and applications from anywhere in the network (D1). The physical security risk and the recommendation for mitigation of this risk are detailed in Table V.

E. *Compliance*

Companies are ultimately responsible for ensuring the security and integrity of their data, even when it is held by service providers in the cloud. Organisations further need to prove compliance with security standards regardless of the locations of their data and applications. Compliance risks

and the recommendations for mitigation of these risks are detailed in Table VI.

F. Virtualization

In previous research we have addressed virtualization security risks and a number of controls that could be considered for the mitigation of virtualization security risks. The controls included those related to security administration and control, logical access, network security, physical security, change control, and management and monitoring. For a detailed discussion of these risks and controls, refer to [25].

TABLE II. DATA SECURITY, ADMINISTRATION AND CONTROL RISKS AND MITIGATING CONTROLS

Ref	Risk	Description of mitigating control
A1	***Data privacy***	
A1.1	The sharing of cloud infrastructures could lead to data privacy and confidentiality issues, including disclosure and remote storage leading to adverse consequences for legal status and/or protection of personal or business information; the location of data could influence the privacy obligations for processing and storage; legal consequences could arise due to data being at multiple locations at the same time; data is stored externally, therefore increasing the vulnerability of being accessed or copied; insider user threats could be made (i.e. by malicious cloud provider user, malicious cloud customer user, or malicious third party user); and data leakage could occur due to failure of security access rights across multiple domains, and failure of electronic and physical transport systems for cloud data and back-up [6, 20].	Information that is allowed in the cloud should be identified and classified appropriately. Cloud service providers should prove to customers the effectiveness of data privacy controls. The cloud service provider's security and information personnel should have adequate knowledge and skills to prevent, detect and react to security breaches in a timely manner. Third party audits should be performed on a regular basis to monitor the cloud service provider's compliance to agreed terms, to ensure adherence to standards, procedures and policies, and to ensure that no major changes occurred to any of these standards, procedures or policies [26-27].
A2	***Data control***	
A2.1	Cloud solutions make it difficult to protect data and to enforce privacy-, identity theft- and cyber-crime security, as the organisation has no direct control over data being hosted by a cloud service provider [16, 22, 28-29]. Sharing computing resources with other companies cloud expose data to be seized if one of the other sharing companies has violated the law [20].	Third party audits should be performed on a regular basis to monitor the cloud service provider's compliance to agreed terms, and the effective implementation of and adherence to security policies, procedures and standards. The cloud service provider should provide customer transparency around controls, security and operations [16, 22, 28-30].
A3	***Availability of data and services***	
A3.1	Disaster recovery procedures and tested plans are vital in the event of a disaster to ensure availability of services and data. Other risks include that the confidentiality of data could inhibit testing of data back-up restore procedures; and in the event of an incident, other cloud customers may receive higher priority in recovery activities [6, 20, 26, 28-29, 31].	Data must be available and data back-up and recovery schemes for the cloud must be in place and effective to prevent data loss, unwanted data overwrite, or destruction. Cloud service providers should have adequate back-up and data replication policies and should keep auditable proof of the adequacy of restore procedures including accurate, complete and timely recovery of data [13, 26, 31].
A3.2	Because cloud computing is based on hosted services, the viability of data in the event of the service provider going out of business presents a major risk of data lock-in [20, 22, 31].	The cloud service provider should support adequate interoperability standards to ensure migration of data and/or the integration of new capabilities. Review bulk data extractions and code copy options before entering into an agreement with the cloud service provider. If leveraging cloud service-oriented offerings, consider supporting more than one provider's offering simultaneously and duplicate data across them to achieve adequate redundancy [26, 32].
A3.3	Reliance on the Internet as the primary medium of data transfer and processing leads to availability issues due to possible connectivity and bandwidth speed limitations [6, 19].	Internet connectivity and bandwidth speed limitations should be investigated before considering moving applications and data into the cloud, as well as guiding the selection of a suitable service provider. Network services and management should provide for adequate provisioning of bandwidth speed and network capabilities. Network monitoring is of the essence to ensure provisioning based on load balancing [33].
A4	***Data integrity***	
A4.1	The integrity of networks, applications, databases and system software in a shared, globally accessed cloud environment is threatened by many vulnerabilities when not adequately and timely patched [20, 31, 34].	Responsibilities for efficient patch management should be clearly defined. Patch management policies and procedures should be implemented. Consider virtual patching and automated patch management services [20, 31, 34].
A4.2	Another risk in cloud computing environments is unauthorised changes to data and systems by the service provider which could affect the integrity and availability of data and applications [6, 20, 31, 34].	All changes in the cloud environment should be managed to minimise the likelihood of disruption, unauthorised changes, or errors (i.e. buy-in from stakeholders, compliance with policies and standards, validation and testing of changes in separate development and testing environments, formal approval and acceptance of changes, and adequate security around migration to production). The cloud service provider should adhere to a similar and/or adequate system development life cycle (SDLC). Standards and policies should be implemented to guide developers during development and restricting users to authorised data only when deploying changes to production. Service providers should keep auditable proof that no unauthorised changes occurred during a specified period [6, 20, 31, 34].
A4.3	The integrity of data in complex cloud hosting environments could provide a threat against data integrity if system resources are not effectively segregated amongst customers [6].	Data segregation should be enforced through correctly defined security perimeters and adequate and secure configuration of virtual machines and hypervisors [6].

A5	*Data encryption*	
A5.1	A major risk in cloud computing environments is inadequate encryption and key management of data. Cloud environments are shared with many tenants, and service providers have privileged access to the data thus posing a risk of data leakage or unauthorised access to data hosted in a cloud. Sensitive and regulated data is in transit over a cloud network increasing the risk of acceptance, hijacking or leakage. Data on disks or in the live production environment is also open to malicious cloud service providers or a malicious co-tenant [6, 13, 16, 20, 30, 34].	Clear responsibilities for control and access over encryption standards and key management for data at rest, in transit and on back-up media should be agreed upon and regular proof of adherence provided. Encryption and key management should be based on industry and government standards. Effective key management includes the protection of the key stores in storage, in transit and in back-up; access to key stores being limited to the entities that specifically need the individual keys, as well as the enforcement of segregation of duties; and secure back-up and recovery solutions for keys to prevent the loss of keys and subsequent loss of data [6, 13, 16, 20, 30, 34].
A5.2	Insecure absolute cryptography due to novel methods of breaking the cryptography or crucial flaws in the implementation of cryptographic algorithms could turn strong encryption into very weak encryption [35].	Controls and management of cryptographic material and methods, whether in transit or at rest, should be implemented [30].

TABLE III. LOGICAL ACCESS

Ref	**Risk**	**Description of mitigating control**
B1	Administrator access is through the Internet rather than a controlled and restricted on-site connection. The risk of unauthorised or inadequate privileged access, such as administrator access, increases as data are processed outside the organisation, meaning that outsourced service providers can by-pass control exerted over in-house programs. Access via the Internet also means more exposure and subsequently more risks. The cloud characteristic of 'on-demand self-service' requires a management interface that is accessible to users of the cloud service. Unauthorised access to this management interface is much higher in online cloud environments than for traditional systems where this management facility is only accessible to a few administrators [6, 16, 20, 28, 31, 34].	Service providers must demonstrate existence of effective and robust security controls, assuring customers that data and applications are adequately secured against unauthorised access, change and destruction. Regular reviewing and monitoring of privileged access should be performed, including who manages and administers data and the adequacy of such rights, proper segregation of duties, the handling and disclosure of changes in system controls and access restrictions, and controls and formal procedures to prevent, detect and react to security breaches. Also enquire about the adequacy of the service provider's hiring and management process for administrators and those responsible for management and monitoring of cloud services. Cloud service providers should ensure that all access or changes to cloud services, resources and data produce auditable records regardless of success or failure. Audit trails should include clear indications of any delegations of identity or authorizations. Formal approval should be obtained and kept for new or changed rights to privileged accounts. Administrator access should be encrypted and extra strength applied through security tools such as one-time password protections or multi-factor authentication (i.e. Secure Access Gateway) [6, 20, 27, 30-31, 34].
B2	Weak authentication mechanisms could increase the risk of unauthorised access to data and applications which are globally accessible through the cloud and being shared with other customers due to the multi-tenancy nature of cloud computing. Weak authentication mechanisms may include insecure user behaviour (i.e. weak passwords or re-using of passwords), the inherent limitation of one-factor authentication mechanisms and inadequate segregation of duties. Migrating workloads to shared infrastructures leads to potential unauthorised access and exposure, including challenges such as credential management, strong authentication (i.e. multi-factor authentication), delegated authentication and managing trust across all types of cloud services [6, 13, 29, 32, 35].	Trusted user profiles should be established based on role definition and information classification. Ensure implementation and adherence to security policies and best practices. A browser client cannot be fully secure. Therefore, ensure strong integration between the server-side data security framework and the client security framework. Adequate authentication, identity management, compliance and access security tools and techniques should be implemented and regularly monitored for compliance. Ensure that a high degree of transparency to the service provider's operations are negotiated, documented in the SLA and formally agreed upon [6, 13, 29, 32, 35].

TABLE IV. NETWORK SECURITY

Ref	**Risk**	**Description of mitigating control**
C1	There is an increased risk of hacking and intrusions in cloud environments. Hacking and intrusion risks include attackers gaining access to data and applications via some kind of remote access system and web application, and injection vulnerabilities exploited by manipulating input to a service or application so that parts of the input are interpreted as executed code against the programmer's intention (i.e. SQL and command injections, and cross-site scripting). Security threats such as man-in-the-middle attacks, authentication attacks, side channel attacks, social networking attacks, and denial of service (DoS) attacks pose major threats in cloud computing environments. [6, 16, 31, 35].	Network level controls should be implemented to secure systems and data and prevent unauthorised use, disclosure, damage, or loss of data. The service providers should prove adequate set-up and the effectiveness of the firewall, and provide auditable proof of the adequacy of access rights and the execution of authorised changes only. Regularly perform or mandate a security audit, including the assessment of web components of current cloud offerings to show the prevalence of injection vulnerabilities. Policies ensuring secure traffic at the switch, router and packet level should be implemented [6, 16, 31, 35].
C2	The enterprise perimeter evaporates in cloud computing environments, therefore the lowest common denominator impacts the security of all. The enterprise firewall establishes the foundation for security policy and zoning for networks, which in a cloud solution is either no longer reachable, or its policies are no longer under control of the resource owner, but the responsibility of the cloud service provider [34].	Established zones of trust should be implemented through virtual machines that are self-defending, effectively moving the perimeter to the virtual machine itself [34].

C3	Mobile device attacks are a new emerging risk. Cloud enabled users can access business data and services without transferring through the corporate network, leading to security vulnerabilities [6, 20].	Adequate security controls should be enforced between mobile users and cloud based services [6, 20].

TABLE V. PHYSICAL ACCESS

Ref	Risk	Description of mitigating control
D1	Placing large amounts of data in globally accessible clouds leaves the organisation open to large distributed threats as attackers can gain access at one virtual location rather than a secured on-site location [20, 28].	Network level security (see Table IV) and data encryption controls (see Table II, A5).

TABLE VI. COMPLIANCE

Ref	Risk	Description of mitigating control
E1	Companies must comply with requirements, set by their own organisation or by an industry or government body, for securing both internal and external data and applications. Cloud computing, in most instances, means that data and applications are hosted at an off-site location, outside the legal and regulatory umbrella of the organisation. Compliance needs to be proved regardless of the location of data. Compliance with some laws and regulations include: - Payment Card Industry Data Security Standard (PCI DSS); - Geographical restrictions applicable to the transit and storing of data; - Sarbanes Oxley Act (SOX); - Gramm-Leach-Bliley Act (GLBA); - Health Insurance Portability and Accountability Act (HIPAA); - Auditing standards such as SAS70 and ISO [6, 16, 19-20, 22, 26, 31].	Ensure that the cloud service provider is willing to undergo external audits and security certifications, and that logs ensuring compliance are readily available. Cloud service providers should prove that data, including all copies and back-ups, are stored only in geographic locations permitted by a formal contract, SLA or regulation. Adherence to the following controls should be ensured: meeting requirements specific to the data location; complying with location specific laws and regulations; and the laws and regulations being formally incorporated and documented in governance policies [6, 16, 19-20, 22, 26, 31].

VII. CONCLUSION

Cloud computing predictions for growth indicate substantial developments for and implementations of cloud computing services. To make cloud environments more secure and robust, proper controls, mitigating security risks should be enforced. In this paper, we provided an overview of cloud computing benefits and security risks as a general guideline to assist management in the implementation of cloud computing processes, procedures and controls. Consideration should be given to risks to ensure completeness, integrity and availability of applications and data in the cloud. We also suggested a number of controls that could be considered for the mitigation of cloud computing security risks. The controls included data security, administration and control, logical access, network security, physical security, compliance and virtualization. Further research will focus on the development of a complete risk and control framework for cloud computing and virtualization to provide management with guidelines and control standards to deal coherently with cloud computing and virtualization risks.

REFERENCES

[1] Deloitte. (2010, 31 August 2010). *Executive Forum - Cloud Computing: risks, mitigation strategies, and the role of Internal Audit*. Available: http://www.deloitte.com

[2] C. Pettey and B. Tudor. (2010, 5 August 2010). *Gartner says worldwide cloud services market to surpass $68 billion in 2010* Available: http://www.gartner.com/it/page.jsp?id=1389313

[3] Press Office. (2010, 31 August 2010). *Cloud Computing Services - New Market Report Published*. Available: http://www.companiesandmarkets.com/r.ashx?id=41AETZYHJ289173&prk=ecb8413c602cb89051067456b636c7b9

[4] I. Berger. (2010, 6 May 2010). *Keeping Cloud Computing's Prospects Safe and Sunny*. Available: http://www.theinstitute.ieee.org/portal/site/tionline/menuitem.130a3558587d56e8fb2275875bac26c8/index.jsp?&pName=institute_level1_article&TheCat=2201&article=tionline/legacy/inst2010/may10/featuretechnology.xml&

[5] K. McCabe and R. Nachbar. (2010, 18 October 2010). *SURVEY BY IEEE AND CLOUD SECURITY ALLIANCE DETAILS IMPORTANCE AND URGENCY OF CLOUD COMPUTING SECURITY STANDARDS* Available: http://standards.ieee.org/announcements/2010/pr_cloudcomputing_survey.html

[6] Centre for the Protection of National Infrastructure (CPNI). (2010, 20 June 2010). *Information Security Briefing 01/2010: Cloud Computing*. Available: http://www.cpni.gov.uk/Docs/cloud-computing-briefing.pdf

[7] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Information Technology Laboratory2009.

[8] S. Baca. (2010, 14 May 2010). *Cloud Computing: What it is and what it can do for you*. Available: www.globalknowledge.com

[9] S. Bennett, *et al*. (2009, 8 April 2010). *Architectural Strategies for Cloud Computing*. Available: http://www.oracle.com/technology/architect/entarch/pdf/architectural_strategies_for_cloud_computing.pdf

[10] Cloud Computing Use Case Discussion Group. (2010, 31 March 2010). *Cloud Computing Use Cases Version 3.0*. Available: http://groups.google.com/group/cloud-computing-use-cases

[11] Sun Microsystems Inc. (2009, 8 April 2010). *Introduction to cloud computing architecture* [White Paper]. Available: http://www.sun.com/featured-articles/CloudComputing.pdf

[12] VMware Inc. (2009, 18 August 2010). *Eight Key Ingredients for Building an Internal Cloud*. Available: http://www.vmware.com/files/pdf/cloud/eight-key-ingredients-building-internal-cloud.pdf

[13] Cloud Security Alliance. (2009, 20 May 2010). *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*. Available: www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[14] D. Brink. (2010, 12 September 2010). *Much Ado about Cloud Computing*. Available: http://research.aberdeen.com/index.php/information-technology/89-information-technology-insights/1313-much-ado-about-cloud-computing

[15] D. Durkee, "Why cloud computing will never be free," *Communications of the ACM*, vol. 53, pp. 62-69, 2010.

[16] M. Gregg. (2010, 14 May 2010). *10 Security Concerns for Cloud Computing*. Available: www.globalknowledge.com

[17] J. Hagel and J. S. Brown. (2010, 15 April 2010). *Cloud Computing: Storms on the Horizon*. Available: http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/TMT_us_tmt/us_tmt/ce/CloudsStormsonHorizon_102210.pdf

[18] J. Hurwitz, *et al.*, *Cloud Computing for Dummies, HP Special Edition*. Indianapolis, Indiana: Wiley Publishing, Inc, 2010.

[19] N. Kelson. (2010, 2 September 2010). *Cloud Computing Management Audit/Assurance Program*. Available: www.isaca.org

[20] J. W. Rittinghouse and J. F. Ransome, *Cloud Computing: Implementation, Management, and Security*. Florida: CRC Press, 2010.

[21] A. T. Velte, *et al.* (2010, 8 April 2010). *Cloud Computing: A Practical Approach*. Available: http://skillport.books24x7.com/

[22] C. Weitz, *et al.* (2010, 31 August 2010). *A balancing act: What cloud computing means for business, and how to capitalize on it*. Available: www.deloitte.com

[23] F. Gens. (2010, 28 August 2010). *IDC's Public IT Cloud Service Forecast: New Numbers, Same Disruptive Story*. Available: http://blogs.idc.com/ie/?p=922

[24] N. Leavitt, "Is Cloud Computing Really Ready for Prime Time?," *Computing Now*, pp. 15-20, 2009.

[25] M. Carroll, *et al.*, "Secure Virtualization: Benefits, Risks and Controls," presented at the CLOSER 2011: The 1st International Conference on Cloud Computing and Services Science, Noordwijkerhout, The Netherlands, 2011.

[26] B. Robertson. (2009, 1 December 2009). *Top Five Cloud Computing Adoption Inhibitors*. Available: http://www.gartner.com/it/initiatives/pdf/KeyInitiativeOverview_CloudComputing.pdf

[27] M. Vael. (2010, 24 July 2010). *Cloud Computing: An insight in the Governance & Security aspects*. Available: http://www.isaca.org/Groups/Professional-English/information-secuirty-management/GroupDocuments/Across%20Cloud%20Computing%20governance%20and%20risks%20May%202010.pdf

[28] L. Ponemon. (2010, 29 September 2010). *Security of Cloud Computing Users: A Study of Practitioners in the US & Europe*. Available: http://www.ca.com/~/media/Files/IndustryResearch/security-cloud-computing-users_235659.pdf

[29] V. Raval, "Risk Landscape of Cloud Computing," *ISACA Journal*, vol. 1, 2010.

[30] Distributed Management Task Force. (2010, 17 March 2011). *Architecture for Managing Clouds*. Available: http://www.dmtf.org/about/policies/disclosures.php.

[31] Clavister. (2010, 13 November 2010). *Security in the Cloud*. Available: www.clavister.com/resources/

[32] Open Cloud Manifesto. (2009, 2 September 2010). *Open Cloud Manifesto: Dedicated to the belief that the cloud should be open*. Available: www.opencloudmanifesto.org

[33] T. W. Singleton, "IT Audits of Cloud and SaaS," *ISACA Journal*, vol. 3, 2010.

[34] Third Brigade. (2008, 21 July 2009). *Cloud Computing Security: Making Virtual Machines Cloud-Ready* [White Paper]. Available: http://resources.thirdbrigade.com/

[35] B. Grobauer, *et al.* (2010, 31 August 2010). *Towards a cloud-specific Risk Analysis Framework*. Available: www.siemens.com/it-solutions