Sudan University of Science and Technology

College of Graduate Studies

A Methodology for the Assessment of Security Risk in Cloud Computing

منهجية لتقييم المخاطر الامنية للحوسبة السحابيه

A Dissertation Submitted to the Faculty of

the **College of Graduate Studies**

in Partial Fulfilment of the Requirements for the Degree of

Doctor of Philosophy

by

Ishraga Mohamed Ahmed Khogali

Supervisor

Prof. Hany Ammar

December 2018

Sudan University of Science & Technology
College of Graduate Studies
كلية الدراسات العليا

جامعة السودان للعلوم والتكنولوجيا
كلية الدراسات العليا

Ref: SUST/ CGS/A11

Approval Page

(To be completed after the college council approval)

Name of Candidate: Ishraga | Mohamed | Ahmed | Khogali

Thesis title: A Methodology for the Assessment of Security Risk in Cloud Computing

Degree Examined for: منهجية لتقييم المخاطر الأمنية للحوسبة السحابية

Approved by:

1. External Examiner

Name: Tagelsir Mohamed Gasmelseid

Signature: ..... Date: 14/11/18

2. Internal Examiner

Name: Izzeldin mohamed Osman

Signature: ..... Date: 14/11/18

3. Supervisor

Name: c/ Salah Elfaki Elrofai

Signature: c/ ..... Date: 14/11/2018

cgs @ sustech edu. البريد الالكتروني 83 769363 فاكس/ 407 ص ب

ACKNOWLEDGMENTS

First I would like to thank to my supervisor Prof. Hany Ammar for his valuable guidance and advises . He inspired me and contributed greatly to my work in this study.

Besides, I would specially thank my family who support me for completing this study.

To both Prof. Ammar and my family, I acknowledge that their help was crucial to the success of this thesis.

Abstract

Cloud computing has been one of the major emerging technologies in recent years. However, cloud computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. Moreover, cloud computing comprises of various technologies like virtualization, transaction management etc., so it also inherits their security issues.

The cloud computing technology introduces new security risks that need to be assessed and mitigated. However, a traditional security risk assessment methodology is not suitable to cloud computing due to its several characteristics. Recently, several risk assessment methods and models have been proposed to assess the security risk in cloud computing. None of these methods is fully quantitative. Moreover, none of them are scenarios based to fit the dynamic nature of the cloud computing environment. Therefore, assessing the security risk in cloud computing is still an open research issue.

In this thesis we present a scenario-based methodology to assess security risk in cloud computing. This methodology enables the provider to assess the security risk in cloud computing applications. This methodology is based on the National Institute of Standards and Technology (NIST) Risk Management Framework. In this framework the risk is derived by multiplying the ratings assigned for threat likelihood and the threat impact. We propose using Bayesian networks to determine the likelihood which enables us to compute the probability of failures over variables of interest given the evidence for the certain scenario of usage for the application. In addition, we propose two methods to specify the impact factor. The first is to categorize impact by expert assessment according to MIL-STD-882E standard severity categories. The second method is using the worst case sensitivity analysis to assess the threat impact.

To validate the proposed methodology we use two case studies, the E-commerce application, and a Live VM Migration scenario. As we compare the proposed method with the existing methods base on assessing risk in the dynamic scenarios. Furthermore, we apply security controls on a case study and the result show significant reduction in risk values and mitigation for significant risk.

الـم ستـخلـص

الحوسبة السحابية هي واحدة من التكنولوجيات المهمة الناشئة في السنوات الأخيرة . ومع ذلك ، تقدم الحوسبة السحابية مستوى إضافيًا من المخاطر نظرًا لأن الخدمات الأساسية يتم الاستعانة بها في كثير من الأحيان لطرف ثالث ، مما يجعل من الصعب الحفاظ على أمان البيانات والخصوصية ، وبيانات الدعم وتوفر الخدمة ، وإثبات الا لتزام. علاوة على ذلك ، تتألف الحوسبة السحابية من تقنيات متنوعة مثل المحاكاة الافتراضية وإدارة المعاملات وما إلى ذلك ، لذلك فهي ترث أيضًا مشكلاتها الأمنية .

تقدم الحوسبة السحابية مخاطر أمنية جديدة تحتاج إلى تقييمها وت قليلها. ولكن طرق تقييم المخاطر الأمنية التقليدية ليست مناسبة للحوسبة السحابية بسبب خصائصها المتعددة. في الآونة الأخيرة ، تم اقتراح العديد من طرق تقييم المخاطر والنماذج لتقييم المخاطر الأمنية في الحوسبة السحابية. لا شيء من هذه الأساليب كمي بالكامل . علاوة على ذلك ، لا يعتبر أيا منها يستند إلى سيناريوهات لتناسب الطبيعة الديناميكية لبيئة الحوسبة السحابية. لذلك ، لا يزال تقييم المخاطر الأمنية في الحوسبة السحابية مسألة مفتوحة للبحث.

نقدم في هذه الرسالة منهجية لتقييم المخاطر الأمنية في الحوسبة السحابية قائمة على أساس السيناريو. تمكن هذه المنهجية مزود الحوسبة السحابيه من تقييم المخاطر الأمنية في تطبيقات الحوسبة السحابية . تستند هذه المنهجية على إطار إدارة المخاطر الخاص بالمعهد الوطني للمعايير والتكنولوجيا (NIST). في هذا الإطار ، يتم حساب المخاطر من خلال ضرب القيم المحددة لاحتمال التهديد وتأثير التهديد. وقد تم اقتراح استخدام شبكات بيزيان Bayesian networks لتحديد الاحتمالات و التي تمكننا من حساب احتمال ال قصور على المتغيرات

المرغوب الاهتمام بها مع النظر للأدلة المتوفرة لسيناريو معين للاستخدام المحدد للتطبيق. بالإضافة إلى ذلك ، قد اقترحنا طريقتين لتحديد عامل التأثير . الأولي هي تصنيف الأثر من خلال تقييم الخبراء تبعاً لفئات الخطورة القياسية في المعيار العسكري رقم 882هـ –MIL) (STD–882E. الطريقة الثانية هي استخدام أسوأ حالة في تحليل تأثير المتغيرات علي المتغيرات الأخرى لتقييم أثر التهديد.

للتحقق من المنهجية المقترحة قد تم استخدام دراستي حالة ، وهما تطبيق التجارة الإلكترونية ، وسيناريو الهجرة المباشرة للآلات الإفتراضية Live VM Migration. كما تمت مقارنة الطريقة المقترحة مع الطرق الحالية علي أساس تقييم المخاطر في السيناريوهات المتغيرة dynamic scenarios. علاوة على ذلك ، قد تم استدعاء عناصر تحكم أمنية على دراسة حالة وقد أظهرت النتائج انخفاضًا كبيرًا في قيم المخاطر والتخفيف من المخاطر الكبيرة.

Table of Contents

List of Tables

List of Figures

List of Symbols /Abbreviations

NIST	National Institute Of Standards And Technology
IaaS	Infrastructure As A Service
PaaS	Platform As A Service
SaaS	Software As A Service
API	Application Programming Interface
DDoS	Distributed Denial Of Service
DoS	Denial Of Service
SLA	Service Level Agreement
CSA	Cloud Security Alliance
SSL	Secure Socket Layer
NIST	National Institute Of Standards.
OCTAVE	Operationally Critical Threat, Asset, And Vulnerability Evaluation
COBIT	Control Objectives For Information And Related Technology
IOT	Internet Of Things
VA	Vulnerability Assessment
IDS/IPS	Intrusion Detection/Prevention Systems
ENISA	European Network And Information Security Agency
QUIRC	Quantitative Impact And Risk Assessment Framework For Cloud Security
FISMA	Federal Information Security Management Act

FIPS	Federal Information Processing Standards
SO	Security Objectives
FUD	Fear, Uncertainty And Doubt
SLAs	Service Level Agreements
T&VA	Threat And Vulnerability Assessment
AHP	Analytic Hierarchy Process
RBS	Risk Breakdown Structure
AHP	Analytic Hierarchy Process
CCM	Cloud Control Matrix
BNs	Bayesian Networks
CPDs	Conditional Probability Distributions
NPTs	Node Probability Tables
DoD	Department Of Defense
UML	Unified Modeling Language
FFA	Functional Failure Analysis
FMEA	Failure Mode And Effect Analysis
FTA	Fault Tree Analysis
TLS	Transport Layer Security

HTTPS	Hypertext Transfer Protocol
SDLC	Software Development Lifecycle
OWASP	Open Web Application Security Project
XSS	Cross-Site Scripting
CSRF	Cross-Site Request Forgery
DDoS	Distributed Denial Of Service
VMs	Virtual Machines
VMM	Virtual Machine Monitor
LM	Live Migration
NAS	Network-Attached-Storage
TCCP	Trusted Cloud Computing Platform

CHAPTER 1

INTRODUCTION

Chapter 1 : Introduction

1.1 Cloud Computing

Cloud computing is a new technology that provides a real promise to business with real advantages in terms of cost and computational power. The National Institute of Standards and Technology (NIST) defines cloud computing as ‘‘a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Drissi et al., 2013)’’. These resources can managed to dynamically scale up to match the load, using a pay-per-resources business model.

The Cloud Computing architecture comprises of many loosely coupled components that divides into Front End and Back End. Front End refers to the client part, which consists of interfaces and applications that are required to access the cloud computing platforms. Back End consists of all the resources required to provide Cloud computing services. It includes huge data storage, virtual machines, security mechanisms, services, deployment models, servers, etc. Figure1.1 illustrates this where each of the end connected through a network, usually via Internet (Varsha & Kousar, 2016).

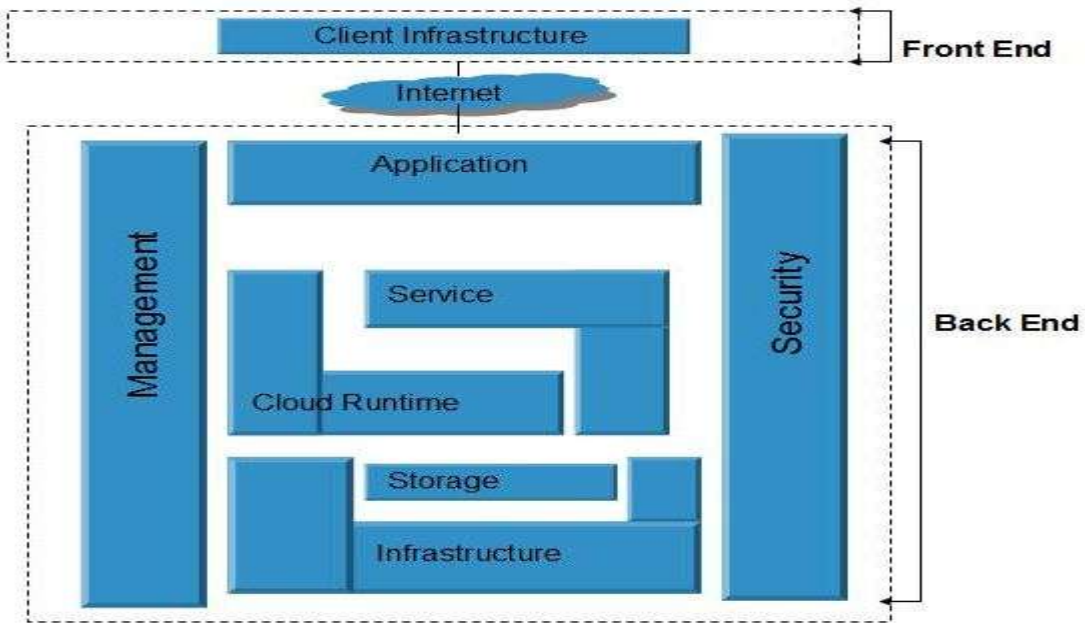


Figure 1. 1: Cloud computing architecture (Varsha & Kousar, 2016)

Although Cloud computing is a major technological trend that continues to evolve and flourish it raises severe security concerns that limit its widespread adoption. Such as loss of governance, lock-in, isolation failure, data protection and insecure data deletion. A recent survey by Cloud Security Alliance (CSA) &IEEE indicates that enterprises across sectors are ready to adopt cloud computing but that security needed to accelerate cloud adoption on wide scale (Subashini & Kavitha, 2011).

Therefore, it's important to consider security and data protection when it comes to widespread cloud adoption, especially for bigger banks. For most banks, finding a truly protected third party cloud service can be a challenge as many "secure" services on the market have security gaps that leave data and private company info wide open to third party attacks, leaks, or hacking.

However, different Cloud computing models have emerged at different degrees of flexibility, which involve distinct risks. The needs and goals of each organization will vary. Therefore, before utilizing cloud-services, organizations should ensure that they understand the security and privacy risks in the cloud environment and their security and privacy requirements based on their business requirements are satisfied (Cloud Security Alliance , 2013).

1.1.1 Cloud Computing Deployment Models

There are four deployment models, where the organizations can select the appropriate Cloud computing model according to their needs:

1) Private cloud: where cloud platform is operating for specific organization.
2) Community cloud: where the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns.
3) Public cloud: where cloud platform is available to public users to register and use the available infrastructure.
4) Hybrid cloud: that can combine two or more clouds (private, community or public) (Drissi et al., 2013)

Public cloud is used as a service via Internet by the users, whereas a private cloud, deployed within certain boundaries like firewall settings and is completely managed and monitored by the users working on it in an organization (Vikas et al., 2013).

Therefore, public cloud providers are much larger targets for hackers than private clouds. Private clouds will immediately seem to be more secure than public clouds because of how the infrastructure is designed. It gives the organization more control over their policies and security. However, private clouds typically would suffer from perimeter complacency; thinking that because it is on the internal network, it must be secure; the Internet and viruses are still present. Private clouds have the same security concerns as public clouds do, but typically on a smaller scale since private clouds are operated solely for an organization. So, caution and security standards should not be lowered just because it is private. Moreover, the private cloud requires that to have total control over all layers of the stack, which includes any traditional network perimeter security you might want to have in place (Simmonds & Wahab, 2012).

Table 1.1 explain brief comparison between public cloud and private cloud.

Table 1. 1 A brief comparison between public and private cloud

(Simmonds & Wahab, 2012).

public cloud	private cloud
No control over data security	IT organization retains control over data
Higher risk of multi-tenancy data transfer	Fewer security concerns

Both public and private cloud models have their own advantages and challenges.

1.1.2 Cloud Computing Delivery Models

Cloud computing utilizes three delivery models by which different types of services are delivered to the end user. These delivery models can be deployed as private cloud, public cloud, community cloud or hybrid Cloud. The three delivery models are the SaaS, PaaS and IaaS that provide software as services, application platform and infrastructure resources to the customer. Each customer selecting the appropriate model depending on its own approach, characteristics and level of security requirement (Subashini & Kavitha, 2011) as explained in the following.

1) Infrastructure as a Service (IaaS): This model provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. pooled and made available to

handle workloads. The capability provided to the customer is to rent processing, storage, networks, and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has the control over operating systems, storage, deployed applications, and possibly select networking components (e.g., firewalls, load balancers etc.) (Sen, 2016)

2) Platform as a Service (PaaS): In this model, a layer of software or development environment encapsulated and offered as a service, upon which other higher levels of service are built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. Hence, a capability provided to the customer to deploy onto the cloud infrastructure customer-created applications using programming languages and tools supported by the provider. Although the customer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage, he/she has the control over the deployed applications and possibly over the application hosting environment configurations (Sen, 2016)**.**

3) **Software as a Service (SaaS):** In this model, the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as web browser. Everything from application level down to the infrastructure level is under the responsibility of the provider and the customers do not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, with the exception of limited user-specific application configuration settings (Sen, 2016). Therefore, Organizations that are considering SaaS adoption and engage in a rational decision process entailing gathering information about each potential provider's ability to address the security dimension (Bernard et al., 2011).

1.2 Security Risk Assessment

The idea of handing over important data to another company is worrisome such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment (Kuyoro et al., 2011). So, in spite of the

advancement in cloud technologies and increasing number of cloud users, Cloud computing being a new technology introduces new risks that need to be assessed and mitigated (Drissi et al., 2013).

The synonyms that much related to risk assessment is defining as follows and they interrelate as shown in Figure 1.2.

A. Assets: It include hardware, networks or software (always related to an IS) and all those supporting the underneath infrastructure such as staff (administrators, operators, users...) or facilities. Even much more intangible ones like information, brand image or reputation.

B. Threats: The events or root causes that may provoke an incident, with unwanted results for an Organization's objectives materialized on harm or loss of assets.

C. Vulnerabilities: Flaws or weaknesses on procedures, design, implementation or internal security controls in IS, that may be exploited purposely or accidentally.

D. Impact: It is the result arising from a threat taking advantage of asset vulnerabilities, and thus causing a certain degradation or loss of the asset's value.

E. Probability: Likelihood of a threat happens over a given period of time.

F. Risk: It is the potential that a given threat will exploit a vulnerability of an asset and thereby cause harm to the Organization.

G. Safeguards*:* They are security measures (resources or procedures) that somehow mitigate risk (López et al., 2013).

H. Residual Risk: The risk remaining after the implementation of new or enhanced controls. The extent of the risk reduction generated by the new or enhanced controls (Stoneburner et al., 2002).

Accordingly, Security risk assessment identified as the process of identifying the security risks to a system and determining their probability of occurrence, their impact, and the safeguards that would mitigate that impact (Drissi et al., 2013). It aimed to examining possible threats, vulnerabilities, the likelihood and impact of them (López et al., 2013) to define appropriate controls for reducing or eliminating the risks (Drissi et al., 2013). Then organizations can analyze the extent of the risk reduction generated by the new or enhanced controls in terms of the reduced threat likelihood or impact, the two parameters that define the mitigated level of risk (Stoneburner et al., 2002).

Implementation of new or enhanced controls can mitigate risk by:

- Eliminating some of the system's vulnerabilities.
- Adding a targeted control to reduce the capacity and motivation of a threat-source.
- Reducing the magnitude of the adverse impact .

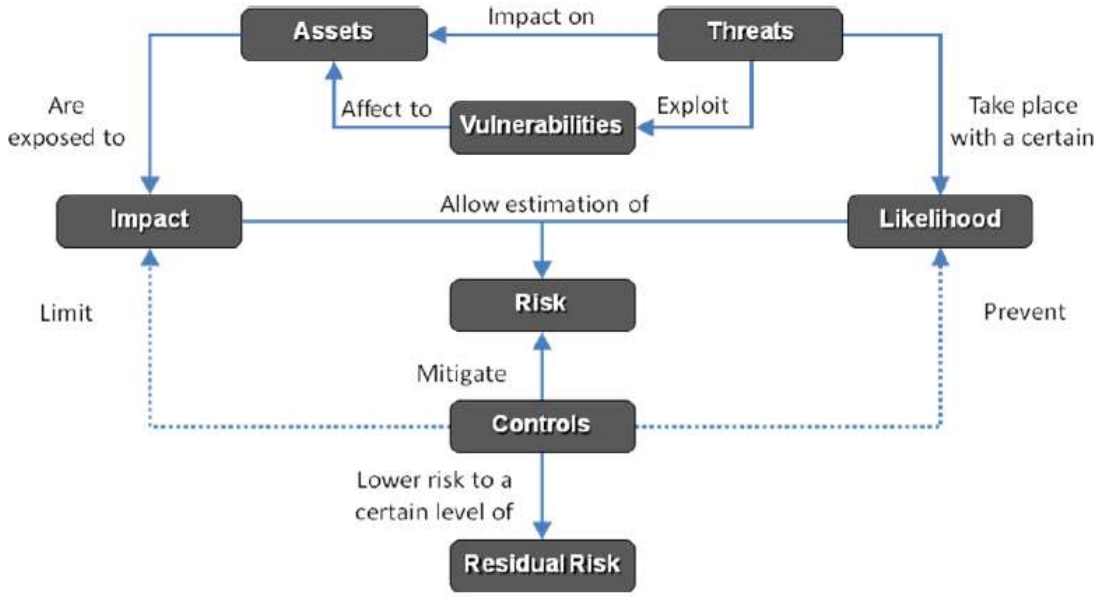


Figure 1. 2: Conceptual diagram of risk assessment key factors and their interrelations (López et al., 2013)

In general, there are three categories for risk assessment methods: quantitative, qualitative and semi-quantitative (or hybrid). Quantitative risk assessments, provides accurate measurements of impacts' magnitude but involves calculations that are tedious and include a strong element of arbitrariness. Moreover these quantitative impacts may be unclear, thus requiring to be interpreted in a qualitative way. On the other hand, the qualitative assessments do not provide enough quantifiable measurements concerning probabilities and impacts of risks but prioritize risks and identify the most important areas for improvement. As a result, semi-quantitative risk assessments replace very well tedious quantitative approaches, and incomplete qualitative methods (Fit´o et al., 2010)

1.3 Cloud Computing Security

According to the CSA final 2016 report (Cloud Security Alliance, 2017), experts identified the following 12 critical issues to cloud security (ranked in order of severity):

1. Data Breaches
2. Weak Identity, Credential and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Vulnerabilities (Cloud Security Alliance, 2017)

Hence, while using cloud-based solutions, organizations need to be aware of these concerns. Although most of these concerns are not new, already exist in traditional IT environment, they need more consideration because of the dynamic nature of cloud computing platform.

1.3.1 Cloud Computing Threat Model

(Amini et al., 2015) propose dynamic model of identifying vulnerabilities and threats in cloud computing environment. They present a methodology of the threat model to deploy a secure computing environment by showing threats and vulnerabilities in the cloud computing and determining security solutions as explained in the following.

❑ **Cloud computing threats:** The most of significant threats that are related to on-demand nature of cloud computing are categorized as below:

- Data lose or leakage (T1): Any data deletion by service provider or baleful accident such as fire can lead to lose the consumer's data.

- Account or service hijacking (T2): This weakness allows attackers to steal credentials and access to critical areas of cloud computing services.

- Insecure interface (T3): Cloud computing's customers use malicious Application Programming Interface (API) or software interfaces to interact and manage cloud services.

- Denial of service (T4): Distributed Denial of Service (DDoS) is the major security threat to availability when it comes to increase reliability of organizations on public cloud services. On the other hand, this attack prevents users from accessing their data or applications and there is no way to reach their destination.

- Malicious insider (T5): The system has been damaged by authorized employee, business partner or administrator that has access to a network or resources.

- Data breaches (T6): One of the worse situations for each organization is unauthorized access or illegal viewing data by competitors. Data encryption can reduce the risk of this threat, but should be careful about encryption key because if you lose it, you will lose your data as well

- Abuse of cloud services (T7): Cloud computing providers do not enforce any strong registration process and any user with a valid credit card can register to receive cloud services.

- Insufficient due diligence (T8): The cost reduction, access to pool of resources and improving security are the most important interesting factors for organization to rush cloud computing. However, for sufficient qualification of resources, organizations have to understand the service provider offerings and risks

- Insecure VM migration (T9): By migrating different VMs during hybrid and

federated clouds, attackers can access data illegally and transfer VM to untrusted host (Amini et al., 2015).

❑ **Cloud computing vulnerability:** The following significant vulnerabilities should be considered on cloud computing based on CC's technologies, essential cloud characteristics, known security controls and state-of-the-art cloud offerings:

- Session riding (V1): Session riding refers to send command to web application by hackers to gain unauthorized access for the information or use web service weaknesses for giving the chance to hackers to do malicious activities same as deleting of user data or sending spam to a network via internet.

- Virtual machine escape (V2): This vulnerability allows attacker runs code on a VM that let operating system to break out and interact directly with the hypervisor to access host operating system and other virtual machines.

- Obsolete cryptography (V3): Developing not enough strong encryption or no encryption at all allows attacker to decode encrypted data. To protect system from this vulnerability, user should be sure the true data is encrypted, use proper key storage and develop a good algorithm

- Unauthorized access to management interface (V4): The cloud management interface has access to cloud service users to manage on-demand services. An unauthorized access enables attackers to gain total control of users and applications

- Internet protocol (V5): The lack of authentication methods that is not a part of the base protocol design, allows attackers to inject their malicious traffic to network. On the other hand, the IP protocol or related protocols same as UDP and TCP are vulnerable to different type of Denial of Service (DoS) attacks, including session hijacking and cash poisoning.

- Data recovery (V6): Cloud computing allows resources to be allocated or reallocated by different users. This elastic characteristic could lead to data stolen, data breaches and other security threats. The most of organizations use third party

vendors to recover data so they should consider security risk of handling data with outside company and ensure proper security vetting of the service provider.

- Metering and billing (V7): Cloud computing meters and measures services such as storage, user account and processing are used to optimize service delivery. Applicable vulnerabilities contain metering and billing data treatment and billing elusion.

- Vendor lock-in (V8): Vendor lock-in is the situation that cloud's user is dependent to a single vendor and is unable to deal with another provider without substantial and inconvenience. The lack of the standards is the main reason that users cannot transfer easily from one provider to another (Amini et al., 2015).

Table 1.2 explains threats and vulnerabilities and their countermeasures.

Table 1.2: Relation between threats, vulnerabilities and their countermeasure (Amini et al., 2015).

Threats	Vulnerabilities	Countermeasure
T1	V1,V2,V3,V4,V5,V6	Data encryption, data signature, DLP as a service
T2	V1,V3,V5,V6	Identity and Access Management (IAM) services
T3	V1,V3,V4	Authentication, Access control
T4	V1,V2,V4,V5,V6,V7	Apply security patches, use an IPS for monitoring, configuring firewall, minimize IP spoofing
T5	V2,V5	Cryptography, separation of duties, logging and auditing, legal contracts and insider detection models
T6	V1,V3,V4,V5	Stop incursions, data protection policies, automating periodic check, security event management, monitoring technologies and authenticate identities
T7	V1,V4,V5	Stricter initial registration, credit card fraud monitoring, black list monitoring
T8	V8	Trusted Third Party (TTP), Rating cloud service provider
T9	V2	Trusted Cloud Computing Platform (TCCP), secure protocol and live migration

Moreover, The fact that cloud computing utilized different types of service models (IaaS, PaaS, SaaS) makes it even more complex in security terms. Table 1.3 illustrate threats according to the Microsoft's STRIDE model along with the countermeasures proposed and responsible party for applying countermeasures (Lourida et al., 2013).

Table 1. 3 : Cloud Threat Model (Lourida et al., 2013)

Threat	Countermeasure	Responsible in IaaS	Responsible in PaaS	Responsible in SaaS
Spoofing	Authentication techniques	Cloud Client	Cloud Provider Cloud Client	Cloud Provider Cloud Client
Tampering	Digital Signatures	Cloud Client	Cloud Provider Cloud Client	Cloud Provider Cloud Client
Repudiation	Auditing	Cloud Client	Cloud Provider Cloud Client	Cloud Provider Cloud Client
Information disclosure	Encryption	Cloud Client	Cloud Client	Cloud Client
Denial of Service (DoS)	Monitoring Provisioning	Cloud Provider	Cloud provider	Cloud provider
Elevation of privilege	Authorization	Cloud Provider Cloud Client	Cloud Provider Cloud Client	Cloud provider

1.3.2 Cloud Computing Risk Per Service

(Baggar & Sinha, 2013) identify and categorize the risk according to type of service model as the following:

A. Risk in IAAS

a. Business Risk due to Disaster: If the critical application for business hosted in IAAS environment, the down time due to man mad or natural disaster can introduce business risk**.**

b. Physical security of the IAAS environment: physical security and environmental controls.

c. The Service Level Agreement (SLA): Violating SLA will also be subject to many business risks .

d. Compatibility of IAAS and internal infrastructure: virtual environment compatibility from Client to server (Baggar & Sinha, 2013).

B. Risk in PAAS

a. Data Protection: because in PaaS data stored and processed by the third party.

b. Expertise of the Service provider: Before contacting any service provider, the client must be sure about the service providers' development team whether they have the expertise to build applications with strong information security foundation.

c. Data Location: data is stored at the third party end so the client is unaware about how the data is stored and where it is stored.

d. Loss of Governance: the client grants control to the Service Provider on different issues, which may affect the security.

e. Lack of performance due to dependency: When the data can only accessed via someone else's server, it demands the guarantees of its uptime (Baggar & Sinha, 2013).

C. Risk in SAAS

a. Unauthorized access of data: the service provider of SaaS providing services to the other clients and the data of those clients also stored at the same storage area.

b. Incomplete and insecure data deletion: it is possible that data it will not delete truly and wholly due to the multi tenancy approach and reuse of hardware resources.

c. Data back-up or Data Replication: If any disaster occurs then whether the service provider is using sufficient amount of precautions like storing data off-site in a secure storage facility or replicate the data in any other secondary memory.

d. Lack of Standards: The service provider must follow the standards or must be a certified service provider like SSAE16 certification.

e. Lack of Isolation: due to multi tenancy approach, there must be some distinction between all the resources (storage, hardware, memory, routing etc) of all the tenants.

f. Market Reputation of Service Provider*:* If any risk affects the service provider image or reputation of service provider or failure of his business then it will be hard to the client to compensate for this.

Beside these, there can be many more risks in a SaaS application (Baggar & Sinha, 2013).

1.4 Cloud Computing Security Risk Assessment

Cloud computing encompasses new technologies such as virtualization and there are both new risks to be determined and old risks to be re-evaluated (Fit´o et al., 2010).

If Cloud providers and its users will always expose to hazard events it will greatly reduce all Cloud computing benefits (Fit´o et al., 2010). However, not all data is created equal, and no need to provide maximum protection to all data. So, it's important to classify data based on how sensitive or valuable it is to know what most sensitive data is, where it is and how well it's protected (Federal communications commission, 2012). Of course Cloud cost must be proportional to the security level consequently if the information is high sensitive customer have to select high secure provider and pay more to provide more security for them but if data is not sensitive he don't have to pay more to gain cloud services. Because if the cloud solution require additional security some security technologies that provides some capability in cloud computing must be implemented such as SSL (Secure Socket Layer), digital signatures, and authentication protocols for proving authentication and access control methods for managing authorization. However, these security technologies are lacking the complementary tool for managing trust effectively (Sangroya et al., 2010). Risk assessments provide significant value in increasing trust and thus appear particularly beneficial to the adoption of cloud computing (Burton et al., 2010).

1.4.1 Why Cloud Security Are Hard to Assess with Existing Tools

There are five cloud characteristics articulated in NIST's definitions that also make cloud security and privacy are "immeasurable" with current assessment approaches (Burton et al., 2010). Which explained as the following:

1. On -Demand Self-Service

A traditional assessment, however, may assume the existence of trained individuals in certain roles. To be effective in a cloud environment, it must equally address the increasing presence of their automated equivalents (Burton et al., 2010).

2. Broad Network Access

Broad network access affects assessments by changing the attack surface that must be assess from a relatively static set of approved devices to a dynamic

collection of end points of varying security postures and capabilities (Burton et al., 2010)

3. Resource Pooling

Resource pooling imposes perhaps the greatest collective set of challenges. First, the dynamic allocation of resources according to consumer demand means that the specific resources deployed for a given application are not known a priori and therefore cannot assessed in advance. Second, the service of multiple consumers with the same pool of resources means that the impact of the presence of other tenants in the cloud infrastructure must also be taken into account. Finally, location independence of the physical resources introduces the complicating possibility that those resources may be subject to varying local regulations (Burton et al., 2010).

4. Rapid Elasticity

In the cloud, the assessment must not only cover the consumer and a given target provider, but the provider's own sub-providers, and so on recursively since they can be cloud bursting to handle the rapidly increasing workloads where migrating to meet demand is possible between different clouds. Moreover, the systematic migration of a consumer's computational workload across multiple providers not specified in advance; also, the movement of actors, not data (Burton et al., 2010).

5. Measured Service

Lastly, the "metering capability" by which cloud systems "automatically control and optimize resource use" presents one more challenge for assessments, that the assessment in a cloud environment must consider the much finer level of detail resulting from the focus on cost and dynamic resource sharing. Furthermore, even if the metering information for each tenant is individually well protected, there remains the possibility that an adversarial consumer can infer behavioral patterns of other tenants by analyzing its own usage. The extent of such disclosures, once again, must factored into the assessment of security and privacy in the cloud (Burton et al., 2010).

Therefore, the traditional assessments developed for conventional IT environments do not readily fit the dynamic nature of clouds. Hence, the introduction of cloud specific security assessment methodology has significant importance and scope.

1.5 Problem Statement

Cloud computing offers a new economic model which enables enterprises to shift from the conventional way of developing their own IT departments to outsourcing their needs of software, platform and infrastructure by enabling selling and sharing resources altogether while the infrastructure is transparent to both the users and programmers (Khan et al., 2012). Despite of all these considerations, cloud raises severe security risk where the day-to-day interactions between cloud users and providers, as well as between providers themselves needing for high level of trust (Fit´o et al., 2010). While creating a zero risk service is impractical, if not impossible, assessing security risk of cloud-based solutions is important to establish trust and to increase the level of confidence of cloud service consumers, on one side, and the cost effective and reliable service and infrastructure of cloud providers on the other (Alturkistani & Emam, 2014).

However, for cloud computing, the risk assessment becomes more complex as there are several issues that likely to emerge (Drissi et al., 2013). Therefore, the traditional assessments developed for conventional IT environments do not readily fit the dynamic nature of clouds where Cloud computing provides opportunity to dynamically scale the computing resources for applications and end-users can arrive and leave the cloud at any time.

However, there are significant shortcomings in the area of security and risk assessment and mitigation although there are several studies which have been conducted to improve traditional security assessment techniques and present new paradigms for analysing and evaluating security risks in cloud environment. Therefore, security risk assessment in cloud still constitutes a challenging domain and a growing area of research (Subashini & Kavitha, 2011).

This research will focus on **Software as a Service (SaaS) mode**l because the SaaS providers are completely responsible for deploying and managing the IT infrastructure and processes required to run and manage the full solution and to deliver reliable, secure and cost effective services according to requirements of their customers at the proper cost of resources. Moreover, in this scenario, potentially sensitive data are entrusted to the provider, and SaaS customers need reassurances that their data are secure and accessible while residing in the provider's IS

infrastructure. As well as, the fact that the SaaS application resides on, and is accessed, via the open Internet, creates a plethora of security and continuity risks.

Therefore, there is a strong worry about insider breaches, along with vulnerabilities in the applications and systems' availability that could lead to loss of sensitive data and money. Consequently, addressing enterprise security concerns has emerged as the biggest challenge for the adoption of SaaS applications in the cloud. However, such challenges can dissuade enterprises from adopting SaaS applications within the cloud (Subashini & Kavitha, 2011). Therefore, to overcome the customer concerns about application and data security, the provider must address these issues and should stop any data breach as quickly as possible, restore secure access to the service as soon as possible, apply best practice to ensure that it does not recur. However, the identification and evaluation of all risks is a critical task where a risk is composed of a threat, a probability and an impact. However, it is a challenge to the SaaS provider to be able to assess the likelihood and impact of attacks depending on the currently active components of a service with the given the information about them and their interactions. Therefore, there is a need to integrate the cloud computing environment with tools and method that enable the cloud provider to calculate risk factor depending on the given information in order to prioritize issues to take suitable responses to ensure that security and control processes are functioning as intended, identify unanticipated vulnerabilities, and take actions to close them. However, all this will increase the likelihood an organization will use cloud computing and this lead to increase cloud adoption.

1.6 Research Objectives

This research have the following objectives:

1. Develop and specify the framework for security risk assessment based on industry standards.
2. Propose a methodology for security risk assessment of cloud SaaS application that enables SaaS providers to assess security risk for events using a use case scenario of the system.
3. Use commercial or open source tools to support the proposed methodology.

1.7 Research Questions

1. What is the risk assessment framework that is suitable to cloud environments for SaaS providers?

A Framework is a general guideline that an organization can adopt. 'standard' usually refers to something (documents) a professional organization establishes for others to use (Ajam, 2013).

Risk assessment framework is procedures for the tasks of identifying, analyzing, evaluating, treating and monitoring risk. There are several risk assessment frameworks that are accepted as industry standards-'standard' usually refers to something (documents) a professional organization establishes for others to use- including:

- Risk Management Guide for Information Technology Systems (NIST guide) from the National Institute of Standards.
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) from the Computer Emergency Readiness Team.
- Control Objectives for Information and related Technology (COBIT) from the Information Systems Audit and Control Association (Rouse, 2010).

To create a risk management framework, an organization can use or modify the NIST guide, OCTAVE or COBIT or create a framework in-house that fits the organization's business requirements (Rouse, 2010). Therefore, we have to select the suitable standard that can be modified in some of its application to suit the cloud computing environment.

2. How to calculate impact and likelihood of the risk quantitatively?

In General, risk is presented as a probability of an event and its impact or a consequence of the event when a threat was materialized. Therefore, we have to determine how to calculate them.

3. How to evaluate the proposed risk assessment methodology?

A methodology means there has to be a certain way of doing something; like systematic process (Ajam, 2013). Risk will be assessed and rated based on the risk rating methodology. There are many methods proposed for assessing a security risk for the cloud computing environment. Therefore, we have to evaluate the

methodology we propose to explain the efficiency of it. To achieve this step we will compare the proposed method with methods in the literature. Furthermore, we will use case study to explain the efficiency of the proposed method.

1.8 Research Scope

In this research we will focus on public cloud computing since private cloud are considered more secure than public cloud. Moreover, most information found during the research is related to either public cloud computing or cloud computing .

In public cloud all delivery models offered on demand over the Internet in a pay-as-you-go model. Software as a service (SaaS) is one of these delivery model; it is the most mature category of cloud service, since it evolved from the application service-provider model of software hosting.

The opportunistic use of SaaS has yielded benefits such as cost savings, improved agility, and faster time-to-market, as well as increased flexibility in scaling to support more users as necessary. It has also provided a venue for experimenting with new capabilities. The following examples *-illustrate different use for software-as-a-service :

1. Suite of SaaS business applications for accounting, human resources and more offered by Oracle.
2. Mobile services which enable mobile access to applications and information to facilitate for mobile users to take full advantage of cloud computing.
3. Internet of Things (IOT) in order to fulfil various goals such as intelligent home and remote health-care in a more cost effective way.

Moreover, a survey of 600 enterprises by Enterprise Strategy Group 2012 indicates that SaaS use is bound to continue rising. In this survey, 46% of these enterprises currently use it, 17% do not use it but plan to use it, 21% do not use nor plan to use it but were interested to-to do so, 14% neither use, plan nor interested in it and 1% was not clear (López et al., 2013).

However, security is one of the most important concerns of SaaS. In a survey, 51% of the people thought security was the biggest concern . Therefore, security concerns are the most commonly cited reason why enterprises are not interested in SaaS (Subashini & Kavitha, 2011). Consequently, in order to build, trust cloud

computing provider need to be able to address the different risks associated with cloud computing security.

Therefore, in this thesis we will focus on security risk assessment by the cloud provider in SaaS model because in SaaS the infrastructure, software and data are primarily the responsibility of the provider and the consumer has little control over any of these features of the service.

Focusing on the cloud provider security risk assessment for PaaS and IaaS deployment models, and security risk assessment by cloud costumer is beyond the scope of this research.

1.9 Research Methodology

In order to successfully address the risk in cloud computing environment, the cloud provider system must contain components such as physical security system, antivirus, SIEM (i.e. Security Information and Event Management, which offers features such as log management, compliance reporting, real-time monitoring and incident management), vulnerability assessment (VA) tools and IDS/IPS (Intrusion Detection/Prevention Systems). These components will collect and correlate events in order to trace malicious activity continuously to feeds the dynamic risk assessment method with continuous inputs about security status. Then, the cloud provider should be able to calculate the risk factor dynamically through the two risk factors, the impact and likelihood. According to NIST in (National Institute of Standards and Technology, 2012) where the risk is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Therefore, in this research we will:

1. Propose a methodology using existing open source or commercial tools for software modelling and analysis to enable the SaaS providers to calculate security risk interactively depending on the given input. The methodology will be based on sequence diagrams of the intended scenarios.

2. Validate the proposed methodology using case studies and compare it with related works.

1.10 Research Hypothesis

This research assumes the following:

1. The Information security risks are those risks that reflect the potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation (National Institute of Standards and Technology, 2012).

2. SaaS provider should analyze threats and vulnerabilities to calculate risk of security events and assess the affect of security control in mitigating the risk .

3. The proposed method will enable the SaaS providers to calculate the security risk factor precisely and dynamically for the certain use case scenario of the system and conduct sensitivity analysis to calculate impact without expert intervention.

1.11 Structure of the Thesis

This thesis organized as follows: chapter 1 is the introduction, chapter2 present the literature review, chapter 3 introduce the proposed method, Chapter 4 present case studies, Chapter 5 present discussion and comparison. Finally, Chapter 6 conclusion and future work.

CHAPTER 2
RELATED WORK

Chapter 2: Related work

2.1 Introduction

This review, covers the related work in section 2.1. In Section 2.2 A classification of cloud-based security risk assessment methods and tools will be introduced. Section 2.3 will discuss the open issue directions.

2.2 Related work

2.2.1 Cloud Computing: Benefits, Risks and Recommendations For Information Security

Catteddu & Hogben (2009) in the European Network and Information Security Agency (ENISA) report provided an approach for risk assessment based on the estimation of risk levels on ISO/IEC 27005:2008. Security risk would be high if both the probability of the event and its impact are high. Risks are categorized into three groups: policy and organizational risks, technical risks and legal risks. The assessment provided is semi-quantitative, as it uses value ranges for both event probability and impact, but does not consider their combined influence in a quantitative manner. Instead, the final risk assignment (as High, Medium or Low) is based on expert opinion, which takes the two factors into consideration. For example, risk due to vendor lock in is assessed to be High, because its probability is high, but impact is Medium. Loss of Governance is shown as a risk with both high probability and high impact, and hence a 'very high risk' (Catteddu & Hogben, 2009).

A fully quantitative risk assessment framework would further improve this methodology, because it enables the stakeholders to comparatively evaluate the risks involved and protection measures (Catteddu & Hogben, 2009).

2.2.2 Toward Risk Assessment as a Service in Cloud Environments

Burton et al. (2010) introducing risk assessment as a service. They contend that the way that cloud computing should be assessed, is the same as the way cloud computing is delivering: *as a service*. Indeed, the same characteristics of the cloud that makes it hard to assess with existing tools, also make it easy to assess with new

ones, especially the metering that is already built in for billing and service-level assurance (Burton et al., 2010).

Risk assessment as a service is a new paradigm for measuring risk as an autonomic method that follows the on-demand, automated, multi-tenant architecture of the cloud – a way to get a continuous "risk score" of the cloud environment with respect to a given tenant, a specific application, or more generally, for use by new tenants and applications. They envision such assessments as being made available in real-time by one or more of the entities in the cloud ecosystem. For instance, a cloud provider could perform continuous self-assessments as a best practice through evaluation of its own run-time environment; a trusted third party could assess the provider on an ongoing basis through privileged access to certain internal measurement interfaces; or a consumer could assess the provider through non-privileged access (Burton et al., 2010).

In each case, the dynamic assessment service would rest on a foundation periodic, underlying, static assessments. Static assessments should focus on the elements of the provider's underlying IT infrastructure and governance that (a) changes infrequently and (b) drives security in the dynamic environment. This point to the importance of assessing security policies, policy enforcement mechanisms, and policy compliance mechanisms. Since a provider may itself be a consumer of services from other providers, it is reasonable to expect that a provider would also be assessing the providers it relies on, thus addressing the point about the recursive nature of cloud computing. Indeed, even if the ultimate business consumers and their customers are not directly assessing providers, the providers themselves will likely be assessing one another. The addition of real-time assessment capabilities into the cloud environments parallels managed security services whereby an external provider monitors the internal security of a conventional data center. The results of such services kept confidential to the relevant organization. In the cloud, the comparable results would be like the cloud itself, open to all consumers. An assessment service for the cloud involves more than just the automation of traditional surveys and scoring systems. The metrics must also be adapted to the nature of cloud computing, for instance the dynamic allocation of resources and multi-tenancy. Updating a traditional assessment to address cloud characteristics, then applying it manually, although accurate in principle, still may not fit the dynamic nature of the

new environment. Rather, the “new wine” of cloud risk assessment should put into the “new wineskin” of a cloud service (Burton et al., 2010).

They proposed a cloud-based assessment as a service paradigm as a promising alternative. However, they didn’t implement such a service but rather offer it as a paradigm to be followed (Burton et al., 2010). As well as they don’t suggest method to calculate risk score.

2.2.3 Towards Analyzing Data Security Risks in Cloud Computing Environments

(Sangroya et al., 2010) present a risk analysis approach that can be primarily used by the perspective cloud users before putting their confidential data into a cloud.

Their approach aim to build a better trust mechanism between the cloud service provider and users. It is based on the idea of trust model, principally used in distributed information systems. They extend the general idea of trust management and present its use in analyzing the data security risks in cloud computing.

They build a trust matrix to analyze the data risk. To build the trust matrix, a number of heuristics can be used for selecting the security parameters. They select following two trust variables to build the trust matrix:

(a) Data Cost:

Where, data can be assigned a cost by the users based on the criticality of the data and the data criticality needs to be computed by the service.

(b) Provider’s History:

Where, service provider history includes a provider’s profile of past services. If users are dissatisfied with a particular service, they can record their experience. If a service provider do not possess a good history of data security then it may also decrease the trust factor.

However, other variables can also be used for building the trust matrix such as Service Cost, Monitoring support etc.

Along with trust variables, few parameters used in measuring trust can be applied to fine-tune these trust variables. The parameter, which they choose in this category, are Data Location such that data located at the sites, which are

geographically or politically sensitive, would likely to have lower trust than other locations.

Figure 2.1 represents an example trust matrix with area representing the Low Risk/High Trust zone and, High Risk/Low Trust zone where x-axis represents the data cost, y-axis represents the service provider's history and z-axis represents the data location.

Of course, it is clear now that a high data cost with poor service provider history combining with a very sensitive location will result in a higher risk/lower trust. High trust zone signifies the region of high trust. It can specify the security risk for the current transactions and for future transactions with that service provider. Similarly, low trust zone signifies the region of low trust (Sangroya et al., 2010).

As a risk preventive approach, they also define here a trust action, which can be taken as part of a preventive or reactive measure.

The variables have been defined in this method can be used where there are some past statistics about the service provider. The method has been used to measure the trust and will be used for all future transactions. Based on this method, we were able to define the trust actions, for all future transactions with the service provider.
The most obvious finding to emerge from this study is that, there is a need of better trust management framework and there is a lack of structured analysis approaches that can be used for risk analysis in cloud computing environments. The approach suggested in (Sangroya et al., 2010) is a first step towards analyzing data security risks it is easily adaptable for automation of risk analysis.

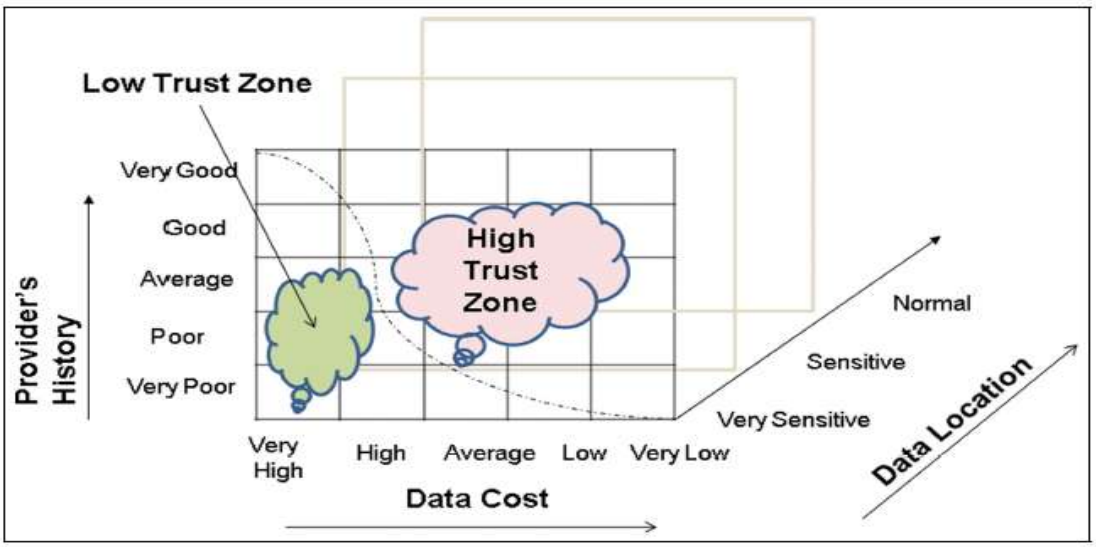


Figure 2. 1: A Trust Matrix for Risk Analysis (Sangroya et al., 2010)

2.2.4 Information Security Risk Management Framework for the Cloud Computing Environments

Zhang et al. (2010) present information risk management framework that provide better understanding for critical areas of focus in cloud computing environment, to identifying a threat and identifying vulnerability. It is covering all of cloud service models and cloud deployment models. Cloud provider can be applied this framework to organizations to do risk mitigation. This framework was developed in a standard quality management (or Plan, Do, Check, Act) cycle of continuous improvement. The framework was to describe critical areas of focus in cloud computing that should be protect and designed to protect the confidentiality, integrity and availability of information assets. The framework have seven processes, including: processes-selecting relevant critical areas, strategy and planning, risk analysis, risk assessment, risk mitigation, assessing and monitoring program, and risk management review. Where Risk assessment is the determination of quantitative or qualitative an output from risk analysis process. This step have four major processes:

- Likelihood Determination: To derive an overall likelihood rating that indicates the probability vulnerability may be exercised within the construct of the associated threat environment. The likelihood that a potential vulnerability could be exercised by a given threat-source can be describe as high, medium, low. The output from likelihood determination step is likelihood rating. Table 2.1 explained this (Zhang et al., 2010).

Table 2. 1: Likelihood Definitions (Zhang et al., 2010)

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

- Impact Analysis: The step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of vulnerability. The adverse impact of a security event can be described in terms of loss or degradation of any, or combination of any, of the following three security goals: integrity, availability, and confidentiality that can be describes qualitative categories as high, medium, low (Zhang et al., 2010). Table 2.2 explained this.

Table 2. 2: Magnitude of Impact Definitions (Zhang et al., 2010)

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

- Risk Determination: The purpose of this step is to find the risks and opportunities that impact of critical area's risk that selected in Selecting Critical Area step. The sample matrix derived in Table 2.3 shows how the overall risk levels of High, Medium, and Low are derived. The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level (Zhang et al., 2010).

Table 2.4 describes the risk levels shown in the above matrix. This risk scale, with its rating of High, Medium, and Low, represents the degree of level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level. Output from this step is risk level (High, Medium, or Low).

Table 2. 3: Risk Determination – risk level (Zhang et al., 2010).

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low 10 x 1.0 = 10	Medium 50 x 1.0 = 50	High 100 x 1.0 = 100
Medium (0.5)	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	High 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 = 1	Medium 50 x 0.1 = 5	High 100 x 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

Table 2. 4: Risk Scale and Necessary Actions (Zhang et al., 2010).

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be out in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA (Designated Approving Authority) must determine whether corrective actions are still required of decide to accept the risk.

- Control Recommendations. - During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operation are provided. The goal of the recommend controls is to reduce the level of risk to cloud computing environment and its data to an acceptable level (Zhang et al., 2010).

However, the risk assessment in this paper is not quantitative.

2.2.5 QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security

Saripalli & Walters (2010) present a Quantitative risk and impact assessment framework (QUIRC), to assess the security risks associated with cloud computing platforms. This come in response to the U. S. Federal Information Security Management Act (FISMA) of 2002, where the Federal Information Processing Standards (FIPS) proposed confidentiality, integrity, availability, authenticity and accountability as the key principles of information security. Further, proportionality as a security principle implies that security controls should be proportional to the risks of modification, denial of use, or disclosure of the information (Saripalli & Walters, 2010).

This approach allows categorization of the security risks and impacts by Security Objectives (SO) that set based on the potential impact on an organization when faced with attack events that may threaten the information and information systems. Such impact assessed in terms of the organization's ability to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. FIPS recommended that the security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization (Saripalli & Walters, 2010).

They propose six Security Objectives: three security objectives for information and information systems (Confidentiality, Integrity and Availability), three requirements unique to cloud platforms (multi-party trust considerations, mutual auditability and Usability). These six Security Objectives for the cloud platforms may be referred to as the CIAMAU framework (Saripalli & Walters, 2010).

STRIDE may be considered an alternative to the Security Objectives based CIAMAU categorization. For the purposes of QUIRC analysis, any one such categorization is sufficient. Table 2.5 illustrates the STRIDE threat events mapped to one or more of the 6 Security Objectives (SO), shown within square brackets [ ]. This is not an exact correspondence between the STRIDE and CIAMAU frameworks. While STRIDE is a well-tested framework for traditional software systems, a framework such as the CIAMAU, which explicitly includes the cloud-specific Security Objectives, would be more appropriate for cloud security risk assessment.

Security architects may also device their own alternative SO frameworks. QUIRC methodology would work with any such framework, by assigning relative weights of importance to each SO category (Saripalli & Walters, 2010).

They define a risk as a product of the Probability (*Pe*) of a security compromise, i.e. a threat event, *e*, occurring and its potential Impact or Consequence (*Ie*) (Saripalli & Walters, 2010):

$$R_e = P_e I_e$$

Pe typically is a fraction less than one, whereas *Ie* may be assigned a value on a numerical scale. They propose these ranges for Impact (*Ie*): LOW (1-5); MODERATE (6-10); HIGH (11-15). These values are relative, and may be amplified depending on the required granularity for the visualization of risk metrics (Saripalli & Walters, 2010).

Table 2. 5: Correspondence between STRIDE and SO models

(Saripalli & Walters, 2010)

THREAT	EXAMPLE
Spoofing: adversary poses as a user or entity with an identity. [CONFIDENTIALITY]	Illegally using another user's authentication information, such as username and password.
Tampering: modification of data to achieve a malicious goal. [INTEGRITY]	Unauthorized changes to persistent data, or alteration of data over a network.
Repudiation: ability to deny a malicious action lacking proof. [AUDITABILITY]	User performs an illegal operation in a system that lacks the ability to trace it.
Information Disclosure: exposure of protected data to adversary. [CONFIDENTIALITY]	A cloud user reads a file from a co-tenant's workflow, without permission.
Denial of Service: adversary gains a higher trust level and attacks. [AVAILABILITY]	An adversary gains control of a tenant's VM, and makes another's Web server unavailable.
Elevation of Privilege: unprivileged user gains privileged access. [CONFIDENTIALITY]	An attacker penetrates all system defense to join the trusted system itself

They propose the following impact definitions for the security of cloud platforms. The potential impact is LOW if the loss of confidentiality, integrity, availability, mutual trust or mutual auditability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. The potential impact is MODERATE if loss of confidentiality, integrity, availability, mutual trust or mutual auditability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. The potential impact is HIGH if the loss of confidentiality, integrity, availability, mutual trust or mutual auditability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individual. These definitions are based heavily on the FIPS descriptions, with appropriate modifications for the cloud applications.

Security risk under each CIAMAU category is assessed, and the overall platform security risk for the given application under a given category (*Rs*) would be average over the cumulative, weighted sum of *n* threats that map to that SO category (Saripalli & Walters, 2010):

$$R_s = \frac{1}{n}\sum_{i=1}^{n} P_e I_e$$

It is also necessary to assign a weight for each of the SO categories, such that their sum always adds up to 1. This weight, *ws*, represents the relative importance of a given SO to a particular organization and/or business vertical. Then, Net Security Risk (R) to the application integrated over the six CIAMAU objectives is a weighted average:

$$R = \sum_{s=1}^{6} w_s R_s$$

Where w_S is the relative weight assigned to an SO category s. Evaluation of the probabilities of several threat events currently is difficult, due to a lack of historic data. A more accurate assessment of probabilities will be business and application specific, based on characterization data from actual incidence of security compromise events. Once the probability of occurrence of all such events is calculated, risk (R) can be calculated as explained. Such calculations are useful in

identifying the high-risk threats, and investigating them in greater detail (Saripalli & Walters, 2010) .

Advantages of the QUIRC methodology are as follows. A quantitative approach gives vendors, customers and regulation agencies the ability to comparatively assess the relative robustness of different cloud vendor offerings and approaches in a defensible manner. It also can be helpful in alleviating the considerable FUD (Fear, Uncertainty and Doubt) associated with cloud platform security issues and helping that they are dealing in an effective way (Saripalli & Walters, 2010).

However, Limitations of the approach include that it requires the meticulous collection of input data for Probabilities of events, which requires collective industry SME inputs (Saripalli & Walters, 2010). Moreover, this framework does not cover risks during all the stages of the lifecycle of the service when it exists on the cloud (Sen, 2016). A fully quantitative risk assessment framework would further improve this methodology. In general, there is lack of structured analysis approaches that can be uses for risk analysis in cloud computing environments (Drissi et al., 2013).

2.2.6 Security Risks and their Management in Cloud Computing

Khan et al. (2012) presents a paper that investigates the security challenges posed by the transparency of distribution, abstraction of configuration and automation of services by performing a detailed threat analysis of cloud computing across its different deployment scenarios (private, bursting, federation or multi-clouds). This paper also presents a risk inventory, which documents the security threats identified in terms of availability, integrity and confidentiality for cloud infrastructures in detail for future security risks. They also propose a methodology for performing security risk assessment for cloud computing architectures presenting some of the initial results. They consider the deployment and operation stages in the cloud lifecycle. Deployment stage where the initial placement of services on cloud providers, and the service operation stage where cloud resources and data managed by the cloud provider to fulfill the Service Level Objectives (Khan et al., 2012).

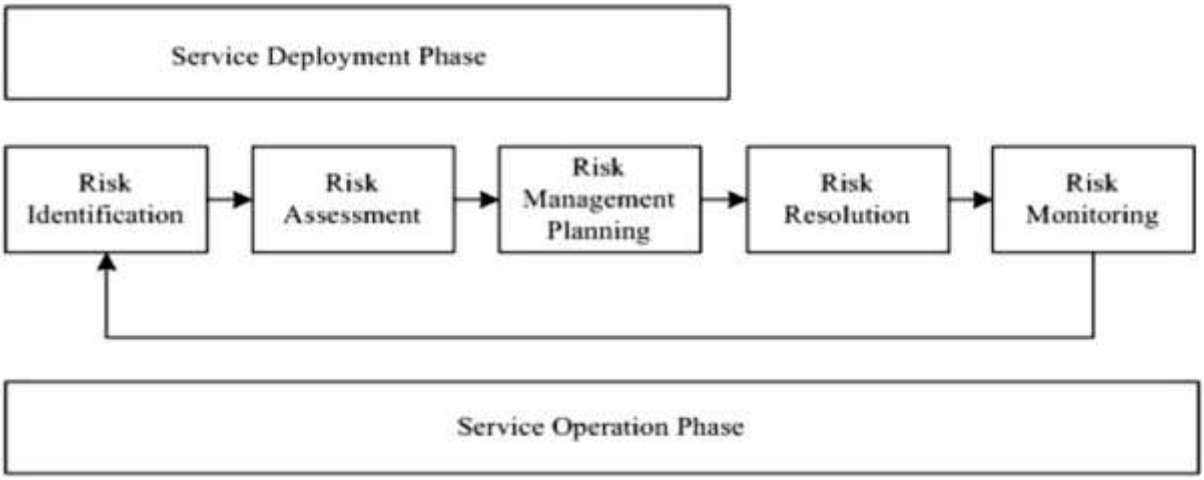


Figure 2. 2: Risk assessment lifecycle during service deployment/operation

(Khan et al., 2012)

A number of stages have identified for performing a complete risk assessment on clouds by considering core risk assessment approaches as explained below (Khan et al., 2012) :

A. High level analysis of the system

An initial high-level analysis of the deployment scenarios helps identifying the actions and assets involved at the different stages in the cloud. This helps isolate the assets involved and how they change over time to identify the vulnerabilities of the cloud environment. Generally, security needs to be assessed before deployment of the service to check for security concerns of the other provider or if service level agreements (SLAs) demand certain security aspects to be met (Figure 2.2). During the operation, security concerns monitored while the service is executing (Khan et al., 2012).

B. Identifying the assets involved

There are various assets involved either at the deployment or operation stage such as the SLA or customer data. These can be monitor in relation to the specific threats in the environment (Khan et al., 2012).

C. Identify the threats in each cloud deployment scenario

In which threats and vulnerabilities of a system can be identified. To do this they coupled information risk analysis methodology with the threat and vulnerability assessment tool (T&VA) which provides a standard list of threats relating to IT systems, then adopting the threats relevant to the cloud deployment scenarios being investigated. In addition to other threats that have been added to introduce the

differences between cloud computing and other forms of distributed computing. These listed in Table 2.6 (Khan et al., 2012).

Table 2. 6: Threats identified in the various use cases and their details (Khan et al., 2012)

Threat category	**Threats (threat id) {Threat classification – Availability (A) confidentiality (C) Integrity (I)}**	**Stage of cloud (Deployment/Operation)**	**Assets involved**	**Priority (1 is low , 5 is high)**	**Likelihood(1 is low, 5 is high)**
External attacks	Carrying out of Dos (Denial of Service) attack (T1) {A}	Operation	Customer data, infrastructure of the provider	4	3
	Hacking (T2) {I,C}	Operation	Customer data or service	3	1
	Undertaking malicious probes or scans (T3) {I,C}	Operation	Hypervisor code	4	2
	Cracking password (T4) {A, I, C}	Operation	Customer data or service	3	1
	Cracking Keys (T5) {A,I,C}	Operation	Customer data or service	3	1
	Spoofing user identities (T8) {A,C}	Operation	Customer data or service, all services	3	1
	Modifying network traffic (T9) {I}	Operation	Software, connections, service (runtime)	2	2
	Eavesdropping (T10) {I,C}	Operation	Software, connections, service (runtime)	2	1
	Distributing computer viruses (T11) {I}	Operation	Software, connections, service	3	1
	Introducing Trojan horses (T12) {I}	Operation	Software, connections, service	3	1
	Introducing malicious code (T13) {C}	Deployment and Operation	Software, connections, service	3	3
	Distributing Spam (T15) {A}	Deployment and Operation	Mailing lists	1	4
Theft	Gaining unauthorized access to system or networks (T16)	Operation	Customer data or	5	4

	{A,I,C}		service		
	Theft of business information (T27) {A,C}	Operation	Customer data	4	2
	Theft of computer equipment(T29) {A,C}	Operation	Customer data	1	2
System malfunction	Malfunction of software (T34) {I}	Operation	Toolkit, all services	1	4
	Malfunction of computer network equipment (T35) {I}	Operation	Toolkit, all services	1	5
Service interruption	Natural disaster (T40) { I }	Deployment / Operation	Customer data	1	3
	System overload (T41) {A,C}	Operation	Customer data	4	3
Human error	User error (T42) {C}	Deployment / Operation	Data	5	3
System specific threats and abuse	Data Leakage (T50) {I,C}	Operation	Data	5	3
	Usage control (T51)	Operation			
	Hypervisor level attacks (T52) {A}	Operation	Data	3	2
	Data ownership (T53) {I}	Deployment	Data		2
	Data exit rights (T54) {I,C}	Deployment	Data, SLA	4	3
	Isolation of Tenant application (T55) { I,C}	Deployment and Operation	Data	5	2
	Data encryption (T56) {A,I,C}	Operation	Data	5	3
	Data Segregation(T57) {A,I }	Operation	Data, programs	4	2
	Tracking and reporting service effectiveness (T58) {A,I }	Operation	Data, Hosted VMs	5	3
	Compliance with laws and regulation(T59) {A,I }	Deployment and Operation	Data	3	2
	Use of validated products meeting standards (T60) {A,I }	Operation	Data	3	3
	Guest virtual machines (T61) {A, I }	Operation	Data	1	3

D. High-level analysis of each threat

Each of the threats can be further analyzed in terms of who causes them and the incidents leading up to them, which can then prioritized depending on this information. This also helps measure the impact of the security risk on the service and the providers (Khan et al., 2012).

E. Risk Evaluation

Depending on the priority of the assets and likelihoods of the threats occurring, the threat items can be plotted into an evaluation matrix to document their occurrences. Table 2.7 depicts this in relation to the threats identified in Table 2.6 (Khan et al., 2012) .

Table 2. 7: Risk evaluation matrix (Khan et al., 2012).

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Rare	T40	T10	T2,T4,T5,T8, T11, T12		
	Unlikely	T29	T9		T3,T27	
	Possible	T41		T13	T1,T50	T51, T52
	Likely	T15,T34				T16
	Certain	T35				

The impact also denotes the affect the threat will have on the business such as loss of confidentiality can cause loss in trust having the highest impact (Table 2.8) (Khan et al., 2012).

Threats belonging to confidentiality are classed as high because these have severe effect on trust and the provider's image. Loss of confidentiality can also convert low threats like theft of information to very high. For instance losing unencrypted data is a more severe risk compared to loss of encrypted data. Loss of availability is relatively classified as medium compared to loss of confidentiality. This is because enterprises are better off using infrastructure provider’s resources rather than deploying their own because of the investment involved. Integrity classed as low because relative to confidentiality and availability the impact is much lower. Loss of

integrity can be because of software error, user error, and equipment failure and due to an adversary changing data (Khan et al., 2012).

Table 2. 8: Range of threats for Confidentiality, Availability and Integrity

(Khan et al., 2012)

		Likelihood rating				
Business impact rating		Very Low	Low	Medium	High	Very High
	Very High					
	High	Confidentiality				
	Medium	Availability				
	Low	Integrity				
	Very Low					

F. Risk Treatment

Once evaluated, the risk mitigation strategies can be generated in terms of the actions taken to resolve them. These can be to accept, treat or outsource the risk.

At the deployment stage, the risk assessment tool will read inputs from the risk inventory, which documents all the threats, the vulnerabilities, assets affected and their likelihoods. The risk inventory is based on the threats collected in table 2.6. Based on this information, security risk can be calculate as:

1. Calculate the number of threats recorded at deployment stage and use case.
2. For each threat:
    a. probability of likelihood given asset affected (p(B|A)) = likelihood/ 5.0
    b. probability of asset priority (p(A)) = priority/5.0
    c. probability of likelihood regardless of asset (p(B))= p(B|A) * p(A) + p(A') *1
    d. probability of threat occurring (p(A|B)) = ((p(B|A) * p(A))) / p(B)

3. Security risk = Sum all probabilities of threats occurring / threats found (Khan et al., 2012).

Based on rules of Bayesian dependencies, the probability of each threat affecting the particular assets can be calculate before making the decision to accept the service by the IP (Khan et al., 2012).

However, at the operation stage, along with the calculated security risk for this stage, the risk assessment tool will be interacting with the monitoring database and additional tools like the network and historical database to monitor if certain threats are becoming live. The stages 1-2 are similar to the deployment stage but in addition, new stages added for operation phase. The historical database can contain details of previously recorded threats that have occurred in the past. The network can include intrusion detection systems and logs that can be parse to find out if certain events have been recorded (Khan et al., 2012).

3. Security risk = Sum all probabilities of threats occurring / threats found

4. For each threat to be monitored:

    4a. Read monitoring inputs

    4b. If (event found==true) count ++

5. Calculate total_event_rate= events_found/ total monitored time

6. Relative risk (RR) = total_event_rate/ security risk

7. If RR=1 do nothing, RR<1 accept risk, If RR>1 apply mitigation strategy (Khan et al., 2012).

Depending on the value of relative risk (RR), the components can make a decision whether to accept or apply a mitigation strategy stored in the risk inventory to compensate for the risk (Khan et al., 2012).

However, they consider the three security requirement for information systems (Confidentiality, Integrity and Availability), but they do not consider other security requirements that unique to cloud platforms such as (multi-party trust considerations, mutual auditability and Usability).

They future work includes testing this system on a cloud platform with monitoring agents installed which will log certain threats when they occur. This will then be extended to work on determine threats which may be eventually seen based on the data being collected and difficult to determine directly from the events (Khan et al., 2012) .

2.2.7 A New Shared and Comprehensive Tool of Cloud Computing Security Risk Assessment

Drissi et al (2015) proposed a new risk assessment method in which the measure of an IT risk can be determined as a product of threat, vulnerability and asset values. Where the asset value of each cloud actor is the average of the weight of confidentiality, availability and integrity ; the vulnerabilities value for each cloud actor specified basing on the absence or ineffectiveness of controls; threat value is calculated as product of probability of occurrence and the impact where each threats is mapped to indicative number of vulnerabilities and assets. However, the risk value will be depend on the actor and their corresponding assets, their security objectives and their corresponding vulnerabilities. To improve the architecture and consolidate the security risk assessment for cloud computing multi-agent systems can be used. (Drissi et al., 2015).

2.2.8 A Risk Management Framework for Cloud Migration Decision Support

Islam et al (2017) presents a risk management framework that enables users to identify risks, based on the relative importance of the migration goals for specific migration scenarios and analyzed the risks with a semi-quantitative approach. They use the analytic hierarchy process (AHP) where each goal is compared with the other goals based on its importance level within the organizational context for the cloud migration. The net risk calculation depends on the associated risk factor values. Each risk factor value is estimated through the product of its probability and impact of overall risk. However, they use subjective judgment depending on individual perception for probability definition and impact values. The risk value is obtained by averaging the risk factors' values. Finally, the net risk level is the sum product of risk level and relative importance of affected migration goal. However, if the number of goals were to increase, the net risk level estimation would be more complex (Islam et al., 2017). They are currently working on defining a guideline for risk management activities along with a checklist so that the framework could provide better hands-on support to potential cloud users. They are also planning to develop migration goals and a risk taxonomy and integrate it with the guidelines.

In table 2.9 those related work are summarized with the technique suggested therein, their problems and the model or tool proposed in it. However, Burton et al. (2010) just present a paradigm to be followed. Catteddu & Hogben (2009) present semi-quantitative method. Zhang et al. (2010) framework is not quantitative. Sangroya et al. (2010) approach need past statistics about the service provider. Saripalli & Walters (2010) framework does not cover risks during all the stages of the lifecycle of the service when it exists on the cloud. Khan et al. (2012) do not consider other security requirements that are unique to cloud platforms. In Drissi et al. (2015) the risk value will be depend on the actor. Islam et al. (2017) use subjective judgment depending on individual perception for probability definition and impact values. Moreover, none of them are dynamic to fit the dynamic nature of the cloud computing environment.

Table 2. 9: Summary of the related works.

Lit. Ref	**Context of Research**	**Technique Used**	**Problems**	**Model/ Tool/ Proposed**
(Catteddu & Hogben, 2009)	Security risk assessment method for cloud computing	Likelihood of an incident scenario, mapped against the estimated negative impact.	-Semi-quantitative. -The estimation of risk levels is based on ISO/IEC 27005.	-Framework include additional standards. -Set of assurance criteria designed to assess the risk of adopting cloud services. - A fully quantitative risk assessment framework (Alturkistani & Emam, 2014)

(Sangroya et al., 2010)	Risk analysis approach that can be primarily used by the perspective cloud users.	Build a trust matrix to analyze the data risk.	- The variables have been defined in this method can be used where there are some past statistics about the service provider. - A lack of structured analysis approaches that can be used for risk analysis in cloud computing.	Better trust management framework.
(Zhang et al., 2010)	Information risk management framework	The Risk assessment step have four major processes (Likelihood Determination, Impact Analysis, Risk Determination according to Risk Scale, and Control Recommendations).	Risk assessment in this paper is not quantitative.	-

(Saripalli & Walters , 2010)	Quantitative risk and impact assessment framework (QUIRC)	Security risk under each Security Objective category would be average over the cumulative, weighted sum of n threats that map to that SO category and assign a weight for each of the SO categories. Then, Net Security Risk (R) to the application integrated over the SO is a weighted average.	This framework does not cover risks during all the stages of the cloud lifecycle (López et al., 2013)	-
(Burton et al., 2010)	Risk assessment as a service	It is a paradigm to be followed.	No implementation as well as there are no method suggested to calculate risk score.	The dynamic assessment service
(Khan et al.,2012)	Methodology for performing security risk assessment for cloud computing architectures.	A number of stages have identified for performing a complete risk assessment (High level analysis of the system, Identifying the assets involved, Identify the threats in each cloud deployment scenario, High-level	They consider the three security requirement for information systems but they do not consider other security requirements that unique to cloud platforms.	Testing this system on a cloud platform with monitoring agents installed which will log certain threats when they occur.

		analysis of each threat, Risk Evaluation using evaluation matrix, and Risk Treatment).		
(Saadia et al., 2015)	Comprehensive and shared risk assessment method for cloud computing	Risk determined as a product of threat, vulnerability and asset values.	The risk value will be depend on the actor and their corresponding assets, their security objectives and their corresponding vulnerabilities.	-Use Multi-agent systems to improve the architecture and consolidate the security risk assessment for cloud computing.
(Shareeful et al, 2017)	A risk management framework for cloud migration decision support	Identify risks based on the relative importance of the migration goals for specific migration scenarios and analyzed the risks with a semi-quantitative approach.	Risks based on the relative importance of the migration goals.	- Guideline for risk management activities along with a checklist. - Develop migration goals and a risk taxonomy and integrate it with the guidelines.

2.3 A Classification of Cloud-based Security Risk Assessment Methods and Tools

Alturkistani & Emam in (2014) presents a review of the security risk assessment methods in cloud computing. They present a classification of cloud-based security risk assessment methods and tools as follow:

1) Risk assessment as a service: It is available in real-time by one or more of the entities in the cloud. A cloud provider can perform continuous self-assessments as a best practice through evaluation of its own run-time environment (Onwudebelu & Chukuka, 2012).

2) Qualitative and quantitative assessment: Risk assessment have analyzed security risk by using qualitative or/and quantitative approach. However, a simple method for qualitative or quantitative analysis will lead to the inaccuracy and one-sidedness of the evaluation results. In the research article by (Peiyu & Dong., 2011) an integrated method of qualitative and quantitative analysis used to build the assessment model in cloud.

3) Graphs analysis assessment: Graphs and mathematical models can be used to address and calculate security risk in clouds by simulating attacker possibilities. Leitold & Hadarics in 2012 have presented a mathematical model for threats that considers communication in order to identify security risk for individual entities, and then calculates it for a whole enterprise. The model built by representing communications as a directed graph and then established a matrix to discover the risk before finally making a simulation. Furthermore, in another study, Tanimoto et al. (2011) have used a hybrid risk-analysis method based on decision tree analysis (quantities) and risk matrix (qualitative). In this method, risk factor from a user's viewpoint systematically extracted with the Risk Breakdown Structure (RBS) method then analyzed and evaluated. A detailed countermeasure and proposal produced based on these results. The risk matrix method classifies risk into four kinds (Risk Avoidance, Risk Mitigation, Risk Acceptance, and Risk Transference) in accordance with the generation frequency and degree of incidence. The result of risk analysis is well organized and provided in a statistical diagram.

4) Hierarchal assessment: In a research article by Zhang et al. (2012) a hierarchical framework built to analyze the risk and set the goal for the assessment. After that, an

indicator system is built under each principle and sub-indicators introduced for assessment. In addition, another assessment method has been introduced based on an Analytic Hierarchy Process (AHP) model. The assessment model consists of three layers: level one is the problem (assessment of cloud platform), level two is the major factors identified for assessing level one, level three is the lowest level for the concrete assessment factors. AHP carried out using the following three principles: decomposition, pairwise comparison, and synthesis of weights (Peiyu & Dong., 2011).

5) Security matrix assessment: Trust Matrix is a method used for security risk analysis in cloud environments. As well as, Cloud Control Matrix (CCM), which has been release by CSA in 2013, as a baseline security control framework designed to help enterprises assess the risks associated with a cloud provider. It gives a detailed understanding of security concepts and principles that are aligned to the CSA guidance in 13 domains. The CCM has included a risk management domain to ensure that formal risk assessments are aligned with the enterprise-wide framework, planned and scheduled at regular intervals determining the likelihood and impact of identified risks, using qualitative and quantitative methods. Thereby, it facilities transparency and increase trust level between the cloud customer and the cloud in order to make cloud a secure environment to the future of business (Cloud Security Alliance , 2013).

At the end, Alturkistani & Emam (2014) suggests to have a collaborative security risk assessment method that will add great assistance to both service providers and consumers.

2.4 Open Issues

Security risk assessment in clouds is needed for both customers and cloud providers. The security concerns arise from that cloud customers do not see what happens inside a cloud and how their data handled. They have to fully trust the cloud providers to act honestly and not breach the confidentiality of data and computations. On the other hand, cloud providers prefer to hide the cloud topology and operational details. Thus, there is a necessity to balance the opposing needs of the providers and customers (Alturkistani & Emam, 2014). There are many open issues need research to make cloud computing more trustworthy and reliable like the following:

(1) Building distributed, collaborative and intelligent risk assessor that guide customer to evaluate the security level of cloud provider and identify the associated risk before the decision of cloud adoption has been taken.

(2) Designing a mechanism that will allow the cloud provider to prove the confidentiality and integrity of the data and computation without disclosure of sensitive cloud topology information.

(3) Security standards for cloud risk assessment. Security standards are important to measure security risks of cloud providers. Thus, security assessment can give little information unless there is a standard to compare it with (Alturkistani & Emam, 2014).

(4) Risk assessment approach for cloud consumers to check the effectiveness of the current security controls that protect an organization's assets. At present, there is a lack of risk assessment approaches for cloud consumers. A proper risk assessment approach will be of great help to both the service providers and the cloud consumers. With such an approach, the cloud consumers can check the effectiveness of the current security controls that protect an organization's assets and the service providers can maximize and win the trust of their cloud consumers if the level of risk is not high. In addition, the cloud consumers can perform the risk assessment to be aware of the risks and vulnerabilities present in the current cloud computing (Drissi et al., 2013).

(5) Developing a SaaS-specific risk assessment framework to further promote the SaaS adoption process, streamline SaaS provider evaluation, and reduce business risks (Bernard et al., 2011). Since SaaS is rapidly emerging as the dominant delivery model for meeting the needs of enterprise IT services and the biggest challenge be to gain customer's confidence which can be achieved by implementing efficient application-level security mechanism, with proper definition of SLA guarantees .

CHAPTER 3

PROPOSED METHODOLOGY FOR SECURITY RISK ASSESSMENT FOR CLOUD COMPUTING

Chapter 3:Proposed Methodology for Security Risk Assessment for Cloud Computing

3.1 Proposed Method for Security Risk Assessment for Cloud Computing

The proposed methodology is a scenario based methodology for Security Risk Assessment for Cloud Computing. Scenarios is the sequences of actions aimed at accomplishing some task goal (Kaindl, 2011). Scenario-based analysis techniques provide a way to decompose requirements to understand the said attributes of real-time systems (Saiedian et al., 2005). An increasing number of designers are interested in scenario- driven approaches that allow them to focus on the main functional aspects of the system to be specified (Amyot et al., 1998). The proposed methodology depends on the National Institute of Standards and Technology Special Publication 800-30 (NIST SP 800-30). The purpose of Special Publication 800-30 is to provide guidance for conducting risk assessments of federal information systems and organizations (Joint Task Force Transformation Initiative, 2012). NIST SP 800-30 publication provides a comprehensive framework that defines a set of risk assessment activities in nine steps (Stoneburner et al., 2002) . These nine steps are explained in figure 3.1.

We will focus in step 5 likelihood determination and step 6 impact analysis. The framework use a qualitative scale for Likelihood and impact rating that's high, medium or low.

In step 5, we will use the key computer technology for dealing with probabilities, namely Bayesian networks. Bayesian network model it is an excellent tool where we need to compute the posterior probability distribution of some variables of interest conditioned on some other variables that have been observed.

In step 6, we propose to use the severity categories as specified in MIL-STD-882E or use sensitivity analysis. MIL-STD-882E is Standard approved for use by all Military Departments and Defence Agencies within the Department of Defence (DoD). MIL-STD-882E be a standard, generic method for the identification,

classification, and mitigation of hazards that can be practically applied by not only system safety professionals, but also by other functional disciplines such as fire protection engineers, occupational health engineers, etc (AIK & SANG, 2013). Another method of assessing the impact of uncertainty is through sensitivity analysis.

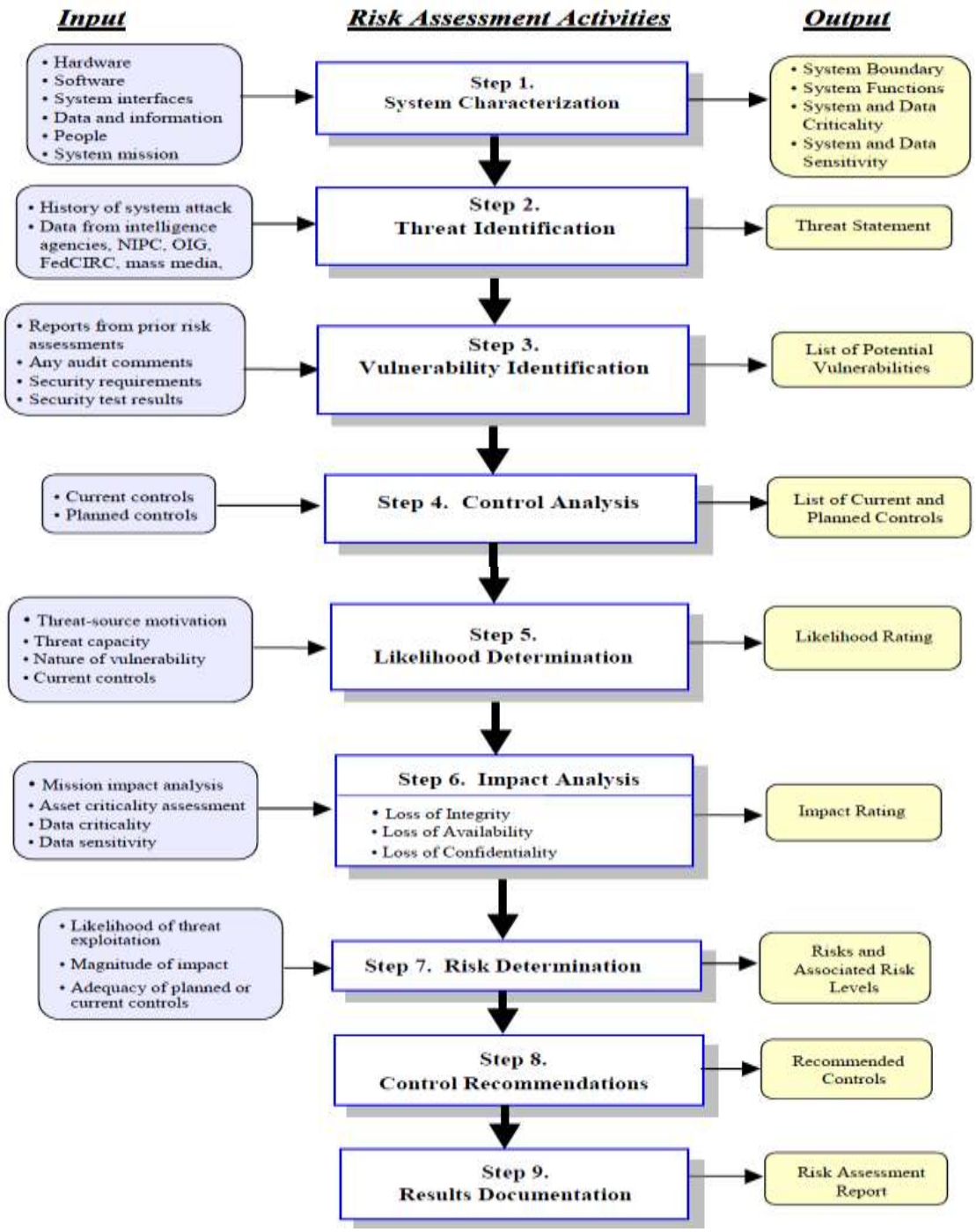


Figure 3. 1: NIST Risk Assessment Methodology Flowchart (Stoneburner et al., 2002)

3.1.1 Bayesian Networks

In recent years, Bayesian Networks (BNs) have become increasingly recognized as a potentially powerful solution to complex risk assessment problems. BNs have been widely used to represent full probability models in a compact and intuitive way. In the BN framework, the independence structure in a joint distribution is characterized by a directed acyclic graph, with nodes representing random variables and directed arcs representing causal or influential relationships between variables. If the variables are discrete, then the conditional probability distributions (CPDs) CPDs can be represented as node probability tables (NPTs), which list the probability that the child node takes on each of its different values for each combination of values of its parents (Fenton et al., 2007).

BNs offer the advantage of being able to reason in the presence of uncertainty, prior assumptions, and incomplete data. Further, they are able to learn from evidence in order to update their prior beliefs. Similarly, BN models do not just predict a single value for a variable; they predict its probability distribution. By taking the marginal distributions of variables of interest, we get a ready-made means of providing quantitative risk assessment (Hearty et al., 2009).

3.1.2 Proposed Methodology Steps

STEP 1: SYSTEM CHARACTERIZATION

In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system. The scope of the system needs to be defined in terms of the assets or values that will be considered in the modelling. Therefore, output from this step will be a clear picture of the system environment, and delineation of system boundary (Stoneburner et al., 2002). For proposed method we will consider the sequence diagrams to model the scenarios of using the system as a suitable model for capturing the interactions of the using system and the internal interaction of the component.

STEP 2: THREAT IDENTIFICATION

The goal of this step is to identify the potential threat-sources and compile a threat model statement listing potential threat-sources that are applicable to the IT

system being evaluated. Therefore, output from this step will be a threat statement containing a list of threat-sources that could exploit system vulnerabilities (Stoneburner et al., 2002). For our method we will identify the threats for each event explained in sequence diagram of the system.

STEP 3: VULNERABILITY IDENTIFICATION

This step is aimed to developing a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources. Therefore, output from this step will be a list of the system vulnerabilities (observations) that could be exercised by the potential threat-sources (Stoneburner et al., 2002). For our method we will identify the vulnerabilities that could be exploited by each threat explained in the last step.

STEP 4: CONTROL ANALYSIS

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability (Stoneburner et al., 2002).. Therefore, output from this step will be List of current or planned controls used for the IT system to mitigate the likelihood of a vulnerability's being exercised and reduce the impact of such an adverse event (Stoneburner et al., 2002)..

STEP 5: LIKELIHOOD DETERMINATION

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment. Therefore, output from this step will be Likelihood rating (Stoneburner et al., 2002).

In this step, we will use Bayesian network model since it is enable to compute the posterior probability distribution of some variables of interest (unknown parameters and unobserved data) conditioned on some other variables that have been observed. Our methodology for developing scenario based Bayesian network as follows:

5.1 Identifying the important SaaS application interaction events and components.

Base on step 1 (system characterization) we will have sequence diagram that represent the specific scenario to SaaS application to be considered. Therefore, we can identify the important system interaction events and components. From this point we can begin a first stage to construct a nodes for a Bayesian network for each event and some components. Included nodes should at least be measurable, observable or predictable and should have unambiguous definitions (Kragt, 2009).

5.2 Establishing the links between nodes for the Bayesian network.

Once the nodes are chosen, the links between them will be represented using directed arcs implying direct causal influence between the linked events and components. It is recommended that the number of parent nodes is kept to three or fewer, to limit the size of the Conditional Probability Table (Kragt, 2009). The identification of nodes and the links between them should result in influence diagram representing the system under consideration.

5.3 Assigning states and probabilities to each event or component state

This step is to assign states and probabilities to each event or component such as it is secure or unsecure. The states for each node represent the potential values or conditions that the node can assume. The estimation of probabilities associated with each state can be elicited from experts, learned from data or a combination of these (Kragt, 2009). Once the state type and number of states have been defined, the conditional probabilities for the states of each child node are specified for all combinations of states of their parent nodes.

5.4 Testing diagnostic to find probabilities for intended state.

Diagnostic analysis is done by selecting a specific states of nodes to observe their probability.

5.5 Measure the probabilities when set evidence base on given information.

The most important type of reasoning in Bayesian networks is known as belief updating, and amounts to computing the probability distribution over variables of interest conditional on others, observed variables. In other words, the probability distribution over the model variables is adjusted for a particular case, in which some

of the model variables assume given values. Therefore, by specifying the state for one or more input nodes, the impacts on other nodes can easily be predicted. This can be done through the use of Bayesian calculus to determine the state probabilities of each node from the predetermined conditional and prior probabilities. Therefore, BNs can be allow the assessment of the relative changes in outcome probabilities, associated with changes in management actions or system parameters.

To conducting those steps, we will use Genie(Graphical Network Interface) tool. It is a development environment for building graphical decision-theoretic models. It provides tools for users such as an interface to build Bayesian network model and to perform model diagnosis.

STEP 6: IMPACT ANALYSIS

This step designed is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. Therefore, output from this step will be magnitude of impact (Stoneburner et al., 2002).

Before beginning the impact analysis the following necessary information have to be collected from existing organizational documentation:

• System mission

• System and data criticality

• System and data sensitivity.

Therefore the appropriate approach to analyzing impact is to interview the system and information owner(s).

There are many method proposed for impact analysis as follows:

1. MIL-STD-882E Standard Severity Categories

The severity category for impact as specified in MIL-STD-882E which is Standard approved for use by all Military Departments and Defense Agencies within the Department of Defense (DoD) (DEPARTMENT OF DEFENSE, 2012). The following table explain the MIL-STD-882E Severity categories definitions.

Table 3. 1: MIL-STD-882E Severity categories (DEPARTMENT OF DEFENSE, 2012)

SEVERITY CATEGORIES		
Description	**Severity Category**	**Mishap Result Criteria**
Catastrophic	1	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M.
Critical	2	Could result in one or more of the following: permanent partial disability,injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1M but less than $10M.
Marginal	3	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100K but less than $1M.
Negligible	4	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than $100K.

For the purposes of the present research , the events or components insecurity severity can be classified as negligible, marginal, critical, and catastrophic depending on the impact of the loss or degradation of any, or a combination of any, of security goals and its consequence effect on organizational operations, organizational assets, or individuals.

Based on the effects observed, we assign severity indices of 0.25, 0.50, 0.75, and 0.95 to negligible, marginal, critical, and catastrophic severity classes respectively.

2. Worst Case of Sensitivity Analysis

Sensitivity analysis is the assessment of the impact of changes in input values on model outputs (Frey et al., 1999).

Technically defined , sensitivity is the influence of one parameter (the independent variable) on the value of another (the dependent variable) (Björklund, 2002).

3. Severity Analysis Technique at Architectural Level Based on UML Diagrams

Hassan et.al.(2003) in (Severity Analysis at Architectural Level Based on UML Diagrams) propose a severity analysis technique based on the Unified Modeling Language (UML) which is performed using hazard analysis techniques such that:

- The first part of the technique involves Functional Failure Analysis (FFA) and use case level sequence diagram to perform an early hazard analysis at the system level design. The functional failures at the system level arise as a result of lower level (component/connector) functional failures and malfunctions (Hassan et al., 2003).

- The second part of the technique combines Failure Mode and Effect Analysis (FMEA) and UML sequence diagrams to determine all failure modes at the low level of design (component/connector level). The FMEA results from a certain construction level of the system (e.g. component/connector level), for which failure criteria are known (Hassan et al., 2003).

- Finally the Fault Tree Analysis (FTA) is used for addressing low level failure conditions and their potential effect for causing the top-level hazardous events. Failure of component/connector (lower level) of design will propagate to the system level (higher level), so FTA is used to correlate component/connector failures with system level failures. Therefore, they estimate the component/connector severity by correlating the component/connector failure with the system level functions failure (Hassan et al., 2003).

The proposed severity analysis technique by Hassan et.al. (2003) is explained by figure 3.2.

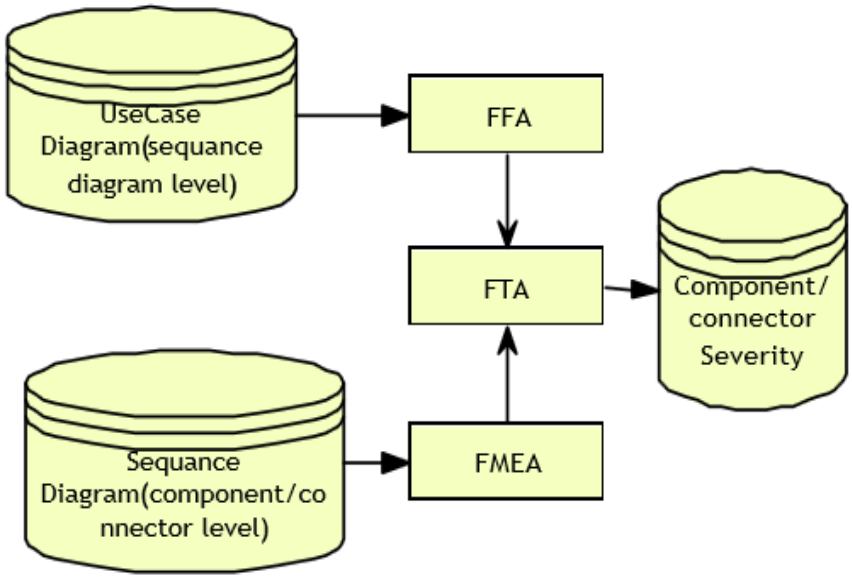


Figure 3. 2: Suggested Method for Severity Analysis Technique (Hassan et al., 2003).

STEP 7: RISK DETERMINATION

The purpose of this step is to assess the level of risk to the IT system. The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact (Stoneburner et al., 2002). Therefore, risk define as:

Risk = Probability x Impact

In this thesis we propose to calculate the risk by two methods as the following:

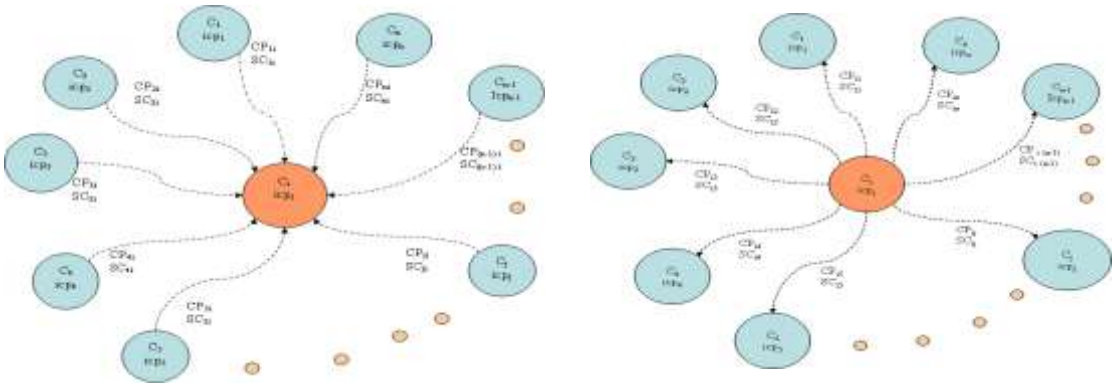
- According to severity categories specified by expert :

  The probability value for insecurity of the event or component without evidence will be multiply by the value specified depending on severity category for the event or component.

  In addition, the probability value for particular event or component (for example Ci) be insecure if other event or component (for example Cj) be insecure will be multiply by the value specified depending on severity category for the event or component (Ci).

- According to worst case of sensitivity analysis result:

  The probability value for a particular event or component (for example Ci) would be insecure if the other events or components (for example Cj) are insecure as explained in Figure 3.3 (a). This value will be multiplied by the value of sensitivity for the event or component which mean how the change in probability for particular event or component (Ci) will affect in changing in the probability value for all other events or components (C j) as explained in Figure 3.3 (b).



LIKELIHOOD **SEVIRITY**

Figure 3.3 (a) : Likelihood values **Figure 3.3 (b): Severity values**

Figure 3. 3: Likelihood and Severity values (Ammar, 2006)

Therefore, the decision maker can predict the risk, and the events or components with significant risk value have to be given more attention and higher priority to add control for them.

STEP 8: CONTROL RECOMMENDATIONS

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided.

The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level through decreasing the impact or the probability of the event that cause a risk. Therefore, output from this step is recommendation of control(s) and alternative solutions to mitigate risk (Stoneburner et al., 2002).

It should be noted that not all possible recommended controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis, should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition, the operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option

should be evaluated carefully during the risk mitigation process. Therefore, selecting the appropriate security controls for the organization's information systems can have major implications on the operations and assets of an organization.

In general, the implementation of effective controls and safeguards is an ongoing process, based on control recommended the analysis will be redone to reassessment the risk. Therefore the service provider has to add suitable security controls such as the following :

- **First example: HTTPS for all incoming/outgoing data transfer**

In the cloud computing environment, all the data flows through the internet are subjected to influence by various type of attacks. Therefore, the service provider has to use some network security mechanism to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security. SSL (Secure Socket Layer) is a protocol that enables a web browser and a web server to communicate securely; it allows the web browser to authenticate the web server. The secure hypertext transfer protocol (HTTPS) is a communications protocol designed to transfer encrypted information between computers over the World Wide Web. HTTPS is http using a Secure Socket Layer (SSL).

The SSL protocol involves exchange a series of messages between an SSL-enabled server and an SSL-enabled client when they first establish an SSL connection to facilitate the following:

- Authenticate the server to the client.
- Allow the client and server to select the cryptographic algorithms, or ciphers, that they both support.
- Optionally authenticate the client to the server.
- Use public-key encryption techniques to generate shared secrets.
- Establish an encrypted SSL connection.

The SSL protocol uses RSA algorithm which is a public key algorithm for encryption and decryption developed by Rivest, Shamir, and Adleman.

SSL protocol also uses concept of Certificates. Certificates are digital documents attesting to the binding of a public key to an individual or other entity. An SSL certificate contains the following information:

1. The domain for which the certificate was issued.

2. The owner of the certificate (who is the also the person/entity who has the right to use the domain).

3. The physical location of the owner.

4. The validity dates of the certificate.

Therefore, SSL provides confidence in the integrity and security in network infrastructure.

- **Second example: Secure application design, development and testing**

From the standpoint of both cost and effectiveness, considering security as an integral part of the software development lifecycle (SDLC) is the best way to build and maintain robust, reliable, and trustworthy applications. The SDLC phases are: Requirements analysis , Design , Implementation , Testing and deployment (Pescatore, 2004).

Therefore , incorporating security-based techniques in each phase of the SDLC will improve quality and resistance to attack in the final product. A critical first step to develop a secure application is to learn important secure coding principles and how they can be applied. Secure coding practices must be incorporated into all life cycle stages of an application development process. Compliance with this control is assessed through Application Security Testing Program which includes testing for secure coding principles described in Open Web Application Security Project (OWASP) Secure Coding Guidelines:

1. Input Validation
2. Output Encoding

3. Authentication and Password Management (includes secure handling of credentials by external services/scripts)
4. Session Management
5. Access Control
6. Cryptographic Practices
7. Error Handling and Logging
8. Data Protection
9. Communication Security
10. System Configuration
11. Database Security
12. File Management
13. Memory Management
14. General Coding Practices (Pescatore, 2004)

STEP 9: RESULTS DOCUMENTATION

Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing . Therefore, output from this step is risk assessment report that describes the threats and vulnerabilities, measures the risk (Stoneburner et al., 2002).

CHAPTER 4

MOTIVATING EXAMPLES

(CASE STUDIES)

Chapter 4: Motivating Examples (Case Studies)

4.1 Introduction

The methodology adopted in this research, will be based on a specific scenario. Thus, every step on our method will be explained using the following two case studies.

4.2. First Motivating Example (Ecommerce application):

Ecommerce on Cloud Computing is the specific application making good use of the cloud technology application in the business field, taking effective use of resources and reduce costs (Juncai & Shao, 2011). For some e-commerce companies, entrusting the work to the third party contains some elements of risks. Going too much, the risks may be greater than the benefits for the business. Therefore, our first case study will be security risk assessment in a book purchase scenario for e-commerce in cloud computing environment. In the following part we will explain our method using the book purchase scenario for e-commerce application in cloud computing environment :

STEP 1: SYSTEM CHARACTERIZATION

We will apply the proposed method for e-commerce in cloud computing environment on a sequence diagram for a book purchase scenario book presented in (Said et al., 2011) which explained in figure 4.1 to give good picture of the system.

STEP 2: THREAT IDENTIFICATION

We explained the potential threat for each event in the book purchase scenario in figure 4.1.

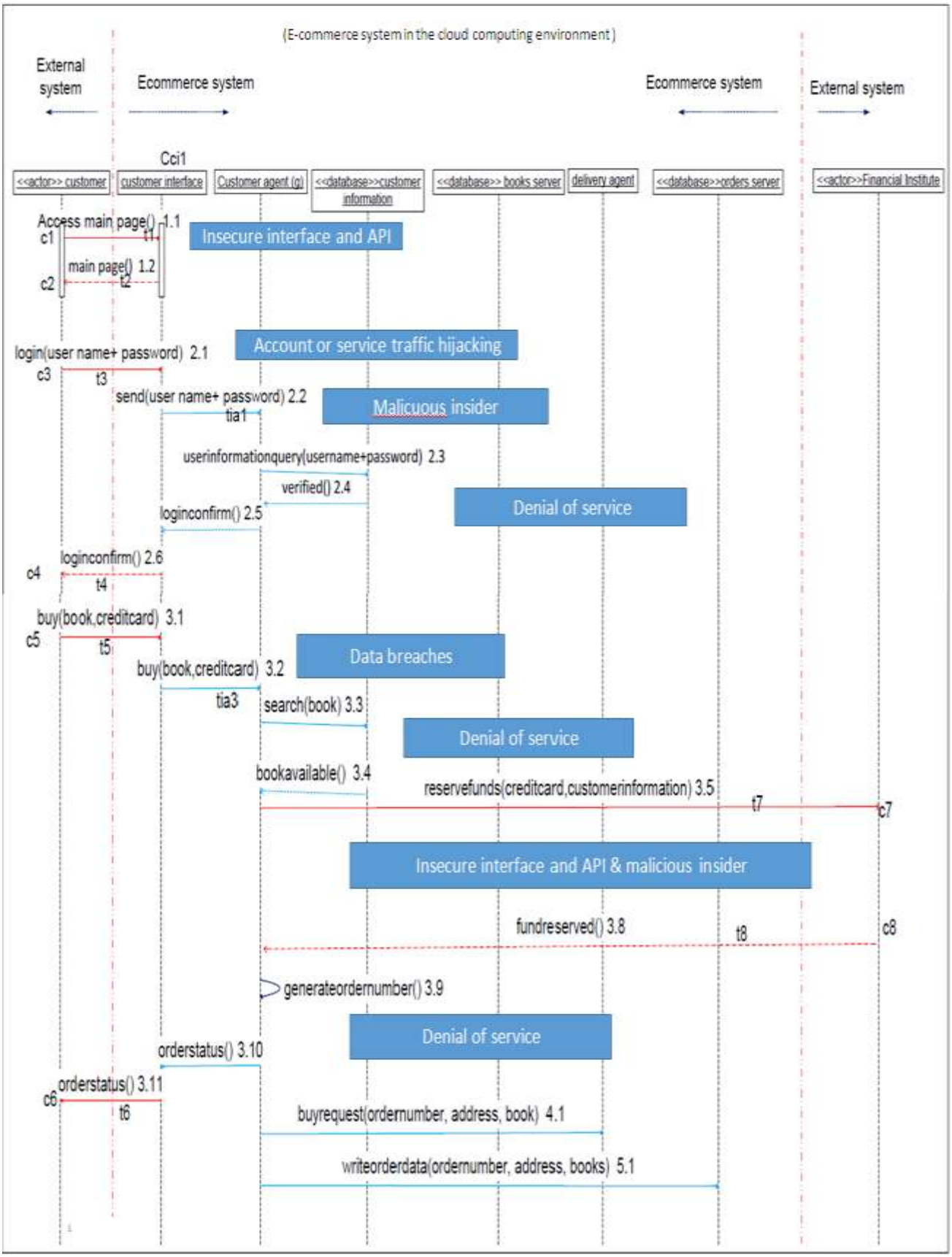


Figure 4. 1: Sequence diagram of the book purchase scenario (Said et al., 2011)

STEP 3: VULNERABILITY IDENTIFICATION

The common cloud computing security vulnerabilities are :

- Insecure Coding (Injection Flaws, Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF) , Buffer Overflows , Weak Authentication and/or Session Credentials) .
- Security Misconfiguration (Leitold & Hadarics, 2012)
- Unauthorized access to management interface.
- Internet protocol vulnerabilities.
- Data recovery vulnerability.
- Metering and billing evasion (Tanimoto et al., 2011).

STEP 4: CONTROL ANALYSIS

There are many details to be asked to analyze control used for securing the system in the cloud computing environment including the following:

- The physical security and mechanical robustness of the data centers
- Controls used to commission and decommission equipment within the data center, including hardware security controls such as hardware encryption devices
- Network operations and security features, including firewalls, protection against distributed denial of service (DDoS) attacks, integrity, file/log management, and antivirus protection.
- Basic IT controls and policies governing personnel, access, notification of administrator intervention, levels of access, and logging of access events (Zhang et al., 2012).

STEP 5: LIKELIHOOD DETERMINATION

In this step, we will use Bayesian network model so we developed Bayesian network for the buy book scenario for e-commerce in cloud computing environment with states for each node which explained in figure 4.2 with some probabilities tables contain probability that we assume for each state.

- **Testing Diagnostic to Find Probabilities for Intended States**

In figure 4.2, we explain the diagnostic analysis for the Bayesian network for the book purchase scenario by selecting some state of the event and see their probability.

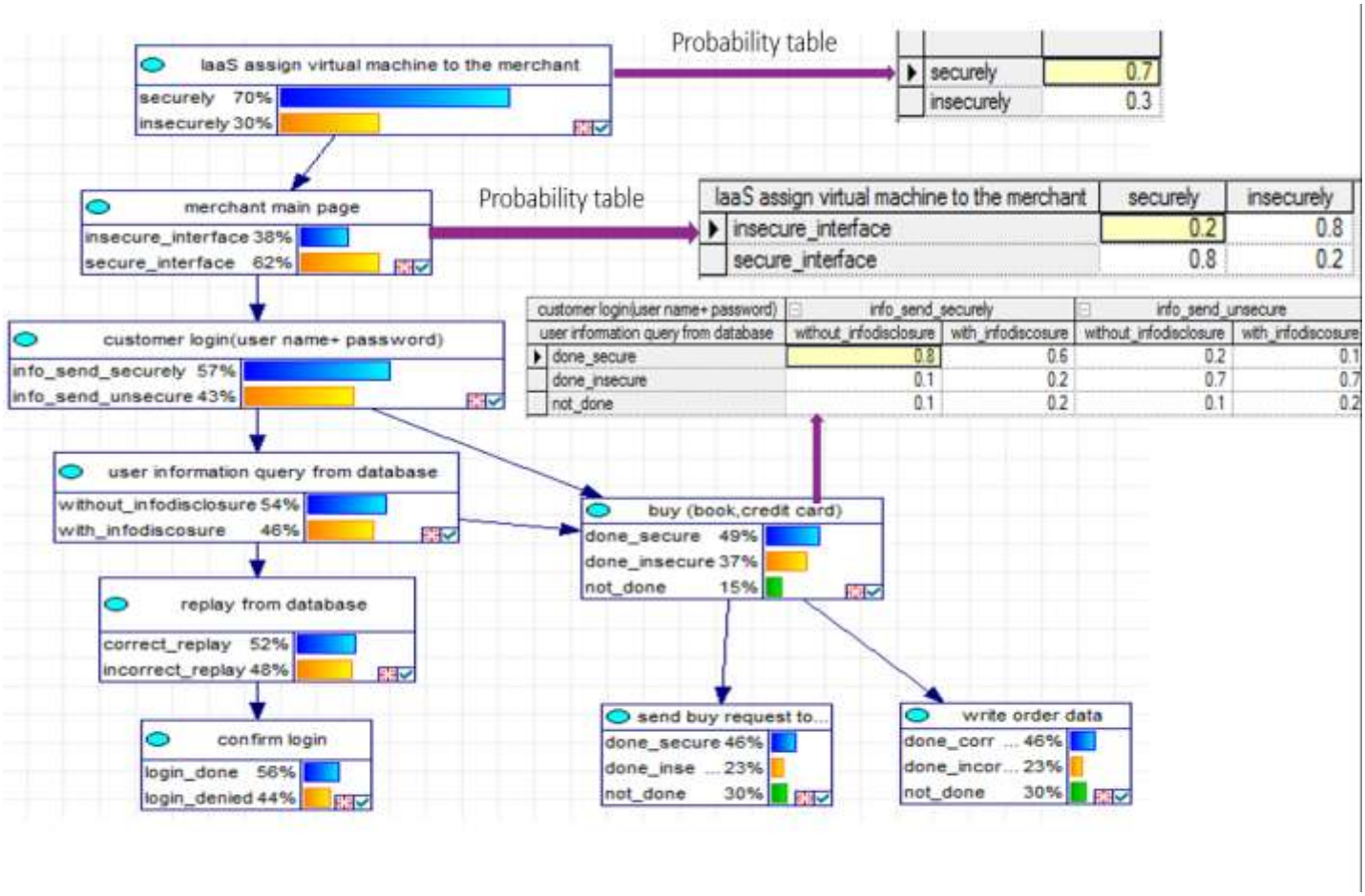


Figure 4. 2: Bayesian network for the book purchase scenario.

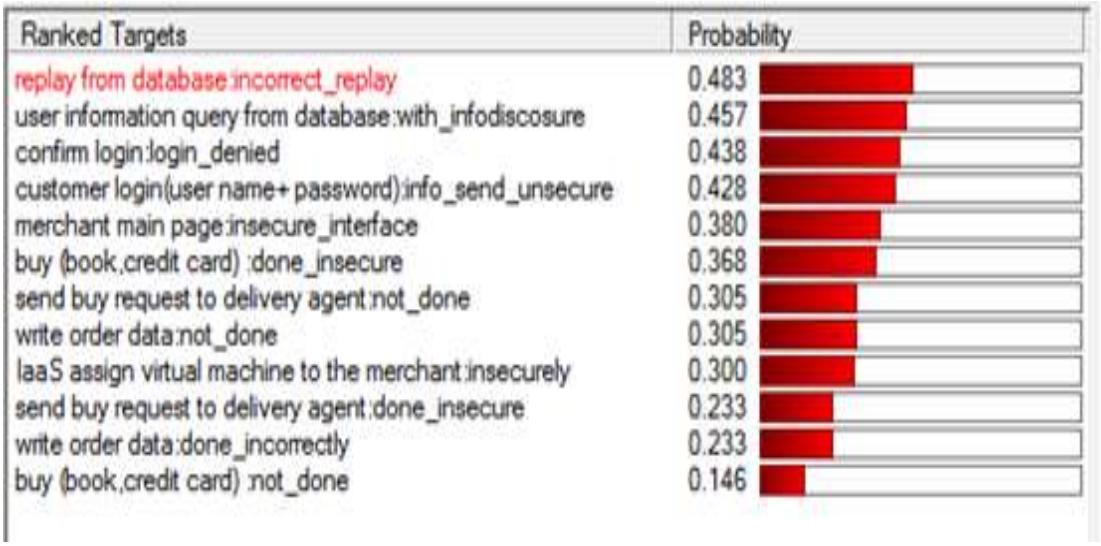


Figure 4. 3: Testing diagnostic result for book purchase scenario.

Figure 4.3 shows the ranked list of targets states of events or components with their probabilities. For example:

- Replay from database : incorrect reply have higher probability
- User information query from data base: with info disclosure have second higher probability
- Buy (book, credit card) :not done have lower probability.

- **Measure the probabilities when set evidence base on given information**

When set evidence base on given information we will notice the change in the probabilities for each state of the events. For example, for the buy book scenario in the customer login event if the evidence set to customer info sent insecurely, it will lead to change in the probability of states of all nodes as explained in figure 4.4.

In this way we can see if we change the probability of insecurity for any event the related changes in the posterior probabilities for each events after setting evidence.

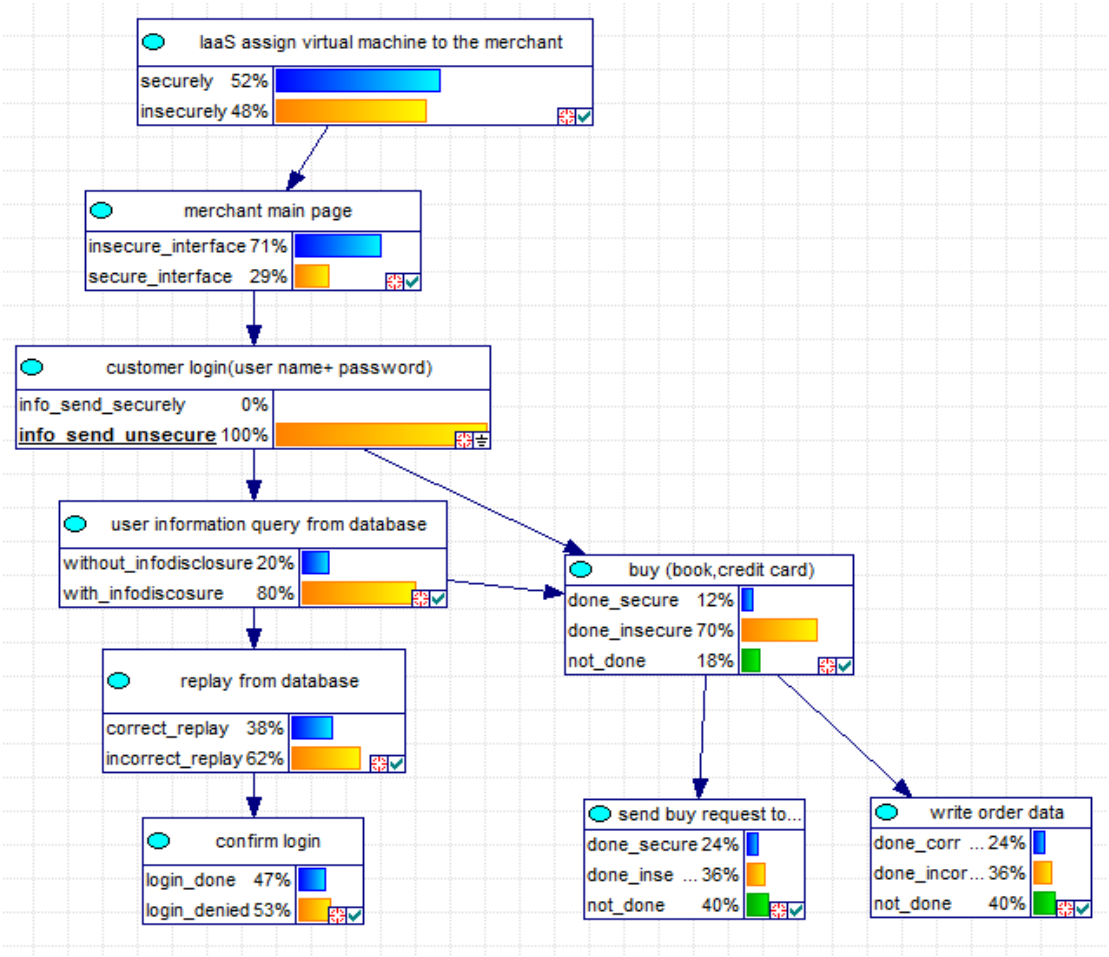
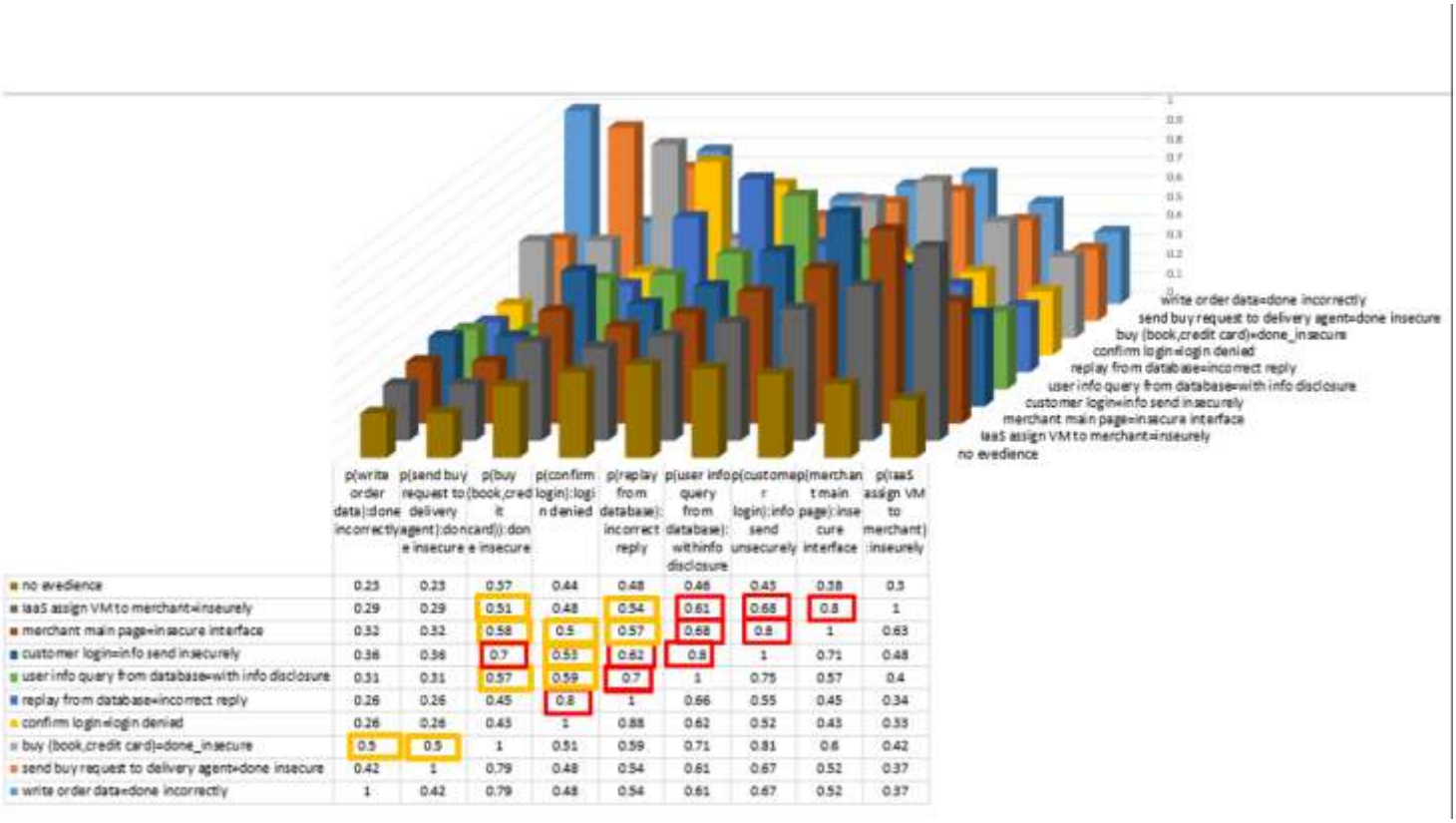


Figure 4. 4: Bayesian network when customer info send unsecure for the book purchase scenario.

3-D Matrix For Probability Values

The 3-D matrix explained in figure 4.5 such that both the rows and the columns of the matrix are labeled with the names of intended state of nodes and the values of probabilities are expressed by a full perspective 3-D map of the data.

From this 3-D matrix in figure 4.5, we can see at the first row the probability for the all events to be insecure without setting for any evidence. Then we can see each time if we set the evidence for one of the event to be conducted insecurely and observing the related changes in the posterior probabilities for other events. Therefore, at the second row we can see if we set the evidence for the IaaS assign VM to merchant event to insecurely. Then the third row explains if we set evidence for the merchant main page to insecure interface and so on.



	p(write order data):done incorrectly	p(send buy request to delivery agent):done insecure	p(buy (book,credit card)):done insecure	p(confirm login):login denied	p(replay from database): incorrect reply	p(user info query from database): withinfo disclosure	p(customer login):info send unsecurely	p(merchant main page):insecure interface	p(IaaS assign VM to merchant): inseurely
no evedience	0.23	0.23	0.57	0.44	0.48	0.46	0.45	0.38	0.3
IaaS assign VM to merchant=inseurely	0.29	0.29	0.51	0.48	0.54	0.61	0.68	0.8	1
merchant main page=insecure interface	0.32	0.32	0.58	0.5	0.57	0.68	0.8	1	0.63
customer login=info send insecurely	0.36	0.36	0.7	0.53	0.62	0.8	1	0.71	0.48
user info query from database=with info disclosure	0.31	0.31	0.57	0.59	0.7	1	0.75	0.57	0.4
replay from database=incorrect reply	0.26	0.26	0.45	0.8	1	0.66	0.55	0.45	0.34
confirm login=login denied	0.26	0.26	0.45	1	0.88	0.62	0.52	0.43	0.33
buy (book,credit card)=done_insecure	0.5	0.5	1	0.51	0.59	0.71	0.81	0.6	0.42
send buy request to delivery agent=done insecure	0.42	1	0.79	0.48	0.54	0.61	0.67	0.52	0.37
write order data=done incorrectly	1	0.42	0.79	0.48	0.54	0.61	0.67	0.52	0.37

Figure 4. 5: The probability of insecurity for each event with the related changes in the posterior probabilities after setting evidence.

STEP 6: IMPACT ANALYSIS

For the book purchase scenario we determine the impact resulting from a successful threat in table 4.1 that explain each event with it is severity (Impact). The impact resulting from a successful threat for each event in the book purchase scenario.

Table 4. 1: The impact resulting from a successful threat for each event in the book purchase scenario.

Event	Threat	Effect on system	Severity
IaaS assign VM to merchant	Insecure VM assigned to merchant	Deal with infected VM	Catastrophic

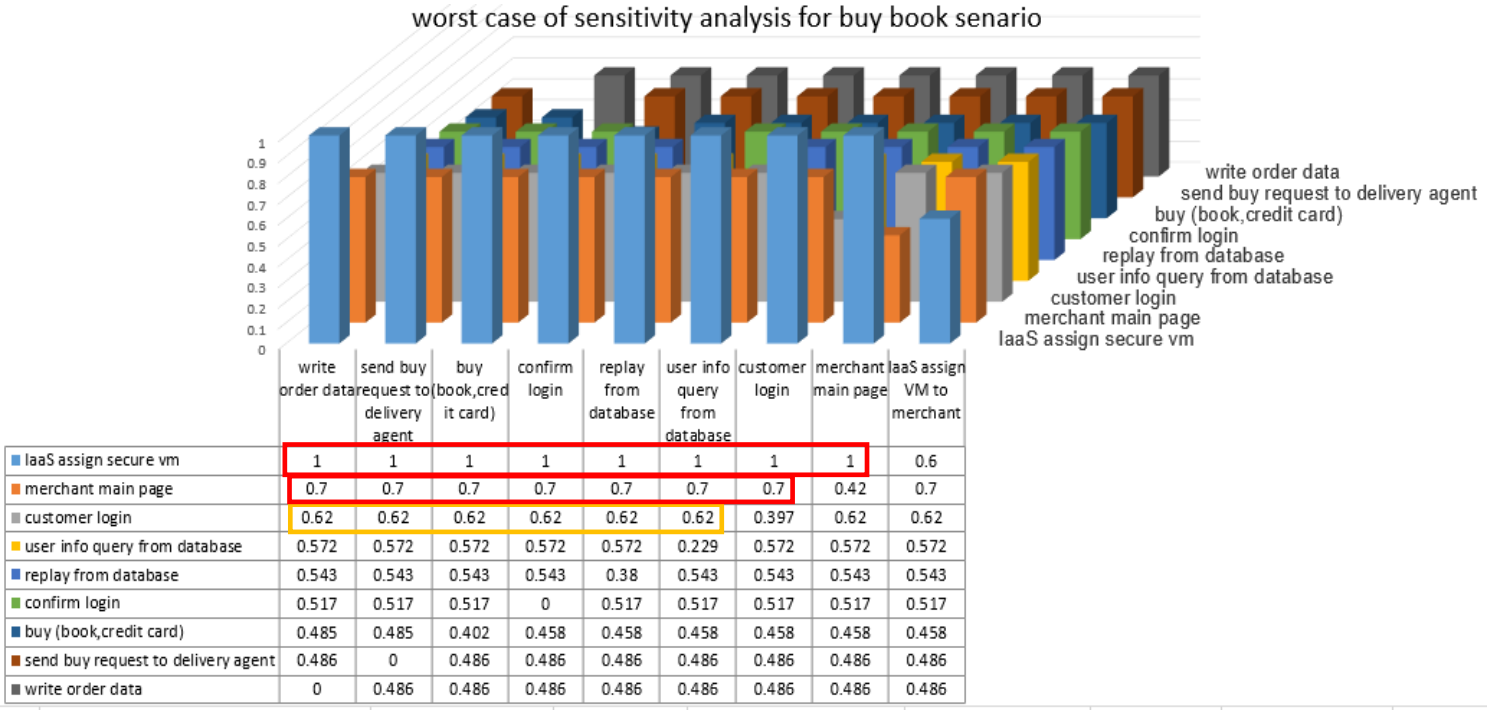
Access main page	Insecure main page accessed	Deal with another website(hacker web site)	Critical
Login :send (user name +password) to customer agent	Insecure sending	User name and password disclosed	Critical
user information query from database	Information disclosure	User name and password disclosed	Critical
replay from database	database does not work correctly or denial of service attack is done and reply not done correctly	Service denied	Marginal
confirm login	denial of service attack is done and confirmation not done	Service denied	Marginal
buy (book , credit card)	Insecure sending	credit card disclosed	Catastrophic
send buy request to delivery agent	Insecure sending	Buy request updated	Critical
write order data	Inconsistent database	System inconsistent	Critical

Risk Scale: Catastrophic (.95); Critical (.75); Marginal (.5)

If the severity of events is not known we can use value for severity from sensitivity analysis results which enable us to see the impact of each event on the other events.

We explain in figure 4.6, the worst case of sensitivity analysis result for the Bayesian network, which we constructed for book purchase scenario. As we can see from the figure 4.6 , the first event IaaS assign VM to merchant affecting on all event by 100% percent so it should be given more priority to add control methods for it to be more secure. Then, the merchant main page security affecting on all event after it

by 70% so it should given the second level of priority. Then, the customer login effect on all event after it by 62% so it must be given the third level of priority and so on.



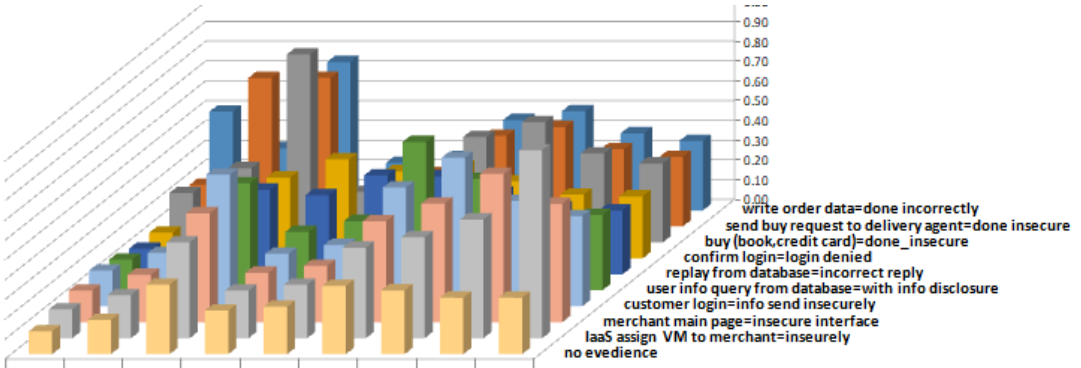
	write order data	send buy request to delivery agent	buy (book,credit card)	confirm login	replay from database	user info query from database	customer login	merchant main page	IaaS assign VM to merchant
IaaS assign secure vm	1	1	1	1	1	1	1	1	0.6
merchant main page	0.7	0.7	0.7	0.7	0.7	0.7	0.7	0.42	0.7
customer login	0.62	0.62	0.62	0.62	0.62	0.62	0.397	0.62	0.62
user info query from database	0.572	0.572	0.572	0.572	0.572	0.229	0.572	0.572	0.572
replay from database	0.543	0.543	0.543	0.543	0.38	0.543	0.543	0.543	0.543
confirm login	0.517	0.517	0.517	0	0.517	0.517	0.517	0.517	0.517
buy (book,credit card)	0.485	0.485	0.402	0.458	0.458	0.458	0.458	0.458	0.458
send buy request to delivery agent	0.486	0	0.486	0.486	0.486	0.486	0.486	0.486	0.486
write order data	0	0.486	0.486	0.486	0.486	0.486	0.486	0.486	0.486

Figure 4. 6: Bayesian network sensitivity analysis results for the book purchase scenario.

STEP 7: RISK DETERMINATION

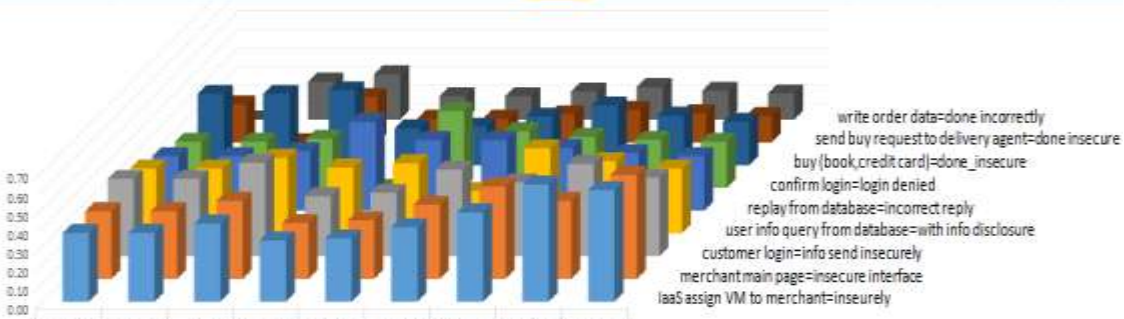
We create the following 3-D matrix in figure 4.7 to explain the result after we calculating the value of risk by multiplying the ratings assigned for event likelihood (e.g., probability) and its impact to assess the of risk of insecurity of every event on the other events.

As we can see from figure 4.7, at the first row we explain the probability for the all events to be insecure without setting for any evidence. Then we see each time if we set the evidence for one of the event to be done insecurely and observing the related changes in the posterior probabilities for other events. Therefore, at the second row we see if we set the evidence for the IaaS assign VM to merchant event to be done insecurely. Then the third row explains if we set evidence for the merchant main page to insecure interface and so on.



	write order data:done incorrectly	send buy request to delivery agent:done insecure	buy (book,credit card)):done insecure	confirm login:log in denied	replay from database:incorrect reply	user info query from database:with info disclosure	customer login:info send unsecurely	merchant main page:insecure interface	IaaS assign VM to merchant:inseurely
no evedience	0.12	0.17	0.35	0.22	0.24	0.35	0.32	0.29	0.29
IaaS assign VM to merchant=inseurely	0.15	0.22	0.48	0.24	0.27	0.46	0.51	0.60	0.95
merchant main page=insecure interface	0.16	0.24	0.55	0.25	0.29	0.51	0.60	0.75	0.60
customer login=info send insecurely	0.18	0.27	0.67	0.27	0.31	0.60	0.75	0.53	0.46
user info query from database=with info disclosure	0.16	0.23	0.54	0.30	0.35	0.75	0.56	0.43	0.38
replay from database=incorrect reply	0.13	0.20	0.43	0.40	0.50	0.50	0.41	0.34	0.32
confirm login=login denied	0.13	0.20	0.41	0.50	0.44	0.47	0.39	0.32	0.31
buy (book,credit card)=done_insecure	0.25	0.38	0.95	0.26	0.30	0.53	0.61	0.45	0.40
send buy request to delivery agent=done insecure	0.21	0.75	0.75	0.24	0.27	0.46	0.50	0.39	0.35
write order data=done incorrectly	0.50	0.32	0.75	0.24	0.27	0.46	0.50	0.39	0.35

Figure 4. 7: The risk of each event with the related change after setting evidence based on probability of insecurity and severity we specified for each event.



	write order data=done incorrectly	send buy request to delivery agent=done insecure	buy (book,credit card)=done_insecure	confirm login=login denied	replay from database=incorrect reply	user info query from database=with info disclosure	customer login=info send insecurely	merchant main page=insecure interface	IaaS assign VM to merchant=inseurely
IaaS assign VM to merchant=inseurely	0.37	0.37	0.42	0.33	0.34	0.40	0.48	0.63	0.60
merchant main page=insecure interface	0.36	0.36	0.42	0.30	0.32	0.40	0.50	0.42	0.56
customer login=info send insecurely	0.42	0.42	0.50	0.32	0.34	0.47	0.40	0.50	0.42
user info query from database=with info disclosure	0.35	0.35	0.41	0.35	0.38	0.23	0.46	0.39	0.35
replay from database=incorrect reply	0.29	0.29	0.32	0.48	0.38	0.38	0.34	0.31	0.29
confirm login=login denied	0.25	0.25	0.26	0.00	0.41	0.31	0.27	0.26	0.25
buy (book,credit card)=done_insecure	0.38	0.38	0.40	0.20	0.21	0.26	0.32	0.27	0.23
send buy request to delivery agent=done insecure	0.20	0.00	0.24	0.13	0.13	0.15	0.17	0.16	0.14
write order data=done incorrectly	0.00	0.20	0.24	0.13	0.13	0.15	0.17	0.16	0.14

Figure 4. 8: Risk value based on likelihood and sensitivity analysis results.

In figure 4.8, we explain the result after we calculating the value of risk by multiplying the ratings assigned for event likelihood (e.g., probability) and its impact from sensitivity result which explained in figure 4.6. We can see the how significant the risk will be if the IaaS assign VM to merchant insecurely the risk of the merchant main page be insecure will be.63.

STEP 8: CONTROL RECOMMENDATIONS

The best practices around security controls and processes for cloud computing are:

1. PHYSICAL SECURITY

- Fortifying physical data centers
- Multiple control layers
- Access authentication and 7×24 monitoring

2. NETWORK SECURITY

- Production environment completely separate
- Firewall and network zone segregation
- Two-factor authentication remote access
- Host based intrusion detection

3. APPLICATION SECURITY

- HTTPS for all incoming/outgoing data transfer
- Data encryption for credit card payment information
- Secure application design, development and testing
- Application firewall for an extra layer of perimeter protection

4. VULNERABILITY MANAGEMENT

- Internal and external network scans
- Security application scans

- Web application penetration testing
- Keep critical patches up-to-date (Peiyu & Dong., 2011)

STEP 9: RESULTS DOCUMENTATION

❑ Significant likelihood

If we consider threshold for significant likelihood from .6 we can see from figure 4.5 the following significant likelihood :

- If the IaaS assign VM to merchant insecurely the probability that:
  - The merchant main page insecurity will increase to .8
  - Customer login(info send insecurely) will increase to .68
  - User info query from database with info disclosure will increase to .61
- If the merchant main page be insecure interface the probability that:
  - Customer login(info send insecurely) will increase to .8
  - User info query from database with info disclosure will increase to .68
- If the customer login info send insecurely the probability that:
  - User info query from database with info disclosure will increase to . 8
  - Reply from database will be incorrect by .62
  - Buy (book, credit card) done insecurely will increase to .7
- If the user info query from database with info disclosure the probability that:
  - Reply from database will be incorrect reply by .7
- If the reply from database be incorrect reply the probability that:
  - Confirm login (login denied) will increase to .8

❑ Significant risk

If we consider threshold for significant risk from .6 we can see the significant risk as follows:

- **According to severity categories specified by experts :**

From figure 4.7 we can see the risk value for every event in the book purchase scenario without evidence and the risk value for each event if there is information or evidence that a specific event is done insecurely. Therefore, the event with maximum risk value and the event influencing on it have to give more attention and high priority to add control for it.

If we consider threshold for significant risk from .6 we can see the following significant risk:

- If the IaaS assign VM to merchant insecurely the risk of:
  - The merchant main page to be insecure will be.6
- If the merchant main page be insecure interface, the risk of :
  - Customer login(info send insecurely) will be.6
- If the customer login info send insecurely the risk of:
  - User info query from database with info disclosure will be .6
- If the customer login info send insecurely the risk of:
- the buy (book, credit card) to be done insecurely will be .67.

- According to worst case of sensitivity analysis result:

If we consider the book purchase scenario, the result of the risk calculated depending on sensitivity result, which is explained in figure 4.8, we can see how significant the risk will be if the IaaS assign VM to merchant insecurely, and the risk of the merchant main page be insecure will be.63.

4. 3 Effect of using security controls in reducing the risk factors

If we add security control to the book purchase scenario for example if we add the following controls:

- HTTPS for all incoming/outgoing data transfer as discussed in section 4.1. 2
- Secure application design, development and testing as discussed in section 4.1. 2

we can set evidence depending on new added controls to see the new probabilities for each state. Figure 4.9 illustrate Bayesian network for book purchase scenario if setting evidence the merchant main page is secure interface , info send securely for customer login and without info disclosure for query from database.

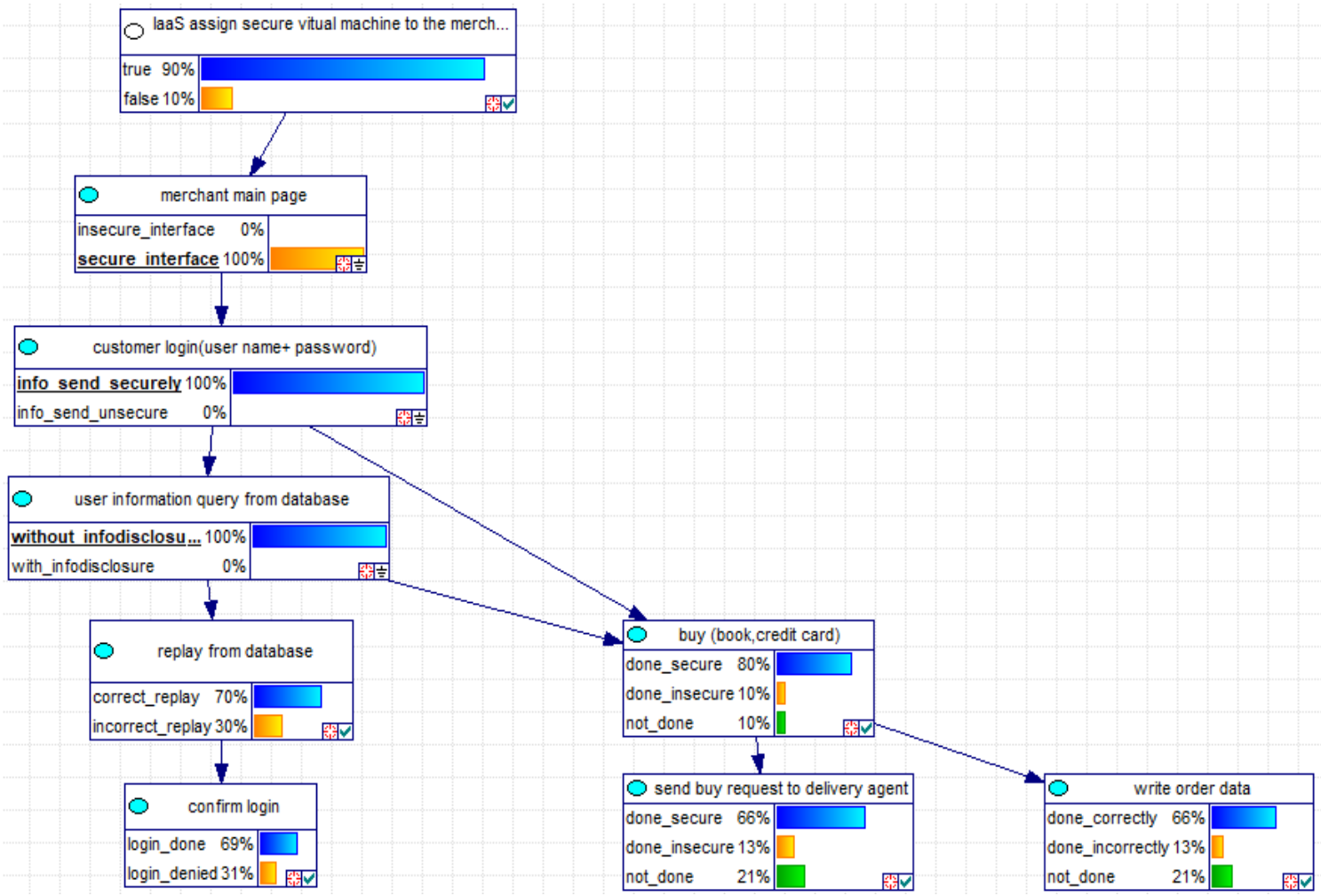


Figure 4. 9: Bayesian network for book purchase scenario if setting some evidence.

Moreover, we can change in the conditional probability tables for each node and reassess the security risk depending on the new value for conditional probability tables that we changed to see its effect in reducing the risk factors. Figure 4.10 illustrates the Bayesian network for book purchase scenario after change in it is conditional probability tables.

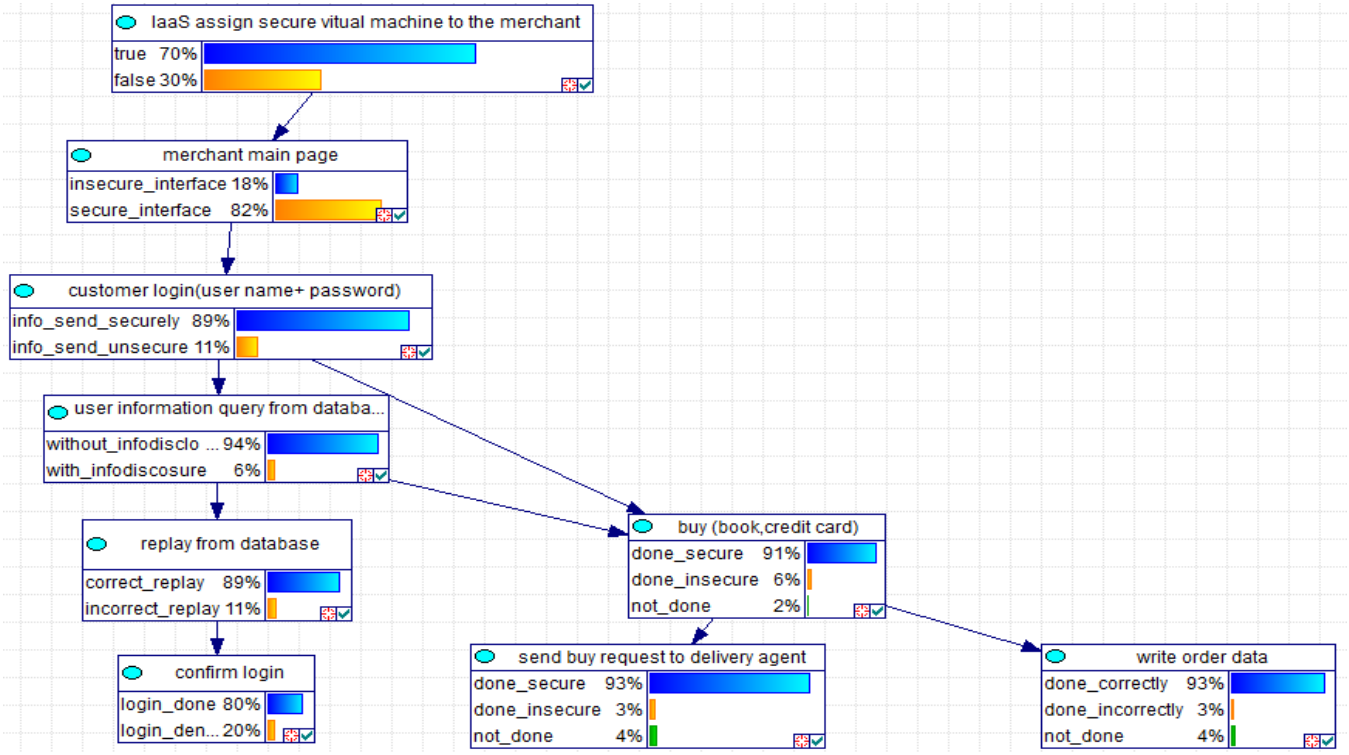


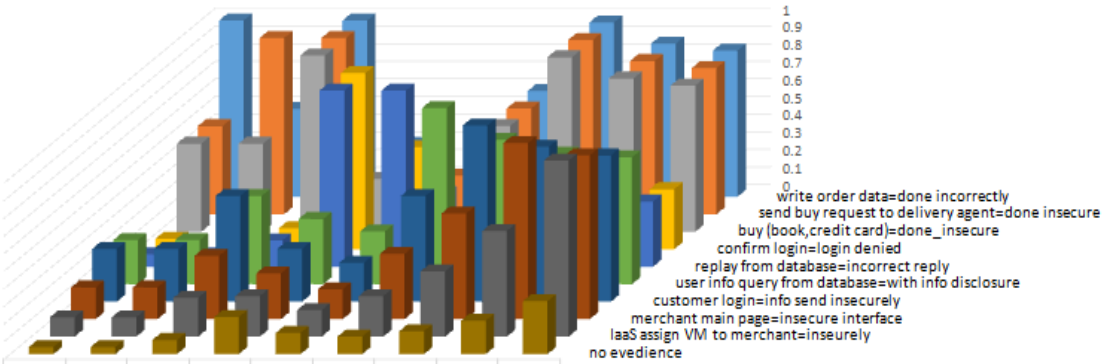
Figure 4. 10: Bayesian network after add some security controls and change in the conditional probability tables.

Based on the new probabilities, the new testing diagnostic result for the book purchase scenario will be as explained in figure 4.11.

Ranked Targets	Probability
IaaS assign secure vitual machine to the merchant:false	0.300
confirm login:login_denied	0.202
merchant main page:insecure_interface	0.180
replay from database:incorrect_replay	0.113
customer login(user name+ password):info_send_unsecure	0.108
buy (book,credit card) :done_insecure	0.065
user information query from database:with_infodiscosure	0.065
send buy request to delivery agent:not_done	0.041
write order data:not_done	0.041
send buy request to delivery agent:done_insecure	0.032
write order data:done_incorrectly	0.032
buy (book,credit card) :not_done	0.022

Figure 4. 11: Testing diagnostic result for book purchase scenario after add some security controls and change in the conditional probability tables.

In addition, we explain in figure 4.12 the new value of the probability of insecurity for any event and the related changes in the posterior probabilities for each events after setting evidence.

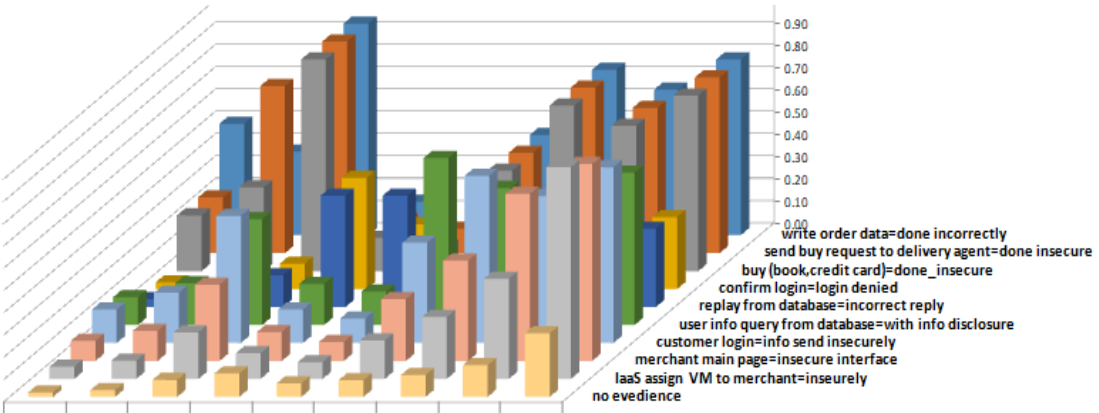


	p(write order data):done incorrectly	p(send buy request to delivery agent):done insecure	p(buy (book,credit card)):done insecure	p(confirm login):login denied	p(replay from database): incorrect reply	p(user info query from database): withinfo disclosure	p(customer login):info send unsecurely	p(merchant main page):insecure interface	p(IaaS assign VM to merchant) :inseurely
no evedience	0.04	0.04	0.08	0.21	0.12	0.1	0.13	0.19	0.3
IaaS assign VM to merchant=inseurely	0.11	0.11	0.22	0.23	0.15	0.23	0.37	0.60	1.00
merchant main page=insecure interface	0.18	0.18	0.36	0.26	0.17	0.37	0.60	1.00	0.93
customer login=info send insecurely	0.30	0.30	0.60	0.30	0.22	0.60	1.00	0.88	0.83
user info query from database=with info disclosure	0.25	0.25	0.50	0.37	0.30	1.00	0.82	0.74	0.72
replay from database=incorrect reply	0.07	0.07	0.15	1.00	1.00	0.24	0.24	0.28	0.37
confirm login=login denied	0.06	0.06	0.12	1.00	0.58	0.17	0.19	0.24	0.34
buy (book,credit card)=done_insecure	0.50	0.50	1.00	0.30	0.22	0.60	0.99	0.87	0.83
send buy request to delivery agent=done insecure	0.50	1.00	1.00	0.30	0.22	0.60	0.99	0.87	0.83
write order data=done incorrectly	1.00	0.50	1.00	0.30	0.22	0.60	0.99	0.87	0.83

Figure 4. 12: The probability of insecurity for each event after add some security controls and change in the conditional probability tables.

- **Risk values according to severity categories specified by expert :**

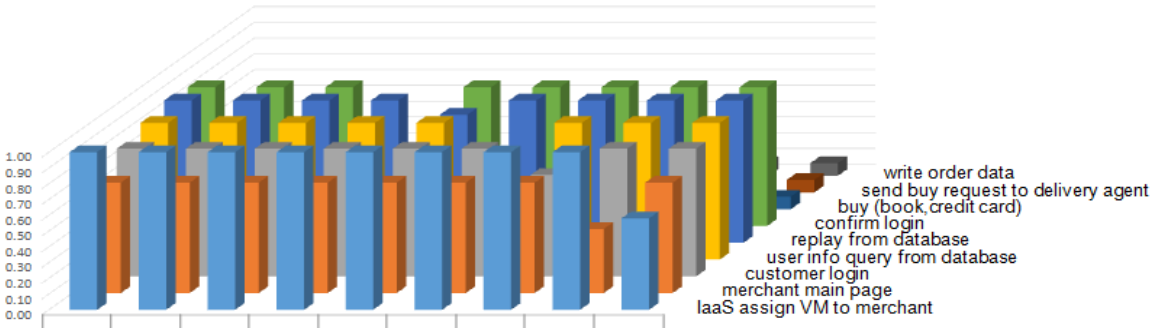
From figure 4.13 we can see the risk value for every event in the book purchase scenario after add specified security controls. At the first row without evidence. After that for each row the risk values for each event if there is information or evidence that is specified event in that row done insecurely.



	write order data:done incorrectly	send buy request to delivery agent:done insecure	buy (book,credit card)):done insecure	confirm login:login denied	replay from database: incorrect reply	user info query from database: withinfo disclosure	customer login:info send unsecurely	merchant main page:insecure interface	IaaS assign VM to merchant: inseurely
no evedience	0.02	0.03	0.08	0.11	0.06	0.08	0.10	0.14	0.29
IaaS assign VM to merchant=inseurely	0.06	0.08	0.21	0.12	0.08	0.17	0.28	0.45	0.95
merchant main page=insecure interface	0.09	0.14	0.34	0.13	0.09	0.28	0.45	0.75	0.88
customer login=info send insecurely	0.15	0.23	0.57	0.15	0.11	0.45	0.75	0.66	0.79
user info query from database=with info disclosure	0.13	0.19	0.48	0.19	0.15	0.75	0.62	0.56	0.68
replay from database=incorrect reply	0.04	0.05	0.14	0.50	0.50	0.18	0.18	0.21	0.35
confirm login=login denied	0.03	0.05	0.11	0.50	0.29	0.13	0.14	0.18	0.32
buy (book,credit card)=done_insecure	0.25	0.38	0.95	0.15	0.11	0.45	0.74	0.65	0.79
send buy request to delivery agent=done insecure	0.25	0.75	0.95	0.15	0.11	0.45	0.74	0.65	0.79
write order data=done incorrectly	0.50	0.38	0.95	0.15	0.11	0.45	0.74	0.65	0.79

Figure 4. 13: The risk values for each event after add some security controls and change in the conditional probability tables.

On the other hand, we can see sensitivity analysis for constructed Bayesian network after adding specified security controls as explained in figure 4.14.



	write order data	send buy request to delivery agent	buy (book,credit card)	confirm login	replay from database	user info query from database	customer login	merchant main page	IaaS assign VM to merchant
IaaS assign VM to merchant	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.58
merchant main page	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.41	0.70
customer login	0.81	0.81	0.81	0.81	0.81	0.81	0.64	0.81	0.81
user info query from database	0.87	0.87	0.87	0.87	0.87	0.17	0.87	0.87	0.87
replay from database	0.90	0.90	0.90	0.90	0.81	0.90	0.90	0.90	0.90
confirm login	0.88	0.88	0.88	0.00	0.88	0.88	0.88	0.88	0.88
buy (book,credit card)	0.08	0.08	0.07	0.08	0.08	0.08	0.08	0.08	0.08
send buy request to delivery agent	0.08	0.00	0.08	0.08	0.08	0.08	0.08	0.08	0.08
write order data	0.00	0.08	0.08	0.08	0.08	0.08	0.08	0.08	0.08

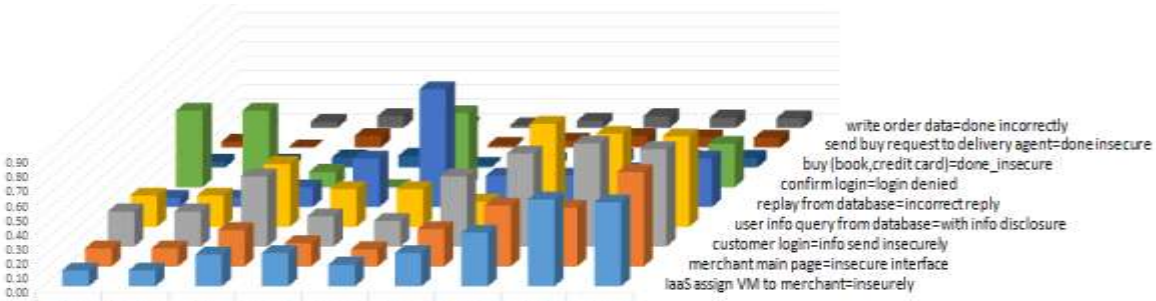
Figure 4. 14: Worst case of sensitivity result after adding specified security controls.

As we can see from the figure 4.14 , after adding specified security controls the first event IaaS assign VM to merchant affecting on all event by 100% percent. Then, the reply from database affecting on all event after it by 90% so it should given the second level of priority. Then, the confirm login effect on all event after it by 88% so it must be given the third level of priority and so on.

- **Risk values according to worst case of sensitivity analysis result:**

From figure 4.15 we can see the risk value for each event if there is information or evidence that is specific event done insecurely based on worst case of sensitivity analysis result.

As we can see from figure 4.15 the significant risk will be if the IaaS assign VM to merchant insecurely the risk of merchant main page will be insecure will be .6 .



	write order data=done incorrectly	send buy request to delivery agent=done insecure	buy (book,credit card)=done_insecure	confirm login=login denied	replay from database=incorrect reply	user info query from database=with info disclosure	customer login=info send insecurely	merchant main page=insecure interface	IaaS assign VM to merchant=inseurely
IaaS assign VM to merchant=inseurely	0.11	0.11	0.22	0.23	0.15	0.23	0.37	0.60	0.58
merchant main page=insecure interface	0.13	0.13	0.25	0.16	0.12	0.26	0.42	0.41	0.65
customer login=info send insecurely	0.24	0.24	0.49	0.21	0.18	0.49	0.64	0.71	0.67
user info query from database=with info disclosure	0.22	0.22	0.43	0.26	0.26	0.17	0.71	0.64	0.62
replay from database=incorrect reply	0.06	0.06	0.14	0.33	0.81	0.22	0.22	0.25	0.33
confirm login=login denied	0.53	0.53	0.11	0.00	0.51	0.15	0.17	0.21	0.30
buy (book,credit card)=done_insecure	0.04	0.04	0.07	0.08	0.02	0.05	0.08	0.07	0.07
send buy request to delivery agent=done insecure	0.04	0.00	0.08	0.02	0.02	0.05	0.08	0.07	0.07
write order data=done incorrectly	0.00	0.04	0.08	0.02	0.02	0.05	0.08	0.07	0.07

Figure 4. 15: Risk value based on likelihood and sensitivity analysis results after add specified security controls.

4.4 Second Example (Hybrid Live VM Migration):

In recent years, there has been a huge trend towards running network intensive applications, such as Internet servers and Cloud-based service in virtual environment, where multiple virtual machines (VMs) running on the same machine share the machine's physical and network resources. In such environment, the virtual machine monitor (VMM) virtualizes the machine's resources in terms of CPU, memory, storage, network and I/O devices to allow multiple operating systems running in different VMs to operate and access the network concurrently. A key feature of virtualization is live migration (LM) that allows transfer of virtual machine from one physical server to another without interrupting the services running in virtual machine. Live migration facilitates workload balancing, fault tolerance, online system maintenance, consolidation of virtual machines etc. However, live migration itself creates new security problems that need to be addressed before any wide-scale implementation (Aiash et al., 2014).

Therefore, our second case study will be security risk assessment for hybrid live VM migration scenario in cloud computing environment. In the following part , we will explain our method on it:

STEP 1: SYSTEM CHARACTERIZATION

Live migration refers to a transparent transfer of an active guest or virtual machine from a source server to a chosen destination server. We will apply the proposed method on hybrid Live VM migration scenario that is proposed by Narander & Swati in (2014) as efficient Live VM migration technique and use network-attached-storage (NAS) devices that store the profile of every VM. The sequence diagram that explains hybrid Live VM migration scenario is shown in figure 4.16.

STEP 2: THREAT IDENTIFICATION

Live migration of virtual machines exposes the contents of the VM state files to the network. An attacker can do the following actions:

a)Access data illegally during migration

b)Transfer a VM to an untrusted host

c)Create and migrate several VM causing disruptions or DoS

This can be possible because VM migration transfers the data over network channels that are often insecure, such as the Internet (Hashizume, 2013) **.**

We explained the potential threat for each event in figure 4.16.

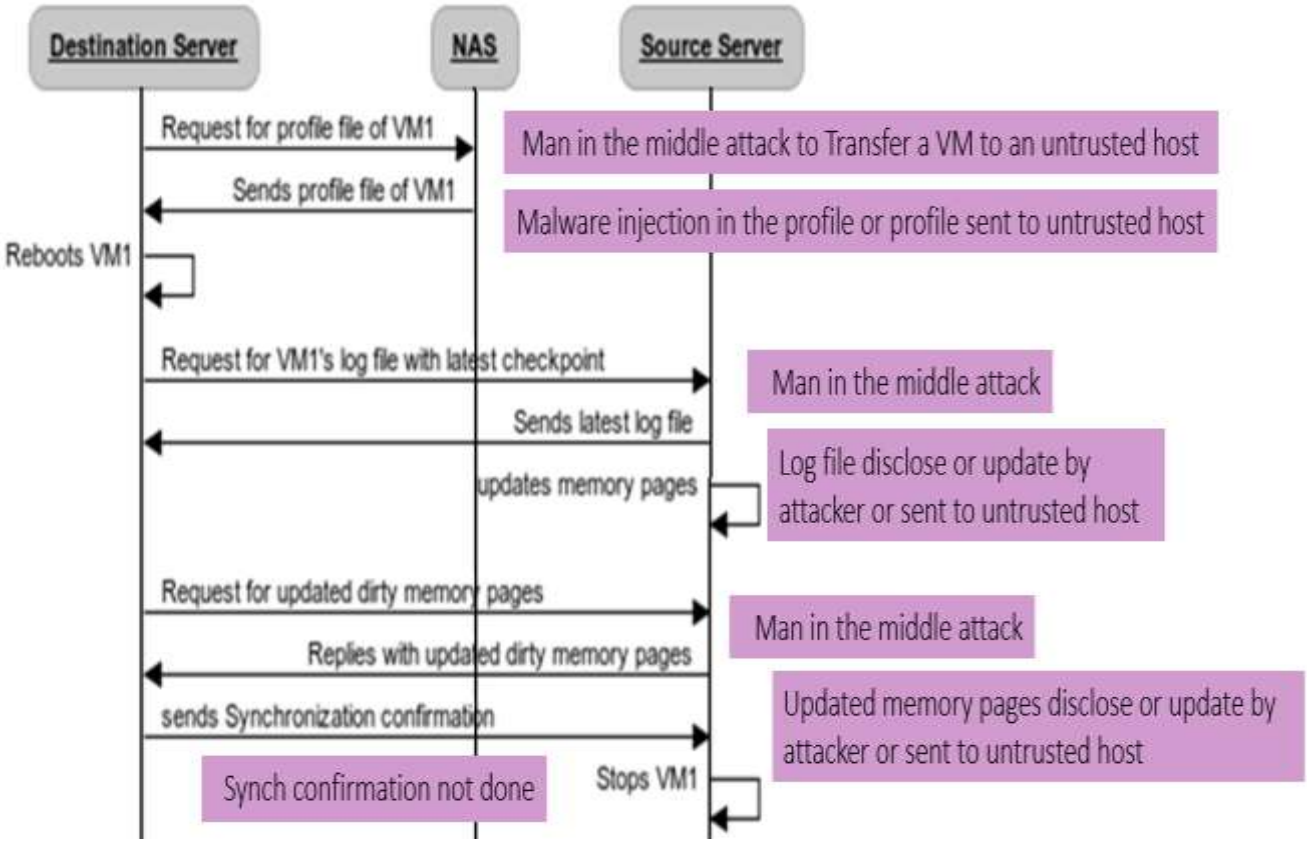


Figure 4. 16: Sequence diagram of the hybrid Live VM migration scenario (Narander & Swati, 2014)

STEP 3: VULNERABILITY IDENTIFICATION

The most vulnerabilities that are inherent in cloud computing due to using virtual machine and migration of it are:

-The co-location of virtual machines due to multi-tenant environment where an attacker's virtual machine tries to reside in the same server of the victim's virtual machine with purposes of misuse .

- An attacker who creates a valid account can create VM image containing malicious code such as a Trojan horse. If another customer uses this image, the virtual machine that he creates will be infected .

- The contents of virtual machines such as the kernel, applications, and data being used by these applications can be compromised during live migration (Hashizume, 2013).

STEP 4: CONTROL ANALYSIS

The analysis include security control to be applied before migration, during migration process, and after migration. The detail to be asked to analyze control include the following:

• Are the source and destination physical hosts trusted.

• Are an authorized access to management interface; authenticated and authorized management capabilities (VM creation, deletion, migration etc) are in place.

• Is the migration data remains confidential and unmodified during the transmission.

• Control used for protection against network attacks, intrusions and malicious codes.

• The presence of mechanisms to detect and report suspicious activities.

• Protection against vulnerabilities in the migration software (Aiash et al., 2014).

STEP 5: LIKELIHOOD DETERMINATION

In figure 4.17, we explain the Bayesian network we developed for the hybrid Live VM Migration in cloud computing environment with states for each node and their probability that we assume.

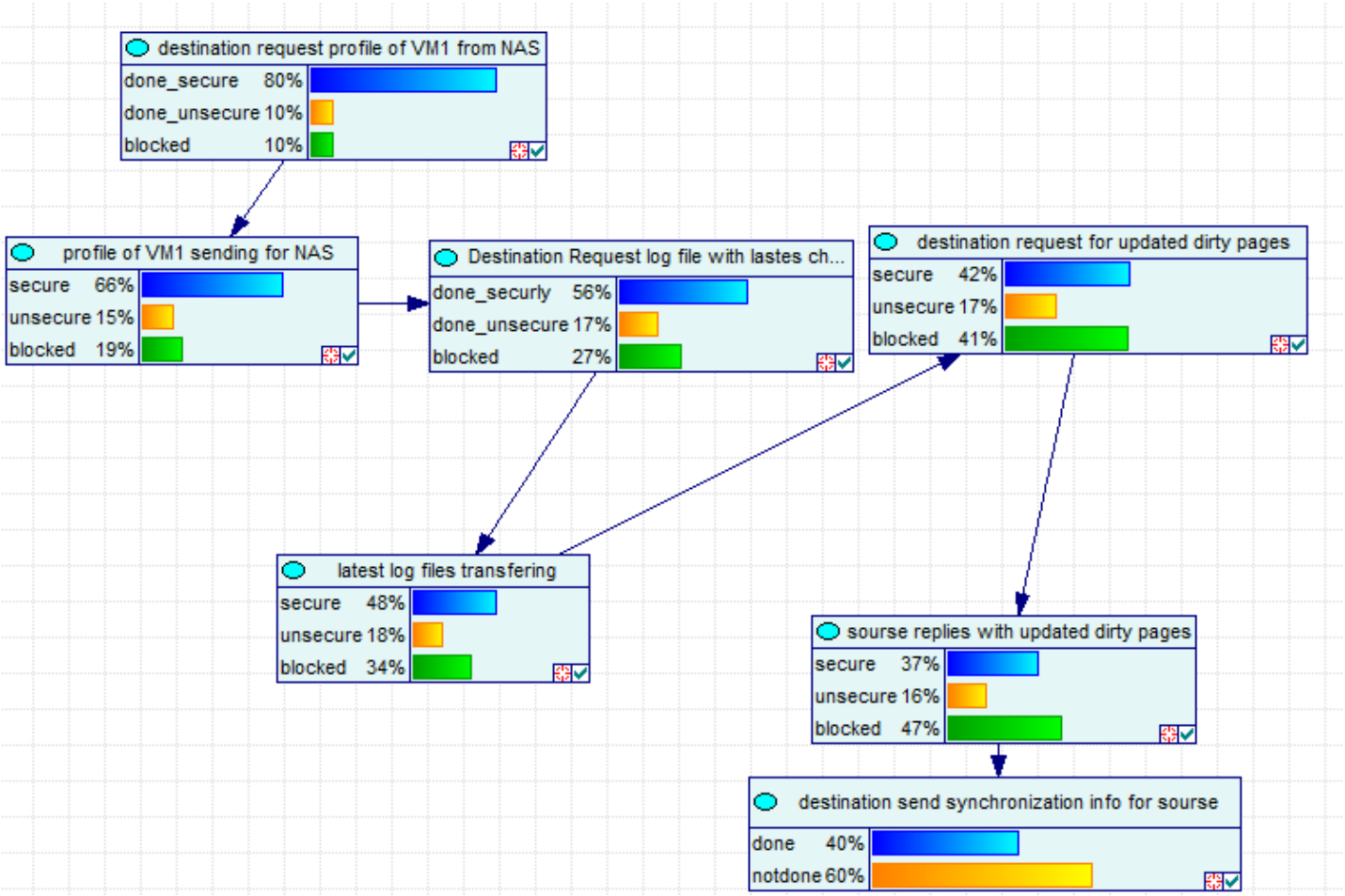


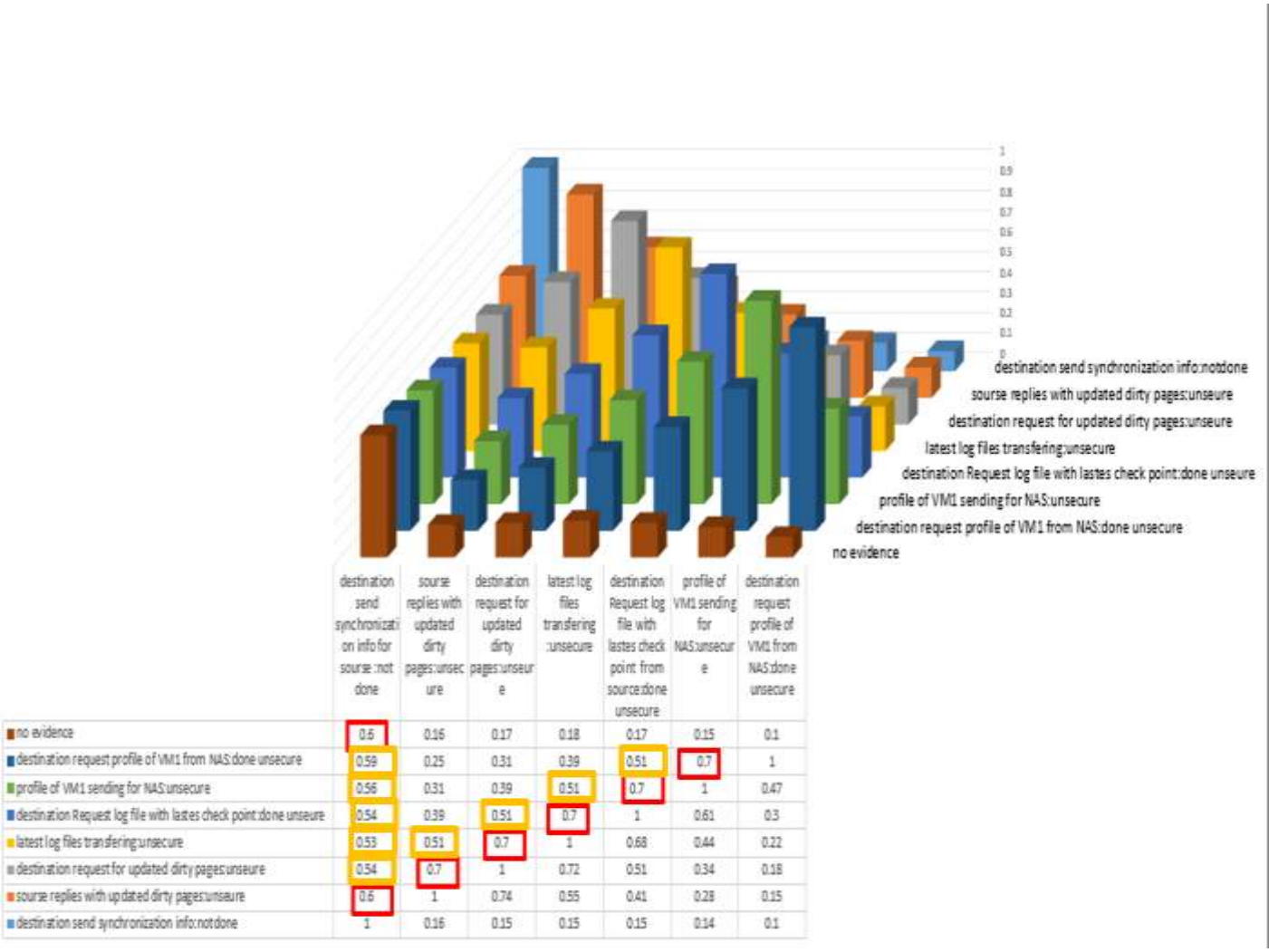
Figure 4. 17: Bayesian network for the hybrid Live VM Migration scenario.

In figure 4.18, we explain the diagnostic analysis for the Bayesian network for the hybrid Live VM migration by selecting some state of the event and see their probability.

Then from figure 4.19, we can see the probability of insecurity for each event with the related changes in the posterior probabilities for each event if there is information or evidence that is specific event done insecurely for the hybrid Live VM migration scenario.

Ranked Targets	Probability
destination send synchronization info for sourse :notdone	0.603
sourse replies with updated dirty pages:blocked	0.469
destination request for updated dirty pages:blocked	0.410
latest log files transfering :blocked	0.344
Destination Request log file with lastes check point from source:blo...	0.271
profile of VM1 sending for NAS:blocked	0.190
latest log files transfering :unsecure	0.175
Destination Request log file with lastes check point from source:don...	0.171
destination request for updated dirty pages:unsecure	0.171
sourse replies with updated dirty pages:unsecure	0.162
profile of VM1 sending for NAS:unsecure	0.150
destination request profile of VM1 from NAS:blocked	0.100
destination request profile of VM1 from NAS:done_unsecure	0.100

Figure 4. 18: Testing diagnostic result for the hybrid Live VM migration scenario.



	destination send synchronization info for sourse :not done	sourse replies with updated dirty pages:unsecure	destination request for updated dirty pages:unseure	latest log files transfering :unsecure	destination Request log file with lastes check point from source:done unsecure	profile of VM1 sending for NAS:unsecure	destination request profile of VM1 from NAS:done unsecure
no evidence	0.6	0.16	0.17	0.18	0.17	0.15	0.1
destination request profile of VM1 from NAS:done unsecure	0.59	0.25	0.31	0.39	0.51	0.7	1
profile of VM1 sending for NAS:unsecure	0.56	0.31	0.39	0.51	0.7	1	0.47
destination Request log file with lastes check point:done unseure	0.54	0.39	0.51	0.7	1	0.61	0.3
latest log files transfering:unsecure	0.53	0.51	0.7	1	0.68	0.44	0.22
destination request for updated dirty pages:unseure	0.54	0.7	1	0.72	0.51	0.34	0.18
sourse replies with updated dirty pages:unseure	0.6	1	0.74	0.55	0.41	0.28	0.15
destination send synchronization info:notdone	1	0.16	0.15	0.15	0.15	0.14	0.1

Figure 4. 19: The probability of insecurity for each event with the related changes in the posterior probabilities for each event after setting evidence.

STEP 6: IMPACT ANALYSIS

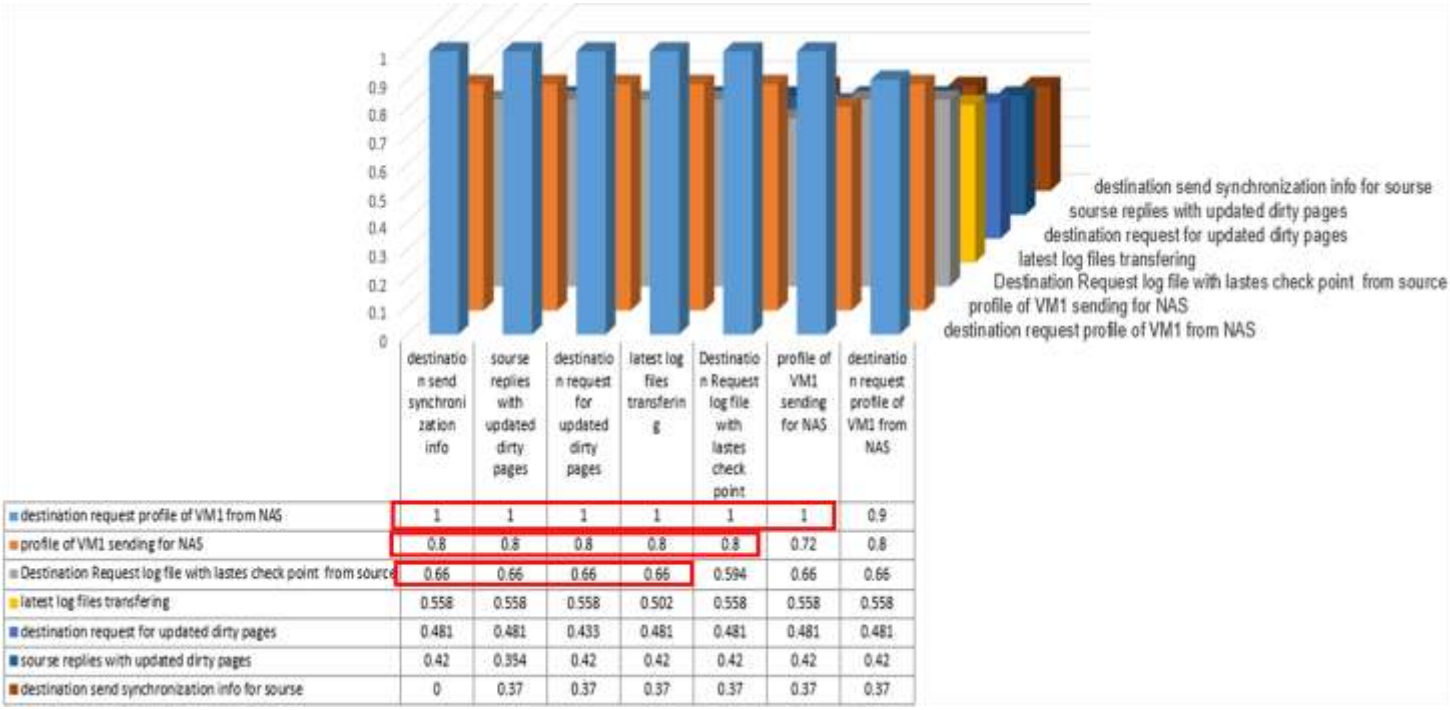
In table 4.2 we explain the impact resulting from a successful threat for each event in the hybrid Live VM migration scenario.

Table 4. 2: The impact resulting from a successful threat for each event in the hybrid Live VM migration scenario.

Event	Effect On System Severity
destination request profile of VM1 from NAS	Critical
profile of VM1 sending for NAS	Catastrophic
Destination Request log file with lasts check point from source	Critical
latest log files transferring	Catastrophic
destination request for updated dirty pages	Critical
source replies with updated dirty pages	Catastrophic
destination send synchronization info for source	Marginal

On the other hand, we can conduct sensitivity analysis for constructed Bayesian network. Using that will enable us to see the impact of every event on the others.

In figure 4.20, we explain the worst case of sensitivity analysis result for the hybrid live VM migration Bayesian network , which we constructed.



	destination send synchronization info	sourse replies with updated dirty pages	destination request for updated dirty pages	latest log files transfering	Destination Request log file with lastes check point	profile of VM1 sending for NAS	destination request profile of VM1 from NAS
destination request profile of VM1 from NAS	1	1	1	1	1	1	0.9
profile of VM1 sending for NAS	0.8	0.8	0.8	0.8	0.8	0.72	0.8
Destination Request log file with lastes check point from source	0.66	0.66	0.66	0.66	0.594	0.66	0.66
latest log files transfering	0.558	0.558	0.558	0.502	0.558	0.558	0.558
destination request for updated dirty pages	0.481	0.481	0.433	0.481	0.481	0.481	0.481
sourse replies with updated dirty pages	0.42	0.354	0.42	0.42	0.42	0.42	0.42
destination send synchronization info for sourse	0	0.37	0.37	0.37	0.37	0.37	0.37

Figure 4. 20: Bayesian network sensitivity analysis results for the hybrid Live VM migration scenario.

As we can see from figure 4.20, the first event destination request profile of VM1 from NAS is more event affecting on all other events. Then, the profile of VM sending for NAS affecting on all event after it by .8 so it must be given the second level of priority. Then, the destination request log file with latest check point from source effect on all event after it by .66 so it must be given the third level of priority and so on.

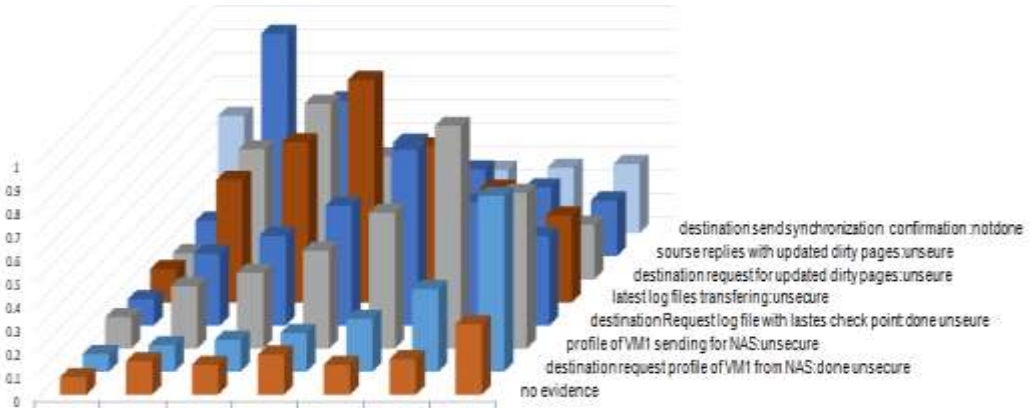
STEP 7: RISK DETERMINATION

- According to severity categories specified by expert :

From figure 4.21, we can see the risk for every event in the hybrid Live VM migration scenario without evidence and the risk value for each event if there is information or evidence that a specific event is done insecurely.

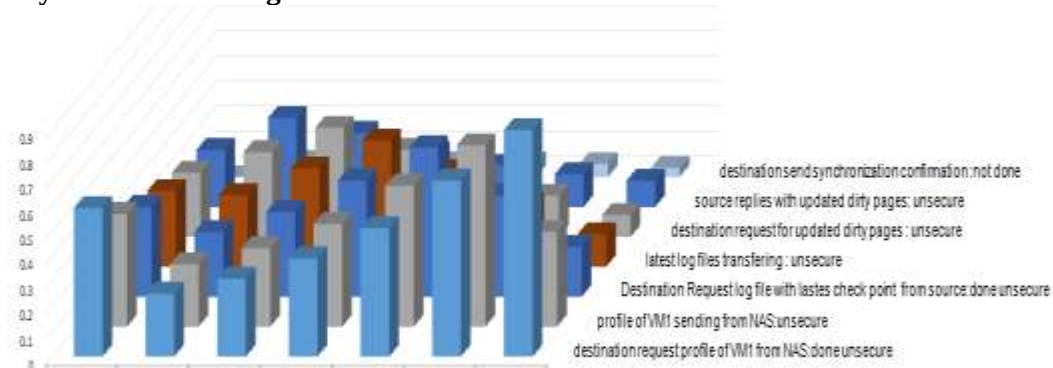
- According to worst case of sensitivity analysis result:

From figure 4.22, we can see the risk values for the hybrid Live VM migration scenario for each event if there is information or evidence that is specific event is done insecurely.



	destination send synchronization confirmation :notdone	sourse replies with updated dirty pages:unseure	destination request for updated dirty pages:unseure	latest log files transfering:unsecure	destination Request log file with lastes check point:done unseure	profile of VM1 sending for NAS:unsecure	destination request profile of VM1 from NAS:done unsecure
no evidence	0.075	0.1425	0.1275	0.171	0.1275	0.152	0.3
destination request profile of VM1 from NAS:done unsecure	0.075	0.1125	0.135	0.165	0.225	0.3525	0.75
profile of VM1 sending for NAS:unsecure	0.133	0.266	0.323	0.418	0.5795	0.95	0.665
destination Request log file with lastes check point:done unseure	0.1125	0.3075	0.3825	0.51	0.75	0.525	0.3825
latest log files transfering:unsecure	0.1425	0.5225	0.684	0.95	0.665	0.4845	0.3705
destination request for updated dirty pages:unseure	0.1125	0.555	0.75	0.525	0.3825	0.2925	0.2325
sourse replies with updated dirty pages:unseure	0.152	0.95	0.665	0.4845	0.3705	0.2945	0.2375
destination send synchronization confirmation :notdone	0.5	0.3	0.27	0.265	0.27	0.28	0.295

Figure 4. 21: The risk values of each event with the related change after setting evidence for the hybrid Live VM migration scenario.



	destination send synchronization confirmation :not done	source replies with updated dirty pages: unsecure	destination request for updated dirty pages: unsecure	latest log files transfering: unsecure	Destination Request log file with lastes check point from source:done unsecure	profile of VM1 sending from NAS:unsecure	destination request profile of VM1 from NAS:done unsecure
destination request profile of VM1 from NAS:done unsecure	0.59	0.25	0.31	0.39	0.51	0.7	0.9
profile of VM1 sending from NAS:unsecure	0.448	0.248	0.312	0.408	0.56	0.72	0.376
Destination Request log file with lastes check point from source:done unsecure	0.3564	0.2574	0.3366	0.462	0.594	0.4026	0.198
latest log files transfering : unsecure	0.30132	0.28458	0.3906	0.502	0.37944	0.24552	0.12936
destination request for updated dirty pages : unsecure	0.25493	0.3367	0.493	0.34632	0.24531	0.16354	0.08658
source replies with updated dirty pages: unsecure	0.2268	0.394	0.294	0.2142	0.1638	0.1302	0.105
destination send synchronization confirmation :not done	0	0.0592	0.0555	0.0555	0.0555	0.0518	0.037

Figure 4. 22: Risk values for the hybrid Live VM migration scenario based on likelihood and sensitivity analysis result .

STEP 8: CONTROL RECOMMENDATIONS

Insecure VM Migration can be stopped by the following countermeasures:

- A Trusted Cloud Computing Platform (TCCP) that provides confidential execution of guest virtual machines. It provides secure VM launch and migration operations.

- PALM is a secure migration system that provides VM live migration capabilities under the condition that a VMM protected system is present and active.

- The connection between the source and the destination VMMs should be authenticated and encrypted during the migration process.

- Isolate VM migration traffic to prevent eavesdropping attacks (Hashizume, 2013)

STEP 9: RESULTS DOCUMENTATION

❑ **Significant likelihood**

From figure 4.19 , we can see the following significant likelihood:

➢ Without evidence the destination send synchronization info for source :not done probability is .6

➢ If the destination request profile of VM1 from NAS: done unsecure the probability that:

- The profile of VM1 sending for NAS: unsecure will increase to .7

➢ If the profile of VM1 sending for NAS: unsecure the probability that:

- The destination request log file with lasts check point from source: done unsecure will increase to .7

➢ If the destination request log file with lasts check point from source: done unsecure the probability that:

- The latest log files transferring :unsecure will increase to .7

➢ If the latest log files transferring :unsecure the probability that:

- The destination request for updated dirty pages: unsecure will be .7

➢ If the destination request for updated dirty pages: unsecure probability that:

- The source replies with updated dirty pages: unsecure will be .7

➢ If the source replies with updated dirty pages: unsecure probability that:

- The destination send synchronization confirmation for source :not done will be .6

❑ **Significant risk**

From figure 4.21, we can see the following significant risk:

➢ If the latest log files transferring :unsecure the risk that:

- The destination request for updated dirty pages: unsecure will be .684

From figure 4.22, we can see the following significant risk:

➢ If the destination request profile of VM1 from NAS: done unsecure the risk that:

- The profile of VM1 sending for NAS: unsecure will be .7

CHAPTER 5

DISCUSSION AND COMPARISON

Chapter 5 :Discussion and Comparison

5.1 Result Discussion

In this thesis we proposed scenario based methodology for security risk assessment for cloud computing and apply it on two important case studies:

- Book purchase scenario
- Hybrid live VM Migration scenario

Where we need to imply high security module. Therefore, in order to develop an efficient security module, it is necessary to clearly identify existing risk.

The proposed method using Bayesian network for likelihood determination and two way to determine impact is as follows:

- According to severity categories specified by expert.
- According to worst case of sensitivity analysis result.

Where sensitivity analysis for assessing the severity without expert involvement in simple and fast way to evaluate the severity.

Depending on the assessment results the cloud provider can establish controls so that the risk can be reduced to an acceptable level.

We Applied the method after using security controls to verify the risk level reduction or mitigation.

In the following subsections we will discuss the results for the book purchase scenario and hybrid live VM Migration scenario to validate from the proposed methodology.

5.1.1 Book purchase scenario results

In this subsection we will discuss the results for the book purchase scenario.

5.1.1.1 Comparison Between Insecurity Probability Values Before And After Adding Specified Security Controls

We can see in table 5.1 a comparison between insecurity probability values before and after adding specified security controls for book purchase scenario.

Table 5. 1: Comparison between insecurity probability values before and after adding specified security controls for bok purchase scenario

Intended states for events or components	Before add controls	After add controls
merchant main page : insecure	71%	18%
Customer login: info send unsecure	43%	11%
User information query from database: with info disclosure	46%	6%
Replay from database : incorrect reply	48%	11%
Buy (book, credit card) : done insecure	37%	8%
Confirm login : login denied	44%	20%
Send buy request to delivery agent: done insecure	23%	4%
Write order data : incorrect reply	23%	4%

As we can see from the table 5.1 the probability value for events or components insecurity will be decrease more after add specified security controls.

5.1.1.2 Comparison Between Risk Values Before And After Adding Security Controls Based On The Two The Two Methods That We Use For Impact Analysis

The following tables explain the risk values before and after adding security controls based on impact according to severity categories specified by expert and impact according to worst case of sensitivity analysis result with the difference between their values. For example table 5.2 explains risk values if IaaS VM insecure.

Table 5. 2: Risk values if IaaS VM insecure

	Before Adding Security Controls		After Adding Security Controls	
	Based on impact categories by expert	**Based on sensitivity analysis result**	**Based on impact categories by expert**	**Based on sensitivity analysis result**
The merchant interface insecure	0.60	0.63	0.45	0.6
Login info send unsecure	0.51	0.48	0.28	0.37
Info query from database with info disclosure	0.46	0.4	0.17	0.23
Replay from database incorrect	0.27	0.34	0.08	0. 15
Login denied	0.24	0.33	0.12	0.23
Buy (book, credit card) insecure	0.48	0.42	0.21	0.22
Send buy request to delivery agent insecure	0.22	0.37	0.08	0.11
Write order data incorrectly	0.15	0.37	0.06	0.11

As we can see from table 5.2 there are significant risk before adding security controls base on impact according to severity categories specified by expert and impact according to worst case of sensitivity analysis result that if IaaS VM insecure the merchant interface will be insecure. Security controls which we add not affect on IaaS assign VM to merchant and the merchant main page is the first event after it. Therefore, as we can see from table 5.2 after adding security controls base on sensitivity analysis result if the IaaS assign VM to merchant insecurely then the merchant main page may be insecure is still significant risk.

Table 5.3 explains risk values if the merchant interface insecure for all events after it.

Table 5. 3: Risk values if the merchant interface insecure

	Before Adding Security Controls		**After Adding Security Controls**	
	Based on impact categories by expert	**Based on sensitivity analysis result**	**Based on impact categories by expert**	**Based on sensitivity analysis result**
Login info send unsecure	0.60	0.5	0.45	0.42
Info query from database with info disclosure	0.51	0.4	0.28	0.26
Replay from database incorrect	0.29	0.32	0.09	0.12
Login denied	0.25	0.3	0.13	0.16
Buy (book, credit card) insecure	0.55	0.42	0.34	0.25
Send buy request to delivery agent insecure	0.24	0.36	0.14	0.13
Write order data incorrectly	0.16	0.36	0.09	0.13

As we can see from table 5.3 there are significant risk before adding security controls base on impact according to severity categories specified by expert that if the merchant interface insecure the login info send unsecure. Security controls which we add affect on merchant interface to be secure. Therefore, as we can see from table 5.3 after adding security controls there are no significant risk.

Table 5.4 explains risk values if login info send unsecure for all events after it.

Table 5. 4:Risk values if login info send unsecure

	Before Adding Security Controls		After Adding Security Controls	
	Based on impact categories by expert	**Based on sensitivity analysis result**	**Based on impact categories by expert**	**Based on sensitivity analysis result**
Info query from database with info disclosure	0.60	0.47	0.45	0.49
Replay from database incorrect	0.31	0.34	0.11	0.18
Login denied	0.27	0.32	0.15	0.21
Buy (book, credit card) insecure	0.67	0.5	0.57	0.49
Send buy request to delivery agent insecure	0.27	0.42	0.23	0.24
Write order data incorrectly	0.18	0.42	0.15	0.24

As we can see from table 5.4 there are two significant risk before adding security controls base on impact according to severity categories specified by expert. The first if login info send unsecure then info query from database will be with info disclosure. The second if login info send unsecure then buy (book, credit card) will be insecure. After security controls which we add the login info will be send securely. Therefore, as we can see from table 5.4 after adding security controls there are no significant risk.

Table 5.5 explains risk values if info query from database with info disclosure for all events after it.

Table 5. 5: Risk values if info query from database with info disclosure

	Before Adding Security Controls		After Adding Security Controls	
	Based on impact categories by expert	**Based on sensitivity analysis result**	**Based on impact categories by expert**	**Based on sensitivity analysis result**
Replay from database incorrect	0.35	0.38	0.15	0.26
Login denied	0.30	0.35	0.19	0.26
Buy (book, credit card) insecure	0.54	0.41	0.48	0.43
Send buy request to delivery agent insecure	0.23	0.35	0.19	0.22
Write order data incorrectly	0.16	0.35	0.13	0.22

Table 5. 6 explains risk values if replay from database incorrect for all events after it.

Table 5. 6: Risk values if replay from database incorrect

	Before Adding Security Controls		After Adding Security Controls	
	Based on impact categories by expert	**Based on sensitivity analysis result**	**Based on impact categories by expert**	**Based on sensitivity analysis result**
Login denied	0.40	0.48	0.50	0.33
Buy (book, credit card) insecure	0.43	0.32	0.14	0.14
Send buy request to delivery agent insecure	0.20	0.29	0.05	0.06

Write order data incorrectly	0.13	0.29	0.04	0.06

Table 5.7 explains risk values if login denied for all events after it.

Table 5. 7:Risk values if login denied

	Before Adding Security Controls		**After Adding Security Controls**	
	Based on impact categories by expert	**Based on sensitivity analysis result**	**Based on impact categories by expert**	**Based on sensitivity analysis result**
Buy (book, credit card) insecure	0.41	0.26	0.11	0.11
Send buy request to delivery agent insecure	0.20	0.25	0.05	0.53
Write order data incorrectly	0.13	0.25	0.03	0.53

Table 5.8 explains risk values if buy (book, credit card) insecure for all events after it.

Table 5. 8: Risk values if buy (book, credit card) insecure

	Before Adding Security Controls		**After Adding Security Controls**	
	Based on impact categories by expert	**Based on sensitivity analysis result**	**Based on impact categories by expert**	**Based on sensitivity analysis result**
Send buy request to delivery agent insecure	0.38	0.38	0.38	0.04
Write order data incorrectly	0.25	0.38	0.25	0.04

As we can see from the tables in this subsection the risk values will be decrease more after add specified security controls.

5.1.1.3 Percent error for the two methods that we use for impact analysis

In this subsection we will compare the two methods that we use for impact analysis. We will compare the two method before adding security controls using percent error. Percent error is used when comparing an experimental result E with a theoretical value T that is accepted as the "correct" value to check for consistency.

$$\text{percent error} = |T - E| / T \times 100\%.$$

We will calculate the percent error to compare between risk values calculated based on severity categories specified by expert and risk values based on worst case of sensitivity analysis. For our purpose the risk values based on impact categories by expert is accepted as the "correct" value since we consider it more precise than the other.

We will calculate the average for percent error for risk values separately in three categories:

High risk(over 0.5)

Medium risk(0.35-0.5)

Low risk (0.2-0.35)

The following tables explain risk values according to specified category. As we can see for example in table 5.9 the high risk values.

Table 5. 9: High risk values(over 0.5)

	Based on impact categories by expert	Based on sensitivity analysis result	Difference	Percent error
If IaaS VM insecure the merchant interface insecure	0.6	0.63	0.03	5.00%
If IaaS VM insecure login info send unsecure	0.51	0.48	0.03	5.88%
If the merchant interface insecure login info send unsecure	0.6	0.5	0.1	16.67%
If the merchant interface insecure info query from database with info disclosure	0.51	0.4	0.11	21.57%
If the merchant interface insecure buy (book, credit card) insecure	0.55	0.42	0.13	23.64%
If login info send unsecure info query from database with info disclosure	0.6	0.47	0.13	21.67%
If login info send unsecure buy (book, credit card) insecure	0.67	0.5	0.17	25.37%
If info query from database with info disclosure buy (book, credit card) insecure	0.54	0.41	0.13	24.07%
Average for percent error for high risk values				17.98%

Table 5. 10 Medium risk values (0.35-0.5)

	Based on impact categories by expert	Based on sensitivity analysis result	Difference	Percent error
If IaaS VM insecure info query from database wih info disclosure	0.46	0.4	0.06	13.04%
If IaaS VM insecure buy (book, credit card) insecure	0.48	0.42	0.06	12.50%

If info query from database with info disclosure replay from database incorrect	0.35	0.38	0.03	8.57%
If replay from database incorrect login denied	0.4	0.48	0.08	20.00%
If replay from database incorrect buy (book, credit card) insecure	0.43	0.32	0.11	25.58%
If login denied buy (book, credit card) insecure	0.41	0.26	0.15	36.59%
If buy (book, credit card) insecure send buy request to delivery agent insecure	0.38	0.38	0	0.00%
Average for percent error for medium risk values				16.61%

Table 5. 11: Low risk (0.2-0.35)

	Based on impact categories by expert	**Based on sensitivity analysis result**	**Difference**	**Percent error**
If IaaS VM insecure replay from database incorrect	0.27	0.34	0.07	25.93%
If IaaS VM insecure login denied	0.24	0.33	0.09	37.50%
If IaaS VM insecure send buy request to delivery agent insecure	0.22	0.37	0.15	68.18%
If the merchant interface insecure replay from database incorrect	0.29	0.32	0.03	10.34%
If the merchant interface insecure login denied	0.25	0.3	0.05	20.00%
If the merchant interface insecure send buy request to delivery agent insecure	0.24	0.36	0.12	50.00%
If login info send unsecure replay from database incorrect	0.31	0.34	0.03	9.68%

If login info send unsecure login denied	0.27	0.32	0.05	18.52%
If login info send unsecure send buy request to delivery agent insecure	0.27	0.42	0.15	55.56%
If info query from database with info disclosure login denied	0.3	0.35	0.05	16.67%
If info query from database with info disclosure send buy request to delivery agent insecure	0.23	0.35	0.12	52.17%
If replay from database incorrect send buy request to delivery agent insecure	0.2	0.29	0.09	45.00%
If login denied send buy request to delivery agent insecure	0.2	0.25	0.05	25.00%
If buy (book, credit card) insecure send buy request to delivery agent insecure	0.38	0.38	0	0.00%
If buy (book, credit card) insecure write order data incorrectly	0.25	0.38	0.13	52.00%
Average for percent error for low risk values				32.44%

Table 5.12 explains the average of errors for book purchase scenario.

Table 5. 12: Average of errors for book purchase scenario

Risk category	**Percent error**
High risk(over 0.5)	17.98%
Medium risk(0.35-0.5)	16.61%
Low risk (0.2-0.35)	32.44%
Total average for Percent error	**22.34%**

As we can see from table the average of error is not big.

5.1.1.4 Confusion matrix for the two methods that we use for impact analysis

Confusion matrices are the major mean to evaluate errors in classification problems. They encode the complete specification of misclassifications: the numbers of misclassified items for each pair {original class in which items should be classified, incorrect class in which items are erroneously classified} (Beauxis & Hardman, 2014).

The statistical error analysis, confusion matrix etc. require large number of events, so we combined high with medium, to have more risk values in the analysis.

For our purpose we will use the confusion matrix to compare between risk values calculated based on the two methods that we use for impact analysis. The risk values based on impact categories by expert will be consider as the actual values and risk values based on worst case of sensitivity analysis as predicted values.

Table 5.13 explains the confusion matrix for book purchase scenario.

Table 5. 13: A confusion matrix for book purchase scenario

	Predicted high-medium	Predicted low	Total
Actual high-medium	13	2	15
Actual low	10	10	20
Total	23	12	35

High-medium risk(>= .35), Low risk (< .35)

From this matrix we calculated the following:

High-medium accuracy = predicted high-medium / actual high-medium = 13/1 5= 86.6%

Low accuracy = predicted low / actual low= 50%

Misclassification Rate: Overall, how often is it wrong?

High-medium error rate = 2/15=13.3%

Low error rate = 50%

As we can see from this matrix the high-medium accuracy is large and the high-medium error rate is small.

Therefore, the sensitivity analysis can be used to identify the risk in an automated way without expert intervention.

5.1.2 Hybrid live VM Migration scenario results

In this subsection we will discuss the results for the Hybrid live VM Migration scenario. The following tables explain the risk values based on impact according to severity categories specified by expert and impact according to worst case of sensitivity analysis result with the difference between their values and the percent error. For example table 5.14 explains risk values if destination request VM profile insecurely.

Table 5. 14: Risk values if destination request VM profile insecurely.

	Based on impact categories by expert	**Based on sensitivity analysis result**	**Difference**	**Percent error**
The profile of VM sending unsecure	0.33	0.70	0.375	115.38%
Request for log file be unsecure	0.23	0.51	0.285	126.67%
Latest log files transferring unsecure	0.17	0.39	0.225	136.36%
Destination request for updated dirty pages be unsecure	0.14	0.31	0.175	129.63%
Source replies with updated dirty pages unsecure	0.11	0.25	0.1375	122.22%
Destination send synchronization info for source not done	0.08	0.59	0.515	686.67%

Table 5. 15 explains risk values if the profile of VM sending unsecure for all event after it.

Table 5. 15: Risk values if the profile of VM sending unsecure

	Based on impact categories by expert	Based on sensitivity analysis result	Difference	Percent error
Request for log file be unsecure	0.58	0.56	0.02	3.45%
Latest log files transferring be unsecure	0.42	0.41	0.01	2.38%
Destination request for updated dirty pages be unsecure	0.32	0.31	0.013	4.02%
Source replies with updated dirty pages unsecure	0.27	0.25	0.016	6.02%
Destination send synchronization info for source not done	0.13	0.45	0.317	238.35%

Table 5.16 explains risk values if request for log file be unsecure for all event after it.

Table 5. 16: Risk values if request for log file be unsecure

	Based on impact categories by expert	Based on sensitivity analysis result	Difference	Percent error
Latest log files transferring be unsecure	0.51	0.46	0.05	9.80%
Destination request for updated dirty pages be unsecure	0.38	0.34	0.04	10.53%
Source replies with updated dirty pages unsecure	0.31	0.26	0.05	16.13%
Destination send synchronization info for source not done	0.11	0.36	0.25	227.27%

Table 5.17 explains risk values if latest log files transferring be unsecure for all event after it.

Table 5. 17:Risk values if latest log files transferring be unsecure

	Based on impact categories by expert	Based on sensitivity analysis result	Difference	Percent error
Destination request for updated dirty pages be unsecure	0.68	0.39	0.29	42.65%
Source replies with updated dirty pages unsecure	0.52	0.28	0.24	46.15%
Destination send synchronization info for source not done	0.14	0.30	0.16	114.29%

Table 5.18 explains risk values if destination request for updated dirty pages be unsecure for all event after it.

Table 5. 18: Risk values if destination request for updated dirty pages be unsecure

	Based on impact categories by expert	Based on sensitivity analysis result	Difference	Percent error
Source replies with updated dirty pages unsecure	0.56	0.34	0.22	39.29%
Destination send synchronization info for source not done	0.11	0.25	0.14	127.27%
If source replies with updated dirty pages unsecure then destination send synchronization info for source not done	0.15	0.23	0.08	53.33%

Table 5.19 explains risk values if source replies with updated dirty pages unsecure for the event after it.

Table 5. 19: Risk values if source replies with updated dirty pages unsecure

	Based on impact categories by expert	Based on sensitivity analysis result	Difference	Percent error
Destination send synchronization info for source not done	0.15	0.23	0.08	53.33%

5.1.2.1 Percent error for the two methods that we use for impact analysis

In this subsection we will calculate the percent error to compare between risk values calculated based on severity categories specified by expert and risk values based on worst case of sensitivity analysis for the Hybrid live VM Migration scenario.

The following tables explain risk values according to specified category with the percent error for each category. As we can see for example in table 5.20 the high risk values.

Table 5. 20: High risk values (over 0.5)

	Based on impact categories by expert	Based on sensitivity analysis result	Difference	Percent error
If the profile of VM sending unsecure then request for log file be unsecure	0.58	0.56	0.02	3.45%
If request for log file be unsecure then latest log files transferring be unsecure	0.51	0.46	0.05	9.80%
If latest log files transferring be unsecure then destination request for updated dirty pages be unsecure	0.68	0.39	0.29	42.65%

If latest log files transferring be unsecure then source replies with updated dirty pages unsecure	0.52	0.28	0.24	46.15%
If destination request for updated dirty pages be unsecure then source replies with updated dirty pages unsecure	0.56	0.34	0.22	39.29%
Average for percent error for high risk values				28.27%

Table 5. 21: Medium risk values (0.35-0.5)

	Based on impact categories by expert	**Based on sensitivity analysis result**	**Difference**	**Percent error**
If the profile of VM sending unsecure then latest log files transferring be unsecure	0.42	0.41	0.01	2.38%
If request for log file be unsecure then destination request for updated dirty pages be unsecure	0.38	0.34	0.04	10.53%
Average for percent error for medium risk values				6.45%

Table 5. 22: Low risk values (0.2-0.35)

	Based on impact categories by expert	**Based on sensitivity analysis result**	**Difference**	**Percent error**
If destination request VM profile insecurely then the profile of VM sending unsecure	0.33	0.70	0.38	115.38%

If destination request VM profile insecurely then request for log file be unsecure	0.23	0.51	0.29	126.67%
If the profile of VM sending unsecure then destination request for updated dirty pages be unsecure	0.32	0.31	0.01	4.02%
If the profile of VM sending unsecure then source replies with updated dirty pages unsecure	0.27	0.25	0.02	6.02%
If request for log file be unsecure then source replies with updated dirty pages unsecure	0.31	0.26	0.05	16.13%
Average for percent error for low risk values				53.64%

Table 5.23 explains the average of errors for the Hybrid live VM Migration scenario.

Table 5. 23: Average of errors for the Hybrid live VM Migration scenario.

Risk category	**Percent error**
High risk(over 0.5)	28.27%
Medium risk(0.35-0.5)	6.45%
Low risk (0.2-0.35)	53.64%
Total average for Percent error	29.46%

5.1.2.2 Confusion matrix for the two methods that we use for impact analysis

Table 5. 24 explains the confusion matrix for the Hybrid live VM Migration scenario.

Table 5. 24: A confusion matrix for hybrid live VM Migration scenario

	Predicted high-medium	Predicted low	Total
Actual high-medium	4	3	7
Actual low	6	8	14
Total	10	11	21

High-medium risk(>= 0.35), Low risk (< 0.35)

From this matrix we calculated the following:

High-medium accuracy = predicted high-medium / actual high-medium =4/7=57.1%

Low accuracy = predicted low / actual low=8/14=57.1

Misclassification Rate:

High-medium error rate = 3/7=42.9%

Low error rate = 6/14=42.9%

However, the high error for this scenario is due to the low number of events.

5.2 Comparison Between The Related Work And Proposed Methodology

The proposed method was compared with other methods from the literature. The comparisons show that the proposed method is effective as explained in the following:

▶ (Catteddu & Hogben, 2009), (Zhang et al., 2010) methods don't calculate likelihood quantitatively.

▶ (Sangroya et al., 2010) method need past statistics about the service provider.

▶ (Saripalli & Walters, 2010) method does not cover risks during all the stages of the cloud lifecycle.

▶ (Burton et al., 2010) is just a paradigm. There was no implementation nor was there any method suggested to calculate risk score.

▶ (Khan et al., 2012) do not consider other security requirements that are unique to cloud platforms.

▶ (Islam et al., 2017) identify risks based on the relative importance of the migration goals.

Table 5.25 explains comparison for the proposed method with "comprehensive and shared risk assessment method for cloud computing" proposed by (Drissi et al., 2015)

Table 5. 25: Comparison for the proposed method with Drissi et al. method

	Drissi et al. method	**Proposed method**
Use values specified base on	Actor view	**Experts**
Value of risk for	Threats	**Events**
Use Empirical formula	Use (less accurate)	**Not use (more accurate)**
Follow standard	Don't follow	**Follow**
Scenario based	No	**Yes**

None of the methods in related work are scenario based to fit the dynamic nature of the cloud computing environment and be possible to use at any stage of development.

5.3 Research Outcomes

From this research, we specify framework and propose methodology to calculate the risk factor that:

- Enable SaaS providers to evaluate and manage the security of the service they provide with the goal of mitigating risk.
- If there are any security control added or if at any time want to add new Iaas provider as a destination may be migrate to it (migration for service to more powerfull VM) or the Iaas provider itself add new control there will be possible to change in the percentage of states for events and components. Therefore, the Risk values will be updated as the system being changed to be able to recommend countermeasures based on current level of risk.
- Using existing tools for software modelling and analysis and risk assessment to enable SaaS providers to calculate security risk interactively. Therefore, giving enterprises more knowledge about the risks related to the assets they provide to provide protection for it.

CHAPTER 6

CONCLUSION AND FUTURE WORK

Chapter 6:Conclusion And Future Work

6.1 Conclusion

Network security risks will always be with us. The downside of being in a highly connected network is that we are all connected with the best and worst of society. The best we can do is to manage the risks: employ technological and procedural mitigation while at the same time allowing businesses to thrive.

However, cloud computing uses networked infrastructure, software and computing power to provide resources to customers in an on-demand environment. While clients may be attracted to the SaaS model due to the resource savings and reduced responsibility for administering the cloud environment, they should be aware that these models also correspond to a greater loss of control of the environment housing their sensitive data. Therefore, he have to ensure that the required security measures will be met and maintained by the cloud service provider in the duration of the agreement. Therfore, despite the fact that cloud computing offers many cost benefits for their cloud consumers, number of security risk are emerging in association with cloud usage that need to be assessed

However, Risk assessment is a complex undertaking, usually based on uncertain information while managing uncertainties is a tedious task and the nature of occurrence of threats and vulnerabilities change rapidly.

This study reviewed the different existing methods for security risk assessment in cloud computing and proposes a scenario-based methodology for security risk assessment in cloud computing. The proposed methodology will enable the cloud provider to assess the risk based on existing scenario, and prioritizing security risks. It is using Bayesian network for likelihood determination that allows entering evidence. So probabilities in the network are updated when new information is available. In addition, the proposed method enables to specify impact base on severity categories specified by expert or worst case of sensitivity analysis result for assessing the severity without expert involvement in simple and fast way.

We applied the proposed method on two important case studies where we needed to imply high security. Therefore, in order to develop an efficient security

module, it is necessary to clearly identify the existing risk. Depending on the assessment results, the cloud provider can establish controls so that the risk can be reduced to an acceptable level.

We Applied the methodology after using security controls to verify the risk level reduction or mitigation. The result analysis show significant reduction for specific risk values and mitigation for significant threats.

In addition, we compare the two methods that we use for impact analysis. The results show the total average of errors between risk values calculated base on severity categories specified by expert and worst case of sensitivity analysis is 10% before add security control and 16% after add security control. Therefore, the results show sensitivity analysis can identify the significant risk in an automated way without expert intervention.

Moreover, we compare the proposed method with the existing methods base on assessing the dynamic scenarios. As we saw none of the existing methods is scenario based to fit the dynamic nature of the cloud computing. Moreover, none of them can be use at any stage of development life cycle.

6.2 Research contribution

The contribution of this research are:

1) A Scenario-Based Methodology for Cloud Computing Security Risk Assessment
2) Verification of the methodology using two case studies:
   - E-commerce application
   - Live VM Migration
3) Verification of the methodology by applying security controls on a case study and measuring the effect of risk mitigation.

6.3 Future work

Cloud security is the most significant obstacles to the spread of Cloud Computing. The future developments of this research are:

- Develop a fully automated tool for the proposed methodology.

- Dynamic assessment method that update existing risk using the results from ongoing monitoring tools and dynamically add security controls base on predicted risk.

Dynamic risk assessment is frequent updates of risk evaluation information to evaluate risk exposure, as close as possible to real-time (López et al., 2013). This kind of thinking is especially important in dynamic environments. On the other hand, cloud monitoring is needed for continuous measurements to assess resources or applications on cloud platform in terms of performance, reliability, power usage, ability to meet SLA, security, etc. (Alhamazani et al., 2015). Therfore, accurate and fine-grained monitoring activities are required to efficiently operate Cloud Computing platforms and to manage their increasing complexity and security requirements.

References:

Aiash, M., Mapp, G. & Gemikonakli, O., 2014. Secure Live Virtual Machines Migration: Issues and Solutions. In *The 28th IEEE International Conference on Advanced Information Networking and Applications (AINA-2014)*. Canada, 2014.

AIK, W.F. & SANG, F.Y., 2013. *AN UPDATE ON THE REVISION TO MIL-STD-882E*. SYSTEM SAFETY SOCIETY SHARING SESSION.

Ajam, M., 2013. *CAM2P, Framework, Maturity, Methodology, PMBOK Guide*. [Online] Available at: http://blog.sukad.com/differences-between-standard-framework-methodology/.

Alhamazani, K. et al., 2015. An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state-of-the-art. *Springer-Verlag New York, Inc.*.

Alturkistani, F. & Emam, A., 2014. A Review of Security Risk Assessment Methods in Cloud Computing. *New Perspectives in Information Systems and Technologies*, pp.pp 443-453.

Amini, A., Jamil, N., Ahmad, A.R. & Z`aba, .M.R., 2015. Threat Modeling Approaches for Securing Cloud Computing",. *Journal of Applied Sciences*, pp.953-67.

Ammar, H.H., 2006. *Introduction to Risk Management And Software Architecture Risk Assessment*.

Amyot, D., Hart, N., Logrippo, L. & Forhan, P., 1998. Formal Specification and Validation using a Scenario-Based Approach: The GPRS Group-Call Example. *Research Gate*.

Baggar, C. & Sinha, R., 2013. Identific For Cloud Computing In IAAS, PAAS And SAAS. *International Journal of Computer & Organization Trends*.

Beauxis, E. & Hardman, L., 2014. Simplifying the Visualization of Confusion Matrix. In *Benelux Conference on Artificial Intelligence*., 2014.

Bernard, L., Bolesta, M., Gelatte, J. & Evanchik, M., 2011. A Risk Assessment Framework for Evaluating Software-as-a-Service (SaaS) Cloud Services Before Adoption.

Björklund, A.E., 2002. Survey of Approaches to Improve Reliability in LCA. *Int. J. of Life Cycle Assessment*, pp. pp. 64-72.

Burton, S., Pauley, W. & Kaliski, J., 2010. Toward Risk Assessment as a Servicei n Cloud Environments.

Catteddu, D. & Hogben, G., 2009. *cloud computing :Benefits, risks and recommendations for information security*". The European Network and Information Security Agency (ENISA).

Cloud Security Alliance , 2013. The Notorious Nine: Cloud Computing Top Threats in 2013.

Cloud Security Alliance, 2017. CLOUD SECURITY ALLIANCE: The Treacherous 12 - Top Threats to Cloud Computing + Industry Insight., 2017.

DEPARTMENT OF DEFENSE, 2012. *Standard Practice: System Safety (MIL-STD-882E)*.

Drissi, S., Benhadou, S. & Medromi, H., 2015. A New Shared and Comprehensive Tool of Cloud Computing Security Risk Assessment. In *The International Symposium On Ubiquitous Networking, At Casablanca*. Morocco, 2015.

Drissi, S., Houmani, H. & Medromi, H., 2013. Survey:Risk assessment forcloud computing. *IJACSA*.

Federal communications commission, 2012. Cyber Security Planning Guide.

Fenton, N.E., Neil, M. & Caba, J.G., 2007. Using Ranked Nodes To Model Qualitative Judgments In Bayesian Networks. *IEEE Transactions On Knowledge And Data Engineering*.

Fit´o, J.O., Mac´ıas, M. & Guitart, J., 2010. Toward Business-driven Risk Management for Cloud Computing. In *2010 International Conference on Network and Service Management*. Canada, 2010. IEEE.

Frey, H.C., Mokhtari, A. & Danish, T., 1999. Evaluation of Selected Sensitivity Analysis Methods Based Upon Applications to Two Food Safety Process Risk Models.

Hashizume, K., 2013. *A Reference Architecture For Cloud Computing And Its Security Applications*. Florida Atlantic University.

Hassan, A. et al., 2003. Severity Analysis at Architectural Level Based on UML Diagrams. In *PROCEEDINGS of the 21st INTERNATIONAL SYSTEM SAFETY CONFERENCE*., 2003.

Hearty, Fenton, N., Marquez, D. & Neil, M., 2009. Predicting Project Velocity in XP Using a Learning Dynamic Bayesian Network Model. *IEEE Transactions On Software Engineering*.

Islam, S., Fenz, S., Weippl, E. & Mouratidis, H., 2017. A Risk Management Framework for Cloud Migration Decision Support. *Journal of Risk and Financial Management*.

Joint Task Force Transformation Initiative, 2012. *Guide for Conducting Risk Assessments*.

Juncai, S. & Shao, Q., 2011. Based on Cloud Computing E-commerce Models and Its Security. *International Journal of e-Education, e-Business, e-Management and e-Learning*.

Kaindl, H., 2011. *Scenario-based Requirements Engineering and User-Interface Design*. Vienna University of Technology, ICT.

Khan, A.U. et al., 2012. Security Risks and their Management in Cloud Computing. *4th International Conference on Cloud Computing Technology and Science*.

Kragt, M.E., 2009. *A beginners guide to Bayesian netnetwork modelling for integrated catchment management*. Technical Report No. 9. LANDSCAPE LOGIC.

Kuyoro, S.O., Ibikunle, F. & Awodele, O., 2011. Cloud Computing Security Issues and Challenges. *International Journal of Computer Networks (IJCN)*.

Leitold, F. & Hadarics, K., 2012. Measuring security risk in the cloud-enabled enterprise. In *2012 7th International Conference on Malicious and Unwanted Software (2012)*., 2012.

López, D., Pastor, O., Javier, L. & Vill, G., 2013. Dynamic Risk Assessment In Information Systems: State-Of-The-Art. In *6th International Conference on Information Technology*., 2013.

Lourida, K., Mouhtaropoulos, A. & Vakaloudis, A., 2013. Assessing Database and Network Threats in Traditional and Cloud Computing. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*.

Narander, K. & Swati, S., 2014. An Efficient Live VM Migration Technique in Clustered Datacenters. *Research Journal of Recent Sciences*.

National Institute of Standards and Technology, 2012. *Guide for Conducting Risk Assessments, NIST Special Publication 800-30*.

Onwudebelu, U. & Chukuka, B., 2012. Will adoption of cloud computing put the enterprise at risk? In *2012 IEEE 4th International Conference on Adaptive Science & Technology (ICAST)*. Ghana , 2012. IEEE.

Peiyu, L.I.U. & Dong., L.I.U., 2011. The new risk assessment model for information system in cloud computing environment. *Procedia Engineering*, pp.Pages 3200-3204.

Pescatore, J., 2004. Application Security by Design :SECURITY AS A COMPLETE LIFECYCLE ACTIVITY. *Gartner Research*.

Rouse, M., 2010. *Risk assessment framework (RAF)*. [Online] Available at: https://searchcio.techtarget.com/definition/risk-assessment-framework-RAF.

Said, F.H., Hassouneh, Y. & Ammar, H., 2011. Security Risk Assessment of Software Architecture. *ICCTA*.

Saiedian, H., Anan, M. & Kumarakulasingam, P., 2005. Scenario-based requirements analysis techniques for real-time software systems: A comparative evaluation. *Requirements Engineering*.

Sangroya, A., Kumar, S., Dhok, J. & Varma, V., 2010. Towards Analyzing Data Security Risks in Cloud Computing Environments. In *International Conference on Information Systems, Technology, and Management (ICISTM 2010)*., 2010.

Saripalli, P. & Walters, B., 2010. QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. In *In the Proceedings of the IEEE 3rd International Conference on Cloud Computing*., 2010.

Sen, J., 2016. Security and Privacy Issues in Cloud Computing.

Simmonds, D. & Wahab, A., 2012. Public Cloud Computing vs. Private Cloud Computing: How Security Matters.

Stoneburner, G., Goguen, A. & Feringa, A., 2002. *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-30.

Subashini, S. & Kavitha, V., 2011. Review A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*.

Tanimoto, S., Hiramoto, M., Iwashita, M. & Sato, H., 2011. Risk Management on the Security Problem in Cloud Computing. In *2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering*. South Korea, 2011. IEEE.

Varsha, V. & Kousar, H., 2016. A Survey on Cloud Computing Its Application and Security Issues. *International Journal Of Advancement In Engineering Technology, Management and Applied Science (IJAETMAS)*, pp.90-98.

Vikas, S., Gurudatt, K., Vishnu, M. & Prashant, K., 2013. Private Vs Public Cloud. *International Journal of Computer Science & Communication Networks*, pp.79-83.

Zhang, J., Sun, D. & Zhai, D., 2012. A research on the indicator system of Cloud Computing Security Risk Assessment. In *2012 International Conference on Quality, Reliability, Risk,Maintenance, and Safety Engineering (ICQR2MSE)*., 2012.

Zhang, X., Wuwong, N., Li, H. & Zhang, X., 2010. Information security risk management framework for the cloud computing environments. In *10th IEEE International Conference on Computer and Information Technology (CIT 2010)*. China, 2010.