Chapter 4
A Methodology for Cloud Security Risks Management

Mariam Kiran

Abstract Cloud computing is an extremely attractive model for both the users and the providers of Cloud-based infrastructure, who have their own business angle for using and providing these services. However, as with many business ventures, as the use of Cloud environments grow, the risks and the threats associated with a successful use of the model also increase. Although, the Cloud paradigm is an evolution of grid systems, Clouds have particular threats specific to virtualized and multi-tenant environments, which need to be managed with proper methodologies to ensure that the entire ecosystem is secure. Security consists of three main aspects—availability, integrity and confidentiality—and each of these needs to be considered to make sure that the complete ecosystem is secure. This chapter presents a comprehensive discussion of the concerns associated with the Cloud security depicting the best practices currently used in the industry. This chapter presents an in-depth analysis of these issues with an innovative holistic approach on how to manage and assess security risks for different kinds of Cloud ecosystems which allows documentation as well as design tools which can be in place to monitor security at both deployment and operation phases. The proposed risk methodology approach allows better management and mitigation of security threats when they occur during the service lifecycle of any kind of Cloud ecosystem and Cloud services provision.

Keywords Cloud computing · Risk modelling · Security · Threats · Service lifecycle

4.1 Introduction

Cloud computing is a market, which was worth US$ 42 billion in 2012, but is technologically still being developed [1]. Being attractive to the IT industry, where the leasing model can allow powerful software tools to be developed on top of the infrastructures, which are not always available, the Cloud brings a number of advantages which include remote accessibilities to resources, elasticity, scalability based on

M. Kiran (✉)
Department of Computer Science, University of Sheffield, Bradford, Richmond Road, Bradford BD7 4DP, UK
e-mail: m.kiran@bradford.ac.uk

Z. Mahmood (ed.), *Cloud Computing,* Computer Communications and Networks,
DOI 10.1007/978-3-319-10530-7_4

user demands, pay-per-use models to save energy and costs, to name but a few [2]. However, Clouds still have a long way to go to build the trust of the average Cloud users on issues of risks, data securities, the kind of services being processed and the governance characteristics in general [3].

Forrester Research [4] describes the market potential of Cloud computing through the hype curve, divided into 12 segments, based upon level of sharing and business value (see Fig. 4.1). Figure 4.2 shows that Cloud computing is a field, which covers a wide range of abilities being offered, estimated worth around $ 18 billion.

Security is a priority concern for many Cloud computing customers where it can affect the reputation of the providers in terms of confidentiality, resilience and integrity of the company. Kiran et al. [6] have described some of these examples such as data leakage that has been investigated with access control measures like discretionary access control [7] or mandatory access control [8] to control access to an object. Both of these approaches can be used to control access to virtual machines (VMs) via the hypervisor or VM monitor. However, traditional access control models focus on the assumption that the data controller and data owner is in the same trust domain, an assumption which does not hold for Cloud computing. Another example is network access control software like Symantec data-loss prevention [9], which cannot control data leakage within an organisation, as only the end points or network points are scanned for violation of enterprise security policy. Hypervisor attacks are the most serious security threats to the Cloud environment [10] where if infected, such attacks can be used to gain control over a VM (Bluepill) [11]. Even the smart meters cannot monitor false data injections; cyber-attacks having serious implications on the infrastructures [12].

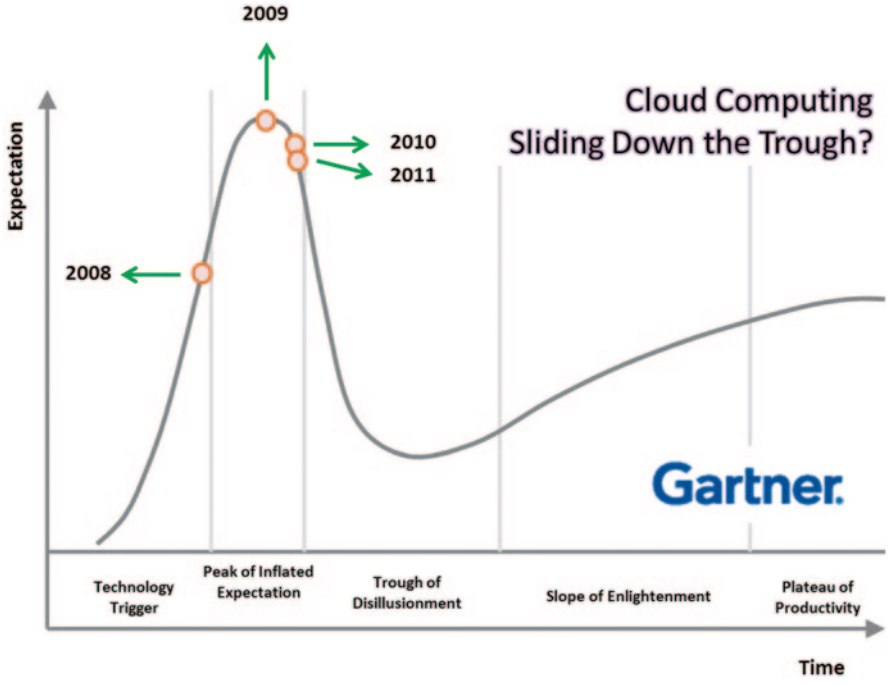

Fig. 4.1 Hype cycle for Cloud computing 2011 [5]

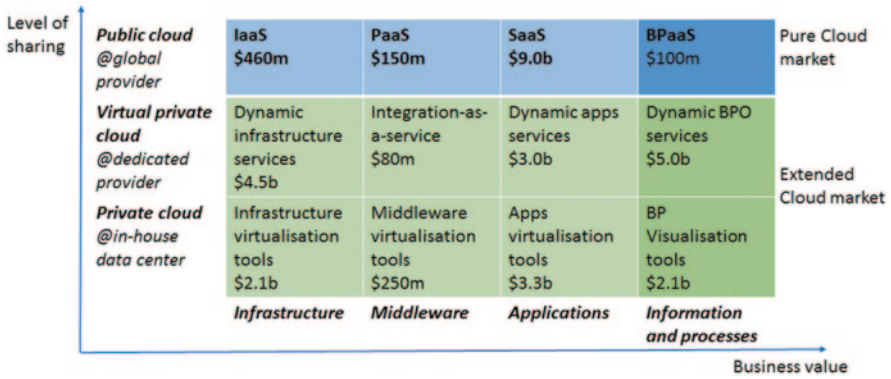

Fig. 4.2 Cloud computing business value [5]. *IaaS* infrastructure as a service, *PaaS* platform as a service, *SaaS* software as a service, *BPaaS* business process as a service, *BPO* business process outsourcing

This chapter discusses the research challenges in security and the best practices employed by the industry with the various policies and measures adopted. Based on these approaches, a uniform risk methodology is presented discussing a step-by-step procedure for handling security risks on Cloud ecosystems. This involves the policies, documentations, governance checks as well as designs tools, which can be implemented based on local infrastructures to implement security checks at the deployment and operations phases of the service lifecycle. The chapter has been organised to present a comprehensive detail on security concerns and findings in the Cloud. Section 4.2 starts with the security concerns and some general characteristics found in industry with a distribution of money spent on the different sectors to improve its issues. Sections 4.3 and 4.4 present different Cloud ecosystems and the service lifecycle as a background on which the methodology applies relevant to security risk assessment. Section 4.5 presents the actual risk assessment methodology introducing the documentation methods, which include reviewer documentation, provider policies, legal implications and risk assessment data sheets that can be filled in advance as a risk report for monitoring security concerns of the Cloud ecosystems. Based on this analysis, the next section identifies six Cloud threat categories which encompass all kinds of threats on Clouds. This identification is extended in Sects. 4.7–4.9, where the risk methodology for the Cloud is presented with accompanying algorithm and simulation results. Section 4.10 discusses the issues with Cloud security testing and the potential future within this domain. This chapter concludes with a case study applying the methodology to a video scalability problem using Clouds and concludes with further future work to be carried out in this domain.

4.2 Security Concerns in Clouds

The UK government is investing in the G-Cloud programme initiative in order to improve the economic sustainability by delivering information and communication technologies (ICT) systems that are flexible, on-demand and in compliance with

the government policies in order to support emerging small business suppliers [13]. However, to target the issues relating to security, they released a statement saying that they will ease these issues by promoting the use of open source software [14]. Open sourcing the software's will not be a solution to securing the already being used initiatives of the G-Cloud. For securing data transfer and hosting, various considerations need to be taken for data management on multi-tenancy in Clouds [15]. But these still lack detailed analysis in terms of what needs to be done to target these issues [16]. Comparatively, the National Institute of Standards and Technology (NIST) have come up with a list of security risk and mitigation mechanisms with reference to a strategy for performing risk assessment [17]. Whistle et al. [18] discuss the certification and accreditation for threats in accordance with the government laws analysed per stage accompanied with a detailed analysis.

Security can make or break deals, either convincing organisations to use the Cloud or deferring on security concerns. Best performances in a survey conducted by Ried et al. [4] show the following characteristics on security issues and how they are influenced by various factors, grouping them into three areas:

- *Policies and control*: security control objectives prioritised as functions of requirements for risk, audits and compliance(69%), policies for protection (85%), acceptable use (81%) and regular monitoring, analysis and reporting (70%) on information assets, baseline security requirements for all applications, databases and network infrastructures (74%)
- *Organisation*: responsible team with ownership for security (67%), formal end-user awareness and training programs (70%), non-disclosure agreements in place and reviewed at intervals (74%), defined steps for employee termination (67%)
- *Knowledge and performance management*: audit plans agreed in advisory boards (70%), compliance with SLAs demonstrated at various intervals (69%), formal risk ass at regular intervals (52%)

Risk models in security can be used to define and document some of the security concerns. Pullman [19] conducts an in-depth threat analysis for concerns making sure every part is covered. Microsoft has described a similar threat modelling technique to keep security concerns intact. Figure 4.3 shows a preliminary investigation in threat analysis for data loss in the Cloud and how it can be worked through to assets and mitigation strategies.

Figure 4.3 shows a threat analysis tree of the threat of data loss. The process involves working out each possibility which may have lead to this threat. It then links up with which assets need to be protected for this. As a result of this analysis, various mitigation actions can be identified such as security audits, hardware wipe policy whenever data moved, encrypting data and keeping the protected keys safe. Therefore the risks categories help identify each risk separately and the different models to analyse them separately.

4.2.1 General Security Characteristics

Security is a major concern for organisations and for businesses who are interested in Cloud investments [20–22]. The Aberdeen group [22] conducted a survey of

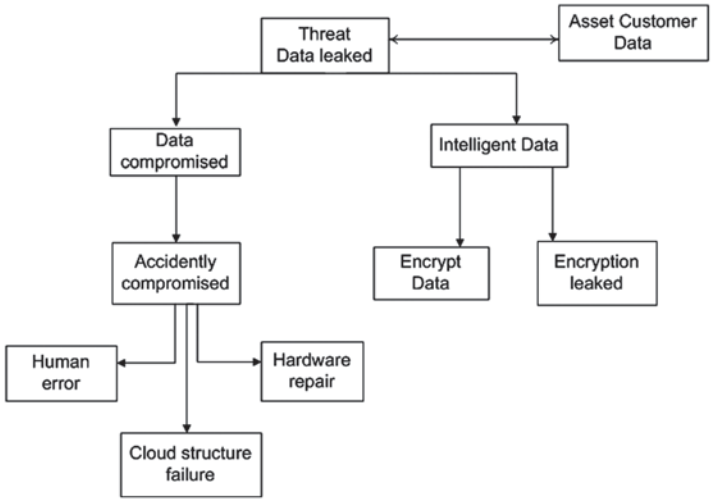

Fig. 4.3 Security threat analysis carried out by Microsoft [19]

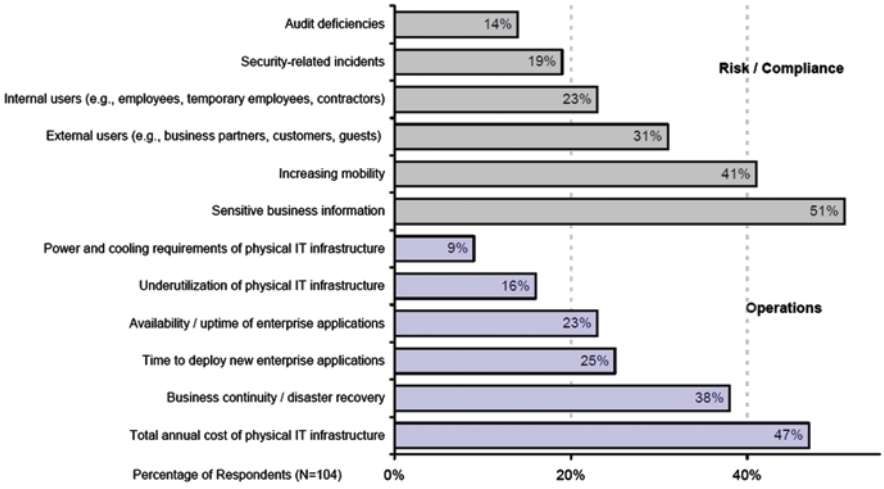

Fig. 4.4 Leading pressures driving the current investments in security for Cloud initiatives. (Adapted from [22])

security practices relating to risks and the leading pressure for areas of investments in the Cloud initiatives. Their findings are presented in Fig. 4.4.

Table 4.1 summarises their findings in terms of the best practices adopted across the different dimensions of security mechanisms on Cloud infrastructures.

Table 4.1 Best practices across various domains [22]. Numbers represent percentage of respondents with $N = 104$

Best practices across following domains	Best in class (%)	Industry average (%)	Laggards (%)
Data security			
Policies and controls to ensure data security (e.g. access controls, data loss prevention, encryption)	85	60	55
Encryption of sensitive data in storage (e.g. file servers, databases, end-user endpoints)	50	46	45
Encryption of sensitive data during transmission (e.g. over public networks, electronic messaging)	70	62	65
Effective key management to support encryption of data in storage and in transmission	56	53	45
An audit function is involved if the integrity of enterprise data has potentially been compromised (e.g. data loss or exposure, unauthorised access)	59	56	55
Identity and access management			
Consistent minimum standards for user authentication and access controls	96	81	70
Minimum authentication requirements for secure remote access	96	86	75
All requirements for access to data are identified and in place prior to access being granted	74	69	50
Timely suspension/revocation/de-provisioning of end-user access upon termination or change in role	85	71	65
Periodic validation that end users have appropriate access rights (attestation)	74	56	55
Enforcement for separate of duties	74	56	50
Data governance			
All data (and objects containing data) have been identified and classified	54	46	32
All data has a designated owner/steward	58	38	37
Policies and processes are in place for data labelling and data handling	54	51	42
Production data is not replicated or used in non-production environments	64	56	37
Data backup and recovery mechanisms, tested at regular and planned intervals	74	72	63

Table 4.1 (continued)

Best practices across following domains	Best in class (%)	Industry average (%)	Laggards (%)
Policies for secure disposal and complete removal of data from all storage media	70	57	47
Security mechanisms to prevent data leakage	58	56	39
Network access, mobility and application security			
Network infrastructure is designed and configured to restrict connections between trusted and un-trusted segments	81	73	70
Policies ad controls to protect wireless network environments	78	76	65
Policies and controls to limit access to sensitive data from mobile devices (e.g. laptops, smart-phones, tablets)	74	49	40
Policies and controls with respect to code for mobile devices	52	37	35
All functions and application programming interfaces (APIs) that will be used in conjunction with software development are analysed for security risk	52	38	30
Monitoring, auditing, forensics and incident response			
Security-related logs, information and events are retained and regularly reviewed	69	68	58
Monitoring and tracking of security-related incidents and events (e.g. types, volumes, time and cost to remediate)	78	70	56
Communications channels and escalation procedures for security-related incidents and events	59	52	50
Forensic procedures (e.g. chain of custody) for collection, retention and presentation of evidence in support of potential legal action	52	48	35
Segmentation and access controls to prevent compromise and misuses of log data	65	59	55
Access to diagnostic and configuration ports is restricted to authorised individuals and applications	77	68	55

4.3 Cloud Ecosystems

To make them more attractive for users, Cloud providers attempt to hide a lot of the processes in the background to promote the easy usability for users. Having automated security policies and access control measures are examples of these, but there are still a lack of standards to be followed during these activities. These have been on the active research agenda of bodies like NIST [23] and Gartner [5].

NIST describes the Cloud as a convenient model using efficient computing resources stressing on four deployment models [24]:

- Private Cloud: operated for an organisation by either itself or a third party
- Public Cloud: for general public use and is owned by an organisation selling Cloud services
- Community Cloud: an infrastructure that is shared by several organisations, also called federation of Clouds
- Hybrid Cloud: a composition of two, more Clouds or multi-Clouds (community, private, public)

Each of these models or Cloud ecosystems brings different issues in terms of data hosting, security, risks and business models. This chapter discusses Cloud ecosystems in relation to the roles of the actors—namely service provider, infrastructure provider and brokers—involved in the ecosystem, which do not have a direct mapping from the NIST documentations. This is done to ease discussion in the later sections.

Figure 4.5 describes the different Cloud ecosystems and shows the roles of the actors who play in them. A private Cloud involves only a service and an infrastructure provider who communicate directly to each other and possibly in the same geographical location. A Cloud-bursting environment is when one infrastructure provider is close to running out of resources and thus bursts to another. Figure 4.5c describes a federation of infrastructure providers working together as a team to complete the

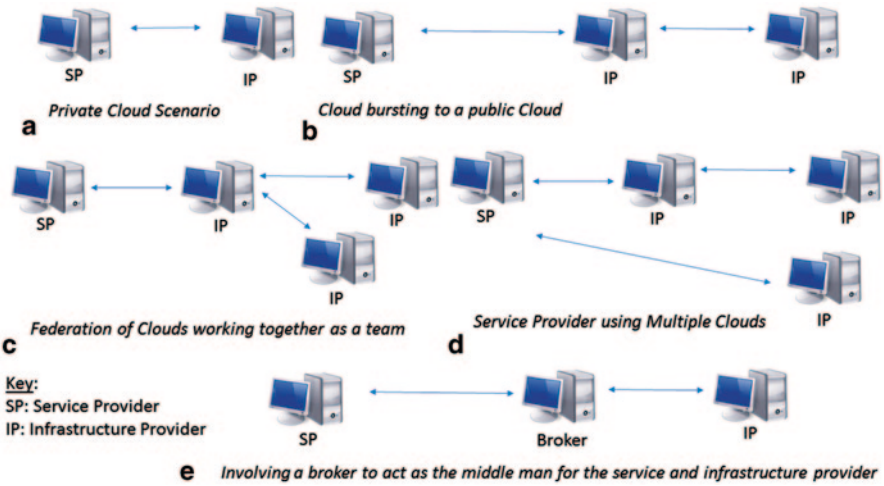

Fig. 4.5 **a**–**e** Various Cloud scenarios or ecosystems

service execution. Figure 4.5d shows a similar situation, but this time the infrastructures are working independently of each other and only guided by the service provider. Lastly, Fig. 4.5e describes a situation which involves a broker to mediate between the two parties. The broker can take responsibilities to monitor, test and make sure the service is completed and delivered at the right time to the service provider.

In addition to the Cloud ecosystems, Clouds can be recognised by the form of functionality they offer. These are as follows:

- Software as a service (SaaS): Uses the Web to deliver third-party applications to Clients. Example: Gmail
- Platform as a service (PaaS): Provides framework to build applications on top as well. This provides the client highly scalable infrastructure and hardware for computing. Examples: GoogleAppEngine [25], Heroku [26]
- Infrastructure as a service (IaaS): Third party allows you to install a virtual server on their IT infrastructure

This chapter focuses on Cloud security in terms of the different ecosystems and the security threats that need to be monitored. Functionality models of Clouds form part of these ecosystems, depicting how the services will be offered. Based on the functionality and ecosystems, various threats can be highlighted which would otherwise not need to be monitored in a different scenario. Section 4.7 provides a case study for a video scalability application to demonstrate this use of identifying threats for the particular scenarios.

4.4 Cloud Service Lifecycle

Before we discuss the different kind of threats across the ecosystems, we have to recognise the different phases in which the services can exist. This also highlights that only particular threats will be active during, either the service engineering phase, onboarding or operation phase. The services lifecycle is represented in Fig. 4.6, where the first phase of service engineering is when the service is constructed, the second phase is when the service is actually deployed on to the Cloud and the third phase is when the service is in operation and executing on the Cloud.

4.5 Risk Assessment of Security threats on Clouds

Security can essentially be broken into three main aspects, which, if guaranteed, becomes fully optimal (Fig. 4.7). These are:

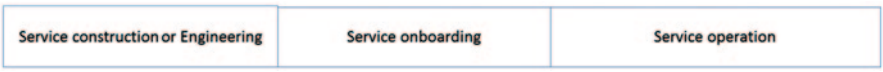

Fig. 4.6 Service lifecycle covering construction, deployment and operation of the service on the Cloud

Fig. 4.7 Security triangle

- *Availability*: The data is available when needed.
- *Integrity*: The data is not modified without being detected.
- *Confidentiality*: The data remains undisclosed to unauthorised parties.

Comparing to grid infrastructures, due to their nature, Clouds have additional threats that need to be considered for security reasons. For instance, data access in Clouds is a huge threat because geographically the data can be hosted anywhere as a service. This would not be a threat on Grid infrastructure which are usually business owned and located internally. Therefore there is a need to consider the geographical location and the access rights to the Cloud for safety of the data. Another example is when migrating the VMs securely across the different infrastructures on the Cloud. Depending on the situation, the data manager on the Cloud should consider if the VM's new location still complies with the legal agreements made between the end user and the Cloud for where the data is allowed to be hosted. Various authentication models can be introduced to make it more secure as a mechanism to overcome this threat.

There is a need to identify the different kinds of security issues in Cloud computing. For example, Fig. 4.8 describes how data being hosted in isolation, can be compromised.

Figure 4.8 describes a tree structure which can be used to perform a fault-tree analysis style to find, where human errors, faults and the business being affected helps to determine how to mitigate similar situations if this happens in real life.

4.5.1 Documenting a Security Risk Assessment

Different Cloud ecosystems and the services executing on them, are prone to different number of threats, particularly the public or hybrid Cloud scenarios. In public Clouds, the data is hosted externally on a Cloud, being used by multiple users of the public. Hybrid Clouds can include different Clouds joining to form a federation or multiple Clouds working together to fulfil a service. Threats, such as unauthorised data access, are a problem on public Clouds rather than a private Cloud, where everything is maintained internally. Not having formal procedures in place is a major problem because of these different natures. When using multiple Clouds a few common rules should be maintained to allow uniform protocols that are followed by all Cloud providers in case certain security threats are realised. Cloud networks can be set up with various sensors to gather the informa-

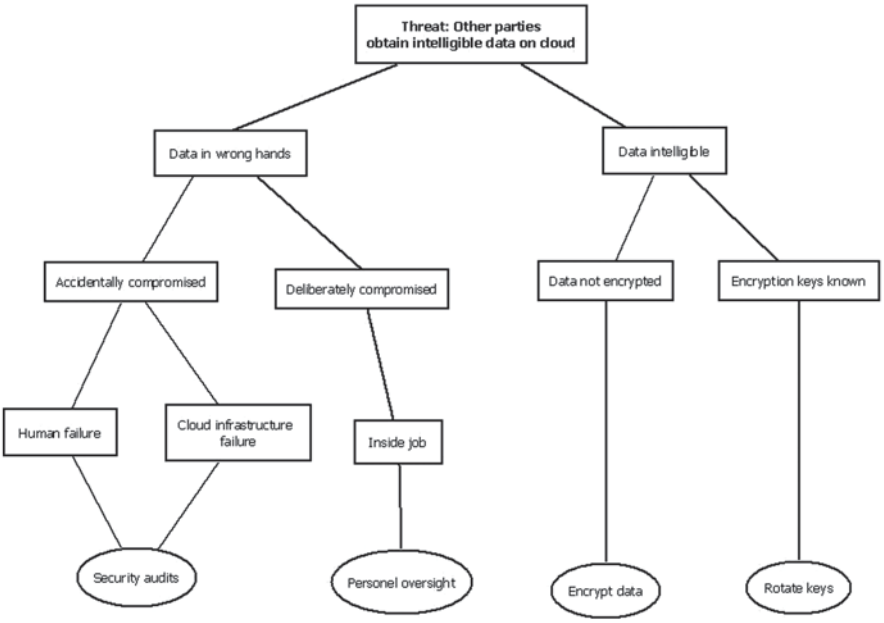

Fig. 4.8 Tree analysis for threat of data leakage. (Adapted from [1])

tion, on how the service is performing on the Cloud within the applications. The introduction of formal methods can make Clouds secure by applying them to the Cloud industry as a whole [6]:

- *Reviewing various documentations*: These include using sniffers to filter output logs produced by the monitoring software installed on the infrastructures. These can include system logs (for details of service start-up, downtimes, file and account access and changes to file privileges), firewall logs (authorisation attempts from various locations and identify the users, if possible), antivirus logs (for detecting malicious code accessing the system), and intrusion detection system logs (detecting the changes to the hypervisor code), and legal implications of security threats have to be set to measure the impact of certain threats.
- *Provider interaction policies*: Policies have to be set for the providers, which include action management policies for necessary legal steps to be taken, if threats happen and how to mitigate them. These should include an incident response plan, which may include communication protocols (how information will be displaced to within the team or outside such as the attacking internet protocol (IP) addresses to block those organisations) [6], software vendors providing the software, (if the actual software being installed is corrupted), internal team management procedures, vulnerability assessment with certain auditing procedures and using these for future incident planning. An important issue is revealing the performance information to Cloud customers. Should the end users be told of threats occurring at the time their services were hosted on the Cloud and when?

In cases of multiple locations hosting data, this can be an attractive requirement from the users to ensure their data is secure.

- *Legal implications on the security aspects*: Data protection and security can be specified in a legal contract, being drawn with the end users and the providers. This may include analysing all privacy concerns specific to the Cloud usage. This may start with analysing the data flow in the Cloud use cases and understanding the legal issues with the multiple vendor situations and how these should be handled. Information security-related standard (ISO/IEC 27001:2005) has recognised protection of personal data including protection against alteration, unauthorised modifications and against unauthorised access as a standard [3]. Further recommendations concerning information security are mainly based on control and industry best practices relevant to Cloud providers (security framework). However, this needs to be defined, clarifying questions concerning intellectual properties and ownership rights in information and services placed *in the Cloud*. This also involves clarifying ownership rights among all potential stakeholders and includes them within the service level agreements (SLAs) drawn.

4.5.2 Security Risk Assessment Data Sheet

An example of a data sheet used to perform a security risk assessment has been described below: This can be filled out by the providers or the end user as part of the SLA, when they try to ask for certain security measures to be taken.

1. Details:

Service name: _____
Department: Service provider/infrastructure provider
Date of this assessment: _____
Risk reference no: _____

2. Hazards overview:

- Example unencrypted data
- Example lost keys

3. Control measures:
(Option to complete this section for any risk which is rated as four or more, or for which the likelihood is three).
For each hazard name responsible person and action
Note: The choice of controls should be implemented according to the following hierarchy:

1. Eliminate the hazard
2. Substitute
3. Reduce

4. Isolate (enclose the hazard)
5. Regulate (e.g. numbers at risk, engineering controls or safe system of work)
6. Protection
7. Discipline

Copies: (a) The original of this form is to be retained by the originating department and a copy is to be supplied to the safety department. (b) Relevant information on risks and preventive/protective measures are required by law to be provided to employees so that they can ensure their own health and safety and not put others at risk.

4. Evaluation of risk:

Hazard details		Services at risk		Frequency/ (duration)	Controls in place	Residual risk evaluation	Risk rating
Hazard	Nature of hazard/ adverse effects (how is the hazard likely to put services at risk?)	Insert code and (number of people)	Insert code letter and (duration)	Insert code numbers	Severity of harm score 1–3	Likelihood of occurrence score 1–3	Multiply severity × likelihood
Unencrypted data	Third party acquires data	*A, B, D* (5)	*D/*(4)	1, 3, 5	3	3	9
Lost keys	Third party has data	*A, B, D* (10)	*D/*(4)	2, 4, 5	2	3	6

*Key: services at risk***:**
(a) Operator (skilled), (b) operator (inexperienced), (c) end users, (d) office staff

*Key controls***:**
(1) Data encryption algorithms, (2) refreshing keys, (3) segregating data, (4) assessment of personnel, (5) monitoring login logs

*Severity of harm***:**
(1) Slight, e.g. minor data leaks, less important data, (2) serious, e.g. personal data compromised, (3) major, e.g. business lost, reputation jeopardised

*Likelihood of occurrence***:**
(1) Low (harm will seldom occur), (2) medium (harm will often occur), (3) high (certain or near certain)

Table 4.2 Security threats and their categories (*C* confidentiality, *I* integrity, *A* availability) [6]

Threat category	Description (specific to Clouds)	Factor	Example
External attacks	These include all the threats in scenarios involving use of public infrastructures	C, I, A	Carrying out of denial of service (DoS) attack
Theft	Cloud computing supports multi-tenant architecture with multiple users using same resources. This can lead to the theft of data by an adversary	C, I, A	Gaining unauthorised access to systems or networks
System malfunction	Some software used extensively on Clouds has bugs	A, I	Malfunction of software
Service interruption	Unavailability of service/data due to DoS attacks	C, I, A	Natural disaster
Human error	No control on how users use the system	C	User error
System specific	System specific threats and abuse	C, I, A	Usage control

4.6 Identifying Cloud Threat Categories

Khan et al. [6, 24] describe how the various security threats can be bunched together in six specific categories, represented by Table 4.2. The main differences from grids to Clouds have added a few unique threats, such as data leakage (an unauthorised transmission of data from within an organisation to outside or the unauthorised access to the system, which compromises the confidentiality of the data), usage control (access control to cover conditions independent of environmental factors), hypervisor level attacks (enable an adversary to exploit vulnerability at the virtualisation layer that is running underneath the VMs). Most threats have a domino effect on the other components, where one affects multiple components. For instance, if the hypervisor gets corrupted, all the corresponding VMs, their locations and data can be compromised. Inappropriate use of any technical or data available on the Cloud affects the trust customers place on the Cloud, having implications on the business objectives of the Cloud providers.

4.7 Need for Risk Management

Risk management addresses the possibility that future events may cause adverse effects and is defined as "the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities" [2]. Figure 4.13 describes the stages in a risk management cycle. The most important concepts in risk management are as follows:

- An *asset*: to which has a value and hence for which the party requires protection.
- An *unwanted incident*: an event that harms or reduces the value of an asset.

Fig. 4.9 Risk management process

- A *threat* is a potential cause of an unwanted incident whereas vulnerability is a weakness that opens for, or may be exploited by, a threat to cause harm or reduce the value of an asset.
- *Risk* is the likelihood of an unwanted incident and its consequence for a specific asset, and *risk level* is the level or value of a risk derived from its likelihood and consequence. For example, a server is an asset; a threat may be a computer virus and the vulnerability a virus protection not up to date, which leads to an unwanted incident.

A risk management process consists of a risk identification stage, where it is identified, assessed for likelihood and impact, managed through planning and resolved with a plan on what to do if it occurs. Risk monitoring phase allows it to be continually monitored in case it becomes active in the future (Fig. 4.9).

4.7.1 Cloud Threats Identified

The security risk methodology uses the threat modelling as an approach for identifying the threats and vulnerabilities of the system. Two sources of information were used to collect the threats, unique to Clouds. The sources of information are as follows:

For collection purposes:

- The information security forum [1, 3] for providing data on attacks on IT systems and the frequency of attacks
- The public data on attacks on the Cloud platforms such as Amazon EC2 and Google Apps Engine [8, 9]

For evaluation purposes:

- Defense Advanced Research Projects Agency (DARPA) intrusion detection evaluation data sets [3]

Based on the data collected, a risk catalogue can be created to document the threats, the affected assets and their vulnerabilities. An entry into the risk catalogue can be stated and shown in the example in Table 4.3.

The data from the threat analysis tool [28] helps to identify the form the threats in the form of ids, assets, and the values for priority and likelihood. The ecosystems relate to Cloud scenarios being private, bursting, federation and multi-Clouds. The lifecycle stage shows which phase of the service lifecycle, during execution, is the threat active—during deployment or operation. A risk methodology is then generated

Table 4.3 Example of the threat entry in the risk inventory

Threat id	27
Name of threat	Theft of business information
Cloud ecosystem at which active	All (private, bursting, federation, multi, brokerage)
Service lifecycle stage	Operation
Asset affected	Customer data
Priority assigned	4
Likelihood assigned	2

which will use this risk catalogue as a reference database when making decisions on the security risks in the Cloud.

4.8 Risk Methodology Stages

This section describes the various stages involved when performing a risk assessment for Cloud computing environments. The methodology follows a 5-stage procedure from a high level analysis of the system to the asset identification, threat assessment and then the final evaluation of risk from the matrix to calculate as the assessment of the risks that need to be managed in order of high probability and impacts.

Stage 1: High-Level Analysis of the System An initial high-level analysis of the Cloud ecosystem or scenarios, to help identify the actions and assets involved. This will help isolate the assets involved and how they change over time to identify the vulnerabilities of the Cloud environment.

Generally security needs to be assessed before deployment of the service to check for security concerns of other provider or if the SLAs demand certain security aspects. During the operation, as security concerns are monitored while the service is executing, certain live data have to be assessed continuously.

Stage 2: Identifying the Assets Involved There are various assets involved either at the deployment or operation stage such as the SLA or customer data. These can be monitored in relation to the specific threats in the environment.

Stage 3: Identify the Threats in Each Cloud Deployment Scenario This is where a threat analysis tool can be used to perform a detailed analysis of each threat. Figures 4.10 and 4.11 describe the threat distribution across the six threat categories identified earlier [28].

The threat analysis, accompanied by an expert opinion, sets the threat and vulnerability ratings for each threat from a scale of 1–5 (very low, low, medium, high and very high). The tool also allows mapping the threat with respect to business impact produced as an information risk profile. These results have been shown in Table 4.4.

Stage 4: High-Level Analysis of Each Threat Each of the threats can be further analysed in terms of who/what causes them and the incidents leading up to them, which

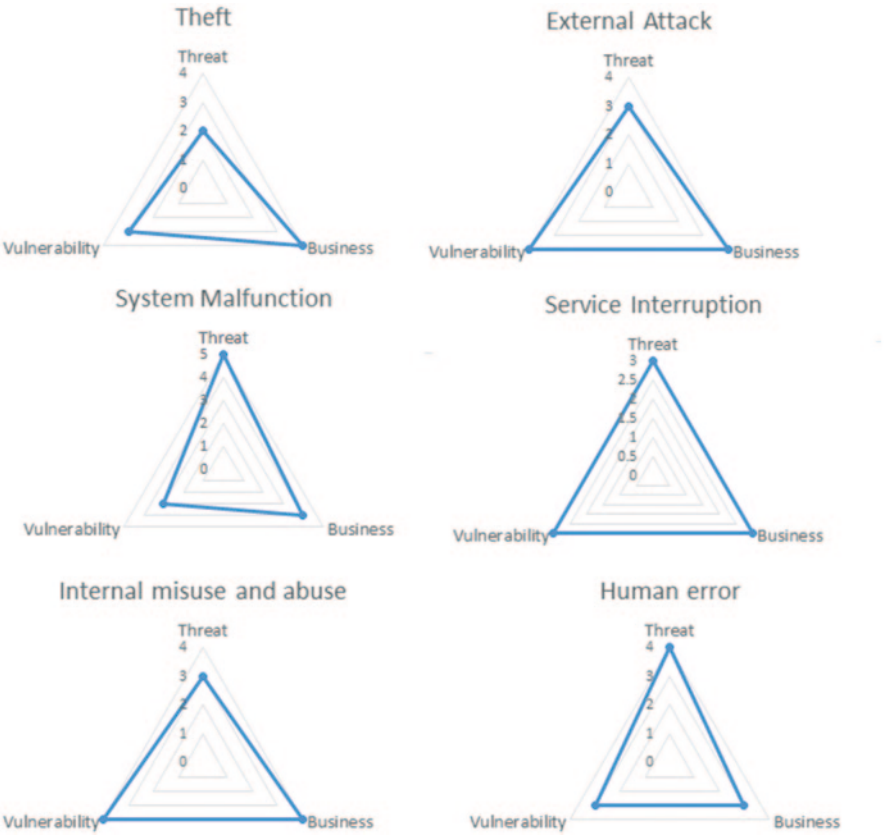

Fig. 4.10 Business impact, threat and vulnerability rating for the six threat caetgories. (Adapted from [28])

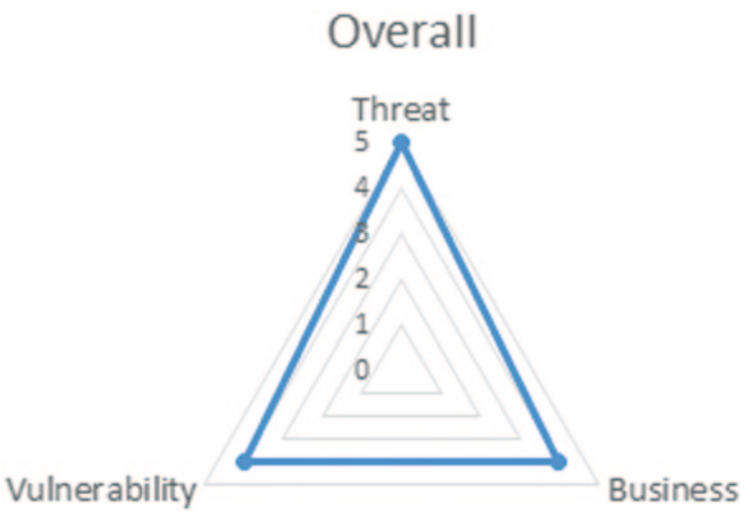

Fig. 4.11 Overall threat rating in terms of business impact. (Adapted from [28])

Table 4.4 Threats identified in the various use cases and their details. (Adapted from [24])

Threat category	Threats (threat id) {threat classification: availability (A) confidentiality (C) integrity (I)}	Stage of service lifecycle (deployment/operation)	Assets involved	Cloud ecosystems	Priority (1—low, 5—high)	Likelihood (1—low, 5—high)
External attacks	Carrying out of denial of service (DoS) attack (T1) {A}	Operation	Customer data, infrastructure of the provider	All	4	3
	Hacking (T2) {I, C}	Operation	Customer data or service	All	3	1
	Undertaking malicious probes or scans (T3) {I, C}	Operation	Hypervisor code	All	4	2
	Cracking password (T4) {A, I, C}	Operation	Customer data or service	All	3	1
	Cracking keys (T5) {A, I,C}	Operation	Customer data or service	All	3	1
	Spoofing user identities (T8) (A, C) {A, C}	Operation	Customer data or service, all services	All	3	1
	Modifying network traffic (T9) {I}	Operation	Software, connections, service (runtime)	All	2	2
	Eavesdropping (T10) {I, C}	Operation	Software, connections, service (runtime)	All	2	1
	Distributing computer viruses (T11) {I}	Operation	Software, connections, service	All	3	1
	Introducing Trojan horses (T12) {I}	Operation	Software, connections, service	All	3	1
	Introducing malicious code (T13) {C}	Deployment and operation	Software, connections, service	All	3	3
	Distributing Spam (T15) {A}	Deployment and operation	Mailing lists	All	1	4

Table 4.4 (continued)

Threat category	Threats (threat id) {threat classification: availability (A) confidentiality (C) integrity (I)}	Stage of service lifecycle (deployment/operation)	Assets involved	Cloud ecosystems	Priority (1—low, 5—high)	Likelihood (1—low, 5—high)
Theft	Gaining unauthorised access to systems or networks (T16) {A, I, C}	Operation	Customer data or service	All	5	4
	Theft of business information (T27) {A, C}	Operation	Customer data	All	4	2
	Theft of computer equipment (T29) {A, C}	Operation	Customer data	All	1	2
System malfunction	Malfunction of software (T34) {I}	Operation	Toolkit, all services	All	1	4
	Malfunction of computer network equipment (T35) {I}	Operation	Toolkit, all services	All	1	5
Service interruption	Natural disaster (T40) {I}	Deployment/Operation	Customer data	All	1	3
	System overload (T41) {A, C}	Operation	Customer data,	All	4	3
Human error	User error (T42) {C}	Deployment/operation	Data	All	5	3
System specific threats and abuse	Data Leakage (T50) {I, C}	Operation	Data	All	5	3
	Usage control (T51)	Operation		All		
	Hypervisor level attacks(T52) {A}	Operation	Data	All	3	2
	Data ownership (T53) {I}	Deployment	Data	All		2
	Data exit rights (T54) {I, C}	Deployment	Data, SLA	All	4	3
	Isolation of tenant application (T55) {I, C}	Deployment and Operation	Data	All	5	2
	Data encryptions (T56) {A, I,C}	Operation	Data	All	5	3
	Data segregation (T57) {A, I}	Operation	Data, programs	All	4	2
	Tracking and reporting service effectiveness (T58) {A, I}	Operation	Data, Hosted VMs	All	5	3
	Compliance with laws and regulations (T59) {A, I}	Deployment and operation	Data	All	3	2
	Use of validated products meeting standards (T60) {A, I}	Operation	Data	All	3	3
	Guest virtual machines (T61) {A, I}	Operation	Data	All	1	3

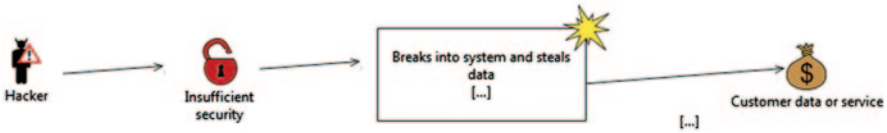

Fig. 4.12 Analysing the threat *hacking*, drawn using the CORAS (A Framework for Risk Analysis of Security Critical Systems) risk modeling tool [27]

Table 4.5 Risk evaluation matrix. (Adapted from [24])

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

Table 4.6 Range of threats for confidentiality, availability and integrity. (Adapted from [24])

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

can then be prioritised depending on this information. This also helps to measure the impact of the security risk on the service and the providers. Figure 4.12 depicts an example of the hacking threat and its related asset and vulnerabilities.

Stage 5: Risk Evaluation Depending on the priority of the assets and likelihoods of the threats occurring, the threat items can be plotted into an evaluation matrix to document their occurrences. Table 4.5 depicts this in relation to the threats identified in Table 4.4.

The likelihood and impact rating is set using the data collected and the threat analysis. The impact values also denote the affect the threat will have on the business such as loss of confidentiality or availability eventually leading to loss of money. The loss in trust has the highest impact (Table 4.6).

Once the inventory has been created for security risks, the level of risk can be calculated by the following algorithms. These are different both for deployment and operation phases.

4.9 Algorithms for Security Risk Assessment

The algorithms used to measure security risks can be unique depending on the deployment and operation phases. These are described below:

4.9.1 Algorithm: Deployment Phase

Security_risk_at_deployment (Cloud_ecosystem)

1. Calculate number of threats recorded, at deployment stage and the involved ecosystem.
2. For each threat, calculate:
   a. probability of likelihood given the asset is affected ($p(B|A)$) = likelihood / 5.0
   b. probability of asset priority ($p(A)$) = priority / 5.0
   c. probability of likelihood regardless of asset ($p(B)$) = $p(B \mid A) * p(A) + p(A')$
   d. probability of threat occurring ($p(A \mid B)$) = (($p(B \mid A) * p(A)$)) / $p(B)$
3. Security risk = sum all probabilities of threats occurring/threats found

The maximum value of the asset priority and the likelihood of it being affected are set in the range 1–5. Based on the list of threats that need to be monitored, these can be assessed based on each asset and the likelihood that each asset actually fails as a result of the threat. Bayes rule can be used to calculate the underlying probability:

Let A = "Something is wrong with asset with its priority"

Let B = Asset has failed as a result

In steps 2c and 2d, the aim is to calculate $P(A \mid B)$, the probability that the asset has indicated a risky event as a result of the threat.

$$P(A \mid B) = P(B \mid A) * P(A) / P(B)$$

$P(B \mid A)$, indicates that likelihood that the asset has been affected when something is wrong but not related to the kind of threat. $P(A)$ gives the asset affected with its priority. $P(B)$ is then defined by calculating the total probability:

$$P(B) = P(B \mid A) \times P(A) + P(B \mid A') \times P(A')$$

Note: A and A' are mutually exclusive where (A') means any kind of fault in the system without this asset being involved.

$$P(A') = 1 - P(A)$$

Assuming $P(B \mid A') = 1$, because this means that $P(B)$ (probability that the asset has failed) given the asset is not present $P(A')$. Thus this determines that if the asset is not present, the system has failed already.

Therefore:

$$P(B) = P(B \mid A)P(A) + 1 \times P(A')$$

Once calculated, using substitution to find $P(A|B)$ probability that the asset has failed due to this threat is given by:

$$P(A \mid B) = P(B \mid A) \times P(A) / P(B)$$

The algorithm above shows how the security risk probability is calculated at deployment stage. Considering the recorded risks in the risk inventory (Table 4.4) for each particular use case and using the values of priority and likelihood as described in the algorithm, the probability of that particular threat can be calculated. The security risk values are depicted in Fig. 4.13 which show the probabilities returned for each of the use cases, private, bursting, federation and multi-Cloud during deployment and operation (Fig. 4.14).

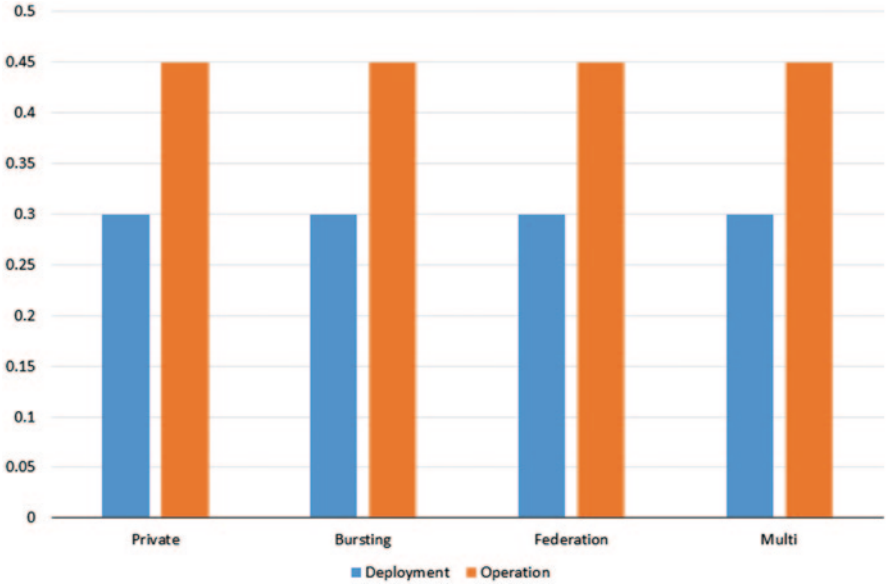

Fig. 4.13 Security risk probability as calculated from the risk catalogue from value 0–1 and the different use cases. (categories are private (private at deployment and operation), bursting (bursting at deployment and operation), federation (federation at deployment and operation), multi (multi-Cloud at deployment and operation))

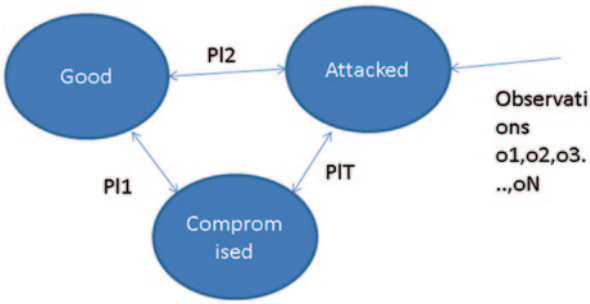

Fig. 4.14 State changes for each asset from good, attacked or compromised. *Pl1* probability likelihood 1 can be calculated using the risk inventory, *Pl2* probability 2 is calculated at operation depending on the monitored logs, *PlT* the relative probability threshold is measured using the relative probability between Pl1 and Pl2

4.9.2 Algorithm: Operation Phase

Security_risk_at_operation (Cloud_ecosystem)

1. Make a list of threats to be monitored at operation stage for the *particular ecosystem.*
2. Make a list of the affected threats to be monitored.
3. For each asset make observations Oi for every 10 min.
4. Return the sample to the risk assessor, which records the probability of the event occurring.
5. Calculate total_event_rate = events_found/total monitored time.
6. Relative risk (RR) = total_event_rate/risk (risk from catalogue).
7. If RR = 1 do nothing, RR < 1 accept risk, if RR > 1 apply mitigation strategy.

A collection of monitoring logs can be parsed to calculate the event rate for the risk assessor to calculate the relative risk. Figure 4.15 shows the states of a particular asset changing with time, 1 h 40 min (collecting 10 min samples). The probability collected is returned to the risk assessor, which calculates the relative risk as shown in the algorithm at operation stage.

Various monitoring logs will be assessing its state during operation. Initially the asset starts with state "good", but because it is to be monitored, it moves into the "attacked" state where the various logs are counting the number of events occurring. This is the event rate returned to the risk assessor.

During this time, if the risk assessor receives an event rate, which is too high, this causes the relative risk to go above 1, the asset moves into a "compromised" state.

When the risk assessor witnesses the assets in a *compromised* state, if then fires relative mitigation strategies to allow the asset to be repaired and go back to a "good" state. Then once in the "good" state, it will then again move to an "attacked" state so that it can be continuously monitored for attacks and return event rates to the risk assessor.

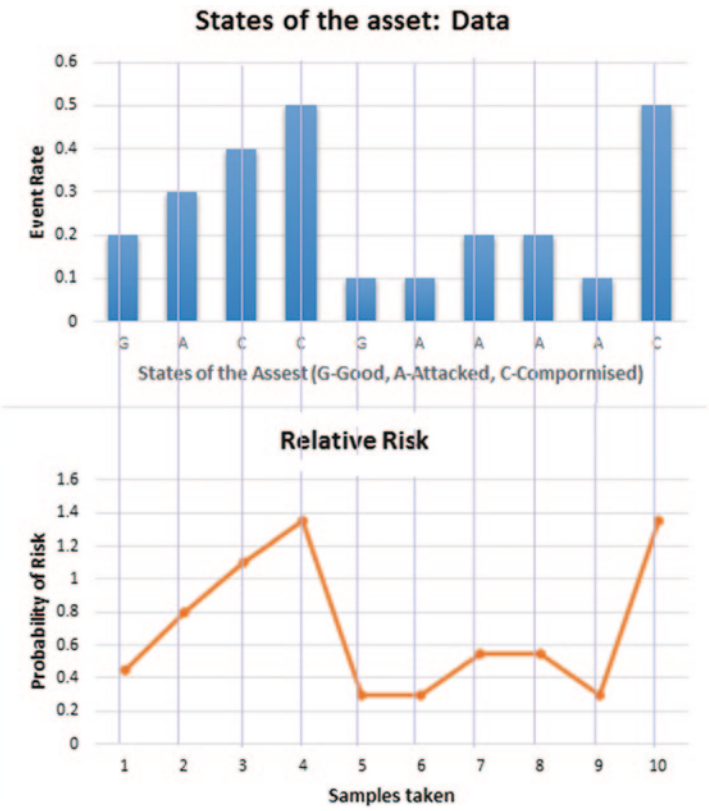

Fig. 4.15 Example of rates counted for asset data. The asset data being monitored for 10 samples and the corresponding state changes (good, attacked, compromised) with event rate (*top graph*) is shown in relation to the relative risk (*bottom graph*)

4.10 Testing Security

A kind of testing, particularly "penetration testing", seeks to get past security protocols. Security as a whole involves static design issues, as well as run-time verification of security. In this sense, security is a measure of reliability, to test if the data is secure assessing in terms of vulnerability, availability and integrity.

Non-functional requirements specify how a system should perform, in terms of its efficiency and reliability in the SLAs. Some of these aspects can also be defined as specific variables, such as response time, scalability, reliability, availability, security or maintainability. Various kinds of testing included here are performance testing, security testing or dependability testing for satisfying customer needs.

4.11 Application: Case Study for Video Scalability in Cloud Environment

Khan et al. [29] describe an implementation of threat methodology to assess the video scalability when being distributed as an IaaS on the Cloud. Scalable video is a means of distributing media content to many users using Clouds, as this allows heterogeneous networks to be connected to devices. This is a highly distributed environment with an IaaS focus, but centralized with many users connecting to it.

Security measures have to be taken to make sure copyright laws are intact, pay-per-view models for business value and economic return and it caters to the different levels of bandwidth used by the users. Usually, past models have distributed encrypted video files when broadcasted, such as satellite television, investing in set-top box to subscribe to encrypted channels. Shared encryption keys are used with each subscriber, which changed periodically.

Figure 4.16 describes the unique service lifecycle, which would exist in this particular scenario. To prevent past users accessing the data, when unsubscribed, there will be a continuous pre-deployment stage, where new keys will be generated, deployed and used periodically.

When identifying the threats, some of these do not apply to video broadcasting, from the general Cloud scenarios such as the following [29]:

- *Isolation of tenant application*: Affects integrity, confidentiality and does not apply to video broadcasting.
- *Data encryptions*: Applies to all three availability, confidentiality and integrity and is already covered in the key authentication process during the pre-deployment process.
- *Data segregation*: Affects the availability and integrity also does not affect broadcasting issues.
- Tracking and reporting service effectiveness can be given by customer review and end-user experience affecting the credibility of the server.
- Compliance with laws and regulations of copyright issues and contract breach. Affects the confidentiality and integrity of the business during the pre-deployment stage.

Based on Table 4.4, the threats which apply in this scenario are identified in Table 4.7, with corresponding risk evaluation in Table 4.8 and priority concerns for business in scalable video in Table 4.9.

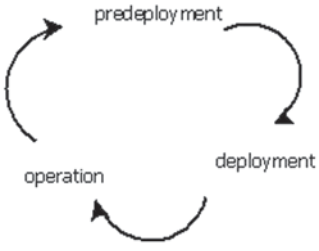

Fig. 4.16 Service lifecycle for scalable video. (Adapted from [29])

Table 4.7 Threats referring to Table 4.4 which apply to scalable video on the Cloud

Threat category	Threats (video threat id) {Threat classification: availability (A) confidentiality (C) integrity (I)}	Stage of Cloud (Pre/deployment/ operation)	Assets involved	Priority (1—low, 5—high)	Likelihood (1—low, 5—high)
External attacks	(T1.) Carrying out of denial of service (DoS) attack {A}	Operation	Broadcasting server	5	4
	(T2.) hacking {I, C}	Operation	Customer data, comprising service, company reputation	3	1
	(T3.) Undertaking malicious probes or scans {I, C}	Operation	Hypervisor code, virtual machine, video server	4	4
	(T4.) Cracking password {A, I, C}	Operation	Customer data or service	3	1
	(T5) Cracking keys {A, I, C}	Pre-deployment, operation	Customer data or service	2	1
	(T8) Spoofing user identities {A, C}	Pre-deployment, operation	Customer data or service data, all services	3	1
	(T9.) Modifying network traffic {I}	Operation	Software, connections, service, video streaming (runtime)	2	2
	(T10) Eavesdropping {I, C}	Operation	Software, connections, service (run-time), video streaming	4	3
	(T11) Distributing computer viruses {I}	Operation	Software, connections, service, broadcast is usually patched with security modes	2	1
	(T12) Introducing Trojan horses {I}	Operation	Software, connections, service	3	1
	(T13) Introducing malicious code {C}	Deployment and operation	Software, connections, service, not through video easy to, broadcast is controlled	2	1
	(T15) Distributing spam {A}	Deployment, operation	Mailing lists, server lists	2	1

Table 4.7 (continued)

Threat category	Threats (video threat id) {Threat classification: availability (A) confidentiality (C) integrity (I)}	Stage of Cloud (Pre/deployment/ operation)	Assets involved	Priority (1—low, 5—high)	Likelihood (1—low, 5—high)
Theft	(T16) Gaining unauthorised access to systems or networks {A, I,C}	Operation	Customer data or service, extract data from the video	4	3
	(T27) Theft of business information {A, C}	Operation	Customer data	4	2
	(T29) Theft of computer equipment {A, C}	Pre-deployment, Operation	Customer data	1	2
System malfunction	(T34) Malfunction of software {I}	Pre-deployment, operation	Toolkit, all services video server, end user, because of the key generation	1	4
	(T35) Malfunction of computer network equipment {I}	Pre-deployment, deployment, operation	Toolkit, all services, video server, malfunction during the key generation will affect the broadcasting of the video and the server	1	3
Service interruption	(T40) Natural disaster {I}	Pre-deployment, deployment, operation	Customer data, video server	4	1
	(T41) System overload {A, C}	Operation	Customer data, video server	1	2
Human error	(T42) User error {C}	Pre-deployment, deployment, operation	Data	3	3
System specific threats and abuse	(T50) Data leakage {I, C}	Operation	Data, video data	4	2
	(T53) Data ownership {I}	Pre-deployment, deployment	Data relates to video rights	4	2
	(T54) Data exit rights {I, C}	Pre-deployment, deployment	Data, SLA relating to copyrights	4	3

Table 4.8 Risk evaluation Matrix for scalable video

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	*Rare*		T5, T11, T14, T15	T2, T4, T12, T8	T40	
	Unlikely	T29, T41	T9		T27, T50, T53,	
	Possible	T35		T42	T3, T10, T16, T54	
	Likely	T34				T1
	Certain					

Table 4.9 Range of threats for confidentiality, availability and integrity for scalable video

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

Based on the above analysis, availability is the highest concern, so we can implement changes that target these threats like implementing fast authentication key mechanisms and secure access to data throughput.

The above threat analysis can help determine the important threats to watch for, concentrating staff efforts and costs to make sure they do not occur. This helps manage the critical parts of the systems and also manage the costs.

4.12 Conclusions

Cloud computing refers to *on-demand access to a shared pool of computing resources*, providing reduced costs, reduced management responsibilities and increase in business agility. For these reasons, it is a popular paradigm to be used by end users from different professions. Security is, however, a major player in this equation as it can make or break deals for Cloud users and infrastructure providers alike.

The way forward is to come up with standards on how security can be assessed to minimize the risks in the systems as well as manage the costs as efficiently as possible. This chapter discussed a security risk methodology approach to assess the items which can jeopardise the security of the Cloud ecosystems and the actors involved in the Cloud. By performing a detailed documentation assessment and assigning a like-

lihood and priority to each of these threats, the items can be listed in order of priority to see which particular measure need to be taken first to reduce that kind of security risk. This allows work to be categorized in terms of the most important first when assessing complex ecosystems such as Cloud environments which have too many components that can go wrong during the service deployment or operation phases.

There is a further need for proper documentation and legal agreements to be drawn up to restore the trust of consumers in Clouds and effectively making business more aware of a detail approach to take when securing their systems.

Acknowledgments This work has been partially supported by the EU within the seventh framework programme under contract ICT-257115—Optimized Infrastructure Services (OPTIMIS).

References

1. Wills G (2009) Technical review of using Cloud for research, University of Southampton, Final Report 2009
2. Foster I, Zhao Y, Raicu I, Lu S (2008) Cloud computing and grid computing 360-degree compared. In GCE '08: Grid Computing Environments Workshop, pp 1–10. IEEE, Nov 2008
3. Catteddu D, Hogben G (2009) Cloud computing: benefits, risks and recommendations for information security, Technical Report, European Network and Information Security Agency (ENISA) 2009
4. Ried S, Kisker H, Matzke P (2010) The evolution of Cloud computing markets. Forrester Research 2010
5. Stamford C (10 Aug 2011) Press Releases, Gartner's 2011 Hype Cycle special report evaluates the maturity of 1,900 Technologies, 2011
6. Kiran M, Khan AU, Jiang M, Djemame K, Oriol M, Corrales M (2012) Managing security threats in Clouds, Digital Research 2012
7. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I (2008) Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Gener Comput Syst 25:599–616
8. Information Security Forum (ISF), Information risk analysis methodology (IRAM). https://www.securityforum.org/iram#iramtva. Accessed April 2014
9. Symantec Ltd., Symantec Data Loss prevention. http://www.symantec.com/en/uk/business/solutions/solutiondetail.jsp?solid=sol_info_risk_comp&solfid=sol_data_loss_prevention&om_sem_cid=biz_sem_emea_uk_Google_DLP. Accessed Nov 2010
10. Carpenter M, Liston T, Skoudis E (2007) Hiding virtualization from attackers and malware. IEEE Secur Priv 5(3):62–65
11. Naraine R (2011) Blue pill prototype creates 100% undetectable malware. http://www.eweek.com/c/a/Windows/Blue-Pill-Prototype-Creates-100-Undetectable-Malware, 2011. Accessed Dec 2013
12. Grid Security (2012) Industry insiders: insufficient security controls for smart meters, Published Online: 10 April 2012. http://www.homelandsecuritynewswire.com/dr20120410-industry-insiders-insufficient-security-controls-for-smart-meters, 2012. Accessed Dec 2013
13. HMGovernment (2010) HMGovernment G-Cloud, Crown copyright, 2010. http://gcloud.civilservice.gov.uk/. Accessed Dec 2013
14. Huddle Inc. Government storage. http://www.huddle.com/campaign/government-storage/. Accessed Oct 2012
15 UK Government (2012) G-Cloud brochures. http://www.fcoservices.gov.uk/eng/files/Government_Cloud_Solutions_Brochure.pdf. Accessed Oct 2012
16. Millman R (2012) SCC launches secure multi-tenancy Cloud on G-Cloud. Published Online: April 30, 2012. http://www.cloudpro.co.uk/cloud-essentials/3493/scc-launches-secure-multi-tenancy-cloud-g-cloud, 2012. Accessed Dec 2013

17. Scarfone K, Souppaya M, Cody A, Orebaugh A (2008) Information security testing and assessment, National Institute of Standards and Technology (NIST), Special Publication 800-115. http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf. Accessed Sept 2008
18. Whiteside F, Badger L, Iorga M, Shilong Chu JM (2012) Challenging security requirements for US government Cloud computing adoption (draft), Special publication 500-296, NIST, May, 2012
19. Pallman D (2010) Azure Blog, Threat modelling the Cloud, August 2010. http://davidpallmann.blogspot.com/2010/08/threat-modeling-cloud.html#fbid=8qxQ6O6UvEq. Accessed Dec 2010
20. Brink DE (2010) Security and the software development lifecycle: secure at the source. Aberdeen Group December 2010, research brief, 2010
21. Jansen W, Grance T (2011) Draft NIST special publication guidelines on security and privacy in public Cloud computing, Computer Security, Jan 2011
22. Brink D (2011) Security and cloud best practices July 2011, Aberdeen Group, 2011
23. Mell P, Grance T (2009) The NIST definition of Cloud computing, National Institute of Standards and Technology, Oct 2009
24. Khan AU, Kiran M, Oriol M, Jiang M, Djemame K (2012) Security risks and their management in Cloud computing. CloudCom, pp 121–128, 2012
25. Google Inc (2013) GoogleAppEngine platform as a service, Google developers. https://developers.google.com/appengine/. Accessed Dec 2013
26. Heroku Inc (2013) Heroku platform. https://www.heroku.com/. Accessed Dec 2013
27. den Braber F, Braendeland F, Dahl HEI, Engan I, Hogganvik I, Lund MS, Solhaug B, Stolen K, Vraalsen F (2006) The CORAS Model-based method for security risk analysis, SINTEF, Oslo, September, 2006. http://www.uio.no/studier/emner/matnat/ifi/INF5150/h06/undervisningsmateriale/060930.CORAS-handbook-v1.0.pdf. Accessed Dec 2013
28. Khan AU (2013) Data confidentiality and risk management in Cloud Computing, PhD thesis, Department of Computer Science, University of York, 2013
29. Khan AU, Kiran M, Oriol M (2013) Threat methodology for securing scalable video in the Cloud, 8th international conference for internet technology and secured transactions (ICITST-2013), Dec 9–12, 2013, London, UK