Sudan University of Science and Technology
(SUST)

College of Graduate Studies

A Design of an Econometric model for evaluating the Security in Cloud Computing Environment

تصميم نموذج إقتصادي لتقدير الأمن في بيئة الحوسبة السحابية

A Thesis Submitted for the fulfillment of the requirement of the degree of PhD in Computer Science

By:
Nahla Murtada Ahmed

Supervisor:
Professor. Dr. Ali Mili

January 2017

DEDICATION

This dissertation is dedicated to my husband Dr.Yahia Abdallah, who helped and encouraged me to realize my dreams and finish my dissertation.

To my Parents Murtada and Salwa, for helping me in all things, thanks for your valuable support.

To my dear brother Engineer. Ahmed and my dear sister Amal.

To my lovely kids Khalid, Yumna and Menna.

ACKNOWLEDGMENTS

First I thank Allah for helping me to complete this research, and I would like to express my special deep appreciation and thanks to my advisor Professor Dr. Ali Mili for the valuable guidance and feedback, I appreciate all his contributions, ideas, and time, to make my Ph.D. experience productive and stimulating.

I would also like to thank professor Eiz-aldeen Osman, Dr. Yahia Abdalla, Dr. Osama Rayis, Dr. Rashid, Dr. Hisham abu-shama, Dr Afraa, Dr. Mohammed Abdel-hameid, Engineer Abdelrahman Almamoun and engineer Mohammed Al-aalem for helping me and giving me many valuable comments and guidelines during my study. I also want to thank them for your innovative and brilliant comments and suggestions.

I would especially like to thank Engineers, Statistician and Economists at SUST, Khartoum University, Cairo University and Sudatel Data Center for helping me to understand the statistical relevant rules, economical relevant aspects and a cloud computing operations in a real life which helped me to obtain realistic and reasonable results. All of you have been there to support me when I built the proposed approaches and when I collected the relevant data.

Finally, I am also thankful to several colleagues at Sudan University of Science and Technology (SUST) for their help and support. Their participations are sincerely appreciated and gratefully acknowledged.

PUBLICATION BASED ON THIS THESIS

1. Nahla Murtada, 2013. Measuring the cybersecurity of cloud computing: A stakeholder centered economic approach, *Proceedings - International Conference on Computer, Electrical and Electronics Engineer (ICCEEE 2013)*, pp.294–299.
2. Nahla Murtada, 2016a. Comperhensive Model for Building Presice MFC Matrices for Cloud Computing, In *10TH INTERNATIONAL CONFERENCE ON COMPUTING IN ARABIC (ICCA)*.
3. Nahla Murtada, December 2016b. Measuring Cloud Security Risk by Mean Failure Cost, *2016 IEEE Symposium Series on Computational Intelligence (IEEE SSCI 2016 Greece)*.

4. نهلة مرتضى. 2016 , قياسية مبتكرة لحساب متوسط تكلفة الفشل في الحوسبة السحابية من المنظور الإقتصادي, الدورة العاشرة للمؤتمر الدولي لعلوم وهندسة الحاسوب (ايكا ICCA) بالتزامن مع الدورة الثالثة للمؤتمر الدولي لتقنيات المعلومات والاتصالات في التعليم والتدريب: (تيسات TICET**).**

ABSTRACT

Cloud computing offers an innovative business model for all cloud enterprises to serve IT services with no need to have technical details. The extreme growth of cloud usage increases the probability of threats occurrence, which in turn leads to financial and other losses. So there is a need to use appropriate metrics to assess the failure cost among cloud stakeholders according to their different needs; we propose a measure called "Mean Failure Cost" (MFC) which quantifies the impact of failure (per unit of time) by representing the losses for each stakeholder as a result of possible security failure.

This study investigates this MFC measure which has been adapted to cloud computing by proposing four innovative models: The main model is "The Abstract Representation Model" which is used as a generic model, and then the MFC metric is enriched by proposing three expanded models which are used to refine the MFC cyber-security measure, these new expanded models are: "Multi-dimensional MFC model" (M^2FC), "Service Based MFC Model (SBMFCM)" and "The Hybrid Model", these models are used to serve different cloud sectors. The MFC matrices are filled by empirical data with analytical reasoning, these data is used as a "Default Data" which leads to gain reasonable, accurate and precise results that are compliant with a disciplined "Probability Disruption Rule", cloud experts can re-adjust these default data. Some of Verification and Validation (V&V) measures are used to reduce the failure cost; these models can be evaluated using an innovative cost/benefit analysis model by matching the deployment cost of these V&V measures against the benefit.

These new expansions on MFC give us a clear refinement, accurate estimation and useful interpretation for security related decision-making. Moreover, all proposed models of the MFC provide a unified model of security concepts because security lacks a clear taxonomy of all MFC parameters which leads to the improvement of the system's software quality.

The overall aim of this study is to refine, investigate and adapt the MFC model with cloud computing systems by using cloud-specific knowledge.

These aspects are supported by an automated tool which aim to fill all MFC matrices based on empirical data and analytical reasoning then evaluate the obtained results using economical based approaches that help the decision makers to decide whether the measure is worthwhile or not and expected results are achieved.

المستخلـــــص

قدمت الحوسبة السحابية نموذج عمل لكل المؤسسات لتتمكن من تقديم خدمات تقانة المعلومات بدون الحاجة لمعرفة التفاصيل الفنية, نتيجة لذلك إزدادت إحتمالية حدوث المهددات للأنظمة، مما يسبب الخسارة المالية، بالتالي ظهرت الحاجة لطرق لقياس وتقييم الخسارة الناتجة عن توقف الأنظمة على كل شركاء الحوسبة السحابية الذين لديهم متطلبات مختلفة. يجب أن تستصحب طريقة القياس طبيعة الشركاء في نظام الحوسبة السحابية ومتطلبات أنظمة الحوسبة السحابية واهم المهددات لانظمة الحوسبة السحابية والتي بدورها تختلف من صاحب مصلحة لآخر، تسمى هذه الطريقة متوسط تكلفة الفشل والتي تقوم بتقييم أثر الأعطال (في وحدة الزمن) عبر تمثيل الخسارة التي يتعرض لها الشركاء نتيجة للعطل الذي قد يحدث بالنظام.

تقوم هذه الدراسة بالتحقيق في قيم متوسط تكلفة الفشل (م ت ف) والتي تم تطويرها لتتوائم مع نظام الحوسبة السحابية عبر تقديم أربعه نماذج إبتكارية: النموذج الاساسي وهو "نموذج التمثيل المجرد" والذي إستخدم كنظام عام، ثم نموذج (م ت ف) الذي تم تحسينه عبر إقتراح ثلاث نماذج إستخدمت لتحسين القياسات المختصة بالتأمين وهي: "نموذج متوسط تكلفة الفشل متعدد الأبعاد" و "نموذج متوسط تكلفة الفشل المعتمد على الخدمة" و "النموذج الهجين"، وبالتالي هذه النماذج تخدم قطاعات مختلفة. هذه النماذج تقوم بإعداد المصفوفات المستخدمة في نظام متوسط تكلفة الفشل عبر بيانات تجريبية وعبر إستخدام بيانات ناتجة عن التحليل المنطقي، تعتبر هذه بيانات "بيانات إفتراضية" والتي بدورها تعطي نتائج مناسبة ودقيقة وذلك عن طريق تطبيق "قانون التوزيع المحتمل" بصورة منضبطة وصحيحة, يمكن للخبراء في المجال إعادة ضبط هذة القيم الإفتراضية، وتستخدم بعض نظم قياس التحقق والتثبت لتقليل قيمة الخسارة بسبب توقف النظم، يمكن تقييم هذه النماذج بإستخدام نظام مبتكر لنموذج لحساب الثمن والفوائد المجنية وذلك عبر مقاربة ثمن تطبيق نظام التحقق والتثبت مع الفوائد المجنية.

هذا التوسع في نموذج متوسط تكلفة الفشل سيعطي تحسين واضح وتخمين صائب ودقيق وتفسير مفيد لعملية إتخاذ القرارات المتعلقة بأمن المعلومات، هذا بالإضافة لأن كل النماذج المقترحة لنموذج متوسط تكلفة الفشل أعطت نموذج موحد لمفاهيم التأمين حيث أن نظم التأمين تعاني من عدم توحيد التصنيف لمعاملات نظام متوسط تكلفة الفشل الأمر الذي أدى لتحسين جودة أنظمة البرمجيات.

الهدف العام لهذه الدراسة هو التحسين و التحقق من نموذج متوسط تكلفة الفشل وموائمته مع بيئة الحوسبة السحابية بإستخدام المعارف الخاصة بالحوسبة السحابية.

طرق القياس هذه تم تقييمها بإستخدام نموذج حساب الثمن والفوائد المجنية لتقديم دعم كمي مبني على أسس إقتصادية. معظم النتائج تم الحصول عليها بواسطة بناء أداة مؤتمتة تم تطويرها لتعبئة المصفوفات المستخدمة بواسطة بيانات تجريبية ثم إدخالها على هذة الأداة وجاءت النتائج المتحصل عليها كما هو متوقع.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATION

Abbreviation	Meaning
AES	Advanced Encryption Standard
ALE	Annual Loss Expectancy
API	Application Programming Interface
APT	Advanced Persistent Threats
APTA	The American Public Transportation Association
CCTA	Central Communication and Telecommunication Agency
CERT	Computer Emergency Response Team
COTS	Commercial off the Shelf
CRAMM	CCTA Risk Analysis and Management Method
CSA	Cloud Security Alliance
CSPs	Cloud Service Providers
DDoS	Distributed Denial of Service
DoS	Denial of Service
DP	Dependency Matrix
ENISA	The European Union Agency for Network and Information Security
IaaS	Infrastructure as a Service
ICT	Information and Communication Technologies
ISTR	Internet Security Report
ISTRs	Internet Security Threat Reports
IT	Information Technologies
M^2FC	Multi-dimensional of the MFC model
MFC	Mean Failure Cost
MTBF	Mean Time To Between Failure
MTTCF	Mean Time To Catastrophic Failure
MTTD	Mean Time To Detection
MTTD	Mean Time To Detection
MTTE	Mean Time To Exploitation
MTTF	Mean Time To Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
NIST	National Institute of Standards and Technology

NISTIR	(NIST) Internal Reports
NoC	No Component has been Compromised
NoR	No Requirement has been violated
NoT	No Threat has been Materialized
NPV	Net Present Value
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PaaS	Platform as a Service
PCS	Public Cloud Server
PI	Personal Information
PII	Personally Identifiable Information
PTM	Probability of Threat Materialized
ROI	Return On Investment
ROSI	Return on Security Investment
RQ	Research Question
RTP	Risk Treatment Plans
SaaS	Software as a Service
SBMFCM	"Service Based MFC Model
SEI	Software Engineering Institute
SLA	Service Level Agreements
SLE	Single Loss Expectancy
SLR	Systematic Literature Review
SLR	systematic Literature Review
SME	Small Medium Enterprise
SMEs	Subject Matter Experts
SPII	Sensitive Personally Identifiable Information
SQA	Software Quality Assurance
ST	Stake Matrix
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service and Elevation of privilege
TIM	Threat Impact Matrix
TV	Threat Vector
UPS	Uninterruptible Power Supplies
V&V	Verification and Validation

V&V	Verification and Validation
VBSE	Value-Based Software Engineering
VMs	Virtual Machines
WWW	World Wide Web

CHAPTER ONE

CLOUD COMPUTING ISSUES

1.1. Introduction

Throughout its short history, the discipline of computing has evolved through many different paradigms, starting with mainframe-based computing, where computing services were delivered by institutional departments responsible for running and maintaining a mainframe computer. In the early eighties, this paradigm was progressively phased out in favor of personal computing, where most of the computing was done in personal workstations, and communication between workstations was supported by networks of various scales, culminating in the World Wide Web (WWW). In the last few years, cloud experts have been witnessing the emergence of a new computing paradigm, whereby end users avail themselves of computing and storage resources delivered by service providers, who commit to manage and maintain vast resources, for which end users are charged according to their use.

The cloud evolution parallels the evolution of other utilities: water utility, electricity utility, gas utility and telephone utility, so with the emergence of cloud computing, end users no longer have to deal with the operation and maintenance of complex workstations, the storage of important information on loose memory devices, downloading software of uncertain origin, etc All these functions are delegated to highly skilled professionals specialized in the operation and maintenance of the cloud infrastructure.

But this paradigm has shortcomings and the most obvious potential of security breakdowns is the large numbers of users and other stakeholders which having access to the cloud computing infrastructure with a complex measures of access privileges (different stakeholders having different privileges, sharing different access rights with others), so it is very difficult for the cloud service provider to ensure the security of the data to be fully protected, and trust issues should be considered from the cloud consumers side.

This study will explore the application of a metric of cyber-security to a cloud computing infrastructure; this metric, will have the following attributes (Aissa et al. 2010b):

- It is not an attribute of the system alone, but varies according to the stakeholder.
- It is not an abstract number on an arbitrary scale, but is rather an economic function expressed in dollars per unit of operation time.
- Because it is expressed in economic terms, this measure enables us to make economically motivated decisions pertaining to cyber-security, such as selecting a cyber-security solution, justifying the cost of a cyber-security solution, sharing the cost of a cyber-security solution over different stakeholders, etc This measure called the *Mean Failure Cost* (*MFC*) is the subject of chapter 3.

Cyber-security metrics are often defined imprecisely, and used improperly. However, our proposed approach on this study is distinguished between how a metric is well defined and how it is practically computed based on this defined metric.

1.2. Problem statement and it's significance

Despite the existence of several researches on cloud computing areas, to the best of our knowledge, there is no research conducted to ***adapt the MFC to all cloud aspects and all cloud service models by the calculation of all the relevant MFC parameters*** to compute how much failure will cost on cloud environment which is our main contribution. There is a need to build ***automated support to computing MFC in the cloud***.

There is a need to consider the variation that may exist between stakeholders, impact, severity, amount, failure cost from one stakeholder to another, from one requirement to another, from one component to another and variance in system specification levels of verification and validation. This will be done by seeking help from stakeholders and engineers, architects, and analysts to have input within their respective *Subject Matter Experts* (SMEs) and intend to make a V&V activity with reducing the failure cost. The National Institute of Standards and Technology Internal Report (NISTIR 7628), Cloud Security Alliance (CSA) and Symantec do not actually do this, but it does provide the data to populate the metrics.

In spite of the existence of quantitative metrics which estimate the attributes like the Mean Time To Failure (MTTF) for reliability and Mean Time Between Failure (MTBF) for maintainability, there is no way to measure directly the dependability of the system or to quantify security threat, this study tries to solve this dependability issue by focusing on the following problems (Abercrombie et al. 2013):

- Until now there are no statistics on the volume of failure cost on cloud computing environment per unit of time.
- One of the most important things is "How to fill the MFC matrices" using interdisciplinary approach which follows the right statistical rules that considering all possible events.
- Distinction between low-stake clauses and high-stake clauses of the requirements.
- There is a need to find sample applications where deployment of the MFC metric shows its usefulness of providing a basis for analysis and decision making.
- Dispatch investment costs among different stakeholders based on their stakes.
- Few people argue that it is too complex to evaluate the failure cost due to heterogeneity of security requirements.

- There is a need to provide metric that measures the failure cost per unit of time. This cost must be balanced against the benefit of operating the system for the same unit of time, to determine the desirability of operating, moreover, MFC should be used to determine how much each stakeholder may stand to lose as a result of, for example, a security failure, a hardware failure or any other service corruption.

1.3. Research Scope

This research is concerned with the estimation of threat probability in cloud computing to compute MFC rather than preventing, detecting and recovering from failure.

This approach is concentrated on the main dimension of dependability attributes such as security, safety and integrity…etc and is not concerned with other marginal attributes such reparability, maintainability survivability and fault tolerant issues on cloud computing.

In addition, this study concern on maximize benefit; minimize cost and quantify failure in security for a given stakeholder.

This research will specialize the MFC to the cloud with using economic function rather than arbitrary abstract scale or possible risk state quantified in monetary terms (dollars per hour), in such a way as to enable rational decision making.

In addition, this study will adopt all main aspects of cloud computing with adoption to all cloud service models (IaaS, PaaS, and SaaS) with the MFC measure by proposing some models that support these adoptions.

Moreover, evaluate the proposed one of these models using V&V measures with economic based approaches such as ROI and NPV which will be discussed later.

1.4. Research Question/Hypothesis/Philosophy

Research questions, research methodologies and research plan are presented in the following sections.

1.4.1. Research Question

These following research questions are addressed:

RQ 1. What information security threats have in cloud computing?

The main objective of this research question is to understand information security threats that are relevant to cloud computing. In addition, the answer of this question will enable us to focus on cloud computing issues and to consider some statistical reports that consider seriously the internet security threats report which are used for identifying information security threat in cloud computing environment rather than the other traditional computing environment.

RQ 2. Which framework is suitable for developing security metrics?

This research aims to build framework that is compatible with the MFC metric which is followed in identifying information security metrics. This is question is important because several frameworks may be found in literature but some of which may not be effective in identifying security metrics and also due to absence of a clear refinement of the visible framework, numerous information security metrics may be found and may lead to vague results, so in this study the framework should be clearly defined and measured for developing security metrics.

RQ 3. What is the suitable metrics used to asses failure cost in cloud computing?

There is a need to consider some types of metrics considering the variance that may exist between stakeholders, security requirement, components and threats. This study will be considered these types of metrics that are used to assess the mean failure cost on cloud computing.

RQ 4. How can the decision makers tell whether the V& V action is worthwhile or not?

Using econometrics approach as a measure of MFC metrics will be useful to those organizations operating in the cloud which intend to make V&V actions and reduce the failure cost, so it may be useful to provide a novel way to verify this MFC metric using a cost/benefit analysis measures which is called the Return On Investment (ROI) which can determine is the V&V actions are worthwhile or not.

1.4.2. Research hypothesis

Security metrics are quantitative measurements which are used to assess security operations in organization environment. They aid the cloud stakeholders to make decisions based on analyzing the cost benefit using MFC metrics which will make big contribution to field of assessing cyber-security in quantitative base. The following points are representing as a research hypothesis:

- MFC can be used to measure probability of failure per unit of time.
- This study assuming that no more than one requirement has been violated at a time.
- This study assuming that no more than one component has been compromised at a time
- This study assuming that no more than one threat has materialized at a time.
- Stakeholders can use the MFC to reduce his/her loss by means of the security measure.
- By using the cost/benefit analysis model, decision makers can determine weather the measure is worthwhile or not.

1.4.3. Research Philosophy

The philosophy of suggested metrics is based on the concept that different stakeholder meet different requirement and variance impact of failures that may exist among stakeholders and different impact, failure severity, failure amount, levels of verification and validation from one requirement to another and also a failure probability is differ across cloud components, so this metric support all these variation aspects.

Boehm and Nowey (Boehme & Nowey 2008) claim that, all dilemmas that arise in software engineering are of an economic nature rather than a technical nature, and that all the decisions ought to be modeled in economic terms: maximizing benefit; minimizing cost and risk. Our work is perfectly compatible with this philosophy using Value-Based Software Engineering (VBSE).

Organization's assessment and cost reduction will be done by considering the following:

- Use MFC to assess "Probability" that specific threat materializes during a unit of operational time (e.g. 1 hour).
- Using comparative data to asses reducing failure progress.
- When using comparative data this will help to extract estimation and producing recommendation.
- Stakeholders can use security measures, and assess their cost effectiveness by matching their implementation cost against their benefits, measured in terms of reduction in MFC.

1.5. Research aims and objectives

The concept of cloud computing has become one of the main topics of discussion in the industry over the past period, so this study will focus, investigate, and discuss the concept of the cloud computing, and its failures impact in the event of security breakdown, in addition to studying the threats and challenges facing this transformation, accordingly the main objectives of this study are:

- Make an empirical research on cyber-security and cloud computing to support the calculation of all the relevant MFC parameters to obtain more realistic results and building an automated tool

that used for computing MFC which has been supported by an economic based decision in the cloud computing aspects.

- Quantify the cost/benefit analysis by maximizing benefit; minimizing cost and risk, because the MFC modeling system security not by an arbitrary abstract scale but rather by an economic function and validate the proposed metrics using empirical observations.
- Propose different models with different choices that help to obtain clear refinement, accurate estimation and useful interpretation for security related decision-making.

1.6. Data collection

On this study, empirical data will be obtained using Systematic Literature Review approach (SLR) which will be collected from different Internet security Threat Reports such as (CSA), Symantec, National Institute of Standards and Technology (NIST) Interagency/Internal Reports (NISTIR), VERIZON, and ENISA (The European Union Agency for Network and Information Security)…etc who are representing as "Threat Working Group" to compile professional opinions on the greatest security issues within cloud computing, these threat groups are:

- In the domain of cloud computing and who attempt to involve many practices which are related to security failure in the event of threat occurrence.
- Cover other issues such as stakeholders environmental needs, cyber-security requirements for system, the impact of threat to our cloud component, financial view, reusability view, and technical view…etc,
- Proposing yearly Internet Security Threat Reports.

All these ISTRs are based on a survey of industry experts (such as Requirements Engineer of System, Architect of System, Verification and Validation Team…etc).

CSA proposed the recent statistical reports based on the number of incidents, these reports have quickly become the industry-standard catalogue of best practices for cloud companies which are used to secure Cloud Computing aspects and provide organizations with an up-to-date, and expert-informed understanding of cloud security concerns in order to make studied risk management decisions regarding cloud adoption strategies.

1.7. Open Issues

According to (Putri and Mganga 2011), although there are several different approaches for developing security metrics, not all approaches have been successful and accepted in the industry. This argument is supported by (Putri and Mganga 2011) who argues that security practitioners often develop technical security metrics which cannot be used to measure organization security using some metrics.

From the literature review, there is still an open research issues that need to be addressed such as:

- The interactions between stakeholders layers of needs.
- There is a need to deploy MFC in a real environment which is useful for verification and validation activity.
- No practical and real studies exist showing the gathered information that deal with a cost per unit of time in a quantitative value.
- Cloud motivates highly skilled hackers, thus creating a need for the security to be considered as one of the top issues while considering Cloud Computing. (Abercrombie et al. 2013).
- Few people argue that it is too complex to evaluate the failure cost due to heterogeneity of security requirements (some requirements carry more stakes than others), and the heterogeneity of system architectures (some components are more security-critical than others), the heterogeneity of security threats (some threats are more threatening than others).

As few studies are proposed in research institutions, there is a need for making more studies about failure cost metrics which can be applied by stakeholders, so this study tries to build framework which combines all the security requirements, stakeholders, cloud architectural components and cloud threat per unit of time through real investigation of the cloud environment, and suggests recommendations for improvement and refinement of failure cost through Verification and Validation (V&V) activity.

1.8. Proposed Solution

This study is concerned with adapting the MFC to cloud computing. The proposed solution is an attempt to contribute on this area. In particular, it considers the following solutions Issues:

- Make an empirical research on cyber-security and cloud computing to support the calculation of all the relevant MFC parameters.
- Collect statistical data that may help to fill the MFC matrices.
- Consider the variance that may exist amongst different stakeholders of the same environment and similarly for a given stakeholder, it reflects the variance that may exist amongst the stakes that attaches to meet each requirement.
- Quantify a failure cost per unit of time in terms of financial loss per unit of operation time (e.g. $/h).
- Using an economically based decision regarding the amount and severity of threat by using the cost/benefit analysis.

- Using suitable measures such as (mitigation measures, hardening measures and evasive Measures) to control stakes matrix, Threat Impact Matrix, Dependency matrix and Threat Vector.
- Dispatch the cost of the measure across cloud stakeholders based on disciplined approach to decide whether the measure is worthwhile or not.
- Build an automated support to computing MFC in the cloud, that may help decision makers to decide whether the measure is worthwhile or not.

To achieve the objectives, this study has been divided to five main phases which are described in the following stages:

1) Shift/Expand the focus of cyber-security.
2) Challenge the traditional metrics.
3) The MFC (deal with all relevant models).
4) Illustration: Cloud Computing.
    a. Analyze different models of cloud computing.
    b. Collect Empirical data in the various terms of the MFC.
    c. Applications for decision support.
    d. "Verify and Validate" the proposed models using economic based approaches.
    e. Compile data with automated support.
5) Summary and Assessment.

1.9. Evaluation Technique

Security measures have been built to assess and estimate the failure cost that may help to avoid or mitigate the occurrence and impact of the risk in the future, and most of cloud companies should use some econometric model as an evaluation technique such as the Return On Investment (ROI), Net Present Value (NPV) to evaluate their selected model, this econometric model may help the decision makers to decide whether the measure is worthwhile or not. This thesis will propose these evaluation techniques with all options of dispatching the investment cost across stakeholders which has been supported by automated tool.

The presented approach will investigate appropriate measures that will be used for each matrix such as (Mitigation measures, Failure Tolerance measures, Fault Tolerance Measures and Evasive Measures …etc), all these aspects will be discussed later in more details.

1.10. Expected outcomes

By proposing this research the following issues will be expected:

- The automated support that computing MFC in the cloud will help cloud companies to easily quantify their benefits.
- An efficient method of self assessment and evaluation for failure cost in cloud organization.
- Comparable results with the benchmark model.
- Software companies can get the benefits of the new model by applying it and get the recommendations that help them to improve there applied processes area.
- Developing and implementing the proposed metrics.

1.11. Concept of Cloud Computing

According to (Mondal & Sarddar 2015), Cloud computing is a new research area that provide utility computing. Utility computing is the packaging of computing resources as a metered service. The idea is to have computing as the fifth utility (after water, electricity, gas and telephony) which is supported by some sort of grid that can be accessed at the point of need without worrying about all the details of the generation of this computation power. The only thing a customer needs to be aware of is the dependability through good quality of service and the price for this utility.

Cloud computing gives advantages of public utilities, such as (Dixit 2015), (Mell et al. 2011)(Avram 2014), (Ms. Shubhangi Ashok Kolte1 & M.Sc. 2016), (Antonopoulos & Gillam 2010),(Quest Technology Management for Buisiness 2015) (Quest Technology Management for Business 2015) (Talukder, A. etal. 2010):

- Efficiency due to higher usage rates of data storage, processing and accessing using servers.
- Economies of scale based on time sharing of computing resources, capacity as virtually unlimited computing power, controlled and managed only by cloud provider rather than by other cloud stakeholders.
- Convenience, because no need for expert users and technical support from subscriber site.
- Dependability, because service is provided by highly trained provider staff.
- Service quality, because data is highly protected against damage and loss.

And according to (NIST in SP 800-145) (Mell et al. 2011), cloud computing may be represented as management and provision of resources, software, applications and information as services over the cloud based on agreed contractual manner (Bohn 2016).

On the other hand, cloud computing is a model for enabling convenience, on demand network access to a shared pool of resources that can be rapidly provided and released with minimal effort and avoid large amount of costs. Cloud Computing has recently emerged as a promising hosting platform that performs an intelligent combination of services, applications, information and infrastructure, information and storage resources and network. However, storing a large amount of data including confidential and secure information on the cloud motivates highly skilled hackers and leads to create a need for the security to be considered as one of the top issues while considering Cloud Computing (Bohn 2016).

In addition, cloud computing is the collection of virtualized and scalable resources and providing *required services* to the users with the "*pay-as-you-go*" strategy, whenever the user requests service, he will pay only for the number of service units they request and consume (Wang et al. 2010).

Cloud computing has simultaneously switched business, the shift from server to service-based thinking and replaced computing from a personal utility to public utility and offers all the advantages of a public utility system, according to (John McCarthy, 2008), cloud computing services are to provide common online business applications that are accessed from a web browser, while the software and data are stored on the servers. The service is accessible anywhere that provides access to network infrastructure.

The most users on computer networks were using less than 10% of their capacity at one time and now Amazon plays an important role to develop the idea of computer network which is provisioning of cloud computing by updating and enhancing their data centers. In the present year Google, Amazon, Microsoft and IBM are the most famous providers of cloud computing solutions followed by Sun and Ubuntu in the cloud. Around beginning of the 21^{st} Century, the term cloud computing started to be used widely, besides the fact that most of the focus at that time was limited to SaaS (John McCarthy, 2008) (Srinivas et al. 2013).

Cloud computing has come out again as a method of computing, in which they are providing computing resources as services, and allow users to access via the Internet (cloud), without the need to acquire knowledge, or experience, or even control the infrastructure which supports these services.

The cloud computing is different from the outsourcing industry, "the cloud computing" is not to provide services to others only, but also to provide technical support, equipment and contribute for removal of maintenance problems and the development of Information Technology (IT) Information Technology programs for subscribers (Organizations/users), it also contributes to built and readiness of the network infrastructure (Yigitbasioglu et al. 2013), thus the concentrated effort will be concerned with “how to use these services only” rather than knowing the technical details. The infrastructure for cloud computing is based on advanced data centers, which offers a large storage space for users as they provide software as a service for users.

The concept of cloud computing has become one of the main topics of discussion in the industry over the past period. So this study will focus, investigate, and discuss the concept of the cloud computing, in addition to study the risks and challenges facing this transformation.

From the previous definition the aspect of cloud computing is concerned on-demand computing with minimal effort and minimal cost.

However, the migration from a personal computer based paradigm to a cloud computing paradigm carries some challenges and risks along with it, not only for the loss of control and the loss of security but also built trust feeling, cloud provider knowing the critical data of cloud consumer (individual or an organization) and take risks with the availability, confidentiality and integrity of this data:

- Availability may be affected if the provider’s data is unavailable when needed, due for example to a Denial of Service (DoS) attack or system failure.
- Confidentiality may be affected if data is a maliciously accessed by an unauthorized user, or otherwise someone exposed to the system.
- Integrity may be affected if data is maliciously damaged or destroyed.

This study proposes a security metrics that enable all cloud stakeholders to quantify the risks that they suffer from as a result of security threats in term of cost per unit of time. The reason why security is a much bigger concern on cloud computing than other shared utility paradigms is that cloud computing involves a “two-way relationship” between the provider and the consumer: whereas the electric grid and water grid involve a one-way transfer from the provider to the consumer, cloud computing involves two-way communication, including transferring information from/to consumer/providers, which raises security concerns.

1.11.1. Essential Characteristics

Cloud model has five essential characteristics that are common between all clouds; these characteristic are (CSA 2009), (Jin;, Michael D. Hogan; Fang Liu; Annie W. Sokol; Tong, 2011), (Brian et al. 2012) ,(NIST 2014) , (Jackson, 2015):

- **On demand self-service:** Whenever customers need a service or resources, they are able to request it and then immediately access without knowing the technical details. Cloud provider is responsible for managing all the technical details.
- **Broad network access:** Access to that computational resource is available through many different kinds of devices with standard network interfaces, and the customer can get access to the resources using whatever media is available for him.
- **Resource pooling:** The computing resources of the cloud provider are pooled together in such a way that it is able to serve multiple clients at the same time, with no physical hardware instance reserved to any particular client.
- **Rapid elasticity:** Elastic nature of the infrastructure means allowing rapid allocation and de-allocation of the resources to the customer on demand basis.
- **Measured service:** The commercial model of the cloud needs transparent billing of the used resources. Though, utilization of computing services needs to be monitored. Monitoring also helps in controlling the quality of service of the provided services. As a result, payment will be a simple process.

1.11.2. Cloud Service Models

The service models for cloud computing can be seen as layers of computing. As shown in the following figure 1-1, the cloud service consists of levels that roughly correspond to these models, cloud service models consist of three models (CSA, 2009) (Bohn 2016):

- Software as a Service (SaaS).
- Platform as a Service (PaaS).
- Infrastructure as a Service (IaaS).

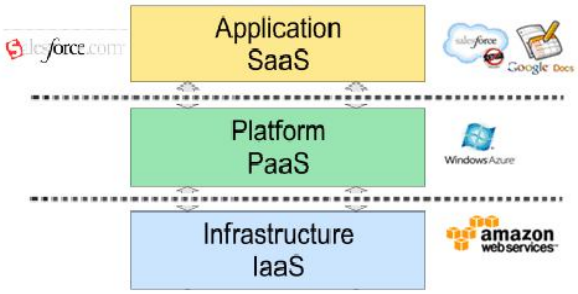


Figure 1-1: Some Cloud Providers providing specific Cloud Service Model

1. Software as a Service (SaaS)

The cloud user may use applications on demand through the internet which is provided by the cloud provider, these applications may be accessed through a web browser or other program. The user does not control any part of the cloud infrastructure, developing of the application, technical issues on servers networking and storage infrastructure because SaaS offers developed and finished applications that end users can only access and use it (as shown in figure 1-2). Examples of SaaS include Salesforce.com, Gmail and Google Docs (as shown in figure 1-2).

SaaS is very similar to the old thin-client model of software provision. The aim of using SaaS applications is to reduce the cost of software ownership by removing the need for technical staff to manage, install, deploy, test and upgrade software, and also reducing the cost of licensing software (NIST 2013).

2. Platform as a Service (PaaS)

First PaaS functions at a lower level than SaaS, typically providing a platform on which software can be developed and deployed. It offers an operating system as well as suites of programming languages, libraries, software development tools that customers can use to develop their own applications which are supported by cloud provider (as shown in figure 1-2), examples of PaaS is: Microsoft Windows Azure and Google App Engine (as shown in figure 1-1). PaaS gives end users control over application design and aim mainly to facilitate software development by providing a computing platform with large programming capabilities. These usually include facilities for software development, deployment and/or hosting and possibly testing. The platform may include security, database, and web services components. The metering service of the cloud is typically enhanced and the payment methods may also be provided simply.

PaaS will be the best option if the user is planning to build a website/application and he/she don't want to buy Visual studio/Oracle…etc software by their own. In this case the user will think if someone would rent to him/her the software license for a week or month as examples (NIST 2013).

3. Infrastructure as a Service (IaaS)

IaaS give end users direct access to processing, storage, and other computing resources, allowing them to configure those resources and run operating systems and software on them as they need because the end user has a full control on them, but has no control over the hardware that is used to provide these capabilities (as shown in figure 1-2). These users do not know the technical issues about these hardware (NIST 2013).

IaaS is technologically enabled by the technology of hardware virtualization. A Virtual Machine (VM) simulates a proper hardware computer using software for virtualization i.e. Xen, and VMWare, and VirtualBox. All these VMs software enable multiple virtual machines to be installed and run on a single hardware computer. Examples of IaaS include Amazon Elastic Compute Cloud (AmazonEC2), Amazon Web service, IBM Blue (as shown in figure 1-1).

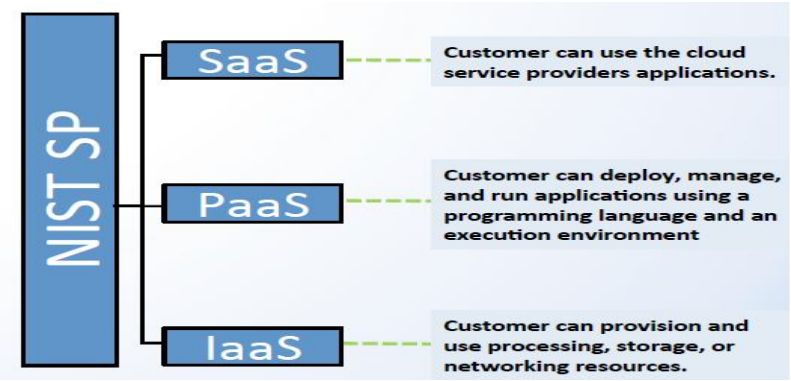


Figure 1-2: NIST Visual Model of Cloud Computing Definition

On the other hand, due to varieties of users who use the cloud concept (either consumer or provider), varieties on the nature of deploying the data and varieties on nature of service, all these varieties lead to emergence of threats each threat targeting users based on his/her interest, and these threat cause users hesitate using cloud and also loss of security lead to trust problem, following sections concern on these threats in much more details.

1.11.3. Cloud Computing Security Challenges

Cloud Computing has simultaneously switched business and government, and created new security challenges. The shift from server to service-based thinking is transforming the way technology departments think about, design, and deliver computing technology and applications. Yet these advances have created new security vulnerabilities, including security issues whose full impact is still emerging. The cloud provider cyber-security guarantees to cloud users, such as confidentiality, integrity, and availability, however security requirement faced too many threats that mitigate their positive effects which affected all stakeholders in cloud computing, so too many working groups analyzed the security concerns using their suitable threat models (such as STRIDE threat model, ENISA threat model, CSA threat model and Verizon threat model…etc) which are developed by security working group to evaluate information security threats and some of them are discussed in the following sections.

1.11.4. CSA Threat Model (CSA 2016)

Cloud Security Alliance (CSA) is one of the most discipline standard that creates industry-wide standards for the top threats on Cloud Computing and identifies the associate guidelines and best practices to avoid or to mitigate the threat's impact and amount, this will be done by releasing "The Treacherous 12: Cloud Computing Top Threats in 2016", "Security Guidance for Critical Areas in Cloud Computing" and the "Security as a Service Implementation Guidance" reports, which has been provided by CSA with an up-to-date threat faced in cloud computing environment, accordingly many organizations have followed this guidance to their cloud strategies. However, CSA recognizes this report to understand the nature of that security threats and manage risks and threats on cloud computing, their reports are recognized using a survey of industry experts to know the greatest vulnerabilities within cloud computing, and accordingly CSA threats working groups have used these surveys' results to craft the final 2016 report. This survey reflects the most current concerns of threat in the industry by returning to this most recent edition of the **F report**, experts identified the following 12 critical issues to cloud security (ranked in order of criticality per survey results that they made recently), (CSA 2016) (CSA 2013b):

1. ***Data breaches***: A data breach is an incident in which confidential, protected or sensitive internal information is seen/falls into the hands of their competitors and been violated, modified, viewed, stolen or used by unauthorized individual to do so.

2. ***Insufficient Identity, Credential and Access Management:*** This threat can occur due to lack of scalable identity access management systems, weak password use, and a lack of periodical automated rotation of cryptographic keys.

3. ***Insecure Application Programming Interfaces:*** It is relatively weak set of interfaces or APIs these interfaces are used by customers to manage and interact with cloud services which are generally exposed part of a system, CSA experts provide provisioning, management and monitoring practices that lead to decrease the impact of this threat.

4. ***System Vulnerabilities:*** When the program has bugs this makes it vulnerable to attacks, and attackers can use this vulnerabilities to steal data, taking control of the system or disrupting the delivered service.

5. ***Account, Service and Traffic Hijacking:*** It is an attack method (such as phishing or reusing the password in an authorized activity). Attackers here can gain access to users credentials, accordingly they can monitor users activities and transactions, manipulate on their data, return falsification information and redirect your clients to illegal and dangerous website

6. ***Malicious Insiders:*** When malicious inside organization has access to everything, this malicious insider intentionally cause damage by exceeding or misusing that access.
7. ***Advanced Persistent Threats (APT)***: It is a network attack where an unauthorized party gains access to a network and stays for a long period of time without being detected, attacker gain to stole some data here.
8. ***Data Loss/Leakage:*** This threat occurred due to deletion or alteration of records without a backup of the original content or loss of an encoding key.
9. ***Insufficient Due Diligence:*** In this type of threat, the consumer do not know many details of the internal security procedures because it's not clearly defined, so leaving customers with an unknown risk profile that means serious threats.
10. ***Abuse and Nefarious Use of Cloud Computing:*** Providers offer unlimited resources (such as network bandwidth, memory and storage capacity…etc) to their customers which may lead anyone (may be hacker) immediately to begin using cloud services.
11. ***Denial of Service (DOS):*** When the attackers are attacked to prevent users to be able to access their data or their applications by consuming huge amounts of system resources such as processor power, memory, disk space or network bandwidth.
12. ***Shared Technology Issues:*** Cloud service providers deliver their services by sharing infrastructure (such as platforms, runtime and applications) for different consumers that were not support strong isolation properties for a multiple stakeholders.

In this section each threat is briefly identified, in the later chapters all these threats will be discussed in detail.

1.11.5. Number of Incidents in some Cloud Companies

Financial, insurance, healthcare, education, governmental, educational sector, or any industry that deals with private financial or health information is not safe and continue to be targeted by hacking groups and each of these sector has its own rankings based on a criticality of threats occurrence, so the following table 1-1 considers the failures with respect to "Number of Incidents" on some cloud companies (Maarten Gehem, Artur Usanov, Erik Frinking 2015) (Amazon 2015) (Engineers 2015) (Alex Deac 2015) .

There are some advisory organizations that gain to enhance cyber-security measures such as CSA and NIST which they are promoting a more proactive and adaptive process to avoid or minimize the impact and the amount of threats. CSA is recently issued with updated guidelines which enhance risk

assessment strategy that recommend a shift toward real-time assessments with continuous monitoring which will be discussed later.

CSA and Symantec are attempting to investigate Cloud Computing reliability, CSA have reviewed 11,491 news articles on cloud computing-related outages from 39 news sources, and Symantec also covering a wide range of area and they proposed an annual report that considers the impact and the amount of threat occurrences, CSA and Symantec effectively covering the first five years of cloud computing and now these proposed reports will help decision makers to estimate the impact and the amount of each cloud's threat and take the appropriate measures and estimate the decline rate and the effectiveness rate in the event of deploying some countermeasures that gain to reduce these impacts - (this estimation aspects will be presented on more details in chapter 6) (Symantec 2015), (CSA 2013a).

Recently, CSA reviewed more than 50 online news archives on cloud computing with 10000 articles on various aspects of cloud computing. They used Google which is returned about 168,000,000 results on cloud computing (As Google was the top search engine), the cloud researchers group used it to search for the number of threat's incidents on cloud computing and proposed some statistical reports that have been used as a guideline by the most Cloud Service Providers. Most news reports before 1st march 2016 were accessed. However, due to a lack of documented reports on cloud threats, all data was based on news published online news archives, survey of industry experts and other trusty sources. This chapter will focus on most known report that is concerned with threats on cloud computing.

Table 1-1 shows the top three cloud providers, Amazon, Google and Microsoft, account for about 56% of all incidents of cloud. Beginning in 2010, cloud providers became more transparent with their reports of cloud threat incidents, most likely because Amazon became more open about the causes of their incidents, Table 1-2 present *Number of incidents (N) for some Cloud Service Providers (CSPs)* from year (2008 until 2015).

Table 1-1: Number of incidents (N) per year for some Cloud Provider

Cloud Provider Company	**N**
Google	9
Amazon	8
Microsoft	7
Apple	3

Salesforce.com	3
Facebook	2
Flickr	1
Intuit	1
LastPass	1
Netflix	1
Oracle	1
Rackspace	1
Sage	1
EMC	1
Tumblr	1
Yahoo	1
Netsuite	1
Total	43

CSA and Symantec security threat reports from 2008 to 2015 found that the number of cloud incidents has increased (as shown in table 1-2 and figure 1-4), the main reason is the growth of cloud services. Symantec claim that, about thirty-seven percent of threats were blocked by Symantec in 2015, which is generic detection for hacking tools that can exploit threat in order to gain root privilege access on the compromised cloud services, this had been done by patching some components which were used by many manufacturers that took much longer to provide patches to protect their customers, so as noticed in table 1-2 this will lead to a slight increase in incidents ratio in 2015. (CSA 2013b) (Symantec 2014) (Symantec 2015) (Symantec 2016).

Table 1-2: The Number of Incidents from year (2008 – 2015)
(CSA 2013b) (Symantec 2014) (Symantec 2015) (Symantec 2016)

The Number of Incidents from year (2008 – 2015)	
Year 2008	7
Year 2009	26
Year 2010	43
Year 2011	101
Year 2012	157
Year 2013	253
Year 2014	312
Year 2015	318

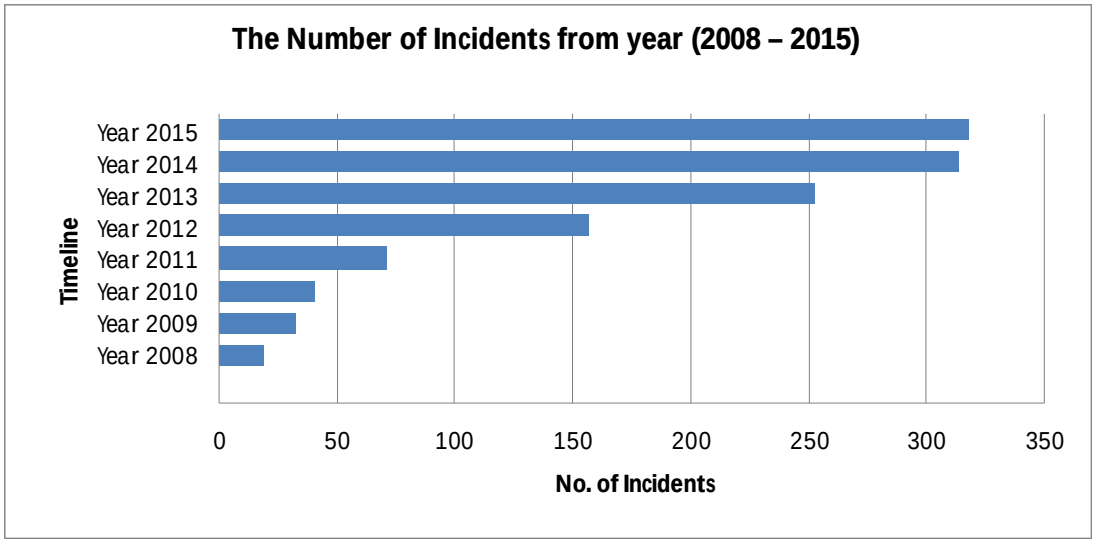


Figure 1-3: Incidents frequency from (2008 – 2015)

It can be observed from table 1-2 that with the growth of cloud services from 2008, there was also a corresponding rise in the number of cloud computing threats.

The investigation detected that the top four threats were ***"Insecure Interfaces & APIs"*** (51 incidents; 29% of all threats), ***"Data Loss & Leakage"*** (43 incidents; 24.5%), ***"Denial of Service"*** (15 incidents; 8.6%) and "***Data Breaches"*** (18 incidents; 10%) – as shown in table 1-3. These four threats accounted for 72.5% of all cloud outage incidents (see Figure 1-5).

Table 1-3: Number of Incidents for Each Threat on Cloud

Threat No.	**Threat Name**	**No. of Incidents**	**Threat Probabilities**
T1	Data Breaches	18	0.002054795
T2	Weak Identity, Credential and Access Management	4	0.000456621
T3	Insecure APIs	51	0.005821918
T4	System and Application Vulnerabilities	4	0.000456621
T5	Account Hijacking	3	0.000342466
T6	Malicious Insiders	3	0.000342466
T7	Advanced Persistent Threats (APTs)	6	0.000684932
T8	Data Loss	43	0.004908676
T9	Insufficient Due Diligence	11	0.001255708
T10	Abuse and Nefarious Use of Cloud Services	12	0.001369863
T11	Denial of Service	15	0.001712329
T12	Shared Technology Issues	5	0.000570776
	NoT		0.9800

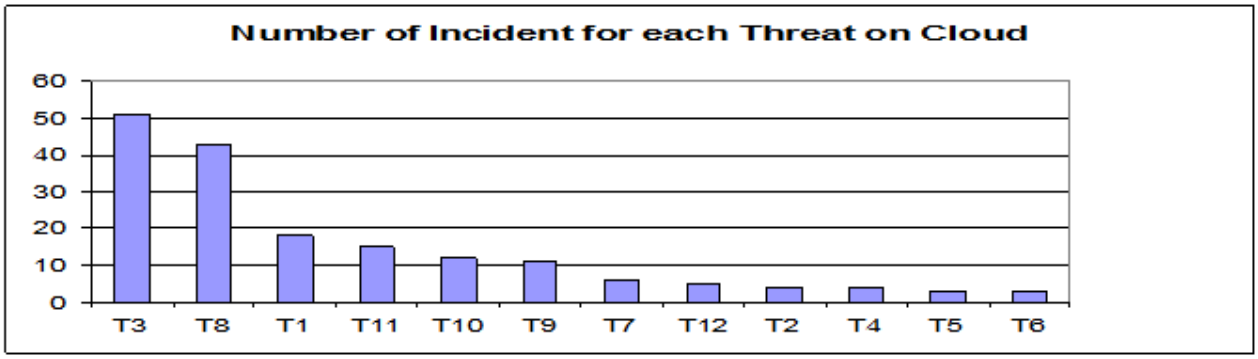


Figure 1-4: Number of Incidents for Each Threat on cloud

During the period from 2011 to 2015, the healthcare sector has reported the largest number of data breaches (as shown in table 1-4 and figure 1-6). Healthcare and some other governmental organizations were breached and accordingly some of these organizations decided to avoid using the cloud service to protect their reputations, and avoiding penalties as a result. But this may be changed in the future, and now the most popular cloud companies are already looking at bringing in regulation surrounding the proper disclosure of data breaches because they knew that the number of breaches increased (23%) in 2014 and some organizations decided to withhold their data, attackers are the first suspicious for the majority of these breaches (Symantec 2015). The following table is showing the Top 5 Sectors Breached by Number of Incidents.

Table 1-4: Top 5 Sectors Breached by Number of Incidents

Top 5 Sectors Breached by Number of Incidents		
sector	No. of incident	Ratio
Healthcare	116	37%
Retail	34	11%
Education	31	10%
Gov. and Public	26	8%
Financial	19	6%
Other	89	28%
	315	100%

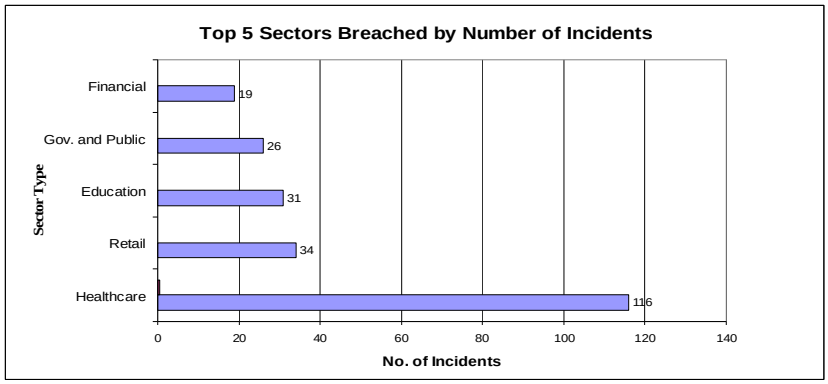


Figure 1-5: Top 5 Sectors Breached by Number of Incidents

1.11.6. Related Failure "Cost" in some companies

Despite all the mentioned advantages of using cloud computing service which is supported by different cloud companies, there are still a number of challenges and barriers facing cloud services and until now specialists were failed to solve them, this leads to catastrophic failure with huge financial losses.

When moving to mission-critical systems, companies here need to pay a lot of cash to gain high revenue; however, the investment doesn't always deliver the hoped revenue. Despite the progression in infrastructure robustness, many IT enterprises still face database, hardware, and software failures. Yet, the most of IT failure and control failures cost on cloud environment are unfamiliar, so the proposed model considered an econometric approach that estimates the expected revenue using ROI approach.

Since the beginning of 21st, many organizations have many ways that IT downtime can hurt businesses due to "Unplanned Outages" and many IT professionals suffer form security failures, which lead to: lost revenue, reputation and productivity. So there is a need to revisit the issue, and see how organizations should address, assess and estimate the cost failure of threats occurrence and know the impact of that threat on all cloud aspects, and accordingly look at reliable and precise numbers around the potential costs for that security failure which complicates the business, and this is the main agenda of this research.

Failure cost also varies significantly within industries, due to the different effects of that failure. Business size is one of the most obvious factors, but it is not the only one, there is a need for setting a measure means to establish the nature and implications of the failure that may occur due to threats materialize, compromising components or security requirement violation.

As many researchers observed, the main failures of critical applications can lead to two main types of losses:

- Loss of the application service – the impact of failure is varying from one application to another and from one business to another.
- Loss of data – the potential loss of data due to a system failure can lead to financial losses and significant legal problems.

So, today's all data centers should never go down, applications should be available constantly, and the end-users need to be able to trust on data center availability for their data and their application which should be available at anytime regardless of the failure occurrence on that data center.

1.11.7. Ponemon Institute Survey of Data Center Outages (January 2016)

Ponemon Institute (Ponemon Institute 2016) presented a case study which is dedicated to educational research that is concerned with privacy management practices and information; and conduct high quality studies on critical issues within business (people and organizations), government and furthermore, they are using paper means interviews, rather than an electronic survey, to provide greater assurances of obtained data and follow strict quality standards to ensure that their questions and data collection is relevant and proper.

According to (Dr. Ponemon) the most common reasons for data center outages are (as shown in figure 1-7):

- IT equipment failure.
- Threats and cybercrime.
- Uninterruptible Power Supplies (UPS) failures (UPS battery failure, UPS capacity being exceeded and UPS equipment failure).
- Water failure (air-conditioner failure) or heat failure (Heat-related/computer-room).
- Generator failure.
- Human error or accidental error.
- Weather related.

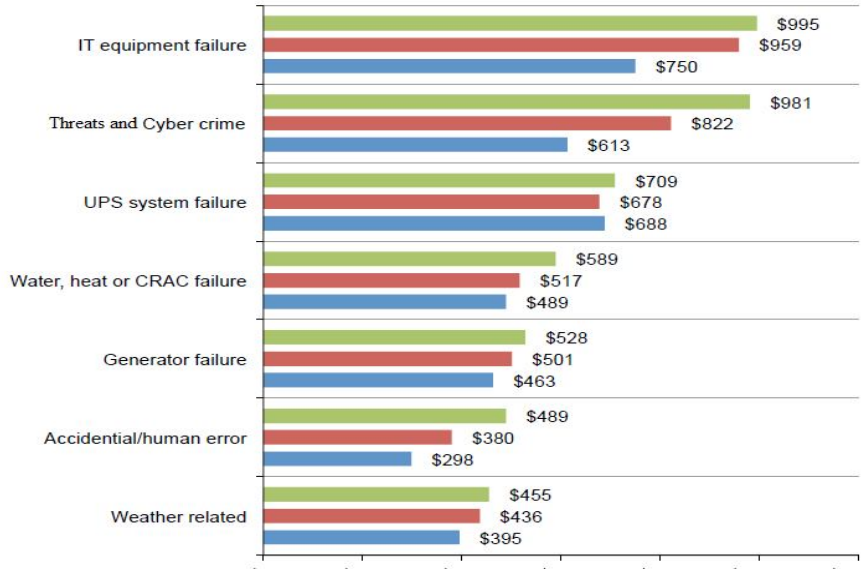


Figure 1-6: Root causes of data center outages with the average repaired cost **(**Comparison of 2010, 2013 and 2016 results)

However, the main reason for outage is due to IT equipment failures and threats occurrence, this failure (which will lead to chain of failures) affect on architectural components, that lead to security requirement failures, and accordingly will affect cloud stakeholders.

Ponemon Institute and Emerson Network Power present the results of the latest *Cost of Data Center Outages* study. Previously they published in 2010, 2013 *and now in 2016* the purpose of their study is to continue analyzing the cost related to threats occurrence and the cost of behavior of data center outages then compare the results of it among these years (Ponemon Institute 2010) (Ponemon Institute 2013) (Ponemon Institute 2016).

According to their new study, the average cost of a data center outage (which is due to threat and cybercrime occurrence) is increased from ($505,502 in 2010), and ($690,204 in 2013) to ($740,357 in 2016) that can be expressed as a 38 percent net change.

Their benchmark analysis focus on representative samples of a different industry sectors and they use the activity-based costing methods to analyze these results. The analysis of this report is derived from 63 data centers and 631 cloud companies in the United States.

The following are some of the key findings of their benchmark research involving the 63 data centers (as shown in the following figure 1-8):

- The *average* cost of a data center outage increased from $690,204 in 2013 to $740,357 in 2016 which represent as 7 percent increase. The cost of downtime has increased 38 percent from the first study in 2010.

- The *Maximum* downtime costs have been increased significantly: (1,017746 $ for 2010, 1.734,433 $ for 2013 and 2,409,991 $ for 2016).

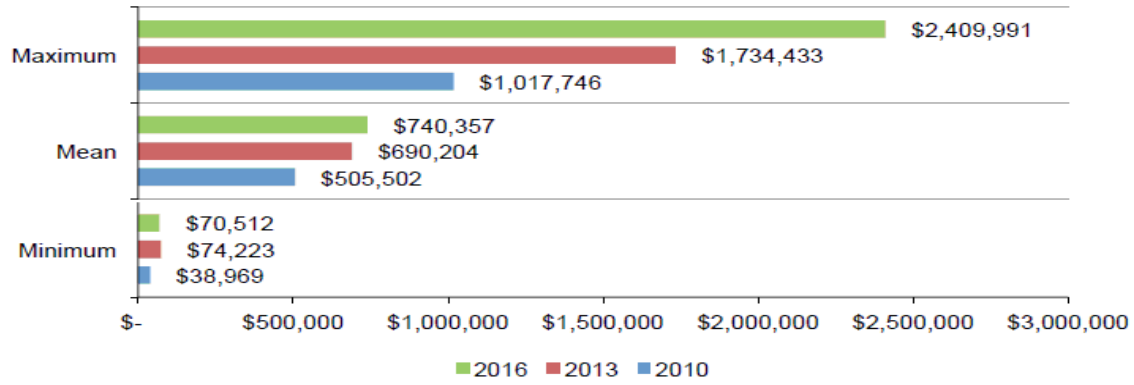


Figure 1-7: Key statistics on data center outages due to threat occurrence with financial losses (Comparison of 2010, 2013 and 2016 results)

The following section is describing some failures and failures cost on a real case of some specific cloud companies.

1.11.8. Cloud Failures "Cost and Impact" in a some cloud companies (From 2013 to 2016)

Experts and analysts can easily estimate the change in the industry, as example previously "Facebook" reached 500 million active users. Today the number has grown to 1.5 billion users, and similarly the rates of growth have occurred in other data centers. And according to research conducted by BI Intelligence company and Ponemenon institute "less than 500,000 smart phones were shipped globally in 2011, that number is over 1.5 billion for 2015", experts expected this number to be doubled by 2017", in 2015 this number is doubled because the 64 percent of US adults own a Smartphone. Cloud computing has a similar growth today and Cloud Computing will grow to $1.7 trillion in 2020 from $655.8 billion in 2014, the following table1-5 represented some cloud failures with respect to "Failures Costs" and table 1-6 represented some cloud failures with respect to "Failures Impact" in a some well-known cloud companies (From 2013 to 2016).

Table 1-5: Cloud Failures with respect to "Failures Costs and Impact" in some cloud companies

Company	Event of failure	Cost losses (USD)	Date of occurrence
Facebook	Facebook was down for about 2.5 hours and this is the longest such outage since 2010. This failure is occurred due to Handle of an error condition when verifying the configuration, some users data has been lost, so handling process ended up causing much more damage than it fixed.	The company loses around half a million dollars ($500.000) in a revenue. This is according to its official report.	2016
Target (US based retail company)	Data breach for more than 70 million shoppers and more than 40 million credit cards details were stolen.	148 million cost of failure + 61 million in anti-cyber attacks technology.	January 2014
Carbanak	Up to 100 financial institutions have been hit due to malware attack, this targeted attacks have been done by attackers who abused of cloud services.	The total loss is up to 1 billion from financial institutions in many countries has been lost.	2013
Boleto Bancario	Malware that compromised over 400,000 transactions within a period of two years.	They lose 3.7 billion.	July 2014
Home Depot	Their data were stolen which comprised approximately 40 million credit cards.	60 million	September 2014

Company	Event of failure	Threat Impact In term of severity	Date of occurrence
Amazon EC2	Disruption in the US East Region due to change the configuration to upgrade the capacity of the primary network, usually this type of failures may occur due to share technology issues.	Their network being exhausted lead to cause a failure on its available capacity, the cluster became unable to serve the requests.	2015
UCLA Health	4.5 million Records were compromised.	Extremely Severe. Individual lives have the potential to be fully impacted by identity theft.	2015
Premera BlueCross	11 million records impacted.	Extremely Severe. The victims are vulnerable to identity theft.	2015
Anthem	87.6 main records (such as names, addresses, email addresses, social security numbers, dates of birthdays and income information) were compromised and lost.	Extremely Severe, due to the amount of Personally Identifiable Information (PII) compromised.	2015
OPM	25.7 million Sensitive Personally Identifiable Information (SPII) of Federal and contractor was exposed.	Extremely Severe due to the exposure of confidential data that could be used in other cyber-espionage operations including blackmailing and spear-phishing attacks.	2015
IRS	In 2014 – 1.4 million individual records were compromised. In 2015 – 334,000 additional records were compromised.	Severe, their return files were fraud, and the potential for identity theft.	2015 and 2014.

JP Morgan	76 million individual and 7 million Small and Medium Enterprises (SMEs) impacted because of their compromised data. This was a new attack against one of the major banks in the world.	Severe. They lose their reputation across the banks and financial sector in the USA, they hold some of the most sensitive data about their clients.	2014
eBay	148 to 233 million accounts were compromised over a period of 229 days.	High, due to the length of the breach and the number of accounts compromised.	2014
Home Depot	56 million payment cards compromised.	Severe. Faced a number of legal problems and lose their revenue and reputation.	2014
Target	110 million records were compromised. This breach led to one of the largest incidents of credit card fraud and identity theft in history.	Severe. The chain of impacted in revenue, reputation, insurance organizations, banking organizations, and credit cards issuers were affected by this breach as well.	2013
* Black mailing: "a person threatens another person with some form of punishment if they do not offer some form of concessions, and Spear means phishing intend to install malware on a targeted user's computer"			

The cost of cloud failures increasing significantly since 2010, as many researches concerned with predicting and estimating the failure and the failure cost in the future, according to the historical failures and costs, since Cloud Computing is a relatively recent phenomenon, no published analysis of cloud threat incidents with MFC dimension could be found.

Summary

Due to system failures that has been highly increased recently, specifically on cloud computing companies, so too many measures have been built to assess and estimate the failure cost that may help to mitigate the amount and the impact of security failures and failure cost in the future, so this chapter considers two aspects: the first part considering some cases of failures from two points of views: in section 1.14.9. The concern is the “Number of Incidents” that affect on cloud computing and this representing as “Amount” point of view, while section 1.14.10. present some other cases of failures from “Cost and Impact” point of view, and most of cloud companies should use these measures that may help decision makers to decide whether the countermeasure that should be deployed is worthwhile or not, so the next chapter will propose some measures for risk estimation metrics (such as CRAMM, OCTAVE, SLE and ALE, CORAS, and a set of MTTx such as MTTF, MTTR, MTBF, MTTCF…etc) then will present the proposed measure (MFC) in term of “Failure Cost” per a unit of time.

CHAPTER TWO

RISK ESTIMATION METRICS

2.1. Introduction

(Boehme & Nowey 2008) argue that, there is a huge development on security concerns of information systems which never stops to grow. In fact, individuals or organizations everyday using these information systems which suffer from information security attacks due to different threats; threat occurrence will lead to lose a large amount of money, effort, time and other resources, so too many companies may pay millions of dollars on technical security equipments such as firewalls, load balancer, data mirroring, encryption tools and anti-viruses…etc, so there is a need to use these technologies to mitigate the damage(s) from an attack(s) (Tsiakis, 2010), however, there are different types of security technologies, a big challenge to choose which one of them is better than other that may gain the high return in the shortest time, another challenge is how to evaluate the chosen security technology, because it's hard to estimate the benefits of it because it depends on attack(s) rate of occurrence or frequency expectation. Now the "Information Security Risk Management Models" comes to reduce the investment cost without increasing the risk. "A risk is the probability of problem occurrence when a threat is enabled by vulnerabilities". Threats are much related to the characteristics of the assets and vulnerabilities are relevant to the security controls (Foroughi, 2008), asset is defined as any element of information system that has a value.

2.2. Cybersecurity Metrics:

The security metrics measures the current security status of a computing environment then monitor and compare the level of security and privacy attained to help decision makers to predict and decide correctly and accordingly propose proactive planning (Alberto & Ferreira 2012).

Measurement is the process of metric collection with pre-established rules that help in the interpretation of results. Any restrictions or controls relating to the metric should be defined before starting the measurement process. A metric can be expressed in one of the following ways:

- (#) "Number", expressing an absolute value of any element measured;
- (%)"Percentage", expressing a percentage of an element measured in relation to the total number of elements;
- "Logic values", such as (Low), (High), (Severe) or (Extremely Severe) for an event.

From this point of view, two questions should be answered "How The Measure Is Being Done?", and the second one is "Why Quantifying Security Metrics?"(Venkatesh & Brown 2013)

"How The Measure Is Being Done?"

Quality assurance experts can use two ways to measure an attribute:

1. **Qualitative measures** which are still the norm in many organizations and decision here is based on subjective information and often these types of measurement processes are inefficient.

2. **Quantitative measures** are measurement of data that can be put into numbers format (e.g. *number of incidents*). The main goal of quantitative measurement is to run statistical analysis; data here is represented as numerical form which is useful for decision making as a result.

"Why Quantifying Security Metrics?"

(Black and Paul, 2008) (Scarfone 2008) were discuss **cyber-security metrics issues**, they characterize as reflecting to what extent the system's security controls are combatable with relevant procedures, processes or policies. They argue that cyber-security metrics are often defined imprecisely, and used improperly. However, the proposed approach on this study is distinguished between how a metric is well defined and how it is practically computed based on this defined metric.

Too many measures present a qualitative information risk management frameworks for better understanding critical areas on cloud computing environment and identifying threats, threats impact and threat amount. The qualitative risk analysis proposed a method which is used as approach risk assessment and rank (Criticality of Threats) by using classes such as low, medium and high and the (Threat Probabilities) by using the number of incidents per unit of time. That is, to help them to control their security position and then to proceed to the risk mitigation measures (Zhang et al. 2010).

One of the most important differences between various security risk assessment techniques is the security risk decision which includes at least the following aspects:

- Value of the asset.
- Likelihood or probability that vulnerability will be exploited.
- Criticality or Severity of the impact.

Despite all the mentioned advantages of using cloud computing service which is supported by different cloud companies, but there are still a number of challenges and barriers they face and cloud experts fail to solve it which lead to catastrophic failure that lead to huge financial losses. The following section considering some risk estimation measures that may use to help the decision markers to identify which suitable avoidance or mitigation measures should be taken to reduce the amount and the impact of threat occurrence.

2.2.1. Security risk management framework for cloud computing

According to Zhang et al, this framework of security assessment tool present a qualitative framework for better understanding of the critical area in cloud computing by identifying the threats and vulnerabilities (Zhang et al. 2010).

Each process will be necessary to clarify specific roles, responsibilities, and accountability for each major process step, the proposed framework has seven processes including:

- Selecting relevant critical areas: this step is concerned with identifying areas of concern in cloud computing environment.
- Selecting relevant strategy and planning: this step is concerned with identifying risk, vulnerabilities and threats to organization
- Risk analysis: this step is concerned with identifying the source of threat (internal or external hacker)
- Risk assessment: identifying essential vulnerabilities in their hosts, network devices, and applications.
- Risk mitigation: this step presenting the probability and the impact of a possible vulnerability resulting from a successful threat in a qualitative way (high, medium, low). This step has been divided into four sub-processes:
    - Probabilities determinations,
    - Impact analysis,
    - Risk determination, and
    - Control the recommendations.
- Risk management review: this final step presenting in a qualitative way, the risk levels (high, medium or low) and propose recommendations to reduce this risk amount and impact in a cloud computing system. In this step cloud provider should provide a Risk Treatment Plans (RTP) to mitigate vulnerabilities and threats.

However this measure can not measure the failure cost per unit of time and it does not consider any of the cost benefit analysis approaches; this framework ignores the variance stakes among different stakeholders, requirements, components and threats.

This framework represented as qualitative measure (its results, asset value, and its Recommendations are Subjective), and most of cloud experts feel that a quantitative measure is more useful than a qualitative attribute.

Goal:

- Using approach risk assessment and ranking threats by using classes such as low, medium and high which considering the threat severity rather than threat probability.
- Helping the cloud providers to control their security aspects and then propose the risk mitigation measures.

Advantages:

- This measure is compliance with different standards.
- It can measure the impact of investments on the IT security aspects.

Disadvantages:

This framework inherits the weaknesses of the qualitative analysis, which are:

- Subjective Results.
- Subjective Asset Value.
- Subjective Recommendations.
- Difficult to Track Improvements.

2.2.2. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

One of the other risk-based strategic assessment is Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) which was developed by the Software Engineering Institute (SEI), Carnegie Mellon University in USA and the Computer Emergency Response Team (CERT) and used since 2009 (Mayer, 2009) it is a risk-based strategic assessment and planning technique for security, its method goals are examining and assessing organizational and technological issues based on a defined organization's security strategy and plan. This framework consists of three OCTAVE methods (AIT 2014):

- Making file of cloud's threat scenarios based on assets. This can be done by identifying assets of the system, main vulnerabilities, threat profiles, security requirements (availability, confidentiality and integrity) by interviewing some people during workshops, then
- Recognizing the vulnerabilities about major facilities, this can be done by identifying vulnerabilities that expose those threats and creates risks to the organization, and finally
- Assessing the risk and developing security strategies, this can be done by developing risk mitigation plans and practice-based protection strategy to support the organization's missions and priorities.

The OCTAVE methods are designed to be used for Small and Medium Enterprises (SMEs) (< 100 employees), and it allows to use some Software Quality Assurance (SQA) experts, some skilled analysis team or some external experts for improving their software process activities, if necessary.

So, one of the main qualitative risk estimation metrics is "**OCTAVE**" that has been used to reflect the loss risk of the whole application. However, this measure can not measure the failure cost per unit of time and it does not consider an economic base approaches; this assessment method ignores the variance stakes among different stakeholders, requirements, components and threats.

Goal:

OCTAVE is represented as a set of tools, techniques and methods which provide "risk-based information security strategic assessment planning" that can be used for identifying and managing information security risks which focus on information assets mainly.

Advantages:

- It can be carried out by Small and medium Enterprises (SMEs) with small number of employees.
- Flexible, because it contains several methods tailored for organizations with a well defined catalogue.
- Widely used, because it supports documentation and compatible third-party mechanism.
- Yearly developed with avoiding the versions control problems.

Disadvantage:

- The first version of OCTAVE is a heavyweight method, comprehensive, consisting of many volumes, worksheets and processes.
- Largely incompatible with other standards frameworks, however, the recent version of OCTAVE treat with most of these obstacles, making for a simplified version, with increased applicability.

2.2.3. CCTA Risk Analysis and Management Method (CRAMM)

The CRAMM method was originally developed by the Central Communication and Telecommunication Agency (CCTA) of the UK government; a British government organization then has undergone several revisions and is currently owned by a British company and consulting by a Siemens Enterprise Communications Ltd. It is one of the risk-based strategic assessments, which consists of three categories:

- Asset identification and valuation via interviews, the main assets are:
  - Physical assets.
  - Software.
  - Data.

  Asset value has been identified in terms of financial loss from risk impact that has occurred due to data destroyed, disclosed, modified for software and data or unavailable application.

- Identify and estimate the level of vulnerabilities and threats by providing some *mapping between (threats and assets) and between (threats and it is impacts)* in a qualitative manner.
- Provide a set of countermeasures that has been considered to manage the identified risks.

So, one of the main qualitative risk estimation metrics is "**CRAMM**" that has been used to reflect the level of vulnerabilities, threats and its impact of the whole application. However, most current companies require quantitative measures for risk identification and estimation and this method also ignore the variance stakes among different stakeholders, components, requirements (Aissa et al. 2010a)**.**

Goal

CRAMM can be used to adjust security investments by investigating the needs for action at management level. Secondary their applications can show the compliance with the other standards (like the BS7799 - British standard for information security management). CRAMM is designed for large enterprises, like a governmental sectors and industry.

Advantages:

- Their assessment can be tailored to customer needs.
- Useful for large enterprise.
- Most of their processes were *automated* by using their software tool.

Disadvantages:

- It needs an expert knowledge to deal with this method.
- Their full assessment is very comprehensive and complex to be applied specially for SMEs.
- Can only be used with their automated tool.

2.2.4. Single Loss Expectancy (SLE) and Annual Loss Expectancy (ALE):

One of the most popular and known metric that used to *quantify* and estimate risk to precise numeric monetary values to assets is called Annual Loss Expectancy (ALE) which is based on Single Loss Expectancy (SLE). It designates the financial risk of threats impact and frequency. ALE used for a single type of security event that can be computed as the product of SLE with the annual rate of occurrence (ARO), (Boehme & Nowey 2008) (Rabai 2014) (Tsiakis, 2010).

Single-loss expectancy (SLE): its approach is based on risk assessment and management control which represent the monetary value expected from risk occurrence on an asset.

Single-loss expectancy is mathematically expressed as:

$$SLE = AssetValue(AV) \times ExposureFactor(EF)$$

Where, the Exposure Factor (EF) is an impact of the risk over the asset that has been represented as "% of asset lost". As an example, the asset "X" is valued at ($500,000) and the Exposure Factor (EF) for this asset is (50%), then 50% * $500,000 = $250,000. EF is expressed within a range of 0% to 100% that an asset's value will be destroyed by risk and if the exposure factor is 1.0 this mean the asset is completely lost or destroyed.

Single-loss expectancy can be expressed by (dollars, euro, yens…etc) and EF is a potential percentage of loss to a specific asset when a specific threat has materialized. The exposure factor is a *subjective* value that should be defined and identified by the person who is assessing that risk.

The **Annual loss expectancy** (ALE) is the product of the Annual Rate of Occurrence (ARO) and the single loss expectancy (SLE). ARO is the number of occurrences of that type of event per year.

Mathematically expressed as:

$$ALE = ARO \times SLE \quad (1)$$

For example, if the Annual Rate of Occurrence is 3 that affect on the asset "X" this mean the equation will be shown as:

ALE = 3 * $250,000. Therefore: ALE = $750,000

Goal:

The overall goals of these perspectives on IT security are:

- Measuring the *impact* of investments on the IT security aspects.
- Determining the *cost* and benefits of different security measures.
- Representing the financial gain of a project compared to its total cost.

So, one of the main *quantitative* risk estimation metrics is "SLE and ALE" that has been used to reflect the *loss risk of the whole application*. However, this measure is also ignoring the variance in stakes among different stakeholders, components, requirements and threats.

Advantages:

- It can measure the impact of investments on the IT security aspects.
- It can present the financial loss of a project (by considering threats impact and frequency).
- It can assess the investments costs and its benefits

Disadvantages:

- The EF is subjective.
- May be required for some company managers after risk analysis, (It needs an expert knowledge to deal with all security aspects).

2.2.5. CORAS

CORAS is a platform for risk analysis of security-critical systems on cloud computing, it was developed by EU-funded project and still being maintained by the Open Source community. CORAS is the one of the main *quantitative* risk estimation metrics that has been used to reflect the risk analysis of security-critical systems of the whole application, it's supported by *automated tool* that facilitates documenting, maintaining and reporting analysis results through risk modeling and it designed mainly at risk analysis of security-critical systems (CORAS is a project name). The CORAS method complies with ISO 17799, ISO 27002, ISO/IEC 13335, and ISO 27005 standard (Jan Colpaert 2015).

The methodology defines four kinds of diagrams as a "model-based" approach to support various steps of the process, these diagrams are:

- Cloud Asset diagrams.
- Cloud Threat diagrams.
- Cloud Risk diagrams.
- Cloud Treatment diagrams.

Assets are the objects that have a value and need to be protected; and *threat has been classified to three categories*:

- Human threat (accidental).
- Human threat (intentional).
- Non-human threat (Natural disaster).

The main steps of CORAS are:

- Where the actual risk assessment is performed (identify the target of assessment analysis).
- Meeting with the customer (understand the overall goals of the assessment).
- Document the detailed description of the target using the CORAS language.
- Customer approval should be done to verify the assumptions and conditions.
- Risk identification: this step will be done through workshop to identify all possible risks on cloud computing environment.
- Risk analysis: This step is also done through session that determined the likelihood and the impact of each identified threat.
- Risk evaluation: this step used to evaluate each risk as either acceptable or requiring treatment.
- Risk treatment: this step is used to identify the possible treatments and mitigations measures.

Goal:

- Develop a practical model–based framework which has been supported by automated tool for precise, efficient and unambiguous security risk assessment systems.
- CORAS is a model-based approach based on UML modeling to conduct the Risk Assessments, to serve three purposes:
    - Describing the *target of assessment* (who is benefiting from the assessment).
    - Documenting the *results based on their assumptions*.
    - *Facilitates interaction between different groups of stakeholders* inside the company.

Advantages:

- Their supported tool is open Source (free).
- Facilitates the communication and collaboration between different stakeholders.
- Broad, suitable for large organizations that have a security-critical system.

Disadvantages:

- Requires expert knowledge from various security backgrounds.
- Comprehensive platform (contain a lot of details), so it's inappropriate for SMEs.
- No longer developed.

In spite of all mentioned benefits. However, this measure also ignores the variance that may exist between different cloud components, requirement and threat because it can not reflect (to what extent) each component of the system contributes to meeting each security requirement and to what extent each cloud component's safety are dependent on the threat occurrence.

2.2.6. Mean Time To x (MTTx)

MTTx: mean "Mean Time To (Failure, Repair, Between Failure, Exploit …etc)", It's a set of quantitative prediction measures that are used to measure the reliability term that used to provide the amount of failures per million hours. This is the most common measures that are important in the decision-making process of the end user to know "what product to buy for their application", all MTTx are providing a numeric value based on a compilation of data to quantify a failure rate and the result is a time of expected performance. This numeric value is commonly expressed using a unit of time (hours is the most commonly unit in practice) (Stanley 2011).

“If we can’t measure we can’t improve our practices”, so there are different taxonomies of metrics which are proposed in such a way to measure the failure and its cost such as (Josson and Pirzadeh , 2011) (Mili & Sheldon 2007) (Speaks 2002):

- MTTF (Mean Time to Failure).
- MTTCF (Mean Time to Catastrophic Failure).
- MTTR (Mean Time to Repair).
- MTTBF (Mean Time Between Failure)…etc

All MTTx provide a numeric value to quantify a failure rate and the resulting time of expected performance based on a compilation of data. This numeric value can be expressed using any measure of time.

For example: if a data-center “D1” has been failed due to outage for a period of time (assuming that the affected device is repair-able, the following scenario represented in the following table 2-1) describes the case in much more details:

Table 0-1: Operation Time for Specific Device

Total production time (up time + down time) Total hours of service of all devices	700
The Total down time	200
The Total up time	500
Numbers of breakdowns	5

MTTR: “Mean Time" means, statistically, the average time. "Mean Time To Repair" is an average time that it takes to repair system after a failure, *it is a simple indicator of “Maintainability” aspects,* this measure used as an indicator of “*maintainability*” aspects. MTTR (for repair-able devices) is the average time that it takes to repair something after a failure.

MTTF: "Mean Time To Failure": Is the mean time to the next failure, regardless of whether it can be repaired or not, so it describes the expected time that a system will operate before the first failure occurs, it is the number of total hours of service (before the first failure occurs) of all devices divided by the number of devices, *it is a simple indicator of “Reliability” aspects.*

MTBF: "Mean Time Between Failures" is literally the average time elapsed from one failure to the next or the time from one failure to another or the expected time *between two consecutive failures* for a repairable system, , *it is a simple indicator of “Repairability” aspects.* Usually people think of it as the average time that system works well until it fails and needs to be repaired (again). Each of these measures is defining its associate equation as shown below:

$$MTTR = \frac{Total\ \ Down\ Time}{Number\ \ Of\ \ Breakdowns} = \frac{200}{5} = 40\ \ Hours$$

$$MTBF = \frac{Total\ Up\ Time}{Number\ \ Of\ \ Breakdowns} = \frac{500}{5} = 100\ \ Hours$$

However, all these metrics dependent exclusively on the system under observation and ignore the variance in stakes amongst different stakeholders, the variance in failure impact from one stakeholder to another. They also make no distinction between requirements, so all the MTTx measures consider that any failure to meet any requirement is a failure to meet the whole specification.

Verification and Validation activities (V&V) may give us higher levels of confidence in meeting some requirements than in meeting others. Yet these metrics does not account for this variance.

A complex specification is typically the aggregate of many individual requirements/sub-specification; the stakes attached to meeting each requirement vary from one requirement to another. Yet the MTTF makes no distinction between requirements; failing any requirement counts as a failure.

Typically the operation of a system involves many stakeholders, who have different stakes in the system meeting any given requirement. Yet the MTTF is not dependent on the stakeholder but exclusively on the system under observation.

Goal

It is designed to provide an understanding of product maintainability and reliability, and it's based on methods and procedures for lifecycle prediction for a product.

Advantages

- Measuring system reliability for non-repairable systems.
- Measuring system maintainability for repairable systems.
- Providing a numeric value to quantify a failure rate per hours for a product.
- MTTx supported by automated tools.

Disadvantages

- All MTTx do not consider the variation in stakeholders needs.
- All MTTx do not consider the structure of the requirements specification, it respects to the whole specification.
- V&V measure improve the likelihood of meeting one clause more than another, MTTx do not reflect this.
- All MTTx are blind to this structure, and captures only the likelihood of satisfying the overall specification.

2.3. Mean Failure Cost (MFC)

The MFC is a function that measures, for a given system and a given stakeholder, the mean of the random variable that represents the loss incurred by the stakeholder as a result of possible system failure. When the cause of system failure being considered as a security breaches, the MFC can be used to quantify the loss that results from violations of security requirements, such as confidentiality, integrity, availability, etc Chapter 4 will consider the application of the MFC model to reference cloud architecture. So the MFC is a measure that is used to quantify the impact of failures by providing a failure cost per unit of time. This *cost must be balanced against the benefit* of operating the system for the same unit of time.

The most cloud failures occur due to malicious attack which increased during the last decade. Most experts on software measures stated that, "If you cannot measure it, you cannot improve your practices" In other words; security cannot be managed, if it cannot be measured. This clearly states the importance of metrics to evaluate the ability of systems to resist attacks, quantify the loss caused by security breach and assess the effectiveness of security solutions. Hence, there are quantitative models that estimate the dependability of a system which can be measured according to the reliability, maintainability, availability, usability and security metrics such as the MTTF, *Mean Time to Catastrophic Failure* (MTTCF), the *Mean Time To Discovery* (MTTD) and the *Mean Time To Exploitation* (MTTE)…etc Broadly speaking, however, all of these metrics reflect the failure rate of the whole system and it fails to consider the following attributes:

- Variance in stakeholders' needs and their requirements (different stakeholders have different stakes in the secure operation of the system).
- Variance in failure (impact, severity and count...etc). A system may have a wide range of security requirements, so it is important to consider failures with respect to different requirements.
- Variance in failure cost from one requirement to another. The stakes of failure may vary greatly depending on which requirement has been violated, even for the same stakeholder.
- Variance in failure probability from one requirement, component or threat to another. The system may have different probabilities of failure with respect to different security requirements.

The MFC consider all these variations which quantifies the cyber-security of a system in terms of dollars per hour of operation; the MFC considers the stakeholders variations in term of their needs, each stakeholder need some security requirement. However, until now there are no statistics on the volume of estimating failure cost on Cloud Computing environment per unit of time.

2.4. The MFC advantages:

The MFC presents many advantages:

- **It provides a failure cost per unit of time:** MFC quantifies the cost in terms of financial loss per unit of operation time (e.g. $/h)
- **It quantifies the impact of failures:** it provides cost as a result of security attacks.
- **It distinguishes between stakeholders:** it provides cost for each system's stakeholder as a result of a security failure. So it reflects the **variance that may exist amongst different stakeholders** of the same system and similarly for a given stakeholder, it reflects the variance that may exist amongst the stakes she/he attaches **to meet each requirement**.
- MFC used to make **economically based decisions** regarding the **amount and severity** of threat.
- **Quantify the cost/benefit analysis:** The investment cost must be *balanced against the benefit* of operating the system for the same unit of time, to determine whether the measure is worthwhile or not, so it's used to make *economically based decisions*.
- Moreover, MFC may be used to determine and illustrate **how much each stakeholder may stand to lose** as a result of, for example, a security failure, a hardware failure or any other service disruption.
- MFC **consider all these mentioned variations** which quantifies the cyber-security of a system in terms of dollars per unit of time; the MFC consider the stakeholders variations in term of their needs, each stakeholder has a different need on security requirement level.
- MFC provides **cost** as a result of security attacks.
- Make **economically motivated decisions** pertaining to cyber-security, such as selecting a cyber-security solution, justifying the cost of a cyber-security solution, sharing the cost of a cyber-security solution over different stakeholders…etc.

2.5. Comparisons of security measures, methods and metrics:

According to The American Public Transportation Association (APTA 2014), Cyber-security measures, technologies, processes or best practices that should be taken to protect networks, computers, programs and data on the internet against damage or unauthorized access or attack. In a computing context, the term *security* implies cyber-security.

The following table 2-2 summarized and compared all the mentioned cyber-security measures that use mainly to reduce the amount and the impact of failure and failure cost.

Table 0-2: A Cyber-security measures Comparisons

Measures, methods or metrics	Advantages	Disadvantages	Comments
Security risk management framework for cloud computing	- This measure is compliance with different standards. - It can measure the impact of investments on the IT security aspects	- Subjective Results. - Subjective Asset Value. - Subjective Recommendations. - Difficult to Track Improvements.	- Qualitative measure. - Helping the cloud providers to control their security aspects and then propose the risk mitigation measures.
OCTAVE	- It can be carried out by (SMEs). - Flexible, because it is containing several methods tailored for organizations. - Widely used, because it is supporting documentation. -Yearly developed and motivated.	- The first version of OCTAVE is comprehensive consisting of many volumes, worksheets and processes. - Largely incompatible with other standards.	- Qualitative measure. - The goal of the OCTAVE set of tools that can be used for identifying and managing information security risks which focus on information assets.
CRAMM	- Their assessment can be tailored to customer needs. - Useful for large enterprise. - Supported by automated software tool.	- Need an expert knowledge to deal with this method. - Their full assessment is very comprehensive and complex to be applied specially for SMEs. - Can only be used with their automated tool.	- Qualitative measure. - It can be used to adjust security needs at management level. - Compliance with different standards. - Designed for large enterprises, like a governmental sectors.
SLE and ALE	- It can present the financial loss of a project (by considering threats impact and frequency). -Determine the cost and benefits of different security measures.	- It needs an expert's knowledge to deal with this method.	- Quantitative measure. - It is designed to measure the impact of investments on the IT security aspects.

Measures, methods or metrics	Advantages	Disadvantages	Comm
CORAS	- Their supported tool is open Source. - It's facilitates the communication between different stakeholders. - Comprehensive, suitable for large organizations.	- Requires expert knowledge from various security backgrounds. - Comprehensive and inappropriate with SMEs. - No longer developed.	- Quantitative measure. - Develop a practical m automated tool for prec unambiguous security r systems. - CORAS is a model-ba on UML modeling to co Assessments.
MTTx	- Measuring system reliability for non-repairable systems. - Providing a numeric value to quantify a failure rate per millions - hours for a product. - It has useful tools.	- MTTF does not consider the variation in stakeholders needs. - The MTTF not consider the structure of the requirements specification it respect to the whole specification. - V&V measure improve the likelihood of meeting one clause more than another, MTTx not consider it. - The MTTF is blind to this structure, and captures only the likelihood of satisfying the overall specification.	- Quantitative measures - It designed to provide product maintainability it's based on methods a lifecycle prediction for -It's based on methods lifecycle predictions for - It gives the probability within the time interval
MFC	- It provides a failure cost per unit of time. - It quantifies the impact of failures. - It distinguishes between different stakeholders, requirements,	- MFC infrastructure does not reflect the direct interactions between all the MFC layers of need. - Users who may use this method to derive threats may have completely	- It's Quantitative meas - Entries: real number. - Result: $/hour. - It's designed to quanti failures, interruptions, e

	components and threats. - Compatible with the cost/benefit analysis model. - MFC quantifies the cost in terms of financial loss per unit of operation time (e.g. $/h). - MFC provides cost as a result of security attacks.	different results. - It difficult to recognize that different *components* of the specification carry different stakes, even for the same *stakeholder*.	failure cost per unit of t - It's represent how mu may stand to lose as a r failure - Compatible with Valu Engineering (VBSE).

Too many articles discussed the concept of reliability and maintainability, and its used measurement (such as MTTF, MTTR and MTBF…etc). Our work presents a *dependability metric* with a security aspect which differs from all MTTx measures because it reflects variance in stakes and stakeholders, variance in security requirements and their impact on stakeholders, variance in system components and their impact on requirements, variance in security threats and their impact on components, and variance in the likelihood that threats materialize. However, all the mentioned measures consider the specifications as a whole.

Summary

Barry, LiGuo and Boehm et al (Barry, 2006) (Barry and LiGuo, 2003) (Boehme & Nowey 2008) claim that, all problems that arise in a software are due to economic reasons rather than technical reasons, and all decisions makers are going to maximizing benefit; minimizing cost without increasing risk. MFC is perfectly compatible with this philosophy which is based on Value-Based Software Engineering (VBSE) with using econometric model that quantified in monetary terms (dollars per hour), this will be done by analyzing the cost of various countermeasures that may deploy to improve security, then the decisions makers or the investor match these costs against the benefits that result from these countermeasures in terms of reduced the failure costs. This metric enables to derive an economic model that captures the tradeoffs involved in deploying security countermeasures.

All of these developments mean more data flowing across the internet and more opportunities for data centers to use technology to increase their revenue and improve their business process by applying a novel cyber-security measures such as the MFC, accordingly, data center will be the central one that can utilize those opportunities and there is a need to move quickly to adapt this MFC with this significant changes that occurred in social media, mobile devices and cloud services. However, in future cyber attacks will represent a major challenge for data center operators in the coming years.

CHAPTER THREE
MFC AS AN ECONOMETRIC APPROACH

3.1. Introduction

After the era of mainframe computing (from the nineteen fifties to the nineteen seventies), and the era of personal computing (from the nineteen eighties to the first decade of this millennium), researchers are now witnessing the emergence of the era of cloud computing (starting from the second decade of this millennium). In the era of cloud computing, end users of computing resources subscribe to service providers, and pay for services on the basis of their level of use. This means that large numbers of users share computing and storage resources in a context where they have little control over access privileges. This raises massive security concerns, which must be addressed in order for the cloud computing paradigm to fulfill all its potential and deliver all its promise. This chapter discusses the economic based measure of cyber-security, and explores how it can be used to measure the security of the cloud, that affect the various stakeholders.

In the last few years, a lot of evidence is pointing to the emergence of a new computing paradigm, whereby end users avail themselves of computing and storage resources delivered by service providers, who commit to manage and maintain huge resources, for which end users are charged according to their needs. This evolution parallels the evolution of other utilities such as water utility, gas utility, electricity utility …etc With the emergence of cloud computing, end users no longer have to deal with the operation and maintenance of complex workstations, the storage of important information, buying licenses …etc All these functions are delegated to highly skilled professionals specialized in the operation and maintenance of the cloud infrastructure. Cloud computing involves tens of thousands of end-users and other stakeholders who share massive, highly distributed computing resources, and huge, highly distributed storage space; ensuring that all these users share all these resources without mutual interference, so this research will discuss and illustrate a cyber-security metric which expected to be highly adapted with cloud computing.

3.2. MFC Metrics

Whereas reliability is usually measured by Mean Time To Failure (MTTF), a number of similar measures have been proposed to quantify the cyber-security of a system. These include Mean Time To Detection (MTTD): the mean time it takes for perpetrators to detect vulnerability, Mean Time to Exploitation (MTTE): the mean time it takes perpetrators to exploit a detected vulnerability, Mean Time To Repair(MTTR), etc. Broadly speaking, all these metrics fail to consider the variance that may exist between cloud stakeholders, security requirements, components and threats. However, the MFC consider all these variations and quantifies the cyber-security of a system in terms of dollars per hour of operation; the MFC considers the stakeholders variations in term of their needs.

Accordingly the MFC quantifies the impact of failures by providing a failure cost per unit of time. It determines the desirability of the operation assuming no more than one event occurred at a time. The main parameters of MFC metrics are (Aissa et al. 2010a):

1. Stakeholders,
2. Requirements,
3. Components,
4. Threats.

In the proposed case the Cloud Computing environment denoted by (V) that has many stakeholders, say H1, H2, H3… Hn. Then the value Xi has been defined which represents the loss that these stakeholder Hi stand to lose as a result of possible security failures on cloud environment (V). Each of these stakeholders has it failure cost that is different from other stakeholder. So the MFC is defined for stakeholder Hi as a statistical mean of value Xi. That has been denoted by MFC(Hi). Then the MFC vector is presenting the failure cost per unit of time for each stakeholder, a vector of all MFC(Hi) values for all stakeholders is denoted simply by MFC. A formula (1) is given for computing the mean failure vector as in (Aissa et al. 2010a):

$$\mathbf{MFC = ST \,.\, DP \,.\, TIM \,.\, TV} \qquad \mathbf{(1)}$$

Where

- **ST**, the Stakes matrix, is a matrix that has as many rows and many columns has:
  - Many rows → are stakeholders (Hi) and
  - Many columns → are cyber-security requirements (Rj) for cloud environment V.
  - The entry ST(Hi,Rj) represents (in dollars) the loss that stakeholder Hi stands to lose if requirement Rj is violated.

  This matrix is filled by individual stakeholders or stakeholder classes, and represents for each requirement the loss (in dollars) that a stakeholder (class) loses if the indicated requirement is violated. Stakes Matrix is shown in table 3-1.

- **DP**, the Dependency matrix, has as many rows and columns that has:
  - Many rows → are cyber-security requirements (Ri), and
  - Many columns → are cloud components (Cj).
  - The entry DP(Ri,Cj) represents the probability that requirement Ri is violated assuming that component Cj has been compromised.

The Dependency matrix produces a co-relation between security requirements and its components; specifically, it represents the probability of security requirements violation given that specific component has been compromised as shown in table 3-2.

- **TIM**, the Threat Impact Matrix, has as many rows and many columns that has:
    - Many rows → Cloud architecture/components (Ci), and
    - Many columns → are the technical cyber-security threats (Tj).
    - The entry TIM(Ci,Tj) represents the probability that component Ci is compromised assuming that threat Tj has materialized.

The Threat Impact Matrix produces a co-relation between cloud components and its security threats; specifically, it represents the probability of components failure given that specific security threat has materialized as shown in table 3-3.

- **TV**, the Threat vector, is a vector that has:
    - Many rows and one column → cyber-security threats.
    - The entry TV(Ti) represents the probability that threat Ti materializes during a unitary period of time (for example: an hour).

Threat Vector (TV) in table 3-4 characterizes the threat situation by assigning to each threat the probability that this threat will materialize per a unitary period of time.

All these matrices can be adjusted and each matrix has specialist ones who are responsible for filling the matrix, changing the content of any matrix or adding/removing either row/column is allowable based on their current needs, table 3-1 represent a responsible specialist who deal with that MFC matrices.

Table 3-1: MFC Matrices and Responsible Specialist for Filling its

Matrix	**Responsible entities**
ST	Individual stakeholders
DP	System architects
TIM	Analyst and Cyber-security experts
TV	Security team

Accordingly, this study will discuss the effort to specialize the MFC formula to Cloud Computing, by modeling and composing the following parameters:

- The typical stakeholder classes for Cloud Computing.
- The typical cyber-security requirements for Cloud Computing.
- The typical system architecture for Cloud Computing systems.
- The typical cyber-security threats for Cloud Computing.

3.3. MFC Metrics "Algebra Point of View":

As an example to compute the MFCs, the following four basic Matrices/Vectors needed to be filled:

- **The Stakes Matrix (**ST**)** – this matrix represent to what extent that each stakeholders stand to lose as a result of security failures (as shown in table 3-2):
  - Requirement clauses: R1, R2, R3… Rn.
  - STi,j: stakes that stakeholder Hi has in meeting requirement Rj (loss that Hi incurs if Rj is not satisfied),
  - PRj: probability that Rj is not satisfied.
- **MFC(Hi):**

$$MFC_i = \sum_{1 \le j \le n} ST_{i,j} \times PR_j. \qquad (2)$$

- **Algebraically**:

$$MFC = ST \circ PR. \qquad (3)$$

Table 3-2: Stake Matrix Structure (ST Matrix)

ST	R1	R2	R3	R4	…	…	…	Rn	**NoR**
ST									**0**
H1		**Stakes that stakeholder Hi puts on meeting requirements Rj**							**0**
H2		*(loss that Hi exposed if Rj is not satisfied)*							**0**
H3									**0**
H4									**0**
…									**0**
…									**0**
Hn									**0**

The PR computation:

- **The Dependency Matrix (DP)**: reflect the dependency between cloud **components** and cloud **security requirements**; this relation reflects how/to what extent each component of the system contributes to meeting each security requirement (as shown in table 3-3) , e.g. if the **Operating System** or **application component** is compromised, then the **confidentiality** will be affected with a certain probability.

  Compute the PR is being done by knowing the probability of failing to meet requirement Ri.

  - The architecture of the system is considered as:
    - Components C1, C2, C3, … Ch
  - Events Ei, $1 \leq i \leq h+1$:
    - Ei, $1 \leq i \leq h$: Ci has failed.
    - Eh+1: No component has failed.
  - Hypothesis: Single fault per unit of time.
  - Events Fj: System S has failed with respect to requirement Rj,
  - Bayesian Formula (4),

$$PRj = \sum_{k=1}^{h+1} P(F_j \mid E_k) \times P(E_k). \qquad \textbf{(4)}$$

  Where:

  - PRj: probability of event Fj,
  - Events Ek disjoint,
  - Hence:
  - Algebraically, formula (5) is shown below:

$$PR = DP \circ PE. \qquad (5)$$

Table 3-3: Dependency matrix Structure (DP Matrix)

DP	**C1**	**C2**	**C3**	**C4**	**…**	**…**	**…**	**Ch**	**Ch+1**
R1									**0**
R2		*Probability that Requirement Ri is violated*							**0**
R3		*If component Cj is compromised*							**0**
R4									**0**
…									**0**
…									**0**
…									**0**
Rn									**0**
Rn+1									**1**

The PE computation:

- **The Threat Impact Matrix (**TIM): This matrix represents the probability that certain **component** is compromised assuming that certain **threat** has materialized, e.g. the occurrence probability of the *shared technology issues* threat, which affected to IaaS components (such as VM and OS) – (see table 3-4).
  - Compute the PR is being done by knowing the probabilities that various components are compromised.
  - Threat configuration of the system considered as,
    - Threats T1, T2, T3, … Tp.
- **Events** Ti, $1 \leq i \leq p+1$:
  - Ti, $1 \leq i \leq p$: Threat Ti has materialized.
  - Tp+1: No threat has materialized
  - Hypothesis: Single threat per unit of time.
- **Events Ek:** Component Ck has been compromised as a result of threat occurrence.
- **Bayesian Formula,** formula (6) is shown below:

$$PE_k = \sum_{q=1}^{p+1} P(E_k \mid T_q) \times TV_q. \qquad (6)$$

Where:

- PE_k: probability of event E_k,
- Events Tq disjoint.
- Hence:

- **Algebraically**, formula (7) is shown below:

$$PE = IM \circ TV. \qquad (7)$$

Table 3-4: Threat Impact Matrix Structure (TIM Matrix)

DP	**T1**	**T2**	**T3**	**T4**	**…**	**…**	**…**	**Tp**	**Tp+1**
C1									0
C2		*Probability that component Ci is compromised*							0
C3		*if threat Tj has materialized*							0
C4									0
…									0
…									0
…									0
Cn									0
Ch+1									1

- **The Threat Vector (TV)**: it reflects the threat **probability per unit of time** (as shown in table 3-5) e.g. certain portability of "*Data Breaches threat*" per unit of time.

Table 3-5: Threat Vector (TV)

TV	**Probability**
T1	
T2	
T3	
T4	
..	*Probability that threat Tq materializes during a unit of operational time (e.g. 1 hour)*
..	
..	
Tp	
Tp+1	*Probability that no threat materializes*

Then by using the previous data, the vector of MFCs can be calculated in dollars per hours ($/Hrs) using the formula (1).

Table 3-6: the MFC for each stakeholder

Stakeholders	**MFC $/Hour**
H1	
H2	
H3	
T4	
..	*MFC per a unit of time* *MFC = ST.DP.TIM.TV*
..	
..	
Hn	

3.4. Generate and Fill Matrices Using Abstract MFC Model

This part represents how the MFC matrices will be generated based on Systematic Literature Review (SLR) with analytical reasoning and empirical data that may help to build and quantify an associated matrix which has been supported by the automated tool. Surely some threats are more likely to cause failure than others, and some components are more critical to meeting security requirements than others, to represent these variations the following matrices were represented (Nahla Murtada 2016b):

1. ***Stake Matrix*:** This matrix has been proposed based on rationale, many articles compared the cost aspects between cloud stakeholders, they claim that whenever the number of served users being bigger the failure cost will be higher, so cloud provider usually paying more than other stakeholders in the event of security failures, because the provider here serve the highest number of users, however usually the case of cloud consumer (normal user) is opposite; and cloud broker and cloud carrier are in the middle, the most reliable data is that data that has been published by NIST, CSA and Symantec ISTR reports, because most of the trusted articles refer to them and they are representing as a most and a well known sectors for proposing up-to-date information about Internet Security Threat Report and all relevant aspects of Cloud Computing (see table 3-7).
2. ***Dependency and Threat Impact Matrix:*** four Levels (0,1, 2 and 3) has been assigned to each entry (Nahla Murtada 2016b), (CSA 2013a), (Ponemon Institute 2016), (Symantec 2015), (Symantec 2014), (Verizon 2014) as shown in the following tables 3-8:
    - Level 3: This level take the value of "3" and representing the most affected requirements in case of compromising component or the most affected component in case of threat materialized (here data has been published in some of trusted articles called "ISTR" that are focusing mainly on the impact of failures such as (NIST, CSA, Symantec reports, and some others trusted articles published by "Threats Working Group"), and when it is mapped to probabilities it takes the highest probabilities.
    - Level 2: This level takes the value of "2", the effect here is less than level 3, data here has been obtained from another journal that has been published by authors and other researchers and it doesn't exist on all reviewed "ISTR" articles, and when mapped it to probabilities, it takes median probabilities.
    - Level 1: Take the value "1", here either some journal mentioned the minor effect on those entities in the event of failures occurrence or no one considering this effect- when mapped to probabilities, it takes the lowest probability.
    - Level 0: Take the value "0", here if explicitly mentioned that no effect of that failures on this entity (No Impact).

However, the lowest row (NoR and NoC row) take probabilities (0.1, 0.2, 0.3, 0.4…etc) depending on how critical the component or threat is. The following table 3-8 presenting the DP Matrix as example which presenting a sample of data that demonstrate the levels which has been assigned to each entry, accordingly table 3-9 and table 3-10 has been generated which presenting how to map these levels to probabilities.

3. ***Threat Vector:*** This vector is proposed based on many incidents on ISTR on cloud computing, most of collected data here is based on the proposed reports by Symantec ISTR and CSA (which were discussed in chapter one), these incidents have been mapped to probabilities per a unit of time by calculating "Probability of Threat Materialized" which is denoted by (PTM) using the following proposed formula (8) and formula (9) has been generated based on "Probability Distribution Rules":

$$PTM_i / hr = \frac{Number\ \ of\ \ Incident\ \ Per\ \ Year}{365\ \ DY * 24\ \ Hrs}, Where\ \ (1 <= i <= n) \qquad \textbf{(8)}$$

$$PTM_i / hr = 1 - \sum_{i=1}^{i=n} \frac{Number\ \ of\ \ Incident\ \ Per\ \ Year}{365\ \ DY * 24\, Hrs}, Where\ (i = n + 1) \qquad \textbf{(9)}$$

Accordingly, a number of incidents (No. of Incident) for each threat has been recognized for creating Threat Vector (TV) as shown in Table 3-11, then table 3-12 were mapped these No. of Incidents to probability format, so this vector representing the probability of threat materialize per a unitary period of time (e.g. an hour) which shown in table 3-12.

By using the MFC formula table (3-13) has been resulted as an output representation that present the MFC result for each stakeholder per unit of time.

Table 3-7: Stake Matrix (ST)

Cloud Stakeholders	**ST**	**Security Requirements**				
		Authentication	Authorization	Confidentiality	Data Integrity	Availability
	Cloud Consumer	10	24	25	20	20
	Cloud Provider	120	70	140	110	105
	Cloud Carrier	20	40	40	35	30
	Cloud Broker	20	60	50	40	40

Table 3-8: Assign level number to each entry (Nahla Murtada 2016)

DP		Cloud Components						
		Level No.	Applications	Runtime	Middleware	OS	Hyper visor	Infrastructure
Security Requirement	Authentication	Level No.	1	1	1	3	3	1
	Authorization	Level No.	1	1	1	3	3	1
	Confidentiality	Level No.	1	1	1	2	2	1
	Data Integrity	Level No.	2	2	2	1	1	2
	Availability	Level No.	3	2	1	1	2	2
	NoR	Criticality Factor	0.5	0.125	0.125	0.25	0.375	0.375

It is difficult to explain all MFC entries (as example DP has 6 rows *7 columns = 42 entries and TIM has 7 rows * 13 columns = 91 entries) so this measure has a lot of entries, for the MFC matrices each of them has been filled according to an assigned proposed criteria, but the following part represents the sample of the reasoning for filling some values in the MFC matrices:

- This step starts by filling the lowest row of the matrix, for example: the probability of violating requirements given a component compromise, here experts estimate the likelihood that a component failure causes no violation of any requirement, and place that value in the lowest row (0.1, 0.2, 0.3, 0.4, etc) which is denoted by (NoR) depending on how critical the component is (here the intersection between the "NoR" and "Application" column is 0.5), same thing for the Threat Impact Matrix.
- Then remaining probability (0.9 or 0.8,0.7, 0.6 or 0.5…etc) will be distributed on the remaining entries of that column according to the levels (0, 1, 2 or 3) that were assigned to each entry – using the below proposed formula (10), formula (11), and formula (12) using the probability of remaining entries and the probability factor of each entry, (as shown in table 3-9 and table 3-10):

$$\Pr obability\ of\ \ \mathrm{Re}maining\ Entries(\Pr) = 1 - NoX \quad \textbf{(10)}$$

$$\Pr obability\ \ Factor\ \ Of\ \ Each\ \ Entry\ \ (PF) = \frac{\Pr Ratio}{\sum_{i=1}^{n} Level\ \ No(SLNO.)\ \ Value} \quad \textbf{(11)}$$

$$\Pr obabilityFormat(i) = PF \times LevelNo.Value(i) \quad \textbf{(12)}$$

Where: NoX: mean NoR, NoC or NoT, $\forall$ 1<=i<=n.

For example: let's assuming the "Application Component" is the one of the most critical component in the Dependency Matrix so (here the intersection between NRF and "Application" column is 0.4), then distributing the remaining probability (0.6) on the remaining entries of the column to Keep MFC matrix balanced by submitting the "Probability Distribution Rules" by assuming that no more than one event has been occurred at a time (which means no more than one requirement has been violated at a

time, no more than one component has been compromised at a time and no more than one threat has been materialized at a time), so each selected component (e.g. Application Component), for these remaining entries determine if the security requirement is most affected by failure of this component or not, (in this case it is "Availability Requirement"), accordingly assigning level 3 that entering the highest probability 0.1875 (in the remaining entities *(from 1 to n)*) on that column (refer o table 3-9) same thing for the TIM.

$$\Pr = 1 - 0.5 = 0.5$$

$$\Pr obability\ Factor\ Of\ \ Each\ Entry\ \ (PF) = \frac{\Pr\ Ratio}{\sum_{i=1}^{n} Assigning\ \ Value\ \ for\ The\ Level\ \ No\ \ (SLNO)} \quad \textbf{(11)}$$

$$= 0.5/8 = 0.0625 \quad \textbf{(12)}$$

$$\Pr obability\ \ Format(i) = PF \times Level\ \ No.Value(i)$$

Probability format(i) = 0.0625 * 1 = 0.0625, where i=1

Probability format(i) = 0.0625 * 2= 0. 0.125, where i=2

Probability format(i) = 0.0625 * 3= 0.1875, where i=3

Table 3-9: Mapping the Level No. to Probability Format

I		Applications (with Level No format)	Application with (Probability Format)
1	Level No.	1	1* 0.0625= 0.0625
2	Level No.	1	1* 0.0625= 0.0625
3	Level No.	1	1* 0.0625= 0.0625
..	Level No.	2	2* 0.0625= 0.125
N	Level No.	3	3* 0.0625= 0.1875
N+1	Criticality Factor	0.5	Sum = 1
	Pr = (1-0.5)	0.5	
	SLNo. = (1+1+1+2+3)	8	
	Pr(i) Ratio = 0.5/8	0.0625	

Table 3-10: Mapping Level No. Approach To Distribution Probability Approach

		Cloud Component					
		Applications	Runtime	Middleware	OS	Hyper visor	Infrastructure
Security Requirement							
Authentication	Level No.	0.0625	0.125	0.1458333	0.225	0.170455	0.089286
Authorization	Level No.	0.0625	0.125	0.1458333	0.225	0.170455	0.089286
Confidentiality	Level No.	0.0625	0.125	0.1458333	0.15	0.113636	0.089286
Data Integrity	Level No.	0.125	0.25	0.2916667	0.075	0.056818	0.178571
Availability	Level No.	0.1875	0.25	0.1458333	0.075	0.113636	0.178571
NoR	Criticality Factor	0.5	0.125	0.125	0.25	0.375	0.375

Table 3-11: The number of incidents for each threat

	Threat Vector (TV)	
Threat No.	Threat Name	No. of Incident
T1	Data Breaches	51
T2	Weak Identity, Credential and Access Management	6
T3	Insecure APIs	51
T4	System and Application Vulnerabilities	4
T5	Account Hijacking	3
T6	Malicious Insiders	3
T7	Advanced Persistent Threats (APTs)	15
T8	Data Loss	43
T9	Insufficient Due Diligence	11
T10	Abuse and Nefarious Use of Cloud Services	12
T11	Denial of Service (DoS)	40
T12	Shared Technology Issues	5

Table 3-12: Threat Vector (TV) mapped to probability distribution

Threat	**No. Inci.**	**Threat Probability (TP)** PTM_i / hr	**Week0**
T1	51	51/24*365	0.00582192
T2	6	6/24*365	0.00068493
T3	51	51/24*365	0.00582192
T4	4	4/24*365	0.00045662
T5	3	3/24*365	0.00034247
T6	3	3/24*365	0.00034247
T7	15	15/24*365	0.00171233
T8	43	43/24*365	0.00490868
T9	11	11/24*365	0.00125571
T10	12	12/24*365	0.00136986
T11	40	40/24*365	0.00456621
T12	5	5/24*365	0.00057078
Not		1-sum(TP)	0.97214612
Sum			1

NoT: No Threat has been Materialized

No. Inci. : Is Number of Incidents

Table 3-13: MFC for each stakeholder ($/h)

Stakeholders	MFC($/Hrs)
Cloud Consumer	1.549470
Cloud Provider	456.148403
Cloud Carrier	199.400446
Cloud Broker	163.069010

3.5. Rationale for Systematic Literature Review (SLR):

According to (Putri & Mganga 2011) cloud computing is emerging at this moment. However, there is less information to collect from industry practitioners, for this reason this study only rely on information from literature to attain some of the objectives of this study. So data has been collected through SLR which adopted as a systematic, comprehensive, structured and repeatable process that is used to identify and analyze published studies.

This study used SLR to gather data regarding security threats and information security attributes in cloud computing form a different threat models as well as proposing a suitable framework for identifying information security metrics.

3.6. Summary of the MFC Metrics

ST contains the cost of a security breach in dollars (not dollars per hour, but dollars). TV is the probability of threats PER HOUR. When you multiply ST (in DOLLARS) by DP.TIM (which are probability metrics without dimension) by TV (which in probability PER HOUR), you get DOLLARS per HOUR. whereas ST represents the cost of a failure event when it happens, MFC represents the MEAN failure cost over the many hours (those where a failure occurs and those no failure occurs), the following table 3-14 presented and summarized these MFC metrics and it's characteristics.

Table 3-14: The MFC Metrics

ST Matrix	Is matrix Rows = Cloud Stakeholders Column = Security Requirements Entries: Dollar ($)	ST(H,R)	- Is the Stakeholders (H) satisfying a Requirement R? - Is quantified in term of cost ($).
DP Matrix	Is a matrix Rows = Cloud Security Requirements Columns = Cloud Components Entries: Failure Probability	DP (R,C)	- The Probability that the system fails to meet Requirement R if Component C is Compromise.
TIM Matrix	Is a matrix Rows Entities = Cloud Component	TIM (C,T)	- The Probability that Component C is Compromised if Threat T has materialized.

	Column Entities = Cloud Security Requirement Entries: Failure Probability		
TV : Threat vector	Is a Vector Entities : Threats Entries: Threat Probability	TV (T)	- The Probability that Threat T Materialized for a unit of operation time (one hour of operation).
MFC	Is a Vector Entities = Cloud stakeholders Entries: Failure Cost per unit of time.	MFC(H)	- Is Mean Failure Cost per unit of time for each stakeholder, it represented in term of ($/Hrs).

3.7. MFC Features

This quantitative model enables all cloud stakeholders (especially Cloud Service Providers) to quantify the threat they take with the security of their assets and to make security related decisions on the basis of quantitative analysis, which maps a Threat Vector onto a vector of MFCs for all stakeholders. When a security measure is deployed, its impact can be measured by considering how it affects on the Threat Vector (say, TV' instead of TV) and accordingly how it affects on the MFC vector (MFC' instead of MFC) in term of reduced MFC, so this measure can be used to support the following decisions:

- The system manager can determine whether a security measure is worthwhile by matching its deployment cost against its benefit (which represented in terms of reduced MFC). The decision can in fact model as a return on investment decision.
- Dispatching the investment cost can be based on the MFC reduction of each stakeholder which can be used on the various system stakeholders.
- The MFC has been calculated by using the MFC formula which results in MFC vector for each stakeholder, this will be done by considering the existing variance between stakeholder's requirements, components, and threats that cause failures.
- MFC gives stakeholders a reasonable estimate of their failure cost per unit of time, which measured by a unit of currency per time frame (e.g. dollars per hour or dollars per week).

3.8. Framework for Measurement of Cloud Security Risk by MFC

The following Figure 3-1 presenting the whole life cycle of the MFC with using the cost/benefit analysis model that can be adapted to all cloud service models which can be performed by the following steps (Nahla Murtada 2016a) (Nahla Murtada 2016b):

- Filling all MFC matrices (ST, DP, TIM and TV) using the proposed filling approach with adherence to "Distribution Probability Rule" with entering an empirical data to achieve realistic and accurate results, and this step is one of the main contributions of this study, because until now, there are no statistics on the volume of failure cost on cloud computing environment per unit of time

- Computing the MFC0 (as shown in table 3-12).
- Deploying a suitable countermeasure that helps to enhance the security of the Cloud Computing in term of reducing the MFC. Cloud investors may need to deploy some countermeasures to reduce the failure impact and amount, in the proposed measure there are four countermeasures that used to enhance and control the MFC metrics, each measure is used to control specific MFC matrix. The following section will discuss these measures.
- Reflecting the enhanced values of measure to associate matrix (by "Decreasing" the probability of failure and "Increasing" the probability of no failure).
- Recalculating the MFC to obtain the MFC1 and calculate the difference (MFC Gain) =MFC0 - MFC1.
- Dispatching the investment cost for accruing the measure across stakeholders in proportion to the MFC Gain.
- Comparing the cost of measure against the benefits (MFC Gain) to decide if the measure is worthwhile or not and this will be done for each stakeholder.

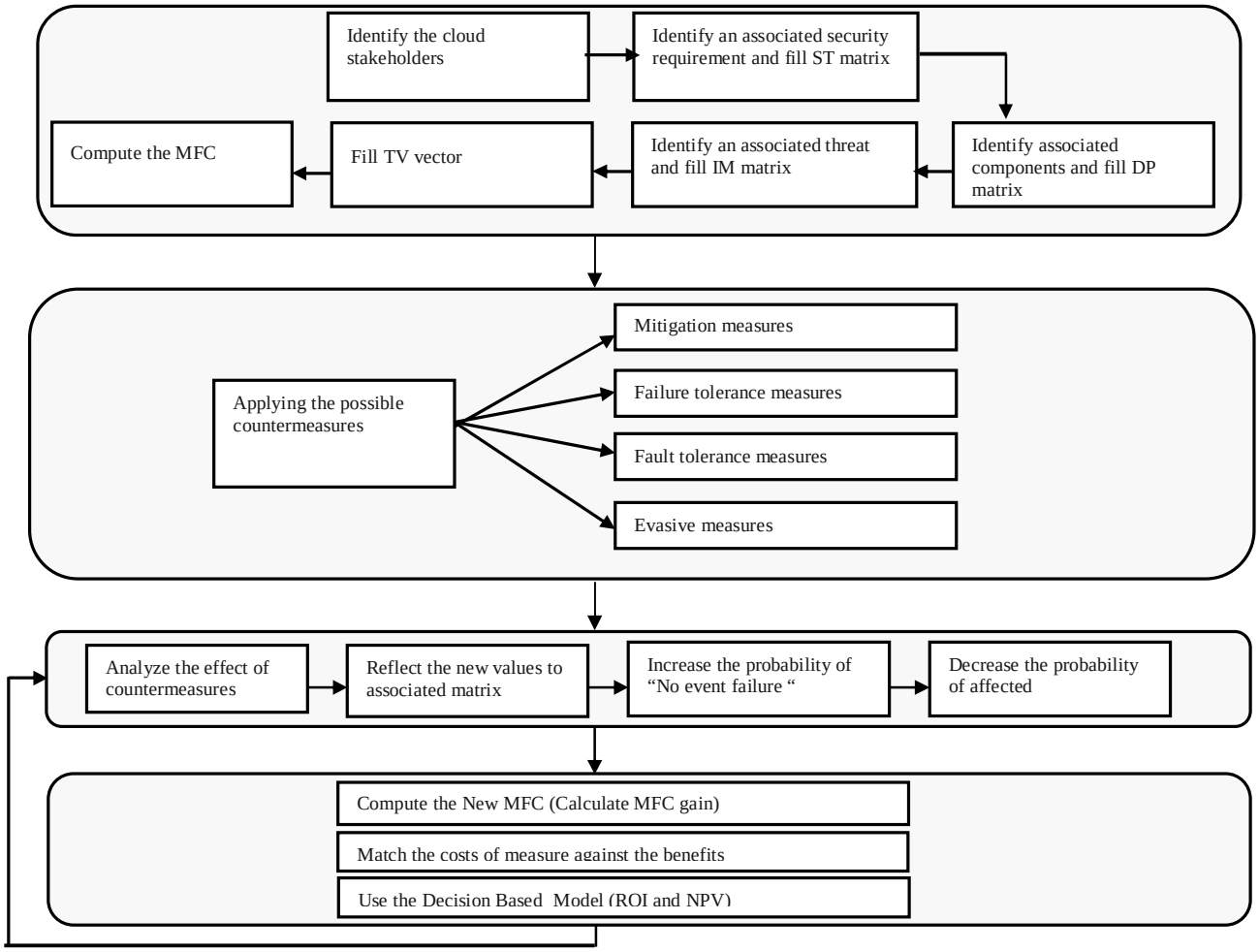


Figure 3-1: Framework for Measurement Cloud Security Risk by MFC

3.9. Enhancement and Controlling Measures:

Too many experts (such as CSA and NIST experts) provide some cyber-security measures that may decrease the effect of threats by applying some mitigation and avoidance guidelines, so MFC proposed multiple enhancement measures (**Mitigation measures, Failure tolerance measures**, **Fault tolerance measures, Evasive measures**) each of these measure is used to control and enhance specific MFC factor that may use to obtain better MFC values in term of reduced MFC. A given security enhancement measure (which can be represented as investment project) can be done either by using one of the following countermeasures (See Figure 3-1) (Nahla Murtada 2016):

- **Mitigation measures:** controlling the stakes matrix. This family designates measures which it takes to reduce the impact of failures on costs incurred by users.
- **Failure tolerance measures**: controlling the Dependency matrix. This family designates measures which minimize the impact of component failures on system failures by enhancing the failure tolerance of the system (using Redundancy, for example).
- **Fault tolerance measures**: controlling the Threat Impact Matrix. This family designates measures which minimize the incidence of component failures by eliminating or mitigating component vulnerabilities.
- **Evasive measures**: controlling the threat vector. This family designates measures which aim to conceal component vulnerabilities, or otherwise making it harder to exploit them.

MFC has different matrices used to estimate the failure cost per unit of time for each stakeholder. Investors usually need to deploy some countermeasures to obtain more revenue, to mitigate the impact of security failures, and controlling the MFC metrics in term of reduced MFC. These countermeasures are represented as investment project which need the investment cost, decision makers can determine the cost effectiveness by comparing the cost of installing the enhancement versus the gained benefit by using economic assessments known as cost-effectiveness analysis that can be quantified by a Return On Investment function which will be discussed in the next sections .

3.10. Economic Approach

Most economic approaches are built to measure and investigate the amount of additional profits produced due to a certain investment (in specific period of time). this type of calculation have been used to *compare between different scenarios for investments* to decide which would be produced to lead the greatest profit and benefit for the company by comparing the revenue with the total investment cost,

there are too many econometrics approaches support this philosophy such as (Mccready 2005) (Botchkarev & Andru 2011) (Bliss et al. 2015):

- Return On Investment (ROI).
- Net Present Value (NPV).
- Internal Rate of Return (IRR).
- Total cost of investment (TCO).

3.10.1. Return On Investment (ROI) History:

ROI is a collective term for different cost benefit economic aspects, which is used to ***estimate the profit ratio for each stakeholder*** by representing the financial gain of investment compared to its total cost. This ROI can be used to help decision makers to decide correctly against the deploying security measure, If (***ROI >0***) then the investment is judged as profitable, Otherwise decision makers should not implement the measure (Boehme & Nowey 2008).

ROI is a measure that investigates the amount of additional profits produced due to a certain investment (in specific period of time). Businesses use this calculation to compare different scenarios for investments to decide which would produce the greatest profit and benefit for the company, this calculation can also be used to analyze the best scenario for other forms of investment.

Sonnenreich et al. (Sonnenreich et al. 2006) presented an easily understandable metric which is called Return on Security Investment (ROSI). ROSI is a collective term for different cost benefit economic aspects. The basic idea of ROSI is derived from the classic return on investment (ROI) which represent the financial gain of investment compared to its total cost, as shown on the following formula (13) (Blakley, 2001), (Purser, 2004):

$$ROSI = (ALE0 - ALE1) - Cost \qquad \textbf{(13)}$$

Where:

ALE0: Represent the current Annual Loss Expectancy cost *without* deploying the security measures, and

ALE1: Represent the current Annual Loss Expectancy cost *with* deploying the security measures.

Cost: Represent the total investment cost.

This ROSI can be used to help decision makers to decide correctly against the deploying security measure.

If (ROSI >0) then the investment is judged as profitable,

Otherwise decision makers should not implement the measure.

However, this metric gives only the investment return without building *ratio* for comparing the result with the capital employed and thus cannot be used to compare different alternative scenario in the IT security measures.

So other researchers change the shape of the formula and give up a ROSI definition that puts the precise value of a security measure in relation to its costs, the formula (14) has been shown below (Sonnenreich et al. 2006):

$$ROSI = \frac{((RiskExpousreCost)(\$) \times \%RiskMitigated) - Cost}{Cost} \qquad \textbf{(14)}$$

It is worth mentioning that the product (risk exposure cost * % risk mitigated) and ALE0-ALE1 is very similar to each other, all of them represented as" Gain from Investment".

This metric does not only represent a monetary unit only, but also considers a *ratio* (usually expressed in percentage). This has two advantages:

- First, it enables the comparison of different security measures.
- Second, it enables the comparison of different investment projects, so companies can see how efficiently its capital is used when the IT security investments can be compared to other investment projects.

Some other researchers introduced other similar measure called "Risk Leverage" that can be used to demonstrate the efficiency of a security measure; the formula (15) has been shown below (Sonnenreich et al. 2006):

$$ROSI = \frac{(Risk\ \ Expousre\ \ Before\ \ \text{Re}duction) - (Risk\ \ Exposure\ \ After\ \ \text{Re}dudction)}{Cost\ \ Of\ \ Risk\ \ \text{Re}duction} \qquad \textbf{(15)}$$

This simplest form of the formula for ROI can also be represented as the following formula and only two values should be considered: the cost of the investment and the gain from the investment. The formula (16) is as follows:

$$ROI(\%) = \frac{(Gain\ \ From\ \ Investment\ \ (B)) - Cost\ \ Of\ \ Investment}{Cost\ \ Of\ \ Investment} \times 100 \qquad \textbf{(16)}$$

The ratio is multiplied by 100, making it in a *percentage value*. This way, a person is able to see what percentage of their investment has been gained back again. However, someone prefers to leave it in decimal form.

Though, this concept assuming a planning interval is a one year, but in reality most investment decisions not only affect the current period only but also have an impact on the future as an extension investment, so another researcher enhance the "Risk Leverage" equation by **considering and calculating the present value of future inflows** (receiving an inflow from an investment project) with outflows (charging out flow to investment project) which seems necessary. This can be done by adding new parameter which is called the "Discount Rate" that is discounting the expected future cash flows to the present with an appropriate IR (Interest Rate) (Publique et al. 2007), each stakeholder can decide it individually according to what his/her investment policy is. It is constant for each stakeholder, it takes the same value year to year for each stakeholder, and economist can determine this value based on their knowledge.

3.10.2. Net Present Value (NPV):

Net Present Value is intended to calculate the present value of an investment by discounting the sum of cash flow payments over a period of time.

Gordon and Loeb (Gordon and Loeb, 2006) found that economic analysis in budgeting for information security has been increasingly required by security managers, so they conduct the NPV which is a well established approach for determining whether the investment is "Profitable or Not" by considering the cost and benefit of a decision (over a period of time), the following table 3-15 calculated the difference between the present values of *future inflows* minus the present value of *outflows* of a project investment. An investment project is judged as profitable if NPV > 0, so this NPV compares the *future values of cash with its present (current) value*. Economists produced a sophisticated calculation formula for the NPV that has been particularly developed for a financial services company by evaluating of security investments, as shown below (Žižlavský 2014),(Jawad & Ozbay 2006), (Kooten 2016):

$$NPV = Initial\ \ Investment + \sum_{i=1}^{Time} \frac{Cash\ \ Flowi\ \ (Bi)}{(1 + Discount\ \ Rate)^{i}}$$, Or

$$NPV = \sum_{w=0}^{Time} \frac{B(w) - C(w)}{(1 + Discount\ Rate)^{w}} \qquad (17)$$

Where:

- A Benefit function $B(w)$, that maps weeks from 0 to W onto benefits (valued in dollars). With these parameters, the *ROI* is computed according to the previous formula.
- A cost function C(w), that maps weeks ***from 1 to W*** onto costs (valued in dollars), and $C_i(w)$ is the investment cost for stakeholder (i) toward the acquisition of the product (in week *w)*.
- C(0): Is the cost ***at week 0***, i.e. the Initial Investment Cost (the contribution that each stakeholder makes toward acquiring a cyber-security solution).
- A discount rate (abstract number), which represents the time value of money, that it's denoted by d (1 dollar today is worth (1 + d) dollars next year).
- *w*: A cycle length (investment cycle of stakeholder, counted in years, months or weeks), that it's denoted by (*y, m* or *w*).
- NPV: Net Present Value of an investment.

So ROI can be interpreted as a measure for the impact of the event on the market rating of companies. Therefore, estimates from different methods can be compared to assess the robustness of the results obtained (this will be explained in chapter 6).

3.10.3. ROI Over Time with Enhancement Measures

Investors calculate ROI over time to see how the value changes or when a positive ROI will occur. This gives them a better timeframe of how long it will take them to get an adequate return on their purchase.
The motivation for using ROI methods is to enhance and improve the efficiency of enhancement actions by comparing the different possible scenarios for the possible investment, the ROI formula has been shown below:

$$ROI = \frac{NPV}{C(0)} \qquad \textbf{(18)}$$

Table 3-15: Example of NPV for an investment of US $500,000 and a rate of 10 percent over 3 years:

Year	Cash Flow	Present Value
0	- $500,000	- $500,000
1	$200,000	$181,818
2	$300,000	$247,933
3	$200,000	$150,262
	Total Inflow	=$ 580,015
	Outflow	- $500,000
Investment NPV =		**$80,015**

$$NPV = Initial\ \ Investment + \sum_{i=1}^{Time} \frac{Cash\ \ Flowi\ \ (Bi)}{(1 + Discount\ \ Rate)^{i}}$$

$$NPV = -\$500{,}000 + \frac{\$200{,}000}{1.10} + \frac{\$300{,}000}{(1.10)^2} + \frac{\$200{,}000}{(1.10)^3}$$

$$ROI = \frac{580{,}015}{500{,}000} = 16\%$$

3.10.4. Calculate Benefits in term of MFC Gain

Calculate the benefits for each stakeholder by considering their MFC (table 3-16), their MFC gain (table 3-17) and how much each stakeholder uses the service which differs from one stakeholder to another in term of service availability (table 3-18), the obtained Benefits per week (B(w)) result (table 3-19) will help us to calculate the ROI and NPV to take a correct decision, this benefits can be calculated using the following formula (19):

$$Benefit(i) = MFC\ \ Gain_i(w) \times Hrs\ Of\ \ Usage_i(w) \qquad \textbf{(19)}$$

$$(\forall\ \ 1<=i<=\text{Time}(y,w))$$

The following table represents the MFC results for all stakeholders from week 0 – week 50 (*w0-w50)*

Table 3-16: MFC results with deploying enhanced measures (antivirus as example)

Week	0	5	10	15	20	25	30	35	40	45	50
MFC with anti-virus / **Stakeholders**	MFC0	MFC1	MFC2	MFC3	MFC4	MFC5	MFC6	MFC7	MFC8	MFC 9	MFC10
Cloud Consumer	2.18	2.08	2.03	2.01	2.00	2.00	2.00	2.00	1.99	1.99	1.99
Cloud Provider	640.96	610.69	598.46	592.81	590.03	588.61	587.88	587.50	587.30	587.20	587.14
Cloud Auditor	280.57	267.22	261.83	259.34	258.11	257.49	257.17	257.00	256.91	256.87	256.84
Cloud Broker	229.37	218.49	214.09	212.06	211.06	210.55	210.28	210.15	210.07	210.04	210.02
Sum	2.18	2.08	2.03	2.01	2.00	2.00	2.00	2.00	1.99	1.99	1.99

The following Table 3-17 presented the amount of improvement which is measured by obtaining the difference between the MFCs, by using the following formula (20).

$$MFC\ Gain = Old\ Value\ Of\ \ MFC(MFC0) - New\ Value\ Of\ \ MFC(MFC1) \quad \textbf{(20)}$$

Table 3-17: Amount of improvement in term of "MFC Gain"

Week	0	5	10	15	20	25	30	35	40	45	50
Stakeholders											
Cloud Consumer	0	0.10	0.15	0.17	0.18	0.18	0.18	0.19	0.19	0.19	0.19
Cloud Provider	0	30.27	42.50	48.15	50.93	52.35	53.08	53.46	53.66	53.76	53.82
Cloud Auditor	0	13.35	18.74	21.23	22.45	23.08	23.40	23.57	23.66	23.70	23.73
Cloud Broker	0	10.89	15.28	17.32	18.32	18.82	19.09	19.23	19.30	19.34	19.35

However, not all stakeholders are using the cloud service all the time (see table 3-18), for example cloud consumer may using the cloud service 7 hours per week, however the remaining stakeholders exploit all working hours per week (24 hours per day for the 7 days of the week) = 24* 8 = 168 hours, so this MFC Gain is based on "How much time you gain from the service".

Table 3-18: Hours of operation for each stakeholder

Week	0	5	10	15	20	25	30	35	40	45	50
Stakeholders											
Cloud Consumer	7	7	7	7	7	7	7	7	7	7	7
Cloud Provider	168	168	168	168	168	168	168	168	168	168	168
Cloud Auditor	168	168	168	168	168	168	168	168	168	168	168
Cloud Broker	168	168	168	168	168	168	168	168	168	168	168

To know the actual benefits (for each stakeholder) that have been gained in term of actual MFC Gain, apply the following formula 19 (see table 3-19):

Table 3-19: Calculated Benefit for each stakeholder

Benefit, B(w)	W0	W5	W10	W15	W20	W25	W30	W35	W40	W45	W50
Cloud Consumer	0	0.73	1.03	1.17	1.23	1.27	1.29	1.30	1.30	1.30	1.30
Cloud Provider	0	5085.35	7139.71	8088.81	8556.27	8794.03	8916.97	8981.09	9014.69	9032.33	9041.60
Cloud Auditor	0	2241.99	3147.70	3566.13	3772.22	3877.04	3931.24	3959.51	3974.32	3982.10	3986.19
Cloud Broker	0	1828.84	2567.65	2908.97	3077.08	3162.59	3206.80	3229.86	3241.94	3248.29	3251.62

As mentioned before, deploying a suitable countermeasure helps to enhance the security of the Cloud Computing in term of reducing the MFC, but how an investment cost is dispatched for accruing this measure across stakeholders?

3.10.5. Dispatching The Investment Cost Using Economical Based Approach:

Once the MFC has been computed for each stakeholder, it will be empowered to make economically based decisions regarding the amount of risk they want to take with regards to cyber-security. For example, if users are given the choice for upgrading their security risks using protection strategy at a given cost C, then they may determine whether the cost is justified or not by matching its benefits against the reduction in MFC. This becomes a Return On Investment decision, this ROI can be applied to each separate stakeholder to see whether the acquisition of the cyber-security solution is advantageous or not.

According to the MFC basis, a given security enhancement measure can be done by using one of the controlling measures and accordingly MFC gain (the difference between the MFC with and without deploying the security measure) can be calculated, investors and stakeholders are frequently needed to deploy some enhancement measures, these measures are represented as investment project and this project need the investment cost to be deployed, so all stakeholders should participate financially in this project, so the Investment Cost has been dispatched across these stakeholders to deploy this measure.

Questions:

How do decisions makers know if the measure is worthwhile?

How to Dispatch this Investment Cost across these stakeholders to deploy the measure?

1. **Question one: how do decision makers know if the measure is worthwhile?**
   Answer: this study proposing it by "Computing its ROI", For each stakeholder: if ROI>0, (then this investment is profitable), so the decision makers and economists can decide "to what extent this ROI must be greater than zero with gaining highest revenue".

2. **Question two:** How to Dispatch this Investment Cost across these stakeholders to deploy the measure? If implementation of the solution costs, for example, 8500$, how much will each stakeholder pay to cover this cost?
   Answer: There are two possible options:
   A. *Option 1*: In proportion to MFC gains, scenario (1)
   B. *Option 2*: Or dispatch that ICi are determined in such a way that all ROI's are Identical, scenario (2).

A. (Option 1): Let us Consider The First Option

By assuming that investment cost is charged on the stakeholders in proportion to their stake in the system (as measured by their respective MFCs Gains).

Here each stakeholder pays ICi as a proportion of their MFC reduction (Proportion to MFC gains/ΔMFC) which is represented as ($/hour), for example Let us consider the following scenario:

$MFC_{0=}$ MFC ***Without*** cyber-security solution.

$MFC_{1=}$ MFC ***With*** deploying a cyber-security solution.

Δ MFC: It means the difference before and after deploying the measure.

B(*w*): It means the Benefits in year (*w*).

IC, C(0) or C(*w*): It means the Initial Investment Cost at year(*w*) 0 (The whole Investment Cost to deploy the measure).

Estimating *B*(*y*) for each stakeholder being done by analyzing the reduction in MFC each stakeholder will experience as a result of deploying the countermeasure.

To simplify the analysis, this scenario assumed that the cost of acquiring and deploying the antivirus for example is 8,500 $ (which is less than the benefit result).

In This first option (Scenario 1): Dispatching cost in proportion to the MFC Gain, as shown in table 3-20 , here assumed that the cost of installing and deploying the countermeasure is 8,500 $, and this cost will be paid only once, that means $Ci(w)=0 \ \forall \ w>=1$.

Table 3-20: Dispatching cost in proportion to the MFC Gain

Stakeholders	MFC_0	MFC_1	Δ MFC (B(w)), for w>0	Prorate of cost	C(0) (distribution)
Cloud consumer	8	6	2	2/42	$C_1(0)=8500*2/42 =$ **$ 404.76**
Cloud Provider	113	93	20	20/42	$C_2(0)=8500*20/42 =$ **$ 4047.62**
Cloud Carrier	31	25	6	6/42	$C_3(0)=8500*6/42 =$ **$ 1214.29**
Cloud broker	54	40	14	14/42	$C_4(0)=8500*14/42 =$ **$ 2833.33**
			Total = 42		C(0) = 8500

The remainder of this section will review some scenarios of security measures, and assess their cost effectiveness by matching their implementation cost against their benefits, measured in terms of reduction in MFC. Cost/benefit analysis has been quantified by using ROI formulas, and compare alternative measures by comparing their respective ROIs. The NPV and ROI have been expressed by the following formula 17 and formula 18:

B. (Option 2): Let us consider "The Second Option"

Under some circumstances (as shown in table 6-17), the ROI of some stakeholders may be negative, hence the proposed investment is not representing as a worthwhile for all the stakeholders. In this situation, the formula in option one has been resolved by recalculating the initial investment costs, Instead of charging stakeholders according to their MFC Gain, so this second option will charge them in such a way that makes all ROIs identical.

Here dispatch that ICi are determined in such a way that make all ROI's identical. In this case, ICi's are derived from the following (4 equations, 5 unknowns):

IC = IC1 + IC2 + IC3 + IC4 (1)

ROI1 = ROI2 (2)

ROI1 = ROI3 (3)

ROI1 = ROI4 (4)

∀ stakeholders H*i*, assuming that the B*i* (0) = 0 and all C*i* (*w*) = 0 ∀ week(*w*) between 1 and W*i*, the ROI equation of stakeholder H*i* is shown in formula (21):

$$ROI_i = -1 + \frac{1}{C_i(0)} \times \sum_{w=1}^{wi} \frac{B_i(w)}{(1+d)^w} \qquad (21)$$

If supposing that the ROI*i* are equal ∀ stakeholders H*i* , $1 \le i \le n$

Knowing the initial cost C*i* (0) for all stakeholders need to resolve the *n* equations which are represented as shown in the following formula (22) and formula (23):

$$\begin{cases} ROI_1 = \ldots = ROI_i = ROI_n, i \in [1,n], & \textbf{(22)} \\ \sum_1^n C_i(0) = C(0) & \textbf{(23)} \end{cases}$$

The solution is shown in the following formula (24):

$$C_i(0) = \frac{C(0) \times \sum_{w=1}^{wi} \frac{B_i(w)}{(1+d)^w}}{\sum_{i=1}^{n} \sum^{wi}_{w=1} \frac{B_i(w)}{(1+d)^w}} \qquad \textbf{(24)}$$

(Assuming these numbers 1, 2, 3, 4 refer to the four stakeholders). Here they are five unknowns, hence calculating $C_i(0)$ using the previous equation, and once solved compute just one ROI, and announce that it is the ROI for all stakeholders. This Identical ROI has been supported by our proposed automated tool which will be presented in chapter 6.

By assuming that the (B(y)=Δ MFC), C(0)=325$ and after calculating the Bi(w) and the B(w) with a given Investment Cost subscribers can easily have Ci(0) which is representing the investment cost for each stakeholder, accordingly table 3-21 represents how the identical ROIs can be estimated.

Table 3-21: Dispatch that ICi with identical ROI's

For the Cloud Consumer														
Week	0	1	2	3	4	5	6	7	8	9	10	B1		
C(w)	C1(0)	0	0	0	0	0	0	0	0	0	0			
B(w)	0	2	2	2	2	2	2	2	2	2	2	20		
D	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023			
1+d^w	1	1.0023	1.00460529	1.006916	1.009232	1.011553	1.01387959	1.016212	1.018549	1.020891	1.02324	B1	C1(0)	ROI
B(w)	0	1.99541056	1.99083164	1.986263	1.981705	1.977158	1.97262082	1.968094	1.963578	1.959072	1.954577	19.74931031	15.47619048	0.276109282
For the Cloud Provider														
Week	0	1	2	3	4	5	6	7	8	9	10	B1		
C(w)	C2(0)	0	0	0	0	0	0	0	0	0	0			
B(w)	0	20	20	20	20	20	20	20	20	20	20	200		
D	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023			
1+d^w	1	1.0023	1.00460529	1.006916	1.009232	1.011553	1.01387959	1.016212	1.018549	1.020891	1.02324	B2	C2(0)	ROI
B(w)	0	19.9541056	19.9083164	19.86263	19.81705	19.77158	19.7262082	19.68094	19.63578	19.59072	19.54577	197.4931031	154.7619048	0.276109282
For the Cloud Carrier														
Week	0	1	2	3	4	5	6	7	8	9	10	B1		
C(w)	C3(0)	0	0	0	0	0	0	0	0	0	0			
B(w)	0	6	6	6	6	6	6	6	6	6	6	60		
D	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023			
1+d^w	1	1.0023	1.00460529	1.006916	1.009232	1.011553	1.01387959	1.016212	1.018549	1.020891	1.02324	B3	C3(0)	ROI
B(w)	0	5.98623167	5.97249493	5.95879	5.945116	5.931474	5.91786247	5.904283	5.890734	5.877216	5.86373	59.24793094	46.42857143	0.276109282

For the Cloud Broker												
Week	0	1	2	3	4	5	6	7	8	9	10	B1
C(w)	C4(0)	0	0	0	0	0	0	0	0	0	0	
B(w)	0	14	14	14	14	14	14	14	14	14	14	140
D	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	0.0023	
1+d^w	1	1.0023	1.00460529	1.006916	1.009232	1.011553	1.01387959	1.016212	1.018549	1.020891	1.02324	
B(w)	0	13.9678739	13.9358215	13.90384	13.87194	13.8401	13.8083458	13.77666	13.74505	13.7135	13.68204	B4
												138
											Total (B)	414

On the result chapter (Chapter 6), some aspects are more complicated in two ways:

- By using a weekly increment By 5 rather than a weekly increment By 1.
- By assuming that B(w) changes from a weekly increment to another.

B(*w*): May previous be varying by week if needed; the calculation would not be that different.

ΔMFC = (MFC Gain): Difference between the MFC with and without deploying the security measure.

The proposed approach can be characterized by the following premises:

The decision of whether the V& V action is worthwhile can be made separately for each stakeholder.

Each stakeholder computes his own ROI based on his contribution to the cost of V&V action, and the benefits he gains in terms of reduced MFC.

The cost of the V& V action must be distributed in such a way as to make the ROI positive for all stakeholders.

One possible formula for distributing the cost of the V& V action is to distribute it to the reduction in MFC for each stakeholder.

There are several strengths that an ROI and NPV approaches can offer relative to our decision (Tear et al. 2014):

When decision makers have different scenarios and they need to decide which one is better than another, in this case ROI and NPV are the most effective econometric measure to decide, each of them were used to compare which projects will obtain higher NPV value with higher profitability.

ROI and NPV provide a snapshot of profitability values, in case of comparing projects the higher NPV value will lead to higher profitability.

Evidence (the data used to calculate ROI) is used in the supporting of the decision making.

Net Present Value is intended to calculate the present value of an investment by the discounted sum of cash over a period of time.

One of the main contributions is to provide a flexible and convenient MFC model either when filling the MFC matrices or when structuring it, this chapter proposed how the MFC matrices will be filled with "Default Values" using analytical reasoning and some statistical reports (such CSA, Symantec and NIST).

This model allows re-adjusting the "Default Values" with keeping the balance of the MFC's Matrices, by proposing "Propagation Formula" as shown in the following formula (25):

$$\mathrm{Pr}opagateioneEquation = \frac{The\ \ Old\ \ Value\ \ Of\ \ \ Entry - New\ Value\ \ Of\ \ \ Entry}{Number\ \ Of\ \ \ Entries\ \ Of\ \ That\ \ Column - 1} \qquad \textbf{(25)}$$

The following chapters (Chapter 4) proposing a novel strategy for structuring the MFC and re-structuring (in Chapter 5), all of them resulting in MFC vector for all stakeholders with a different structuring and filling approach considering some other aspects, namely:

1. The abstraction aspects (in chapter 4) which are based to build the MFC metrics based on the main parameter of the MFC on cloud computing.
2. The new expansion aspects (in chapter 5) which are based on two categories:
    - The first category (in chapter 4): this category is called "the Multi-dimensional Model for the MFC" which building the MFC metrics based on a "Sub-classification of the MFC's main parameter".
    - The second category (in chapter 5): this category called "Service Base Model for the MFC" which building the MFC metrics based on identifying the MFC parameter in all Cloud Service models (IaaS, PaaS and SaaS).

Summary

MFC is one of the brilliant quantitative models that represents "to what extent that each stakeholder stand to lose as a result of security failure in software or hardware due to security breaches" which quantify the impact of failures per unit of time for each stakeholder by considering all variation that may exist between stakeholders, requirement, components and threats.

This MFC represents the typical cyber-security aspects that will be adapted with cloud computing such as cloud stakeholders (e.g. cloud providers and cloud consumers), cloud requirements (e.g. availability, authentication …etc), cloud components (e.g. Application, runtime, middleware…etc) and the most common threats on cloud computing (e.g. data breaches, shared technology issues , DoS…etc) along with their probability of occurrence per unit of time.

One of the most challenges that faced MFC model is "How to fill it's matrices and how it can be validated with adherence to probability distribution rules?", this chapter proposed a method for enriching the MFC entries which help to fill these matrices with logical entries and validate it using an empirical data with analytical reasoning that has been supported by SLR.

Fill data represented as a "Default Values" which can be re-adjusted using the propagation formula, then filling the probability matrices by adhere the distribution probability rules with a right and precise manner that helps to obtain a realistic results which will be shown in chapter 6, the whole details with adapt MFC with cloud computing services will be presented in the next chapter (chapter 4).

CHAPTER FOUR

ADAPTING MFC PARAMETERS WITH CLOUD COMPUTING ASPECTS

4.1. Introduction

Cloud computing is an emerging paradigm of modern computing, that represents a natural evolution from the current distributed, networked infrastructure. For all its advantages, in terms of convenience, economy, and effectiveness, cloud computing also poses serious challenges, and at least it needs to provide cyber-security guarantees to cloud users, such as confidentiality, integrity, and availability.

We believe that a sound discipline of cyber-security starts with a set of accurate metrics, so this chapter will discuss and illustrate a cyber-security metric which is believed to be highly adapted to cloud computing. The greatest challenge to the widespread use of this metric in the management of cyber-security is the need to fill all the matrices that are needed to compute it. The agenda for this research is calling for collecting analytical and empirical data on the cloud in order to make this task systematic, possibly even providing automated support for it (Nahla Murtada 2013).

4.2. MFC Parameters

The MFC consider all existing variations between stakeholders in term of their needs, each stakeholder needs security requirement which has quantified the cyber-security of a system in terms of dollars per hour of operation. Until now there are no statistics on the volume of estimating failure cost on Cloud Computing environment per unit of time.

As mentioned previously the MFC quantifies the impact of failures by providing a failure cost per unit of time. It determines the desirability of the operation assuming no more than one event will occur per unit of time. The main dimensions of MFC metrics are:

- Stakeholders,
- Requirements,
- Components,
- Threats.

4.3. MFC Dimensions on Cloud Computing

This chapter is going to define all (Cloud Stakeholders, Security Requirements, Components and Threats) that have been adapted to all MFC contexts which will be represented in terms of abstract representation which is called “Abstract Model for the MFC”, then a Multi-dimensional Model of the MFC (M^2FC) is proposed to enrich these MFC metrics by refining the MFC cyber-security measure which is based on a sub-classification of each MFC. Moreover, the proposed model of the MFC proposed a unified model of

security concepts because security lacks a clear taxonomy of all MFC parameters which leads to the improvement of the system's software quality.

This new expansion gives a multiple and better choices for re-structuring the MFC metrics, clear refinement, accurate estimation and useful interpretation for security related decision-making, the following section presents the main parameters of the MFC in cloud computing with decomposing these MFC parameters.

4.3.1. Cloud Stakeholders

There are many stakeholders that contribute in cloud computing **as a general** such as cloud provider, cloud consumers, lawmakers and regulatory bodies nationally and internationally, software companies, communication companies and investors. However, cloud consumers and cloud providers are the most affected bodies in the event of security failure. This section briefly review the stakes that they have in meeting the security requirements, which determine the corresponding values in the stakes matrix, all these stakeholders are represented under the following classification (NIST 2013), (Bohn, 2016) (Liu et al., 2011) (Jouini et al. 2012) (NIST 2012) (Cloud & Program , 2011):

- **Cloud Consumer:** The person or organization that uses the Cloud Computing services and uses the service that has been provided by a cloud provider.
- **Cloud Provider:** A cloud provider is the entity (a person or an organization) who is responsible for making a service available to the interested parties.
- **Cloud Carrier:** A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.
- **Cloud Broker:** A cloud consumer may request cloud services from a cloud broker, instead of direct contacting to cloud provider in case of the integration of cloud services that are too complex.

The following table 4-1 is proposing a variety of taxonomy of primary and secondary stakeholders. As presented in the definition, the primary one is abstract representation, and the secondary one is the refinement of this abstraction which is representing as a sub-factors that give a more clarity and accuracy estimation. This refinement process is recommended to offer more details about security guidelines.

Table 4-1: Abstract and multi-dimensional representation of cloud stakeholders (NIST 2011) (Liu et al. 2011)

Main Stakeholders (Abstract Representation)	Sub-classifications of Stakeholders (Multi-dimensional Model)
Cloud Consumer	- Organizations providing access
	- End users
	- Software application/system administrators
	- Application/system developers
	- Application/system testers
	- Application/system deployers
	- Application/system administrators
	- Application/system end users
	- System application administrators.
	- IT managers.
Cloud Provider	- Public cloud
	- Private cloud
	- Community cloud
	- Hybrid cloud
Cloud Broker	- Service Provision
	- Service Consumption
Cloud Carrier	- Cloud distribution
	- Cloud Access

4.3.2. Cloud Security requirements (NIST 2013):

Security requirements are defined as constraints on the system, these constraints lead to achieve the security goals which are represented as a subset of the most important quality sub-classification related to security (e.g., integrity and privacy). This study will deal with all technical aspects on security requirements on cloud computing, namely (NIST 2013), (NIST 2011) (Bodeau et al. 2010) (Rjaibi & Aissa 2013) (Marta & Calderon 2007) (NSA Information Assurance Service Center 2013):

- **Availability:** Cloud Computing system enables its users to access the system (e.g., applications, services) from anywhere at any time.
- **Confidentiality:** Confidentiality means keeping users' data secret in the Cloud systems.
- **Authorization:** It is concerned with legal compliance and user trust and decrease privacy risk and ensures legal compliance.
- **Data Integrity:** Data integrity in the Cloud system means to guard information integrity (i.e., not lost or modified by unauthorized users).
- **Authentication:** It is concerned with managing identities at cloud providers to have robust identity management architecture
- **Hardware-level security requirements:** are the configuration that the cloud system must have in order for a hardware or software application to run smoothly and

efficiently. Failure to meet these requirements can result in performance problems or installation problems.

The following table 4-2 presents the proposed basic taxonomy of the technical security requirements which is based on a variety of investigations; six security requirement criteria and their relative sub criteria has been considered (NIST 2011) (Liu et al., 2011), (Rjaibi & Aissa 2013), (Friedman & West 2010).

Table 4-2: Abstract and multi-dimensional representation of cloud security requirement

Main Security Requirement (Abstract Representation)	**Sub-classifications of Security Requirement (Multi-dimensional Model)**
R1: Confidentiality	- Traces
	- Cardinality
	- Consent and notification
	- Anonymity
	- Encryption
	- Confidentiality
	- Consistent collection
	- Use and disposition of disposition of Personal Information (PI)
	- Personally-identifiable information
	- Secure images
R2: Integrity	- Software Integrity
	- Personal Integrity
	- Data Integrity
R3: Availability	- Resource allocation
	- Expiration
	- Response time
	- Service availability
R4: Authentication	- Access control
	- User name, Password and certifications issues (local credentials) - Communication security
	- Active Directory Account (Active Directory credentials) – Communication security.

R5: Authorization	- Access control
	- Authorized access and disclosure
	- Privileges and fine grains aspects
	- Security in multitenant environment
Authentication, Authorization	Data security and protection from exposure (remnants)
	Application security
	Software security
R6: Hardware-level security requirements	- Hardware Integrity
	- Hardware security
	- Hardware reliability
	- Infrastructure control
	- Network protection
	- Network resources protection
	- Legal not abusive use of cloud computing

And accordingly when identifying cloud stakeholders and its security requirement, this will lead to introduce a new matrix which is called "Stake Matrix", this relation reflects to what extent each stakeholder stands to lose as a result of security failures, as shown on the following table 4-3.

Table 4-3: Building ST Matrix using a sub-classification of stakeholder with a sub-classification of security requirements

		R.1.					R.2.				…	Rn		NoR
	ST	1.	2.	3.	…	R.1.n	1.	2.	3.	…	R.2.n	…	R.n.n.	
H1	-													
	-		**Stakes that stakeholder Hi puts on meeting requirements Rj** *(loss that Hi exposed if Rj is not satisfied)*											
	…													
	H.1.n.													
	•													
	•													
	…													
	H2.n.													
H3	-													
	-													
	…													
	H.3.n.													
Hn	H.n.n													

4.3.3. Cloud Component/Architecture of Cloud Computing (SATW, 2012)

Service models describe what kind of services can be obtained from the cloud; Table 4-4 shows the six common components on a service classes of cloud computing. In this table there are two colors (G.Somasekhar 2013) (Brian et al. 2012) (NSA Information Assurance Service Center 2013) (Mishra et al. 2013) (Nahla Murtada 2013):

- White color: indicates the responsibility of the cloud consumer.
- Gray color: indicates the responsibility of the service provider.

Table 4-4: The Generic Components of Cloud Computing Service Model

Traditional IT	**IaaS**	**PaaS**	**SaaS**
- Applications	Applications	Applications	Applications
- Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
OS	OS	OS	OS
Hyper visor	Hyper visor	Hyper visor	Hyper visor
Infrastructure	Infrastructure	Infrastructure	Infrastructure

- **Applications:** The *special applications that are used by a cloud users*, this application is represented as (web browser, display and reporting, menu and navigation, users interface, access controls, and authentication …etc) which includes software applications targeted the end users or programs..
- **Runtime:** The *environment in which the application is executed*, this component represented as (the runtime library cloud management, the runtime library of the application's requisite functions, and asset Repositories and Registries).
- **Middleware:** Used for switching software for *communication* with other applications, databases and the operating system. The middleware layer represented as (database, libraries, and other communications tool…etc) that used for developing application software in the cloud computing environment.
- **OS:** The OS layer provides and *manages the system resources of the hardware* such as OS and drivers. Cloud provider allows one or multiple guest OS's to run virtualized on a single physical host. Here, cloud consumers have a full freedom to choose which OS to be hosted among all available OS's that could be supported by the cloud provider.

- **Hypervisor:** It is the virtualization layer that virtualizes infrastructure resources to the operating system. This layer represents as (virtual machines, virtual data storage, hardware virtualization, other computing resource abstractions, and abstract software's components), these software's have been used by the cloud providers to provide and manage *access to the physical resources through these software's.*
- **Infrastructure:** This layer represent as "*Physical resource layer"* which includes all the physical computing resources such as hardware resources (CPU, storage unit, and memory…etc) and networks and Internet connectivity component (servers, routers, firewalls, switches, network links and interfaces).

The following Table 4-5 presents the proposed basic taxonomy of cloud component with a ***sub-classification category*** which is based on classifying the main component of cloud computing. It is based on a variety of investigations; author studied 6 cloud component criteria and their relative sub criteria.

Table 4-5: Abstract and multi-dimensional representation of cloud Component

Main Component (Abstract Representation)	**Sub-classifications of Cloud Component (Multi-dimensional Model)**
Main component (Cn)	**Sub-components**
- Applications	- Communication component
	- Exception handling component
	- Alerting and Notification Component
	- Data Synchronization component
	- User Profile component
	- Web server component
- Runtime	- Execution runtime component
	- Libraries
	- Database component
	- Tools and execution resources
- Middleware	- Communicator component
	- Integrator component
	- Libraries
- OS	- Component for access controls.
	- C.4.2. Component for the logical separation
	- Component for security
	- Component for operation implementation

- Hyper visor (Boniface et al. 2010)	- Virtual Machine (VM)
	- Virtual Data Storage
	- Hardware virtualization
	- Abstract Software's Components
- Infrastructure (Computing resources)	- Networks and Internet connectivity component (Servers, switches, routers, load balancers…etc)
	- Computer Hardware components and physical resource (CPUs , Storage Devices and Processor units…etc)

And accordingly when identifying security requirements and cloud components, this will lead to introduce a new matrix which is called "Dependency Matrix", this relation reflects to what extent each component contributes to meet each security requirement, as shown in table 4-6.

Table 4-6: Building DP Matrix using Multi-dimensional aspects of cloud security requirements with cloud component

DP		C.1.					C.2.				…	Cn	NoC
		1.	2.	3.	…	C.1.n	1	2	…	C.2.n.	…	C.n.n.	
R1	-												
	-		*Probability that Requirement Ri is violated if component Cj is compromised*										
	…												
	R.1.n.												
R2	-												
	-												
	…												
	R2.n.												
R3	C.												
	D.												
	…												
	R.3.n.												
Rn	R.n.n												
NoR													

4.3.4. Top Threats on Cloud Computing (CSA 2016)

Similar to the earlier mentioned research artifacts, the "The Treacherous 12 - Cloud Computing Top Threats in 2016" report which is proposed by CSA (CSA 2016), this report play a radical role to provide organizational guideline with an up-to-date of cloud security concerns in order to make studied risk management decisions regarding cloud adoption strategies. This section will reflect the most common security threat which has been agreed among different security experts in CSA community who is concerned with the most significant security issues in the cloud. In this most recent edition of the threats in 2016, CSA experts create report that identified the most critical issues to cloud security, accordingly CSA experts identified the following 12 critical threat on cloud (ranked in order of criticality) (CSA 2013b), (CSA 2016), (Singh & Negi 2015) (Nahla Murtada 2016b):

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 Issues

The following part deals with the description of "The Treacherous 12 - Cloud Computing Top Threats in 2016" report, which has been identified by CSA:

- **Data breaches:**

A data breach is an incident in which *confidential, protected or sensitive internal information is seen/falls* into the hands of their competitors and been violated, *modified, viewed, stolen* or used by unauthorized individual to do so. Sometimes simply it's occurring due to:

- Human error.
- Application vulnerabilities.
- Poor security practices.

The main victim of data breach is the cloud consumer's information and this threat may involve any type of information that is not for public release such as personal health information, financial information, Personally Identifiable Information (PII) and trade secrets.

When cloud providers are well known, highly accessible and have a big amount of data, they will be an attractive target for attackers, so also cloud provider being victim here, however The Impact of a "Data Breach" can be minimized through deploying strong encryption mechanisms.

- **Insufficient Identity, Credential and Access Management:**

This threat can occur due to lack of scalable identity access management systems, fails to use multi-layers authentication, data is not encrypted periodically, weak password use and a lack of periodical automated rotation of cryptographic keys, insufficient identity can allow unauthorized access to (view, modify and delete data) which lead to catastrophic damage to organizations or end users.

- **Insecure Application Programming Interfaces (API):**

Insecure API threat means a set of APIs have materialized, which is relative to weak set of interfaces or APIs. This threat is usually targeting cloud computing providers and consumers who use that interface. To mitigate the probability of occurrence, this interface must have access control, secure authentication, encryption and activity monitoring mechanisms especially when third parties may exist.

- **System Vulnerabilities:**

When the program has bugs this will lead to be exploitable for attacks, and attackers can use these vulnerabilities to steal data, taking control of the system or disrupting the delivered service.

- **Account, Service and Traffic Hijacking:**

It is an attack method (such as phishing or reusing the password and unauthorized activity). This threat is another issue that cloud users need to consider. This threat is represented as man-in-the-middle attacks, and if the attackers can gain access to your system, they can make transactions to its data "instead of you", return false facts and redirect your clients to illegal sites, so the most affected security requirements in the event of security failures are: (confidentiality, integrity and availability). Cloud provider should look to prohibit the sharing of account among users and services, and also should provide strong authentication techniques.

- **Malicious Insiders:**

When malicious inside organization has access to everything (organization's network, system, or data), this malicious insiders *is intentionally causing damage* by exceeding or misusing that access which is negatively affected the confidentiality, integrity, or availability of the organization's information by adding, modifying or releasing organization's data.

- **Advanced Persistent Threats (APT):**

An advanced persistent threat (APT) is a network attack in which an unauthorized party gains access to a network and stays for a long period of time without being detected. The main goal of this threat is to *steal data rather than to cause damage* to the network or organization. APT attacks target organizations (such as defense ministry, manufacturing and the financial industry) that have high-value of information, such as military information and secret information in secrets trade.

- **Data Loss/Leakage:**

This threat occurred due to *deletion or alteration* of records *without a backup* of the original content or loss of an encoding key, it was described as the biggest disaster that affect on cloud computing, however

data stored in the cloud can be lost for reasons other than malicious attacks, it can happen either due to *natural disaster* such as a fire and earthquake, or an *accidental deletion* by the Cloud Service Provider (CSP) which may lead to lose customer's data because no good backup strategies has been made.

- **Insufficient Due Diligence:**

Actually, the risk of "Insufficient Due Diligence" is the only one risk that is not dedicated to security architecture and technology matters. In this type of threat, the consumer not know many details of the internal security procedures because it's not clearly define, so leaving customers with an unknown risk profile that means serious threats, it is relative to the provider trust. Security should always in the upper portion of the priority list. Code updates, security practices, vulnerability profiles and intrusion attempts – all these things should be known and considered from all cloud parties and without a complete understanding of the CSP environment, applications or services being pushed to the cloud, cloud consumers were be exploitable for these type of threat. Most needed requirement is: confidentiality, integrity and availability were always part of any service provided by internal IT and cloud consumers, all these requirements should be clearly defined through SLA with internal IT organization, however if this organization is not playing their role as required, and these requirement being un-satisfy, who is responsible in the event of failure?

- **Abuse and Nefarious Use of Cloud Computing:**

Providers offer *unlimited resources* (network bandwidth, memory, disk space and storage capacity…etc) to their customers, this may lead anyone (may be hacker) from anywhere immediately using cloud services. However, not everyone wants to use this power and resource for good. It is relatively weak registration. A simple example of this threat is the way to spread spam, attackers can expose a public cloud (as example) and find a way to *upload malware* to thousands of computers and use the power of the cloud infrastructure to attack other machine.

- **Denial of Service (DoS) :**

When the attacker attacks to *prevent users or stakeholders of a cloud service from being able to access their data or their applications*, so it relatively affect on availability aspects, it can be done by sending too many requests per a unitary period of time or consume huge amounts of system resources such as processor power, memory, disk space or network bandwidth.

Attackers can "Distribute a Denial-of-Service" (DDoS) attack which causes system slowdown and leaves all of the user's service confused and not responding.

- **Shared Technology Issues:**

Threat on cloud environment looks like traditional network but in cloud the main problematical issue is the shared resources. Cloud Service Providers (such as IaaS provider) delivered their services by sharing resources and infrastructures (e.g., CPU caches, GPUs, Storage media …etc) for different consumers that do not supported by strong isolation properties across stakeholders, so stakeholders here are vulnerable to attacks, this threat will occur when: the existence of weak isolation, re-deploying the platforms to multiple customers, or sharing the computing resource, this threat affect all delivery models (IaaS, PaaS and SaaS) which may lead to a compromise the entire service of cloud provider.

In case of multitenant in cloud computing when sharing memory and resources, the effect of all threats will be more, because too many users sharing the same resource and one threat may affect on different tenants.

- **Hardware attack:**

A hardware attack means any physical attempt to compose damage, investigate or alter of any physical resource or by composing the inner information of the platform, the attackers here can change the integration between these platforms. It is very likely that a hardware attack will cause permanent damage to any hardware and usually these types of damage cannot be exploited by the attacker in any meaningful way it's just for "injury", however sometimes this threat will be materialize due to natural disaster with un-intentional circumstances, it may simply being resulted due to human errors, vulnerabilities or poor security practices (Slezak 2008).

The following table 4-7 presenting the expansion aspects that has been proposed using a lot of threat models that propose an Internet Security Threat Report such as (STRIDE, CSA, NIST, ENISA, VERIZON, and Symantec), this new expansion is very powerful, because any one use the MFC model can use any of these proposed models based on his/her knowledge about the threat model standard. So one of the main contribution here is mapping the CSA threat model with the other most known threat models (Marinos & Sfakianakis 2012) (CSA 2016) (Yahya et al. 2015) (European Network and Information Security Agency (ENISA) 2016) (Marinos 2013) (Symantec 2015) (Symantec 2014) (Carlson & Petersburg 2011) (Shostack 2014).

Table 4-7: A Multi-dimensional aspects of Threats on Cloud Computing

Main Categorization (CSA 2016)	Sub-classification (e.g., STRIDE, NIST, ENISA, VERIZON, Symantec) (Yahya et al. 2015)
- Data Breaches	- Information Disclosure (I) - Privacy Breach or Data Leak - Impersonation or Fraud Activities - Failure of security access rights. - Failure systems for cloud data and backups - Privacy Breach
- Weak Identity, Credential and Access Management	- Spoofing Identity (S) - Tampering With Data (T) - Repudiation (R) - Information Disclosure (I) and Privacy Breach - Denial of Service (D) - Elevation of Privilege (E) - Modification of data at rest/transit. - Data Interruption (deletion) - Software Modification - Exposure in Network/Network attack - Defacement - Software Interruption (deletion) - Interception on access control

- Insecure APIs	- Interception on access control - Tampering With Data (T) - Repudiation (R) - Information Disclosure (I) - Elevation of Privilege (E)
- System and Application Vulnerabilities	- Spoofing Identity (S) - Tampering With Data (T) - Repudiation (R) - Information Disclosure (I) - Denial of Service (D) - Elevation of Privilege (E) - Session Hijacking - Exposure in Network/Network attack - Disrupting Communication
- Account Hijacking	- Spoofing Identity (S) - Tampering with data (T) - Repudiation (R) - Information Disclosure (I) - Denial of service (D) - Elevation of privilege - Session hijacking - Impersonation or fraud activities - Interception on access control

- Malicious Insiders o Malicious cloud provider user o Malicious cloud customer user o Malicious third party user (Supporting	- Spoofing identity (S) - Tampering with data (T) - Information Disclosure (I) and Privacy Breach - Exposure in network/network attack - Interception on access control
- Advanced Persistent Threats (APTs)	- Information Disclosure (I) - Elevation of privilege (E) - Spear-Phishing - Direct Hacking Systems - Delivering attack code through USB devices - Penetration through partner networks - Use of unsecured or third-party networks - Application & Interface Security attack - Attack on Infrastructure & Virtualization
- Data Loss/leakage	- Interception on access control - T8.2. Repudiation (R) - T8.3. Denial of Service (D)
- Insufficient Due Diligence	- Privacy Breach - Spoofing Identity (S) - Tampering With Data (T) - Repudiation (R) - Information Disclosure (I) - Denial of Service (D) - Elevation of Privilege (E) - Disrupting Communication - Interception on access control
- Abuse and Nefarious Use of Cloud Services	- Denial of Service (D) - DDOS - Disrupting Communication - Impersonation or Fraud Activities - Connection Flooding

- Denial of Service	- Denial of service (D) - DDOS - Traffic Flow Analysis - Exposure in Network/ Network Attack - Disrupting Communication - Connection Flooding - Interception on access control - Information Disclosure (I)
- Shared Technology Issues	- Elevation of Privilege (E) - Interception on access control
- Hardware attack	- Hardware Modification - Hardware Theft - Hardware Interruption - Misuse of Infrastructure

Accordingly the impact that security breach has on the proper operation of individual *components* of the architecture depending on which part of the system each *threat* targets; this will lead to introduce the new matrix which is called "Threat Impact Matrix" as shown in table 4-8.

Threat is represented by a vector of probabilities of occurrence in the event of security breakdowns per unit of time as shown in table 4-9, this vector is called "Threat Vector".

Table 4-8: Building TIM Matrix using Multi-dimensional aspects of cloud component with cloud threat

TIM		T.1.					T.2.				…	Tn	T n+1
		3	4	5	…	T.1.n.	1.	2.	…	T.2.n.	…	T.n.n.	
C1	6												
	7		*Probability that component Ci is compromised if threat Tj has materialized*										
	…												
	C.1.n.												
C2	8												
	9												
	…												
	C2.n.												
C3	-												
	-												
	…												
	C.3.n.												
Cn	C.n.n												
C n+1													

Table 4-9: Building TV vector using a sub-classification of a Top Threat on cloud component

TV		Probability
T1	13.	
	14.	
	15.	
	…	
	T.1.n	
T2	16.	*Probability that threat Th materializes during a unit of operational time (e.g. 1 hour)*
	17.	
	18.	
	…	
	T.2.n	
T3	19.	
	20.	
	21.	
	…	
	T.3.n	
	…	
Tn	T.n.n.	
NoT		*Probability that no threat materializes*

4.4. The Extraction of MFC Parameters with Cloud Computing Aspects

This chapter proposed the MFC metric that has been highly adapted with cloud computing aspects and obtaining reasonable results accordingly (these results will be shown in chapter 6) then MFC parameter has been extracted to obtain more precise and accurate results on cloud computing aspects, same criteria (that has been discussed in chapter 3) for structuring, filling and gaining the results can be applied here, so this new refinement model will give a new expansion to obtain more precise and accurate results, so using the: *abstraction model* being done by using the main classification of the MFC parameter on cloud computing, *the multi-dimensional model* being done by using the sub-classification of each MFC parameter (which needed much more entries to fill out and resulting more precise and accurate estimation), or *a hybrid model* by mixing these two models, your selection is based on your needs, goals, knowledge, accessible data and a size of your enterprise…etc, the following chapter will focus on building another dimension on cloud computing which gains to adapt the MFC parameter with all cloud service models by specifying it's associate stakeholders, requirements, components and threats because the impact and cost of failure is differs across these service models, so new critical and valuable expansion has been built which results in MFC vector from a "service model" point of view this new

expansion called a “Service Base Model”, the following table 4-10 will summarize all dimensions of the MFC which are represented as abstract representation (main classification of cloud computing) that give a comparable results across main stakeholders on cloud computing (the obtained results will be presented in chapter 6).

Table 4-10: Abstract Representation of the MFC Parameter with Cloud Computing Aspects

Cloud stakeholders (NIST 2013)	Security requirement (NIST 2013)	Cloud component (SATW, 2012)	Cloud threat (CSA 2013b), (CSA 2016), (Singh & Negi 2015)
Cloud provider	Authentication	Applications	Data Breaches
Cloud consumer	Authorization	Runtime	Weak Identity, Credential and Access Management
Cloud carrier	Confidentiality	Middleware	Insecure APIs
Cloud broker	Integrity	OS	System and Application Vulnerabilities
	Availability	Hyper visor	Account Hijacking
	Hardware-level security requirements	Infrastructure	Malicious Insiders
			Advanced Persistent Threats (APTs)
			Data Loss
			Insufficient Due Diligence
			Abuse and Nefarious Use of Cloud Services
			Denial of Service
			Shared Technology Issues
			Hardware Failure

After filling all MFC matrices of cloud computing, it can be easy to compute the MFC per unit of time for each cloud stakeholder either by using the abstract model (as shown in table 3-13 and table 4-11) or the multi-dimensional model with a much precise representation (as shown in table 4-12).

Table 4-11: The MFC vector when using the "Abstract Representation Model"

Main stakeholders	MFC $/hour
Cloud Consumer	
Cloud Provider	MFC per unit of time
Cloud Broker	MFC = ST. DP. TIM. TV
Cloud Carrier	

Table 4-12: The MFC vector when using the "Multi-dimensional Representation Model"

Main stakeholders	Sub-classification of cloud stakeholders	MFC $/hour
Cloud Consumer	Organizations providing access	
	End users	
	Software application/system administrators	
	Application/system developers	
	Application/system testers	
	Application/system deployers	MFC per unit of time
	Application/system administrators	MFC = ST. DP. TIM. TV
	Application/system end users	
	System application administrators.	
	IT managers.	
Cloud Provider	Public cloud	
	Private cloud	
	Community cloud	
	Hybrid cloud	
Cloud Broker	Service Provision	
	Service Consumption	
Cloud Carrier	Cloud distribution	
	Cloud Access	

Summary

Among the major concerns of software engineering, this study presents the topic of software security measure. So, all MFC parameters are useful to be considered in the early software specification and development process.

This chapter show all these parameters by representing the high level abstraction (by using an Abstract Model for the MFC) of the security architectural mechanism which is very useful for the SMEs, and for the presented security quality Sub-factors, M^2FC has been proposed for each MFC parameter here this new expansion is very powerful, useful and helpful specially for a large enterprise, so these proposed models are useful for all cloud companies regardless of their size, the main contribution here is to provide a generic model that serve all cloud companies.

Refined taxonomies of MFC parameters have been provided, which adapted to all system contexts and this would be done by referring to multiple proposed models from the literature to propose an aggregate

model and move away from the abstraction presentation to a multi-dimensional or expansion model of security concepts, and also the proposed composition enriched the MFC metric by making an expansion architecture that gives us more accurate and precise estimation.

The following chapter will focus on another dimension that adapt all MFC parameters (stakeholders, security requirements, conceptual architecture of cloud components and then threat vector) with all cloud service models (IaaS, PaaS and SaaS) which is represented as another powerful expansion model.

CHAPTER FIVE

ADAPTING MFC PARAMETERS ON ALL CLOUD SERVICE MODELS

5.1. Introduction

One of the big software engineering concerns is a topic of software security. Therefore, this study considers all the main relevant parameters of the MFC that deal with this aspect; this chapter will represent the main attribute in term of the high level of abstraction of the security architectural mechanism for all cloud service models. For the security Sub-classification, new expansion will be established, which is more relevant to "Cloud Computing Service Models", this refinement will result in better and more accurate estimation.

The main contribution in this chapter is proposing new model which is called a Service Based MFC Model (SBMFCM) which aims to produce another dimension of enriching and structuring the MFC metrics with much more relevant parameters of cloud computing. However, this new model needs experts who have great deal with cloud computing aspects with having a relevant and real data acquisition, because this model has much more details rather than the abstract model, accordingly, this research is presenting four innovative models that have been established: abstract, multi-dimensional, hybrid model and service based model which are useful to serve all cloud relevant sectors regardless of the size of the beneficiary sites. All these variety models are proposed with a keen eye on Systematic Literature Review to derive all the expected relevant aspects in each model to obtain much relevant and precise estimation results and to serve all types of beneficiary sites on cloud computing areas.

5.2. Cloud Service Models

An organization should consider what kinds of services can be provided to customers, these services can be seen as layers of computing, cloud service models consist of three main models (NIST 2014), (NIST 2013) (Khurana & Verma 2013):

- ***Infrastructure as a Service (IaaS):*** this model is presenting as a set of provisioning computational resources such as (processing, storage, networks, and other computing resources…etc), and here cloud consumer can deploy and run their software (e.g., operating systems and applications), or store and process their data (storage and processing resources) example for IaaS (Microsoft Azure, Google Compute Engine (GCE), Amazon Web Services (AWS)…etc).
- ***Platform as a Service (PaaS)***: PaaS is representing as a set of (programming languages, tools and services) which are designed for the PaaS stakeholders to make coding and deploying their applications quick and efficient. This stakeholder has a control over the deployment of applications but not on the cloud infrastructure, examples for PaaS (Windows Azure, Google Application Engine, AWS Elastic Beanstalk…etc).

- ***Software as a Service (SaaS)***: this model is designed for end users, they use the provider's applications that is running on a cloud infrastructure, this application delivered on the web through client's interface such as web based email, examples for SaaS (Salesforce.com, Google Apps, WebEx…etc).

The Cloud services are made available as "pay-as-you-go" where users pay only for the resources they actually needed, unlike traditional services, Moreover, the pricing for cloud services generally varies according to QoS component and requirements, and all cloud deployment models are based on "Utility Computing" aspects.

The following section focus on all MFC parameters (stakeholders, security requirements, architecture component's and then threat vector) that has been adapted for all Cloud Service Models: IaaS, PaaS, and SaaS.

5.2.1. Stakeholders on each Cloud Service Model:

This section will propose the basic expansion of cloud stakeholders. It is based on a variety of investigations; there are many stakeholders that contribute in cloud computing as general such as lawmakers and regulatory bodies nationally and internationally, software companies, communication companies and investors, all these stakeholders are represented under cloud service model classification (see table 5-1), the following section is concerned with recognizing those cloud stakeholders who stand to lose if security requirement violated (NIST 2012) (Nahla Murtada 2016a) (Nahla Murtada 2016b), (Liu et al. 2011) (Lee Badger etal. 2011).

5.2.1.1. IaaS stakeholders

On IaaS, stakeholder gets access to network accessible storage, network infrastructure components and virtual computers, such as firewalls, virtual storage which helps stakeholders to mitigate and reduce energy, cost, and space. The main **IaaS stakeholders (**who are costly affected in the event of security failure) are (NIST 2012):

- ***System administrators,*** who manage the VMs and the need to perform system administrator work (such as configuring an infrastructure for end users).
- ***IaaS providers,*** who constructed the operating system images and services, replicated storage, firewalls, monitoring, etc.

5.2.1.2. PaaS stakeholders

In PaaS, stakeholders get the use of the PaaS cloud provider's tools and execution resources to develop, test, deploy and administer their applications. In short, the stakeholders of PaaS (who are affected in the event of security failure) are (Boniface et al. 2010):

- ***Application developers**:* Those who designs and implement software applications.
- ***Application testers:*** Those who run applications in various testing environments.
- ***Application deployers:*** Those who are responsible for deploying, publishing and managing the possible conflicts appearing from multiple versions of application.
- ***Application administrators**:* Those who configure, monitor and tune application performance on a platform.
- ***Application end users**:* Those who subscribe in deploying the applications on a PaaS and access to applications is the same as using a SaaS cloud.
- ***PaaS providers**:* Those who maintains a set of development tools and a set of execution environments.

With PaaS, developers can:

- Build web applications without purchasing and installing any tools on their computer.
- Deploy those applications without any specialized systems administration skills.

5.2.1.3. SaaS stakeholders

On SaaS, stakeholders get the right to access applications on demand, and application data management such as backup and data sharing between stakeholders, these SaaS applications being accessible via a client's web interface. The main stakeholders of SaaS (who are affected in the event of security failure) are (Lee Badger, Tim Grance etal., 2012) (NIST 2012):

- ***Organizations*** providing their employees with access to typical software applications such as office productivity or email.
- ***End users*** who directly use software applications.
- ***Software application*** administrators who configure an application for end users.
- ***SaaS provider***: who ensure that the supplied software that it supplies is robust and tested.

Table 5-1: Cloud Stakeholders on each Service Model

Cloud stakeholders	
Type of service	**Associated stakeholders**
SaaS	Cloud Consumers - Organizations providing access - End users - Software application administrators
PaaS	- Application developers - Application testers - Application deployers - Application administrators - Application end users
IaaS	- System administrators - Expert end user - Technical user
IaaS, SaaS, PaaS	Cloud Provider - Private Cloud - Community Cloud - Public Cloud - Hybrid cloud
IaaS, SaaS, PaaS	Cloud Broker Cloud Carrier

5.2.2. Security Requirement on Each Cloud Service Model

The existing security measures that can be applied to the existing complex infrastructure and systems have been proven difficult, because of the variance that may exist between different security requirements needs (same requirements have different stakes and different requirements may have same stake), so our proposed model addresses the security requirements that have to be developed. Due to this complexity of these systems and their differentiating environments, these security requirements have been classified for each cloud service model (Prof. Sonika A. Chorey1 etal. 2016), (Macdermott, Áine, Shi, Qi, Merabti, Madjid, Kifayat 2014), (Singh & Negi 2015), (Nahla Murtada 2016a), (Nahla Murtada 2016b); table 5-2 identifies these classifications.

5.2.2.1. IaaS Security Requirement

This layer is represented as "*Physical Layer*" that is concerned with providing all cloud infrastructures needs which is presented as "IaaS security Requirement", namely:

- ***Hardware Security*:** cloud providers should provide an access to hardware and cloud computing infrastructure with strong protection mechanism that avoid compromising it by monitoring where, when, and how stakeholders are using these infrastructures.
- ***Hardware Reliability***: it means the ability of a hardware components to operate correctly over a specified period of time which differs from fault tolerance, meaning that there is an ability to continue operation in the event of failure conditions.
- ***Network Resources Protection:*** that means protecting computing resources (e.g., hardware and software) that are delivered as a service over a network.
- ***Infrastructure Control:*** it's designed to ensure that every application is used on its optimum capacity, so there is a great need to analyze and evaluate the upgrades of infrastructure which becomes relevant to deploy customized infrastructure management software; accordingly organizations meet their upcoming needs adoption in cloud computing environment.
- ***High Scalability and On Demand Provisioning Infrastructure***: (IaaS) service should provide scaling and on-demand hardware provisioning, this scaling is extending until the latest hardware resource is available in cloud.
- ***Sharing with Strong Isolation:*** Multiple customers (multi-tenancy) shared platform and infrastructure in order to gain price and performance advantages, so there is a need to use some isolation protect measures to avoid the resources interference.

5.2.2.2. PaaS Security Requirement

This layer represented as "*Virtual platform layer*" which help developers to deploy their software on a cloud infrastructure – the main security requirements on PaaS are (Beimborn et al. 2011):

- ***Access controls:*** in this layer cloud providers and cloud consumers should have a number of mechanisms and solutions of access control such as (management of user identities and application level configuration), cloud consumers alone cannot deny the possibility of an insider attack created by the service provider's, an access control policy has to be proposed for both cloud providers and consumers to prevent such attacks.
- ***Security for application:*** In this case the interfaces have to be properly developed using security techniques of web applications that have to be protected from diverse HTTP

requests, identity management and access control are very critical for cloud security in order to limit the access of data and applications from un-authorized users.

- ***Secure data image:*** On PaaS, data should be securely transfer to Public Cloud Server (PCS), so an extra security measure has been proposed such as the algorithms for Advanced Encryption Standard (AES) that has been proposed to increase the key level and using some portioning method which is used to divide the encrypted data and images in order to transfer into the public cloud server.
- ***Virtual cloud protection***: The typical protection strategy for provisioning physical resource in cloud which is heavily virtualized environment. This provisioning being highly automated process; however using virtual machines within the context of a cloud computing infrastructure introduce a lot of security threats with critical security challenges.
- ***High Availability:*** PaaS platforms should provide a runtime environment for developer's applications that have a failover and load balancing capabilities which guaranteed application availability in the event of application runtime breakdown.
- ***High Scalability:*** PaaS can scale and stretch applications across the hardware. Cloud providers should provide users with a feeling of infinite scalability without technical intervention for deployment and delivery.
- ***Sharing with Strong Isolation:*** Multiple customers (multi-tenancy) share a common platform in order to gain price and performance advantages and to run software, so there is a need to use some isolation protect measures to avoid a platform interference.

5.2.2.3. SaaS Security Requirement

This layer representing as "*Application layer*"– end client applies to a person or organization who subscribes to a service which is offered by a cloud provider who is responsible for its use – SaaS security requirements are:

- ***Security on access control:***

  Enable controls to be adaptive, based on the user's identity and group memberships, its very similar to access control on PaaS, however, greater responsibility rests with the cloud provider.
- ***Communication protection:*** All communication should be protected using protection measures such as encryption and key management, theses protections play critical role in cloud computing because services can be accessed from anywhere by any one.

- ***Software security:*** it means security measures that should be implemented to protect software against malicious attack so that the software continues to work correctly under such potential risks.
- ***Service availability:*** it means that the data can be accessed from anywhere at any time via different protocols.
- ***Delegation control:*** Delegation without risk profile will lead to additional risk which should be mitigated using appropriate security controls with a well defined SLA.
- ***Sharing with Strong isolation (Privacy in multitenant environment):***
  Multiple customers (multi-tenancy) share a common application, database and schema in order to gain price and performance advantages, so there is a need to use some isolation and protection measures to obtain the highest isolation between stakeholders.

Table 5-2: Cloud Security Requirement for each Cloud Service Model

Type of service	Associate-requirement
IaaS	- Hardware security - Hardware reliability - Infrastructure control - High Scalability - Sharing with Strong Isolation
PaaS	- Access controls: - Security for application - Secure data image - Virtual cloud protection - High Availability - High Scalability - Sharing with Strong Isolation
SaaS	- Security and access control - Communication protection - Software security - Service availability - Delegation control - Sharing with Strong isolation

After identifying stakeholders and its security requirements this will lead to introduce “ST Matrix” that aims to identify the stake that each stakeholder has in meeting each clause of the security requirements specification

5.2.3. Components on each Cloud Service Model

Cloud Computing represents a new computing model that proposes many demanding security issues at all cloud component levels (e.g., data, application, network, virtualization server, infrastructure, host, application, web servers…etc). Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential aspects for all cloud stakeholders as well, if any one of cloud service model's component is compromised this will lead to violate these essential requirements (Nahla Murtada 2016a) (Nahla Murtada 2016b), so the following sections will present the most important components that will directly affect security requirements in the event of failure for all cloud service models (IaaS, PaaS and SaaS) as shown in table 5-3.

5.2.3.1. IaaS Components

IaaS delivery model consists of several components that have been developed through past years by offering an interface to a pool of physical resources (CPUs, Storage Devices and Processor units …etc) and network resource (e.g., servers, load balancer, router …etc) (Dawoud et al. 2010), (Somasekhar 2013), so these IaaS components consist of the following:

- ***Utility computing components:*** Utility Computing is not a new concept; these components have been used for packaging the infrastructure resources (e.g. computation, bandwidth, storage…etc), these resources represented as "metered services" that has been delivered to cloud subscribers.
- ***Cloud Software:*** it joins the cloud software components together by using some integration tools, cloud software is either "Open Source" or "Commercial off the Shelf (COTS)" closed source, and usually these software components have been used to communicate with a hardware infrastructure.
- ***Network and Internet connectivity***: this component is used for handling workloads in a Network Components (e.g., Servers, switches, routers and Load balancers) and for maintaining the cloud infrastructure to reduce the latency and the damage of unpredicted disasters.
- ***Virtualization Server:*** Virtualization is a one of fundamental technology platform for Cloud Computing services which facilitates sharing of multiple OSs and stand alone systems into a single hardware platform which will be done by the resources virtualization with a configurable resource size to a running virtual machine.

- ***Computer hardware and physical storage***: IaaS offers an interface to *a pool of distributed physical resources* (e.g., Storage media, CPUs, processor and ram) and delivers a shared business model to serve multiple consumers.

5.2.3.2. PaaS Components

PaaS cloud provides a toolkit that may be used to help multiple subscribers for developing, deploying, and administering their software application; it refers to the almost needed software (e.g., Oracle and other commercial development tool) that may need to buy a license to use it, accordingly the main PaaS component are (Jackson et al. 2012), (Beimborn et al. 2011), (Walraven et al. 2015), (Standards & Council 2016):

- ***Database components:*** PaaS Provides "Database Query Languages" for querying the relational database which are used as a backend component.
- ***Web server components:*** PaaS offers web server functionality by returning a configured resource (web content and images…etc) which involve retrieval of data from files, databases, HTTP-services in response to an HTTP request that may be used to handle requests for multiple subscribers.
- ***Development tools component:*** PaaS provides a development environment and provide an entire solution stack that can be used to build, test, deploy and manage the developer's code in the cloud (based on their needs).
- ***Runtime software execution stack:*** It refers to all runtime components that may be used to guarantee running the application in a more stable manner.
- ***Component for all OS capabilities:*** that serves as the development, service hosting, service management environment, parameters and all capabilities that are used to link and communicate between applications components with OS.
- ***Middleware components:*** a middleware component is a platform component that is used for developing and operating multi-tenant SaaS applications in a multi-PaaS environment. It enables the SaaS provider to have fine-grained privileges controls over the storage of application data and execution of applications which is offering some degrees of customization and self-service for the tenants. The middleware dynamically decides which requests and tasks are executed in a particular part of the multi-PaaS environment.
- ***Deployment tool***: PaaS offerings facilitate deployment of applications without the cost and complexity of buying the commercial license and managing the underlying hardware and software with provisioning hosting capabilities.

5.2.3.3. SaaS Components

SaaS uses an approach in which the software is already deployed as a host service and is accessed via the internet, by providing a rental convenient computing resources, these resource must be measurable in units that can be individually allocated to specific stakeholders, so this chapter focuses on these type of measure – how much each stakeholders suffer from failure in cost context, again many essentials requirement has been negatively affected in the event of such components compromised (e.g., presentation, security, application components…etc) On SaaS service model the main components here that should be considered are (Somasekhar 2013), (Meenakshi 2012) (Singh & Negi 2015):

- ***Presentation Component***: it's responsible of displaying, reporting, profiling, monitoring items, which include (menu and navigation, user control, display and reporting), this component has been represented as "Front End" component.
- ***Security Component***: this component responsible of all issues of security including authentication, authorization, encryption, regulatory and access control.
- ***Application Component***: it is the most important component on SaaS where it is responsible for the task monitoring, configuration, backup and all other provisioning control such as (exception handling, messaging, data Synchronization, metadata service, user profile and notification …etc).
- ***Operation Component***: this component is presenting as "Metering Indicators" for operating backups and restore, provisioning, monitoring and alerting, configuration and customization performance and availability, "Metering Indicators": this indicator has been documented in (SLA) which concern tracking and reporting aspects, such as mean time to respond to and fix problems, usage period, availability and another number of failures.
- ***Infrastructure Component* (*Backend Layer*)**: it is a component that is responsible to communicate with Platform and Infrastructure as a Service, it's also a part of the SaaS architecture where different issues are needed to handle for SaaS such as communication bandwidth, databases, the computers' hardware and networking, accordingly, the following table 5-3 identifies the most important component for all service models.

Table 5-3 : Cloud Component for each service model

Type of service	Associate-Components
IaaS	- Utility computing components - Cloud Software - Network and Internet connectivity - Virtualisation server
PaaS	- Database component - Webserver component - Development tools - Runtime software execution stack - Component for all OS capabilities. - Middleware components - Deployment tool.
SaaS	- Presentation component (Front end Layer) - Security component - Application component - Operation component - Infrastructure component (Backend Layer)

So when identifying the most violated security requirements in the event of compromising the component, this will lead to introduce a “Dependency Matrix”, this relation reflects to what extent that each component contributes to meet each security requirement.

5.2.4. Top Threats on each Cloud Service Model in 2016

Cloud computing offers an innovative business model for all cloud enterprises to serve IT services without a huge capital on hardware and software and sometimes with no need to have some technical knowledge. One of the big innovative issues specially in cloud computing is”Sharing Resources” concepts that drastically reduce purchasing cost, however it is creating new challenge and risks on what and how strategies should be used to support the full isolation between all users, so as shown in table 5-2 that all cloud service models consider this as one of the main requirement. With the extreme growth of cloud usage that is increased in number of stakeholders and cloud based applications probability of threats occurrence is also increased rapidly. This section will present the most critical threat for each cloud service model which is represented as a sub-set of “The Treacherous 12 - Cloud Computing Top Threats in 2016”, according to (CSA 2016) (Singh & Negi 2015) (Dawoud et al. 2010) (Marinos & Sfakianakis 2012) (Nahla Murtada 2016a) (Nahla Murtada 2016b) (Shostack 2014) (Marinos & Sfakianakis 2012) (Symantec 2015) the most relevant threats on each service model has been determined (as shown in table 5-4).

5.2.4.1. IaaS Threat

Threat on IaaS: IaaS should deliver computer infrastructure (such as a platform virtualization environment, storage, and networking). Instead of purchasing hardware, or network equipment, users can rent these resources based on the amount of resources consumed. Usually the cloud provider and cloud broker allow installing a virtual server on their IT infrastructure; however this infrastructure has been shared across different stakeholders who lead to increase the probability of failure occurrence and increase the number of affected sectors. Cloud provider manages all infrastructure components (e.g., virtualization, servers, hard drives, storage, and networking) and installs any required platforms, cloud consumers is responsible for updating these if new versions that are released, accordingly IaaS should deal with a lot of threat, namely:

- Hardware theft.
- Hardware modification.
- Hardware interruption.
- Network attack.
- Connection floodin.
- Distributed Denial of Service (DDOS).
- Misuse of infrastructure.
- Storage devices attack.
- VMs provisioning and migration.

5.2.4.2. PaaS Threat

PAAS is the most complex layer of the three models because it's a middle layer which have two communication channels (one channel for SaaS and another one for IaaS layer), PaaS should deliver computational resources through a platform which is needed by developers who gain with PaaS framework, they can build their application based on existing developed or customized applications and also PaaS can made testing and deploying applications quickly, simply, and cost-effectively, and can easily eliminate the useless software components based on their users needs. PaaS includes a lot of components that may compromise in the event of threat materialized. These components are: runtimes component (like java runtimes), Databases (like mySql, Oracle), Web Servers (tomcat etc), and most of Subject Matter Experts (SMEs) investigated that the most frequent threats on this PaaS service model are:

- Exposure in network/network attack.
- Session hijacking.
- Software modification.

- Traffic flow analysis.
- Disrupting communication.
- Software interruption or deletion.
- DDOS.
- Impersonation.

5.2.4.3. SaaS Threat

SAAS are probably the most popular form of cloud computing and are easy to use by everyone by using the Web to deliver applications, which are managed by a cloud provider or third-party vendor whose interface is accessed on the clients' side. Most SaaS applications can be run directly from a Web browser, with no need to download some components or tools and here everything (applications, runtime, data, middleware, O/S, virtualization, servers, storage, and networking) should be managed by cloud vendors. Gmail is one famous vendor of SaaS. This layer is on top of PaaS, which includes applications like email (Gmail, Yahoo mail etc), Social Networking sites (Facebook, Twitter…etc) which faced a lot of threats, namely:

- Privacy Breach.
- Traffic Flow Analysis.
- Exposure in network/network attack.
- Session Hijacking.
- Data Interruption (deletion).
- Impersonation.
- Modification of data at rest/transit.
- Application and Interface Security attack.
- Interception on Access Control.

Accordingly, the following table 5-4 identifies the top threats on Cloud Computing for each service model and each of these threats are a subset of "The Treacherous 12 - Cloud Computing Top Threats in 2016" that has been proposed by CSA.

Table 5-4: Cloud Threats for Each Service Model

Type of service	Associated Threats
IaaS	- Hardware Theft - Hardware Modification - Hardware Interruption - Network Attack - Connection Floodin - DDOS - Misuse of Infrastructure - Storage Devices Attack - VMs Provisioning and Migration.
- PaaS	- Exposure in Network/Network attack - Session Hijacking - Software Modification - Traffic Flow Analysis - Disrupting Communication - Software Interruption or Deletion - DDOS - Impersonation
- SaaS	- Privacy Breach - Traffic Flow Analysis - Exposure in Network/Network attack - Session Hijacking - Data Interruption (deletion) - Impersonation - Modification of Data at transit. - Application and Interface Security attack - Interception on access control

Accordingly when identifying the most compromised component in the event of threat materialized, this will lead to introduce an "Threat Impact Matrix", this relation reflects the probability that specific component has been compromised given that specific threat has been materialized.

In addition, TV has been created by considering the probabilities of all these threats per unit of time.

So the following table 5-5 summarize all MFC parameters (Stakeholders, Requirements, Components and Threats) on each cloud Service Model (IaaS, PaaS and SaaS), accordingly, ST Matrix Combine between the stakeholders of (IaaS, PaaS and SaaS) and the security requirement of (IaaS, PaaS and

SaaS) each stakeholder will pay more for their associated requirements (which exist on same service model), DP matrix will combine between security requirements and cloud components (for all service models) this matrix reflect the probability of requirement violation given that a component has been compromised, so the probability of this requirement will be higher when intersect with associated component (that exist on the same service model). For the remaining service model probability will be less, same thing for TIM and filling TV is based on number of incidents of each threat on each service model.

Table 5-5: MFC Parameters on each Cloud Service Model

Type of service	Stakeholders	Security requirement	Components/ Architecture	Threat
IaaS	- System administrators - Expert end user - Technical user - IaaS Provider - IaaS Broker - IaaS Carrier	- Hardware security - Hardware reliability - Infrastructure control - Sharing with Strong isolation	- Utility computing components - Cloud integration Software - Network and Internet connectivity - Virtualisation server	- Hardware Theft - Hardware Modification - Hardware Interruption - Network Attack - Connection Floodin - DDOS - Misuse of Infrastructure - Storage Devices Attack - VMs Provisioning and Migration
PaaS	- Application developers - Application testers - Application deployers - Application administrators - Application end users - PaaS Provider - PaaS Broker - PaaS Carrier	- Access controls - Security for application - Secure data image - Virtual cloud protection - Sharing with Strong isolation	- Database component - Webserver component - Development tools - Runtime software execution stack - Component for all OS capabilities. - Middleware components - Deployment tool.	- Exposure in network/network attack - Session Hijacking - Software Modification - Traffic Flow Analysis - Disrupting communication - Software Interruption or Deletion - DDOS - Impersonation

SaaS	- Cloud Consumers - Organizations providing access - End users - Software application administrators - SaaS Provider - SaaS Broker - SaaS Carrier	- Security and access control - Communication protection - Software security - Service availability - Secure Delegation - Sharing with Strong isolation	- Presentation component - Security component - Application component - Operation component - Infrastructure component (Backend Layer)	- - - - - - - - -

5.2.5. Structuring the MFC Metrics

The MFC is a quantitative function that measures failure cost "per unit of time" for each stakeholder, the mean variable represents the loss for each stakeholder stand to lose as a result of possible security failure. When the cause of system failure being considered is security breaches, the MFC can be used to quantify this loss (that are resulting from these type of security violations) on security requirements, such as confidentiality, integrity, and availability…etc and this would be done by considering all MFC parameters (stakeholders, security requirements, components and threats), our contribution is to provide a flexible and elastic structured model, namely (Nahla Murtada 2016b), (Murtada 2013) – (as shown in figure 5-1):

- The first model is called the "Abstract Model of the MFC": It is a generic model, this model building, composing and structuring the metrics based on identifying the main dimension (only) of all MFC parameter in cloud computing as general, which were presented in chapter 4; this model is very powerful for SMEs and individuals investors.
- The second Model is called a "Multi-dimensional Model of the MFC" (M^2FC): this model is concerned with building, composing and structuring the metrics which is based on identifying the sub-classification of all MFC parameter, this model is better when need a much better, precise, meaningful and innovative estimation, this model represented as an expansion model from the abstract model, it may be better for a bigger enterprise because it contain much more details (refer to chapter 4).
- The third Model is called a "Service Based MFC Model" (SBMFCM): this model is concerned with building, composing and structuring the metrics which is based on identifying the MFC parameters for all Cloud Service Model separately, this new expansion is very powerful with cloud stakeholders to build the MFC metrics based on the relevant attribute of each model, and also gives more precise, meaningful and innovative estimation than the generic model (which is represented on this chapter).
- The fourth Model is called a "Hybrid Model of the MFC": this model building, composing and structuring the metrics based on mixing any two models from the previous one, this model is very powerful when you need to build your own model based on your own data, needs and knowledge, for example: when you need to build "Stake Matrix" you can select the security requirement (in the row) form the comprehensive model and selecting stakeholders (in the column) from the service based model.

By proposing these new expansions many professionals can use any of the proposed model based on their enterprise size, needs, goals, knowledge…etc, and the structure of this model is very flexible and elastic.

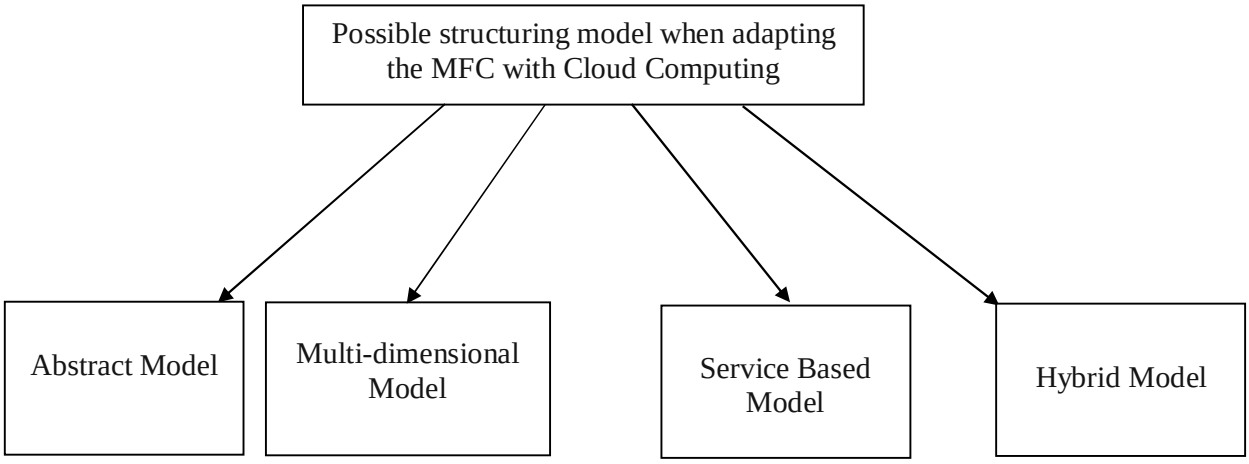


Figure 5-1: Proposed Models for Structuring and Filling the MFC Matrices

5.2.6. Advantages of Structuring and Re-structuring The MFC Matrices

Due to the lack of a clear taxonomy of cloud stakeholders, security requirements, cloud components and cloud threat the new basic taxonomies forms a unified model of security concepts; therefore it is useful in many directives (Nahla Murtada 2016a):

- Creating an orthogonal decomposition of MFC parameter and sub factors.
- Empirical data can be used to obtain more realistic and precise results because its values are near to the reality and useful in practice (as shown in chapter 6) the obtained data is that data that has been adapted with an abstract model.
- Reducing the redundancy of values on each matrix.
- User can create his own model by mixing any two of the proposed models.
- Easy to map all threat classifications to CSA classification.
- Deep understanding of all main classification with its all dimensions.
- Solve the terms ontology problem.
- All refine expansion models give more precise and accurate estimation.
- Evaluation for any of these models can be done by applying V&V measures using the same economical base approach such as ROI and NPV because output of all of these models is MFC vector (chapter 6 will present this concern).
- The proposed models can be verified by using an empirical observation.
- The proposed models can be validated using a supportive automated tool.

5.2.7. Generate and Fill MFC Matrices using Service Base Model

This new expansion for creating MFC has been adapted with all cloud service models and here there are two aspects for generating and filling the MFC matrices using the "Service Base Model" either by considering (as shown in figure 5-4):

- *The position of security failure*: In our case it's looks like the failure aspects on traditional system that assume:
    - The impact of security failure on infrastructure layer (IaaS) is higher than being on a middleware component or application layer and
    - The impact of security failure on a middleware layer (PaaS) is higher than being on a software or application layer.
    - The impact of security failure on application layer (SaaS) is less than being on a middleware or infrastructure, or
- *The scope of control aspects*: whenever the scope of responsibility is bigger the probability of a security failure will also be higher, this new classification is based on NIST classification which is proposed the scope of control for each service model.

In the beginning, any of these two aspects follow the same criteria for calculating and evaluating the MFC result and each of them used the 2^{ed} level No., the only difference: on the first aspect (*The position of security failure*), assigning 2^{ed} level No here is based on identifying the criticality of failure across the different service models (by answering the question: "which service model will be highly affected in the event of security failure?") in the proposed case whenever we go deeper the impact of failure will be increased, defining criticality here is based on professionals opinions and knowledge and its matrices deal with service model (in rows and columns) only, on the second aspect (*The scope of control aspects*) the 2^{ed} level No. is used to determine the criticality based on the scope of control (whenever scope being bigger the impact of failure will be higher) the criticality here is defined based on NIST scope of control classification and it's matrices combined between cloud service model with the generic cloud aspects, so the criteria for assigning the 2^{ed} level No. is differ across these two aspects, all of these details will be presented in the next sections.

5.2.7.1. Generate and Fill the MFC Matrices based on the "Position of Failure" aspect

To generate and fill these MFC matrices let's assume there are a lot of cloud providers, filling the ST Matrix and TV vector looks like the previously assigned approach (which presented in chapter 4), and for the DP and TIM consider the following scenario:

Figure 5-2 has two entries (in the first two boxes): "*The First Box"* is used to represent the 1st level number "based on the impact of each requirement failure given that component has been compromised", 1st level in tables (table 5-6 and table 5-7) are used for filling each small cell based on the original approach of generating and filling DP, same thing for the TIM – which were previously proposed in chapter 4, this study assuming that only one event occurs at a time, that means for each unit of time focus on a column on each cell, however *"The Second box"* is used to identify the criticality of failure on each service model (as shown in table 5-6), for example if the requirement has been violated on (IaaS) service model that means IaaS component is the most affected layer, then PaaS and then SaaS, so the intersection between IaaS requirement (IaaS req.) with IaaS Component (IaaS Comp.) will take the highest 2ed level No. and with SaaS will take the lowest 2ed level No (so table 5-7 is focus On IaaS column only same thing will be done for the remaining columns) and same thing will be done for TIM. Moreover, this study assuming that only one service model has been failed at a time, which means just focus on a specific service model for each unit of time which represented as a bigger cell (IaaS, PaaS or SaaS column), this category is useful when comparing the impact of failure between service models, and on the third box results have been calculated, accordingly: on the second box, when the 2ed Level No equal:

"0": means no impact, "1": lowest impact, "2": medium impact and "3": means highest impact.

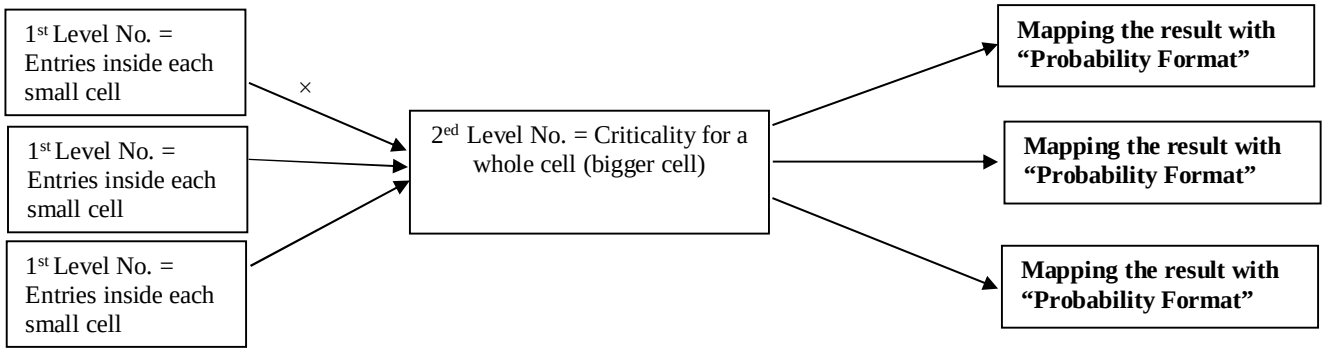


Figure 5-2: Position of where assigning 1st level and 2ed level on a "Service Base Model"

Table 5-6: Assigning 1st Level No. and 2ed Level No. on a "Service Base Model"

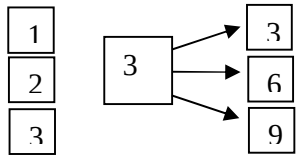
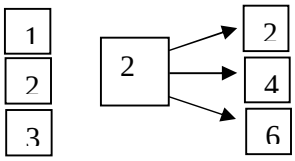
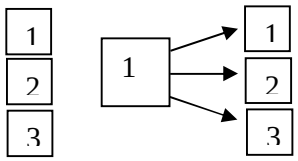
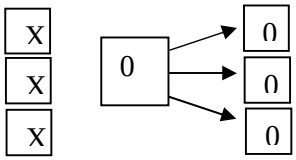
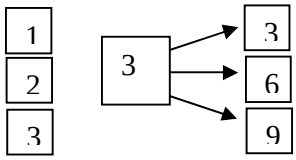
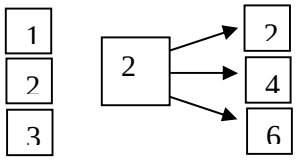
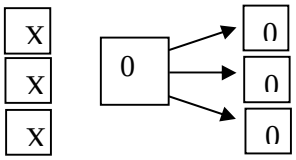
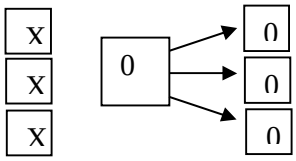
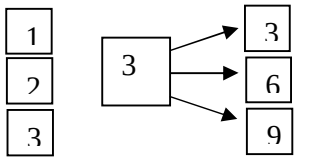
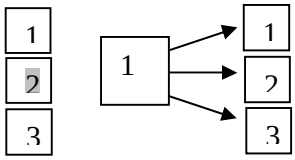
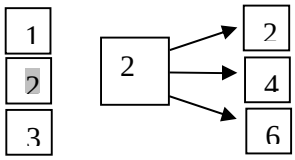
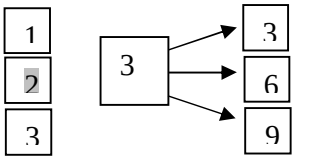
DP	SaaS Comp.	PaaS Comp.	IaaS Comp.
SaaS Req.			
PaaS Req.			
IaaS Req.			 3*1=3 & 3*2=6 & 3*3=9

Table 5-7: IaaS Column's description

	IaaS	Meaning	Description
SaaS		1*1= 1 **2***1= 2 3*1= 3	SaaS take the lowest impact (*second box*) which is lower than PaaS and lower than IaaS, so it takes 2ed level No.=1
PaaS		1*2= 2 **2***2= 4 3*2= 6	PaaS take the medium impact (*second box*) which is higher than SaaS and lower than IaaS, so it takes 2ed level No.=2
IaaS	 3*1=3 & 3*2=6 & 3*3=9	1*3=3 **2***3=6 3*3=9	Here IaaS take the highest impact (*Second box*) when comparing with SaaS and PaaS, so it takes 2ed level No.=3.

Same 1st Level on all service models (in the *first box* with gray color) resulting different probability because the criticality of failure (2ed level) is differ across these service models (*which represent on the second box)*, for example criticality of failure (2ed level) on SaaS is less than PaaS, so SaaS take 2ed level No. =1 and PaaS take 2ed level No.=2), same thing with IaaS.

In this model assuming that one service model fails at a time. Let's focus on the third column, (IaaS Comp. intersect with SaaS, PaaS and IaaS req.) to explain application of this model and same thing will be done for all remaining columns.

Let's assume the professional experts on cloud domain consider the following scenario (as shown in figure 5-3):

- If the failure in on IaaS layer, that means:
    - IaaS take the highest impact (2ed Level = 3) and
    - PaaS take the lower impact than the IaaS (2ed Level = 2)
    - SaaS take the lower impact than the PaaS and IaaS (2ed Level = 1)

- If the failure is on PaaS layer, that means:
    - PaaS take the highest impact (2edLevel = 3) ,
    - SaaS take the lower impact than the PaaS (2ed Level = 1) and
    - IaaS was not affected (2ed Level 0).

- If the failure is on SaaS layer, that means:
    - SaaS take the highest impact (2ed Level = 3) and
    - PaaS and IaaS were not affected (2ed Level = 0).

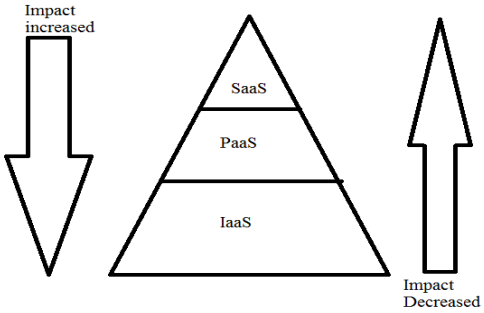


Figure 5-3: The Gradual Impact of Failure as in "Traditional System"

As shown in table 5-8, the 2ed level No column used to determine the criticality of a failure on specified service model, the value of the "2ed Level. No." can be re-adjusted if needed, so for example if the "2ed Level. No.=1" this values can be changed by (0, 2 or 3), any change you made will keep the summation of any column being "1", (even if there is no impact or 2ed level No = 0 in any cell) so:

- If you don't like to consider the criticality of security failures between cloud service models you can give the same value by using same 2ed level No., or
- If Two cells have the same criticality you can put same value for them and assign different value for the third cell…etc, so when tried to do all possibilities, the final result keep the summation with "1".

5.2.7.2. Generate and Fill the MFC Matrices based on the "Scope of Control" Classification

Cloud Service Models describe what kind of services can be obtained from the cloud, table A-6 shows the six common components of cloud computing. In this table there are two colors (G.Somasekhar 2013) (Brian et al. 2012) (NSA Information Assurance Service Center 2013) , refer to table 5-8:

- White color: indicates the responsibility of the cloud consumer (the one who use the service).
- Gray color: indicates the responsibility of the service provider (the one who manage the service).

Table 5-8: The Generic Components of Cloud Computing Service Model responsibilities

Traditional IT	**IaaS**	**PaaS**	**SaaS**
Applications	Applications	Applications	Applications
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
OS	OS	OS	OS
Hyper visor	Hyper visor	Hyper visor	Hyper visor
Infrastructure	Infrastructure	Infrastructure	Infrastructure

The Application Layer: this layer includes software applications which targeted and end users. These applications are ***used by*** SaaS consumers and installed, maintained and ***managed by*** PaaS consumers, IaaS consumers and SaaS providers.

The Middleware Layer: this layer aim to provide software building blocks (e.g., libraries, database, and Java virtual machine…etc) for developing application software on cloud computing environment.

This layer is ***used by*** PaaS consumers and installed, maintained and ***managed by*** IaaS consumers or PaaS providers, or SaaS provider; this layer is ***hidden*** from SaaS consumers.

The OS Layer: This layer includes OS and drivers. An IaaS cloud allows one or multiple Operating Systems to run virtualized on a single physical host, which are shared across cloud stakeholders. Generally, cloud consumers have broad freedom to choose which OS to be hosted among all the possible Operating Systems, which supported by the cloud provider. The IaaS consumers have a full responsibility for that chosen OS, while the IaaS provider controls the host OS, The OS is ***used by*** IaaS consumer, and installed, maintained and ***managed by*** PaaS provider, SaaS provider or IaaS provider, this layer is ***hidden*** from SaaS consumers and PaaS consumers , assigning 1st levels No. looks like the first approach for assigning it (here it is applied for each service model) this 2ed levels No. are used as shown in figure 5-2, and here the 2ed levels No. is used for representing the scope of control aspects as shown on the following:

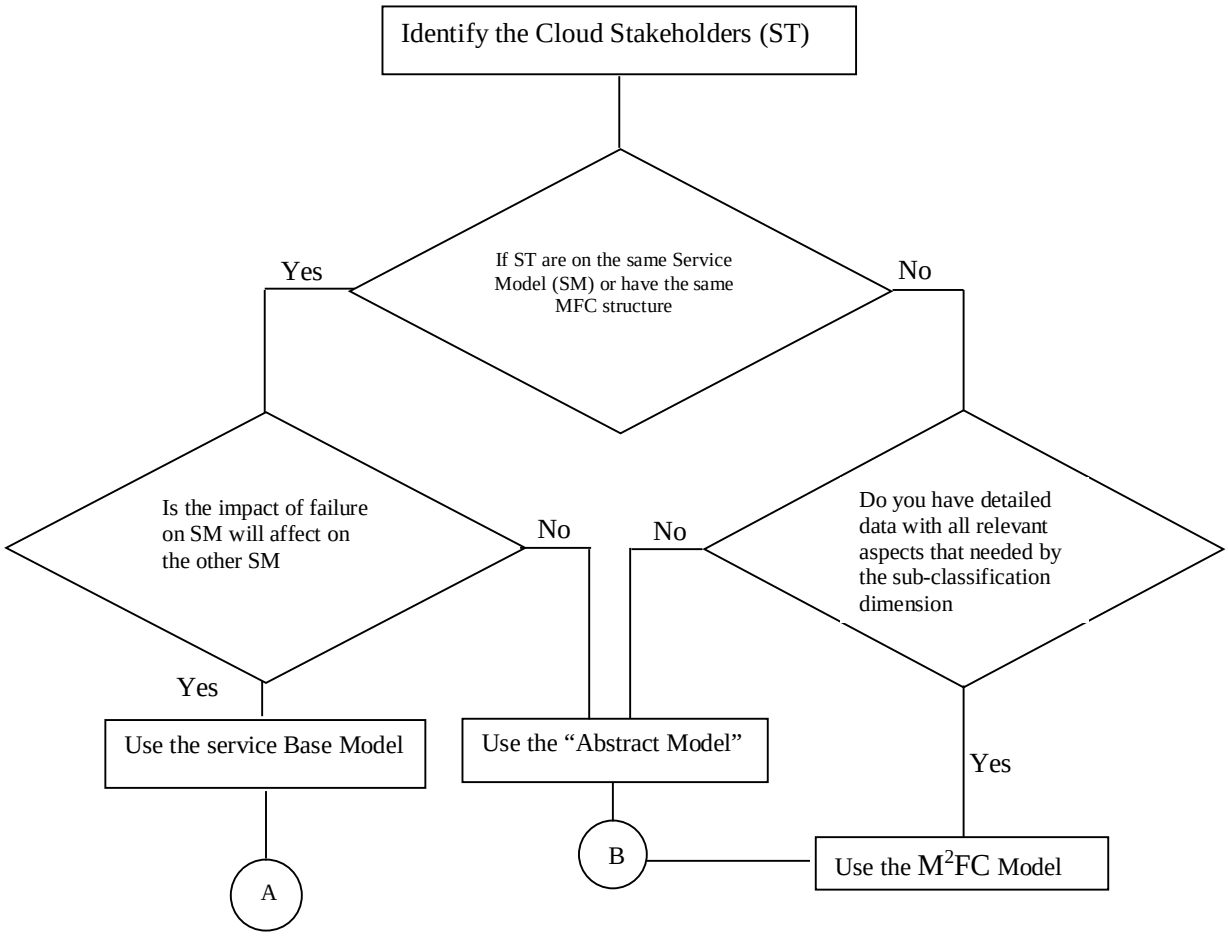
- 2ed Level L2=***2*** (=2): This level means some components are ***managed by*** some stakeholders (the site who provide the service), so the *highest* impact of failure will exist here.
- 2ed Level L1=***1*** (=1): This level means some components are ***used by*** some stakeholders (The site who consume the service), so the impact of failure here is *less* than Level 2.
- 2ed Level L0=***0*** (=0): This level means some components are ***hidden*** from some stakeholders (as example, the middleware layer is hidden from SaaS Consumer) which means "No Impact" and lead 2ed Level=0.

SBMFCM is useful when we have different stakeholders from different service models and the failure on a service model affect on the other service model, however if the:

- *Stakeholder are from the same service model* (here we just consider the abstract model by using the associated MFC parameter on each cloud service model and obtain only one MFC vector for each stakeholder that are on the same service model – as shown in table 5-5) or
- If *failure on some service model will not affect the other service model* (here we build the MFC metrics for each stakeholders that are on the same service model, accordingly for each service model we have an associated MFC vector, this will be done by considering the mentioned MFC parameters on each service model (as shown in table 5-5)

In these two cases we don't consider the different criticality factors across cloud service models, so here the "abstract model" is most the appropriate model for these two cases).

5.2.8. Flowchart for adapting the MFC with Cloud Computing



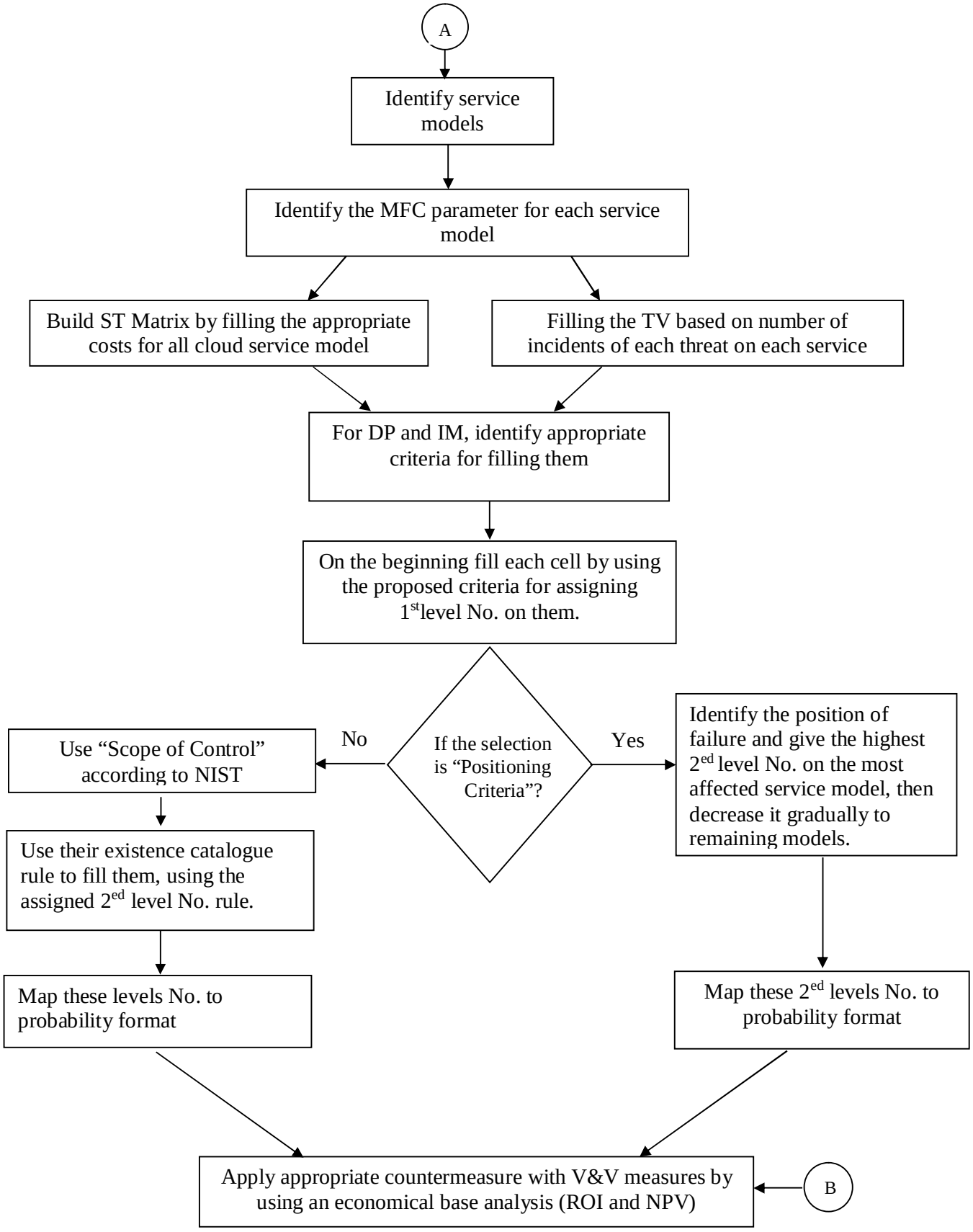


Figure 5-4: Flowchart for Presenting when to use each model for Structuring and Filling the MFC Metrics that has been adapted with Cloud computing

Summary

The essential characteristics and advantages of cloud computing encourage to work in a cloud environment, however all these characteristics are affected by security threats in all cloud service models. This chapter focused on all MFC parameters (stakeholders, component, security requirement and corresponding threats) for all Cloud Service Model (IaaS, PaaS and SaaS) and the output from this chapter is MFC vectors that have been adapted with all cloud computing aspects, the output from all proposed models is the MFC vector per unit of time for each stakeholders, MFC metric has been evaluated using V&V measures in term of economic base analysis such as ROI and NPV, chapter 6 will represent one of these models with its metrics, then will show how can the selected model be verified using V&V measures, chapter 4 and this chapter referred to the propose multiple models from the Systematic Literature Review to drive new refined models. With the recent drastic growth in cloud environment, there is also increase in a number of cloud consumers, cloud service providers and cloud based applications and accordingly, the number of threats and incidents is also growing rapidly which lead to lose a huge amount of money, time, effort and reputation…etc and also the probability and impact of these threat are increased, so a lot of models should be proposed to serve variants cloud experts for structuring the MFC metric and filling their matrices, Our contribution is to provide a basic and refined models which deal with all of these aspects considering all the variance that may exist between different cloud (stakeholders, security requirement, components and threats) which is not exist in the most of security metrics, this new expansion resulting more accurate and precise estimation because of its relevance to all cloud computing aspects with their service models.

CHAPTER SIX

MFC APPLICATION ON CLOUD COMPUTING, RESULTS, EVALUATION AND RECOMMENDATION

6.1. Introduction

This chapter will present the MFC Application with Cloud Computing Aspects and resulting data after applying some appropriate countermeasures in terms of reduced MFC (MFC gain) then evaluating the model using some econometric approaches such as ROI and NPV to estimate the efficiency of these countermeasures in term of investment cost, which should be used to enhance the cloud environment in term of controlling the MFC metrics.

Cloud Computing has simultaneously transformed from buying infrastructure equipments to rent these infrastructure for a business, and faced new security challenges and now deliver business-supporting technology more efficiently than ever before and this will be done by developing the cloud service model by using an appropriate countermeasures (which will be shown later) and each measure is used for controlling specific matrix, so on 2016 CSA proposed the recent "Security Guidance for Critical Areas in Cloud Computing" and the "Security as a Service Implementation Guidance", these guidance have quickly become the industry-standard catalogue of best practices for cloud companies which are used to reduce threat probability on cloud computing, the purpose of these guidelines are also providing organizations with an up-to-date and expert-informed understanding of cloud security concerns in order to propose some measures that mitigate the amount and impact of security failures by providing a studied risk management decisions regarding cloud adoption strategies, so this chapter will identify the top countermeasures that are concerned with the cloud computing and most of these guidelines have been conducted by CSA and some other standards such as (NIST, Symantec, VERIZON, ENISA…etc), data collected from these standards are based on a survey of industry experts to compile professional opinions on the greatest security issues within cloud computing. The following section is summarizing the MFC parameters which are used on this chapter.

6.2. MFC Parameters On Cloud Computing

This section is summarizing the MFC parameters on cloud computing, which are (as shown in table 6-1):

- Cloud's Stakeholders,
- Cloud's Security Requirements,
- Cloud's Components and
- Cloud's Threats.

Table 6-1: MFC parameters on Cloud Computing

Cloud's Stakeholders (NIST 2013)	Cloud's Security Requirement (NIST 2013)	Cloud's Component (SATW, 2012)	Clouds' Threat (NIST 2013) (CSA 2016)
Cloud Provider	Authentication	Applications	Data Breaches
Cloud Consumer	Authorization	Runtime	Weak Identity, Credential and Access Management
Cloud Carrier	Confidentiality	Middleware	Insecure APIs
Cloud Broker	Integrity	OS	System and Application Vulnerabilities
	Availability	Hyper visor	Account Hijacking
		Infrastructure	Malicious Insiders
			Advanced Persistent Threats (APTs)
			Data Loss
			Insufficient Due Diligence
			Abuse and Nefarious Use of Cloud Services
			Denial of Service
			Shared Technology Issues

6.3. Result Generated Using the Proposed Filling Approach

This part represents how the MFC matrices will be generated using statistical data with analytical reasoning that may help to build and quantify an associated matrix which has been supported by the automated tool. Surely some threats are more likely to cause failure than others, and some components are more critical to meeting security requirements than others. So a lot of steps should be considered on this aspect to obtain the realistic results which have been presented in this chapter, so this chapter will be explained as Input/Output representations on abstract model. On input representation some entries with some assumptions (to sake the argument) are used to evaluate the proposed adapting model on a software-level security requirements basis and the output will present the obtained results which is based on those entries, then analyzing, of these obtained results, so the following steps are briefly review the whole cycle of the MFC to use and evaluate the proposed model that has been adapted with the MFC aspects:

1. Cloud Stakeholders is filling the ST Matrix (as shown in table 6-2), then on (DP and TIM Matrix) assigning probability in the lowest row of the matrix and then assigning level no to the remaining

entries on that column based on mentioned assigning criteria (as shown in table 6-3 and table 6-4) and finally fill the TV by considering the number of incidents that has been empirically collected (see table 6-5).

2. Mapping the previous MFC matrices in step 1 to probability matrices (by applying the proposed approaches with its formulas for filling them which were mentioned in chapter 4, so refer to:
    - Table 6-6 which represents the mapping result for the DP Matrix,
    - Table 6-7 which represents the mapping result for the TIM Matrix and
    - Table 6-8 which represents the mapping result for the TV Vector.
3. Computing the MFC0 (as shown in table 6-9) using MFC formula.
4. Deploying a suitable countermeasure that helps to enhance the security of the Cloud Computing in term of reducing the MFC.
5. Reflecting the enhanced values of measure to appropriate and associate factor on the MFC formula (by "Decreasing" the probability of failure and "Increasing" the probability of no failure) in this case the affected factor is the TV that used to estimate the (new TV'), the same method can be applied on the other MFC factors. For the remaining period effectiveness and decline rate have been considered (as shown in table 6-10 and table 6-11).
6. Recalculating the MFC (as shown in table 6-12) to obtain the new MFC1 and calculate the difference (MFC Gain)=MFC0 - MFC1, as shown in table 6-13, then calculating the benefits by considering the hours of usage (as shown in table 6-14 and table 6-15).
7. Dispatching the investment cost for accruing the measure across stakeholders (in this case were assumed that the cost of accruing that measure is 50,000 $, because it's less than the calculated Benefit (B)) refer to table 6-16.
8. Comparing the cost of measure against the benefits (MFC Gain) to decide if the measure is worthwhile or not and this will be done for each stakeholder using the two options of calculating the ROI, refer to table 6-17 for option 1 and table 6-18 for option 2 (this step will be issued with more details in section 6.3.6 and 6.3.7.).

This study proposed a lot of models and explained how to create; structure and fill each of them, the output for all these models is the MFC vector, all remaining steps after filling the matrices of each model are identical.

To facilitate the understanding of these aspects the following sections will present the whole MFC life cycle for the abstract model using INPUT/OUTPUT representations in order to calculate MFC and all relevant economical measures as evaluation action, same thing can be done for all the remaining models.

6.3.1. Filling all MFC Matrices (ST, DP, TIM and TV)

A responsible experts being able to fill all MFC matrices using the proposed approaches for filling each MFC matrix using the extracted empirical data, as shown below:

Inputs:

1. **Stake Matrix:** this matrix reflects the co-relation between cloud stakeholders and cloud security requirements which contains the cost of a security breach in dollars, it reflects to what extent each stakeholder stand to lose as a result of security failure (as shown in table 6-2).

Table 6-2: Stake Matrix (ST)

ST	**Security requirements on Cloud Computing ($)**					
Cloud Stakeholders		***Authentication***	***Authorization***	***Confidentiality***	***Integrity***	***Availability***	***NoR***
	Cloud Consumer	20	40	400	140	20	0
	Cloud Provider	2000	4000	20000	50000	80000	0
	Cloud Carrier	200	400	5000	40000	20000	0
	Cloud Broker	200	400	3000	30000	20000	0

Note: The NoR row represents the case if "No Requirement has been violated" means no stakeholder has been affected in term of financial loss, and leads to event (NoR) with cost 0$, (one of the good things for improving the MFC results is done by considering this NoR case to cover all the possibilities events).

In Stake Matrix (table 6-2):

- Each row filled by relevant stakeholder, or on his behalf.
- Expressed in monetary terms: dollars.
- Represents loss incurred placed on requirement.
- Mostly in the event of failure, cloud provider paid the highest amount of money, cloud consumer paid the lowest amount if money, cloud carrier and cloud broker are in the middle.

2. **Dependency and Impact Matrices Generation**

The following tables (table 6-3 and table 6-4) describe how the TIM and DP matrices can be adapted with cloud computing aspects.

Dependency Matrix: this matrix reflect to what extent each security requirement is dependant on cloud copmponent, the co-relation between cloud components and its security requirements represent the probability of security requirements violation given that specific component has been compromised, the result of the assigning level-No approach has been proposed in table 6-3 and table 6-4, then these level-No will be mapped to probabilities format.

Table 6-3: Dependency Matrix (DP) with Assigning level number to each entry (Nahla Murtada 2016)

DP	**Cloud Components (SATW, 2012) (NIST 2013)**							
Cloud Requirements		***Applications***	***Runtime***	***Middleware***	***OS***	***Hyper visor***	***Infrastructure***	***NoC***
	Authentication	1	1	1	3	3	1	**0**
	Authorization	1	1	1	3	3	1	**0**
	Confidentiality	1	1	1	2	2	1	**0**
	Data Integrity	2	2	2	1	1	2	**0**
	Availability	3	2	1	1	2	2	**0**
	NoR	**0.5**	**0.16**	**0.16**	**0.3**	**0.5**	**0.5**	**1**
Note: The intersection between NoC with NoR means if "No Component has been compromised" that means "No Requirement has been violated", and leads to event (NoC intersect with NoR) with probability 1.0.								

The Dependency Matrix (table 6-3):

- Filled by System Architects,
- Probability of failure with respect to a requirement given that a component has failed.
- Dependent on the operational attributes.

Threat Impact Matrix: this matrix reflects to what extent that each cloud component is compromised in the event of given threat materialized, and also it's converted to probability format, (refer to table 6-4).

Table 6-4: Threat Impact Matrix (TIM) with Assigning level number to each entry (Nahla Murtada 2016)

TIM	**Cloud Threat (CSA 2016) (SATW, 2012)**												
Cloud Component		***T1***	***T2***	***T3***	***T4***	***T5***	***T6***	***T7***	***T8***	***T9***	***T10***	***T11***	***T12***	***NoT***
	Application	1	3	1	3	2	2	1	1	1	2	2	2	**0**
	Runtime	2	3	2	3	3	3	2	2	2	2	2	2	**0**
	Middleware	2	3	2	2	2	2	2	2	2	1	2	2	**0**
	OS	2	3	2	1	3	3	2	2	2	2	2	2	**0**
	Hyper visor	1	2	2	1	1	1	1	1	1	2	1	1	**0**
	Infrastructure	1	1	2	3	1	1	1	2	1	2	1	1	**0**
	NoC	**0.50**	**0.49**	**0.48**	**0.47**	**0.46**	**0.45**	**0.44**	**0.43**	**0.42**	**0.41**	**0.4**	**0.39**	**1**
Note: The intersection between NoT with NoC means if "No Threat has been materialized" that means "No Component has been compromised", and leads to event (NoT intersect with NoC) with probability 1.0.														

The Threat Impact Matrix (table 6-5):

- Filled by V&V Team,
- Probability of compromising a component given that a threat has materialized.
- Dependent on the target of each threat, likelihood of success of the threat.

3. Threat Vector Generation

As it is expected, over the years the number of cloud vulnerability incidents has risen (as shown in chapter one). In fact from 2009 to 2011 the number of cloud vulnerability incidents more than doubled - from 33 to 71, most likely due to the phenomenal growth in cloud services, and from 2012 to 2014 traditional threats increased 6 percentage points. This TV is filled by a number of incidents (as shown in table 6-5) which is mapped to probability of threat materialized per unit of time using the proposed formula for mapping it (as shown in table 6-6) (Symantec 2015), (CSA 2013a).

Table 6-5: Threat Vector that representing a number of incidents for each threat

Threat No.	Threat Name	No. of Incident
T1	Data Breaches	18
T2	Weak Identity, Credential and Access Management	4
T3	Insecure APIs	51
T4	System and Application Vulnerabilities	4
T5	Account Hijacking	3
T6	Malicious Insiders	3
T7	Advanced Persistent Threats	6
T8	Data Loss	43
T9	Insufficient Due Diligence	11
T10	Abuse and Nefarious Use of Cloud Services	12
T11	Denial of Service	15
T12	Shared Technology Issues	5
	NoT	

Threat vector (table 6-5):

- Filled by Security Team,
- Probability of realization of each threat,
- Dependent on extracted empirical data, known threat models and known counter-measures, etc.

Output:

On DP Matrix, notice that the NoR row represent the most three critical components which are: (application, hypervisor and infrastructure), in the event of this security failures:

- The application entity is the most critical component because it's highly affect on availability requirement which is direct affect on cloud users, so failure on application component is catastrophic especially on critical system.
- The failure on Hypervisor and infrastructure component are negatively affect on authentication and authorization requirements, failure on infrastructure component is critical, because the failure here may lead to lose a high amount of data and resolve this type of failure is more difficult than other remaining failures which may take several time to deal with it, so its take the highest probability specially when a provisioning controls is not strong enough, hypervisor component will lead several failures for a several stakeholders due to share a pool of resources between these stakeholders, so these three components take the highest probability.

OS component has a lower impact than the previous components (because if failure occurs here provider can switch these affected users to another OS using another virtual machine without user intervention); finally the remaining components (runtime and middleware) are the least affected components.

Application, hypervisor and infrastructure components takes the highest probability and the remaining 0.5 will be distributed across the remaining column, then the OS component (which take lower probability than Application, hypervisor and infrastructure components) and finally the runtime and middleware components are take the lowest probability.

Table 6-6: Dependency Matrix (DP) when it's mapped to "Probability Format" using "Probability Distribution Rules"

DP	**Cloud component**						
	Applications	Runtime	Middleware	OS	Hyper visor	Infrastructure	NoC
Security Requirement							
Authentication	0.0625	0.11904	0.1388889	0.2	0.136364	0.071429	**0**
Authorization	0.0625	0.11904	0.1388889	0.2	0.136364	0.071429	**0**
Confidentiality	0.0625	0.11904	0.1388889	0.1333	0.090909	0.071429	**0**
Data Integrity	0.125	0.23809	0.2777778	0.0666	0.045455	0.142857	**0**
Availability	0.1875	0.23809	0.1388889	0.0666	0.090909	0.142857	**0**
NoR	**0.5**	**0.16**	**0.16**	**0.3333**	**0.5**	**0.5**	**1**
Sum	1	1	1	1	1	1	1

Note: The intersection between NoC with NoR means if "No Component has been compromised" that means "No Requirement has been violated", and leads to event (NoC intersect with NoR) with probability 1.0.

So these three critical components take the highest probability (NoR = 0.5) the remaining values on the same row take lower values than these three components and each column has summation of one, so the

remaining value of (1- NoR) will be distributed on that column, for example the intersection between (Application component and NoR = 0.5) the remaining is (0.5) this value will be distributed on the remaining entries of the column according to the levels (0, 1, 2, 3…etc) that we assign to each entry, same thing is in TIM (refer to table 6-7), However, building the TV is based on a number of incidents which are mapped to probabilities of threat occurrence per unit of time as shown in table 6-8, obtained data is based on data that has been conducted by a lot of ISTR such as CSA, NIST and Symantec with some analytical reasoning, one of the good things on this study the collected and extracted data give a more accurate, precise and reasonable results as shown later.

Table 6-7: Threat Impact Matrix (TIM) when it's mapped to "Probability Format" using "Probability Distribution Rules"

TIM	Cloud Threat (CSA 2016) [STAW, 2012]												
	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	No
Component													
Application	0.055	0.102	0.047	0.122	0.090	0.091	0.062	0.057	0.064	0.107	0.120	0.122	**0**
Runtime	0.111	0.102	0.094	0.122	0.135	0.137	0.124	0.114	0.128	0.107	0.120	0.122	**0**
Middleware	0.111	0.102	0.094	0.081	0.090	0.091	0.124	0.114	0.128	0.053	0.120	0.122	**0**
OS	0.111	0.102	0.094	0.040	0.135	0.137	0.124	0.114	0.128	0.107	0.120	0.122	**0**
Hyper visor	0.055	0.068	0.094	0.040	0.045	0.045	0.062	0.057	0.064	0.107	0.060	0.061	**0**
Infrastructur	0.055	0.034	0.094	0.122	0.045	0.045	0.062	0.114	0.064	0.107	0.060	0.061	**0**
NoC	**0.50**	**0.49**	**0.48**	**0.47**	**0.46**	**0.45**	**0.44**	**0.43**	**0.42**	**0.41**	**0.40**	**0.39**	**1**
Sum	1	1	1	1	1	1	1	1	1	1	1	1	1

Note: The intersection between NoT with NoC means if "No Threat has been materialized" that means "No Component has been compromised", and leads to event (NoT intersect with NoC) with probability 1.0.

Table 6-8: Threat Vector (TV) when it's mapped to probability format

Threat	**Week0**
T1	0.002054795
T2	0.000456621
T3	0.005821918
T4	0.000456621
T5	0.000342466
T6	0.000342466
T7	0.000684932
T8	0.004908676
T9	0.001255708
T10	0.001369863
T11	0.001712329
T12	0.000570776
Not	0.980022831
Sum	1

NoT: No Threat has been Materialized

In 2016, CSA proposed the twelve up-to-date threats that represent the frequency of occurrence, building this vector is based on the "Frequent of Incidents", using SLR approach which proved there are four most frequent incidents (accounted for 72.5% of all cloud outage incidents) – as a result, improving these four threats will lead to gain more revenue because whenever the probability of failure is being higher, a bigger area for improvement which lead to increase the revenue (as shown later), these top frequent threats are (refer to table 6-8):

1. CSA Threat 1 "***Data Breach***" with 18 incidents accounting for 10% of all threats.
2. CSA Threat 3 "***Insecure Interfaces and APIs***" with 51 incidents accounting for 29% of all threats.
3. CSA Threat 8 "***Data Loss and Leakage***" with 43 incidents accounting for 24.5% of all threats reported.
4. New Threat 11 "***Denial of Service***" with 15 incidents accounts for 8.6% of all threats reported.

6.3.2. Compute Of MFC

This MFC Model assumed that no more than one threat materialized per unit of time, no more than one component has been compromised per unitary period of time and no more than one requirement has been violated per unit of time, by using the adequate values in MFC metrics, the MFC vector can be computed by using the MFC formula (1).

Input:

MFC Matrices.

Output:

In table 6-9, the result of MFC shows that the term Mean is used because of a prediction has been done based on probability. Meaning out of 100 hours of operation, in 90 hours there is no threat, hence our loss is 0 dollars (as shown in ST matrix, "NoR" column), and the remaining 10 hours, some threat materializes, which may affect components that may affect requirements that may affect costs. When that happens, the amount of loose cited in the ST matrix. On average, out of 100 hours, each stakeholder loses MFC $/hour, so the average here is on the hours, as a result of computing the MFC, cloud consumer has the lowest result of MFC and cloud provider has the highest result which is reasonable results because the failure cost on cloud provider is much higher than any other stakeholders.

Table 6-9: Stakeholder Mean Failure Cost

Stakeholders	MFC $/hour
Cloud Consumer	0.829947
Cloud Provider	246.124378
Cloud Carrier	107.914295
Cloud Broker	88.232000

6.3.3. Estimating the effectiveness rate and decline rate of measurements

After applying an appropriate countermeasure, there is a need to estimate the effectiveness and the decline rate for that measure, so let's assume the MFC0 is the first MFC that has been obtained by applying the MFC formula and the remaining MFC values has been obtained after applying suitable measure (such as installing encryption tool, firewall, antivirus…etc) this measure will lead to reducing the MFC by reflecting enhanced values (after applying measure) to appropriate matrix, on the presented case the TV is the affected vector, on TV the probability of threat occurrence is decreasing and the probability of NoT is increasing (in order to keep TV balance), then calculate the MFC again to obtain new MFC (MFC Gain), this step is periodically being applied (on the presented case its every five weeks) over each period of time new MFC vector has been obtained for each stakeholder which represent the failure cost per unit of time and by applying appropriate countermeasure this MFC will be enhanced in term of reduced the MFC0 as shown in table 6-12, However, the effectiveness rate will be declined over the time.

Each "Threat" has its associated "Control Measures", these measures has been proposed by CSA that aimed to mitigate the impact of security failure (all these "Threats" with its "Control Measures" has been displayed in table 6-20). In our proposed case the deployment of the Control Measures (such as installing anti-virus, deploying encrypted tools…etc) - which denoted by "M3" that used to control the "Insecure API Threat" which denoted by "T3" - will lead to "decrease" in the failure probability of T3 and "increase" the probability of NoT for the first time.

After a while the probability of T3 will be increased and this may occur due to: appearance of some new types of viruses, the growth of a number of users who used the service or the growth of their needs…etc, so there is a need to estimate the effectiveness and decline rates over that period of time, as shown on the table 6-11.

Input:

The TV + The average Starting Success Rate (SSR) + The average Starting Decline Rate (SDR).

Output:

Threat working group find ways to estimates these rates, a study that proposed by "AV Comparatives", this modeling strategy has become standard in *comparative* risk estimation and assessments, which gives a concrete data to estimate these rates (result is shown in table 6-10):

- From week 1 to week 3 they declare a rate of effectiveness ratio of "Insecure API" (T3) are detected and mitigated by the antivirus with authentication tool (M3) that varies between 18% in week 1 and 71% in week 3, with an average of 44.2%.
- From week 4 – week 50 they monitor the same M3 products which reveal the success rate is declined that varies between 8% and 67% on that period, with an average decline rate of 40.13%, this case assumed that the decline rate is constant rate of decline, this will allow estimating the weekly decline rate, as shown below:

The average Starting Success Rate (SSR) of the Effectiveness = 44.2%.
The average Starting Decline Rate (SDR) of the Effectiveness = 40.13%.

The weekly decline rate from week 4 (R) ^4= 1-0.4013=0.5987, then
R = 0.87963
R^5=0.5265 (which means the Success Rate will be weekly decline by 0.5265), so:

$$Decline\ Rate\ Of\ That\ Success = Success\ Rate \times Weekly\ Decline\ Rate \quad (26)$$

$$Failure\ Rate = 1 - Decline\ Rate\ Of\ That\ Success \quad (27)$$

$$Estimated\ probability\ of\ Threat = \Pr evious\ Threat\ \ \Pr obability \times Current\ Failure\ Rate \quad (28)$$

6.3.4. Reflecting the enhanced values of measure to associate matrix

This improvement will be represent in a term of reducing MFC by "Decreasing" the probability of threat occurrence and "Increasing" the probability of No Threat (NoT) by keeping balance of all probability metrics with summation of one, this step is reflecting the new values on that TV which positively affected on the MFC result, these new values has been conducted by considering the effectiveness and decline rate which is mentioned in the previous step (result is shown in table 6-11).

Input:

The input here is the output from the previous step (the estimated probabilities for threat occurrence which is decreased over the time and the estimated probabilities for the NoT which is increased over the time).

Output:

New Threat vector with new estimated probabilities which is based on the previous step (result has been shown in table 6-11)

6.3.5. Recalculating the MFC in term of benefits

In this step the MFC should be recalculated again to obtain a new parameter which is called "MFC Gain", this calculation has been done by comparing the difference between old (MFC0) and new MFC (MFC1) applying the formula (1) and formula (20):

Input:

The old and new probability values of a TV with all MFC Matrices, assuming that the

Output:

The output of this step is producing a new vector of MFC with the result of MFC gain for each stakeholder per unit of time, table 6-12 present the MFC results and table 6-13 present the MFC gain, accordingly the benefits can be easily obtained.

6.3.6. Dispatching the Investment Cost C(w)

Cloud computing has simultaneously created new security challenges and now the development of the cloud service model delivers business-supporting technology more efficiently than before, so this development can be applied by deploying some countermeasures, because from time to time cloud stakeholders need to improve some cloud service to improve their QoS, here this deployed measure should use to enhance the MFC results in term of reduced MFC which is called (ΔMFC of MFC Gain) and each of these measures are used to improve specific MFC matrix. However, all of these measures are represented as investment project which needed investment cost to deploy that appropriate measure, the Question here is: "How to Dispatch this Investment Cost across stakeholders?"

To answer these questions two options has been proposed:

- Option 1: *In proportion to MFC gains* – refer to table 6-16 and table 6-17.
- Option 2: Or *dispatching that ICi in such a way that make all ROI's are Identical*, result has been shown in table 6-18.

Option 1 assumed that this investment cost is charged on the stakeholders in proportion to their stake which is measured by their respective MFC Gain as shown on the following formula (refer to table 6-16).

$$C_i(0) = \frac{MFC\ Gain_i(0)}{MFC\ Gain(0)} \times Investment\ Cost\ C(0) \qquad (29)$$

However, under some circumstances (as shown in table 6-17), the ROI of the cloud stakeholder is negative (In this case, the ROI for cloud consumer is -0.9), this value is negative because its MFC gain is very small when comparing with other stakeholders (as shown in table 6-13), hence the proposed investment cannot be deemed worthwhile for all the stakeholders, due to these reasons and in order to avoid this situation, option 2 gain to achieve fairness between all stakeholders with a positive ROI result as much as possible, this situation has been resolved by revisiting the formula in option 1 to determine initial investment costs $C_i(0)$ instead of charging stakeholders according to MFC gains, in this option 2 the investment cost for each stakeholder has been calculated using the following formula 24:

So option 2 will charge them in such a way as to make all ROIs identical, the most benefit feature here (as a result of this option): it is easy to know the benefit of each stakeholder before identifying their investment cost $C_i(0)$, so according to what you need, you can allocate appropriate Investment Cost as shown in table 6-18, this feature has been supported by the proposed automated tool, which has been presented in Section 6.5.

6.3.7. MFC Results with NPV and ROI options

This section concern on "how to evaluate the MFC measure" by considering the two mentioned options, for each option an input, output has been identified and then the obtained results have been analyzed:

Option1:

Input:

- The Investment Cost of each stakeholders Ci(0): this investment cost is charged on the stakeholders in proportion to their stake which is measured by their respective MFC gain by applying the formula 29, formula 17, and formula 18, (results are shown in table 6-16).

- Number of Stakeholders, on this case there are four stakeholders.
- Discount-Rate: the discount rate is enabling to compare money this year and future years.
- (The typical year values of "d": between 0.10 and 0.15), on this case assumed 0.12 as an average value, so will divide it by 52 weeks (each year contain 52 weeks= 0.0023).
- Cycle Length - Number of (Weeks- Months-Years) – here is 50 weeks.
- The Whole Investment Cost for deploying the Measure C(0), this case assumed that the investment cost C(0) = 50,000$.

Output: (results are shown in table 6-16 and table 6-17).

- Obtaining the ROI and NPV for each stakeholder (which is differing across stakeholders, because it's based on their stake), results is shown in table 6-17.
- As shown a cloud consumer has a negative ROI.

Option 2:

Calculate the benefits for each stakeholder by considering how much each stakeholder is use or produce the service because as mentioned before, the most important issue on cloud computing is "pay as you go" concept, each stakeholder differs from another in term of service availability, so here this case assumed that 7 hours per week (7 days * 1 hour for each day = 7 hours) for cloud consumer and for the reaming stakeholders (7 days * 24 hours each day =168 hours) – (as shown in table 6-14), the MFC and MFC Gain give an hourly rate (MFC is treat with hours) so there is a need to obtain the benefits per week which has been done by converting it to a weekly rate and taking into account the number of hours of using or producing the service per week, the obtained benefits per week B(w) result will help us to calculate the ROI and NPV to take a correct decision about deploying the measure, this benefits can be calculated using the formula (19) (as shown in table 6-14):

As a result, the obtained result also is reasonable because the MFC per hour of the cloud consumer is the lowest result and for cloud provider is the highest one, accordingly the failure cost on cloud provider will be much higher than the other stakeholders and also accordingly, an Investment Cost Ci(w) and the benefits Bi(w) for cloud provider will be much higher than all other stakeholders (as shown in table 6-15).

Input:

- All the inputs of option one with it's assumptions except the $C_i(0)$, because $C_i(0)$ has been calculated it in order to obtain identical ROIs for all stakeholders, so here there are five

unknowns (The four $C_i(0)$ + ROI), output can be obtained when applying the following formula 22, and formula 23:

$$B = \sum_{w=1}^{W} \frac{B(w)}{(1+d)^w} \qquad \textbf{(30)}$$

- The solutions of this investment cost and ROI are in the formula (24), formula (21) and formula (18):

Output: (is shown in table 6-18**)**

- Obtaining the ROI for each stakeholder (which is identical across all stakeholders, to achieve fairness between stakeholders).
- Obtaining the benefits B_i (*w*) for each stakeholder and the total of these benefits for all stakeholders B(*w*) ∀ w>=1.

Obtaining the investment cost for each stakeholders based on the calculated benefits.

Obtaining the NPV fore each stakeholder.

6.3.8. Deploying Another Measure

Investor may need to apply another controlling measure such as M8 to reduce the impact of "Account, Service and Traffic Hijacking Threat" (this Threat referred as T8) – as shown in table 6-20, but they don't know if this new controlling measure is profitable or not, or if there is any other measure better than this measure?, in this case the ROI is very powerful to compare, estimate and decide which measure is the best one. Let's assume the deployment of this measure (M8) will enhance and improve T8, same steps will be followed and same assumptions will be considered to facilitate comparing the results of measures that may help to decide which measure will reveal the highest ROI and NPV (this will be shown from table A-1 to table A-9), in this case the following steps should be applied:

- Evolving Threat Probabilities, (as shown in table A-1).
- Reflecting the effectiveness of T8 on a (TV), (as shown in table A-2).
- Calculating the MFC Results when improving T8 by deploying M8 (as shown in table A-3).
- Calculating the MFC gain when deploying M8 (for all stakeholders), (as shown in table A-4).
- Calculating the Benefit B(w) when deploying M8 (for all stakeholders), (as shown in table A-5 and table A-6).
- Calculating the Investment Cost C(w) when deploying M8, (as shown in table A-7).
- Calculating the NPV and ROI in proportion to MFC Gain on T8 when applying M8, (as shown in table A-8).

- Calculating the ROI in order to make all ROI Identical when applying M8 on T8, (as shown in table A-9).

6.4. MFC and ROI Model Premises and results with V&V aspects

MFC with ROI Model Premises with results on cloud computing are:

- The proposed model has been validated using empirical observations.
- In addition, analytical and empirical data has been collected on the cloud computing in order to make this task systematic, this has been done by applying the proposed assigning approach with adherence to the rule of "Distribution Probabilities", and also automated tool has been developed to support these MFC model principles.
- Four stakeholders on the cloud computing were presented, each stakeholder is responsible for a key decision in the process of the V&V action (whether it's worthwhile or not).
- In option 1, each stakeholder computes his associate ROI based on his stake to the cost of V& V action, and the MFC gains.
- In option 2: The cost of the V& V action must be dispatched across stakeholders in such a way as to make all ROIs identical.
- All decisions are based on the economic rationale.
- All decisions can be modeled as investment decisions.
- All decisions can be quantified by means of investment analysis functions.
- Allow to change the "Default values" by applying "Propagation Approach" using the proposed equation for that – (as shown in chapter 3).
- Allow to reflect the impact of countermeasures on the appropriate MFC Matrix by increasing and decreasing some entries in the MFC matrices and obtaining new value of the MFC which is called "MFC Gain".
- Decomposing the MFC parameters using (STRIDE, CSA, NIST and Verizon…etc) different threat models and accordingly, changing the content MFC parameter based on user's needs and knowledge.
- Some of these metrics complement other threat metrics and others extend others.
- Finally, the proposed tool aims to "Quantify the cost/benefit analysis" by investigating the amount of additional profits produced due to a certain investment (in specific period of time) for each stakeholder which may help the decision makers to decide correctly against deploying security measure.

6.4.1. ROI and MFC Benchmark

Thee benchmark analysis here focus on representative samples of a different measures that used to mitigate the impact of threat that use the activity-based costing methods to analyze these results. The analysis of this part is consisting of three countermeasures (M3, M8 and M11) that are relevant to (T3, T8 and T11) as shown in table 6-19, and the proposed options (for dispatching the investment cost) are represented as key findings of our benchmark, that involve three threats with its relevant countermeasures, which are used as sample of representative data.

As shown in table A-10 and table 6-13, the gain result when using M3 is better than the gain when deploying M8, and accordingly the Benefits when deploying M3 is being higher than M8 (as shown in table 6-15 and table A-11), so the ROI of M3 is better than M8 if the same investment cost is assigned for each measure (in this case if the Investment cost is less than 67,880 $), as noticed here if we assign same IC = 50,000$ for each measure (M3 and M8) here the ROI when deploying M3 = 0.4 and the ROI when deploying M8 = 0.36, so to achieve more revenue its better to deploy M3, as an evaluation result, the first controlling measure M3 (which deals with T3) revealing better revenue than M8 (which deals with T8), on this case decision makers can easily identify which measure is cost effective than other by comparing the ROI results of each measure with its premises (refer to table 6-19), however, if the investment cost for deploying M3 is 50,000$, and the same investment cost assigned for M11, in such case negative ROI will be presented, because the benefit here is too small when comparing it with the other measures “M3, M8”, the Investment Cost C(0) is inversely proportional to ROI, however the Benefit (B) is direct proportional to ROI, so these ROIs results reflect to what extent this measure is powerful, by changing the desired premises (which is based on decisions maker’s goals, needs and budget…etc) different results has been obtained that directly lead to the best decision, so this measure is innovative measure because if you have different scenarios with a different premises it can give a comparative and reasonable results for all cloud stakeholders which considering the variance that may exist between these stakeholders, requirements, components and threats as shown as a comparative results in table 6-19.

As a result of applying the ROI options:

- When applying M3, the end results of these two options for dispatching (for the whole B(w), NPV, ROI)) are the same (compare the end row of table 6-17 and table 6-18), all results are the same, however the distribution of cost is different, in option one the distribution of investment cost and the benefits are based on MFC Gain, however in option two distribution is made in such a way that makes all ROI identical (this will be done by applying it’s Investment cost, ROI and benefits (Bi) formulas).

- As expected results, whenever the whole Investment cost C(0) is less than Benefits B(w) greater profits will be resulted and vice versa, and if the C(0) is equal to Benefits B(w) this will lead to ROI=0, which means no revenue, as a result whenever the C(0) is less than B(w) the ROI will be positive (which means it is a profitable measure) otherwise ROI will take negative values which mean (withdraw this measure) because this measure will lead to lose money, (Results shown in table 6-19).
- The most important feature of the second option is that, without knowing the whole Investment Cost C(0) or the Investment Cost for each stakeholder Ci(w), it can be easily determined the benefit for each stakeholder (Bi), the total of Benefit (B), NPV and ROI, so based on the business goals, selecting the most appropriate measure can be easily being done, as shown in table 6-19, deploying M3 will achieve the highest Benefit and M8 achieve the lower Benefit than M3, this due to probability that assigned to each threat (the probability of T3 is higher than the probability of T8), so if the (T3) is improved, the gain will be higher than improving (T8). However, may be the impact of T8 is higher than T3, so if your goal is reducing the most highest impact in this case they have to improve T8 using M8, and if their goal is increasing the revenue its better to improve T3 by deploying M3, finally a lot of scenarios has been existing and based on a business goals (either mitigate an impact, mitigate an amount or achieve higher revenue…etc) decision makers can easily select the most appropriate controlling measure.
- By comparing the cost of measure against the benefits, decision makers can easily decide if the measure is worthwhile or not and this will be done for each stakeholder separately.
- An investment project is judged as profitable if NPV > 0 and ROI>0.
- ROI help the decisions makers to compare between varieties of measures to estimate and decide which measure will achieve their goals (this will be shown on a next section and the result has been shown in table 6- 19).

This study presented the top twelve threats on cloud computing on 2016 which proposed by CSA, TV presenting the probabilities of materializing that threats per unit of time, however cloud stakeholders may need to apply some measures to reduce the probability of threat occurrence, but if there exist a lot of measures (M1,M2,M3…M12) which shown in table 6-20, how do decisions makers decide which measure is better, so the following tables display only three candidates measures (M3 , M8 and M11) with its results for a comparison purpose, but practically there are twelve controlling measure (for controlling a TV) that has been proposed by CSA as shown in table 6-20, and same steps can be applied for all remaining measures (by applying all mentioned steps for computing the ROI and NPV with its associated results), so decisions makers can easily identify which measure is appropriate using this novel economical approach.

Table 6-10: Evolving Threat Probabilities by reflecting the effectiveness of T3 on a (TV)

	Week0	week5	Week10	Week15	Week 20	Week25	week30	week35	Week40	week45	week50
Decline	0.8796	0.8796	0.8796	0.8796	0.8796	0.8796	0.8796	0.8796	0.8796	0.8796	0.8796
Success (effectiveness)	0.4420	0.2327	0.1225	0.0645	0.0340	0.0179	0.0094	0.0050	0.0026	0.0014	0.0007
Fail	0.5580	0.7673	0.8775	0.9355	0.9660	0.9821	0.9906	0.9950	0.9974	0.9986	0.9993
T3	0.0058	0.0045	0.0039	0.0037	0.0035	0.0035	0.0034	0.0034	0.0034	0.0034	0.0034
No Threat(NoT)	0.9800	0.9814	0.9819	0.9822	0.9823	0.9824	0.9824	0.9824	0.9824	0.9824	0.9824
Sum (T1+NoT)	0.9858	0.9858	0.9858	0.9858	0.9858	0.9858	0.9858	0.9858	0.9858	0.9858	0.9858

Table 6-11: The Effectiveness of T3 on a (TV) from Week0 – Week50 when deploying M3

Threat	TV	Week5	Week10	week15	Week 20	Week25	week30	week35	week40	week45	Week50
T1	0.002054795	0.002054795	0.002054795	0.002054795	0.002054795	0.002054795	0.002054795	0.002054795	0.002054795	0.002054795	0.002054795
T2	0.000456621	0.000456621	0.000456621	0.000456621	0.000456621	0.000456621	0.000456621	0.000456621	0.000456621	0.000456621	0.000456621
T3	0.005821918	0.00446708	0.00391976	0.00366690	0.00354236	0.00347902	0.00344626	0.00342918	0.00342023	0.00341553	0.00341306
T4	0.000456621	0.000456621	0.000456621	0.000456621	0.000456621	0.000456621	0.000456621	0.000456621	0.000456621	0.000456621	0.000456621
T5	0.000342466	0.000342466	0.000342466	0.000342466	0.000342466	0.000342466	0.000342466	0.000342466	0.000342466	0.000342466	0.000342466
T6	0.000342466	0.000342466	0.000342466	0.000342466	0.000342466	0.000342466	0.000342466	0.000342466	0.000342466	0.000342466	0.000342466
T7	0.000684932	0.000684932	0.000684932	0.000684932	0.000684932	0.000684932	0.000684932	0.000684932	0.000684932	0.000684932	0.000684932
T8	0.004908676	0.004908676	0.004908676	0.004908676	0.004908676	0.004908676	0.004908676	0.004908676	0.004908676	0.004908676	0.004908676
T9	0.001255708	0.001255708	0.001255708	0.001255708	0.001255708	0.001255708	0.001255708	0.001255708	0.001255708	0.001255708	0.001255708
T10	0.001369863	0.001369863	0.001369863	0.001369863	0.001369863	0.001369863	0.001369863	0.001369863	0.001369863	0.001369863	0.001369863
T11	0.001712329	0.001712329	0.001712329	0.001712329	0.001712329	0.001712329	0.001712329	0.001712329	0.001712329	0.001712329	0.001712329
T12	0.000570776	0.000570776	0.000570776	0.000570776	0.000570776	0.000570776	0.000570776	0.000570776	0.000570776	0.000570776	0.000570776
Not	0.980022831	0.98137767	0.98192499	0.98217785	0.98230239	0.98236573	0.98239849	0.98241557	0.98242452	0.98242922	0.98243169
Sum	1	1	1	1	1	1	1	1	1	1	1

Table 6-12: MFC when deploying M3 by installing an authentication plug-in with anti-virus product

Week	0	5	10	15	20	25	30	35	
Stakeholders									
Cloud Consumer	0.829947	0.777704	0.756598	0.746848	0.742046	0.739603	0.738340	0.737681	0
Cloud Provider	246.124378	230.850505	224.680218	221.829598	220.425565	219.711448	219.342189	219.149604	21
Cloud Carrier	107.914295	101.240636	98.544634	97.299104	96.685635	96.373614	96.212272	96.128126	9
Cloud Broker	88.232000	82.775644	80.571404	79.553064	79.051494	78.796387	78.664475	78.595677	7

Table 6-13: MFC gain when deploying M3 (for all stakeholders)

Week	0	5	10	15	20	25	30	35	
Stakeholders									
Cloud Consumer	0	0.05224	0.07335	0.08310	0.08790	0.09034	0.09161	0.09227	0.
Cloud Provider	0	15.27387	21.44416	24.29478	25.69881	26.41293	26.78219	26.97477	27
Cloud Carrier	0	6.67366	9.36966	10.61519	11.22866	11.54068	11.70202	11.78617	11
Cloud Broker	0	5.45636	7.66060	8.67894	9.18051	9.43561	9.56753	9.63632	9.
Sum		27.45613							

Table 6-14: Hours for using the service

Hrs of Usage	Week0	Week5	week10	Week15	week 20	Week25	week30	week35	we
Stakeholders									
Cloud Consumer	7	7	7	7	7	7	7	7	
Cloud Provider	168	168	168	168	168	168	168	168	
Cloud Carrier	168	168	168	168	168	168	168	168	
Cloud Broker	168	168	168	168	168	168	168	168	

Table 6-15: Benefit B(w) when deploying M3 (for all stakeholders)

Week	Week0	Week5	Week10	Week15	week 20	week25	week30	week35	w
Cloud Consumer	0	0.3657	0.5134	0.5817	0.6153	0.6324	0.6412	0.6459	0.
Cloud Provider	0	2566.0106	3602.6189	4081.5230	4317.4006	4437.3723	4499.4078	4531.7620	45
Cloud Carrier	0	1121.1747	1574.1031	1783.3521	1886.4148	1938.8344	1965.9397	1980.0764	19
Cloud Broker	0	916.6679	1286.9802	1458.0614	1542.3251	1585.1831	1607.3443	1618.9024	16

Table 6-16: Investment Cost C(w) when deploying M3

Stakeholder	**MFC Gain $/Hrs**	**Investment cost, Ci(w) - ($)**
Cloud Consumer	0.05224	95.14
Cloud Provider	15.27387	27815.05
Cloud Carrier	6.67366	12153.31
Cloud Broker	5.45636	9936.50
Sum	27.45613	50,000
C(w) = 50,000$		

Table 6-17: ROI in proportion to MFC Gain on **T3** when applying **M3**

ROI for Stakeholders											
Cloud Consumer											
Week	0	5	10	15	20	25	30	35	40	45	50
B(w)	0	0.3657	0.5134	0.5817	0.6153	0.6324	0.6412	0.6459	0.6483	0.6495	0.6502
C1(w)	95.1400	0	0	0	0	0	0	0	0	0	0
B(w)-C(w)	-95.1400	0.3657	0.5134	0.5817	0.6153	0.6324	0.6412	0.6459	0.6483	0.6495	0.6502
(1+d)^w	1.0000	1.0116	1.0232	1.0351	1.0470	1.0591	1.0714	1.0837	1.0962	1.1089	1.1217
B-C/(1+d)^w	-95.1400	0.3615	0.5018	0.5620	0.5877	0.5971	0.5985	0.5960	0.5914	0.5857	0.5797
D=	0.0023										IC+NPV
Cloud Provider											
Week	0	5	10	15	20	25	30	35	40	45	50
B(w)	0	2566.01	3602.62	4081.52	4317.40	4437.37	4499.41	4531.76	4557.61	4557.61	4562.29
C1(w)	27815.0486	0	0	0	0	0	0	0	0	0	0
B(w)-C(w)	-27815.05	2566.01	3602.62	4081.52	4317.40	4437.37	4499.41	4531.76	4557.61	4557.61	4562.29
(1+d)^w	1.00	1.01	1.02	1.04	1.05	1.06	1.07	1.08	1.10	1.11	1.12
B-C/(1+d)	-27815.05	2536.70	3520.80	3943.27	4123.52	4189.70	4199.75	4181.64	4157.46	4109.98	4067.21
D=	0.0023										IC+NPV
Cloud Carrier											
Week	0	5	10	15	20	25	30	35	40	45	50
B(w)	0	1121.17	1574.10	1783.35	1886.41	1938.83	1965.94	1980.08	1987.48	1991.37	1993.42
C1(w)	12153.31	0	0	0	0	0	0	0	0	0	0
B(w)-C(w)	-12153.31	1121.17	1574.10	1783.35	1886.41	1938.83	1965.94	1980.08	1987.48	1991.37	1993.42
(1+d)^w	1.00	1.01	1.02	1.04	1.05	1.06	1.07	1.08	1.10	1.11	1.12
B-C/(1+d)^w	-12153.31	1108.37	1538.35	1722.94	1801.70	1830.62	1835.01	1827.10	1812.98	1795.79	1777.10
D=	0.0023										IC+NPV
Cloud Broker											
Week	0	5	10	15	20	25	30	35	40	45	50
B(w)	0	916.67	1286.98	1458.06	1542.33	1585.18	1607.34	1618.90	1624.96	1628.14	1629.81
C1(w)	9936.50	0	0	0	0	0	0	0	0	0	0
B(w)-C(w)	-9936.50	916.67	1286.98	1458.06	1542.33	1585.18	1607.34	1618.90	1624.96	1628.14	1629.81
(1+d)^w	1.00	1.01	1.02	1.04	1.05	1.06	1.07	1.08	1.10	1.11	1.12
B-C/(1+d)^w	-9936.50	906.20	1257.75	1408.67	1473.06	1496.70	1500.30	1493.83	1482.29	1468.23	1452.95
D=	0.0023										IC+NPV

ROI	NPV
0.40051	20025.52
* TVM : Time Valu	

Table 6-18: Identical ROIs when applying M3 on T3

Cloud Consumer												
Week	0	5	10	15	20	25	30	35	40	45	50	
B(w)	0	0.3657	0.5134	0.5817	0.6153	0.6324	0.6412	0.6459	0.6483	0.6495	0.6502	
C1(w)	C1(0)	0	0	0	0	0	0	0	0	0	0	
B(w)-C(w)		0.3657	0.5134	0.5817	0.6153	0.6324	0.6412	0.6459	0.6483	0.6495	0.6502	
(1+d)^w	1.0000	1.0116	1.0232	1.0351	1.0470	1.0591	1.0714	1.0837	1.0962	1.1089	1.1217	Bi
B-C/(1+d)^w		0.3615	0.5018	0.5620	0.5877	0.5971	0.5985	0.5960	0.5914	0.5857	0.5797	5.5614
D=	0.0023											
Cloud Provider												
Week	0	5	10	15	20	25	30	35	40	45	50	
B(w)	0	2566.01	3602.62	4081.52	4317.40	4437.37	4499.41	4531.76	4557.61	4557.61	4562.29	
C1(w)	C2(0)	0	0	0	0	0	0	0	0	0	0	
B(w)-C(w)		2566.01	3602.62	4081.52	4317.40	4437.37	4499.41	4531.76	4557.61	4557.61	4562.29	Bi
(1+d)^w	1.00	1.01	1.02	1.04	1.05	1.06	1.07	1.08	1.10	1.11	1.12	39030.02
B-C/(1+d)		2536.70	3520.80	3943.27	4123.52	4189.70	4199.75	4181.64	4157.46	4109.98	4067.21	
D=	0.0023											
Cloud Carrier												
Week	0	5	10	15	20	25	30	35	40	45	50	
B(w)	0	1121.17	1574.10	1783.35	1886.41	1938.83	1965.94	1980.08	1987.48	1991.37	1993.42	
C1(w)	C3(0)	0	0	0	0	0	0	0	0	0	0	
B(w)-C(w)		1121.17	1574.10	1783.35	1886.41	1938.83	1965.94	1980.08	1987.48	1991.37	1993.42	
(1+d)^w	1.00	1.01	1.02	1.04	1.05	1.06	1.07	1.08	1.10	1.11	1.12	Bi
B-C/(1+d)		1108.37	1538.35	1722.94	1801.70	1830.62	1835.01	1827.10	1812.98	1795.79	1777.10	17049.96
D=	0.0023											

Cloud Broker												
Week	0	5	10	15	20	25	30	35	40	45	50	
B(w)	0	916.67	1286.98	1458.06	1542.33	1585.18	1607.34	1618.90	1624.96	1628.14	1629.81	
C1(w)	C4(0)	0	0	0	0	0	0	0	0	0	0	
B(w)-C(w)		916.67	1286.98	1458.06	1542.33	1585.18	1607.34	1618.90	1624.96	1628.14	1629.81	
(1+d)^w	1.00	1.01	1.02	1.04	1.05	1.06	1.07	1.08	1.10	1.11	1.12	Bi
B-C/(1+d)		906.20	1257.75	1408.67	1473.06	1496.70	1500.30	1493.83	1482.29	1468.23	1452.95	13939.98
D=	0.0023										IC+NPV	

B
70025.52

Table 6-19: Comparative results across measures

Measure (M)	Threat (T)	Benefits (B) ($)	Investment Cost C(w) ($)	Return On Investment (ROI)%	Decision	Result Meanin
M3	T3	70,025.5	134018.62	0	Reject	The following results has been concluded:
			50% = 70025.5	1	Accept	* Whenever you pay Investment Cost C(w) that is ROI equal zero.
			Random = 50,000	0.40051		
			80,000	-0.12468	Reject	If IC=B then ROI=0 (No Rever
			200,000	-0.64987		
M8	T8	67,880.4	67880.3	0	Reject	* Whenever you decrease the IC whenever the ROI
			(50%) = 33940.2	1	Accept	If the IC < B the ROI>0 ROI is positive Measure is profita
			Random = 45,000	0.50845		
			80,000	-0.15150	Reject	
			200,000	-0.66060		
M11	T11	25,102.6	40,502.96	0	Reject	* Whenever you pay more than the Benefits (B) v this type of measu If IC>B ROI is Negativ Financial losse
			(50%) = 12551.3	1	Accept	
			Random = 15,000	0.67351		
			50,000	-0.16325	Reject	
			200,000	-0.87449		

6.5. Automated Tool

This tool reads all the MFC matrices from excel sheet and use of these data as a "Default Values" (as shown in Figure A-1), experts on cloud domain can re-adjust these default values when needed, in this case the automated tool will recalculate all the remaining entries on that column to keep balance of the MFC matrices using propagation formula, in this case automated tool will immediately recalculate the other values of this matrix to verify that each column have summation one, because this model assumed that only one event has been occurred at a time (one requirement has been violated at a time, one component has been compromised at a time and one threat has been materialized at a time), this will be done by ***propagating the difference*** between the remaining entries (as shown in Figure A-1 and Figure A-2) using the proposed equation. This proposed tool is ready now to calculate the MFC for each stakeholder by applying the MFC equation (as shown in Figure A-3), if any stakeholder need to deploy some countermeasures (which represent as a V&V actions), this will lead to reflect this enhancement measure values to appropriate MFC matrix, as example if a new provisioning and backup tool has been deployed, this will lead to "Decreases" the probability of "Data Loss" Threat and "Increase" the probability of No Threat "NoT", the remaining entries ***will be as it is*** (see Figure A-4 and Figure A-5) which represent the TV before and after applying appropriate measure, in such case of changing entries this tool identify where you change and display the result before and after applying this change, then an automated tool will recalculate the MFC (as shown in Figure A-6) to obtain the new result of the acquired countermeasure in term of reducing the MFC, this new value of MFC is is called the "MFC Gain" (see Figure A-7), moreover, this tool has a component that gain to calculate The Total Benefits from deploying the measure, Investment Cost for each stakeholder, NPV and the ROI by considering the number of stakeholders, discount rate, MFC Gain (Benefit) and the total investment cost using a lot of an associate equations, to facilitate entering data and for better understanding this tool assumed that benefits are not changed over the time (this step used as an evaluation approach for this study), inputs and output results are shown below.

Inputs:

- Number of stakeholders,
- Discount Rate,
- The MFC Gain in term of benefits and
- The overall cost of measure (the overall Investment Cost) - C(0)

Outputs:

- The Total benefits for all stakeholders – as shown in Figure A-8.
- The appropriate Investment Cost for each stakeholder Ci(0) in such away that makes all ROI Identical – as shown in Figure A-9.
- If C(0) < the Total of Benefits then → ROI Positive (which means this measure is profitable) – as shown in Figure A-10.
- If C(0) = the Total of Benefits then → ROI Zero (which means No Revenue – reject this measure) – as shown in Figure A-11.
- If C(0) > the Total of Benefits then → ROI Negative (which means Financial Losses – also reject this measure) – as shown in Figure A-12.

Accordingly, this tool illustrated an application of the MFC model for estimating system security by means of a concrete case study which is based on a real, empirical data and analytical reasoning which can assess the cost effectiveness of security measures for each stakeholder in such a way that make all ROI Identical which help to decide whether the measure is worthwhile or not by comparing it's investment cost against the benefits (for each stakeholder separately). This quantification tool of security attributes which considers the MFC to each stakeholder opens a wide range of possibilities for further economics based analysis, and provides a valuable resource for rational decision making. Figure 3-1 presenting the whole life cycle of the MFC which has been supported by this proposed tool using the decision based analysis.

6.6. Generating and Filling MFC Matrices using Service Base Model

This new expansion for creating MFC has been adapted with all cloud service models and This study proposed two aspects for generating and filling the MFC matrices using the "Service Base Model" either by considering (as shown in figure 5-4):

- *Option 1 :The position of security failure or*
- *Option 2 :The scope of control aspects*

6.6.1. Option 1: Position of Security Failure

- In table B-1 (which representing as INPUT layer) same entries with same 1st levels numbers have been assigned for all cells, in order to facilitate comparisons between failure impacts on each service model (which can be re-adjusted).
- In table B-2, Mapping these similar 1st levels No. (On each cell) to probability format (which representing as PROCESSING layer), when mapping this 1thlevel No to probability format it will give different results even it take the same 1thlevel No. inside each cell (as shown in table B-2),

because the impact of failures across these service models is differ, so the 2ed level is used to differentiate these impact of failure across cloud service models,

- Table B-3 (representing as OUTPUT layer) represent 1st level= 1 on (IaaS component intersect with SaaS requirement with probability = 0.007143) and also 1st level No.=1 on (IaaS component intersect with IaaS requirement with probability = 0.014286), however the criticality of security failure (2ed level No.) on IaaS is higher than the criticality on SaaS layer and this is what we mean by a *"Position of Failure"*.

6.6.2. Option 2: Scope of Control

The most important stakeholders on the cloud computing environment are cloud consumer and cloud provider who share the control of resources in a cloud system, so let's focus on these two stakeholders as basis of this model (and same thing will be done for the remaining stakeholders).

Scopes of Control tables are illustrated in the appendix (B), in:

- Table B-4 (which represented as INPUT layer), here different service models affect an organization's control over the computational resources which accordingly identify different scope of responsibilities,
- Table B-5 (which represented as PROCESSING layer) representing the DP Matrix (same thing will be done for the TIM Matrix), the 1st Level No. here assigned based on an impact of failures that used to identify which cloud component will affect to which security requirement and then 2ed Level No. represent which component will affect to which cloud stakeholder on each service model), and for ST and TV same proposed criteria for filling them could be applied (as in chapter 4), and then
- Table B-6 (which represented as OUTNPUT layer) this table helps understand the responsibilities of all parties involved in managing the cloud application (as a one of cloud component) same thing for all remaining components (runtime, middleware, hypervisor and OS components,), filling these MFC matrices is based on that scope of responsibilities.

Accordingly, 2ed Level No. here assigned based on an impact of failures which is relevant to the "*scope of control"* rather than the position of failure this model is based on the classification that has been proposed by NIST (refer to table B-4 and table B-5), and again this 1st Level No. were mapped to probability format using the same mentioned criteria for mapping (refer to chapter 4) and this will be shown in table B-6, as mentioned before the 2ed levels No. represent:

- 2ed Level L2=2: This level means some components are *managed by* some cloud stakeholders (the site who provide the service), so the *highest* impact of failure will exist here.

- 2ed Level L1=*1*: This level means some components are *used by* some cloud stakeholders (this is the side which consumes the service), so the impact of failure here is *less* than Level 2.
- 2ed Level L0=0: This level means some components are *hidden from* some cloud stakeholders (as example, the middleware layer is hidden from SaaS Consumer) which means "No Impact" and lead 2edLevel=0.

6.7. Recommendations for acquiring Better Results for MFC and ROI

A lot of obstacles including security issues that will negatively affect the consumers of cloud services, accordingly twelve threats has been considered by CSA which provide some enhanced practices and guidelines that may give opportunities for avoiding or mitigating the impact of these threats, table 6-20 present this CSA guidelines (CSA 2016) (Sunil Batra, 2013), (Vahid Ashktorab and Seyed Reza, 2012).

Some threat materializes, which may affect components that may affect requirements that may affect costs. Accordingly CSA and NIST proposed huge catalogue and guidelines, which are all relevant to how detect and minimize the impact of that failure, too many companies follow their guidelines to obtain better QoS and to provide an acceptable cloud computing services either on software level, platform level or infrastructure level. The following table 6 20 takes some snapshots of these measures that may be used to obtain better MFC, ROI and NPV results.

Table 6-20: The main security threats and its guidelines (CSA 2016)

T	Threat	(Cyber-security measures By CSA)
T1	Data Breaches	M1 - Deploy Application and Interface Security mechanisms. - Deploy Threat and Vulnerability Management tools– Anti-Virus/Malicious Software. - Encrypt the protected data. - Avoid a single point of failure by using efficient and strong two-factor authentication techniques where possible. - Implement strong key generation.
T2	Weak Identity, Credential and Access Management	M2 - Using the Multi-layers authentication systems - Support verification of strong password. - Organization should define rotation period policies. - Encrypt the protected data.
T3	Insecure APIs	M3 - Deploy Threat and Vulnerability Management tools– Anti-Virus/Malicious Software. - Analyze the security model of cloud provider interfaces. - Ensure and validate that comprehensive and strong authentication and access controls are implemented with encrypted transmission data. - Understand the dependency chain associated with the API.
T4	System and Application Vulnerabilities	M4

		- Deploy Application and Interface Security mechanisms (Application Security- Data Integrity). - Business Continuity Management and Operational Resilience Documentation. - Patching Threat and Vulnerability Management – Patch Management - Application Hardening, OS Hardening and Base Controls.
T5	Account Hijacking	M5
		- Avoid the sharing of account data between users and services. - Avoid single point of failure. - Employ efficient monitoring process to detect unauthorized activities. - Understand cloud provider security policies and SLAs.
T6	Malicious Insiders	M6
		- Strictly supply chain management and conduct a comprehensive supplier assessment. - Specify human resource requirements as part of legal contracts. - Require transparency into overall information security and management practices, as well as compliance reporting. - Determine security breach notification processes.
T7	Advanced Persistent Threats (APTs)	M7
		- APTs may require more advanced security controls, process management, incident response plans and IT staff training, - Awareness programs that are regularly reinforced are one of the best defenses against these types of attacks

		- Audit Logging/Intrusion Detection.
T8	Data Loss	M8
		- Implement strong API access control. - Encrypt and protect integrity of data. - Analyze data protection at both design and run time. - Implement strong key generation, storage and management. - Contractually specify provider backup.
T9	Insufficient Due Diligence	M9
		- Disclosure of applicable logs and data. - Partial/full disclosure of infrastructure details (e.g., patch levels, firewalls, etc). - Monitoring and alerting on necessary information. On SLA identify all details.
T10	Abuse and Nefarious Use of Cloud Services	M10
		- Strong initial registration and validation processes. - Apply strong strategy to improve the coordination and credit card fraud monitoring. - Full monitoring of customer network traffic. - Monitoring public blacklists for one's own network blocks.
T11	Denial of Service	M11
		- Apply Capacity/Resource Planning. - Monitoring the Equipment Power Failures. - Conducing security aspects on application.
T12	Shared Technology Issues	M12
		- Implement security best practices for installation/configuration. - Monitor environment for unauthorized changes/activity. - Promote strong authentication and access control for administrative access and operations.

		- Enforce service level agreements for patching and vulnerability treatment and handling. - Conduct vulnerability scanning and configuration audits.

The purpose of this study would be to observe the investigations and assessments made by threat analysts in their process of categorizing threat in a cyber environment. Future studies would be necessary to:

- Collect an analytical and empirical data that are relevant with M2FC and SBMFCM in order to make this task systematic.
- Compare the obtained results across cloud service models.
- Proposing other econometrics measures and compares the results of this proposed measure with the other econometrics measures.
- Apply the proposed measure on a real environment to determine to what extent this measure is powerful.
- Compare the currently obtained results with the future results.
- Build a Sudanese standard metrics for security threats or customize the proposed one to be adapted with Sudanese data centers that may help them in term of security failures.

This study discussed and illustrated a cyber-security metric which believed it's highly adapted with cloud computing aspects. The greatest challenge to the widespread use of this metric in the management of cyber-security is the need to fill all the MFC matrices that are needed to compute it by using an empirical data.

Conclusion

In spite of taking into account all the mentioned advantages when using cloud computing, there are still obstacles that may be found, these obstacles need to be sorted through a collaboration of cloud providers, customers, and regulatory bodies nationally and internationally. Until these obstacles are solved, the use of cloud computing continues to be a tradeoff of achieving the benefits shown earlier against taking the risks, the MFC used the cost benefit analysis which estimate these benefits, which used as a function that quantifies the statistical mean of a random variables that represents a loss by a system stakeholder as a result of security failure, so the MFC model has been adapted to Cloud Computing by considering in turn: the set of typical stakeholders, the set of typical security requirements, standard system architecture, and a standard threat vector, all the relevant matrices and vector with cloud-relevant has been filled using empirical data with analytical reasoning that complying the distribution probability rules. Not all the relevant data is

available, so this study did have to make some assumptions and some approximations, and our results are only as good as these I accepted. Nevertheless, we feel that our cloud-specialized model gave a broad framework, because in the absence of a clear refinement of the framework numerous, information security metrics might be found and lead to vague results, so this study proposed a framework which is clearly defined, refined and measured.

When moving to mission-critical systems, cloud companies pay a lot of cash to gain large revenue; however, the investment doesn't always deliver the hoped revenue, so this study proposed a novel econometric approach that can be used to estimates this revenue by investigating the cost benefit analysis approach by using the ROI with NPV aspects which represented as evaluation measure that help decision makers to decide the desirability of deploying and operating the countermeasures, and also it is useful when we have different scenarios and we need to select one of them.

For reasoning about security-related stakes and costs, this study has briefly discussed an automated tool which aims to fill all MFC matrices based on empirical data and analytical reasoning and expected results are achieved. This tool computes the MFC of a Cloud Computing installation; in particular, it discussed how it can be adapted to a particular cloud installation using installation-specific knowledge.

REFERENCES

1. Abercrombie, R.K. et al., 2013. Risk assessment methodology based on the NISTIR 7628 guidelines. Proceedings of the Annual Hawaii International Conference on System Sciences, pp.1802–1811.
2. Aissa, A. Ben et al., 2010a. Modeling stakeholder/value dependency through mean failure cost. Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, pp.55–57. Available at: http://portal.acm.org/citation.cfm?doid=1852666.1852727.
3. Aissa, A. Ben et al., 2010b. Quantifying security threats and their potential impacts: a case study. Innovations in Systems and Software Engineering, 6(4), pp.269–281. Available at: http://link.springer.com/10.1007/s11334-010-0123-2 [Accessed October 6, 2014].
4. AIT, 2014. Methodology for Risk Assessment and Management , Secure Cloud computing for CRitical infrastructure IT, (312758).
5. Alberto, C. & Ferreira, A.S., 2012. A Methodology for Management of Cloud Computing using Security Criteria.
6. Amazon, 2015. Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region. , p.6. Available at: http://aws.amazon.com/message/65648/.
7. Antonopoulos, N. & Gillam, L., 2010. Cloud Computing: Principles, Systems and Applications. Media, 54, p.379. Available at: http://dx.doi.org/10.1007/978-1-84996-241-4_20.
8. APTA, 2014. Cybersecurity Considerations for Public Transit. AP T A S T AN D AR D S D E V E L O PME N T P ROG R AM, Enterprise(RECOMMENDED PRACTICE, American Public Transportation Association, 1666 K Street, NW, Washington, DC, 20006-1215 APTA, Enterprise Cyber Security Working Group).
9. Avram, M.G., 2014. Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. Elsevier Ltd, Procedia Technology, 12, pp.529–534. Available at: http://www.sciencedirect.com/science/article/pii/S221201731300710X.
10. Barry, B., LiGuo, H., 2003. Value-based software engineering: a case study. IEEE Computer 36 (3), 33–41
11. Barry, B., 2006. Value-based software engineering: overview and agenda. In: Biffl, S., Aurum, A., Boehm, B., Erdogmus, H., Gru ¨ nbacher, P. (Eds.), Value-Based Software Engineering.
12. Beimborn, D., Miletzki, T. & Wenzel, S., 2011. Platform as a service (PaaS). Business and Information Systems Engineering, 3(6), pp.381–384.
13. Blakley, 2001. An Imprecise but Necessary Calculation. Secure Business Quarterly.
14. Bliss, R., Jordan, S. & Kiser, C.Y., 2015. Project ROI Defining the Competitive and Financial

Advantages of Corporate Responsibility and Sustainability.

15. Bodeau, D., Fabius-greene, J. & Graubart, R., 2010. How Do You Assess Your Organization ’ s Cyber Threat Level ? , pp.1–11.
16. Boehme, R. & Nowey, T., 2008. Economic security metrics. Dependability Metrics: Advanced Lectures, 4909, pp.176–187.
17. Bohn, R., 2016. Cloud Computing Standards – A NIST Perspective NIST ’ s Goal To accelerate the federal government ’ s. Nist, (January).
18. Boniface, M. et al., 2010. Platform-as-a-Service Architecture for Real-time\nQuality of Service Management in Clouds. Available at: http://eprints.ecs.soton.ac.uk/21078/.
19. Botchkarev, A. & Andru, P., 2011. A return on investment as a metric for evaluating information systems: Taxonomy and application. Interdisciplinary Journal of Information, Knowledge, and Management, 6, pp.245–269.
20. Brian, O. et al., 2012. Cloud computing. Swiss Academy of Engineering Sciences (SATW) White Paper. Available at: http://www.ncbi.nlm.nih.gov/pubmed/22352137.
21. Carlson, F.R. & Petersburg, S., 2011. Security Analysis of Cloud Computing.
22. Cloud Standards Customer Council, 2015. Practical Guide to Cloud Service Agreements Version 2.0.
23. CSA, 2016. Cloud Computing Top Threats in 2016: Treacherous 12. Online, (February).
24. CSA, 2013a. Cloud Computing Vulnerability Incidents: A Statistical Overview. Cloud Security Alliance, p.21.
25. CSA, 2009. Security Guidance Critical Areas of Focus for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance (CSA), Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, 1(December), pp.1–76. Available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Security+Guidance+Critical+Areas+of+Focus+for#0.
26. CSA, 2013b. The Notorious Nine. Cloud Computing Top Threats in 2013. Security, (February), pp.1–14. Available at: http://www.cloudsecurityalliance.org.
27. Dawoud, W., Takouna, I. & Meinel, C., 2010. Infrastructure as a Service Security : Challenges and Solutions. Security, (May 2016), pp.1–8. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5461732.
28. Deac, A., The Top 10 Worst Cyber Security Breaches from 2013-2015 _ TruShield. Available at: file:///E:/sem3/Ref-ch1/The Top 10 Worst Cyber Security Breaches from 2013-2015 _ TruShield.htm [Accessed June 15, 2015].

29. Dixit, S., 2015. Effect of Cloud Computing on Enterprises : A Review. , 109(5), pp.5–10.
30. Engineers, F., 2015. More Details on Today ' s Outage. , pp.9–11.
31. European Network and Information Security Agency (ENISA), 2016. ENISA Threat Landscape 2015. , (December), pp.67–70. Available at: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-mid-year-2013.
32. Friedman, A.A. & West, D.M., 2010. Privacy and Security in Cloud Computing,
33. G.Somasekhar, 2013. Big Data as a Service. International Journal of Computer Science & Engineering Technology (IJCSET) CLOUD, 4(Lxx), pp.1–7.
34. Gordon, L.A., Loeb, M.P, 2006. Budgeting Process for Information Security Expenditures, Communications of the ACM 49.
35. Jackson, K.L. et al., 2012. Platform as a Service (PaaS) An NJVC and Virtual Global Executive. , (January), pp.1–16.
36. Jackson, K.R., 2015. Discovery 2015 : Cloud Computing Workshop Introduction to Cloud Computing.
37. Jan Colpaert, 2015. CLOUD FOR EUROPE. RISK ANALYSIS, CERTIFICATION AND OTHER MEASURES, VOLUME 1.0(RISK,), p.D9.5 Required Measures from cet.
38. Jawad, D. & Ozbay, K., 2006. the Discount Rate in Life Cycle Cost Analysis of. Transportation Research, pp.1–19.
39. Jin;, Michael D. Hogan; Fang Liu; Annie W. Sokol; Tong, N., 2011. N I S T C l o u d C o m p u t i n g S t a n d a r d s R o a d m a p. , p.76 pp. Available at: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909024.
40. Jouini, M. et al., 2012. Towards quantitative measures of Information Security : A Cloud Computing case study. , 1(3), pp.248–262.
41. Khurana, S. & Verma, A.G., 2013. Comparison of Cloud Computing Service Models : SaaS , PaaS , IaaS. International Journal of Electronics & Communication Technology, 7109, pp.29–32.
42. Kooten, G.C. Van, 2016. Agricultural economics and policy analysis.
43. Lee Badger, Robert Bohn, Shilong Chu, Mike Hogan, Fang Liu, Viktor Kaufmann, J. & Mao, John Messina, Kevin Mills, Annie Sokol, Jin Tong, F.W. and D.L., 2011. US Government Cloud Computing Technology Roadmap Volume II Release 1 . 0 (Draft) Useful Information for Cloud Adopters. , II.
44. Liu, F. et al., 2011. NIST Cloud Computing Reference Architecture Recommendations of the National Institute of Standards and Technology.
45. Maarten Gehem, Artur Usanov, Erik Frinking, M.R., 2015. ASSESSING CYBER SECURITY

The Hague Centre for Strategic Studies. ISBN/EAN: 978-94-92102-12-6, Hoffmann B(The Hague Centre for Strategic Studies).

46. Macdermott, Áine, Shi, Qi, Merabti, Madjid, Kifayat, K., 2014. An elastic scaling method for cloud security. Journal of Internet Technology and Secured Transactions (JITST), 3(3/4), pp.254–262.
47. Marinos, L., 2013. ENISA Threat Landscape 2013 - Overview of current and emerging cyber-threats,
48. Marinos, L. & Sfakianakis, A., 2012. ENISA Threat Landscape - Responding to the Evolving Threat Environment. Enisa, p.96. Available at: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport.
49. Marta, E. & Calderon, C., 2007. A Taxonomy of Software Security Requirements. Avances en sistemas e informatica, 4(3), pp.47–56.
50. Mccready, S., 2005. TCO , NPV , EVA , IRR , ROI Getting the Terms Right. , pp.1–7.
51. Meenakshi, A.C., 2012. An overview on cloud computing technology. International Journal of Advances in Computing and Information Technology, 1(2), pp.219–223.
52. Mell, P., Grance, T. & Grance, T., 2011. The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology.
53. Mili, A. & Sheldon, F., 2007. Measuring reliability as a mean failure cost. Proceedings of IEEE International Symposium on High Assurance Systems Engineering, pp.403–404.
54. Mishra, A. et al., 2013. Cloud Computing Security.
55. Mondal, R.K. & Sarddar, D., 2015. Utility Computing. International Journal of Grid Distribution Computing, 8(4), pp.115–122.
56. Ms. Shubhangi Ashok Kolte1, P.P.E.A. & M.Sc., 2016. A survey on cloud computing. IJARCCE, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 4, 58(December), pp.55–58. Available at: http://unbreakablecloud.com/wordpress/wp-content/uploads/2011/02/A-Survey-On-Cloud-Computing.pdf.
57. Nahla Murtada, N., 2013. Measuring the cybersecurity of cloud computing: A stakeholder centered economic approach. Proceedings - 2013 International Conference on Computer, Electrical and Electronics Engineering, ICCEEE 2013, pp.294–299.
58. Nahla Murtada, 2016a. Comperhensive Model for Building Presice MFC Matrices for Cloud Computing. In 10TH INTERNATIONAL CONFERENCE ON COMPUTING IN ARABIC (ICCA).

59. Nahla Murtada, 2016b. Measuring Cloud Security Risk by Mean Failure Cost, 2016 IEEE Symposium Series on Computational Intelligence (IEEE SSCI 2016) Technical Program Committee, pp.1–8.
60. NIST, 2014. NIST Cloud Computing Forensic Science Challenges. , p.51.
61. NIST, 2011. NIST Cloud Computing Reference Architecture & Taxonomy Working Group.
62. NIST, 2013. NIST Cloud Computing Standards Roadmap.
63. NIST, 2012. The attached DRAFT document (provided here for HISTORICAL purposes) has been superseded by the following publication :
64. NSA Information Assurance Service Center, 2013. Cloud Security Considerations. , (October).
65. Ponemon Institute, 2013. 2013 Cost of Data Center Outages. , (December).
66. Ponemon Institute, 2016. Cost of Data Center Outages in January 2016, Sponsored by Emerson Network Power. , (Data Center Performance Benchmark Series).
67. Ponemon Institute, 2010. National Survey on Data Center Outages. , (September).
68. Prof. Sonika A. Chorey*1, P.P.V.M. and P.R.S.S., 2016. G Lobal J Ournal of E Ngineering S Cience and R Esearches Experimental Investigation of Weld Bead Hardness of Tig. , 1(3), pp.36–42.
69. Publique, M.E. et al., 2007. Discount rate. , pp.1–2.
70. Purser, S.A., 2004. Improving the ROI of the security management process Computers & Security, 23(7), pp.542-546.
71. Putri, N.R. & Mganga, M.C., 2011. Enhancing Information Security in Cloud Computing Services using SLA Based Metrics. Blekinge Institute of Technology, (January), pp.1–75.
72. Quest Technology Management for Buisiness, 2015. The Benefits and Challenges of Cloud Computing. , 32(7), p.2015.
73. Quest Technology Management for Business, 2015. The Benefits and Challenges of Cloud Computing. , 32(7), p.2015.
74. Rabai, M.J. and L.B.A., 2014. A Security Risk Management Metric for Cloud Computing Systems A Security Risk Management Metric for Cloud Computing Systems. International Journal of Organizational and Collective Intelligence, 4(3), 1-21, July-September 2014 1 A, (November).
75. Rjaibi, N. & Aissa, A. Ben, 2013. a Basic Security Requirements Taxonomy To Quantify Security Threats : an E-Learning Application. , pp.96–105.
76. Scarfone, P.E.B. and K., 2008. Cyber Security Metrics and Measures. , (November). Available at: https://www.researchgate.net/publication/227988213.

77. Shostack, A., 2014. Threat Modeling Designing for security Second Edi., Indiana: WILEY.
78. Singh, K. & Negi, S., 2015. Service Model Specific Security Requirements and Threats in Cloud Computing. , 5(7), pp.851–855.
79. Slezak, D., 2008. A Study on The Cryptosystem in a Trusted Computing Platform. , pp.57–64.
80. Somasekhar, G., 2013. CLOUD COMPUTING WITH BIG DATA AS A SERVICE. , 4(8), pp.1201–1208.
81. Sonnenreich, W., Albanese, J. & Stout, B., 2006. Return on security investment (ROSI) - A practical quantitative model. Journal of Research and Practice in Information Technology, 38(1), pp.45–56.
82. Speaks, S., 2002. Reliability and MTBF Overview. Vicor Reliability Engineering, pp.2–10. Available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Reliability+and+MTBF+Overview#0.
83. Srinivas, A., Srinivas, M.K. & Varma, A.V.R.K.H.V., 2013. A Study On Cloud Computing Data Mining. International Journal of Innovative Research in Computer and Communication Engineering, 1(5), pp.1232–1237.
84. Standards, C. & Council, C., 2016. Cloud Customer Architecture for IoT. , pp.1–22.
85. Stanley, S., 2011. Explanation of terms. IMC Network, 9(4), pp.30–31.
86. Symantec, 2015. Internet Security Threat Report. Istr, 20(April).
87. Symantec, 2014. Internet Security Threat Report. Internet Security Threat Report, 20(April). Available at: https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.
88. Talukder, A., Zimmerman, L. and Prahalad, A., 2010. Cloud Economics: Principles, Costs, and Benefits In Cloud Computing, Springer London, pp.343-360.
89. Tear, T.H. et al., 2014. A return-on-investment framework to identify conservation priorities in Africa. Biological Conservation, 173, pp.42–52. Available at: http://dx.doi.org/10.1016/j.biocon.2014.01.028.
90. Venkatesh, V. & Brown, S.A., 2013. BRIDGING THE QUALITATIVE – Q UANTITATIVE D IVIDE : G UIDELINES FOR C ONDUCTING M IXED M ETHODS. MIS Quaterly, 37(1), pp.21–54.
91. Verizon, 2014. 2014 Data Breach Investigations Report. Verizon Business Journal, 2014(1), pp.1–60. Available at: file:///C:/Users/Edward S. Forde/Downloads/rp_Verizon-DBIR-2014_en_xg.pdf.

92. Walraven, S. et al., 2015. PaaSHopper : Policy-driven middleware for multi-PaaS environments.
93. Wang, L. et al., 2010. Cloud computing: a perspective study. New Generation Computing, 28(2), pp.137–146.
94. Wu, D. et al., 2010. Analysis of stakeholder/value dependency patterns and process implications: a controlled experiment. System Sciences (HICSS), 2010 43rd Hawaii International Conference on, pp.1–10. Available at: http://www.computer.org/csdl/proceedings/hicss/2010/3869/00/02-02-04.pdf.
95. Wu, D. et al., 2008. Analysis of Stakeholder / Value Dependency Patterns and Process Implications : A Controlled Experiment.
96. Yahya, F., Walters, R.J. & Wills, G.B., 2015. Modelling Threats with Security Requirements in Cloud Storage. International Journal for Information Security Research (IJISR), 5(2), pp.551–558.
97. Yigitbasioglu, O.M., Mackenzie, K. & Low, R., 2013. Cloud Computing: How does it differ from IT outsourcing and what are the implications for practice and research? The International Journal of Digital Accounting Research, 13(April), pp.99–121.
98. Zhang, X. et al., 2010. Information Security Risk Management Framework for the Cloud Computing Environments. 2010 10th IEEE International Conference on Computer and Information Technology, (2007), pp.1328–1334. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5577860.
99. Žižlavský, O., 2014. Net Present Value Approach: Method for Economic Assessment of Innovation Projects. Procedia - Social and Behavioral Sciences, 156(April), pp.506–512. Available at: http://www.sciencedirect.com/science/article/pii/S1877042814060509.