Journal of King Saud University – Computer and Information Sciences (2013) 25, 63–75

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

ORIGINAL ARTICLE

A cybersecurity model in cloud computing environments

Latifa Ben Arfa Rabai [a,*], Mouna Jouini [a], Anis Ben Aissa [b], Ali Mili [c]

[a] *ISG, Tunis, Tunisia*
[b] *ENIT, Tunis, Tunisia*
[c] *NJIT, Newark, NJ, USA*

Received 18 February 2012; revised 13 June 2012; accepted 26 June 2012
Available online 10 July 2012

KEYWORDS

Cloud computing;
Cyber security;
Mean failure cost;
Security requirements;
Security threats

Abstract Cloud computing is an emerging paradigm of computing that replaces computing as a personal commodity by computing as a public utility. As such, it offers all the advantages of a public utility system, in terms of economy of scale, flexibility, convenience but it raises major issues, not least of which are: loss of control and loss of security. In this paper, we explore a user-centered measure of cyber-security, and see how this measure can be used to analyze cloud computing as a business model.

1. Cloud computing: challenges and opportunities

In the early days of computing, computer resources were a centralized organizational asset, that represents a massive investment of money, time and labor; only large organizations could afford to acquire, maintain and operate such infrastructures. With the advent of personal computers in the 1980s, the prevailing computing paradigm changed drastically: first, the low cost of personal computers opened a worldwide market of people and organizations large and small; second, this situation fostered, in turn, a large pool of talent that was able to develop and distribute PC-based applications, at the same time as it was creating a market for such applications; third, the centralized paradigm of mainframe-based computing at large organizations was progressively replaced by local area networks, linking servers and terminal computers within an organization; fourth, the pervasiveness of the Internet transformed the global mass of personal computers into a massive network of nodes, sharing information, services, software, and malware of all kinds.

Even though personal computers are fairly dependable in general, and require relatively little expertise to maintain and operate, under this computing paradigm end-users are still responsible for operating a complex machine about which they understand very little. Also, each individual computer is used a minimal fraction of the time, and typically deploys only a very small fraction of its wide range of software and hardware capabilities. Furthermore, the safekeeping of a user's data is the responsibility of the user alone, who must rely on precarious media such as hard disks, compact disks, and flash memory, which are prone to loss, damage, and theft.

Against this background, it is easy to see the attractiveness of a computing paradigm where end users avail themselves of computing resources and services as a public utility, rather than a privately run small scale computing facility. In the same way that we use electricity as a public utility (rather than build our own generators), and that we use water as a public utility (rather than dig our own well), and that we use phone service as a public utility (rather than build and operate our own cell tower), we may want to use computing services as a public utility. Such a service would be available to individuals and

* Corresponding author.
E-mail address: latifa.rabai@isg.rnu.tn (L.B.A. Rabai).
Peer review under responsibility of King Saud University.

ELSEVIER Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2012.06.002

organizations, large and small, and would operate on the same pattern as other public utilities, namely:

- Subscribers sign up for service from a service provider, on a contractual basis.
- The service provider delivers services of data processing, data access and data storage to subscribers.
- The service provider offers warranties on the quality of services delivered.
- Subscribers are charged according to the services they use.

This modus operandi offers the usual advantages of public utilities, in terms of efficiency (higher usage rates of servers), economies of scale (time sharing of computing resources), capacity (virtually unlimited computing power, bounded only by provider assets rather than by individual user assets), convenience (no need for users to be computer-savvy, no need for tech support), dependability (provided by highly trained provider staff), service quality (virtually unlimited data storage capacity, protected against damage and loss), etc. This new paradigm is what we refer to as cloud computing (Armbrust et al., 2009; Mell and Grance, 2009, 2010; Vaquero et al., 2009; Wang et al., 2008; Rittinghouse and Ransome, 2010).

The migration from a personal computer based paradigm to a cloud computing paradigm carries some risks along with its many rewards, not least of which are the loss of control and the loss of security (Hanna, 2009; Ibrahim et al., 2010; Subashini and Kavitha, 2010; Rittinghouse and Ransome, 2010; Wooley, 2011; Xuan et al., 2010). Indeed, by trusting its critical data to a service provider, a user (whether it be an individual or an organization) takes risks with the availability, confidentiality and integrity of this data: availability may be affected if the subscriber's data is unavailable when needed, due for example to a denial of service attack or merely to a loss; confidentiality may be affected if a subscriber's data is inadvertently or maliciously accessed by an unauthorized user, or otherwise unduly exposed; integrity may be affected if a subscriber's data is inadvertently or maliciously damaged or destroyed. In this paper, we propose a security metric that enables service providers and service subscribers to quantify the risks that they incur as a result of prevailing security threats and system vulnerabilities. The reason why security is a much bigger concern in cloud computing than it is in other shared utility paradigms is that cloud computing involves a two-way relationship between the provider and the subscriber: whereas the water grid and the electric grid involve a one-way transfer from the provider to the subscriber, cloud computing involves two-way communication, including transferring information from subscribers to providers, which raises security concerns. Note that a telephone service also involves the transfer of (vocal) information from subscribers to providers, and it too raises security concerns (possibility of wiretapping), though on a smaller scale.

The security metric we propose in this paper is quantified in economic terms, thereby enabling providers and subscribers to weight these risks against rewards, and to assess the cost effectiveness of security countermeasures.

2. Related work

In Speaks (2010), discusses the concept of reliability and its measurement using MTTF and MTBF. Our work presents a dependability metric, which encompasses security, and which differs from MTTF and MTBF in that 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.

In Josson and Pirzadeh (2011) offer a taxonomy of security metrics, which they divide between protective metrics (that reflect the extent to which the system protects itself from perpetrator threats) and behavioral metrics (that reflect operational attributes of the system). They propose three security metrics, namely the traditional MTTF (Mean Time to Failure), as well as MTTCF (Mean Time to Catastrophic Failure) and the MTTR (Mean Time to Repair). The distinction that Jonsson and Pirzadeh make between MTTF and MTTCF can be seen as a special case of our stakes matrix: we do not classify failures into catastrophic and low impact failures; rather we let users attach stakes to security requirements, ranging over a continuum of values, hence including low stakes and high stakes (when failure is considered catastrophic).

In (Barry, 2003; Barry and LiGuo, 2003; Barry, 2006), Boehm et al. argue that all dilemmas that arise in software engineering are of an economic nature rather than a technical nature, and that all decisions ought to be modeled in economic terms: maximizing benefit; minimizing cost and risk. Our work is perfectly compatible with the philosophy of value-based software engineering, as it models system security not by an arbitrary abstract scale but rather by an economic function (MFC), quantified in monetary terms (dollars per hour), in such a way as to enable rational decision making.

In Brunette and Mogull (2009) discuss the promise and perils of cloud computing, and single out security as one of the main concerns of this new computing paradigm. Also, they catalog and classify the types of security threats that arise in cloud computing or are amplified by the cloud paradigm. Their work can be used to complement and consolidate our approach, in that it provides a comprehensive catalog of security threats that are classified according to their type.

In Chow et al. (2009) explore the security concerns raised by cloud computing in terms of three categories: provider-related vulnerabilities, which represent traditional security concerns; availability, which arises in any shared system, and most especially in cloud computing; and third party data control, which arises in cloud computing because user data is managed by the cloud provider and may potentially be exposed to malicious third parties. Chow et al. discuss strategies that may be used to mitigate these security concerns. Similar concerns are expressed by Carlin and Curran (2011).

In Black et al. (2009) discuss cyber security metrics, which they characterize as reflecting the extent to which the system's security controls are in compliance with relevant procedures, processes or policies. They argue that cyber security metrics are often defined imprecisely, and used improperly. In our approach, we distinguish between how a metric is defined and how it is computed; while we may have issues with how MFC can be computed in practice, we have no issue with how it is defined; it is the statistical mean of a clearly defined random variable.

In (Center for Internet Security, 2009), a set of MTTF-like metrics are proposed to capture the concept of cyber security. These include: mean time to incident discovery; incident rate;

mean time between security incidents; mean time to incident recovery; vulnerability scan coverage; percentage of systems without known severe vulnerabilities; mean time to mitigate vulnerabilities; number of known vulnerability instances; patch policy compliance; mean time to patch; etc. These metrics feature the same weaknesses that we have discussed previously regarding MTTF; in addition, we feel that MFC subsumes them in that they can be used to enhance the estimate of MFC, and that once we know MFC, we likely do not care to know their specific value.

3. Risk estimation metrics

The importance of security concerns on the development and exploitation of information systems never ceased to grow. In fact, information systems are today used everywhere by individuals or organizations and systems are target to information security attacks; these attacks could be from hackers, viruses or internal employees, and it is very clear now that this would lead to lose a large amount of money, time and other resources. Thus, organizations not only may spend millions of dollars on technical security equipments such as firewalls, IDSs, encryption tools and anti-viruses to try to protect them against known threats, but also are confronted with great difficulties for evaluating security technology investments because the technology benefits are difficult to estimate and these benefits depend on attack(s) frequency expectation, damage occurrence and effectiveness of security technology to mitigate the damage(s) from an attack(s) (Tsiakis, 2010). In this context, the information security risk management model comes to reduce cost investment without increasing the risk.

A risk is the probability of cause of a problem when a threat is triggered by vulnerabilities. Threats are much related to the characteristics of the assets and vulnerabilities are relevant to the security controls (Foroughi, 2008). Information Security assets are Information Technology resources or other components that are part of the Information System, linked to the business assets. An asset is defined as any element of an information system that possesses a value. It includes tangible (software, hardware, personnel) and intangible assets (plans, organization, external factors, and technical factors). The loss (or damage) of assets in an organization due to the cyber security incidents is measured by considering assets, threats, and vulnerability and so, the risk of an information system's asset could be determined by the following formula (Tsiakis, 2010; Foroughi, 2008):

$$\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Impact}$$

In other words, risk is characterized by the opportunity of a threat targeting Information Security assets, to exploit one or more vulnerabilities originating from the design decisions, and leading to an impact on decision goals.

3.1. Risk estimation metrics review

Quantitative risk analysis aspires to cede precise numeric monetary values to assets. It designates the financial risk of threats impact and frequency, costs of control and loss.

As quantitative information risk models, we can cite the single loss expectancy (SLE), and the annual loss expectancy (ALE) (Tsiakis, 2010; Boehme and Nowey, 2008).

3.1.1. Single loss expectancy (SLE)

The single loss expectancy (SLE) is the expected monetary loss every time a risk occurs. It is calculated by multiplying asset value (AV) with Exposure Factor (EF) as shown in formula [2]:

$$\text{SLE} = \text{AV} * \text{EF}$$

Where AV is the financial value of the asset and EF is expressed within a range from 0% to 100% that an asset's value will be destroyed by risk.

3.1.2. Annual loss expectancy (ALE)

The annual loss expectancy (ALE) is the expected cumulative cost of risk over a period of one year. It is defined as the cost (loss in monetary units) of the damage resulted by a failure multiplied by its frequency in a period of one year:

$$\text{ALE} = \text{SLE} * \text{ARO}$$

where: the annual rate of occurrence (ARO) is the probability that a risk will occur in this particular period of one year.

3.1.3. OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a risk-based strategic assessment and planning technique for security which was developed by the Software Engineering Institute of Carnegie Mellon University in USA (Mayer, 2009). The method aims are examining organizational and technological issues as well as defining an organization's security strategy and plan. It consists of three steps: making file of threat scenarios based on assets, recognizing the vulnerabilities about major facilities, and assessing the risk and developing security strategies.

The first step allows identifying assets of the system, security requirements (confidentiality, integrity and availability), threat profiles and main vulnerabilities by interviewing some people during workshops. The second step identifies vulnerabilities that expose those threats and creates risks to the organization. In the last step, it develops a practice-based protection strategy and risk mitigation plans to support the organization's missions and priorities.

3.1.4. CRAMM

The CRAMM (CCTA Risk Analysis and Management Method) method was developed since 1985 by the Central Computer and Telecommunications Agency of the UK government (Mayer, 2009). The methodological part of CRAMM is composed of three steps:

- The first step identifies assets which are divided into three classes: physical assets, software and data. The valuation of assets is generally done in terms of the impact coming from information potentially being unavailable, destroyed, disclosed or modified for software and data. This estimation of assets may be done in a quantitative way by valuing them in financial terms by data owners (the business unit managers).
- The second step identifies and estimates the level of threats and vulnerabilities and provides some mapping between threats and assets and between threats and impacts in a qualitative way.
- The third step produces a set of countermeasures that are considered as necessary to manage the identified risks.

3.1.5. Information security risk management framework for the cloud computing environments

The work presents a qualitative information risk management framework for better understanding critical areas of focus in cloud computing environment and identifying threats and vulnerabilities. The qualitative risk analysis proposed method is used to approach risk assessment and rank severity of threats by using classes such as low, medium and high of probabilities and damages for cloud providers. That is, to help providers to control their security position and then to proceed to risk mitigation (Zhang et al., 2010).

The framework has seven processes including: selecting relevant critical areas, strategy and planning, risk analysis, risk assessment, risk mitigation, assessing and monitoring program, and risk management review. Each process will be necessary to clarify specific roles, responsibilities, and accountability for each major process step (Zhang et al., 2010).

In the first step, the method highlights the areas of concern for cloud computing environment. For example, if you are a SaaS provider, you may select application security, identify access management, assessing threats and risks of vulnerabilities to organization. After proposing a strategy and planning process, the risk analysis step allows identifying threat sources (attacker, hackers) in cloud computing and identifying essential vulnerabilities in order to protect hosts, network devices, and applications from attacks against known vulnerabilities. The risk assessment step was divided into four major processes: likelihood determinations, impact analysis, risk determination and control recommendations. It represents the probability that a potential vulnerability could be exercised by a given threat source in a qualitative way (high, medium, low) and determines the adverse impact resulting from a successful threat exercise of vulnerability and finally it represents, in a qualitative way, the risk levels and control recommendations to reduce this risk in a cloud computing system. In the risk mitigation step, a cloud provider develops risk treatment plans (RTP) to mitigate vulnerabilities and threats. Finally, a cloud provider should monitor the risk treatment plan.

3.1.6. MFC

In BenAissa et al. (2010) present a quantitative infrastructure that estimates the security of a system. The model measures the security of a system in terms of the loss that each stakeholder stands to sustain as a result of security breakdowns. The infrastructure in question reflects the values that stakeholders have in each security requirement, the dependency of security requirements on the operation of architectural components, and the impact that security threats.

3.2. Comparing risk estimation metrics

CRAMM, OCTAVE and the risk management model for cloud computing are simple frameworks for assessing security risks for information systems and they allow selecting appropriate security solutions (countermeasures) after identifying security risks. However, they are qualitative models, i.e., the assessment of probability and risks is based on a ''low/medium/high'' characterization rather than a specific probability and a specific dollar amount of loss. Besides, they do not distinguish between stakeholders: they provide the level of security risk for the system provider.

The SLE and ALE are quantitative risk estimation metrics. However, they reflect the loss risk of the whole system and they ignore the variance stakes among different stakeholders.

On the other hand, the MVC, as a quantitative metric, takes into account:

- The variance in failure cost from one requirement to another.
- The variance in failure probability from one component to another.
- The variance in failure impact from one stakeholder to another.

The MFC presents many advantages:

- It provides a failure cost per unit of time (mean failure cost): it 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.

4. Mean failure cost: a measure of cyber-security

In BenAissa et al. (2010) introduce the concept of mean failure Cost as a measure of dependability in general, and a measure of cyber security in particular. We note that we have used it in an E-commerce environment in BenAissa et al. (2010), and in an E-learning environment in Ben Arfa Rabai et al. (2012).

4.1. The stakes matrix

We consider a system S and we let $H_1, H_2, H_3, \ldots, H_k$, be stakeholders of the system, i.e. parties that have a stake in its operation. We let $R_1, R_2, R_3, \ldots, R_n$, be security requirements that we wish to impose on the system, and we let $ST_{i,j}$, for $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant n$, be the stake that stakeholder H_i has in meeting security requirement R_j. We let PR_j, for $1 \leqslant j \leqslant n$ be the probability that the system fails to meet security requirement R_j, and we let MFC_i (Mean Failure Cost), for $1 \leqslant i \leqslant k$, be the random variable that represents the cost to stakeholder H_i that may result from a security failure.

We quantify this random variable in terms of financial loss per unit of operation time (e.g. \$/h); it represents the loss of service that the stakeholder may experience as a result of a security failure. Under some assumptions of statistical independence, we find that the Mean Failure Cost for stakeholder Hi can be written as:

$$MFC_i = \sum_{1 \leq j \leq n} ST_{i,j} \times PR_j.$$

If we let MFC be the column-vector of size k that represents mean failure costs, let ST be the $k \times n$ matrix that represents stakes, and let PR be the column-vector of size n that represents probabilities of failing security requirements, then this can be written using the matrix product ($\circ$):

$$MFC = ST \circ PR.$$

The stakes matrix is filled, row by row, by the corresponding stakeholders. As for PR, we discuss below how to generate it.

4.2. The dependency matrix

We consider the architecture of system S, and let C_1, C_2, $C_3, \ldots, C_h$, be the components of system S. Whether a particular security requirement is met or not may conceivably depend on which component of the system architecture is operational. If we assume that no more than one component of the architecture may fail at any time, and define the following events:

- E_i, $1 \leqslant i \leqslant h$, is the event: the operation of component C_i is affected due to a security breakdown.
- E_{m+1}: No component is affected.

Given a set of complementary events E_1, E_2, $E_3, \ldots E_h$, E_{h+1}, we know that the probability of an event F can be written in terms of conditional probabilities as:

$$P(F) = \sum_{k=1}^{h+1} P(F|E_k) \times P(E_k).$$

We instantiate this formula with F being the event: the system fails with respect to some security requirement. To this effect, we let F_j denote the event that the system fails with respect to requirement R_j and we write (given that the probability of failure with respect to R_j is denoted by PR_j):

$$PR_j = \sum_{k=1}^{m+1} P(F_j|E_k) \times P(E_k).$$

- If we introduce the DP (Dependency) matrix, which has n rows and $h + 1$ columns, where the entry at row j and column k is the probability that the system fails with respect to security requirement j given that component k has failed (or, for $k = h + 1$, that no component has failed), and
- If we introduce vector PE of size $h + 1$, such that PE_k is the probability of event E_k, then we can write: PR = DP ∘ PE.

Matrix DP can be derived by the system's architect, in light of the role that each component of the architecture plays to achieve each security goal. As for deriving vector PE, we discuss this matter in the next section.

4.3. The impact matrix

Components of the architecture may fail to operate properly as a result of security breakdowns brought about by malicious activity. In order to continue the analysis, we must specify the catalog of threats that we are dealing with, in the same way that analysts of a system's reliability define a fault model. To this effect, we catalog the set of security threats that we are facing, and we let T_1, T_2, $T_3, \ldots T_p$, represent the event that a cataloged threat has materialized, and we let T_{p+1}, be the

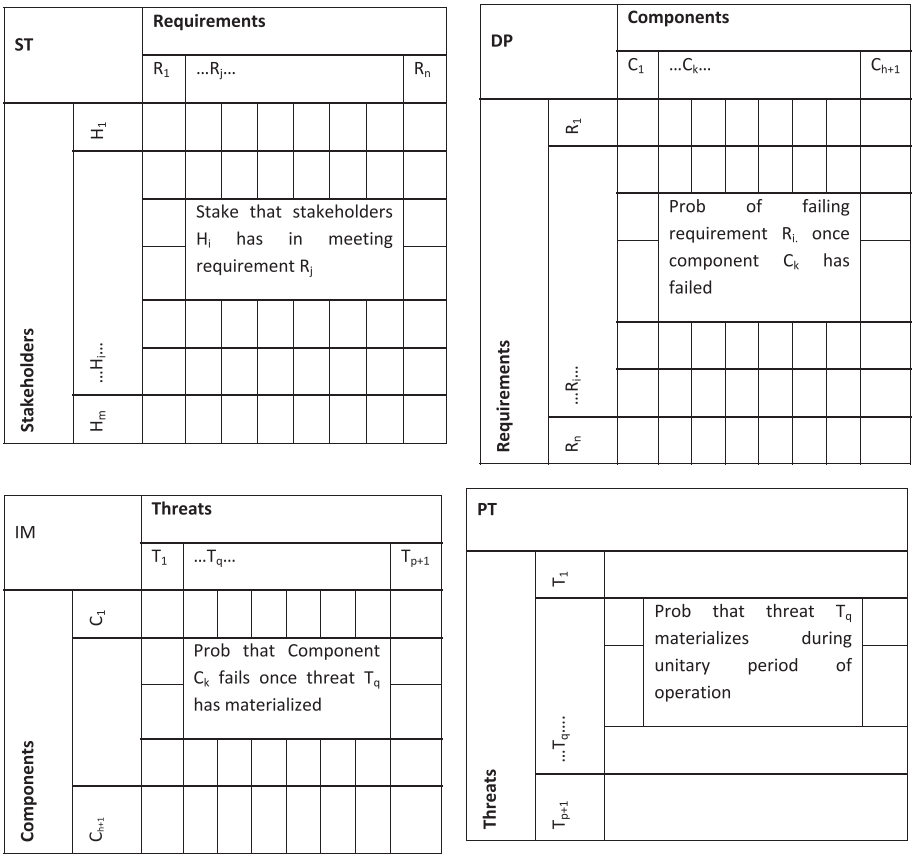

Figure 1 MFC matrices.

event that no threat has materialized. Also, we let PT be the vector of size $p + 1$ such that

- PT_q, for $1 \leqslant q \leqslant p$, is the probability that threat T_q has materialized during a unitary period of operation (say, 1 h).
- PT_{p+1} is the probability that no threat has materialized during a unitary period of operation time.

Then, by virtue of the probabilistic identity cited above, we can write:

$$PE_k = \sum_{q=1}^{p+1} P(E_k|T_q) \times PT_q.$$

If we introduce the following components

- IM (Impact) matrix, which has $h + 1$ rows and $p + 1$ columns, and where the entry at row k and column q is the probability that component C_k fails given that threat q has materialized (or, for $q = p + 1$, that no threat has materialized)
- PT vector of size $p + 1$, such that PT_q is the probability of event T_q.
  Then we can write

$$PE = IM \circ PT$$

Matrix IM can be derived by analyzing which threats affect which components, and assessing the likelihood of success of each threat, in light of perpetrator behavior and possible countermeasures. Vector PT can be derived from known perpetrator behavior, perpetrator models, known system vulnerabilities, etc. We refer to this vector as the *Threat Configuration Vector* or simply as *the Threat Vector*.

4.4. Summary

Given the stakes matrix *ST*, the dependability matrix *DP*, the impact matrix *IM* and the threat vector *PT*, we can derive the vector of mean failure costs (one entry per stakeholder) by the following formula:

$$MFC = ST \circ DP \circ IM \circ PT,$$

where matrix *ST* is derived collectively by the stakeholders, matrix *DP* is derived by the systems architect, matrix *IM* is derived by the security analyst from architectural information, and vector *PT* is derived by the security analyst from perpetrator models. Fig. 1 below illustrates these matrices and their attributes (size, content, indexing, etc.).

5. Stakeholder focus: security requirements

We consider three classes of stakeholders in a cloud computing situation, namely: the service provider, the corporate or organizational subscribers, and the individual subscribers.

The cloud computing system confidentiality, integrity and availability are important pillars of cloud security software assurance (Hanna, 2009; Subashini and Kavitha, 2010; Wooley, 2011; Krutz, 2010). Therefore, as for security requirements, we consider the three principles of information security, namely: availability, integrity, and confidentiality. We further refine this classification by considering different levels of criticality of the data to which these requirements apply:

- *Availability*: Availability refers to the subscriber's ability to retrieve his/ her information when he/she needs it. Un-availability may be more or less costly depending on how critical the data is to the timely operation of the subscriber.
  - o *Critical data*: This data is critical to the day-to-day (or minute-by-minute) operation of the subscriber, and any delay in making this data available is deemed disruptive to the subscriber. For example, product data for an e-commerce merchant; the merchant cannot conduct business without it, and stands to lose sales as well as customer loyalty as a result of un-availability.
  - o *Archival data*: Archival data typically has two attributes that set it apart from critical data: first, it is accessed seldom; second, its access is not time-critical, i.e. delays in delivering it do not cause a great loss. In an e-Commerce application, this data could be, for example, archival order data: such data is accessed only in exceptional cases (for example: a customer has a complaint, or wants to return or exchange merchandise), not a routine operation; and when that data is needed, it is accessed off-line (for example, by staff who are handling a customer complaint), rather than as part of an interactive operation. As a result of these two attributes, unavailability of archival data carries a much lower penalty than unavailability of critical data.

- *Integrity*: Integrity refers to the assurances offered to subscribers that their data is not lost or damaged as a result of malicious or inadvertent activity. Violations of integrity may be more or less costly depending on how critical the data is to the secured operation of the subscriber.
  - o *Critical data:* This data is critical to the normal operation of subscriber functions; if this data is lost, subscribers can no longer operate normally, or can no longer operate at all. For example, if we are talking about a subscriber who is an e-Commerce merchant, critical data would be his product catalog that includes product identification, product pricing, and product availability for his merchandise.
  - o *Archival data*: This data is not critical to the operation of the subscriber, in the sense that the subscriber can operate if this data is lost or damaged. We assume that if integrity is lost, subscribers are duly informed. For example, if we are talking about a subscriber who is an e-Commerce merchant, archival data would be the file that contains customer information or (for even less critical data) or information about customer recommendations.

- *Confidentiality*: Confidentiality refers to the assurances offered by subscribers that their data is protected from unauthorized access. Violations of confidentiality may be more or less costly depending on how confidential the divulged data is.
  - o *Highly classified data*: Exposure of this data to unauthorized parties represents an unrecoverable loss for the subscriber that carries a very high cost, including unquantifiable/imponderable costs (such as loss of life,

mission failure, security implications, etc.). For an e-Commerce subscriber, this may represent detailed personal data of its client database; exposure of such information can lead to identity theft on a massive scale, which leads in turn to customer dissatisfaction, damaged corporate reputation, civil liability, penal lawsuits, etc.

- *Proprietary data*: Exposure of this data to unauthorized parties represents an important but controllable and quantifiable loss; the scale of this loss is limited by its nature (typically: financial loss) and its scale (quantifiable and recoverable). For a corporate subscriber, this may be proprietary information about its intellectual property, its products or its processes.
- *Public data*: Exposure of this data to unauthorized parties represents a minor and recoverable loss, resulting in perhaps a slight loss of competitive advantage. For a corporate subscriber, this could be demographic information about its customer base; a competitor who gains access to that data may cancel whatever marketing advantage the data afforded the subscriber.

For the purposes of our model, we assume that we are dealing with seven generic security requirements, namely:

- AVC: Availability of critical data.
- AVA: Availability of archival data.
- INC: Integrity of critical data.
- INA: Integrity of archival data.
- CC: Confidentiality of classified data.
- CP: Confidentiality of proprietary data.
- CB: Confidentiality of public data.

We assume that the provider makes different provisions for these requirements, putting more emphasis on critical requirements than on less critical requirements. We further assume, for the sake of argument, that for each requirement, the provider makes the same provisions for all its subscribers; hence, if the provider fails to meet a particular requirement, that failure applies to all the subscribers that are dependent on it.

For the sake of illustration, we consider a fictitious running example, where we have a cloud computing provider (PR), and a sample of three subscribers:

- A corporate subscriber (CS).
- A governmental subscriber (GS).
- An individual subscriber (IS).

The purpose of this example is to illustrate the variance in stakes that the various stakeholders have in the operation of the cloud rather than, strictly speaking, to reflect a realistic situation. On the basis of these definitions, we propose the following *Stakes* matrix as shown in Table 1. Each entry of the matrix represents, for stakeholder H and requirement R, the loss incurred by H if requirement R was violated (we use \$K to designate thousands of dollars). In the columns for the availability requirements (AVC, AVA), we assume, for the sake of argument, a repair time of one hour; hence each failure with respect to the availability requirement causes a downtime of one hour; costs will be estimated accordingly. There are a number of dependencies that, for the sake of simplicity, we do not show in this matrix. For example, the stakes of the provider in meeting each security requirement depend on the stakes that each category of subscribers has in meeting that requirement, as well as the number of subscribers in each category; also, the stakes that each subscriber has in meeting each security requirement depends on the volume of data that they file under each category of data (critical, archival, proprietary, classified, etc.). We envision extensions of our current model that take these dependencies into account.

6. System focus: components and services

When we talk about a cloud computing system, we focus on two parts: the front end and the back end, connected to each other through the Internet. The front end is the side of the computer user or client including the client's computer and the application required to access the cloud computing system. The back end is the "cloud" section of the system, which includes the various physical/virtual computers, servers, software and data storage systems. Cloud computing providers can offer services at different layers of the resource stack, simulating the functions performed by applications, operating systems, or physical hardware. The most common approach (Mell and Grance, 2009; Vaquero et al., 2009; Fester et al., 2008) defines cloud computing services as three layers of services:

- Software as a Service (*SaaS*) offers finished applications that end users can access through a thin client. Examples of SaaS include Gmail, Google Docs, and Salesforce.com. The end user does not exercise any control over the design of the application, servers, networking, and storage infrastructure.
- Platform as a Service (*PaaS*) offers an operating system as well as suites of programing languages and software development tools that customers can use to develop their own applications. Prominent examples include Microsoft Windows Azure and Google App Engine. PaaS gives end users control over application design, but does not give them control over the physical infrastructure.
- Infrastructure as a Service (*IaaS*) offers 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 see fit. Examples of IaaS include Amazon Elastic Compute Cloud (EC2) and IBM Blue cloud.

The cloud computing paradigm optimizes in costs of physical resources (servers, CPUs, memories...) by the virtualization techniques. In (Vaughan-Nichols, 2008) Vaughan-Nichols et al. define these techniques as a technology that lets a single PC or server simultaneously run multiple operating systems or multiple sessions of a single OS. This lets users put numerous applications and functions on a PC or server, instead of having to run them on separate machines as in the past. Fig. 2 summarizes cloud computing architecture, services and user tools (Varia, 2008; Orea et al., 2011). Applications/services and basic functions provided in a Cloud are based on the Virtual resources which are abstracted from Physical Resources.

- Virtual physical resources, such as V-CPUs, V-Storages, V-Networks etc.

Table 1 Cloud computing: a sample stakes matrix.

	Requirements						
	AVC	AVA	INC	INA	CC	CP	CB
Stakeholders							
PR	500 $K	90 $K	800 $K	150 $K	1500 $K	1200 $K	120 $K
CS	150 $K	40 $K	220 $K	80 $K	250 $K	180 $K	60 $K
GS	60 $K	20 $K	120 $K	50 $K	2500 $K	30 $K	12 $K
IS	0.050 $K	0.015 $K	0.300 $K	0.200 $K	0.300 $K	0.100 $K	0.010 $K

- V-Networks can be further divided into V-Routers and V-Switches.
- V-Firewalls, VPNs, V-Interfaces, V-Links based on physical Router/Switch equipments.

Computational resources are managed in terms of Virtual Machines (VMs) and/or Virtual Clusters (VCs). Despite of the virtualization of resources, the cloud computing threats do not distinguish between real and virtual components. To simplify the mechanisms of operation in a cloud architecture (Varia, 2008; Orea et al., 2011), we will use the names of components independent of their types (virtual/physical). A sample cloud computing system content includes:

- A browser.
- A proxy server.
- A router/Firewall.
- A load balancer.
- A web server.
- An application server.
- A database server.
- A backup server, and
- A storage server

Assuming no more than one component fails at a time, and considering the additional event that no component has failed, the dependability matrix has (9 + 1 =) 10 columns and 7 rows (one for each security requirement), for a total of 70 entries.

In (Ben Aissa, 2012), we have collected empirical data on a large sample of systems, to enable us to analyze how various security requirements are dependent on the integrity of system components; this information is essential to filling the dependency matrix. To this effect, we have defined broad categories of system components, classified security requirements into standard categories, then collected empirical data on how often a failure of a component of a given category leads to system failure with respect to a given security requirement. In the absence of other sources of information, we use this data to fill out dependency matrix, as shown in Table 2.

7. Provider focus: security threats

Virtualization, the software layer that emulates hardware to increase utilization in large datacenters, is one of the main components of a cloud computing system (Ibrahim et al., 2010), but it causes major security risks. In fact, ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization. Therefore, a cloud computing system is threatened by many types of attacks, including security threats between the subscriber and the datacenter, the hypervisor and the VMs and among the VMs themselves (Wooley, 2011).

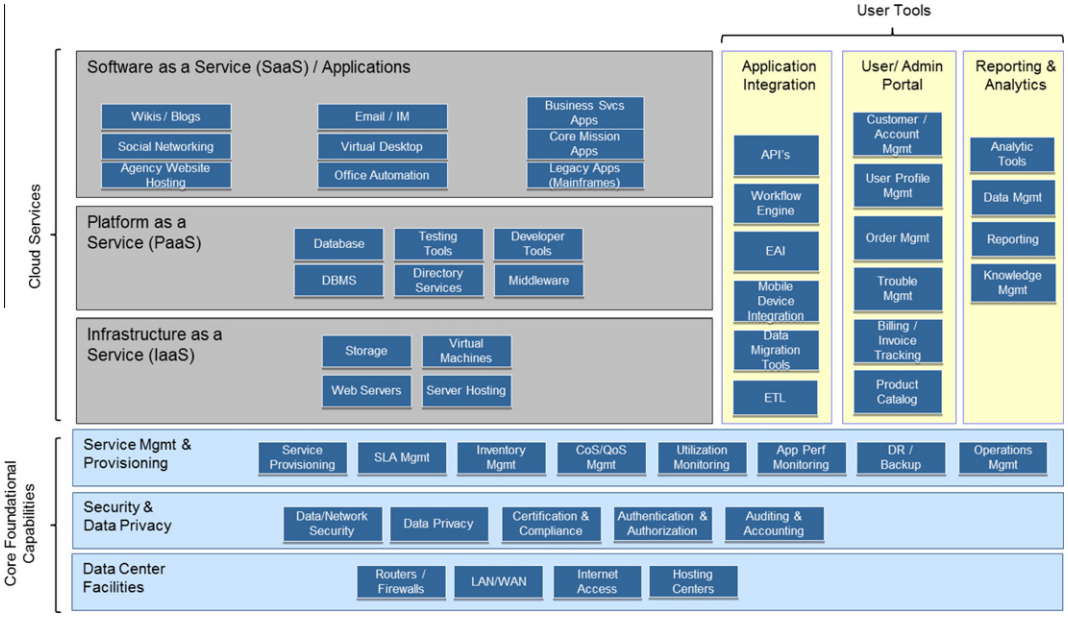

Figure 2 Cloud computing services and architecture.

Table 2 Dependency matrix.

	Components									
	Browser	Proxy server	Router/ firewall	Load balancer	Web server	Application server	Database server	Backup server	Storage server	No failure
Security requirements										
AVC	1	1	1	1	0.44	0.28	1	0.01	1	0
AVA	1	1	1	1	0.44	0.28	0.28	0.01	1	0
INC	0.14	0.14	1	1	0.44	0.14	1	0.01	1	0
INA	0.14	0.14	1	1	0.44	0.14	0.14	0.01	1	0
CC	0.44	0.14	1	1	0.44	0.44	0.44	0.01	0.44	0
CP	0.44	0.14	1	1	0.44	0.44	0.44	0.01	0.44	0
CB	0.44	0.14	1	1	0.44	0.44	0.44	0.01	0.44	0

Table 3 Threat vector.

Threats	Probability
Monitoring virtual machines from host (MVM)	8.063×10^{-4}
Communications between virtual machines and host (CBVH)	8.063×10^{-4}
Virtual machine modification (VMm)	8.063×10^{-4}
Placement of malicious VM images on physical systems (VMS)	8.063×10^{-4}
Monitoring VMs from other VM (VMM)	40.31×10^{-4}
Communication between VMs (VMC)	40.31×10^{-4}
Virtual machine mobility (VMM)	40.31×10^{-4}
Denial of service (DoS)	14.39×10^{-4}
Flooding attacks (FA)	56.44×10^{-4}
Data loss or leakage (DL)	5.75×10^{-4}
Malicious insiders (MI)	6.623×10^{-4}
Account, service and traffic hijacking (ASTH)	17.277×10^{-4}
Abuse and nefarious use of cloud computing (ANU)	17.277×10^{-4}
Insecure application programing interfaces (IAI)	29.026×10^{-4}
No threats (NoT)	0.9682

We consider the security threats that are most often cited in relation with cloud computing systems (Security Alliance, 2010; Ibrahim et al., 2010; Subashini and Kavitha, 2010; Wayne and Timothy, 2011; Wooley, 2011).

7.1. Security threats originating from the host (hypervisor)

7.1.1. Monitoring virtual machines from host

Monitoring the VM from the hypervisor software is an important part of managing and controlling the VMs. Hypervisor is the software that controls the layer between the hardware and the operating systems. The system administrator or other authorized user can make changes to the components of one or more virtual machines (VMs), generating a security risk (Wooley, 2011).

7.1.2. Virtual machine modification

Hypervisor represents the next lower layer of software under the customer's operating system, applications and data. Attacks on the hypervisor layer are attractive to hackers because of the scope of control they can gain if they can install and execute their malicious software on this layer of the VM software (Ibrahim et al., 2010). Compromising the hypervisor means that an attacker can take control of that layer and all of the hosted virtual machines that are hosted on that machine (Ibrahim et al., 2010).

Table 4 Impact matrix.

	Threats														
	MVH	CVH	VMm	VMS	MVV	VMC	VMM	DoS	FA	DL	MI	ASTH	ANU	IAI	NoT
Components															
Brws	0	0	0	0	0	0	0	0.02	0.01	0	0.03	0.02	0	0.03	0
Prox	0.01	0.05	0	0.01	0.01	0.05	0.05	0.02	0.01	0	0.005	0.02	0.01	0	0
R/FW	0.03	0.05	0.033	0.03	0.03	0.05	0.05	0.06	0.04	0	0.005	0.02	0.01	0.01	0
LB	0.02	0.003	0	0.01	0.02	0.003	0.003	0.06	0.04	0	0.005	0.02	0.01	0.01	0
WS	0.03	0.003	0.033	0	0.03	0.003	0.003	0.02	0.04	0	0.01	0.02	0.01	0.01	0
AS	0.02	0.003	0.033	0.06	0.02	0.003	0.003	0.036	0.04	0	0.05	0.02	0.01	0.07	0
DBS	0.001	0	0.033	0.04	0.001	0	0	0.036	0.04	0.05	0.03	0.02	0.01	0.06	0
BS	0.001	0	0	0.04	0.001	0	0	0.036	0.04	0.05	0.03	0.02	0.01	0.06	0
SS	0.04	0.05	0	0.04	0.04	0.05	0.05	0.036	0.04	0.05	0.03	0.02	0.01	0.06	0
NoF	0.06	0.04	0.03	0.03	0.06	0.04	0.04	0.01	0.02	0.01	0.02	0.05	0.06	0.005	1

Table 5 Mean failure cost vector.

Stakeholders	MFC ($K/h)
PR	15.20443
CS	3.53839
GS	8.98502
IS	0.00341

Table 6 The newthreat vector.

Threats	Probability
Monitoring virtual machines from host (MVM)	7.9477×10^{-4}
Communications between virtual machines and host (CBVH)	7.9477×10^{-4}
Virtual machine modification (VMm)	7.9477×10^{-4}
Placement of malicious VM images on physical systems (VMS)	7.9477×10^{-4}
Monitoring VMs from other VM (VMM)	39.7335×10^{-4}
Communication between VMs (VMC)	39.7335×10^{-4}
Virtual machine mobility (VMM)	39.7335×10^{-4}
Denial of service (DoS)	14.1842×10^{-4}
Flooding attacks (FA)	55.6329×10^{-4}
Data loss or leakage (DL)	5.6695×10^{-4}
Malicious insiders (MI)	6.5302×10^{-4}
Account, service and traffic hijacking (ASTH)	17.035×10^{-4}
Abuse and nefarious use of cloud computing (ANU)	17.035×10^{-4}
Insecure application programing interfaces (IAI)	28.619×10^{-4}
No threats (NoT)	0.9704

7.1.3. Threats on communications between virtual machines and host

In a cloud computing system, all communications must pass through the hypervisor to all of the hosted VMs, and at this point, an attacker can inject malicious software in an attempt to eavesdrop or gain control over any or all of the systems. However, the worst case occurs when the hypervisor is compromised by malware, since this puts all the VMs that are being hosted on that machine at risk for security breaches (Wooley, 2011).

7.1.4. Placement of malicious VM images on physical systems

The attack known as cloud malware injection involves creating a malicious virtual machine image and then places that image into the hypervisor so that it is treated like a legitimate system in a collection of virtual machines. If this is successful, then the malicious virtual machine image is allowed to run the adversary's code (Ibrahim et al., 2010; Wooley, 2011).

7.2. Security threats originating between the customer and the datacenter

7.2.1. Flooding attacks

Cloud Computing enables companies to rent server hardware on demand. Thus, instead of buying sufficient server hardware for the high workload times, Cloud Computing enables a dynamic adaptation of these resources. The dynamic provisioning of a cloud in some ways simplifies the work of an attacker to cause threat. The corresponding threat is of flooding attacks which consist of overloading the server hosting services with an enormous number of requests for data processing (Wooley, 2011).

Table 7 Hourly gains in mean failure cost.

Stakeholders	Δ MFC ($/h)
PR	216.531
CS	50.392
GS	127.964
IS	0.048

Table 8 Monthly gains in mean failure cost.

Stakeholders	Δ MFC ($K/month of service)
PR	21.6531
CS	5.0392
GS	12.7964
IS	4.8×10^{-3}

7.2.2. Denial of service (DoS)

The denial of service attack is a critical problem for virtual machines (VMs) used on cloud components. In fact, it indicates that the hypervisor software is allowing a single VM to consume all the system resources and thus starving the remaining VMs and impairing their function (Wooley, 2011).

7.2.3. Data loss or leakage

The threat of data compromise increases because of the architectural or operational characteristics of the cloud environment (user's data is stored outside the enterprise boundary, by the service provider). Data loss may be caused by operational failures due to insufficient authentication or authorization. Data loss may also be caused by deletion or alteration of records without a backup of the original content. Thus, intrusion of data can be done either by hacking through the loop holes in the application or by injecting client code into the system (Subashini and Kavitha, 2010; Wayne and Timothy, 2011).

7.2.4. Malicious insiders

This threat is amplified for consumers of cloud services by the convergence of information technology (IT) services combined with a general lack of transparency into provider process and procedure (Security Alliance, 2010). Such threats include fraud, sabotage and theft or loss of confidential information caused by trusted insiders. The impact that malicious insiders can have on an organization is considerable, given their level of access and ability to infiltrate organizations and assets like brand damage, financial impact and productivity losses.

7.2.5. Account, service and traffic hijacking

Attack methods such as phishing, fraud and exploitation of software vulnerabilities still achieve results. Cloud solutions add a new threat. If an attacker gains access to your credentials, they can eavesdrop on your activities and transaction, return falsified information and redirect your clients to illegitimate sites allowing them to compromise the confidenti-

ality, integrity and availability of those services (Security Alliance, 2010).

7.2.6. Abuse and nefarious use of cloud computing

Cloud computing providers offer their customers an unlimited computing, network and storage capacity coupled with a weak registration process where anyone with a valid credit card can register and immediately begin using cloud services. Cloud computing providers are targets of attack due to the weakness of their registration systems, which allows spammers, malicious code authors and other criminals to perform their activities easily (Security Alliance, 2010).

7.2.7. Insecure application programing interfaces

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. These interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability (Security Alliance, 2010).

7.3. Security threats originating from the virtual machines

7.3.1. Monitoring VMs from other VMs

One of the security risks encountered when using virtual machines is the lack of guaranteed isolation of the application and data when a shared resource such as memory space is utilized by multiple VMs. Cloud computing servers can contain tens of VMs and these are vulnerable to attack whether they are active or not. Active VMs are vulnerable to all of the security attacks that a conventional physical service is subject to. However, once a VM has been compromised by an attack on other VMs residing on the same physical server, they become all vulnerable to the same attack due to the fact that each machine shares memory, disk storage, driver software and hypervisor software (Ibrahim et al., 2010).

7.3.2. Virtual machine mobility

Virtual machines (VMs) which are disk images hosted in a hypervisor platform are easily copied or transferred to other locations. The ability to move and copy VMs poses a security risk because the entire system, applications and data can be stolen without physically stealing the machine (Wooley, 2011).

7.3.3. Threats on communications between virtual machines

VMs are allowed to communicate with other VMs running on the same physical equipment using channels such as the shared clipboard functions. Sharing resources such as memory, real or virtual network connections, between VMs can introduce possible security risks for each machine because there is the possibility that one or more of the VMs has been compromised by malicious programs (Ibrahim et al., 2010; Wooley, 2011).

In this section, we have cataloged fourteen distinct types of threats. To compute the MFC, we need to know the probability of the attack for each threat during one hour. Also, we need to fill the values of impact matrix IM. The IM matrix relates component failure to security threats; specifically, it represents the probability of failure of components given that some security threat has materialized. Tables 3 and 4 represent the impact matrix and the threat vector. For the values in Table 4 (150 entries), it comes from our empirical study (Ben Aissa, 2012) which has an immense source of references.

8. Illustration: a sample service provider

In the previous section, we have cataloged 14 security threats (Table 3); the impact matrix (Table 4) has 15 columns, one for each threat plus one for the absence of threats. Using the 3 Matrices (Stakes, Dependency and Impact) and the threat vector, we can compute the vector of mean failure costs as shown in Table 5 using the formula:

$$\mathrm{MFC} = \mathrm{ST} \circ \mathrm{DP} \circ \mathrm{IM} \circ \mathrm{PT}$$

9. Supporting a cloud computing business model

The security cost model enables us to rationalize security related decision making. We illustrate this premise by two concrete examples.

- *Pricing a security upgrade*. If the provider of cloud computing services has enhanced the security that it provides to its customers, and wants to know how much to charge customers for the security gains, then one way to do this is to compute the gain that each customer achieves as a result of enhanced security. This can be done by estimating the impact of the security enhancement on the various components of the MFC formula, computing the new MFC vector, and inferring the difference between MFC before and after the enhancement. For the sake of illustration, we consider that as a result of a security measure (e.g. an enhanced firewall), the threat vector has been reduced to the new value: PT' presented in Table 6.

  The gain in mean failure cost can then be estimated as:

$$(\Delta\mathrm{MFC}) = \mathrm{ST} \circ \mathrm{DP} \circ \mathrm{IM} \circ (\Delta\mathrm{PT})$$

  where $\mathrm{PT} = \mathrm{PT}' - \mathrm{PT}$. We find the hourly gain in MFC as shown in Table 7:

  Assuming that on average subscribers use the cloud computing service 100 h per month, we find the monthly gain in MFC.

  Table 8 shows the added value gained by subscribers as a result of enhanced security; whether the cloud computing provider wants to charge this amount to subscribers, or make it an option that subscribers can purchase, is a commercial decision; our cost model helps decision makers by putting a monetary value on the service that is delivered to subscribers.

- *Judging the cost effectiveness of a security enhancement*. For a given security enhancement measure, the cloud service provider can determine the cost effectiveness by comparing the cost of installing the enhancement vs. the gains in subscriber fees collected as a result of enhanced security (minus any subscriber loss that may result). This can be modeled as a Return on Investment (ROI) decision, and quantified by a ROI function, as discussed in BenAissa et al. (2010).

10. Conclusion: and Future work

Cloud computing is an emerging computing paradigm that offers end users the benefit of virtually unlimited computing resources, the convenience of professional system operation and maintenance, and the economy of on-demand billing. One advantage cloud computing does not offer is absolute security of subscriber data with respect to data integrity, confidentiality, and availability; security threats that arise in cloud computing include malicious activity, made possible by the provision of shared computing resources, as well as inadvertent loss of confidentiality or integrity resulting from negligence or mismanagement.

In this paper, we offer a quantitative model of security measurement that enables cloud service providers and cloud subscribers to quantify the risks they take with the security of their assets, and to make security related decisions on the basis of quantitative analysis, rather than psychological factors (fear, phobias, perceptions, etc.). Our proposed metric offers the following attributes:

- Security is measured in economic terms, enabling stakeholders to quantify the risks they incur as a result of loss of security, and to make decisions accordingly.
- Security is not an intrinsic attribute of the system, but also depends on stakeholders, and may take different values for different stakeholders, depending on the stakes they have in the secure operation of the system.
- The value of the MFC security metric reflects the heterogeneity of security requirements (some requirements carry more stakes than others), the heterogeneity of system architectures (some components are more security-critical than others), the heterogeneity of security threats (some threats are more menacing than others), and the heterogeneity of perpetrator behavior (some threats materialize more often than others).

We envision extending our current work in several directions, most notably:

- Refine the generic architecture of cloud computing systems, and use cloud-specific empirical data to refine the estimation of the dependency matrix and the impact matrix.
- Collect and maintain cyber security data pertaining to security threats, and use it to refine the estimation of the threat vector as it applies to cloud computing infrastructures.
- Use the concept of mean failure cost to support a quantitative economic model of could computing.

These issues are currently under consideration.

References

Armbrust M, Fox A, Griffith R, D. Joseph A and Katz R, "Above the Clouds: A Berkeley View of Cloud Computing". Technical report EECS-2009-28, UC Berkeley, 2009.

Ben Aissa, A., Abercrombie, R.K., Sheldon, F.T., Mili, A., 2010. Quantifying security threats and their potential impacts: a case study. Innovation in Systems and Software Engineering: A NASA Journal 6, 269–281.

Cloud Security Alliance, "Top Threats to Cloud Computing V 1.0", 2010. < https://cloudsecurityalliance.org/topthreats > .

Hanna, S., 2009. Cloud Computing: Finding the silver lining".

Ibrahim, A.S., Hamlyn-Harris, J., Grundy, J., 2010. Emerging "Security challenges of cloud virtual infrastructure". In: The Asia Pacific Software Engineering Conference 2010 Cloud Workshop.

Mell, P., Grance, T., 2009. Effectively and securely using the cloud computing paradigm. In: ACM Cloud Computing Security Workshop.

Mell, P., Grance, T., 2010. The nist definition of cloud computing. Communications of the ACM 53 (6), 50.

Subashini, S., Kavitha, V., 2010. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications.

Vaquero, L.M., Rodero-Merino, L., Caceres, J., Lindner, M., 2009. A break in the clouds: towards a cloud definition. ACM SIGCOMM Computer Communication Review 39 (1), 50–55.

Wang, L., von Laszewski, G., Kunze, M., Tao, J., 2008. Cloud computing: a perspective study. In: Proceedings of the Grid Computing Environments (GCE) workshop.

Wayne, J., Timothy, G., 2011. Guidelines on security and privacy in public cloud computing. Information Technology Laboratory.

Rittinghouse, J.W., Ransome, J.F., 2010. Cloud Computing: Implementation, Management, and Security. CRC Press, Boca Raton.

Wooley, P., 2011. Identifying Cloud Computing Security Risks. University of Oregon, Master's Degree Program.

Xuan, Z., Nattapong, W., Hao, L., Xuejie, Z., 2010. Information security risk management framework for the cloud computing environments. In: 10th IEEE International Conference on Computer and Information Technology (CIT 2010).

Foster, I., Zhao, Y., Raicu, I., Lu, S., 2008. Cloud computing and grid computing 360-degree compared. In: Grid Computing Environments Workshop: GCE 2008, pp. 1–10.

Vaughan-Nichols, S.J., 2008. Virtualization sparks security concerns. IEEE Computer 41 (8), 13–15.

Varia, J., 2008. Cloud architectures. Technology Evangelist Amazon Web Services.

Orea, J. et al., 2011. VisioTCI Reference Architecture (v2.12). Cloud Security Alliance.

Ben Aissa, A., 2012. Vers une mesure économétrique de la sécurité des systèmes informatiques". Doctoral dissertation, Faculty of Sciences of Tunis, submitted for publication.

Speaks, S., 2010. Reliability and MTBF overview. Vicor Reliability Engineering.

Jonsson, E., Pirzadeh, L., 2011. A framework for security metrics based on operational system attributes. In: International Workshop on Security Measurements and Metrics – MetriSec2011, Bannf, Alberta, Canada.

Barry, B., 2003. Value-based software engineering. ACM SIGSOFT Software Engineering Notes 28 (2), 4.

Barry, B., LiGuo, H., 2003. Value-based software engineering: a case study. IEEE Computer 36 (3), 33–41.

Barry, B., 2006. Value-based software engineering: overview and agenda. In: Biffl, S., Aurum, A., Boehm, B., Erdogmus, H., Grünbacher, P. (Eds.), Value-Based Software Engineering.

Brunette, G., Mogull, R., 2009. Security guidance for critical areas of focus in cloud computing V 1.2. Cloud Security Alliance.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuok, R., Molina, J., 2009. Controlling data in the cloud: outsourcing computation without outsourcing control. In: ACM Workshop on Cloud Computing Security (CCSW).

Carlin, S., Curran, K., 2011. Cloud computing security. International Journal of Ambient Computing and Intelligence 3 (1), 14–19.

Black, P.E., Scarfone, K., Souppaya, M., 2009. Cyber Security Metrics and Measures. Wiley Handbook of Science and Technology for Homeland Security.

The Center for Internet Security, The CIS Security Metrics v1.0.0, 2009. <https://www.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.0.0.pdf>.

Krutz, Ronald L., Dean Vines, Russell, 2010. In: Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley.

Ben Arfa Rabai L, Rjaibi N and Ben Aissa A, "Quantifying Security Threats for E-learning Systems", accepted in ICEELI'2012, Spring 2012.

Tsiakis, T., 2010. Information security expenditures: a techno-economic analysis. International Journal of Computer Science and Network Security (IJCSNS) 10 (4), 7–11.

Boehme, R., Nowey, T., 2008. Economic security metrics. In: Irene, E., Felix, F., Ralf, R. (Eds.), Dependability Metrics, 4909, pp. 176–187.

Zhang, X., Wuwong, N., Li, H., Zhang, X., 2010. Information security risk management framework for the cloud computing environments. In: 10th International Conference on Computer and Information Technology (CIT), pp. 1328–1334.

Foroughi, F., 2008. Information security risk assessment by using Bayesian learning technique. Lecture Notes in Engineering and Computer Science 2170, 91–95.

Mayer, N., 2009. Model-Based Management of Information System Security Risk. PhD Thesis.