Measuring Cloud Security Risk by Mean Failure Cost

Nahla Murtada Ahmed
Software Engineering Department
Sudan University of Science and Technology (SUST)
Sudan, Khartoum
Nahla.rida@gmail.com

Abstract—**The Mean Failure Cost (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 is security breaches, the MFC can be used to quantify specifically the loss that results from violations of security requirements, such as confidentiality, integrity, availability, etc. In this paper we consider the application of the Mean Failure Cost model to reference cloud architecture.**

Keywords— Cyber security, Cloud Computing, Mean Failure Cost, MFC dimension, cloud stakeholders, cloud architecture, threat.

I. INTRODUCTION

Whereas reliability is usually measured by Mean Time To Failure (MTTF), a number of similar measures have been proposed to quantify the cybersecurity of a system. These include MTTD (Mean Time To Detection): the mean time it takes for perpetrators to detect vulnerability, MTTE (Mean Time to Exploitation): the mean time it takes perpetrators to exploit a detected vulnerability, MTTR (Mean Time To Repair), etc. Broadly speaking, these metrics fail to consider the following attributes:

- Variance in stakeholders' needs and requirements. Different stakeholders have different stakes in the secure operation of the system.
- Variance in failure (impact, severity, count). A system may have a wide range of security requirements; failure is not a monolithic event. Rather, it is important to consider failures with respect to different requirements as distinct events.
- 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 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.

Until now there are no statistics on the volume of estimating failure cost on Cloud Computing environment per a unit of time.

This paper discusses the effort to adapt 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 vector of threats of a Cloud Computing environment.
- The typical cyber-security threats of cloud providers and other cloud stakeholders along with their probability of occurrence per a unit of time.

Consider a system S that has many stakeholders, say H1, H2, H3… Hn. Then define the random variable Xi as the loss that stakeholder Hi stand to sustain as a result of possible security failures in system S. Then let the MFC be defined for stakeholder Hi as the statistical mean of variable Xi. Refer to this quantity as the MFC of stakeholder Hi, and denote it by MFC(Hi). The vector of all MFC(Hi) values for all stakeholders is denoted simply by MFC [1].

According to Ben Aissa etal. A formula is given for computing the mean failure vector as in (1):

$$MFC = ST \bullet DP \bullet IM \bullet TV \qquad (1)$$

Where

A. *ST, **the Stakes matrix,*** has as many rows as we have stakeholders and as many columns as we have security requirements.

This matrix represents the co-relation between stakeholders and security requirements; specifically, it represents the stakes that each stakeholder has in meeting each security requirement 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. We produce the stakes matrix as shown in table 1 [2] [3] [4] [5] [6] [7] [8].

B. *DP, **the Dependability matrix,*** has as many rows as we have security requirements and as many columns as we have cloud components.

The dependability matrix produces a co-relation between security requirements and its components; specifically, it represents the probability of requirements failure given that specific component has been compromised as shown in table 2 [9] [10] [11] [12] [13] [14] [15].

C. *IM, the* ***Impact matrix,****h*as as many rows as there are components in the cloud architecture and as many columns are there cyber threats being considered.

The 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 [16] [17].

D. *TV, the* ***Threat vector,*** is a column vector that has as many entries as there are threats under consideration.

Threat Vector (TV) in table 4 characterizes the threat situation by assigning to each threat the probability that this threat will materialize in a unitary period of time (e.g., an hour) [10] [11] [17] [19] [20].

TABLE 1:STAKE MATRIX

ST	**Security requirements on Cloud Computing ($)**						
Cloud Stakeholders		***Authentication***	***Authorization***	***Confidentiality***	***Data Integrity***	***Availability***	***NRF***
	Cloud Consumer	30$	24$	30$	40$	50$	0$
	Cloud Provider	90000$	80000$	100000$	90000$	900000$	0$
	Cloud Carrier	40000$	30000$	70000$	20000$	13000$	0$
	Cloud Broker	40000$	35000$	68000$	19000$	14000$	0$
Note: The NRF row represents the case if "No Requirement has been Failed" means no stakeholder has been affected in term of financial loss.							

TABLE 2: Dependability MATRIX [11] [16] [17]

DP	**Cloud Components**							
Cloud Requirements		***Applications***	***Runtime***	***Middleware***	***OS***	***Hyper visor***	***Infrastructure***	***NCV***
	Authentication	0.057	0.107143	0.125	0.21	0.163636	0.085714	0
	Authorization	0.057	0.107143	0.125	0.21	0.163636	0.085714	0
	Confidentiality	0.057	0.107143	0.125	0.14	0.109091	0.085714	0
	Data Integrity	0.15	0.214286	0.25	0.07	0.054545	0.171429	0
	Availability	0.225	0.214286	0.125	0.07	0.109091	0.171429	0
	NRF	0.4	0.25	0.25	0.3	0.4	0.4	1
Note: The intersection between NCV with NRF means if "No Component has been "Compromised" that means "No Requirement has been "Violated", and leads to event (NCV intersect with NRF) with probability 1.0.								

TABLE 3: IMPACT MATRIX [15] [16] [17]

IM	**Cloud Threat**													
Cloud Component		***Data Breaches***	***Weak Identity, Credential and Access Management***	***Insecure APIs***	***System and Application Vulnerabilities***	***Account Hijacking***	***Malicious Insiders***	***Advanced Persistent Threats (APTs)***	***Data Loss***	***Insufficient Due Diligence***	***Abuse and Nefarious Use of Cloud Services***	***Denial of Service***	***Shared Technology Issues***	***NoT***
	Application	0.1	0.1	0.0818	0.20769	0.095	0.15	0.09889	0.088	0.1	0.1636	0.18	0.18	0
	Runtime	0.2	0.1	0.1636	0.20769	0.143	0.225	0.19778	0.176	0.2	0.1636	0.18	0.18	0
	Middleware	0.2	0.1	0.1636	0.13846	0.095	0.15	0.19778	0.176	0.2	0.0818	0.18	0.18	0
	OS	0.2	0.1	0.1636	0.06923	0.143	0.225	0.19778	0.176	0.2	0.1636	0.18	0.18	0
	Hyper visor	0.1	0.0667	0.1636	0.06923	0.048	0.075	0.09889	0.088	0.1	0.1636	0.09	0.09	0
	Infrastructure	0.1	0.0333	0.1636	0.20769	0.047	0.075	0.09888	0.176	0.1	0.1636	0.09	0.09	0
	NCV	0.1	0.5	0.1	0.1	0.43	0.1	.11	.12	0.1	0.1	0.1	0.1	1
Note: The intersection between NoT with NCV means if "No Threat has "Materialized" that means "No Component has been "Compromised", and leads to event (NoT intersect with NCV) with probability 1.0.														

TABLE 4: THREAT VECTOR [19] [20]

TV	
Cloud Threat	***Probability***
Data Breaches	6.76967E-06
Weak Identity and Access Management	7.96432E-07
Insecure APIs	6.76967E-06
System and Application Vulnerabilities	5.30955E-07
Account Hijacking	3.98216E-07
Malicious Insiders	3.98216E-07
Advanced Persistent Threats (APTs)	1.99108E-06
Data Loss	5.70776E-06
Insufficient Due Diligence	1.46013E-06
Abuse and Nefarious Use of Cloud Services	1.59286E-06
Denial of Service	5.30955E-06
Shared Technology Issues	6.63693E-07
NoT	0.999967612
NoT: Means that No Threat has been materialized.	

All these metrics are flexible in contents and structure, the contents can be filled or updated by the responsible person(s), and the structure can be changed by adding/removing either row/column, these responsible person(s) are show in table 5.

TABLE 5: MFC METRICS and RESPONSIBLE SPECIALIST FILLING IT

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

II. 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 models: Software as a Service applications (SaaS) are designed for end-users, delivered over the web, Platform as a Service (PaaS) is the set of tools and services designed to make coding and deploying those applications quick and efficient and Infrastructure as a Service (IaaS) is the hardware and software that powers it all – servers, storage, networks, operating systems [3] [4] [5] [6].

III. MFC PARAMETERS

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 occurs per time. The main parameters of MFC metric are [1] [2]:

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

Each service model (IaaS, PaaS and SaaS) has its own MFC parameters, so the following sections will consider these parameters for each service model.

IV. MFC DIMENSIONS

A. Cloud stakeholders

This paper recognizes five stakeholders in Cloud Computing environment, namely, the cloud consumer, the cloud provider, cloud carrier, cloud broker and cloud auditor. We briefly review the stakes that they have in meeting the security requirements, which determine the corresponding values in the stakes matrix [2] [3] [4] [5] [6] [7].

- Cloud Consumer: The person or organization that uses the Cloud Computing services. And uses the service from, a cloud provider.
- Cloud Provider: A cloud provider is the entity (a person or an organization) responsible for making a service available to 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.

TABLE 6: CLOUD STAKEHOLDERS FOR EACH SERVICE MODEL [21][22][23]

Cloud stakeholders	
Service model	**Associated stakeholders**
	Cloud Consumers
SaaS	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

According to National Institute of Standards and Technology (NIST), the following table 6 identifies the cloud stakeholders for each service model.

B. Cloud security requirements

We adopt the following security requirements for Cloud Computing identified as follow [2] [3] [8] [9] [10] [11]:

- 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 concern on 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 incumbent on managing entities of cloud providers to have robust identity management architecture.

According to NIST, the following table 7 identifies the security requirements for each service model.

TABLE 7: CLOUD SERCURITY REQUIREMENT FOR EACH SERVICE MODEL [21]

Main service model	Associate-requirement
IaaS	Hardware security Hardware reliability Infrastructure control Network resources protection High confidentiality High availability
PaaS	Application security Data security Access control Communication security

SaaS	Integrity Confidentiality Availability Privacy Service availability Software security

And accordingly when identifying stakeholders and its security requirements this will lead to introduce a new matrix which is called “Stake Matrix” that aims to identify the stake that each stakeholder has in meeting each clause of the security requirements specification (as shown in table 1).

C. Cloud components

This section represents a standard generic cloud computing architecture that specifies common Cloud Computing components [13] [14] [15] [16] [23] which are:

- Applications: The special applications used by a business.
- Runtime: The environment in which the chosen application is executed, including the runtime library of the application’s requisite functions.
- Middleware: Used for switching software for communication with other applications, databases and the operating system.
- OS: provides and manages the system resources of the hardware.
- Hypervisor: It is virtualization layer that used to virtualized infrastructure resources to the operating system.
- Infrastructure: It consists of the physical units, such as servers, CPU, storage, and the network.

According to NIST, the following table 8 identifies the component for each service model.

TABLE 8: CLOUD components FOR EACH SERVICE MODEL [23] [25]

Main service model	Associate-Components
IaaS	Virtual machine Computing capabilities for handling workloads (Servers, switches, routers) Load balancers Network and Internet connectivity Computer hardware and physical storage (Storage media, processor and ram).
PaaS	Database Webserver Development tools Component for all OS capabilities. Middleware Deployment tool Software for application
SaaS	Virtualdesktop Communication Presentation component Security component Application component Operation component Infrastructure component

And accordingly when identifying security requirements and cloud components, this will lead to introduce a new matrix which is called “Dependability Matrix”, this relation reflects to what extent that each component contributes to meet each security requirement (as shown in table 2).

D. Cloud Threats

Experts identify the following 12 critical issues to cloud security (ranked in order of severity) [10] [11] [17]:

- 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.
- 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.
- Insecure Application Programming Interfaces: It is relatively weak set of interfaces and APIs. Insecure API that the Cloud Computing providers usually expose, it is relatively weak set of interfaces and APIs.
- 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, fraud, reusing the password and unauthorized activity).
- Malicious Insiders: When malicious inside organization has access to everything, this malicious insider is intentionally causing damage by exceeding or misusing that access.
- Advanced Persistent Threats (APT): It is a network attack where an unauthorized user gains access to a network and stays for a long period of time without being detected.
- Data Loss/Leakage: This threat occurs due to deletion or alteration of records without a backup of the original content or loss of an encoding key.
- Insufficient Due Diligence: In this type of threat, the consumer does 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.
- Abuse and Nefarious Use of Cloud Computing: Providers offer unlimited resources (such as network bandwidth, memory, storage capacity etc.) to their customers which may lead anyone (may be hacker) immediately begin using cloud services.
- Denial of Service (DOS): When the attacker are attacks to prevent users 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.

- Shared Technology Issues: Cloud service providers deliver their services by sharing infrastructure (such as platforms, runtime and applications) for different consumers that do not support strong isolation properties for multiple stakeholders.

According to NIST, the following table 9 identifies the threats on Cloud Computing for each service model.

TABLE 9: CLOUD THREATS FOR EACH SERVICE MODEL [24]

Service model	Associated Threats
IaaS Threat	Hardware theft Hardware modification Hardware interruption Network attacks Connection flooding DDOS (Distributed Denial of Service) Misuse of infrastructure Storage devices Attack. VMs provisioning and migration.
PaaS Threat	Exposure in network/network attack Session hijacking Software modification Traffic flow analysis Disrupting communication Software interruption or deletion DDOS Impersonation
SaaS Threat	Privacy breach Traffic flow analysis Exposure in network/network attack Session hijacking Data interruption (deletion) Interception on access control Impersonation Modification of data at rest/transit. Application and Interface Security attack Interception on access control

And again 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 “Impact Matrix” as shown in table 3, and threat is represented by a vector of probabilities of occurrence in case of security breakdowns per a unit of time as shown in table 4, this vector is called “Threat Vector”.

V. GENERATING MFC METRICS

This part represents how the MFC metrics will be generated based on analytical reasoning and some 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.

A. ***Stake Matrix****:* This matrix has been proposed based on rationale and some material that comparing the cost aspects between cloud stakeholders, as example: cloud provider always pays the highest value of money comparing to other stakeholders, however the case of cloud consumer is opposite; and cloud broker and cloud carrier pay median cost comparing to cloud provider and cloud consumer, we are assuming here that the most reliable data is that data that has been published in CSA report (Cloud Security Alliance).

B. ***Dependability and Impact Matrix****:* We proposing three Levels (1, 2, 3) that we assign to each entry (table 10):

- Level 3: This level take the value of 3 and representing the most affected requirement/s in case of component violation or the most affected component/s incase of threat materialized (Here data has been published in some of CSA materials and some others materials), when it mapped to probabilities it takes the highest probabilities.
- Level 2: This level take the value of 2, the effect here is less than level 1, data here has been obtained from other journal [25] and it doesn’t exist in CSA reports, when mapped to probabilities it takes median probabilities.
- Level 1: Take the value 1, here either some journal mentioned the minor effect on those entities in case of failures occurrence or no one considering this effect-when mapped to probabilities it takes the lowest probability.

However, the lowest row (NRF and NCV row) take probabilities (0.1, 0.2, 0.3, 0.4…etc) depending on how critical the component or threat is. The following table 10 presenting the impact matrix as example which presenting a sample of data that demonstrate the levels which we assign to each entry, accordingly table 2 and table 3 has been generated which presenting how we map these levels to probabilities.

TABLE 10: ASSIGNING LEVEL NUMBER TO EACH ENTRY

IM		Cloud Threat					
Cloud Component		***Data Breaches***	***Weak Identity, Credential and Access Management***	***Insecure APIs***	***System and Application Vulnerabilities***	***Account Hijacking***	***NOT***
	Application	1	3	1	3	2	0
	Runtime	2	3	2	3	3	0
	Middleware	2	3	2	2	2	0
	OS	2	3	2	1	3	0
	Hyper visor	1	2	2	1	1	0
	Infrastructure	1	1	2	3	1	0
	NCV	0.1	0.5	0.1	0.1	0.43	1

C. ***Threat Vector**:* this vector is proposed based on many incidents reports on cloud computing, most of them which is proposed by CSA, these incidents have been mapped to probabilities.

Due to space constraints, we cannot discuss all MFC entries, but the following part represents the sample of the reasoning for filling some values in the MFC metrics:

- First we start by filling the lowest row of the matrix, for the example: the probability of violating requirements given a component failure, we 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) depending on how critical the component is (here we assuming that the NRF in "Application" column is 0.4), same thing for the "Impact Matrix"
- Then we distribute the remaining probability (0.9 or 0.8, or 0.7…etc) on the remaining entries of the column according to the levels (1, 2, 3…etc) that we assign to each entry (as shown in table 2 and table 3).

For example: let's assuming the "Application Component" is the one of most critical component in the Dependability Matrix so (here we assuming that the NRF in "Application" column is 0.4), then distributing the remaining probability on the remaining entries of the column, so each selected component (e.g. Application Component), for these remaining entries we determine which the security requirement is most affected by failure of this component, (in this case it is "Availability Requirement"), accordingly assigning level 3 that entering the highest probability 0.225 (in the remaining entities) on that column.

There are four countermeasures that used to enhance and control the MFC metrics, each measure is used for specific MFC matrix: "Mitigation measures" is used to enhance and control the Stakes Matrix, "Failure tolerance measures" is used to enhance and control the Dependability Matrix, "Fault tolerance measures" is used to enhance and control the Impact Matrix and "Evasive measures" is used to enhance and control the Threat Vector.

The following Fig.1 presenting the whole life cycle of the MFC with using the cost/benefit analysis model that can be adapted to all cloud service model which can be performed by the following steps:

- Filling all MFC metrics (ST, DP, IM and TV).
- Computing the MFC0 (as shown in table 11).
- Deploying a suitable countermeasure that helps to enhance the security of the Cloud Computing in term of reducing the MFC.
- 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, as shown in Fig. 8 (we assume that the cost of deploying the firewall is 8000 $).
- 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.

TABLE 11: STAKEHOLDER MEAN FAILURE COST

Stakeholders	MFC0 ($/hour)	MFC1 ($/hour)	MFC Gain	C(0) ($)
Cloud Consumer	6.485	6.479	0.006	184.62
Cloud Provider	108.36	108.195	0.165	5076.9
Cloud Carrier	26.013	25.983	0.03	923.08
Cloud Broker	41.551	41.492	0.059	1815.4
			0.256	8000$

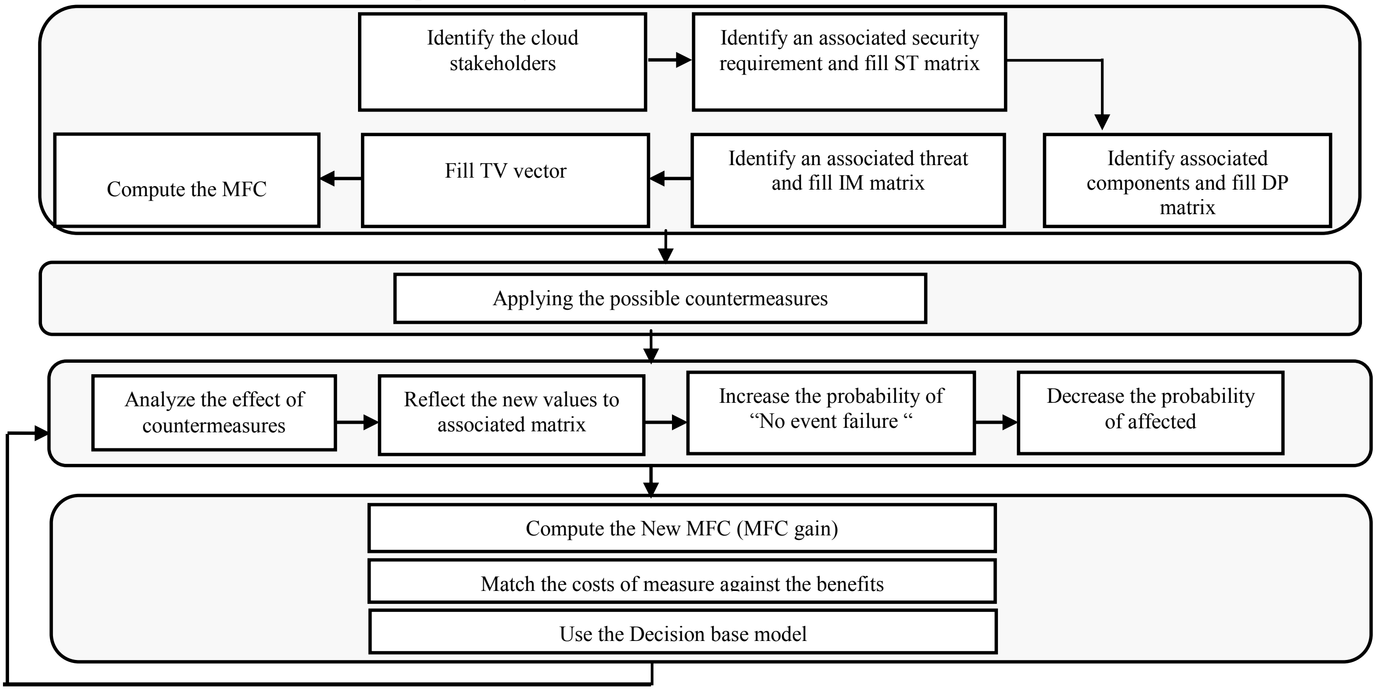
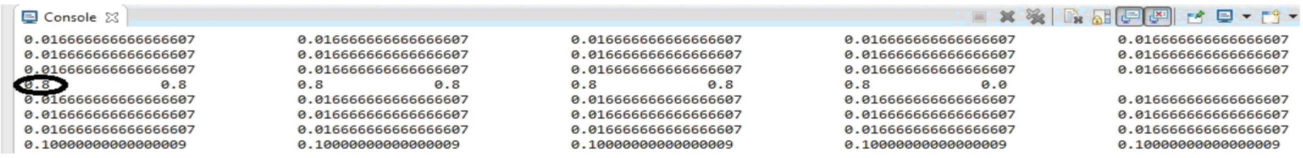

Identify the cloud stakeholders
Identify an associated security requirement and fill ST matrix
Identify associated components and fill DP matrix
Identify an associated threat and fill IM matrix
Fill TV vector
Compute the MFC
Applying the possible countermeasures
Analyze the effect of countermeasures
Reflect the new values to associated matrix
Increase the probability of "No event failure "
Decrease the probability of affected
Compute the New MFC (MFC gain)
Match the costs of measure against the benefits
Use the Decision base model

Fig. 1. Framework for Measuring Cloud Security Risk by Mean Failure Cost

VII. Automated Tool

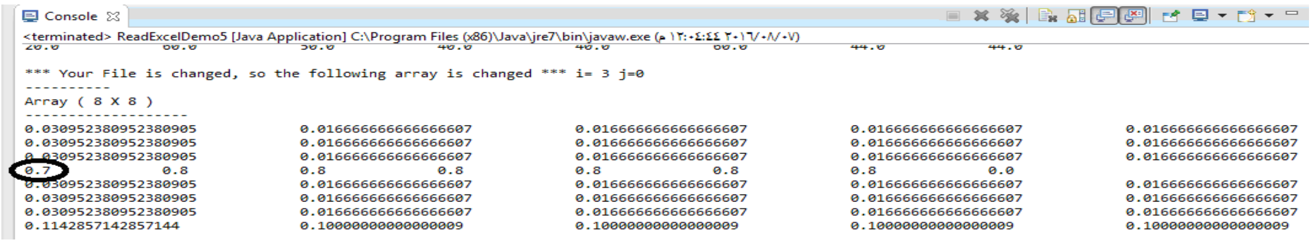
Fig. 1 presenting the whole life cycle of the MFC which has been supported by the proposed tool, this tool read all the MFC metrics from excel sheet and use of these data as a default values (as shown in Fig. 2), experts on cloud domain can adjust these default values when needed, in this case the automated tool will recalculate all the remaining entries on that column to keep balance of the MFC metrics, this will be done by *propagating the difference* between the remaining entries (as shown in Fig. 2 and Fig. 3). The proposed tool is ready now to calculate the MFC for each stakeholder (as shown in Fig. 4), if any stakeholder need to deploy some countermeasures, this will lead to reflect this enhancement measure values to appropriate MFC metrics, as example if we deploying new load balancer, this will lead to "Decreases" the probability of "Data Loss" Threat and "Increase" the probability of No Threat "NoT", the reaming entries *will be as it is* (see Fig. 5 and Fig. 6), and the automated tool will recalculate the MFC to obtain the new result of the acquired countermeasure in term of reducing the MFC, this new value of MFC is called the "MFC Gain" (see Fig. 7), and finally this tool can assess the cost effectiveness of security measures for each stakeholder in proportion to the "MFC Gain" (as shown in Fig. 8) which help to decide whether the measure is worthwhile or not by computing the return on investment of the countermeasure for each stakeholder. This quantification tool of security attributes that 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.

VIII. Automated Tool Snapshots



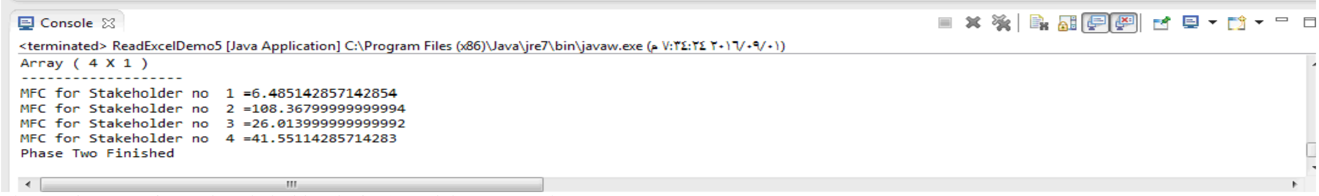
```
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.8             0.8           0.8             0.8           0.8             0.8           0.8             0.0
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.10000000000000009           0.10000000000000009           0.10000000000000009           0.10000000000000009           0.10000000000000009
```

Fig. 2: One of the MFC matrix (before) changing the "Default values"



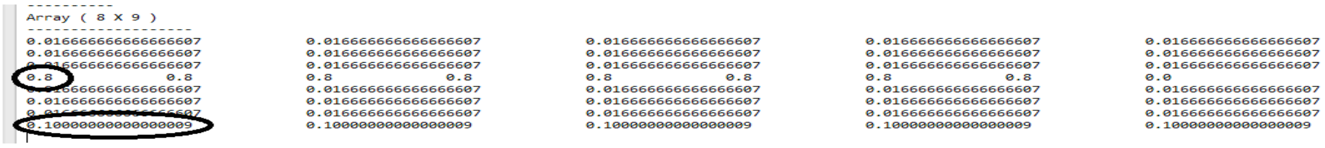
```
<terminated> ReadExcelDemo5 [Java Application] C:\Program Files (x86)\Java\jre7\bin\javaw.exe (م ١٢:٠٤:٤٤ ٢٠١٦/٠٨/٠٧)
20.0      60.0      30.0      40.0      40.0      60.0      44.0      44.0

*** Your File is changed, so the following array is changed *** i= 3 j=0
----------
Array ( 8 X 8 )
--------------------
0.030952380952380905          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.030952380952380905          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.030952380952380905          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.7             0.8           0.8             0.8           0.8             0.8           0.8             0.0
0.030952380952380905          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.030952380952380905          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.030952380952380905          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.1142857142857144            0.10000000000000009           0.10000000000000009           0.10000000000000009           0.10000000000000009
```

Fig. 3: One of the MFC matrix (after) changing the "Default values" with propagation



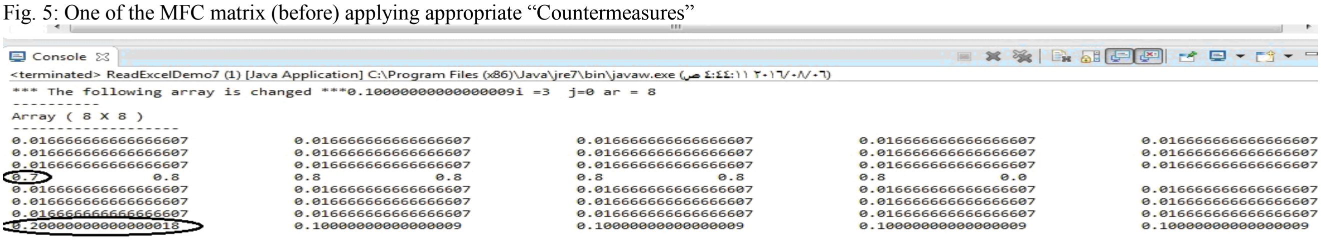
```
<terminated> ReadExcelDemo5 [Java Application] C:\Program Files (x86)\Java\jre7\bin\javaw.exe (م ٧:٣٤:٢٤ ٢٠١٦/٠٩/٠١)
Array ( 4 X 1 )
--------------------
MFC for Stakeholder no  1 =6.485142857142854
MFC for Stakeholder no  2 =108.36799999999994
MFC for Stakeholder no  3 =26.013999999999992
MFC for Stakeholder no  4 =41.55114285714283
Phase Two Finished
```

Fig. 4: The MFC for each stakeholder (before) applying appropriate "Countermeasures"



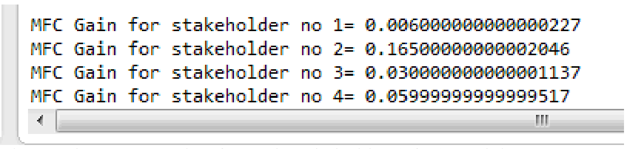
```
----------
Array ( 8 X 9 )
--------------------
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.8             0.8           0.8             0.8           0.8             0.8           0.8             0.8           0.0
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.10000000000000009           0.10000000000000009           0.10000000000000009           0.10000000000000009           0.10000000000000009
```

Fig. 5: One of the MFC matrix (before) applying appropriate "Countermeasures"



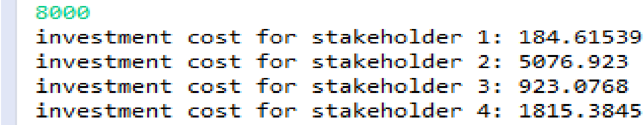
```
<terminated> ReadExcelDemo7 (1) [Java Application] C:\Program Files (x86)\Java\jre7\bin\javaw.exe (ص ٤:٤٤:١١ ٢٠١٦/٠٨/٠٦)
*** The following array is changed ***0.10000000000000009i =3  j=0 ar = 8
----------
Array ( 8 X 8 )
--------------------
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.7             0.8           0.8             0.8           0.8             0.8           0.8             0.0
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607          0.016666666666666607
0.20000000000000018           0.10000000000000009           0.10000000000000009           0.10000000000000009           0.10000000000000009
```

Fig. 6: One of the MFC matrix (after) applying appropriate "Countermeasures"



```
MFC Gain for stakeholder no 1= 0.006000000000000227
MFC Gain for stakeholder no 2= 0.16500000000002046
MFC Gain for stakeholder no 3= 0.030000000000001137
MFC Gain for stakeholder no 4= 0.05999999999999517
```

Fig. 7: The “MFC Gain” for each stakeholder (after) applying appropriate Countermeasures



```
8000
investment cost for stakeholder 1: 184.61539
investment cost for stakeholder 2: 5076.923
investment cost for stakeholder 3: 923.0768
investment cost for stakeholder 4: 1815.3845
```

Fig. 8: Dispatching the investment cost across the stakeholders

IX. Conclusion

Mean Failure Cost is a function that quantifies the statistical mean of a random variable that represents the loss incurred by a system stakeholder as a result of system failure, including security failure. In this paper we apply the MFC model 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. Then we try to fill out all the relevant metrics and vector with cloud-relevant empirical data. Not all the relevant data is available, so we did have to make some assumptions and some approximations, and our results are only as good as these. Nevertheless, we feel that our cloud-specialized model give a broad framework

For reasoning about security-related stakes and costs, we have briefly discussed an automated tool that computes the MFC of a Cloud Computing installation; in particular, we discuss how it can be adapted to a particular cloud installation using installation-specific knowledge.

Acknowledgment

The author is grateful to the anonymous reviewers for their valuable feedback. The completion of this work would not have been possible without their valuable comments. She is also thankful to several colleagues at SUST for their help and support. Their participations are sincerely appreciated and gratefully acknowledged. Finally, the author would like to express her deep appreciation particularly to her supervisor and all members of her family.

References

[1] Aissa, R. Abercrombie, F.T. Sheldon etal., “Quantifying cyber security threats and their impact,” ISSE, 2010.

[2] Nahla Murtada, “Measuring the Cybersecurity of Cloud Computing - A Stakeholder Centered Economic Approach”, International Conference on Computing, Electric and Electronics Engineering (ICCEEE), 2013.

[3] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina and Lee Badger and Dawn Leaf, NIST, Special Publication 500-292, NIST Cloud Computing Reference Architecture, Recommendations of the National Institute of Standards and Technology, 2011.

[4] Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director , NIST (National Institute of Standards and Technology) Cloud Computing Standards Roadmap, Special Publication 500-291, Version 2, NIST Cloud Computing Standards Roadmap Working Group, NIST Cloud Computing Program, Information Technology Laboratory, July 2013.

[5] Lee Badger, Robert Bohn, etal.,” Useful information for cloud adopters,” National Institute of Standards and Technology (NIST), NIST US Government Cloud Computing Technology Roadmap, Volume II, Release 1.0 (Draft) November 2011.

[6] NIST, L. Badger, D. Bernstein, R. Bohn, F. De Vaulx, M. Hogan, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside, and D. Leaf, “US Government Cloud Computing Technology Roadmap Volume II Release 1.0 (Draft): Useful Information for Cloud Adopters,” Nist Spec. Publ., vol. II, p. 85, 2011.

[7] Vahid Ashktorab, Seyed Reza Taghizadeh1, “Security threats and countermeasures in cloud computing,” International Journal of Application or Innovation in Engineering and Management (IJAIEM), October 2012.

[8] Allan A. Friedman and Darrell M. West, “Privacy and Security in Cloud Computing,” Issues in Technology Innovation, 2010.

[9] J. Sen, “Security and Privacy Issues in Cloud Computing,” Archit. Protoc. Secur. Inf. Technol., no. iv, p. 42, 2013.

[10] CSA CSA CLOUD SECURITY ALLIANCE The Treacherous 12 - Cloud Computing Top Threats in 2016 February, 2016.

[11] Rafal Los, HP etal., CLOUD SECURITY ALLIANCE, The Notorious Nine: Cloud Computing Top Threats in 2013, February 2013.

[12] F. Yahya, R. J. Walters, and G. B. Wills, “Modelling Threats with Security Requirements in Cloud Storage,” Int. J. Inf. Secur. Res., vol. 5, no. 2, pp. 551–558, 2015.

[13] Olivier Brian, Thomas Brunschwiler, Heinz Dill, Hanspeter Christ, Babak Falsafi, Markus Fischer etal., “SATW White Paper Cloud Computing”, Swiss Academy of Engineering Sciences, Member of the Swiss Academies of Arts and Sciences, 2012-11-06.

[14] Seyyed Mohsen Hashemi, Mohammad Reza Mollahoseini Ardakani, International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868, Foundation of Computer Science FCS, New York, USA, Volume 4– No.1, September 2012.

[15] Ankur Mishra1, Ruchita Mathur2, Shishir Jain3, Jitendra Singh Rathore4, “ Cloud Computing Security”, International Journal on Recent and Innovation Trends in Computing and Communication ISSN 2321 – 8169, 2013.

[16] Cloud Security Considerations, Confidence in Cyberspace, NSA Information Assurance Service Center, October 2013.

[17] Alex Ginsburg, Luciano JR Santos, Evan Scoboria, Kendall Scoboria etal. , Top Threats Working Group, “The Notorious Nine Cloud Computing Top Threats in 2013”, February 2013.

[18] Amer Deeba, Andy Dancer, Brian Shea, Craig Balding etal, CloudSecurity, Top Threats to Cloud Computing V1.0 Prepared by the Cloud Security Alliance March 2010.

[19] A. Kashyap Horbury and C. etal Arman, “Internet Security Threat Report,” ISTR Internet Secur. Threat Rep. 2014, vol. 19, no. April, 2015.

[20] R. Ko, S. Lee, and V. Rajan, “Cloud Computing Vulnerability Incidents: A Statistical Overview,” p. 21, 2013.

[21] Bohn, R., Cloud Computing Standards – A NIST Perspective NIST Goal To accelerate the federal government ’ s. NIST, January 2016.

[22] Lee Badger, Tim Grance, RobertPatt-Corner JeffVoas, “The attached DRAFT document, (provided here for HISTORICAL purposes), 2012.

[23] Nahla Murtada, “Comperhensive Model for Building Presice MFC Matrices for Cloud Computing”, International Conference On Information and Communication Technologies in Training and Education, 2016.

[24] K. Singh and S. Negi, “Service Model Specific Security Requirements and Threats in Cloud Computing,” vol. 5, no. 7, pp. 851–855, 2015.

[25] G. Somasekhar, “CLOUD COMPUTING WITH BIG DATA AS A SERVICE,” vol. 4, no. 8, pp. 1201–1208.