A Comparison Study of Information Security Risk Management Frameworks in Cloud Computing

Mohammed Alnuem
Information Systems Department
King Saud University
Riyadh, Saudi Arabia
Email: malnuem@ksu.edu.sa

Hala Alrumaih, Halah Al-Alshaikh
Information Systems Department
Al Imam Mohammad Ibn Saud Islamic University
Riyadh, Saudi Arabia
Emails: {hala.alrumaih, halah.al-alsheikh}
@ccis.imamu.edu.sa

***Abstract*—Nowadays, cloud computing is an emerging concept in the Information Technology (IT) industry. Cloud computing is not a new technology, but is a new way of using or delivering resources. It also enhances the efficiency of computation by providing centralized databases, memory processing and on demand network access. Consequently, cloud computing has become an important platform for companies to build their infrastructures upon. It allows organizations to use Internet-based services so that they can reduce start-up costs, lower capital expenditures, use services on a pay-as-you-use basis, access applications only as needed, and quickly reduce or increase capacities. If companies are thinking of taking advantage of cloud-based systems, they will have to seriously re-assess their information security risk management strategies. In recent years, numerous risk management frameworks based on information security have been proposed to manage the risk of cloud computing. This paper discusses how information security risk management is related to the cloud computing environment. It also presents seven different information security risk management frameworks that cover all of cloud service models and deployment models. These frameworks are classified according to coverage area of the framework. Moreover, the paper sheds light on some suggestions that may help cloud users. These suggestions are related to information security risk management in cloud computing and were obtained through a comparison made in this paper between the presented frameworks.**

Keywords-Cloud Computing; Risk Management Framework; Information Security.

I. INTRODUCTION

Recently, cloud computing has gained extensive attention, but the trust and security issues of cloud computing have prevented businesses from fully accepting cloud platforms. The security risks are associated with each cloud delivery model, cloud architecture and security controls involved in a particular cloud environment [1]. One security assessment tool that can reduce the threats and vulnerabilities and mitigates security risks is a risk management framework [2].

Conducting information security risk management is the core element of an Information Security Management System (ISMS). ISO 27001 is the international best practice standard for ISMS [3]. ISO/IEC 27000 provides policies, standards, guidelines and procedures for initiating, implementing, maintaining and improving information security management within an organization [4]. An information security policy consists of roles, responsibilities and defining the scope of information that must be protected across the cloud [5]. Standards ensure security consistency across the cloud and usually contain security controls relating to the implementation [5]. Guidelines consist of recommended, non-mandatory controls that help and support standards. Procedures consist of step-by-step instructions to assist workers in implementing the various policies, standards and guidelines [5]. Risk management frameworks can be based on one or more of the ISO 27001 information security framework requirements.

This paper focuses on presenting some information risk management frameworks for better understanding the critical areas in the cloud computing environment. The rest of the paper is structured as follows: Section 2 presents an overview of cloud computing. Section 3 introduces information security risk management features. Section 4 reviews seven different information security risk management frameworks for cloud. Section 5 shows a comparison between the risk management frameworks, while Section 6 concludes this study. while Section 6 concludes this study.

II. OVERVIEW OF THE CLOUD AND ITS FEATURES

Cloud computing moves the tasks and the resources from a local computer onto the larger computing center, which is shared among a large number of users and distributed on the Internet. The cloud system resource is transparent, as neither the application nor the user knows the location of the resource. Cloud resources are provided as a service on an as needed basis. Moreover, the user can decide to only pay for what they use [6]. Cloud computing include five key characteristics of on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service [7]. According to Buyya et al. [8] the cloud computing has the following definition "Cloud is a parallel and distributed computing system consisting of a collection of inter-connected and virtualized computers that are dynamically

 ISBN: 978-1-61208-388-9

provisioned and presented as one or more unified computing resources based on Service-Level Agreements (SLA) established through negotiation between the service provider and consumers [8]." Vaquero et al. stated that "clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services) [9]", where the resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. There are three cloud delivery models, as follows: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [6][7].

- *Infrastructure as a Service (IaaS):* Providing a working environment as per user wish and demand without manages or controls the infrastructure they simply control the storage and applications. One IaaS example is Amazon Elastic Compute Cloud (EC2).
- *Software as a Service (SaaS):* Cloud providers offer application software as on-demand services.. Examples of SaaS are Flickr, Google Docs, Siri, Amazon and Cloud Drive.
- *Platform as a Service (PaaS):* Provides infrastructure where you can create new applications. Consumer deploys their applications on the cloud computing system and controls their applications but they do not manage servers and storage. Examples of PaaS are Google App Engine, Amazon Web services.

Cloud computing is further divided into private cloud, public cloud and hybrid cloud, according to the different deployment models [6][7].

- *Private Cloud:* Private cloud is deployed for a particular organization and security can be created easily. Private clouds are virtualized cloud data centers inside a firewall. Private cloud refers to internal data centers of a business or other organization not made available to the general public.
- *Public Cloud:* Public cloud runs on the Internet and security is very complex. Public clouds are virtualized data centers outside of the firewall and resources are available to the consumer on demand over the public Internet.
- *Hybrid Cloud:* Hybrid cloud is a composition of two or more clouds and that are bounded by standard or proprietary technology. Hybrid clouds combine the character of both public and private clouds.

A new type of cloud deployment models offers Cloud Computing resources and services to mobile devices called Mobile Cloud Computing. Khan et al. defined mobile cloud computing as "an integration of cloud computing technology with mobile devices to make the mobile devices resource-full in terms of computational power, memory, storage, energy, and context awareness [10]".

However, in cloud computing the security situation is very different as the hardware, software and application data can be deployed and stored by the cloud providers. Therefore, to solve security problems that are occur in cloud computing there are some risk management frameworks can be used to secure the data transmitted, ensure the integrity of the applications and increase trust between users and service providers, etc. [11].

III. INFORMATION SECURITY RISK MANAGEMENT

Recently, cloud computing has gained considerable attention. Due to the involvement of many technologies including networks, databases, operating systems, resource scheduling, transaction management, concurrency control and memory management, various security issues have been highlighted as arising in cloud computing [12]. Indeed, security remains a major roadblock for organizations looking to reap the cost and efficiency benefits of the cloud. Table I summarizes cloud computing features and their corresponding security implications [13].

TABLE I. SECURITY IMPLICATIONS OF CLOUD FEATURES

Feature	Security Implication
Outsourcing	Users may lose control of their data. Cloud providers may use customers' data in a way that has not been agreed upon in the past.
Extensibility and Shared Responsibility	There is a tradeoff between extensibility and security responsibility for customers in different delivery models.
Virtualization	There needs to be mechanisms to ensure strong isolation, mediated sharing and communications between virtual machines.
Multi-tenancy	Issues like access policies, application deployment, and data access and protection should be taken into account to provide a secure multi-tenant environment.
Service Level Agreement	The main goal is to create a negotiation mechanism for the contract between providers and consumers of services.
Heterogeneity	Different cloud providers may have different approaches to providing security and privacy mechanisms. This will generate integration challenges.

As more organizations start to move their IT operations to the cloud, risk management remains a top concern. Risk management is the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analyzing, evaluating, treating, monitoring and communicating risk. It allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability

 ISBN: 978-1-61208-388-9

by protecting the IT systems and data that support their organizations' missions. Risk management encompasses three processes: risk assessment, risk mitigation and risk evaluation [14].

Risk assessment is the determination of a quantitative or qualitative output from risk analysis process [2]. It has four major processes. Likelihood determination process indicates the probability vulnerability that may be exercised within the construct of the associated environment. Impact analysis process determines the adverse impact resulting from a successful threat exercise of vulnerability. Risk determination process finds the risks and opportunities that impact on the associated environment using risk exposure formula and matrix. Control recommendations process provides the process and recommend controls that could mitigate or eliminate the identified risks. Risk mitigation refers to prioritizing, implementing and maintaining the appropriate risk-reducing measures recommended from the risk assessment process [14]. Cloud provider must develop Risk Treatment Plans (RTP) with multiple options (avoidance, transfer, retention, reduction and acceptance) [2]. The outcomes of RTP should be incorporated into service agreements because different models of cloud computing have various ways to mitigate vulnerabilities and threats. Risk evaluation is a continual process for implementing a successful risk management program [14]. It initiates specific follow-on actions as part of a comprehensive continuous monitoring program.

Well-planned risk management activities will be crucial in ensuring that information is simultaneously available and protected [15]. A well-structured risk management framework, when used effectively, can help management identify appropriate controls for providing the essential security capabilities to protect users' information, which is of high importance.

IV. INFORMATION SECURITY RISK MANAGEMENT FRAMEWORKS IN CLOUD

This section provides a review of seven different information security risk management frameworks for cloud computing which can be used to secure the data transmitted, ensure the integrity of the applications and increase trust between users and service providers. The information security risk management frameworks in this study have been classified according to the coverage area of the framework, and fall into the following: information security risk management frameworks for security evaluation in cloud environments, analyzing the risks in cloud environments and frameworks based on security policies.

A. Cloud Environments Security Evaluation Frameworks

Zhang et al. [2] have presented an information risk management framework for better understanding critical areas of focus in the cloud computing environment, to identify a threat and vulnerability by means of Deming Cycle. It is covers all of cloud service models and deployment models. The framework has seven processes, including: selecting relevant critical areas, and strategy and planning under the architecting and establishing the risk management program (PLAN) phase. Risk analysis, risk assessment and risk mitigation under the implement and operate (Do) phase, and then the assessing and monitoring program, and risk management review under the monitoring and review (Check, Act) phase. In selecting relevant critical area process, the authors enumerated twelve domains as areas of concern for cloud computing. At least one critical area that is relevant has to be selected before moving to the next process. The strategy and planning process is performed in collaboration with selecting relevant critical area to ensure plans effectively identify critical areas of focus and provide management with clear choices for resource allocation and optimization. Risk analysis process allows management to examine all currently identified threat and vulnerability concerns. Risk assessment is the following step that has four major processes–likelihood determinations, impact analysis, risk determination and control recommendations. Cloud providers must develop (RTP) with multiple options (avoidance, transfer, retention, reduction and acceptance) through risk mitigation process. The organization subsequently initiates specific follow-on actions as part of a comprehensive continuous monitoring program. Finally, a review is performed to develop a program effectiveness grid that is can be used first to establish a baseline, then set goals and objectives and evaluates progress.

However, the framework of Xie et al. in [11] pays more attention to how to increase the trust between users and service providers. This framework is composed of five basic processes: user requirement self-assessment, cloud service providers desktop assessment, risk assessment, third-party agencies' review and continuous monitoring [11]. At the user requirement self-assessment phase, the user should determine the required cloud computing model and security level. In the desktop assessment, the historical security status should be analyzed as should the potential risk of cloud service providers. The risk assessment of cloud provider includes seven stages: the preparation of risk assessment, asset identification, threat identification, vulnerability identification, existing security measures, risk analysis and risk assessment documentation. The third-party agencies review stage it is necessary to employ third-party agencies to review the procedure and to ensure security of cloud services. Through the previous stages, there is a need for a continuous monitoring process to monitor the ongoing risk assessment [11].

Popa et al. [16] explained the security issues related to private data and mobile cloud applications in detail. They proposed a mobile computing applications security framework called Secure Mobile-Cloud (SMC). It had to fulfill the following features: to make sure that the security of data is achieved when it is transmitted between the components of the same mobile application, also it had to verify the integrity of the applications either at the time of installation or updating on the mobile device. This solution takes into consideration the following constraints: mobile device energy, data sensitivity and users' options. The proposed framework best fits into SaaS layer of the cloud service delivery model by providing security services such

as confidentiality and integrity. SMC framework has several components running in the cloud and on the mobile. There are five kinds of managers: Mobile Manager, Mobile and Cloud Security Manager, Optimization Manager, Application Manager and Policy Manager, where each manager has a well-defined functionality. The framework also contains also the security components deployed on both cloud and mobile devices.

B. Cloud Environments Security Analysis Frameworks

Tanimoto et al. [17] identified various risk factors from a user's viewpoint by using the Risk Breakdown Structure (RBS) method. The risk analysis method is based on a risk matrix. Tanimoto et al. proposed a risk management framework that classified the risks into risk transference, risk mitigation, risk acceptance and risk avoidance, then categorized the problems in cloud computing according to these four classifications. Since risk transference problems tend to come from the cloud service provider, risks classified into risk mitigation tend to involve regulatory compliance of the cloud service provider, such as specification, authentication, etc. Risks in risk acceptance tend to be based on external factors, such as laws, while the risks in risk avoidance tend to be caused by different specifications of the cloud service provider and users [17].

Alhomidi and Reed [18] presented a resource independent framework for security risk analysis as a service (SRAaaS) suitable for IaaS model of cloud computing. The results of the analysis recommend a range of plans that can be used directly by cloud users to enforce the protection of their Virtual Machines (VMs), as the fundamental unit of IaaS, against possible attacks. The resource independence allows the SRAaaS to scan any kind of resources in the IaaS cloud so the framework can be extended to provide analysis for other types of IaaS resources, such as networks or storage. In addition, the framework reduces the need to consistently access the VMs or interrupt the processes and services running on each VM because time-consuming tasks in the risk analysis can be performed offline in the cloud. SRAaaS framework consists of seven steps [18] and only the first step has to be accomplished online while the further steps are performed offline. VM Vulnerability Scanning step aims to check all software and applications as well as the VM's connections and ports. Attack Graph Generation step visualizes how an attacker could exploit the VM by showing the attack paths generated using an attack graph generation tool. Risk Assessment Model step analyzes the produced attack graph by computing the most likely attacks, the highest-risk attacks and the highest loss attack. Security Control Selection step aims to help cloud users or providers with the selecting suitable and cheapest security controls that protect the VM from threats. Genetic Algorithm Optimization step simplifies the full attack graph to a smaller graph representing the most critical attack path. Analysis Results step describes potential vulnerability threats so the cloud user has an overall view of the existing security risks. Finally, Security Recommendations step reports a group of recommendations for the cloud user to make appropriate decisions regarding the security of the VM, including a list of required security controls and the total cost of the security controls as well as the cost of each control.

C. Frameworks Based on Security Policies

SecureCloud has been proposed by Takabi et al. [7]. It is a comprehensive security framework for cloud computing environments that preserves cloud security using identity management models and access control models. The framework consists of various modules to handle security and trust issues of cloud computing environments. The modules deal with issues such as access control to provide the security and privacy specification and enforcement functionality, policy integration among multiple clouds to integrate access policies of different policy domains and define global access policies, secure service that is responsible for secure service discovery, composition and provisioning. In addition, these modules cover issues like trust management, which is responsible for negotiation, establishment, and evolution of bidirectional trust between different clouds and between a cloud and its users, semantic heterogeneity to check the correctness of the integrated policies among policies from different clouds and identity management which is responsible for authenticating users and services based on credentials and characteristics.

Zhao [4] introduced a risk management framework based on aligning policies relating to organization's IT policies and standards and security management to fit with the cloud computing model. The security solutions provider may need some standards and guidelines to evaluate the cloud service provider against regulatory requirements. Some of the standards, frameworks and guidelines such as ITIL, Statement on Auditing Standards (SAS), ISO/IEC 27000 standard series, Control Objectives for Information and Technology (COBIT) framework, Data Security Standard (PCI DSS), Cloud Security Alliance Cloud Controls Matrix (CCM) and others. This framework found that to build a model of security management in any cloud service provider, it is necessary to start by identifying the asset for the cloud deployment then evaluating the risk for the asset [4].

V. DISCUSSION

In this section, the previous information security risk management frameworks are compared according to the ISO 27001 framework, and the classification that was presented previously in this study.

The comparison based on different indications such as cloud service models, deployment, framework concentration, and determine which ISO 27001 requirements the framework based on.

A. Cloud Environments Security Evaluation Frameworks

By examining the prior cloud environments security evaluation frameworks, it is clear that the frameworks of Zhang et al. [2] and Xie et al. [11] focus on user perspectives to evaluate cloud environment security. The two frameworks can fit on all of cloud service models and deployment models. Both frameworks concentrate on

 ISBN: 978-1-61208-388-9

denoting where the user should specify the process information of the cloud computing service, and determining the necessary cloud computing model as well as security level, at the first stage in the their frameworks. In Xie et al.'s framework, before assessing the risk of service provider, users have to evaluate cloud service providers' plans, analyze the historical security status and, furthermore, acquire the potential risk of the cloud service providers. The risk assessment in the framework of Zhang et al. has two processes, risk analysis and risk assessment to identify the threats and vulnerabilities then determine the likelihood that a potential vulnerability could be applied and its impact. In addition both frameworks have monitoring process. As part of assessing cloud provider, specific follow-on actions are initiated for a continuous monitoring program of effectiveness after the RTPs are implemented. According to the framework requirements in ISO 27001, both frameworks implement information security management based on procedures. Moreover, the Zhang et al. framework was developed in a standard quality management (PDCA) cycle of continuous improvement, based on evolving standards of ISO 27001. The other framework that evaluates cloud environment security works on a mobile cloud application called Secure Mobile-Cloud (SMC) [16]. This framework fits in the SaaS layer only. SMC framework aims to secure data communication between the same application components. In SMC framework, there are five different kinds of managers and security components on the mobile side and cloud side. All of these managers have their own functions to analyze and evaluate risks. This framework is also based on procedures according to the framework requirements in ISO 27001.

B. Cloud Environments Security Analysis Frameworks

Regarding the presented cloud environment security analysis frameworks, both Tanimoto et al. [17] and Alhomidi and Reed [18] found that cloud computing security has not been sufficiently investigated, although cloud computing services have. As a result, they developed a number of frameworks capable of analyzing the security risks and extracting of risk factor in the cloud computing environment. In [17], the authors analyzed and extracted risks of utilizing cloud computing by using the Risk Breakdown Structure (RBS) method. RBS is a typical risk Aanalysis method of the project management method. Meanwhile, SRAaaS framework [18] provided a mechanism for risk analysis using attack graph, which is an important tools used to present the relationships between vulnerabilities. Furthermore, Tanimoto et al. started the analysis process by identifying various risk factors from a user's viewpoint, then classified risks using risk matrix method that classified risks into four kinds risk avoidance, risk mitigation, risk acceptance, and risk transference. Finally, it developed countermeasures individually to satisfy extracted risks and then detailed the risk management proposals for each classification. On the contrary, SRAaaS framework, which is suitable for IaaS model of cloud computing, consists of seven steps. It starts with vulnerability scanning step to check all software and applications, as well as connections and ports. Then it ends with the security recommendations step that reports a group of recommendations for the cloud user in order to make appropriate decisions regarding the security; this includes a list of required security controls and the total cost of the security controls as well as the cost of each control. The framework in [17] is based on procedures according to the framework requirements in ISO 27001. Alternatively, SRAaaS framework recommends a range of guidelines that can be used by cloud users to enforce the protection of their services and systems against possible attacks, according to the framework requirements in ISO 27001.

C. Frameworks Based on Security Policies

Looking into the introduced frameworks that are based on security policies, Takabi et al. [7] and Zhao [4] evolved frameworks based on aligning various policies and standards relating to information security risk management frameworks, in order to fit with the cloud computing model. SecureCloud framework [7] was built based on the existing research on multi-domain policy integration and the secure service composition. The framework consists of various modules to handle the security and trust issues of cloud computing environments. The important module in SecureCloud framework is policy integration in the cloud that should be able to address challenges such as semantic heterogeneity, secure interoperability and policy evolution management. On the other hand, Zhao's framework supports standards aligning of one cloud service provider. It found that the building of a model of security management in any cloud service provider starts with identifying the asset for the cloud deployment then evaluating risk for the asset. Accordingly, both frameworks are based on policies according to the framework requirements in ISO 27001.

The following Table II represents a summary of the comparison of the previous information security risk management frameworks:

 ISBN: 978-1-61208-388-9

TABLE II. SUMMARY OF THE COMPARISON BETWEEN SOME INFORMATION SECURITY RISK MANAGEMENT FRAMEWORKS

Criteria / Framework Name	Coverage area	Cloud service and deployment models	Concentration	Framework Requirements in ISO 27001
Zhang et al. [2]	Cloud Environments Security Evaluation	Fit in all of cloud service and deployment models	Identify the threats and vulnerabilities and its impact of using the cloud.	Based on procedures and standard
Xie et al. [11]	Cloud Environments Security Evaluation	Fit in all of cloud service and deployment models	Users have to evaluate cloud service providers' plans, analyze the historical security status and, acquire the potential risk of the cloud service providers.	Based on procedures
SMC framework[16]	Cloud Environments Security Evaluation	Fits in the saas layer	Have five different kinds of managers and security components on the mobile side and cloud side.	Based on procedures
Tanimoto et al. [17]	cloud environment security analysis	Fit in all of cloud service, deployment models	Analyzed and extracted risks of utilizing cloud computing by using the Risk Breakdown Structure (RBS) method. And using risk matrix method that classified risks into four kinds of risks.	Based on procedures
Alhomidi and Reed [18]	cloud environment security analysis	Fits in iaas model.	Provided a mechanism for risk analysis using attack graph to present the relationships between vulnerabilities.	Based on guidelines.
Takabi et al. [7]	Based on Security Policies	Fit in all of cloud service, deployment models	Handle the security and trust issues of cloud computing environments by using various modules.	Based on policies.
Zhao [4]	Based on Security Policies	Fit in all of cloud service, deployment models	Identifying the asset for the cloud deployment then evaluating risk for the asset.	Based on policies.

VI. RESULT

After reviewing seven information security risk management frameworks, this study makes some suggestions related to information security risk management in cloud computing. The organizations that have decided to move to cloud computing have to define the benefits and risks of cloud computing and implement processes to manage security risk. The information security risk management policies should comply with an organization's IT policies and standards to protect the confidentiality, integrity and availability of information security. The study observes some of the main processes that are needed to manage security risks. The first step in risk management is

 ISBN: 978-1-61208-388-9

assessment of the cloud service provider to evaluate the cloud service plans and analyze the historical security status. The second step entails a risk analysis of cloud provider by identifying the assets, threats and vulnerabilities. Risk assessment is the third process in the implementation of risk management. Risk assessment means assessing security incidents from two dimensions, i.e., the likelihood and the adverse impact of an incident. After the risk management plans are implemented, there is a need for follow-on actions as part of a comprehensive assessment and continuous monitoring program for effectiveness. Moreover, the study acquires different recommendations that may help cloud providers and customers with choosing between the existing information security risk frameworks. It is important to specifying the cloud service models and deployment models, the purpose of the framework, and whether there is a need for one or more cloud environments/providers. Moreover, there is a need to specify the framework requirements based on the basic framework requirements in ISO 27001: policies, standards, guidelines and procedures.

VII. CONCLUSION

Cloud computing has the advantages of high efficiency and low costs, as well as scalability. As the march of cloud computing continues, security issues have appeared. Indeed, the investigations in the cloud computing environment have mainly focused on the service side, while the security side has not been sufficiently looked at. This study presented and compared seven different information security risk management frameworks that covered all of cloud service models and deployment models. The comparison was undertaken according to the framework requirements in ISO 27001 and the coverage area of the frameworks that were presented in this study. Moreover, the paper sheds light on some suggestions related to the information security risk management in cloud computing.

REFERENCES

[1] CPNI Centre for the Protection of National Infrastructure, "Information Security Briefing 01/2010 Cloud Computing," pp. 36, March 2010.

[2] X. Zhang, N. Wuwong, H. Li, and X. Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments," 2010, pp. 1328–1334.

[3] ISO/IEC 27001 - Information security management, retrieved from: http://www.iso.org/ accessed in 4/5/2014

[4] G. Zhao, "Holistic framework of security management for cloud service providers," in *Industrial Informatics (INDIN), 2012 10th IEEE International Conference on*, 2012, pp. 852–856.

[5] P. Johnson, "What are Policies, Standards, Guidelines and Procedures? | MindfulSecurity.com – The Information Security Awareness Resource." accessed in 20/4/2014

[6] W. Liu, "Research on cloud computing security problem and strategy," in *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on*, 2012, pp. 1216–1219.

[7] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual , pp. 393–398.

[8] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, no. 6, Jun. 2009, pp. 599–616.

[9] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, 2009, pp. 50–55.

[10] A. U. R. Khan, M. Othman, S. A. Madani, and S. U. Khan, "A Survey of Mobile Cloud Computing Application Models," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, 2014, pp. 393–413.

[11] F. Xie, Y. Peng, W. Zhao, D. Chen, X. Wang, and X. Huo, "A risk management framework for cloud computing," in *Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on*, 2012, vol. 1, pp. 476–480.

[12] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, "Security Issues for Cloud Computing:," *International Journal of Information Security and Privacy*, vol. 4, no. 2, 2010, pp. 36–48.

[13] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," Security & Privacy, IEEE Nov.-Dec. 2010, vol.8, no.6, pp.24,31.

[14] S. R. Vallabhaneni, *Corporate Management, Governance, and Ethics Best Practices*. John Wiley & Sons, 2008.

[15] ISACA, "Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives," An ISACA Emerging Technology White Paper, pp 7.

[16] D. Popa, M. Cremene, M. Borda, and K. Boudaoud, "A security framework for mobile cloud applications," in *Roedunet International Conference (RoEduNet), 2013 11th*, 2013, pp. 1–4.

[17] S. Tanimoto, M. Hiramoto, M. Iwashita, H. Sato, and A. Kanai, "Risk Management on the Security Problem in Cloud Computing," in Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference, pp.147,152.

[18] M. A. Alhomidi and M. J. Reed, "Security risk analysis as a service," in *Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for*, 2013, pp. 156–161.

 ISBN: 978-1-61208-388-9