Table of Contents

International Journal of Secure Software Engineering

Volume 7 • Issue 3 • July-September-2016 • ISSN: 1947-3036 • eISSN: 1947-3044

An official publication of the Information Resources Management Association

Editorial Preface

Research Articles

COPYRIGHT

The *International Journal of Secure Software Engineering* is indexed or listed in the following: ACM Digital Library; Bacon's Media Directory; Cabell's Directories; DBLP; Google Scholar; INSPEC; JournalTOCs; MediaFinder; The Standard Periodical Directory; Ulrich's Periodicals Directory

International Journal of Secure Software Engineering
Volume 7 • Issue 3 • July-September 2016

Migration Goals and Risk Management in Cloud Computing:

A Review of State of the Art and Survey Results on Practitioners

Shareeful Islam, School of Architecture, Computing and Engineering, University of East London, London, UK
Stefan Fenz, SBA Research gGmbH, Vienna, Austria
Edgar Weippl, SBA Research gGmbH, Vienna, Austria
Christos Kalloniatis, Cultural Informatics Laboratory, University of the Aegean, Mitilini, Greece

ABSTRACT

Organizations are now seriously considering adopting cloud into the existing business context, but migrating data, application and services into cloud doesn't come without substantial risks. These risks are the significant barriers for the wider cloud adoption. There are works that consolidate the existing work on cloud migration and technology. However, there is no secondary study that consolidates the state of the art research and existing practice on risk management in cloud computing. It makes difficult to understand the risks management trend, maturity, and research gaps. This paper investigates the state of the art research and practices relating to risk management in cloud computing and discusses survey results on migration goals and risks. The survey participants are practitioners from both public and private organizations of two different locations, i.e., UK and Malaysia. The authors identify and classify the relevant literature and systematically compare the existing works and survey results. The results show that most of the existing works do not consider the existing organization and business context for the risk assessment. The authors' study results also reveal that risk management in cloud computing research and practice is still not in a mature stage but gradually advancing. Finally, they propose a risk assessment approach and determine the relative importance of the migration goals from two real migration use cases.

KEYWORDS

Analytic Hierarchy Process, Migration Goals, Risk Assessment, Risk Management in Cloud, Risks Survey

1. INTRODUCTION

Cloud computing provides several benefits to the organization particularly in the recent economic downtime. The adoption of cloud computing has speed up in the last few years and small to large companies rush to migrate into cloud by using virtual machine through internet for their data and applications. But, there are substantial challenges due to the unique cloud computing characteristics and users' dependencies on the Cloud Service Provider (CSP) to support the business (Mouratidis et al., 2013; Kalloniatis et al., 2014; Gruschka and Iacono, 2009; Ristenpart et al., 2009; Pearson, 2009). These downsides are not well understood and pose risks that could obstruct the benefits of wider cloud adoption. Therefore, it is necessary to understand the risks associated for cloud adoption based on an organizational context and control these risks accordingly.

DOI: 10.4018/IJSSE.2016070103

Recently, cloud migration and security issues associated in cloud have gained a lot of attention by both the research and industry communities. There are studies that consolidate the research in the area of cloud migration, security, and cloud technologies (Jamshidi et al., 2013; Ardagna, 2015; Rong et al., 2013; Sriram and Khajeh-Hosseini, 2010) and survey results for identifying mainly benefits and risks in cloud (ENISA Survey, 2009; Microsoft Survey, 2012; Hitachi, 2014). But, there is no study that consolidates risks and risks management approaches in cloud computing. It makes difficult to assess the maturity of the domain, effectiveness of risk management practice and future directions. The novelty of the presented work is threefold. Firstly, it contributes to review the state of the art works towards the risk management in cloud. We follow systematic literature review along with social commentary to review both academic papers and industry practices relating to the cloud computing risks. The papers are selected by looking at the coverage, timeliness and quality of the context. Secondly, it performs a survey with the experience practitioners from UK and Malaysia to identify the goals and risks in cloud migration. We follow Delphi survey method and select practitioners from both public and private sector organization for the survey purpose. We identify the research trends, gaps and future directions based on the analysis of state of the art review and survey results. Finally, we propose a risk assessment method to quantify the risk based on their influenced on the prioritized migration goals. We consider six main migration goals for this purpose, i.e., business value, organization function, confidentiality, integrity, availability, and transparency based on the review results and determine the relative importance of these goals using Analytic Hierarch Process (AHP). The prioritized goals are then used to assess the risks using a semi-quantitative approach to determine the net risk level. The reason for considering the migration goals for risk assessment is that risk is defined as a negation of a migration goal. Organizations that intend to migrate their data or application into the cloud have certain goals or objectives that they want to achieve with the migration decision, and risks certainly obstruct these goals. We consider two real migration use cases to determine the relative importance of the goals and compare the results.

The paper is structured as follows: section 2 provides an overview of the research methodology for the state of the art review. The subsequent section provides details of our finding from the state of the art review. Section 4 presents the method and context for the survey, while section 5 details about the survey results. Section 6 discusses the overall finding of the state of the art review and survey. Section 7 presents a risk assessment method in cloud computing and section 8 outlines the relative importance of migration goals. Finally, section 9 concludes the paper.

2. RESEARCH METHODOLOGY FOR THE STATE OF THE ART REVIEW

The state of the art review combines a Systematic Literature Review(SLR) with social commentary to understand the recent trend of risk management in cloud computing. SLR has become a popular research methodology for conducting literature review and consolidates the analysis from the review. The combination of these two techniques allows us to systematically identify available evidence on risk management in cloud computing from both the academic and industry works. There are three main review steps, i.e., planning, conducting and documenting (Kitchenham and Charters, 2007; Brereton et al., 2007) as shown in Figure 1. The SLR provides a sequence of methodological steps to research relevant literature.

2.1. Step 1: Planning

The initial step plans the research by identifying the necessity of review of literature, research questions, and relevant methods for the review. As stated previously, risk management in cloud computing are

critical and one of the main barriers of wider cloud adoption. There are works from both research and industry communities relating to risks and risk management practice for cloud computing. However, there is no study that identifies, analyzes and compares these works. Such study is necessary to identify the trend of research, research gap and future directions so that risk management can effectively support organizations with their cloud adoption. The review aims to answer the three research questions given in Table 1. We combine systematic literature review with social commentary as relevant methods for performing this study. Systemic literature review identifies the literature from the research database. Social commentary is the state of the practice follows blogs, industry presentation, CSP websites and white papers. Cloud computing already obtained a huge attention from the industry community; therefore, we believe relevant literature will be available for the purpose of this study.

2.2. Step 2: Conducting

This second step mainly concerns with the final selection of the studies for the review by the step 3. Our aim is to identify literature that deals with the risks, risks management framework in cloud computing. It is important to select the relevant sources for performing a SLR. Therefore, we consider the preliminary keywords, i.e., risk management framework in cloud, risks (security, privacy, business, legal, and organization), and cloud areas for this study. We use search engines from the following five sites: Google Scholar, Elsevier, IEEE Xplore, ACM Digital Library and Science Direct to extract the literature. Our effort relating to social commentary is to identify the practitioners' view relating to the cloud risks and existing industry practice to mitigate these risks. We follow white papers and technical report from well-known CSP and tech websites for this purpose.

The papers and industry related articles were mostly selected that were published from 2008 because the research domain is recent and rapidly changing. Initial, we have identified 52 papers from the sites and 36 items from the industry related sources. After reviewing title and abstract, we observed that most of the works consider security and privacy risks and very few on the business risks in cloud. The final selection is carefully considered based on our inclusion and exclusion criteria as shown in Table 2. The inclusion criteria emphasize on coverage of the area, timeliness of solution, and overall quality. In particular, literatures are selected if they cover the identified areas from the well-known sites. Finally, we have selected a total of 32 academic publications and 10 items of practitioners' views for this review.

2.3. Step 3: Documenting

This is the final step of our review. The selected papers were split into five main categories based on main focus of this review, i.e., risk management framework, risks and controls in cloud based system, security risks, privacy risks, and case study. Table 3 shows the main areas that take into consideration of individual category. Table 4 summarizes the papers based on the category. The review of the selected articles, research trend and future directions are presented in the following sections.

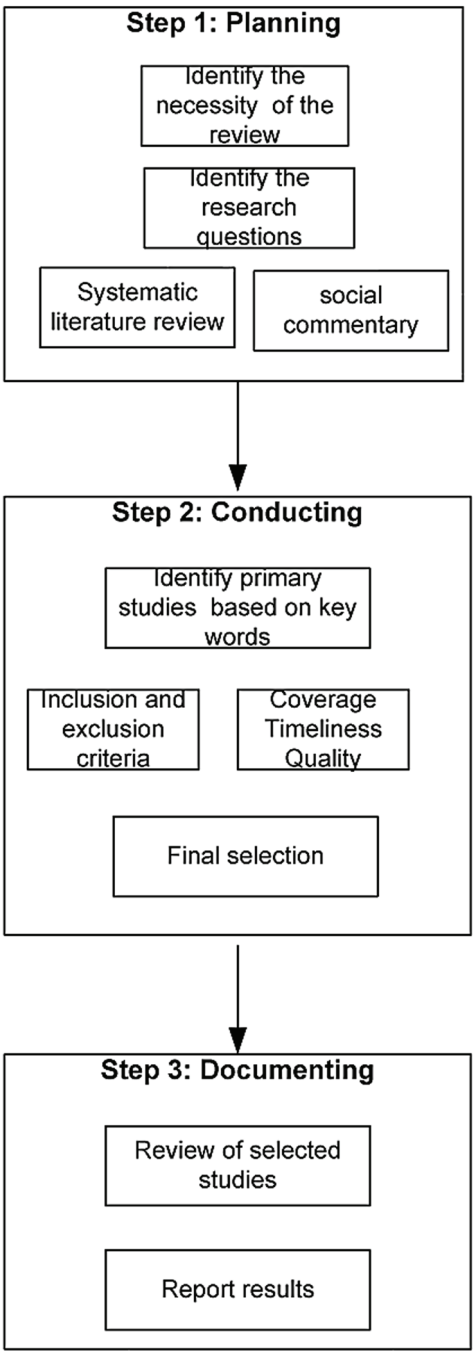
3. ANALYSIS OF THE STUDIES

This section reviews the selected papers and articles from the previous sections for the state of the are review.

3.1. Risk Management Framework

Managing risks is a challenging task for the wider cloud adaption. This section includes work that considers critical cloud areas, risks management process and techniques from both academic and industry communities. Prasad and Ben (2010) propose a QUIRC security risk management framework based on six key cloud specific security criteria, i.e., confidentiality, integrity, availability, multiparty trust, mutual auditability and usability to identify and assess the security risks. Risks assessment considers fully quantitative assessment method by involvement Subject Matter Experts for providing

Figure 1. An overview of research methodology for review



precise information about risks. Such approach helps to assess the CSPs' offerings based on the security needs for the migration. The approach has several limitations. The net risk value does not link with any scale which makes it difficult to understand high, medium and low risk. Moreover, it is not clear how the weight value is defined for the six tuples. Zhang et al (2010) propose a security risk

Table 1. Research questions for review

Research questions	Justification
RQ1: What are the existing framework, process, and techniques to identify, assess, manage, and monitor risks in cloud computing?	This purpose is to obtain in-depth understanding of the existing risk management process of cloud computing.
RQ2: What are the key risks in cloud computing that could oppose the benefits of cloud migration?	This purpose is to identify the key risks from all dimensions in cloud.
RQ3: What is the state of existing research and future directions for risk management in cloud?	This review aims to understand the advancement of research practice of the risk management in cloud domain, gaps and future directions.

Table 2. Inclusion and exclusion criteria

Inclusion Criteria(IC)/Exclusion Criteria(EC)	Justification
IC1(**Coverage, Quality**): Works that focus on the risks and controls in cloud .	We are interested in identifying what are the critical risks for cloud and possible solutions for controlling these risks. Study from real scenario/case study identifies the actual risks that happened in a context.
IC2(**Coverage, Timeliness of the solutions**): Studies that considers risks management framework, process, techniques and tools for risks management.	Such works provide concrete solution how to analysis and control the risks.
IC3(**Timeliness of the solutions**): Industry practice for controlling the risks.	We emphasize on such timely practice as it provides a realistic view how risks are controlled by the organization specifically cloud service provider.
EC1: Works in cloud computer domain that do not specifically focus on the risk management process, or tool support in cloud computing.	Risk management framework and process is a critical area for many domains. We are only interested with the works that explicitly consider risks management for the cloud based context.
EC2: Thesis and book chapters.	Our work mainly considers conference and journal papers from the literature review and industry practice through CSP website, blogs, and industry presentation.

management framework for the cloud computing environment by following the ISO/IEC 27001:2005 standard PDCA model. The process starts with identification of critical areas and strategy and planning followed by risk analysis and control. The risk assessment follows risk likelihood and impact to calculate the risk scales of high, medium and low. The framework is very generic and can be applicable for any context. It also does not provide any guidelines for determining the risk levels. Samad et al. (2013) consider a quantitative risk model for a dynamic mobile cloud environment. Mobile cloud computing should be the next step of advancement of cloud system. Risks relating to such system are due to connectivity, limited resources, security, and limited power supply at the system level. The work follows context aware risk management model so that risks relating to the evolving system environment are addressed properly. Here Bayesian probability is used for calculating the risk event likelihood as it depends on many environmental factors. Every risk includes weight value, therefore a risk with more weights certainly gives higher net value. However, the framework does not provide include a process or steps how to perform the risk management activities. Moreover, it is hard to define the weight to each risk by the stakeholder without solid subject based knowledge, but this weight is important to calculate the net risk value for this context aware risk management model. Fit´o et al (2010) consider business level objectives driven semi-quantitative cloud risk assessment. The risk level is estimated for each business level objective based on the probability of occurrence and impact.

Table 3. Category, main areas and papers from the selected areas

Category	Main areas	Papers
Risk management framework	Risk management process, areas, techniques for the risk assessment and control.	Prasad and Ben, 2010; Zhang et al, 2010; Samad et al., 2013; Fit´o et al., 2010, CSA, 2009; CSA_CCM, 2014; Office 365, 2014; CSA_AREA, 2009.
Risks and controls in cloud computing	Typical risks for cloud computing from technical and non-technical dimensions and suitable controls.	Lemos, 2009; Heiser and Nicolett, 2008; Yanosky et al., 2008; Ryan, 2013; AWS, 2014; ENISA, 2009; FedRAMP, 2014.
Security risks	Security threats and risks form the cloud computing and its surrounding environment.	Khan et al., 2012; Gruschka and Jensen, 2010; Nahar et al., 2012; Gruschka and Iacono, 2009; Jensen et al., 2009; Dahbur et al., 2011; Gregg, 2010; Kalloniatis et al., 2014; CSA, 2009; Heiser and Nicolett, 2008; AWS, 2014; Office 365_CSA, 2014; ENISA, 2009; CSA_ THREAT, 2010; Ardagna, 2015.
Privacy risks	Privacy threats and risks from the cloud computing and its surrounding environment.	Vimercati et al., 2012; Savola, 2010; Theoharidou et al., 2013; Pearson, 2009; Kalloniatis et al., 2014; AWS, 2014; Office 365, 2014.
Case study	Lesson learned from real case study scenario regarding risks and risks management.	Samad et al., 2013; Gadia, 2011; Khosravani et al., 2013; Baars and Spruit, 2012a; Baars and Spruit, 2012b; Khajeh-Hosseini et al., 2010; Islam et al., 2012; ENISA, 2009; NIST, 2009.

Table 4. UK survey participants' details

Participant organization	Business domain and Position
Sky B	Service based industry for news, broadband, Internet. Position: Technical lead(software)
Orange innovation UK Ltd	Research and development for mobile operator orange Position: Principal engineering project manager
University of East London	Higher education sector Position: Business relationship manager, IT service
Ministry of Justice, UK	UK government ministry for the justice Position: Admin (case worker)
Firmdale hotels plc	Service based large private organization Position: Head of IT
Royal marsden hospital	Public health care specializing in cancer Position: Admin assistant
National health care system	Health care based large public organization Position: Computer Aided Facility Management(CAFM) assistant
Stratus technology	IT solution and services based privacy company Position: IT engineering
Ubiquity press	An open access publisher for journal and books Position: Software developer
F5 networks	Provide enterprise, security and cloud solutions Position: Consultant
London school of hygienic and tropical medicine	Higher education sector for public and global health Position: Temporary system support officer

Five different risk levels are defined including critical, unacceptable, negligible, profitable and high profitable. Therefore, the risk could be profitable in terms of the business level objective. The over-provisioning risks are analysed in terms of hazard events minimization energy efficiency maximization and profit maximization from the provider perspective. Such approach helps to determine the profit maximization as business level objective. However, the work is every early stage with a very brief description about the risk level estimation which makes it difficult to understand.

Heiser and Nicolett (2008) in Gartner report recommend integrating cloud computing aspects within existing organizational IT risk assessment capability. The work emphasizes on areas like Privileged User Access, Compliance, Data Location, Data Segregation, Availability, and Recovery and assesses these areas through existing CSP's offerings. They recommended users to demand transparency relating to security and contingency management program and develop a strategy for the delivery mechanism. A report of the Cloud Security Alliance (CSA) recommends a list of critical areas in cloud computing mainly focus on governance and operations issues from both user and provider perspectives (CSA_AREA, 2009). The areas such as architecture framework, governance and enterprise risk management, legal issues, data security and data centre operation are linked from strategic and policies to operational domain of implementing adequate security techniques. Risks could be a cross cutting concerns of these areas. CSA also introduces a Cloud Control Matrix (CCM)) as a general security control framework to strength the existing security control environment of CSP by minimizing the operational and security risks for the overall business continuity (CSA_CCM, 2014). CCM also guides the user to assess the security risks of CSP and follows the industry specific guidelines for the overall assessment. Hence, it helps the customer to make the right decisions when migrating into cloud. The control matrix includes several control objectives relating to compliance and audit, data governance, security policy, access control, human resource security, security management, risk management and security architecture to strength the overall information security environment of CSP. Therefore, CCM encourages the cloud providers to response how they address the requirements relating these objectives using their existing practice. For instance, Microsoft discloses a detailed capability report of mentioning how Office 365 SaaS offerings map to the security, privacy, compliance, and risk management requirements of CSA (Office 365 CSA, 2014). The report includes response of 11 CSA control such as compliance, data governance, security policy, human resource security, information security management, operation and risk management. Office 365 users have also the responsibilities to control and maintain the environment once the service has been provisioned. The European Network and Information Security Agency identifies (ENISA, 2009) reports on the cloud computing benefits, risks, and recommendations The report emphasizes two main recommendations, i.e., assurance for cloud customer and legal recommendation; specifically customers need assurance from of certain security practice and resolving the legal issues during contract evaluation. In terms of benefits, security measures are cheaper on a larger scale such as in cloud and priority concern for the cloud customers.

3.2. Risks and Controls in Cloud Computing

Risks are the potential negative consequences that could outweigh the benefits for the cloud migration. Lemos (2009) identified five main dark sides of cloud computing including less legal protection, sharing hardware, policy, untrustworthy machine instances and individual assumptions. These may pose several difficulties such as audit a CSP infrastructure, or application execution in different environment. Heiser and Nicolett (2008) in Gartner report emphasize to assess legal risks besides security and privacy risks. The European Network and Information Security Agency identifies (ENISA, 2009) report point out legal risks besides security and privacy risks in cloud from an organization perspective. However, the legal issues can be resolved during the contract negotiation and evaluation. The report also recommended that CSP should provide certain level assurance to the user relating to appropriate security practice for protection the user data. Losses of governance, lock-in, isolation failure, compliance, data protection, insecure data deletion are the top risks identified by the report.

The Federal Risk and Authorization Management Program (FedRAMP) is a standardized framework for the security assessment, authorization, monitoring cloud based services and product (FedRAMP, 2014). The main focus is to ensure that adequate security controls are in place to safeguard the migrated assets into cloud system specifically government organizations critical data that are stored, transmitted and processed by the cloud service provider. The approach also concerns the about the minimization risk management cost and rapid and cost-effective government procurement. The framework includes a four process areas, i.e., document, assess, authorize and monitor. The potential CSP need to select, implement, and document FedRAMP security control so that an independent assessor confirm that the controls are effectively implemented for generating authorization document. Finally, a continuous monitoring needs to be taken place if the CSP is authorized by the FedRAMP. Ryan (2013) identified four technical approaches in the context of confidentiality at the SaaS level: fully homomorphic encryption, key translation in the browser, hardware-anchored security, and query processing over encrypted databases. These approaches differ depending on their applicability and assurance of security.

Yanosky et al. (2008) identified the impact of cloud computing within the IT department of educational institutions. In particular, the traditional roles of IT department are changing to consultant or certifier role and such change could negatively impact on the organizational functionalities. Once the users can fulfil their needs through cloud then they will be less tempted to perform individual IT responsibilities such as set update the patch and back-up. Dependencies on cloud could lead outward rather than upward. The central IT is no longer enjoy the connectivity or access to application as well as would not be able to define a safe and auditable system.

3.3. Security Risks

Security risk is the one of the top most barriers for the cloud adoption decision. Such risks are complex in cloud and vary comparing to the traditional computing environment due to unique cloud computing characteristics such as multi-tenancy, shared resource pooling, and elasticity. For instance, data leakage can be controlled within in-house infrastructure by using tool, but such tool is difficult to implement in the cloud. A CSP is hosting data for different customer that makes it hard to identify time and location of the leakage and violation of the policies. There are several works that demonstrate the successfully attacks the CSP infrastructure. Specifically, Amazon EC2 is vulnerable of Signature Wrapping Attack which poses to any Denial of Service (DoS) attack within the EC2 infrastructure (Gruschka and Iacono, 2009). EC2 is also susceptible to side-channel-attacks Ristenpart et al. (2009) that allows attacker to obtain sensitive data about the user. However, Amazon in their latest security report (AWS, 2014) also claims that AWS network provides significant protection against traditional network security issues such as DDoS attack, MITM, IP spoofing, port scanning, and packet sniffing by other tenants. Cloud malware injection attack also helps that attacker to obtain the legitimate user data (Jensen et al., 2009). Khan et al. (2012) identify a list of threats for the security risks analysis considering different cloud scenarios. The threats are categorized into six different types and risks assessment is considered for the cloud deployment and operation phases based on the probability of each threat affecting the particular assets by following Bayesian dependencies. The security threats and risks vary depending on the type of service model (CSA, 2009). The more the users able to extensibility of using own features in cloud such as IaaS provides maximum extensibility and SaaS minimum, the higher the security risks and user responsibilities to control these risks. Similar to the traditional computing environment, attacks like man-in-the middle, cryptographic, and Trojan are also potential attack for cloud computing(Gregg,2010). The technical level security attacks are based from the usage of cloud services such as wrapping attack which can modify the content of a message and successfully exploited in Amazon EC2 (Jensen et al. (2009)). Browser based authentication protocols in cloud are also not secure as browser is not able generate XML based security token and security token within the browser are not protected. Cloud system is responsible for maintaining and coordinating instances of virtual machines (IaaS) or explicit service implementation modules (PaaS),

cloud malware could inject adversary attempts of attackers within these instances through malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS). Service integrity check can overcome such attacks through hash value on the original service instances images and compare it with the new instance. Flooding attack is also applicable in cloud when an attacker sends enormous amount of unnecessary requests to consume the cloud server processing power. A successful flooding attack can also deteriorate the other service instances of the same physical sever. Dahbur et al. (2011) present different real security attacks that is applicable in the cloud, such as tenant-on-tenant attacks and cloud computing outage and data loss with provider like Rackspace.

Gruschka and Jensen(2010) propose a taxonomy for the attacks on cloud computing. The attack taxonomy is based on a triangle of user, service instance and cloud and bi-directional communications among these participants. The service instant towards a user is the well-known attack surface similar to a client server attack model such as buffer overflow and SQL injection. The attack surface extends with cloud system's attack to the service instance such as resource exhaustion, service instance to cloud system such as availability reduction, cloud system to the user such as impersonating as a legitimate to modify the cloud control interface. Several recent attacks on cloud surface such as Amazon EC2 hack are included in the work. Nahar et al. (2012) identify critical risk factors of Business Model and IS Innovations based on empirical investigation on a Scandinavian small cloud based social gaming software company. The top five risks are constant R&D, lack of talent developers, failure to implement new business model, Upgrading IT infrastructure and diverse products. Therefore, business depends on cloud need to deploy new business model for its survival and success. However, the results do not provide any recommendation that should be taken into consideration for the cloud based Software Company. Ardagna et al (2015) consider cloud security threats and attacks from application, tenant-on-tenant, and tenant –on-provider levels. The controls are classified through encryption, signature, IDS/IPS, access control, authentication and trusted computing.

The European Network and Information Security Agency identifies (ENISA, 2009) provides a list security risks based on the three use case scenarios. The risk estimation is based on the likelihood of each incident and business impact of the incident through three different levels, i.e., low, medium and high. The identified high ranked risks are such as lock-in, malicious insider loss of governance, compliance challenges and isolation failure and medium ranked risks are such as loss of business reputation, service failure, cloud provider acquisition, and supply chain failure. The risks impacts are varying depending on the type of cloud model. CSA identifies seven top cloud specific threats such as abuse of cloud computing, insecure interface, malicious insiders, shared technology issues, data loss, account hijacking, and unknown risk profile that could impact any cloud service model (CSA threat, 2010). Heiser and Nicolett (2008) in Gartner report also identify security threats such as privilege user access, regulatory compliance, data location, lack of segregation and recovery, and long-term viability. Some of these threats are similar to the CSA threats such as malicious insiders and data loss. Kalloniatis et al (2014) show how CSA and Gartner identified threats match with the CSA critical cloud areas and cloud service models.

3.4. Privacy Risks

Privacy is the ability of individual to protect information from any unwanted leakage. It is difficult to measure how much privacy should be built into a system and there is no consensus about it. Cloud computing changes the way in which information is being processed. This raises the serious concern of individual privacy. For instance, it is difficult to identify and control any secondary usage of data as data is stored in the CSP's infrastructure and tends to get transferred in data centres in different geographic locations. Theoharidou et al. (2013) examine the privacy risks for the migrated data, applications or services into the cloud by following privacy impact assessment with ten fundamental privacy principals such as accountability, clear purpose, consent, collection, use, accuracy, security, openness, ability to access, and ability to challenge privacy practice. Privacy risks can impact on an organization such as loss of reputation, breach of contractual obligation, economic loss and many

more. Vimercati et al. (2012) review the privacy risks and existing solutions for managing and access data in the cloud. The risks are concerned due to data dissemination and sharing, external storage of data, collaborative query execution, and anonymous communication for the data access and stored into cloud. Protection user's identity while accessing services and resources are necessary for privacy and attribute based access control, user preference on the information based on the information sensitivity are considered as the techniques generally used for the identity protection. A combination of encryption with fragmentation technique is can be used to protect confidentiality of stored data. Kalloniatis et al. (2014) identify a list of privacy properties such as anonymity, pseudonymity and unlinkability along with security properties that should be taken into consideration while protecting from security and privacy threats.

Savola (2010) used risk driven methodology based on privacy threat analysis, utilization of taxonomical information, and decomposition of privacy and system requirement for determining privacy metrics of the cloud services. The metrics development consists of several stages including identification of privacy threats relating to user's information such as secondary usage, change of privacy rights and obligations, user record investigation, ownership of CSP. Nest stage utilizes privacy taxonomies so that privacy objectives and requirements can be identified based on the taxonomies. Based on the privacy requirements next stages emphasize on measurable components, their architectures, feasibility analysis and detailed collection of privacy metrics. However, it is not always possible to measure the metrics values and the metrics can be ambiguous considering the requirements. Pearson (2009) identified several privacy risks for cloud computing from user, organization, cloud platform implementers, and providers. In particular, the risks are mainly disclosed of personal information, non-compliance to enterprise policies, loss reputation. The privacy requirements based on the fair information principles and privacy enhancing technologies support mitigation of these risks.

3.5. Case Study

There are several efforts focus on understanding the risks associated with the specific cloud migration scenario. The main aim is to identify the risks and control them so that the studied context can obtain the real benefits of cloud migration. Samad et al. (2013) demonstrate the proposed context aware risk management model through a mobile cloud based e-health application. The application is a real-time health monitoring and analysis prototype system using Aneka cloud computing platform and Amazon's S3 storage services. The result observed that it is hard to assign probability value of risk factors due to human and environmental issues such as bad weather and noise. The case study considers three different scenarios to analysis the role of context for calculating the risk event probability. Three main risks are resource exhaustion, service unavailability and portability due to the risk factors such as battery hardware problem, connection types, different memory size, data allowance on the 3G plan and low bandwidth and these factors vary on different scenarios. However, the case study does not include any solutions for mitigating the identified risks. Gadia (2011) presents a cloud risk assessment case study of a software development company which intended to migrate into the IaaS based solution instead of existing SaaS solution. The case study is about an audit performed for identifying the risks associated with SaaS solution. Seven high level risk scenarios are considered including technology selection, third party supplier selection, logical attacks, information media, database integrity, logical trespassing and contractual compliance that are applicable for the SaaS based solution and map with the COBIT control objectives. The are several audit finding based on the risks and control objectives such as provider contract does not address the user's security and privacy requirements, multi-factor authentication was missing, sensitive data is exchange without secure a channel, personal identifiable information is stored in plain text and missing independent auditor report. Such findings give a real picture about the gaps by the CSP to achieve the security objectives. Islam et al. (2012) identify three risks data leakage, poor privacy risks and back up from a research institute migration use case. The work recommends several solutions such as data classification, encrypted confidential data, access control policy, pause sync to control the risks through the responsibilities both user and CSP.

Khosravani et al. (2013) present a case study about managing the risks of cloud adoption associated with highly sensitive data held for children and sexual abuse cases of a charity organization. The case study is evaluated through a framework that analysis the trust and control for mitigating the risk of cloud adoption. The risks are considered from three categorizes, i.e., policy and organization (lock-in, lack of customer support and skill), technical (insufficient data, data availability and hidden cost), and legal risk (lack of standard and interoperability). However, losses of control over sensitive data and lock –in are considered the top prioritized risks for the study context. The trust building between the charity and provider was done through ensuring transparency by the provider and giving technology details of the infrastructure. It also helps to mitigate the identified risks. Baars and Spruit (2012a) analysis the security risks of cloud adoption based on a Dutch utility provider using ScCA risk management model Baars and Spruit (2012b). The case study mainly follows action research setting by identifying the risks of the data classification. The model follows data centric approach and differentiates the user rights of the data stored and processed using a list of attributes. The cloud services are analysed based on the data classification and security specification. One of the identified providers is not selected due to the jurisdiction and location problems. The model supports the decision makers to identify the security risks associated per cloud solution with data classification. Khajeh-Hosseini et al. (2010) identified potential benefits and risks for migrating into cloud from a case study of an oil and gas industry SME in UK. The result showed that there is definite cost saving system infrastructure advantage, i.e., 37% less over 5 years on EC2 as well as eliminate 21% support calls from the system. The result also shows that despite the benefits cloud migration such as opportunities to manage income & outgoings and to offer new services, removal tedious work, and improve work satisfaction, there are also risks mainly deterioration of customer care and service quality, dependency to the third party, decease satisfying work, and department downsize. The study concluded that socio-technical issues that must be taken into consideration for the cloud migration. ENISA (2009) analyzes three use-case scenarios, i.e., SME perspective, service resilience, and e-health, for the purpose of risk assessment. The results identified a list of high and medium level risks that was mentioned in the previous section. The report emphasize on the legal issues such as data protection, confidentiality, intellectual property, professional negligence, outsourcing services and changes in control, which are common across all scenarios. The National Institute of Standards and Technology (NIST, 2011) identified a list of cross cutting security requirements from several business cases such as NIST IT Service Management, Virtual Desktop Infrastructure, and USAID Office Productivity, FAA eDiscovery. The requirements are mainly identity management (Single Sign-On (SSO), Strong Authentication, and User Provisioning), security audit information, encryption, physical security and assessment and authorization. A risk mitigation strategy is followed to address the inherent challenges of the requirements so that the requirements can satisfy the mission purposes.

4. A SURVEY OF MIGRATION GOALS AND RISKS IN CLOUD COMPUTING

We perform a survey and compared the survey results with other survey results and our state of the art investigation to consolidate our findings. The survey contributes identifying the goals and risk relating to cloud migration. This section presents the result of a survey investigating the risks to and the goals involved in cloud migration.

4.1. Research Method for the Survey

The method followed in the survey was a three round Delphi process. The main advantage of the Delphi method is that it considers multi-phase iterative surveys with controlled feedback loops (Schmidt, 1997). Phase 1 involved understanding the organizational context for the cloud migration. Phase 2 focused on identifying the goals and risks in cloud computing. These goals and risks were then ranked in phase 3. We followed open question for the survey so that participants can provide

their view and feedback relating to the migration goals and risks for the cloud migration and had the role to reduce the bias of using closed questions.

- **Phase 1: Identify the Organizational Context for Cloud Migration:** The first phase focused on identifying the organization context for the cloud migration. A review of existing organizational IT infrastructure and potential computing services for the migration were considered. Furthermore, if the organization is already migrated into cloud then we gathered information about the migration portfolio.
- **Phase 2: Discover Migration Goals and Risks:** This phase started with identifying the high level goals that could leverage an organization for the cloud migration. These goals were then used to identify the risks that could obstruct the. The participants provided their views based on their experience and the organization context identified from the previous phase. All questions in the questionnaire were open question and a short guideline is provided relating to goals and risks. The open ended questions allowed the participant to provide their own views depending on their roles and responsibilities.
- **Phase 3: Rank the Migration Goals and Risks:** This final phase of the survey ranked the goals and risks. We consolidate the identified goals and risks from the previous phase. We ranked the goals and risks based on the frequency of response. The ranked goals and risk were sent to the participant for their consensus. All the initial ranked goals were agreed by the participant. However, three participants disagreed with the ranked two risks and provide their views. In general, we have concluded with a consensus for the final ranking.

4.2. Survey Context

The survey participants were mainly from two different countries. They were twenty participants from both public and private organizations in UK and Malaysia. The participants were selected based on educational qualification and work experience in the industry. We have considered at least graduation degree in IT or any other related discipline and at least three years job experience. The participants were technical professionals across broad roles and responsibilities within the organizations. We considered the online based questionnaires distribution and response as well as face to face interview in case of some UK participants. The face to face interview lasted for around 60 minutes. Figure 2 summarizes participants' organization type. 55% participants were from the large public organization from both countries such as health care, government ministries and private participants' organization were equally participated 15% each. Table 4 and 5 briefly highlight the survey participants' organization business domain and role of the participant within the organization and a sample survey questions is included in the appendix A. All participants were experienced with their job roles and some of them were in management position when we did the survey.

5. SURVEY RESULTS

This section provides the results of the survey including the existing cloud adoption status, migration goals and risks. The results of the survey showed a high consensus on the identified goals and risks among the participants.

5.1. Cloud Adoption Status

Figure 3 shows the cloud adoption status for the survey participants' organization. 16% of the participants' organization are already have their own cloud Infrastructure as a Service(IaaS) based model for supporting their business and/or using it for various purposes such as data analysis, storage, and corporate social media. 20% of the participants' organizations are migrated into public or private cloud provider for data storage, e-mail, document sharing and management, and code repositories.

Figure 2. Participants' organization types for the survey

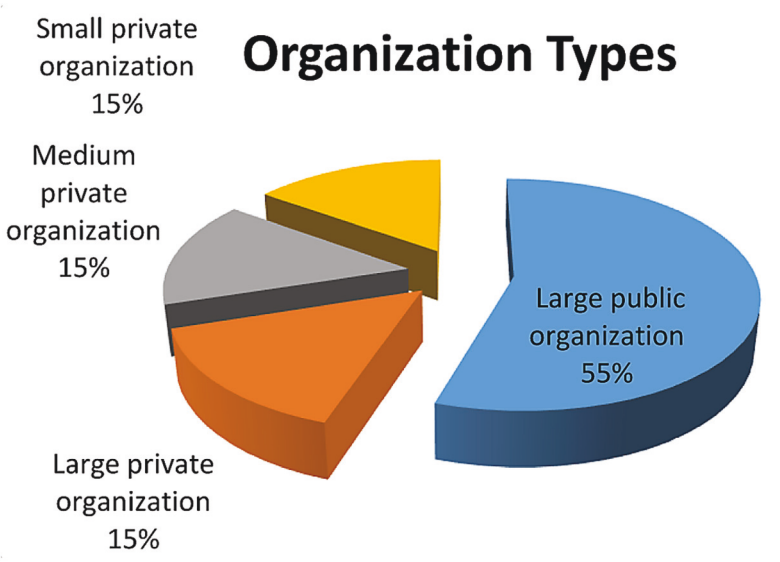


Table 5. Malaysia survey participant's details

Participant organization	Domain and Position
Malaysian Palm oil board	Public organization to support Malaysian oil palm industry Position: Admin
National audit department of Malaysia	Public organization to support the audit activities Position: IT staff
Persona Ilham corporation	Medium private organization for oil and gas, construction Position: Technical manager
Department of statistics	Public organization to release various statistical information Position: Technical supervisor
Ministry, Malaysia	Health care based large public organization Position: IT supervisor
MIMOS	Large private organization for national R& D centre in ICT Position: IT staff
Ministry, Malaysia	Health care based large public organization Position: IT assistant manager
Ministry, Malaysia	Public organization to support the PM office Position: Internal auditor
Protect network PVT limited	Private small organization Position: IT support

There are some participants' organizations, i.e., 20%, which already migrated into cloud and planning to migrate other applications such as application development, property management system, office software, payment service, computer aided facility management, mobile device management, e-mail, and storage. 32% of the participants' organizations are potential to consider migration for storage, application hosting, and e-mail. Most of the government organizations are not still migrated into

cloud and some of them are reluctant to migrate. The main reasons are the extra fund to support the migration, lack of IT skill and knowledge about the cloud through the entire organization, lack of evidence to guarantee data leakage obstruct for cloud migration. Therefore, we have 12% of participants' organization that are not willing to consider migration.

5.2. Migration Goals

The participants agreed five main goals that justify main motivations for the cloud adoption. Figure 4 shows the goals based on the participants' response. The details of the identified goals are given below.

- **Cost Savings:** Cost saving is the top ranked goal for the cloud migration. Most of the practitioners' view that hardware is cheaper but human who is responsible to manage the hardware is very expensive. Operation and maintenance cost is one of the key issues for today's business context. Cloud can reduce this operation and maintenance cost. Operation cost minimization is necessary for small rapid expanding business. One participant considers space saving is another key issue for the cloud migration. Cost saving also includes the licensing cost that could be huge for large government organization and investment for implementing the security measures. Large investment for security is not always possible for organization specifically for SME; cloud can support better security protection for such organization type.

- **Collaboration and Sharing:** Most of the participants agreed that cloud provides a better collaborative virtual working environment, which gives individual with greater remote access flexibility independent of platform and system. This unique access environment eases the sharing of information among all the users. In house environment cannot always provide accessibility to all platform and service. Cloud allows remote working facility, so that organization can save the office space and other logistic support.
- **Better Scalability:** Scalability is always an area that needs constant real time monitoring and infrastructure support with skill staffs. Cloud provides unlimited virtual server in physical infrastructure and eliminate the need for the dependency of advanced technical IT staff. Better scalability also reduces the maintenance overhead.
- **IT Efficiency Increase:** Cloud can reduce the down time for the service continuity. Most of the Malaysian participants mentioned that IT efficiency can be adequately increased by the cloud migration. Reduce complexity for the support service is key for many businesses specifically

Figure 3. Participants' organization cloud adoption status

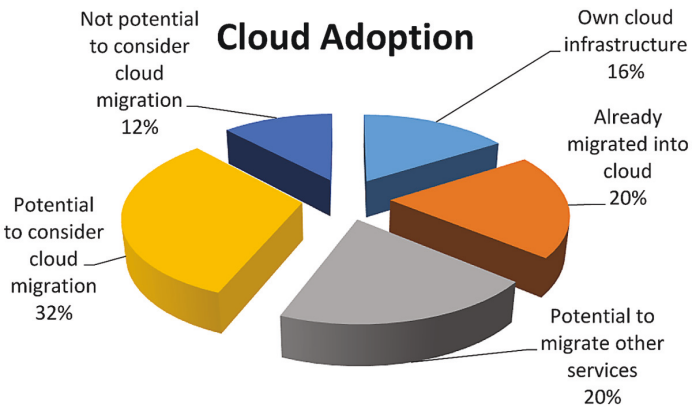
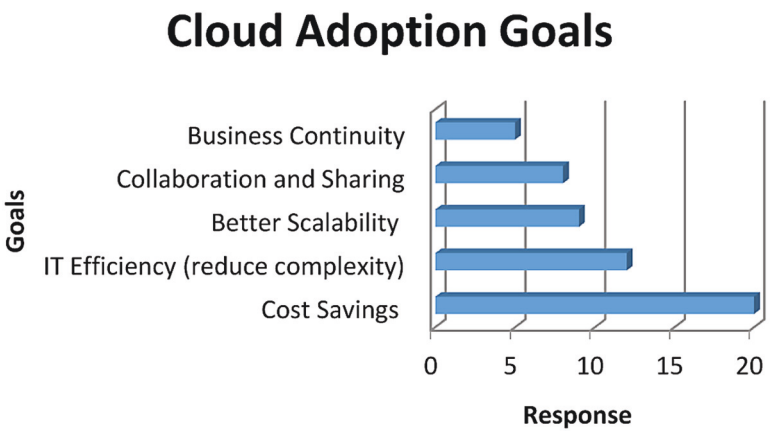


Figure 4. Cloud adoption goals



SME and public organization. The overall IT efficiency can also increase due to centralized document control and quicker response time to the users of the organization.

- **Business continuity:** It is easy to deploy into cloud. Cloud provides higher resilience to support business continuity comparing to the traditional computing environment. In particular, if the in-house service is down cloud could support the business continuity and less maintenance downtime. Users can also obtain full disaster recovery and business continuity support from the CSP. Speed up the business process so that it can effectively deliver services to the customer. Specifically, the government ministry is supporting a large number of users for the various support services and cloud could promote effective public service delivery.

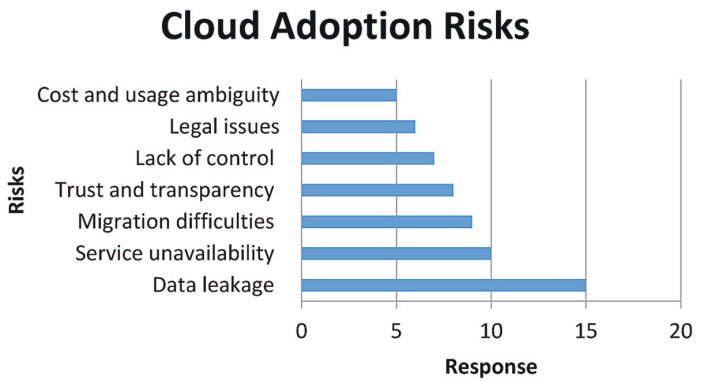
5.3. Risks

Figure 5 shows seven consolidated risks sequentially depending on the frequency of responses. There are several risk factors caused for specific risks are identified by the survey participants. These factors linked with both user and CSP organization.

- **Data Leakage:** Data leakage is ranked as the top risk by the all participants. Some participants' organizations are dealing with high sensitive data such as auditee details, customer bank details, and patient data as well as organization own business plan. Therefore, leakage of the data could pose severe negative impact on the organization. In case of cloud, malicious insiders or tenant can unauthorized access to the user data and incomplete data deletion can cause for the leakage. The risk can happen in both up and down of data as well as communication among different CSPS or data centres. Adequate security protection is necessary not only protect from external attack but also from the internal user attack.

- **Service Unavailability:** Failure to deliver services can severely impact on the business continuity and organizational functionality. Some participants mentioned that resilience is highly important for their business. This risk is due to lack of CSP redundancy, unstable CSP for under provisioning and over provisioning and could interrupt the resilience which is highly important for the business as mentioned by some of the participant.
- **Migration Difficulties:** Participants agreed that migration difficulties need adequate attention from the beginning, specifically if the migration is considering mission critical data or application. This risk is due to the lock-in issue, necessary resource to support the migration, budget overrun,

Figure 5. Cloud adoption risks



adequate training with cloud technology. These difficulties are key concerns specifically for a large public organization and restrict them for undertaking cloud migration. Migration is a great concern due to down-time of services, where staffs are working through different locations. Migration difficulty can also arise from the violation of data integrity during the migration, poor project plan and wrong decision over the cloud environment. There is no standard tool support or procedures that support an organization to migrate into cloud or from one provider to another provider.

- **Trust and Transparency:** Participants were emphasized on trust and transparency as data is generally stored in a multi-tenant platform. Lack of monitoring facility of user data incurs less user trust on the CSP. Data traceability is necessary in terms of traffic to the server, usage and access log. Cloud users expect assurance of transparent services, adequate protection of the data and compliance of the SLA to entrust the CSP. Participants agreed that currently there are lack of transparencies in terms of data usage and storage in different jurisdictions.
- **Lack of Control:** This is due to the more dependency on cloud service provider for the business continuity. Such risks interrupt to the organization functionalities. Users need the ownership and control of their data specifically relating to location, sharing the data with others, and making decision for sharing their own data. Some participants mentioned that the roles for dealing with CSP and migrated data are not completely clear within their organizations. Such unclear role and poor enforcement pose the lack of control of user migrated data.
- **Cost and Usage Ambiguity:** Practitioners agree that cost and usage ambiguity can outweigh the expected cost saving benefits of cloud migration. In particular, it is difficult to forecast future usage of cloud. Furthermore, migration cost can be also a concern due to train the staff using new technology, and recruit consultant, which sometime hard to allocate for the public organization. There is also a variation of cost due to variable bandwidth for billing. This cost ambiguity can out weight the overall cost reduction of cloud
- **Legal Issues:** Legal implication in term of ownership of data, accountability for performing actions and data location are critical and pose for any potential damage. In case of cloud, it is necessary in-depth review of the SLA clauses, specifically defining the right and obligation of related events. If breach of contract happen then provider should be involved in legal penalty.

5.4. Comparing Survey Results with Other Studies

We compare the results of our survey study with other study results from the literature. In terms of identified risks and goals, there is a substantial commonality fully or partially amongst our results and those discussed in the existing literature. For instance, the survey on data migration by Hitachi data systems identified that downtime and extended downtime impact on business and budget

overrun, revenue loss and legal liabilities are the main risks for the data migration (Hitachi, 2014). 25% of the projects have suffered more than 10% budget overrun for cloud migration project. The cost reduction due to data centre operating expenses, labour cost, change management are the key motivations for the data migration. Our results also identified these factors under the migration difficulties risks. Participants in our case also considered other key areas such as necessary resource to support the migration, budget overrun, adequate training with cloud technology and data integrity under the migration difficulties. The European Network and Information Security Agency (ENISA) performed a SME perspective on cloud computing survey focusing on actual needs, requirements and expectation of SME for the cloud computing services (ENISA Survey, 2009). The three main reasons for cloud migration are (1) due to avoiding capital expenditure in hardware, software, IT support and more information security by outsourcing, and flexibility; (2) scalability of IT resource; and (3) business continuity and disaster recover capabilities. The five main concerns to cloud computing are identified as (1) privacy, availability of service and /or data, (2) Integrity of service and /or data, confidentiality of corporate data, (3) loss of control of services and /or data, (4) inconsistency between transnational laws and regulation, lack of liability of providers in case of security incident, and (5) unclear scheme in the pay per use approach. Our study results also find similarities with all these goals and risks, specifically cost reduction and data leakage are the top goals and risk in our case is fully similar with the ENISA report. A survey report by Microsoft TechNet identified that 32% participants considered operational cost saving and IT efficiency, 28% considered ability to grow and shrink IT capacity, and 25% considered hardware cost saving and rapid launch of new products were the most important benefits of the cloud (Microsoft Survey). The report also identified that data sovereignty & privacy (18%), Integration with existing systems (14%), existing infrastructure (13%) were the main barrier for cloud adoption. In summary of these studies, cost savings is the top cloud migration goal for any organization type and size from any geographic region. However, there are several risks such as migration difficulties, data leakage, integrity, and availability of service are the main concerns by the users.

6. DISCUSSION

This section summarizes our finding from both state of the art review and survey results. Most of the existing works in the literature and industry report justify the need and importance of considering the risk management for cloud computing. Our survey results also identify a list of critical risks and associated factors and migration goals from the participant's experience. We have several observations from this state of the art review and survey results as future necessary directions for the cloud computing risks management.

6.1. Risk Management in Cloud

6.1.1. Risk Management Framework

We have provided an overview of the state of the art review that considers risk management framework, risks and control in cloud. The review also includes case study results and lessons learn from real organization context. There are several research articles and industry papers that focus on the risk management framework in cloud mainly considering security and privacy risks. The framework includes a brief process for the risk assessment mainly following qualitative or semi-quantitative approach due to lack of data for full quantitative assessment. The key security objectives, i.e., confidentiality, integrity and availability, are the main concern by most of the works. Risk management challenges for cloud based system are also taken into consideration by the approaches and information security management system standards are also considered for the risk management process. The reviewed frameworks are mainly focused on the security and privacy risks except Prasad and Ben (2010), Fit´o et al. (2010), and ENISA (2009). Prasad and Ben (2010) work consider security risks but the impact is driven from the business benefits. Fit´o et al. (2010) work business level objectives for the risk assessment. However, the reviewed risk management frameworks do not provide any

detailed guideline regarding risk identification, control, and monitor. There is also a lack of focus on the organization migration context for the risk management. ENISA (2009) identifies a list of risks and calculates the risk level based on the impact on the overall business. CSA's cloud control matrix supports the CSP to improve the overall security practice and guides the users to assess the CSP based on their needs CSA CCM (2014).

6.1.2. Goals and Risks

There are commonalities of identified goals and risk by the different works and survey results. Khajeh-Hosseini et al. (2010) identified cost saving, opportunity to offer new product/ service are the potential benefits for the cloud migration. Other studies focus on faster implementation, easier maintenance and upgrading, improved flexibility besides the cost saving advantages in cloud (Lin et al., 2009; Armbrust et al., 2010). ENISA (2009) highlights security, standard interface, rapid scaling are the main benefits of cloud. Our survey also ranked cost saving, better scalability, and IT efficiency as the top three goals for the cloud migration, similar to other survey results presented in the last section. Therefore, despite of any migration and organizational context, cost saving is one of the main motivations for the cloud migration.

Risk factors relating to data leakage and service unavailability in cloud are the top concern by most of the works and survey results. Khajeh-Hosseini et al. (2010) identified risks based on the studies context, i.e., deterioration of customer care and service quality, dependency on the third party, decease satisfying work, and department downsize. Out study results identified a list factors that pose for the seven ranked identified risks as presented in the previous section. Yanosky et al. (2008) observe that traditional roles of IT department are changing to consultant or certifier role and such change could negatively impact on the organizational functionalities due to cloud migration. We also retrieved a number of white papers and report about the risks and existence practice to control the risk by the CSP. Such evidence implies that cloud is already obtained a lot of attention by the industry community. Heiser and Nicolett (2008) in Gartner report and ENISA report emphasize on legal risks besides the traditional security and privacy risks. The works relating to identified goals and risks in cloud are well-progressed and potential cloud users are aware the benefits and possible consequences of cloud adoption.

6.1.3. Case Study

There are contributions that utilize case studies method for identifying the risk factors in cloud computing and determining the applicability of the risk management method. The study results reveal that there are no doubts of significant benefits of considering cloud within the existing business context. But, risks due to the unique cloud computing technology, dependencies with the CSP, security and privacy could severely outweigh the expected benefits. Samad et al. (2013) concluded that it is hard to obtain probability value of risk factors due to human and environmental issues. The main three risks are resource exhaustion, service unavailability and portability for the mobile cloud. Risks such as deterioration of customer care and service quality, dependency to the third party, decease satisfying work, and department downsize identified by Khajeh-Hosseini et al. (2010) are the top prioritized risks for the studied context. Khosravani et al. (2013) consider loss of control over sensitive data and lock –in as top prioritized risk. The case studies results shown variation of risks. It is worth to mention that the identified risks are from both technical and non-technical dimensions. Note that, not all the reviewed studies consider specific risk management framework for evaluating its applicability except Khosravani et al. (2013), Baars and Spruit (2012a), and ENISA (2009). Therefore, the case study approach to identify the applicability of risk management in cloud computing is still not mature stage. More studies are necessary to demonstrate the applicability and importance of risks management in cloud computing.

6.2. Observations for the Future Directions

There are several observations from the review and survey results. These observations are the research gaps for the future directions of risk management in cloud

- **Observation 1 (Necessity for a Comprehensive Risk Management Framework):** Security and privacy areas are the main focus for the risk management approaches. A limited number of works have taken the existing organization and business context for the risk assessment. Cloud computing needs to meet all business and organizational computing requirements, other-wise risks relating to a specific context shall never been addressed by the risk management framework. Hence, a comprehensive risk management framework is necessary in cloud that should deeply look at all technical and non-technical dimensions relating to migration and a systematic process to asses and control the risks.
- **Observation 2 (Risk-Driven Approach for Migration Decision):** Risk management needs to perform before an organization considers any migration decision so that users should early aware of possible risks that could impact on the business continuity if the migration decision is taken. However, there has been a little progress towards development of risk management approach to support migration decision and to monitor the risks after the migration. Risk –driven approach certainly assists the organization to define the migration strategies, avoid migration difficulties, and metrics to measure success of using cloud.
- **Observation 3 (Monitoring Evolving and New Risks after Migration):** Risks are evolving by nature. A CSP may any time amend the service the terms and condition and cloud platform can also evolve. Therefore, new risk can emerge or the probability of existing risk can vary due to the evolution of cloud platforms, user requirements or amendments to the CSP's terms and conditions. Furthermore, risk mitigation plan and its implementation are not always under the user control. In particular, CSP plays a critical role for controlling identified risks. It is necessary to monitor the existing risks and identify any new risk after migration. Risk management framework should include appropriate mechanism for the risk monitoring in cloud.
- **Observation 4(Accurate Risk Level):** Fully quantitative risk assessment approach is difficult to follow for the cloud based system due to lack of data for calculating the risk event likelihood. Moreover, it is also hard to quantitatively determine the impact of a risk. On the other hand, full qualitative approach does not provide an accurate value of a specific risk but able to prioritized the risk. Inaccurate estimation can lead to underestimate a risk that might end up with any loss that could outweigh the expected benefits of cloud. There is a limited effort in the existing works to consider the accurate risk level estimation. Therefore, we need to follow a strategy that provides accurate estimation of risks for cloud based system.
- **Observation 5(Necessity of Considering Migration Goals for Risk Management):** Every potential organization intends to migrate into cloud certainly expects several benefits for using cloud. These benefits are the goals that generally include financial gain, scalability, disaster recovery, and many others that we identified in the previous section. Risk management needs to consider these goals so that the potential risks should be analyzed as obstruction to the goals.
- **Observation 6(Demonstration of Applicability and Importance of Risk Management):** There are works that consider real cloud migration use cases to identify risks relating to the context. However, more studies are necessary to demonstrate the applicability and importance of risk management method for the cloud system and to generalize the risks and associated controls for managing the risks. Empirical investigation methods mainly survey and case study should be appropriate to follow to demonstrate the applicability of risk management.
- **Observation 7 (Automation of Risks Management Process):** There is a lack of tool support to automate the risk management process for the cloud computing. The automation should support generating well documented and graphically visualize artefacts from the risk management process so that identified risks and its value can be used further for similar migration context. The tool should support the monitoring of the highly critical and critical risks once the migration decision

is taken and the migration entities are operational phase. It can be used to generate a risk resource repository of cloud specific risks and their countermeasure.

7. RISK ASSESSMENT METHOD IN CLOUD

We propose a risk assessment method based on our observations from the review of the start of the art research and practice and survey results. The approach uses cloud migration goals to determine the risk level as an obstruction of these goals. These goals are prioritized using Analytic Hierarchy Process (AHP) according to their relative importance for the cloud migration (Saaty, 2008). This section provides an overview the risk management method.

7.1. Migration Goals

We identify six migration goals after reviewing the state of the art and survey results. By looking at the five key cloud adoption goals and seven risks, we summarize that these goals are essential for any migration context. These goals are the benefits and expectations from the cloud migration and have the potential impact on the organization. This allows us to focus on business value and organization function due to cloud dependencies along with the technical issues such as security and privacy so that risks that could obstruct these goals should be taken into consideration from all these dimensions. The reason for considering the migration goals for the risk assessment is that risk is defined as a negation of goal. In particular, organizations intend to migrate into cloud have certain which it desire to achieve and risks certainly obstruct these goals fulfilment. AHP is used to determine the relative importance of the goals on the specific migration and organizational context. A brief overview of the goals is given below:

- **Business Value:** This goal includes the main business gain in terms of financial profit, maintenance benefits, service delivery, business growth specifically into new market, and competitive advantages due to cloud migration.
- **Organization Function:** Organization function considers key operations for successfully running the business including internal process improvement, customer services, human resource, collaboration with internal units and business partners, business continuity and disaster recovery, and efficient IT usage and IT availability.
- **Confidentiality:** This goal deals with not to disclose of data to the unauthorized users includes cloud users, CSP internal users, and malicious attackers. The goal also includes secure deletion and transfer of data among authorized parties to prevent the data leakage.
- **Integrity:** Integrity refers to trustworthiness of the migrated resources. In particular, the data migrated into cloud must be modified by only authorized users.
- **Availability:** Availability is concerned with the migrated resources such as data or application being accessible when needed and cloud service should be available as per the agreement,
- **Transparency:** Transparency refers to the dissemination of information about access and usage of user data, security incident, and audit report by the cloud service provider. It also considers real time monitoring of virtual machine and SLA. Transparency is critical for the mutual trust between the user and CSP.

7.2. Net Risk Calculation

We follow semi-quantitative risk assessment method to determine the risk level. As stated before, a full quantitative risk assessment method is difficult to obtain in cloud computing domain due to difficulties of obtaining precise value of risk event probability and impact from the historic data. Qualitative approaches could replace the tedious quantitative assessment so that lack of availability of data should not impact on determining the accurate risk level. In that case risk value may not be

accurate. Therefore, our assessment method combines both quantitative and qualitative approach for calculating the new risk value. It consists of two steps.

7.2.1. Step1: Relative Importance of Migration Goals

In our case, the net risk calculation depends on the relative importance of the migration goals by following AHP. Each goal is compared with the other goals based on its importance level within the organizational context for the cloud migration. The importance levels follow according to the AHP scales, i.e., 1-9 as shown in Table 6, where 1 denotes equal importance and 9 is the extreme importance of one goal comparing to another. Once the importance level of each goal is obtained comparing to the other goals, then the Comparison Matrix (CM) values are normalized to identify the relative weight of each goal. The weight value should sum up to 1. It is necessary to check the consistency of the importance level assumptions. AHP introduced consistency ratio as shown in Equation 1 for checking the consistency. If the consistency ratio value is more than 10% then the assumptions for the relative importance are inconsistent and we need to redefine the values.

Let,
CR: Consistency ratio
CI: Consistency index
RI: Random consistency index
CM=Comparison matrix value

$$\left(\mathbf{CR}\right) = \frac{\mathbf{CI}}{\mathbf{RI}} \tag{1}$$

7.2.2. Step 2: Net Risk Calculation

The net risk calculation depends on the associated risk factor values. These risk factors are the causes for a risk. We need to determine the risk factor values for the net risk calculation. Each risk factor value is estimated through the product of its probability and impact of overall risk as shown in Equation 2. As stated previously, it is difficult to obtain historic data for risk factor probability and overall risk impact in the cloud environment. We use subjective judgment depending on individual perception for defining probability and impact values. We also consider a rule of thumb with the following three rules to support the estimation:

- **Rule 1:** Risk impact depends on the affected migration goals. If a risk affects important migration goals, impact is certainly high.

Table 6. Comparison matrix scale

Importance level	Definition
1	Equal importance of two comparing goals
3	Moderate importance/slightly favour of one goal comparing to the other
5	Strong importance/strongly favour of one goal comparing to the other
7	Very importance/very strongly favour of one goal comparing to the other
9	Extreme importance/ extremely favour of one goal comparing to the other
2,4,6,8	Intermediate values

Table 7. Comparison matrix scale

		BV	OF	C	I	A	T
	Bv	$CM_{i,j}$	-	-	-	-	$CM_{i,6}$
	OF	$CM_{i+1,j}$	-	-	-	-	$CM_{i+1,6}$
CM_{ij}=	C	$CM_{i+2,j}$	-	-	-	-	$CM_{i+2,6}$
	I	$CM_{i+3,j}$	-	-	-	-	$CM_{i+3,6}$
	A	$CM_{i+4,j}$	-	-	-	-	$CM_{i+4,6}$
	T	$CM_{6,j}$	-	-	-	-	$CM_{6,6}$

- **Rule 2:** If the risk factors may be, at least partially, beyond the control of a user's organization and mainly posed by the CSP, the overall risk impact can be higher.
- **Rule 3:** Individual judgment is always useful for net risk calculation. However, individual perception should be closely mapped with reality, otherwise we may overestimate or underestimate risk value.

The risk value is obtained by averaging the risk factors' values as shown in Equation 3. Finally, the net risk level is the sum product of risk level and relative importance of affected migration goal as shown in Equation 4. This allows us to determine the risk level accurately through its influence to the migration goals. We follow the same scales for probability, impact and net risk value to make a simple estimation process.

Let,
ri: Individual risk factor value
ri1.....rin: n influential risk factors of a risk Ri
P(ri): Probability of a risk factor ri
Probability scales= unlikely(less than 0.30), likely(0.30-0.59), certain/expected (above .60).
I: Impact of overall risk Ri
Impact scales= low(less than 0.30), medium (0.30-0.59), high(above .60)
Ri: Value of a risk Ri
Rnet:Net risk of Ri
We: Relative weight of the affected migration goal [BV, OF, C, I, A, T] by Ri
Risk level scales: low risk (less than 0.30), critical risk (0.30-0.59), highly critical risk(above .60)

$$ri = P(ri) \times I \quad (2)$$

$$Ri = \frac{1}{n} \sum \{ri1, ri2, ri3, ..., rin\} \quad (3)$$

$$Rnet = \sum We \; x \; R\,i \quad (4)$$

Risk levels

- Low risk (less than 0.30) implies that it is recommended to develop a corrective measure and contingency plan.

- Critical risk (between 0.30-0.59) implies the risk has an adverse affect on the organization and corrective actions are needed and a contingency plan should be developed if necessary. A plan should be developed for the execution of the control measure within a specific period of time.
- Highly critical risk (above 0.60) implies the identified control measures for the risk mitigation need to be implemented immediately within a short time frame with a plan. The risk level is highly critical if both the probability of the risk event and its impact are high or one is medium and another high.

8. RELATIVE IMPORTANCE OF MIGRATION GOALS

This final part of our contribution focuses on identifying the relative important of migration goals from different migration scenarios. Two participants of our previous survey agreed to share with us their existing migration use case and gave their views about the relative important of the identified goals. However, due to the confidential reason, we are restricted to present detailed of the migration use case scenario.

8.1. Migration Use Case 1

8.1.1. Organization Context

A SME located in London with open access publishing services of peer-reviewed academic journals and books. The publishing service includes receive articles, assign reviewers, proof read for accepted papers, check anti-plagiarism, publish, indexing and archiving. There are in average thousands of articles published in every month.

8.1.2. Migration Context

The company has recently decided to adopt cloud for performing existing operations to support huge volume publication. There are 25 internal staffs constantly provide technical and operational support. The underlying technology for the open access publication is using a code repository with Python and PHP for storing and archiving documents. The existing in-house systems use three web servers and 20Mbps of bandwidth for up and down stream. The organization expects high availability of cloud service with minimum downtime, continuous and constant customer service support, and integrated of the migrated data so that it can support unlimited number of researchers/users to access published articles through diverse platforms.

8.1.3. Results from the Relative Importance of Migration Goals

Figures 6 shows the relative importance of the migration goals based on the above migration use case scenario. The top three prioritized goals for this migration context is integrity (37%), availability (28%), and organization function (21%). The result reflects the expectations of the organization from the cloud migration perspective. In particular, integrity of the published open access article and availability of the article and support service are critically important for the SME. The main reasons for these high prioritized goals are that if the migration is undertaken then data is managed by the provider infrastructure, therefore no unauthorized modification of the published article is acceptable in any condition. Furthermore, real time service availability is necessary to allow users accessing articles and to manage the underlying support. Business value is scored only 7%, therefore cost saving is not the main prioritized goal in this case. The consistency ratio for the identified relative importance of migration goals is 3.4% which is less than 10%. Therefore, the result is consistent with the migration context.

8.2. Migration Use Case 2

8.2.1. Organization Context

This use case is about a large hotel group providing services such as hotel room booking, event management, and meeting, restaurant, bars, and property management. There are several applications such as property management system, payment gateway, CRM system, office 365, and share point that are integrated to support the business. The business wants an archive solution to ensure record of e-mail transaction for the longest time as possible to comply with the legal requirements.

8.2.2. Migration Context

The company planned to backup all transaction in a cloud infrastructure besides in house storage. There are 1200 users who are using the system. There are three different data sites and each site needs 1 GB bandwidth. There is about 100 TB of storage necessary for the next three years to support the archive. The company expects robust and stable CSP with real time customer support and constant network access.

8.2.3. Results from the Relative Importance of Migration Goals

Figures 7 reflects the relative importance of the migration goals based on the above migration use case scenario. The top three prioritized goals are availability (39%), confidentiality (20%), and organization function (17%). Availability and confidentiality are the most critical goal if the migration is undertaken. This is due to compliance with legal requirements for all transactions with the customer and protects the transaction related information from any leakage. Business value is slightly lower importance than organization function. Therefore, the organization concerns about the business values specifically in terms of cost saving however meeting legal requirements are more important for them if the cloud migration is taken in place. The consistency ratio for the identified relative importance of migration goals is 4.8% which is less than 10%. Therefore, the result is consistent with the migration context.

8.3. Comparisons of the Results

The results of the two migration use cases show that the relative importance of migration goals is highly influenced by the migration and organization context. Moreover, external factors such as legal compliance are also influenced for determining the migration goals. In both cases, business value is not among the top three prioritized goals. Participants admit that cost saving is an important factor, however there are other issues such as integrity of research data for the use case 1 and availability of transaction archive which are more critical to ensure if the migration decision is taken. In both cases, availability is one of the high prioritized goals. Furthermore, organization function is another great concern for the both scenario. This makes sense, as in general data is stored in an environment which is out of user control and there is a strong dependency with the cloud service provider to support the organization operations. Therefore, constant customer support with minimum downtime from the CSP is essential for both organizations. Confidentiality of migrated data is not relatively important for the use case 1 as the SME deals with the open access publication. However, this goal is important for the use case 2 as the organization deals with huge customer transactions and need to retain the transaction for a certain period of time.

9. CONCLUSION

Despite of the rapid adoption and strategic important of cloud, risk management is one of the most important concerns for wider cloud adoption. Risk management in cloud computing has already gained a lot of attention by the industry and research community. In the last few years, the community has worked hard to develop risk management method in cloud computing and identify the key risks that could pose any potential loss due to cloud adoption. Therefore, it is necessary to understand

Figure 6. Relative importance of migration goals for migration use case 1

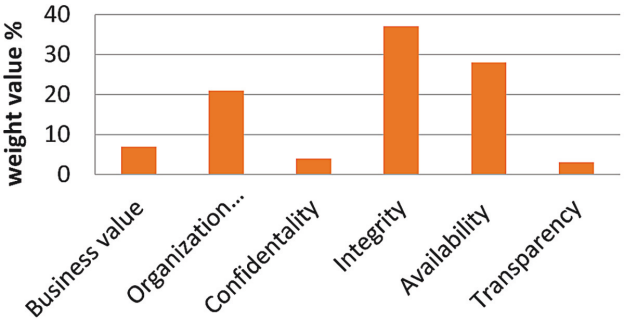
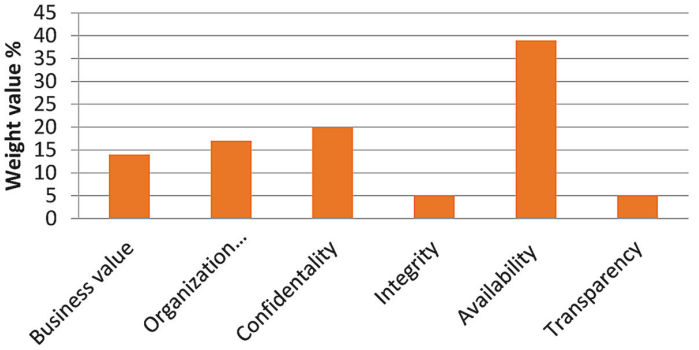


Figure 7. Relative importance of migration goals for migration use case 2



the research trend, gaps and future directions for the domain. Our efforts of this paper is timely and aware the relevant stakeholder for future directions of risk management. We consolidate the start of the art works for the risk management in cloud from both research and industry community. We also performed a survey with experienced practitioner from two different geographic locations. The results from the state of the art review and survey provide a comprehensive view of the existing status of risk management and summarized seven main observations. These observations are future research trends for an effective risk management practice in cloud computing. It is therefore necessary to develop a comprehensive risk management framework that should support the cloud migration decision and monitor the risk after migration.

Our survey results also revealed that despite of cost saving and other benefits, specifically public organizations are not fully convinced for the cloud migration. The main reasons are that risk relating to data leakage, migration difficulties, and others should be identified and controlled through the assurance of cloud service provider. We identified six migration goals that are essential for any cloud migration project. Finally, we propose a risk assessment method to determine the net risk level that impact on the organization if the migration decision is taken. The risks are assessed based on their influence on the prioritized migration goal. Two migration uses case scenarios are taken into consideration to determine the relative importance of the goals. The result shows that

relative importance of migration goals is highly influenced not only by the migration and organization context but also by external factors such as legal compliance. We plan to develop a comprehensive risk management framework by following the observations and this assessment method will be a part of risk analysis. We also focus on developing tool support to automate the risk management process and implement the framework into real industry context.

ACKNOWLEDGMENT

This work was partly supported by the Austrian Science Fund (FWF) project no. P26289-N23. We would like to thank all the survey participants for their valuable comments.

REFERENCES

Amazon Web Services. (2014). Overview of Security Processes. Retrieved from [REMOVED HYPERLINK FIELD]http://aws.amazon.com/security/

Ardagna, A., Asal, R., Damiani, E., & Hieu Vu, Q. (2015, July). From Security to Assurance in the Cloud: A Survey. ACM Computing Surveys, 48(1).

Baars, T., & Spruit, M. R. (2012a). Analysing the Security Risks of Cloud Adoption Using the SeCA Model: A Case Study. *Journal of Universal Computer Science*, *18*(12), 2012.

Baars, T., & Spruit, M. R. (2012b). Designing a Secure Cloud Architecture: The SeCA Model. *International Journal of Information Security and Privacy*, *6*(1), 14–32. doi:10.4018/jisp.2012010102

Binz, T., Leymann, F., Nowak, A., & Schumm, D. (2012). Improving the Manageability of Enterprise Topologies Through Segmentation, Graph Transformation, and Analyzes Strategies.*Proceedings of Enterprise Distributed Object Computing Conference (EDOC)*. IEEE Computer Society Conference Publishing Services.

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from Applying the Systematic Literature Review Process within the Software Engineering Domain. *Journal of Systems and Software*, *80*(4), 571–583. doi:10.1016/j.jss.2006.07.009

Bruening, P. J., & Treacy, B. C. (2009). Cloud Computing: Privacy, Security Challenges, Bureau of Nat'l Affairs. Retrieved from www.hunton.com

Catteddu, D., & Hogben, G. (2009). Cloud Computing: benefits, risks and recommendations for information security. *Enisa.* Retrieved from www.enisa.europa.eu/act/rm/files/deliverables/cloud.../at.../fullReport

Cloud Security Alliance. (2009, December). Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Retrieved from http://www.cloudsecurityalliance.org/csaguide.pdf

Cloud Security Alliance. (2010, March). Top Threats to Cloud Computing V1.0.

Cloud Security Alliance. (2014). Cloud Control Matrix (CCM) Version 3.0.1. Retrieved from https://cloudsecurityalliance.org/research/ccm/

Dahbur, K., Mohammad, B., & Tarakji, A. B. (2011). A survey of risks, threats and vulnerabilities in cloud computing.*Proc. of ISWSA 2011*. Amman, Jordan. doi:10.1145/1980822.1980834

ENISA. (2009, November). Cloud computing Benefits, Risks And Recommendations For Information Security.

ENISA_Survey (2009, April). A SME perspective on cloud computing survey, The European Network and Information Security Agency. Retrieved from https:/www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-sme-survey

FedRAMP The Federal Risk and Authorization Management Program. (2014). Security assessment process. Retrieved from https://www.fedramp.gov/resources/documents/

Fit'o, J. O., Mac'ıas, M., & Guitart, J. (2010). *Toward Business-driven Risk Management for Cloud Computing, Proceeding of IEEE international conference on Network and Service Management*. CNSM.

Fowler, M. (2002). *Patterns of Enterprise Application Architecture*. Addison-Wesley Professional.

Gadia, S. (2011). Cloud Computing Risk Assessment A Case Study. *ISACA Journal*, *4*, 2011.

Gregg, M. (2010). 10 security concerns for cloud computing. *Global Knowledge Training LLC*. Retrieved from http://viewer.media.bitpipe.com/

Gruschka, N., & Jensen, M. (2010). Attack Surfaces: A Taxonomy for Attacks on Cloud Services. *Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD)*.

Gruschka, N., & Lo Iacono, L. (2009). Vulnerable Cloud: SOAP Message Security Validation Revisited. *Proceedings of the IEEE International Conference on Web Services ICWS '09*, Los Angeles, USA. IEEE. doi:10.1109/ICWS.2009.70

Heiser, J., & Nicolett, M. (2008). Assessing the Security Risks of Cloud Computing. *Gartner*.

Hitachi. (2014). Reduce costs and Risks for data Migration. Retrieved from http://www.hds.com/assets/pdf/white-paper-reducing-costs-and-risks-for-data-migrations.pdf

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). (2009). ISO 31000:2009, Risk Management Principles and Guidelines.

Islam, S., Mouratidis, H., & Weippl, E. (2012). A Goal-driven Risk Management Approach to Support Security and Privacy Analyzes of Cloud-based System. In *Security Engineering for Cloud Computing: Approaches and Tools*. Hershey, PA, USA: IGI Global.

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009). On Technical Security Issues in Cloud Computing. *Proceedings of the IEEE International Conference on Cloud Computing (CLOUD '09)*.

Kalloniatis, C., Mouratidis, H., & Islam, S. (2013) Evaluating Cloud Deployment Scenarios Based on Security and Privacy Requirements. Requirements Engineering Journal, 18(4).

Kalloniatis, C., Mouratidis, H., Vassilisc, M., Islam, S., Gritzalis, S., & Kavaklif, E. (2014, June). Towards the design of secure and privacy-oriented Information Systems in the Cloud: Identifying the major concepts. *Computer Standards & Interfaces*, *36*(4), 759–775. doi:10.1016/j.csi.2013.12.010

Khajeh-Hosseini, A., Greenwood, D., & Sommerville, I. (2010). Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS.*Proceedings of the IEEE 3rd International Conference on Cloud Computing*. IEEE Computer Society. doi:10.1109/CLOUD.2010.37

Khan, A. U., Oriol, M., & Kiran, M. Ming Jiang, Djemame, K. (2012), Security risks and their management in cloud computing. *Proceedings of the IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom)*

Khosravani, A., Nicholson, B., Wood-Harper, T. (2013). A case study analysis of risk, trust and control in cloud computing. *Proceedings of IEEE Science and Information Conference.*

Kitchenham, B., & Charters, S. (2007). Guideline for Performing Systematic Literature Reviews in Software engineering. Keele University and University of Durham.

Lemos, R. (2009, August 7). 5 lessons from dark side of cloud computing. *Proceedings of CIO '09*. Retrieved from http://www.cio.com.au/article/314110/5_lessons_from_dark_side_cloud_computing?eid=-156

Lloyd, W., Pallickara, S., David, O., Lyon, J., Arabi, M., & Rojas, K. (2011). Migration of Multi-tier Applications to Infrastructure-as-a-Service Clouds: An Investigation Using Kernel-Based Virtual Machines.*Proceeding of the 12th IEEE/ACM International Conference on Grid Computing (GRID 2011)* (pp. 137–144). IEEE. doi:10.1109/Grid.2011.26

Microsoft. (2012). Microsoft Survey, Cloud computing survey Results. Retrieved from https://technet.microsoft.com/en-gb/gg710912.aspx

Microsoft Office 365. (2014). Mapping of CSA Security, Compliance and Privacy Cloud Control Matrix requirements, Version 3. Retrieved from http://www.microsoft.com/en-gb/download/details.aspx?id=26647

Mouratidis, H., Islam, S., Kalloniatis, C., & Gritzalis, S. (2013). A framework to support selection of cloud providers based on security and privacy requirements. *Journal of Systems and Software*, *86*(9), 2276–2293. doi:10.1016/j.jss.2013.03.011

Nahar, N., Huda, N., & Tepandi, J. (2012). Critical Risk Factors in Business Model and IS Innovations of a Cloud-based Gaming Company: Case Evidence from Scandinavia. In *Technology Management for Emerging Technologies*. PICMET.

NIST. (2011). US Government Cloud Computing Technology Roadmap (Vol. II, Release 1.0).

Office 365. (2014). Security in Office 365 White Paper. Retrieved from http://www.microsoft.com/engb/download/details.aspx?id=26552

Pearson, S. (2009), Taking account of privacy when designing cloud computing services. *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*. doi:10.1109/CLOUD.2009.5071532

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. *Proceedings of the 16th ACM conference on Compute and communications security CCS '09*, New York, NY, USA (pp. 199–212).ACM. doi:10.1145/1653662.1653687

Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013, May). Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering*, *39*(1), 47–54. doi:10.1016/j.compeleceng.2012.04.015

Ryan M. D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. JSS 86, 9 2263–2268.

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, *1*(1), 2008. doi:10.1504/IJSSCI.2008.017590

Samad, S., Loke, W., & Reed, K. (2013). Quantitative Risk Analysis for Mobile Cloud Computing: a Preliminary Approach and a Health Application Case Study. *Proceedings of the12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* doi:10.1109/TrustCom.2013.166

Saripalli, P., & Walters, B. (2010). Quirc: A quantitative impact and risk assessment framework for cloud security. *Proceedings of the2010IEEE 3rd International Conference onCloud Computing (CLOUD)* (pp. 280–288). doi:10.1109/CLOUD.2010.22

Savola, R. M. (2010). Towards a Risk-Driven Methodology for Privacy Metrics Development. *Proceeding of IEEE Second International Conference on Social Computing (SocialCom)* doi:10.1109/SocialCom.2010.161

Schmidt, R. (1997). Managing Delphi Surveys Using Nonparametric Statistical Techniques. *Decision Sciences*, *28*(3), 763–774. doi:10.1111/j.1540-5915.1997.tb01330.x

Sriram, I., & Khajeh-Hosseini, A. (2010). Research Agenda in Cloud Technologies. *Proceedings of the1st ACM Symposium on Cloud Computing (SOCC 2010)*.

Theoharidou, M., Papanikolaou, N., Pearson, S., & Gritzalis, D. (2013). Privacy Risk, Security, Accountability in the Cloud. *Proceedings of the IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom).*

Vimercati, S. De Capitani di. Foresti, S., Jajodia, S. Paraboschi, S., & Samarati, P. (2007, September). Over-encryption: Management of access control evolution on outsourced data. *Proc. Of Proceedings of the 33rd international conference on Very large data bases*, Vienna, Austria.

Yanosky, R. (2008). From Users to Choosers: The Cloud and the Changing Shape of Enterprise Authority. In R. N. Katz (Ed.), *The Tower and the Cloud* (pp. 126–136). Educase.

Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010). Information security risk management framework for the cloud computing environments. *Proceeding of IEEE 10th International Conference on Computer and Information Technology* (pp. 1328–1334). doi:10.1109/CIT.2010.501

Shareeful Islam is currently working at school of ACE, University of East London, UK. He received the PhD Technische Universität München, Germany. He received MSc in Information Communication System Security from Royal Institute of Technology (KTH), Sweden and MSc in CS and BSc (Hon's) in APE from the University of Dhaka, Bangladesh. He is a Fellow of the British Higher Education Academy (HEA). He has published more than 60 referred papers in high quality journals and international conferences. He participated in EU, industry, KTP projects. His research interest and expertise is risk management, requirements engineering, security, privacy, and cloud computing.

Stefan Fenz is a senior scientist at Vienna University of Technology, a key researcher at SBA Research and founder of Xylem Technologies GmbH. From 2012 to 2015, Stefan was an appointed member of the European Network and Information Security Agency's (ENISA) Permanent Stakeholder Group. In 2010, Stefan worked as a visiting scholar at Stanford Center for Biomedical Informatics Research at Stanford University (USA). From 2008 to 2012, Stefan lectured on information security at Peking University (Beijing, China), Beijing Jiaotong University (Beijing, China), Konkuk University (Seoul, Korea) and University of Applied Sciences Technikum Wien (Vienna, Austria). His primary research is on information security, with a secondary interest in semantic technologies and energy efficiency. Stefan received an MSc in software engineering & internet computing from Vienna University of Technology, an MSc in political science from University of Vienna, an MSc in business informatics from Vienna University of Technology, and a PhD in computer science from Vienna University of Technology. He is a member of the IFIP WG 11.1 – Information Security Management, the IEEE Systems, Man, and Cybernetics Society and ISC^2.

Edgar Weippl is Research Director of SBA Research and associate professor at TU Wien. After graduating with a PhD from the TU Wien, Edgar worked in a research startup for two years. He then spent one year teaching as an Assistant Professor at Beloit College, WI. From 2002 to 2004, while with the software vendor ISIS Papyrus, he worked as a consultant in New York, NY and Albany, NY, and in Frankfurt, Germany. In 2004 he joined the TU Wien and founded the research center SBA Research together with A Min Tjoa and Markus Klemen. Edgar is member of the editorial board of Computers & Security (COSE), organizes the ARES conference and is General Chair of SACMAT 2015, PC Chair of Esorics 2015 and General Chair of ACM CCS 2016.

Christos Kalloniatis is an Assistant Professor at the Department of Cultural Technology and Communication, University of the Aegean where he also serves as a member of Cultural Informatics Laboratory (CiLab). He received his PhD from the same department and holds an MSc from the Department of Computer Science, Univeristy of Essex. His research is focused on the design of secure and privacy-aware information systems and services both in traditional and cloud oriented environments. He has served as a program committee member in several International Conferences and as a reviewer in many International Journals. He is a member of Greek Computer Society.

Call for Articles

International Journal of Secure Software Engineering

Volume 7 • Issue 3 • July-September 2016 • ISSN: 1947-3036 • eISSN: 1947-3044
An official publication of the Information Resources Management Association

MISSION

The mission of the **International Journal of Secure Software Engineering (IJSSE)** is to provide a forum for software engineers and security experts to exchange innovative ideas in security-aware software systems and address security concerns in software development practices. This journal discusses methods and applications of systematic, quantifiable approaches to the development, operation, and maintenance of secure software systems. IJSSE addresses the problem of development duality between constructing a functional software system and constructing a secure system at the same time. Emphasizing security issues of software from a software engineering perspective, this journal promotes the idea that security issues must be an integral part in every phase of software development and advocates the development of security-aware software systems from the ground up. This journal facilitates promotion and understanding of the technical as well as managerial issues related to secure software systems and their development practices. Targeting researchers, academicians, software engineers, and field experts, this journal presents cutting-edge industry solutions in software engineering and security research.

COVERAGE AND MAJOR TOPICS

The topics of interest in this journal include, but are not limited to:

Aspect-oriented software development for secure software • Build security in (BSI) • Dependable systems • Experience related to secure software systems • Global security systems • Maintenance and evolution of security properties • Metrics and measurement of security properties • Process of building secure software • Programming security • Relationships between security and other quality concerns • Secure deployment of software applications • Security artifacts, evolution, and documentations • Security assurances, standards, and policies • Security audit and control • Security composition in component and service based software • Security in software architecture and design • Security literacy and education • Security patterns • Security requirement engineering • Security testing and validation • Static and dynamic analysis for security

ALL INQUIRIES REGARDING IJSSE SHOULD BE DIRECTED TO THE ATTENTION OF:

Khaled M. Khan, Editor-in-Chief • IJSSE@igi-global.com

ALL MANUSCRIPT SUBMISSIONS TO IJSSE SHOULD BE SENT THROUGH THE ONLINE SUBMISSION SYSTEM:

http://www.igi-global.com/authorseditors/titlesubmission/newproject.aspx

IDEAS FOR SPECIAL THEME ISSUES MAY BE SUBMITTED TO THE EDITOR(S)-IN-CHIEF

PLEASE RECOMMEND THIS PUBLICATION TO YOUR LIBRARIAN

For a convenient easy-to-use library recommendation form, please visit:
http://www.igi-global.com/IJSSE