Chapter 3
Towards New Quantitative Cybersecurity Risk Analysis Models for Information Systems: A Cloud Computing Case Study

Mouna Jouini and Latifa Ben Arfa Rabai

Abstract The objective of this chapter is to propose new quantitative models to assess security threats of information systems. We adopt methods for assessing the failure cost due to security breakdowns. In fact, the importance of quantifying security risk continues to grow as individuals, enterprises, and governments become increasingly reliant on information systems. Moreover, nowadays security of these deployed systems has suffered because they lack significant security measures and accurate information security risk assessment which is considered as an ongoing process of discovering, correcting, and preventing security problems by providing appropriate levels of security for information systems. In this context, we define economic security risk models to help managers to assess accurately the security threats: the internal mean failure cost and the external mean failure cost, respectively, MFCint and MFCext, which studied the threat space and identified the source of threats space risk by estimating their costs. Moreover, we define the mean failure cost extension (MFCE) model which is based on our hybrid threat classification model.

Keywords Cloud computing · Security quantification · Economic security models · Threats · Security requirements · Components · Stakeholders

M. Jouini (✉)
Strategies for Modelling and ARtificial inTelligence Research Laboratory (SMART Lab), Higher Institute of Management, University of Tunis, Tunis, Tunisia

L. Ben Arfa Rabai
Strategies for Modelling and ARtificial inTelligence Research Laboratory (SMART Lab), Higher Institute of Management, University of Tunis, Tunis, Tunisia

College of Business, University of Buraimi, Al Buraimi, Sultanate Oman

B. B. Gupta et al. (eds.), *Handbook of Computer Networks and Cyber Security*,
https://doi.org/10.1007/978-3-030-22277-2_3

1 Introduction

Organizations, governments, and individuals are facing many information security risks. These risks can cause serious damages that might lead to significant financial losses, breach of the confidentiality of sensitive information, or loss of integrity or availability of sensitive data. In fact, the financial (or economic) security threat loss to organizations could be significant. Recent literature has also documented significant costs related to information systems security breaches. For example, the 2015 Global State of Information Security Survey [2] reveals that a huge heists of consumer data were also reported in South Korea, where 105 million payment card accounts were exposed in a security breach in 2015. The survey compared also the security incidents cost in small and large organizations. In fact, it claimed that small organizations proved the exception in discovering compromises. That is to say companies with revenues of less than \$100 million detected 5% fewer incidents this year (in 2014) compared to 2009. However, larger companies have seen a huge increase in the numbers of incidents between 2009 and 2014. In fact, the number of incidents detected by medium size and large organizations (those with revenues of \$100 million to \$1 billion) jumped by 64% between 2009 and 2014.

Due to serious impacts of security threats, managers must find ways to retrieve and understand threats sources so as to mitigate them. To facilitate effective protection of information systems, we propose in this chapter two economic security risk models that estimate security threats failure of information system.

The chapter addresses quantitative cybersecurity models based on our threats classification models defined in our previous work [22] in order to accurately assess threats breaches. In fact, information system threat classifications help system managers to build their organizations' information systems with less vulnerabilities and implement information security strategies and thus protect their assets from these threats. The first model assesses security risk and let managers identifying the source of space intrusion (either internal or external) to propose appropriate counter measure to mitigate them. The second model is based on our threats classification model that allows studying the threats class impact instead of a threat impact as a threat varies over time. Furthermore, we illustrate the use of our quantitative security analysis model on Cloud Computing (CC) system.

This chapter is organized as follows: The first section presents the context of our chapter. The second section presents the motivation of our work. The third section shows an overview of Cloud Computing environment. The fourth section presents an economic cybersecurity model based on a threat source criterion that we called the internal mean failure cost model (MFC_{int}) and external mean failure cost model (MFC_{ext}). In addition, we provide a new method to validate our security risk models and illustrate their use using a Cloud Computing application. The fifth section introduces the mean failure cost extension (MFCE) model. Also, we validate the MFCE model and show an illustration on practical application of this model.

2 Motivation: Quantitative Cybersecurity Risk Assessment Models

To make effective security decisions, managers need to assess or estimate the cybersecurity breaches of the system and well characterize it. There are many measures in literature to support the analysis of how well a system meets its security objectives [4, 18, 20, 23, 40], and [21]. Several economic security risk assessment models exist in literature. We can cite, for example, the mean failure cost (MFC) model [3] that quantifies the security of information systems that we will present in this section.

2.1 Related Work

Although the ability of existing models to estimate the security breaches due to security threats and vulnerabilities may suffer from several limitations which motivate researchers to develop more models. Basically, there are two security risk analyses or risk assessment approaches: Qualitative and Quantitative methods that we are interested in this work.

Quantitative methods [5, 8, 9, 13, 14, 28, 33, 36, 37, 42], and [7] allow the definition of the consequences of security risks occurrence in a quantitative way. In fact, they estimate the costs in numerical values and hence give an accurate estimation of it. For example, the mean time to failure (MTTF) quantifies the failure rate of the system and the MFC model gives the cost per system stakeholder due to security breaches. However, the existing method analysis results are not precise and are even confusing. In fact, quantitative measures must depend on the scope and accuracy of defined measurement scale. Therefore, they fail to present accurate costs and precise results. On the other side, the analysis results must be enriched by qualitative descriptions to be more precise and comprehensive [5].

For example, in [28], the authors propose a SAEM method which is a cost–benefit analysis process for analyzing security design decisions based on the comparison of a “threat index.” The authors in [12] propose security ontology for organizing knowledge on threats, safeguards, and assets. This work constructs classification for each of these groups and creates a method for quantitative risk analysis, using its own framework. The work does not use known standards or guidelines as an input for its evaluation model, so desired mechanisms and countermeasures have to be defined in the process of risk analysis. The ENISA report [13] also provided an approach for risk assessment based on the estimation of risk levels on ISO/IEC 27005:2008. Security risk would be high if both the probability of the event and its impact are high. The assessment provided is semi-quantitative, as it uses value ranges for both event probability and impact, but does not consider their combined influence in a quantitative manner. Bojanc and Jerman suggested in [33] a model that evaluates the information assets, their vulnerability, and the threats to information assets. The values of the risk parameters are the basis for selecting the appropriate risk treatment and the evaluation of the various security measures that reduce security risks. Singh and Joshi proposed in [36] a risk assessment framework for University computing environment that reduces the security risk breach. The model supports three phase activities, the first phase assesses the threats and vulnerabilities in order to identify the weak point in educational environment, the second phase focuses on the highest risk and creates actionable remediation plan, the third phase of risk assessment model recognizes the vulnerability management compliance requirement in order to improve University's security position.

Yang et al. propose in [8] a measurement and assessment model of Cloud Computing based on Markov chain to describe random risk environment. The model used information entropy to measure risk, effectively reduced the existing subjective factors in the assessment process, provided a practical and reliable method for risk management decisions. Finally, Cayirci and de Oliveira introduce in [7] a quantitative security risk assessment model based on cloud service providers' performance history. The model addresses provider and consumer concerns by relying on trusted third parties to collect soft and hard trust data elements, allowing for continuous risk monitoring in the cloud.

We notice that the existing quantitative security risk models reflect the loss risk of the whole system and they ignore the variance stakes among different stakeholders. In fact, the operation of a system involves many stakeholders, who have different cares (stakes). These models ignore others factors like *the failure cost with respect to requirements, the variability of system threats*. Nevertheless, the mean failure cost (MFC) considers many factors that we will enumerate in the next section.

2.2 Mean Failure Cost Model (MFC): A Quantitative Cybersecurity Risk Assessment Model

The MFC [3] represents a stochastic model that quantifies this random variable in terms of financial loss per unit of operation time (e.g., $/h) due to security threats. It represents for each stakeholder the amount of loss that results from security threats and system vulnerabilities. The MFC varies by stakeholder and takes into account the variance of the stakes that a stakeholder has in meeting each security requirement. 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 have on these components.

The MFC process proceeds in four steps:

- Generation of Stakes Matrix (ST) which represents the cost that each stakeholder would lose if the system failed to meet a security requirement of the system.
- Generation of Dependency Matrix (DP) which represents how to estimate the probability that a particular security requirement is violated in the course of operating the system for some period of time.

- Generation of Impact Matrix (IM) which determines which threats affect which components and assesses the likelihood of success of each threat in light of perpetrator behavior and possible countermeasures.
- Generation of the Threat Vector (PT) which represents the probability that a threat materializes during unitary period of operation.

The mean failure cost is defined by the following formula:

$$MFC = ST \circ DP \circ IM \circ PT \tag{3.1}$$

We will propose in this chapter two new models extension of the mean failure model (MFC). In fact, the MFC model considers the following characteristics:

- It quantifies the cost in terms of financial loss per unit of operation time (dollars per hour).
- It quantifies the impact of failures: it provides cost as a result of security attacks. It offers decision support for security countermeasure design.
- It distinguishes between stakeholders: it provides cost for each system's stakeholder as a result of a security failure.
- It distinguishes between specification components: it considers that each system has many security requirements that represent concerns of the stakeholders.

However, the MFC model does not consider any classification threats and does not take into account any threat perspective either. In fact, such results take a global view at the threats targeting an information system which leads to inaccurate results.

2.3 Mean Failure Cost (MFC) Limits

Security threats may be originating from within or from outside threats that may be manifested, as well, via a threat agent using a particular penetration technique to cause dangerous effects [10, 29], and [22]. Thus, managers need to know and find threats that influence their assets and identify their impact to determine what they need to do to prevent attacks by selecting appropriate countermeasures. Then, they need to evaluate the extent of the damage caused by these threats.

Therefore, it is necessary to have an understanding of the threats and the vulnerabilities. Security threats can be observed and classified in different ways by considering different dimensions or classes of the system like its source code, attacker's motivation or its users, or their roles.

On the other hand, understanding and identifying the threats represent the first step in building a secure system. Indeed, to identify threats and evaluate existing control techniques, it is important to understand well security threat and especially security sources [1, 2, 6, 21, 22, 34], and [35]. Threats classification allows better identifying of threats characteristics and thus an accurate estimation of security risks. For example, if you know that there is a risk that someone could order products from your company but then repudiate receiving the shipment, you should ensure that you accurately identify the purchaser and then log all critical events during the delivery process [34]. Moreover, prior work has been based on the assumption that similar systems tend to produce similar vulnerabilities. For example, the kinds of vulnerabilities in a Windows operating system might be similar to those in the Linux operating system because both operating systems exhibit similar basic functionality [17].

Therefore, threats classification is an important task in security risk assessment models to assess accurately risks. After studying the MFC model in previous section, we notice that this model does not include threat classes and more especially it includes the following shortcomings:

- Security threats are evolutive and variable over time and have several characteristics, and in PT vector, there is no logical or hierarchical structure between the different catalogued threats as they are not based on a particular attribute to classify them.
- Underestimation of the MFC: In fact, in the threat vector PT, the term used to define the threat can be ambiguous (do not include threats classes); this can lead to an overlap between the various threats, i.e., each threat may belong to several classes at once and thus it is computed many times, so we have an underestimation of the mean failure cost.
- Managers cannot identify the source of threats risks in order to suggest appropriate countermeasures.
- The MFC is blind towards the structure and the dimensions of security threats. It considers that any failure due to a threat is a failure with respect to the whole specification. But stakeholders may have different stakes in different security threats dimensions and perspectives which are not reflected in the MFC.

We aim in this chapter to propose three cybersecurity metrics that overcome the limits of the mean failure cost model (MFC). We propose new metrics that take into account security threat dimensions or criteria that give accurate security risk assessment. The proposed models will be applied to a practical case study, namely a Cloud Computing system.

3 Cloud Computing Environments

Cloud Computing is the result of Information and Communication Technology (ICT) evolution. In fact, it is based on several technologies like virtualization, distributed systems, web service oriented architecture, service flows and workflows, and web 2.0. Two major events triggered the spread of Cloud Computing in 2006. The first was the announcement of a new business model, “Cloud Computing,” by Google CEO Eric Schmidt.

Cloud Computing is a system that enabling access to remotely hosted data and computation resources from anywhere. In the same year, Amazon.com announced one of themost important Cloud Computing services till date called Elastic Cloud Computing (EC2) [12].

The National Institute of Standards and Technology defines Cloud Computing as "a model which grants convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [26], and [27].

Cloud Computing plays an important role in many recent critical applications, such as astronomy, weather forecasting, and financial applications.

3.1 Cloud Computing Architecture

The Cloud Computing Architecture of a Cloud Computing system is the structure of the system which includes cloud resources, services, middleware, software components, and the relationships between them [4, 18], and [23]. It is composed mainly of two parts: the front end and the back end connecting 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 to 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. Figure 3.1 summarizes the proposed Cloud Computing architecture [4, 18], and [23].

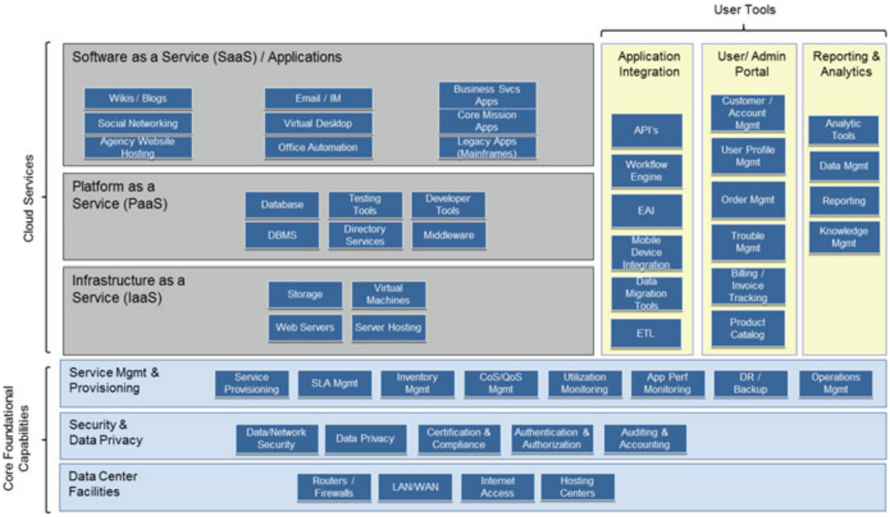


Fig. 3.1 Cloud computing services and architecture

Cloud Computing providers can offer services at different layers:

- Infrastructure as a Service (IaaS): This layer provides the basic computing infrastructure of servers, processing, storage, networks where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.
- Platform as a Service (PaaS): This layer provides a platform upon which applications can be written or deployed.
- Software as a Service (SaaS): This layer delivers applications through a web browser to thousands of customers without having to be installed on their computers.

3.2 Cloud Computing Security Issues

In the last few years, the Cloud Computing reveals a remarkable potential to provide on-demand services to users with greater flexibility in a cost-effective manner. While moving towards the concept of on-demand service, resource pooling, shifting everything on the distributive environment, security is the major obstacle for this new dreamed vision of computing capability. In fact, users' data are stored outside the cloud in data centers where risks out number rewards. In fact, customers' data in the Cloud are stored on multiple third-party servers and thus it is not cared by the user and no one knows where exactly data are saved. Among these we mention the loss of control and the loss of security [22, 24, 30, 36, 38, 41], and [39]. Indeed, by trusting critical data to a service provider (externalization of service), a user (whether an individual or an organization) takes risks with the availability, confidentiality, and integrity of this data. For example, 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) and integrity may be affected if the subscriber's data is inadvertently or maliciously damaged or destroyed.

Many surveys deal with security risks in Cloud environment. For example, according to a Forbes' report published in 2015, cloud based security spending is expected to increase by 42%. According to another research, the IT security expenditure had increased to 79.1% by 2015, showing an increase of more than 10% each year. International Data Corporation (IDC) in 2011 showed that 74.6% of enterprise customers ranked security as a major challenge [15, 16, 38], and [11].

In addition, Cloud Computing is based on several technologies like virtualization that may cause major security risks which can be classified into three categories like virtual machine modification, denial of service, monitoring virtual machines from host (MVM), communications between virtual machines and host (CBVH), etc. [4, 18], and [23].

We propose in this section classification of CC security issues into nine subcategories [19], which include: virtualization security issues, business services continuity, management interfaces risks, privacy issues, data location, data breaches, accountability problems, multi-tenancy problem, and regulation and governance problem.

Security Issues in Virtualization Cloud Computing architecture is based on many virtualization components such as hypervisor and virtual machine. Hypervisor is a controller known also as virtual machine manager (VMM), which allows multiple operating systems to be run on a system at a time. Since multiple operating systems may be running on a single hardware platform, it is not possible to keep track of all such systems and hence maintaining the security of the operating systems is difficult. In this case, guest system can run malicious code on the machine system and bring the system down or take full control of the system and block access to other guest operating systems [22], and [41]. Malicious insiders are very serious attacks; hence, it presents an opportunity for an adversary to harvest confidential data or gain complete control over the Cloud services with little or no risk of detection [22, 41], and [11].

Business Services Continuity One more availability problem in CC environment is distributed denial of service (DDoS) attacks. Attackers make use of large botnets (zombies) to reduce the profits of SaaS providers by DDoS by making their services unavailable [13]. Furthermore, a major risk to services continuity in the Cloud Computing environment is loss of internet connectivity (that could occur due to some circumstances like natural disasters) as Cloud businesses are dependent on the internet access to their information. In addition, there are also concerns that the seizure of a data hosting server by law enforcement agencies may result in the unnecessary interruption or cessation of unrelated services whose data are stored on the same physical machine. This resulted in the unintended consequence of disrupting the continuity of businesses whose data and information are hosted on the seized hardware.

Management Interfaces Risks Cloud Computing providers expose a set of software interfaces that customers use to manage and interact with Cloud services (like provisioning, management, orchestration, and monitoring). The customer management interfaces of public Cloud providers are Internet accessible and mediate access to larger sets of resources and therefore pose an increased risk especially when combined with remote access and web browser vulnerabilities [13]. Unauthorized access to the management interface is therefore an especially relevant vulnerability for Cloud systems. These interfaces must be designed to protect against both accidental and malicious attempts because they allow authentication and access control to encryption and activity monitoring that depend directly on the security and availability of general Cloud services [11].

Data Breaches Cloud Computing system allows the storage of customer data in different ways. In fact, data in Cloud systems travel in clusters, in virtual machines, in databases, or into third-party storages, which increase the risk of information leak and data corruption. Indeed, operations in data centers might lead to information leak caused, for example, by a customer's information being mistaken by another's.

Furthermore, most of the Cloud providers instead of acquiring a server try to rent a server from other service providers because they are cost affective and flexible for operation. This gives a high possibility for malicious insiders to steal customers' data from the external server [12, 22], and [41].

Compliance and Governance As security in Cloud Computing systems presents a big challenge, cloud vendor has to provide some assurance in service level agreements (SLA) to convince the customer on security issues. The SLA illustrates different security levels and tries to make the customer understand the security policies that are being implemented. Customers may also in the SLA indicate its expectations in terms of security for these types of systems. Providers must deliver a comprehensive list of regulations that govern the system and associated services and how compliance with these items is executed [22], and [11]. However, the SLA may not offer a promise to provide such services on the part of the Cloud provider which can create several security breaches (for example, meet privacy and confidentiality needs) for many reasons. In fact, Cloud providers cannot give evidence of their own conformity with the relevant requirements and do not permit external audit by the Cloud customer and/or security certifications [11, 22, 41], and [13].

In addition, a more serious problem is that there is no way to specify the policies on how sensitive data are shared, treated, and located among Cloud service providers. In fact, information is routinely leaked with poor data management practices. Cloud service providers must ensure, for example, the data security in natural disasters. Indeed, there are certain legal issues entangled with Cloud security as well, because there are certain laws that Cloud service providers should comply with and these laws vary from country to country which may cause data replication across multiple sites.

Access Problem: Data Location Cloud Computing environments suffer from lack of transparency since customer' data are located in Cloud provider data centers and anywhere in the world, and hence are out of the customer's control which leads to many problems [11, 22, 32, 41] and [13]. In fact, the user space may be shared across applications that can lead to data replication, making mapping of users and their privileges a complicated task. This, also, requires the user to remember multiple accounts/passwords and maintain them which may entail forgetting them in many cases. Indeed, by using the Cloud, users need to look at who (their role and their privileges, etc.) is managing (get access to) their data (when they release the information into the Cloud for processing) and what types of controls are applied to these individuals [11, 31], and [16].

Data breaches present a crucial problem for organizations. For example: many organizations such as financial institutions, health care providers, and government agencies are legally required to protect their data from compromise due to the sensitivity of their information. Generally, these organizations are required to manage and maintain their own datacenters with stringent physical and logical protection mechanisms ensuring that their data remain protected. These organizations simply cannot utilize Cloud Computing in a generic manner due to the inherent risk of data compromise from systems they do not control.

Privacy Issues Privacy problems in Cloud Computing environments come from many reasons. First, Cloud Computing customer's data and especially personal information can be breached more easily than if stored in users' machines. In fact, customer's data are stored in services provider's data centers and thus it is not guaranteed if the providers will protect their data and especially their personal information. Indeed, as most of the servers are external, the provider should make sure who is accessing the data and who is maintaining the server to protect the customer's personal information. Also, in the shared infrastructure, customers' private information risk more potential unauthorized access and exposure [22, 41], and [13].

Moreover, privacy problems for organizations stem from the diversity of privacy regulations from country to country. In fact, data in Cloud system are stored anywhere and user cannot guess if you are violating privacy regulations in the countries where you operate [22, 41], and [13]. Indeed, there is a need for approaches to label directly the data with security and privacy policies that would travel with sensitive data from one provider to another so that the proper technical controls can be employed by various Cloud providers to protect the data [32]. Data are prone in this case to many attacks like: sniffing, spoofing, man-in-the-middle attacks, side channel, and replay attacks and so in some cases the CP does not guarantee respect for the confidentiality or the nondisclosure of information [13].

Isolation Failure (Multi-Tenancy Problem) Multi-tenancy and shared resources (computing capacity, storage, network, memory, routing, etc.) represent main characteristics of Cloud Computing environments. There is a risk of failure of deferent mechanisms between different tenants of the shared infrastructure due to principally hypervisor vulnerability. In fact, infrastructure as a service (IaaS) Cloud layer relies on architectural designs where physical resources are shared by multiple virtual machines and therefore multiple customers. In fact, resource sharing means that malicious activities (spamming, port scanning, etc.) carried out by one tenant may affect and get access to another tenant host [13].

Accountability Problems Accountability has to do with keeping track of actions that are related to security actions and responsibilities [41]. It aims to give tracking evidence on user behaviors and system status, which can also be used in system performance analysis or intrusion detection purposes.

As security is the most concern for Cloud Computing adoption, we propose in this chapter secutiy metrics to quantify cybersecurity risk in order to let managers to select appropriate countermeasures.

4 MFC_{ext} and MFC_{int}: New Quantitative Security Risk Assessment Models

In this section, we illustrate an extension of the MFC model [3] by suggesting a classification of the identified threats to propose two types of measures: The Internal MFC (MFC_{int}) and the External MFC (MFC_{ext}) in order to know the source of threats shaped information systems and especially the Cloud Computing systems to take appropriate security strategies or mitigate their effects.

4.1 Security Threat Space Intrusion

Threat source or threat space intrusion represents a primordial criterion for identifying threat source in order to take appropriate security decisions. For the purpose of our system, we propose to classify the threat space into subspaces according to a model of three dimensions labeled Internal, External, and InternalExternal. This classification allows to localize the origin (or source) of a threat. In fact, threat is caused either from within an organization, system, or/and architecture or from an external point of origin [18].

4.1.1 Internal Threats

Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network. A threat can be internal to the organization as the result of employee action or failure of an organization process [18].

Regarding internal attacks, we can cite theft of proprietary information, accidental or non-malicious breaches, sabotage, fraud, and eavesdropping/snooping as instances of insider threats.

4.1.2 External Threats

External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers. The most obvious external threats to computer systems and the resident data are natural disasters like hurricanes, fires, floods, and earthquakes. External attacks occur through connected networks (wired and wireless), physical intrusion, or a partner network [18].

Lacey et al. provide an updated profile of sophisticated outside attacks which can compromise the security of Mobile Ad hoc Network (MANET) [25]. They include eavesdropping, routing table overflow, routing cache poisoning, routing maintenance, data forwarding, wormhole, sinkhole, byzantine, selfish nodes, external denial of service, internal denial of service, spoofing, Sybil, badmouthing, viruses, and flattering.

4.1.3 Internal/External Threats

Internal/external threats take place when someone having authorized access to the network (for example, an employee of the organization) causes external threats to the system [18].

4.2 MFC_{ext} and MFC_{int}: The Proposed Model

The threats vector is a vector of probabilities of attack to the system during a time unit. These threats, as we said above, come from external or internal boundaries of the system. This classification lets us to propose two new extension of the threat vector (PT) of the MFC metric. Consequently, there will be two extensions measures of the mean failure cost (MFC). We can calculate the external mean failure cost MFCext and the internal mean failure cost MFCint. Depending on the attack space vector AS, the new MFC formula will be

$$MFC_{ext} = ST \circ DP \circ IM \circ PT \circ AS_{ext} \tag{3.2}$$

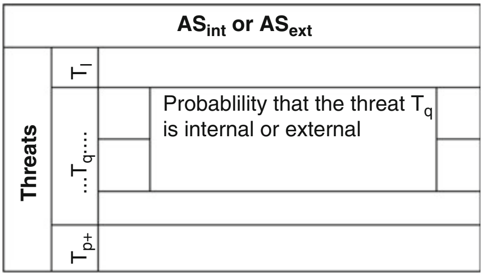
and

$$MFC_{int} = ST \circ DP \circ IM \circ PT \circ AS_{int} \tag{3.3}$$

AS_{int} and AS_{ext} are two vectors having the same dimension of the threat vector PT containing the probability values of threat related to intrusion types (internal or external). Figure 3.2 shows AS_{int} and AS_{ext} structures.

These new extensions of MFC model improve analysis of the vulnerability of the system. They allow specifying the nature of security solution that minimizes the mean failure cost.

Fig. 3.2 Space intrusion vector



4.3 Illustration of the Cybersecurity Model: A Cloud Computing System

In this section, we illustrate the use of the MFC_{int} and the MFC_{ext} in a Cloud Computing system [4]. We identify, hence, the threats intrusion space in Cloud system through the extension mentioned above.

We identify, firstly, the security requirements, the stakeholders and their stakes in meeting these requirements, the architectural components, and the security threats that affect the Cloud Computing system. Then, we fill the matrixes ST, DP, ICM, CM, and PT using empirical data from [38] to obtain the following MFCext and MFCint vectors.

We consider four classes of stakeholders (as described in Sect. 3) in this case study, namely: a Cloud Computing provider (PR), a corporate subscriber (CS), a governmental subscriber (GS), and an individual subscriber (IS).

As for security requirements, we identify seven generic security requirements classified based on the levels of criticality of data as shown in our previous work [4], and [23], namely:

- Availability of critical data (AVC),
- Availability of archival data (AVA),
- Integrity of critical data (INC),
- Integrity of archival data (INA),
- Confidentiality of classified data (CC),
- Confidentiality of proprietary data (CP), and
- Confidentiality of public data (CB).

Based on a quantification of these stakes in terms of thousands of dollars ($K) per hours of operation, we produce the following stakes matrix ST as shown in Table 3.1.

Based on the Cloud Computing system architecture defined in our previous work [4], and [18], we generate the dependency matrix shown in Table 3.2. We consider that the Cloud Computing system components include: a browser (Br), a proxy server (Prx), a router/firewall (R/F), a load balancer (LB), a web server (WS), an application server (AS), a database server (DS), a backup server (BS), and a storage server (SS).

Table 3.1 Matrix of stakes: cost of failing a security requirement in $K/h

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

Table 3.2 Dependency matrix

	Components									
	Br	R/F	LB	WS	AS	DB	BS	SS	NoF	
Security requirements										
AVC	0.14	0.14	0.14	0.14	0.06	0.04	0.14	0.06	0.14	0
AVA	0.16	0.16	0.16	0.16	0.07	0.05	0.05	0.03	0.16	0
INC	0.03	0.03	0.2	0.2	0.09	0.03	0.2	0.02	0.2	0
INA	0.04	0.04	0.32	0.32	0.14	0.04	0.04	0.01	0.32	0
CB	0.1	0.03	0.23	0.23	0.1	0.1	0.1	0.01	0.1	0
CP	0.1	0.03	0.23	0.23	0.1	0.1	0.1	0.01	0.1	0
CC	0.1	0.03	0.23	0.23	0.1	0.1	0.1	0.01	0.1	0

Table 3.3 Probability of threat space intrusion

Threats	Probability outsider committed	Probability insider committed
(MVM)	1	0
(BVH)	1	0
(VMm)	0.6	0.4
(VMS)	1	0
VMM)	0.5	0.5
(VMC)	0.5	0.5
VMM)	0.6	0.4
(DoS)	0.136	0.864
(FA)	1	0
(DL)	0.8	0.2
(MI)	0	1
(ASTH)	1	0
(ANU)	0	1
(IAI)	0.8	0.2

Using empirical data from [3], we can decompose the probability of event threat committed in two complementary probabilities (outsider/insider system committed) as shown in Table 3.3.

We have catalogued fourteen distinct types of threats (Table 3.5). To compute the MFC_{ext} and the MFC_{int} we need to know the probability of the attack for each threat during 1 h. 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 3.4 and 3.5 represent the impact matrix and the threat vector.

Thus, we compute the mean failure cost of external threats (see Table 3.6) and the mean failure cost of internal threats (see Table 3.7) using the formulas presented above. Entries of these three matrices and the two vectors come from our empirical study [3] which has an immense source of references.

Table 3.4 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 3.5 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 (MVV)	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 programming interfaces (IAI)	29.026×10^{-4}
No threats (NoT)	0.9682

Table 3.6 The MFC of external threats

Stakeholders	MFC_{ext}($K/h)
PR	10.61051
CS	2.46562
GS	6.278502
IS	0.002382

Table 3.7 The MFC of internal threats

Stakeholders	MFC_{int}($K/h)
PR	4.5932
CS	1.07261
GS	2.7060
IS	0.001035

Computing the new values of the MFC extensions can give us the critical space of intrusion. In our case, we can adapt some solutions like adding more firewalls, proxy servers, and antivirus servers. In fact, the MFCext values for Cloud systems are more significant compared to the MFCint values and hence the Cloud security risks come mainly from external threats.

The MFC_{ext} and the MFC_{int} give the critical threats space to help managers to take the appropriate countermeasures. They improve the analysis of the system vulnerability. They specify the type of solution to minimize the average cost of failure. In fact, using the threat classification source dimension, they allow identifying the source of the threats space (either internal or external source) to let managers concentrate on the intrusion space having the higher mean failure costs. However, this quantification is not sufficient since threats have several dimensions like motivation and intention that we must take into account. Therefore, these models do not provide accurate estimation of costs resulting from threats breaches.

4.4 Validation of the MFC_{int} and the MFC_{ext}

System stakeholders seek secure information systems to reduce cost and protect their assets from damage and ensure the confidentiality, availability, and the integrity of information. To help stakeholders, the MFC metric gives a quantitative value of security system without any qualification as the security quantification did not allow deciding whether the system is secured or not. The question for all stakeholders is whether their system is secure or not.

For this purpose, we propose to find an interval that classifies the security of information systems. Thus, we propose to find lower and upper bounds of this interval which present, respectively, the mean failure cost for a 100% secure and a 100% unsecure system. In fact, the lower bound Blow represents a secure system with the minimum cost and the upper bound Bupp represents an unsecure system with a maximum cost. Therefore, we say that a system is secure if its MFC is lower than the average between the upper bound and the lower bound, that is, if the $MFC < ([Blow + Bupp]/2)$ and the system is not secure if $MFC > ([Blow + Bupp]/2)$. Finally, we proceed to the classification of our MFC as secure or not.

Assuming that the system is secure, the probabilities of system components failure are very low see null. For this goal, we modify the impact threat classes matrix ICM as follows: we put 0 for lines, 1 at the last column, and the last line is made complementary to the columns and the equilibrium of the line. For an unsecure system, we make the reverse of founded bounds.

We compute, finally, the lower bound vector of mean failure costs and the upper bound vector of MFC as shown in Tables 3.8 and 3.9, using our new formula.

To validate our MFC external vector (MFC_{ext}) and the MFC internal vector (MFC_{int}) presented in Tables 3.10 and 3.11 for Cloud Computing system, we propose to evaluate the stakeholders' security costs in order to decide if this system is secure or not.

Table 3.8 MFC_{ext} lower bound

Stakeholders	MFC_{ext} ($K/h)
PR	14.92
CS	3.222
GS	10.38
IS	0.0032

Table 3.9 MFC_{ext} upper bound

Stakeholders	MFC_{ext} ($K/h)
PR	4400.5
CS	1001.6
GS	2805.5
IS	1.029

Table 3.10 MFC_{int} lower bound

Stakeholders	MFC_{int} ($K/h)
PR	12.899
CS	2.759
GS	9.120
IS	0.0027

Table 3.11 MFC_{int} upper bound

Stakeholders	MFC_{int} ($K/h)
PR	4260.564
CS	969.749
GS	2716.285
IS	0.9969

For the MFC external model, we notice that for each stakeholder the MFCext value is lower than ($[Blow + Bupp]/2$) ($MFC_{ext} < [Blow + Bupp]/2$); thus, the system is secure. For the MFCint vector, for each stakeholder we notice as well that MFCint value is lower than ($[Blow + Bupp]/2$) ($MFC_{int} < [Blow + Bupp]/2$); thus, the system is secure. Thus, we can deduce that Cloud Computing environment is a secure system.

In addition to the contribution of the application of MFC model, we can say that in certain level of Cloud Computing services like the infrastructure as a service layer (IaaS), it is very difficult to specify a threat in a system component because we can find a large number of components, in this layer, so it can be better to associate a class of threats rather than a specific threat for each component. Indeed, as countermeasures, one solution will solve several problems rather than one problem.

4.5 MFC_{ext} and MFC_{int} Limits and Advantages

The MFCext and MFCint models present several advantages. In fact, they can identify the source of the most severe threats causing risk to let managers take the necessary countermeasures against this intrusion space. So, these models take into account the source criterion of security threats.

As these models do not take into account all threats characteristics and just consider one criterion which does not accurately describe a security threat (the source of a threat), they do not give accurate values on the cost of security failure.

On the other hand, the considered criteria are based on a binary classification (internal or external), while threat sources may include three subclasses. Subsequently, these models do not illustrate accurate estimation of security failure cost values. In addition, the underestimation of security threat risk presented does not let managers propose adequate security strategies to mitigate the risk.

5 The MFC Extension Model (MFCE)

In the next section, we will suggest two cybersecurity measures in order to better quantify system threats using the source dimension of security threats. In this section, we propose a new cybersecurity metric referred to as mean failure cost extension (MFCE), based on threats classification and especially on the hybrid threat classification (HTC) model [22]. We, then, illustrate this infrastructure by means of a Cloud Computing application.

5.1 The MFCE Model

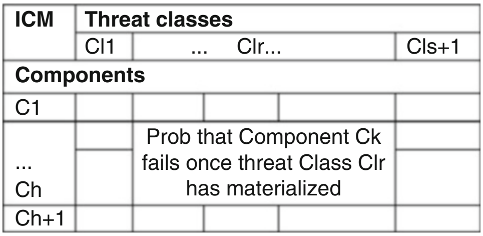
In order to improve the estimation of the costs due to security breakdowns, we propose a quantitative security threats model based on our threats classification (HTC) [22]. We propose a security solution per threat class. For this reason, we propose a novel model in which we focus on refining the estimation of the impact matrix IM and the threat vector PT of the mean failure cost (MFC) model introduced in Sect. 3. We call this model the MFC extension model (MFCE) [18]. Our cybersecurity model allows studying the impact of a whole class of threats rather than a mere threat. Indeed, threats are variable in time and security solutions change over time. The basic idea is to consider a class of threats, try to find solutions to this class, and consider the probability that a class is present will be the average of the probabilities of present threats in this class threats in order to achieve a certain stability of this class in time. This allows converging towards a stability of existence of a class [18].

For the impact matrix IM, we generate two matrices: the new impact matrix IMC and the threat classes matrix CM, as shown in Figs. 3.3 and 3.4. Thus, the MFC extension (MFCE) has the following new formula:

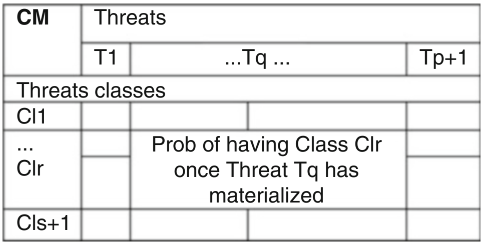
$$MFCE = ST \circ DP \circ ICM \circ CM \circ PT \tag{3.4}$$

The MFCE model represents a cybersecurity metric as a decision-making technique to derive relevant decision-making security solutions. This quantitative

Fig. 3.3 The impact threat classes matrix structure



ICM	Threat classes				
	Cl1	... Clr...			Cls+1
Components					
C1					
... Ch		Prob that Component Ck fails once threat Class Clr has materialized			
Ch+1					



CM	Threats		
	T1	...Tq ...	Tp+1
Threats classes			
Cl1			
... Clr		Prob of having Class Clr once Threat Tq has materialized	
Cls+1			

Fig. 3.4 The threat classes matrix structure

decision-making metric allows selecting countermeasures per threats class rather than a threat to better study and identify security threats.

5.2 *Illustration of the MFC Extension Model: Cloud Computing System*

We illustrate in this section the application of our new cybersecurity metric (MFC extension model) on the same computing system in order to compare the derived results.

We identify, firstly, the security requirements, the stakeholders and their stakes in meeting these requirements, the architectural components, and the security threats that affect the Cloud Computing system. Then, we used the matrixes ST, DP, and PT defined in the previous section. These matrices are shown in Tables 3.1, 3.2, and 3.5.

5.2.1 The Impact Threats Classes Matrix

The following step in our model is to derive the impact threat classes matrix, i.e., the derivation of the set of threat classes we wish to consider in our system. We applied our hybrid threat classification presented in previous work [22] on this case study to generate threat classes. In fact, we proposed in earlier work [22] a dynamic and multidimensional threat classification model that allows better defining and articulating of threat characteristics [18]. The model contains the following criteria:

- Threat source: Origin of threat either internal or external.
- Threat agents: Agents that cause threats that can be human, accidental environmental or technological.
- Security threat motivation: Goal of attackers on a system which can be malicious or non-malicious.
- Security threat intention: The intent of the human who caused the threat that is intentional or accidental.

Thus, the classes we have are presented in Table 3.12.

Table 3.12 Security threat classes for Cloud Computing system

Security threat	Classes description
IHMA	Insider human malicious accidental threat
IHMI	Insider human malicious intentional threat
IHNMA	Insider human non-malicious accidental threat
IHNMI	Insider human non-malicious intentional threat
OHMA	Outsider human malicious accidental threat
OHMI	Outsider human malicious intentional threat
OHNMA	Outsider human non-malicious accidental threat
OHNMI	Outsider human non-malicious intentional threat
EV	Environmental threat
IT	Insider technological threat
OT	Outsider technological threat

Components in a system may fail to meet security requirements due to malicious activity when a threat class is materialized. The ICM matrix represents eleven columns, one for each threat class plus one for the absence of threats classes (NoC), and ten rows, one for each component plus one for the event that no component has failed during one period of time (NoF). The impact threats classes matrix is given in Table 3.13 [18].

5.2.2 The Threat Classes Matrix

The threat classes matrix (Table 3.14) shows that each security threat belongs at most to one threat class, that is, each threat has its proper characteristics. In CM matrix, columns represent security threats (the last column represents the absence of threat (NoT)), rows represent threat classes, and a cell CM(q, s) represents the probability of having Class Clr once Threat Tq has materialized: if a class defines n threats, then this is 1/n and 0 if it is outside.

We have catalogued fourteen distinct types of threats and eleven threat classes. To compute the MFC extension (MFCE), we need to know the probability of the attack class for each threat during 1 h. We need also to fill the values in Table 3.14, they come from our empirical study [3].

Using the four Matrices (stakes, dependency, impact threat classes, and threat classes) and the threat classes vector, we can compute the vector of mean failure costs extension (Table 3.15) for each stakeholder of Cloud Computing system using the formula:

$$MFCE = ST \circ DP \circ ICM \circ CM \circ PT \qquad (3.5)$$

The MFC vector is shown in Table 3.15.

Table 3.13 Impact threat classes matrix

	Threats classes											
	IHMA	IHMI	IHNMA	OHMA	OHMI	OHNMA	OHNMI	EV	ASTH	IT	OT	NoT
Components												
Brws	0.011	0.03	0.005	0.015	0.04	0.027	0.02	0.013	0.01	0.03	0.03	0.769
Prox	0.011	0.03	0.005	0.015	0.04	0.027	0.02	0.013	0.01	0.03	0.03	0.769
R/FW	0.011	0.03	0.005	0.015	0.04	0.027	0.02	0.013	0.01	0.03	0.03	0.769
LB	0.011	0.03	0.005	0.015	0.04	0.027	0.02	0.013	0.01	0.03	0.03	0.769
WS	0.011	0.03	0.005	0.015	0.04	0.027	0.02	0.013	0.01	0.03	0.03	0.769
AS	0.011	0.03	0.005	0.015	0.04	0.027	0.02	0.013	0.01	0.03	0.03	0.769
DBS	0.011	0.03	0.005	0.015	0.04	0.027	0.02	0.013	0.01	0.03	0.03	0.769
BS	0.011	0.03	0.005	0.015	0.04	0.027	0.02	0.013	0.01	0.03	0.03	0.769
SS	0.011	0.03	0.005	0.015	0.04	0.027	0.02	0.013	0.01	0.03	0.03	0.769
NoF	0.09	0.08	0.09	0.09	0.08	0.08	0.09	0.09	0.09	0.08	0.08	0.06

Table 3.14 Threat classes matrix

	Threats														
	MVH	CVH	VMm	VMS	MVV	VMC	VMM	DoS	FA	DL	MI	ASTH	ANU	IAI	NoT
Threats classes															
IHMA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
IHMI	0	0	0	0	0	0	0	0.33	0	0	0.33	0	0.33	0	0
IHNMA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
IHNMI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
OHMA	0.5	0	0	0	0	0	0	0	0	0	0	0	0	0.5	0
OHMI	0.25	0.25	0	0	0	0	0	0	0	0.25	0	0.25	0	0	0
OHNMA	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
OHNMI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
EV	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
IT	0	0	0	0	0.5	0.5	0	0	0	0	0	0	0	0	0
OT	0	0	0	0.5	0	0.5	0	0	0	0	0	0	0	0	0
NoC	0.05	0.083	0.13	0.05	0.05	0.05	0.13	0.08	0	0.083	0.08	0.083	0.08	0.05	0

Table 3.15 Stakeholder mean failure cost extension

Stakeholders	MFCE ($K/h)
PR	280.551
CS	63.856
GS	178.863
IS	0.065

Table 3.16 MFC lower bound

Stakeholders	MFC ($K/h)
PR	8.018
CS	1.824
GS	5.111
IS	0.001

Table 3.17 MFC upper bound

Stakeholders	MFC ($K/h)
PR	1923.666
CS	437.846
GS	1226.416
IS	0.065

5.3 Validation of the MFCE Model

Using the same method presented in the previous section, we calculate the upper and the lower bounds for the mean failure cost extension (MFCE) model.

Assuming that the system is secure, the probabilities of failure of system components are very low see null. For this goal, we modify the impact threat classes matrix ICM as follows: we put 0 for lines, 1 at the last column, and the last line is made complementary to the columns and the equilibrium of the line. For an unsecure system, we make the reverse of founded bounds.

We compute, finally, the lower bound vector of mean failure costs and the upper bound vector of MFC as shown in Tables 3.16 and 3.17, using our new formula.

To validate our MFC extension vector (MFCE) presented in Table 3.15 for Cloud Computing system, we propose to evaluate the stakeholders' security costs in order to decide if this system is secure or not. As we notice that the MFC values for Cloud Computing system are lower than the average of the MFC bounds for each stakeholder presented in Tables 3.16 and 3.17, so we can say that Cloud Computing environment is a secure system.

6 Conclusion

Security represents a major problem for information systems and organizations must estimate costs due to security breaches. Security risks are caused by various interrelated internal and external factors. A security vulnerability could also propagate and escalate through the causal chains of risk factors via multiple paths, leading to different system security risks. In order to estimate threats risks we propose three models that are based on threats classification. The MFC_{int} and the MFC_{ext} are based on the threat source dimension to identify the source of threat space. The MFCE enables a system's stakeholders to quantify the risks they take with the security of their assets and it is based on the HTC model. In addition, we propose to qualify security breaches costs by suggesting a cost interval to classify the security quantification for information system to decide whether the system is secure or not. These security analysis models enable organizations to predict the financial costs to lose due to threats breaches, which is validated via a case study.

We envision to develop an extendable quantitative security risk assessment model that considers several threats dimensions to give more accurate security loss values.

References

1. AhmadKhan, M. (2016). A survey of security issues for cloud computing. *Journal of Network and Computer Applications, 71*, 11–29.
2. Applegate, D. S., & Stavrou, A. (2013). Towards a cyber conflict taxonomy. In *5th International Conference on Cyber Conflict*.
3. Ben Aissa, A., Abercrombie, R. K., Sheldon, F. T., & Mili, A. (2010). Quantifying security threats and their potential impact: A case study. *Innovation in Systems and Software Engineering, 6*(4), 269–281.
4. Ben Arfa, L., Jouini, M., Ben Aissa, A., & Mili, A. (2013). A cybersecurity model in cloud computing environments. *Journal of King Saud University Computer and Information Sciences, 25*(1), 63–75.
5. Boehme, R., & Nowey, T. (2008). Economic security metrics. In E. Irene, F. Felix, & R. Ralf (Eds.), *Dependability metrics* (Vol. 4909, pp. 176–187).
6. Bompard, E., Huang, T., Wu, Y., & Cremenescu, M. (2013). Classification and trend analysis of threats origins to the security of power systems. *Electrical Power and Energy Systems, 50*, 50–64.
7. Cayirci, E., & de Oliveira, A. S. (2018). Modelling trust and risk for cloud services. *Journal of Cloud Computing, 7*(1), 14.
8. Cayirci, E., Garaga, A., De Oliveira, A. S., & Roudier, Y. (2016). A risk assessment model for selecting cloud service providers. *Journal of Cloud Computing, 5*(1), 14.
9. Chanchala, J., & Singh, U. K. (2016). Quantitative information security risk assessment model for university computing environment. In *International Conference on Information Technology (ICIT)*.
10. Chandran, S., Hrudya, P., & Poornachandran, P. (2015). An efficient classification model for detecting advanced persistent threat. In *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*.
11. Cloud Security Alliance. (2018). *The treacherous - Top threats to cloud computing + industry insights*.
12. Demchenko, Y., Gommans, L., de Laat, C., & Oudenaarde, B. (2005). Web services and grid security vulnerabilities and threats analysis and model. In *Proceedings of 6th IEEE/ACM International Workshop on Grid Computing*.
13. ENSIA. (2010). Report on cloud computing security risk assessment. http://www.enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-risk-assessment

14. Feng, N., Wang, H. J., & Li, M. (2013). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information Sciences, 256*, 57–73.
15. Gens, F. (2011). *New IDC IT cloud services survey: Top benefits and challenges. IDC eXchange 2011*. http://blogs.idc.com/ie/?p=730
16. Gururaj, R., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. In *International Workshop on Cyber Security and Digital Investigation (CSDI)* (Vol. 110, pp. 465–472).
17. Igure, V., & Williams, R. (2008). Taxonomies of attacks and vulnerabilities in computer systems. *Communications Surveys & Tutorials, 10*(1), 6–19.
18. Jouini, M., Ben Aissa, A., Ben Arfa, L., & Mili, A. (2012). Towards quantitative measures of information security: A cloud computing case study. *International Journal of Cyber Security and Digital Forensics, 1*(3), 265–279.
19. Jouini, M., & Ben Arfa, L. (2014). Surveying and analyzing security problems in cloud computing environments. In *Tenth International Conference on Computational Intelligence and Security, CIS 2014* (pp. 689–693).
20. Jouini, M., & Ben Arfa, L. (2016). Comparative study of information security risk assessment models for cloud computing systems. In *The 6th International Symposium on Frontiers in Ambient and Mobile Systems (FAMS 2016)* (Vol. 83, pp. 1084–1089)
21. Jouini, M., & Ben Arfa, L. (2018). Threats classification: State of the art. In *Computer systems and software engineering: Concepts, methodologies, tools, and applications* (pp. 1851–1876). Hershey: IGI Global.
22. Jouini, M., Ben Arfa, L., & Ben Aissa, A. (2014). Classification of security threats in information systems. *Procedia Computer Science, 32*, 489–496. ANT/SEIT 2014.
23. Jouini, M., Ben Arfa, L., Ben Aissa, A., & Mili, A. (2012). An economic model of security threats for cloud computing systems. In *Proceedings of International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)* (pp. 100–105).
24. Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. In *International Conference on Smart Computing and Communications (ICSCC2017)* (Vol. 125, pp. 691–697).
25. Lacey, T. H., Mills, R. F., Mullins, B. E., Raines, R. A., Oxley, M. E., & Rogers, S. K. (2011). RIPsec - Using reputation based multilayer security to protect MANETs. *Computers and Security, 31*(1), 122–136.
26. Mell, P., & Grance, T. (2009). Effectively and securely using the cloud computing paradigm. In *ACM Cloud Computing Security Workshop*.
27. Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. NIST Special Publication 800-145. Gaithersburg: National Institute of Standards and Technology.
28. Ming-Chang, L. (2014). Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. *International Journal of Computer Science & Information Technology, 6*, 29–45.
29. Mohammed, A., Abdullah, A., Phu, D., & Bala, S. (2012). Information security threats classification pyramid. In *Proceedings of IEEE 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA)* (pp. 208–221).
30. M'rhaoaurh, I., Okar, C., Namir, A., & Chafiq, N. (2018). Challenges of cloud computing use: A systematic literature review. In *MATEC Web of Conferences 200* (00007).
31. Ramadianti, N., Medard, P., & Mganga, C. (2011). *Enhancing information security in cloud computing services using SLA based metrics*. School of Computing Blekinge Institute of Technology SE-371 79 Karlskrona Sweden, Master's Thesis.
32. Ravi Kumar, P., Herbert Rajb, P., & Jelcianac, P. (2018). Exploring data security issues and solutions in cloud computing. In *6th International Conference on Smart Computing and Communications* (Vol. 125, pp. 691–697).
33. Rok, B., & Bork, J. (2013). A quantitative model for information security risk management. *Engineering Management Journal, 25*, 25–37.

34. Shiu, S., Baldwin, A., Beres, Y., Mont, M. C., & Duggan, G. (2011). Economic methods and decision-making by security professionals. In *The Tenth Workshop on the Economics of Information Security (WEIS).*
35. Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications, 79*, 88–115.
36. Singh, S., Jeong, Y., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications, 75*, 200–222.
37. Speaks, S. (2010). Reliability and MTBF overview. *Vicor Reliability Engineering*.
38. Stergiou, C., Psannis, K. E., Kim, B., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems, 78*, 964–975.
39. Subramanian, N., & Jeyaraj, N. (2018). Recent security challenges in cloud computing. *Computers & Electrical Engineering, 71*, 28–42.
40. The Center for Internet Security (CIS). (2009). The CIS Security Metrics v1.0.0.
41. Wooley, P. S. (2011). *Identifying cloud computing security risks*. Technical report, 7 University of Oregon Eugene.
42. Yang, M., Jiang, R., Gao, T., Xie, W., & Wang, J. (2018). Research on cloud computing security risk assessment based on information entropy and Markov chain. *IJ Network Security, 20*(4), 664–673.