CIRA as a Cloud Service

Vivek Agrawal

February 18, 2014

Contents

Chapter 1

ABSTRACT

Cloud computing has emerged as a growing trend because it serves as an enabler of scalable, flexible and powerful computing. While cloud computing promises efficient infrastructure at a fraction of the cost compared to traditional environments, two primary issues must be considered while offering risk management support as a cloud service i.e. compliance and security for data residing in the cloud. In case of providing a risk analysis tool as a cloud service, a malicious insider can share sensitive information on a public portal or data can be leaked accidentally. Insecure Application Programming Interfaces can also affect the security and operation of cloud service. Therefore, privacy and data protection related issues are raised in this context. It is therefore important to know where the information is and who has access to it and the necessity of proper tools to protect the information. The idea of this research is to understand and exploit benefits of CIRA as a cloud service and to investigate security and privacy related issues of a typical cloud service in the context of CIRA and provide necessary theoretical and practical solution to mitigate it. The artifacts will be constructed and evaluated based on the Design Science Research (DSR) approach.

Chapter 2

Introduction

2.1 Background (< 1/2 p)

Risk Analysis is an integral part of any business activity. It helps to identify and manage potential problems that could undermine key business initiatives or projects [1]. Risk is often made up of two things:

1. The probability of something going wrong.
2. The negative consequences that will happen if it does.

Risk analysis/assessment answers: are there any risks that require some kind of action by the individual exposed to the risk? Risk management is about implementing the necessary action to ensure that unacceptable risks are mitigated. There are basically two types of risk analysis methods. Quantitative risk analysis methods are based on mathematical and statistical tools to assess risk [2]. These methods usually rely on objective/subjective incident data and in the absence of sufficient statistical data they generally fail. In qualitative risk analysis methods, risk is analyzed with the help of adjectives instead of using mathematics. Information security risk analysis is shifting now a days towards qualitative risk analysis methods as quantitative methods are not suitable for the complicated and widespread nature of today's information systems. TUAR [3] is a well known quantitative tool which uses fault trees and fuzzy logic to assess the risk. RaMEX [4] does not use any mathematical or statistical method, hence it is a qualitative tool. Similarly, researchers suggested a new method of Risk analysis based on the idea of qualitative method.[5]. This method is known as CIRA- Conflicting Incentives Risk Analysis. The main aim of CIRA is to understand Human risks in the system. This risk can be intentional as well as unintentional. CIRA considers stakeholders incentives and motivation whereas Risk analysis gives priority to Incident probability.

2.2 Problem Statement (3 lines + 5 lines)

Risk analysis and management seems to be an obscure activity of any organization as there are very few case studies available on public portal. Risk analysis methods may be supported and executed by means of software [6] or by paper-based method [7]. Software based solution is costly in nature and hence it is being avoided in many companies. On the contrary, paper-based method is usually a time consuming process as it includes meetings, discussions and working sheets. Risk analysis can be a very difficult and costly process with dubious accuracy. Alberts and Dorofee [8] mentioned that it is usually not possible to address all the organizational risks through risk analysis methods. Funding, number of staff, and schedule constraints limit how many and to what extent risks can be addressed. There is a need to improve the risk analysis processes both in terms of quality and cost effectiveness.

CIRA is a new and promising method for risk analysis [5]. There is a need to enhance CIRA such that it can be offered as a secure cloud service, taking advantage of efficiency and effectiveness opportunities (from an analyst perspective) that cloud deployment offers. Cloud deployment will result in the exploration of various new useful features in CIRA. The idea of this research work is to investigate the benefits of implementing CIRA services in cloud while addressing security and privacy relates issues. The benefits of CIRA functionality can be exploited in a proper way if it can be provided as cloud service as it can make it scalable, available, less need of maintenance and expert service. In cloud computing, users access the data, applications or any other services with the help of a browser regardless of the device used and the user's location. Maintenance is easier in case of cloud computing applications as they need not be installed on each user's computer. Pay per use facility allows measuring the usage of application per client on regular bases [9]

2.3 Motivation (<1/2 pages)

Currently cloud providers of all shapes and sizes are in a race to move as many products and services as possible to the cloud providing managed services and software-as-a-service rather than traditional, locally-installed, software applications. Cloud delivers highly scalable distributed computing platforms in which computational resources are offered as a services (Software as a service, SaaS) such as Gmail and Google docs, underlying platform (Platform as a service, PaaS) such as Microsoft Azure, and underlying Infrastructure (infrastructure as a service, IaaS) such as Amazon Elastic Compute Cloud (EC2) [10]. Amazon EC2 played an important role in the development of cloud computing. They have upgraded their data center in order to support and provide latest cloud solution to the clients. IaaS service of Amazon EC2 provides user to allocate entire virtual machine on demand. Google app engine provides a language specific APIs and libraries which allow user to use computational power, and storage capacity. In addition, Intel Tashi, IBM BlueCloud, Microsoft Azure and EMC Daoli explore the cloud computing technology in resource management, service application and security [11]. Zhang et al. [11] mentioned about the utilization of computing resource and storage resource to dynamically provide on demand service for users. They focused on the distribution and parallel nature of cloud computing and used these feature in the railway freight system. They implemented a cloud computing based architecture for freight system application.

Cloud deployment has has in many cases proven to offer improved functionality and service quality together with reduced life cycle costs. Since high quality risk analysis can be a difficult, time consuming and costly task, it seems like a very good candidate for explorations into the possibility of harvesting the benefits from a 'cloudification' of both risk analysis concepts and support technologies.

2.4 Research Questions (1/2-1 p)

The following sub questions are formed to attain the research objective and answer the main research question.

1. **RQ1**: What are the quality and cost effectiveness improvement features of CIRA tool as a cloud delivery model?

   This study will identify the potential benefits of cloud implementation of CIRA method/tool. The findings of this study will be helpful to understand the feasibility and necessity of delivering CIRA support through a cloud delivery model.

2. **RQ2**: What are the security requirements of an information sharing tool?

   This study will help to understand the major security requirements which may be of interest to the user community when some kind of information sharing concept is to be supported.

3. **RQ3**: What kind of information sharing features can be of special interest for the participants?

   This investigation will allow to explore various information sharing features which have the potential to offer benefits to the participants. The findings of this study will be helpful to decide relevant information sharing features in the context of CIRA.

4. **RQ4**: How can the desired functionality be implemented without violating the security requirements?

   This question is related to RQ2 and RQ3 and it will be answered based on the findings of RQ2 and RQ3. This investigation will help us to identify potential information security schemes which can be useful to be applied.

5. **RQ5**: What are the benefits and shortcomings of the newly implemented features in the CIRA support tool?

   The idea of this study is to assess major benefits and drawbacks of the added features in the CIRA support tool. The result of this finding will be helpful to decide whether it is meaningful to add those features or not.

6. **RQ6**: What is impact of the security risks and shortcomings of the added feature on adoption of cloud computing?

   This investigation will explore the significance of security risks and shortcoming of the features.

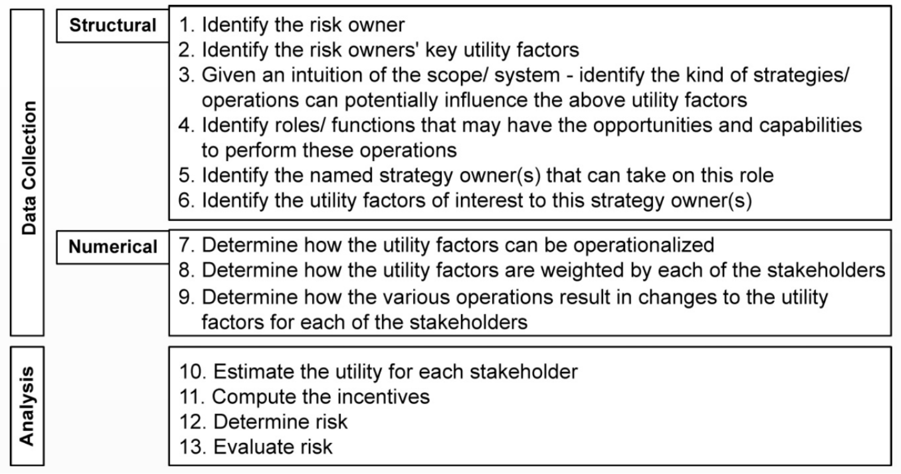
Chapter 3

Related Work (3-10 p)

3.1 Risk Analysis

Risk Analysis helps to identify and manage potential problems that could undermine the main business activity. Risk analysis is one step in the process of risk management. Risk analysis helps to assess potential risks in a system/organization so that by using the output of risk analysis, these organizations could define appropriate controls for reducing or eliminating those risks.

Rajbhandari and Snekkenes [5] have developed a new method for risk analysis and it is know as Conflicting Incentives Risk Analysis (CIRA) method. The main aim of CIRA is to understand Human risks in the system. CIRA expresses risk as “conflicting incentives” rather than as a “likelihood and consequence” pair. This risk can be intentional as well as unintentional. Almost all the risks can be analyzed in terms of Human behavior. CIRA identifies stakeholders, their actions and perceived expected consequences that characterize the risk situation. It categorizes the stakeholders into risk owner and strategy owner(s). The stakeholder, whose perspective is considered when performing the risk analysis, is a risk owner. On the other hand, a strategy owner is the stakeholder who is capable of triggering an action to increase his perceived benefit. CIRA considers stakeholders incentives and motivation whereas Risk analysis gives priority to Incident probability. An incentive motivates a stakeholder to take an action to increase his expected/ predicted utility. Utility is the benefit as perceived by the corresponding stakeholder and it comprises of utility factors. The steps in CIRA method is shown in Figure 3.1.



1. Identify the risk owner
2. Identify the risk owners' key utility factors
3. Given an intuition of the scope/ system - identify the kind of strategies/ operations can potentially influence the above utility factors
4. Identify roles/ functions that may have the opportunities and capabilities to perform these operations
5. Identify the named strategy owner(s) that can take on this role
6. Identify the utility factors of interest to this strategy owner(s)
7. Determine how the utility factors can be operationalized
8. Determine how the utility factors are weighted by each of the stakeholders
9. Determine how the various operations result in changes to the utility factors for each of the stakeholders
10. Estimate the utility for each stakeholder
11. Compute the incentives
12. Determine risk
13. Evaluate risk

Figure 3.1: Procedure in CIRA, based on [12]

3.2 Cloud Computing

This section is based on the published work of the scientists at the U.S. National Institute of Standards and Technology (NIST) [13].

Cloud computing can be defined as a model to provide ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [14]. It has the potential to increase collaboration, scalability, availability and agility. The main advantage of cloud computing is that it provides customers/users to pay per use facility [9]. Customers do not need to pay for the infrastructure, software, installation of different hardwares and maintenance. NIST defines cloud computing (see Figure 3.2) as an aggregation of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud) [13].

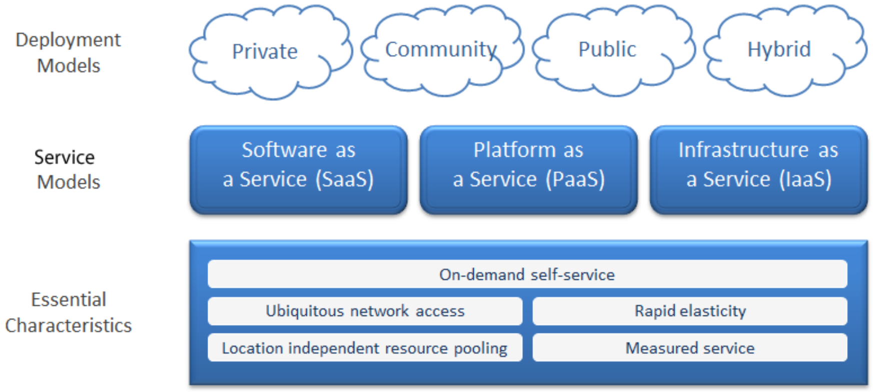

Deployment Models
Private
Community
Public
Hybrid
Service Models
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Essential Characteristics
On-demand self-service
Ubiquitous network access
Rapid elasticity
Location independent resource pooling
Measured service

Figure 3.2: NIST Visual Model of Cloud Computing Definition, based on [13]

3.2.1 Essential Characteristics

Cloud services possess five essential characteristics. These characteristics show how cloud computing is different from and related to traditional computing.

- **On-demand self-service -** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad network access -** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- **Resource pooling -** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- **Rapid elasticity -** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

- **Measured service -** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

3.2.2 Service Models

Cloud service delivery model is divided among three models. It is also known as SPI model where SPI refers to Software, Platform and Infrastructure respectively.

- **Software as a Service (SaaS) -** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Examples of multi tenant SaaS provision from cloud managed environments are Workday.com Inc and SalesForce.com Inc. Workday offersHR and Payroll software, whereas SalesForce.com offers Customer Relationship Management (CRM) software.

- **Platform as a Service (PaaS) -** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. Prominent examples of PaaS are Google AppEngine [15] and SalesForce.com's business software development's platform.

- **Infrastructure as a Service (IaaS) -** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). The most notable IaaS cloud offerings appear to be Amazon's e.g. Elastic Compute cloud (EC2) [10], GoGrid's cloud Hosting/ Storage [16].

3.3 Security and Privacy issues

The U.S. information technology research and consulting firm Gartner issued a report in 2008 [17]. This report was based on mainly from the vendor's point of view about security capabilities analyzed security risks faced by the cloud. Table 3.1 lists seven major security risks that are common in any cloud computing environment.

La'Quata Sumter [18] stated the wide adoption of cloud computing and its concerns related to Internet security. Consumers of cloud computing services have serious concern about the availability and accessibility of their data in the cloud. A mechanism is proposed to ensure the safety and security of data. This design helps to capture the movement and processing of the information kept on the cloud. The proposed mechanism is implemented in a small cloud computing environment. The major advantage of the research work is the assurance of security to cloud users but at the same time the proposed design is not feasible for large scale cloud computing environments.

Risk	Description
Privileged user access	Sensitive data processed outside the enterprise brings with it an inherent level of risk.
Regulatory compliance	Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider.
Data location	When you use the cloud, you probably won't know exactly where your data is hosted.
Data segregation	Data in the cloud is typically in a shared environment alongside data from other customers.
Recovery	Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure.
Investigative support	Investigating inappropriate or illegal activity may be impossible in cloud computing
Long-term viability	you must be sure your data will remain available even after such an event.

Table 3.1: Gartner: Seven cloud-computing security risks, based on [17]

Soren et al [19] stated that cloud computing has gained popularity in recent years but the benefits of clouds are shadowed by security and privacy challenges. These challenges are also affecting the adoption of cloud service in any company. Users can configure highly flexible cloud computing environment through a web services interface. However, misconfiguration of any cloud service can impose severe vulnerability in the system. Authors presented a novel approach for analyzing security at end user configuration. Amazon Elastic compute cloud (EC2) is selected for the security assessment. The focus of the assessment is on the reachability and vulnerability of services in cloud infrastructure. A query and policy language is also proposed in this paper for the analysis. It can be used to understand necessary and unnecessary configuration. This approach enables to remediate common security concerns through validation of configurations of complex cloud infrastructures. The major benefit of this approach is that it provides analysis of vulnerability and security issues. This analysis is helpful for the vendors as they can improve their security policies based on the analysis. The potential drawback of this scheme is its limitation to Amazon [20].

Flavi and Roberto [21] reported that clouds environments are becoming prominent targets for attackers. This paper discusses the integrity problem in the clouds and propsed a new architecture to increase security of cloud resources. They named it as Transparent Cloud Protection System (TCPS). The main idea of TCPS system is that it can be customized to different cloud environments to monitor the integrity of guests and infrastructure components while remaining transparent to virtual machines. The proposed tool improves security, transparency and intrusion detection mechanism. The major drawback of their work is that the proposed tool is not deployed or tested in any cloud computing scenario.

Chapter 4

Research Methodology (2 - 4p)

According to [22], there are two distinct paradigm to acquire knowledge in Information System viz. behavioral science and design science. Behavioral science paradigm is based on natural science research methods. It seeks to develop and justify theories that explain human-organizational interaction phenomenon surrounding the analysis, design, implementation, management, and use of information systems. On the other hand, Design science is fundamentally a problem- solving paradigm and based on engineering. It seeks to create innovations that define the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, management, and use of information systems can be effectively and efficiently accomplished.

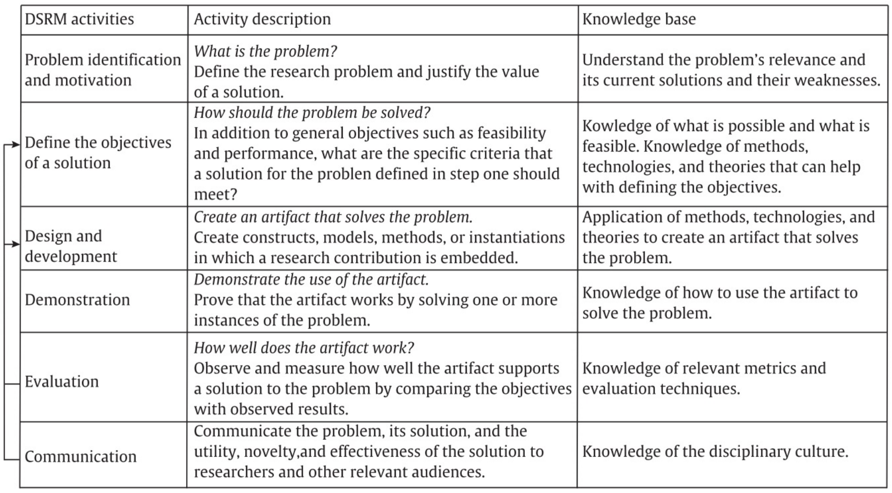
The aim of this research is to solve an existing practical problem in the realm of risk analysis tools by creating an artifact based on the existing theories of CIRA tool and cloud services. The problem will be solved by applying creativity, innovation and problem solving capabilities. The created artifact would then be practically applied to bridge the gap between risk analysis modeling and design of cloud service to support the business. Thus, the research clearly lies in the domain of design science research in information systems.

4.1 Design Science

Design science research, which is popular in disciplines such as engineering and architecture, focuses on creation: "how things ought to be in order to attain goals, and to function". The purpose of design is to change existing situations into preferred ones. The fundamental principle of Design science research is based on seven guidelines. The important guidelines provided by [22] are as follows:

- Design science research must result in creation of an innovative and practical artifact.
- It must provide solution to practical problem of a Business.
- The artifact must be evaluated and verified according to the specified problem
- The artifact must be novel in nature i.e. it must solve an unsolved problem or a solved problem in an effective way.
- Design science research must be based on the application of rigorous methods in both the construction and evaluation of the design artifact
- The research is an iterative search process where available resources are used to achieve desired goals while maintaining the environmental constraints.
- The outcome of the research work must be communicated to both managerial and technical audience.

The DSR process includes six steps: problem identification and motivation, definition of the objectives for a solution, design and development, demonstration, evaluation, and communication. The arrows on the left side of 4.1 emphasize the importance of iteration as part of the DSRM. They show that activities such as Evaluation and Communication often result in revising the artifact's objectives and design. Iteration is ingrained in design science research and [22] illustrate that with their build-and-evaluate loop: evaluation provides feedback information on the designed artifact and a better understanding of the problem which leads to a re-iteration of the design process. Table 4.1 describes DSR process in case of CIRA cloud service.



DSRM activities	Activity description	Knowledge base
Problem identification and motivation	*What is the problem?* Define the research problem and justify the value of a solution.	Understand the problem's relevance and its current solutions and their weaknesses.
Define the objectives of a solution	*How should the problem be solved?* In addition to general objectives such as feasibility and performance, what are the specific criteria that a solution for the problen defined in step one should meet?	Kowledge of what is possible and what is feasible. Knowledge of methods, technologies, and theories that can help with defining the objectives.
Design and development	*Create an artifact that solves the problem.* Create constructs, models, methods, or instantiations in which a research contribution is embedded.	Application of methods, technologies, and theories to create an artifact that solves the problem.
Demonstration	*Demonstrate the use of the artifact.* Prove that the artifact works by solving one or more instances of the problem.	Knowledge of how to use the artifact to solve the problem.
Evaluation	*How well does the artifact work?* Observe and measure how well the artifact supports a solution to the problem by comparing the objectives with observed results.	Knowledge of relevant metrics and evaluation techniques.
Communication	Communicate the problem, its solution, and the utility, novelty,and effectiveness of the solution to researchers and other relevant audiences.	Knowledge of the disciplinary culture.

Figure 4.1: Steps in Design Science Research, based on [23]

Design science research can be seen as an embodiment of three closely related cycles of activities 4.2. The Relevance Cycle bridges the contextual environment of the research project with the design science activities. The Rigor Cycle connects the design science activities with the knowledge base of scientific foundations, experience, and expertise that informs the research project. The central Design Cycle iterates between the core activities of building and evaluating the design artifacts and processes of the research. [22] Suggest that design science research should address either an unsolved problem in a unique and innovative way or a solved problem in a more effective or efficient way.

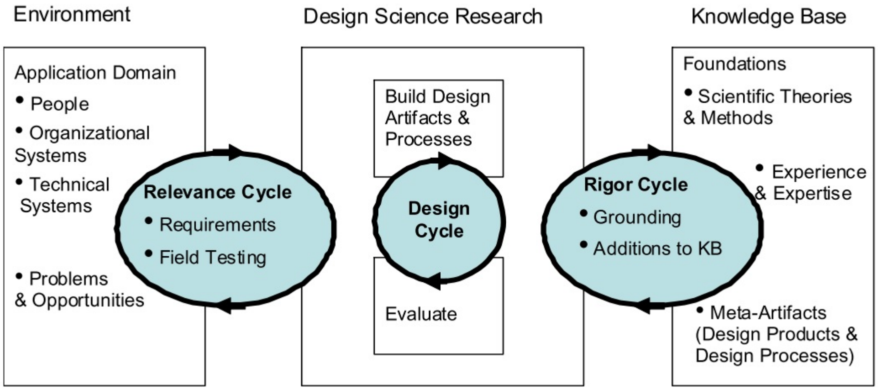


Figure 4.2: cycles of Design Science Research

No.	DSRM Activites	Activity Description	Knowledge Base
1	Problem identification and motivation	The risk analysis methods need to be extended to broader spectrum of information management to ensure secure and efficient data collection, data sharing and data operation service	Literature review of studies that discuss weakness of various risk analysis methods: report published by the OCTAVE, CORAS and a series of research paper that explore the different approaches to make risk analysis method more effective.
2	Define the objectives of a solution	Design of a system that is secure and it can achieve economies of scale, globalize the workforce, reduce capital cost of implement CIRA risk analysis method in a company.	Knowledge of distributed and cloud computing and their security and privacy issues.
3	Design and Development	Design of CIRA cloud service model: a framework to be used in a shared data environment where both experts and non-experts can contribute in risk analysis.	Cloud computing, CIRA methods, service oriented architecture, vCloud api programming, security engineering.
4	Demonstration	Formation of several instances of the problem to understand the effectiveness of the designed framework	Applying CIRA cloud service to real world problems.
5	Evaluation	CIRA cloud service must be evaluated in terms of scalability, security and operation cost?	Definition of performance measures and security metrics.
6	Communication	The work shall be published in relevant conferences and journals.	List of all related conferences and journals according to the impact factors and relevance to the topic.

Table 4.1: DSRM applied to CIRA as a cloud service.

4.2 Methods and research questions

1. **RQ1**: What are the quality and cost effective improvement features of CIRA tool as a cloud delivery model?

   Related to: Define the objectives of a solution, design and development

   Research Method and Strategy: Case study will be used as the research method to investigate the possible improvement features.

   Data Collection Method: Data required to investigate this research work will be collected from the literature review of various existing cloud deliver and risk analysis models. The detailed information of these models can be fetched from different publisher sites such as IEEE Xplorer, ACM digital library etc..

2. **RQ2**: What are the security requirements of an information sharing tool?

   Related to: Define the objectives of a solution, design and development

   Research Method and Strategy:

   Data Collection Method:

3. **RQ3**: What kind of information sharing features can be of special interest for the participants?

   Related to: Define the objectives of a solution,Define the objectives of a solution, design and development

   Research Method and Strategy:

   Data Collection Method:

4. **RQ4**: How can the desired functionality be implemented without violating the security requirements?

   Related to: design and development

   Research Method and Strategy:

   Data Collection Method:

5. **RQ5**: What are the benefits and shortcomings of the newly implemented features in the CIRA support tool?

   Related to: Design demonstration and Design evaluation

   Research Method and Strategy:

   Data Collection Method:

6. What is impact of the security risks and shortcomings of the added feature on adoption of cloud computing?

   Related to: Design evaluation

   Research Method and Strategy:

   Data Collection Method:

Chapter 5

Milestone

semester	code	Title	ECTS	Institute
Spring'14	IMT 6261	Scientific Communication	5	GUC
	IMT 6011	Introduction to information security	5	GUC
	IMT 6221	Mobile Technology	5	GUC
Autumn'14	IMT 6001	Ethics and legal aspects of scientific research	5	GUC
	IMT 6111	Risk management I	5	GUC
	IMT 6061	Risk management II	5	GUC

Table 5.1: Overview of PhD courses

5.1 External Institution

As my PhD research area is related to risk analysis, cloud computing and security engineering, I will target research groups who are working on the implementation of the cloud services, risk analysis, security in software engineering. I have identified few research teams and organizations that are working remarkable research work in the field of cloud computing. The first one is the FP7 Marie Curie Initial Training Network RELATE group. `http://www.relate-itn.eu/`. The other one is IBM zurich computer science department. They are mainly working on the security aspects of cloud ccomputing. `http://www.zurich.ibm.com/csc/security/securevirt.html`. I will start communicating these groups after the approval of my research proposal.

5.2 Paper publications (<2 p)

1. Limitations of Risk analysis models

2. Evaluation of risk analysis methods in the context of cloud service

3. Impact of security issues on the adoption of cloud computing in Conflicting Incentives Risk analysis method

4. Evaluation of security controls to mitigate adoption risk of CIRA to cloud environment.

5. security metrics for CIRA cloud service.

5.3 Research Risk and Mitigation (< 2 p)

Data Availability

The concept of this research work is based on the idea of cloud computing and risk analysis methods focusing mainly on the security and privacy aspects of it. The concept of cloud computing and CIRA is new and several issues are still unsolved or unconsidered. I will consider data published in the reports of companies like IBM, AMAZON, SalesForce. These companies are doing remarkable research work in the field of cloud computing.

Paper rejection

There is always a risk associated with the paper being submitted to a conference or journal. A paper may be rejected due to the low acceptance rate of the conference or because of very high impact factor value. If my paper gets rejected due to any reason, I will discuss the issue with my supervisors so that I can address the shortcoming of the paper and resubmit in other relevant conferences.

5.4 Conferences and Journals

- Security & Privacy
  - IEEE International Conference on Trust, Security and Privacy in Computing and Communications
  - International Conference on Security and Privacy in Communication Networks
  - International Conference on Informatics and Information Technology International Workshop on Software Engineering for the Smart Grid
- Security Management
  - Disaster, Risk and Vulnerability Conference 2014
  - IEEE Colloquium on Risk Analysis Methods and Tools
  - SRA Journal
  - Conference on Cloud Security Management
  - 11th International Workshop on Security in Information Systems
- Cloud Computing
  - The ACM Cloud Computing Security Workshop
  - IEEE International Conference on Cloud Computing
  - IEEE International workshop on Cloud Computing Applications and SEcurity
  - IEEE International Conference on Cloud Computing Technology and Science The Second International Conference on Digital Information Processing, E-Business and Cloud Computing (DIPECC 2014)
- Information Sciences
  - Journal of Emerging Trends in Computing and Information Sciences

Chapter 6

Supervision

For this project I propose Dr. Einar Arthur Snekkenes, Professor, NISLab as my principal supervisor

Chapter 7

Funding Plan

The source is internal funding of NISLAB.

Chapter 8

Ethical and legal considerations

I shall follow the ethical guidelines as published in Guidelines for Research Ethics in Science and Technology by The National Committee for Research Ethics in Science and Technology, Norway (NENT)

Good Publication practice

I shall follow good Publication practice. I shall denote all the source material and respects the original contributions of others through citations. Honorary authorships are unacceptable. Rightful authorship is considered to be defined by three criteria:

1. All the authors must have made a significant and directly academic contribution to at least two of the four components of a typical research project:
   (a) concept or design
   (b) Data collection and processing
   (c) Analysis and interpretation of data
   (d) Written formulation of substantial parts of the work
2. All the authors should have critically read through the different drafts and approved the final version
3. All the authors should be capable of defending the work in its entirety (though not necessarily all the technical details).

Honest research practices

- I shall follow Integrity, honesty and accountability while conducting my research work.
- I shall not follow any scientific fraudulence, either in the form of forgery, manipulation or the selective presentation of data from research con- ducted by themselves or others
- I shall not indulge in plagiarism of research.
- I shall make data accessible to others for verification.
- I shall present research done by others in a balanced and honest manner.

Statement of Compliance

I will conduct my activities as a researcher with integrity and honesty; I will use my scientific knowledge and skills for the benefit of humanity and for a sustainable development; I will show respect for animals and nature; I will act in accordance with research ethics, and I will not allow considerations based on ideology, religion, ethnicity, prejudices or material advantages to overshadow my ethical responsibility as a researcher.

Bibliography

[1] P. Zhou and H. Leung, "An integrated risk analysis method using spatial interpolation," in *Software Engineering Conference (APSEC), 2012 19th Asia-Pacific*, vol. 1, pp. 452–461, Dec 2012. 4

[2] B. Karabacak and I. Sogukpinar, "Isram: information security risk analysis method," *Computers and Security*, vol. 24, no. 2, pp. 147 – 159, 2005. 4

[3] A. Bilbao, "Tuar-a model of risk analysis in the security field," in *Security Technology, 1992. Crime Countermeasures, Proceedings. Institute of Electrical and Electronics Engineers 1992 International Carnahan Conference on*, pp. 65–71, Oct 1992. 4

[4] M. P. Kailay and P. Jarratt, "Ramex: a prototype expert system for computer security risk analysis and management," *Computers and Security*, vol. 14, no. 5, pp. 449 – 463, 1995. 4

[5] L. Rajbhandari and E. Snekkenes, "Using the conflicting incentives risk analysis method," in *Security and Privacy Protection in Information Processing Systems* (L. Janczewski, H. Wolfe, and S. Shenoi, eds.), vol. 405 of *IFIP Advances in Information and Communication Technology*, pp. 315–329, Springer Berlin Heidelberg, 2013. 4, 5, 7

[6] B. Jenkins, "Security risk analysis and management," 1998. 4

[7] I. S. F. (ISF), "Simplified practical risk analysis methodology (sprint) user guide," pp. 43–57, 1997. 4

[8] C. J. Alberts and A. Dorofee, *Managing Information Security Risks: The Octave Approach*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2002. 4

[9] Y. Jadeja and K. Modi, "Cloud computing - concepts, architecture and challenges," in *Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on*, pp. 877–880, March 2012. 5, 8

[10] Amazon, "Amazon elastic compute cloud (ec2) delivers scalable, pay-as-you-go compute capacity in the aws cloud," 2013. 5, 9

[11] B. Zhang, N. Zhang, H. Li, F. Liu, and K. Miao, "An efficient cloud computing-based architecture for freight system application in china railway," in *Cloud Computing* (M. Jaatun, G. Zhao, and C. Rong, eds.), vol. 5931 of *Lecture Notes in Computer Science*, pp. 359–368, Springer Berlin Heidelberg, 2009. 5

[12] L. Rajbhandari, *RISK ANALYSIS USING CONFLICTING INCENTIVES AS AN ALTERNATIVE NOTION OF RISK*. PhD thesis, HÃ¸gskolen i GjÃ¸vik, October 2013. 7

[13] P. Mell and T. Grance, "The nist definition of cloud computing," Tech. Rep. 800-145, National Institute of Standards and Technology (NIST), Gaithersburg, MD, September 2011. 8

[14] P. Simmonds, B. Bhagat, L. Lynch, and M. Pohlman, *Security guidance for critical areas of focus in Cloud Computing V3. 0*, vol. 3.0. CLOUD SECURITY ALLIANCE, 2011. 8

[15] Google, “Google cloud platform,” 2014. 9

[16] G. Grid, “Cloud platform,” 2013. 9

[17] G. J. Brodkin, “Gartner: Seven cloud-computing security risks,” 2008. 9, 10

[18] L. Sumter, “Cloud computing: Security risk,” in *Proceedings of the 48th Annual Southeast Regional Conference*, ACM SE ’10, (New York, NY, USA), pp. 112:1–112:4, ACM, 2010. 9

[19] S. Bleikertz, M. Schunter, C. W. Probst, D. Pendarakis, and K. Eriksson, “Security audits of multi-tier virtual infrastructures in public infrastructure clouds,” in *Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop*, CCSW ’10, (New York, NY, USA), pp. 93–102, ACM, 2010. 10

[20] F. Shaikh and S. Haider, “Security threats in cloud computing,” in *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*, pp. 214–219, Dec 2011. 10

[21] F. Lombardi and R. Di Pietro, “Transparent security for cloud,” in *Proceedings of the 2010 ACM Symposium on Applied Computing*, SAC ’10, (New York, NY, USA), pp. 414–415, ACM, 2010. 10

[22] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design science in information systems research,” *MIS Q.*, vol. 28, pp. 75–105, Mar. 2004. 11, 12

[23] G. L. Geerts, “A design science research methodology and its application to accounting information systems research,” *International Journal of Accounting Information Systems*, vol. 12, no. 2, pp. 142 – 151, 2011. Special Issue on Methodologies in {AIS} Research. 12