The Journal of Systems and Software 86 (2013) 2276–2293

Contents lists available at SciVerse ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

A framework to support selection of cloud providers based on security and privacy requirements

Haralambos Mouratidis[a,*], Shareeful Islam[a], Christos Kalloniatis[b], Stefanos Gritzalis[c]

[a] School of Architecture, Computing and Engineering, University of East London, UK
[b] Cultural Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, Greece
[c] Laboratory of Information and Communication Systems Security, Department of Information and Communications Systems Engineering, University of the Aegean, Greece

ARTICLE INFO

Article history:
Received 20 March 2012
Received in revised form 8 October 2012
Accepted 1 March 2013
Available online 26 March 2013

Keywords:
Secure software engineering
Privacy
Cloud computing

ABSTRACT

Cloud computing is an evolving paradigm that is radically changing the way humans store, share and access their digital files. Despite the many benefits, such as the introduction of a rapid elastic resource pool, and on-demand service, the paradigm also creates challenges for both users and providers. In particular, there are issues related to security and privacy, such as unauthorised access, loss of privacy, data replication and regulatory violation that require adequate attention. Nevertheless, and despite the recent research interest in developing software engineering techniques to support systems based on the cloud, the literature fails to provide a systematic and structured approach that enables software engineers to identify security and privacy requirements and select a suitable cloud service provider based on such requirements. This paper presents a novel framework that fills this gap. Our framework incorporates a modelling language and it provides a structured process that supports elicitation of security and privacy requirements and the selection of a cloud provider based on the satisfiability of the service provider to the relevant security and privacy requirements. To illustrate our work, we present results from a real case study.

1. Introduction

Software systems are a critical component of human society used in areas such as power, telecommunications, health-care, military, and education; not just by major corporations and governments but also by individuals who rely on them to perform every day activities. To support the above scenario, a new paradigm, known as cloud computing, has grown from a promising idea to one of the fastest research and development paradigms of the computing industry. Cloud computing supports software systems' infrastructure where the availability of resources, computational or otherwise, used in the specific model is dynamic; meaning that the hardware and software is dealt as services offered to the users of the cloud every time they need them. By virtually grouping hardware and software and providing it efficiently, cloud users are able to achieve great economical savings both in the functional and administrative cost of the specific ICT infrastructures.

However, the storage of personal and sensitive information in the cloud raises concerns about the security and privacy of such information and how much the cloud can be trusted. Security and privacy in this context requires solutions very different to those provided by current research efforts and industrial practices. Solutions that will not only try to guarantee security and/or privacy from a technical point of view, but solutions that provide clear understanding of the social aspects of security and privacy and take into account, for example, organisational structures, privacy needs and appropriate laws and regulations.

As the concept of cloud computing is relatively new, many organisations and individuals are still avoiding cloud services mostly because they are not sure if the services provided, by different providers, are suitable for their security and privacy requirements. This is especially true since organisations and individuals would have to hand in their personal and organisational data into service providers over which they have no control. This introduces an extra layer of complexity on top of the expected security and privacy issues that are present in any type of software systems and services whether on the cloud or not. These concerns make risky a transition to cloud computing or integration of a cloud solution to an existing IT infrastructure.

It is therefore important, that appropriate software engineering techniques are developed to support the structured and systematic identification of security and privacy requirements that an organisation might have for their systems' and based on those requirements to support selection of appropriate cloud services. However, and despite the recent research interest in developing

* Corresponding author.
E-mail addresses: haris@uel.ac.uk (H. Mouratidis), shareeful@uel.ac.uk (S. Islam), chkallon@aegean.gr (C. Kalloniatis), sgritz@aegean.gr (S. Gritzalis).

0164-1212/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jss.2013.03.011

software engineering techniques to support systems based on the cloud, the literature fails to provide a systematic and structured approach that enables software engineers to identify security and privacy requirements and select a suitable service provider based on such requirements.

Our work fills this gap by providing a process to support elicitation of security and privacy requirements and selection of a service provider based on the satisfiability (Giorgini et al., 2002) of the cloud provider to the security and privacy requirements. This paper is structured as follows. Section 2 provides a brief introduction to the various service and deployment models introduced by the cloud computing paradigm and it discusses security and privacy issues related to those models. Section 3 introduces our framework, while Section 4 presents the application of the framework to a case study based on a collaborative project in the domain of cloud based electronic point of sales (EPOS). Section 5 presents related work and Section 6 concludes the paper.

2. Security and privacy in the cloud

Before we describe our work, it is important to provide a brief introduction to the various cloud computing service and deployment models and discuss the different security and privacy issues related to them. Cloud computing is based on three delivery models, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), and four deployment models, private, community, public, and hybrid cloud. Security and privacy issues are among the most important concerns in cloud computing, as large amounts of personal and other sensitive data are managed in the cloud. Several surveys among potential cloud adopters indicate that security and privacy is the primary concern hindering its adoption (Bruening and Treacy, 2009). Therefore, it is necessary to understand and analyse the relevant security and privacy issues before adopting cloud computing into existing infrastructure. In doing so, we have performed a systematic literature review (Kitchenham and Charters, 2007) for understanding security and privacy issues for cloud based systems. As stated previously, the need to understand such issues are important and timely from both user and provider perspective for successful and trustworthy cloud adaption.

There is not much work that provides a systematic literature review about security and privacy issues in the cloud. The work of Sriram and Khajeh-Hosseini (2010) aim to provide a comprehensive review of the academic research done in cloud computing. The focus is more to define different cloud terminologies such as cloud computing, service model, deployment model, and to identify related technologies for designing and building clouds. Rosado et al. (2012) provide a review of different approaches related to security for migration process in cloud of legacy systems such as model based migration of legacy system into cloud and migrating legacy application to service cloud.

Our literature search process focuses on studies that consider security and privacy issues of cloud based systems. In particular, we focus on the security and privacy challenges, virtualisation, and possible risks, as keywords for the possible inclusion criteria of the cloud based system. We identified relevant literature from major research databases such as IEEE Xplore, SpringerLink, ScienceDirect, Elesevier, ACM Digital Library, and Google scholar. We consider only peer reviewed papers and count the citation of individual papers for establishing the impact of a paper. Initially we focused on titles and abstracts and select 35 papers from a total of 98 relevant papers. Based on the identified studies, we extracted several data items that consider threats, vulnerabilities, and risks within the context of cloud computing, based on security and privacy. The extracted data was combined based on cloud data properties, policies, threats and risks.

2.1. Cloud service models

In IaaS (Infrastructure as a Service), sometimes also called hardware-as-a-service (Grobauer et al., 2011), providers generally supply a set of virtual infrastructure components, such as virtual servers and storage. Users (customers) can order these components and have them running in a matter of minutes. User applications and data run on the provider's virtual machine and are stored in a virtual space. It is the provider's responsibility to ensure basic security, such as virtualisation and low-level data protection capabilities. Virtualisation infrastructure can be used as a launching pad for new attacks (Choo, 2010). Issues such as VM image and securing inter-host communication are critical from the provider's perspective (Gellman, 2009). Users have the responsibility to ensure the security of the applications managed by them. The main idea behind SaaS (Software as a Service) is to replace applications running on local machines and provide customers with the ability to use applications simply through use of web browser from different providers. Software as a Service as the core concept behind cloud computing (Erdogmus, 2009). In particular, at the end it is software, it does not matter whether the software being delivered is infrastructure, platform or application. However customers do not have control over the underlying cloud infrastructure, including network, operating system, storage, core functionality of the application, and the server itself. Security issues arise from the software that is used to manage the relevant customer information. Providers are usually responsible for ensuring the security of the customer data. PaaS (Platform as a Service) providers provide a programming environment as well as tools that have a visible impact on the application architecture deployment with the exception of issues related to the underlying operating system (Gong et al., 2010). It is the bridge between hardware and application. Although customers are mostly responsible for protecting their own applications, providers also need to ensure that the operating system, its modules, and anything below the application layer are secured and inaccessible or that there is limited access between applications.

2.2. Cloud deployment models

Before deploying an organization's data and processes to the cloud, it is recommended to analyse all different deployment models. This is because not all cloud deployment models are appropriate for every service and may not meet specific customer expectations (Bruening and Treacy, 2009). It highly depends on the customer's requirements of the system, such as control needed over the service and importance of data stored. A private cloud is limited to a single customer. Customers generally have control over deployed applications and their own infrastructure and can request customizations to fit their needs. Due to this exclusiveness, a private cloud is considered safer than the other models. Public clouds require much more investment compared to private cloud and usually owned by large organisation. In a public cloud, security issues are more critical due to aspects such as virtualisation, which arise from supporting multiple users. Security measures, such as ensuring access control, data access, and availability of individual customer resources is necessary for a secure multi-tenant environment. In case of a hybrid cloud, the resources are divided between a private and a public cloud. Therefore, security and privacy issues should be paid adequate attention, as there may be multiple providers involve that make it difficult for key distribution and mutual authentication.

2.3. Cloud security and privacy

We consider security and privacy from a holistic perspective based on our extracted data from the literature. The term holistic considers both technical issues, such as data integrity, availability of service, and accountability of provider activities and non-technical issues such as compliance, and policies (Islam et al., 2012b, Islam et al., 2010). Comparing to the other software system paradigms, cloud computing has some unique features in terms of service and deployment models. Therefore these issues require adequate attention for supporting the systematic identification of security and privacy issues in the context of cloud computing. At the same time all types of proactive counter measure such as monitoring, patch management, and hardening virtual machine instances should be implemented (Rosado et al., 2012). The following security and privacy issues are worth considering within the context of cloud computing:

2.3.1. Data integrity

It is one of the most important factors when considering security in the cloud. Data integrity can be easily achieved in a standalone system, but because in a cloud solution multiple databases are used to store multiple tenants' data, it is really complex to ensure transaction durability and consistency. As the cloud environment is virtualised at some level, standard methods, such as HTTP, of maintaining guaranteed transactions are not possible and the only way to do that is at Application Programming Interface (API) level (Subashini and Kavitha, 2011). Sometimes this introduces extra complexity, and, through complexity, possible security vulnerabilities in the API stack itself or the technology handling the API calls. Vulnerabilities in API stack could allow an attacker to dump transaction data, intercept and provide false or corrupt data to the transaction destination which would lead to further data corruption, data theft and service breakdown leading to financial loss. Data integrity is measured by the level of secure channels in place for handling transactions. This is why data have to be transferred among servers and databases though secure channels (e.g. SSL), every transaction has to be verified for legitimacy (e.g. checksums), certain level atomicity, isolation and durable. APIs handling the transactions have to be reliable, well recognised and time-tested (e.g. simple object access protocol (SOAP)).

2.3.2. Data segregation

One of the major cloud characteristics is multi-tenancy. In multi-tenancy environment several users' data might be stored at the same physical location using the hypervisor techniques under the concept of virtualisation. This means that an organization's data may be mingled in various ways with other users' data causing confidential data leakages; while users of other organisations might be exposed with the data of other organisations. For example, in 2009 a security flaw was discovered in Google Docs, which exposed documents to users that belonged to other users. That security problem happened because of crippled user session allocation. The problem was patched within hours, but it showed that users' data storage has to be separated to prevent accidental data leaks.

2.3.3. Data availability

Providers must provide on-request and reliable service with highest up-times (it depends on the type and importance of corporate data and processes, but it might be up to 99.9999%, which is equivalent to 31.56 s of downtime per year (Rosenberg and Mateos, 2011)). If an organization's data gets locked-in and providers fail to provide access, this service disruption could pose potential financial damage to the organisation and its clients.

2.3.4. Network availability

As cloud usage mostly depends on network connectivity and bandwidth, it is vital that the cloud is available whenever needed and that bandwidth throughput is able to handle organisation storing and retrieving data in the cloud. If these conditions are not met, the consequences will be similar to poor data availability. One strategy that could be deployed to attain high availability is obtaining the services of multiple cloud computing providers, other than a single provider (Armbrust et al., 2010). Provider could quick the scale-up in case of disruption of network bandwidth. In terms of availability, quality of service requirements relating to response time, throughput, reliability, scalability, and availability should be negotiated with the service provider (Ferretti et al., 2010).

2.3.5. Backup strategy

An Organization's data might be backed-up and encrypted by the provider but it might be better, in some cases, for an organisation to backup their data on the cloud and then encrypt it. Backup and recovery is essential in case of failure. Data backups and recovery should be done regularly, and as another security measure backed-up data should be encrypted and stored on the different location. Encryption keys should be managed by the organisation in this case.

2.3.6. Provider's transparency

Cloud provider should provide the details of how client data will be handled, what types of security they already apply to the cloud infrastructure, what happens in case the system was compromised, if and how they will participate in the investigation and prosecution. If some details about the internal policies and technology implementation are kept in secret, clients must not blindly trust the provider's claims about security in their environment (Cachin and Schunter, 2011). In this case provider must be investigated well by the organisation, first assuming that provider's environment is insecure and after investigation making corrections to the initial assumption. Cloud provider might give all the important details when contacted directly, but it is better to be safe first and hold from quick decisions.

2.3.7. Data protection

Customer data protection is a core concern of security and privacy measures in cloud computing. Privacy is a moral and legal right of individuals. Data owner need to be ensured that their data is not shared with any third party (Takabi et al., 2010). Storing data and applications that reside outside the organization's premises poses the potential risk of unauthorised access and processing of the data and application (Chen et al., 2010). Customers may lose control over their critical assets. Data confidentiality and privacy risks may be more critical when providers reserve the right to change their terms and conditions. Apart from the data theft from external attackers, data leakage can also be carried out by the employees of the service providers. Therefore, measures such as privacy policy, data subject consent and control, unlinkability, transparency of data, data operations, and assurance of data protection are necessary and should be included in the SLA.

2.3.8. Organisational policies

The cloud provider needs to establish trust in the service offered to the customers (Chen et al., 2010). To achieve a certain level of trust, organisations need to develop, document, and deploy policies relating to information security management systems, legal compliance, and service level agreement. Policy refers to a set of rules to be followed by the participating entities within the cloud environment (Islam and Dong, 2008). Organisations should have a clearly defined access control, privacy, back up, disaster recover, business continuity and key management policy (Islam et al., 2012b). Access

control determines how customers and providers can be identified, authenticated and authorised to access data and service. Privacy policy is a comprehensive description of the way the information is handled, stored and used. It should truly protect customer privacy and the customer should have maximum control over the data and processing. Key management policy deals with the management of keys for the cryptographic operation. This policy provides guideline how to generate exchange, store, distribute, and replace keys. Disaster recovery and business continuity focus how in particular cloud service provider recovers from any failure and continue their business to support the customer. This policy should also suggest approaches to satisfying information security and data privacy laws and directives with a view to minimising the impact of management overhead on organisational resources and efficiency. Policies should be unambiguous, understandable and agreed upon by all participating entities. Cloud users should understand all the above mentioned provider's policies before undertaking cloud to support existing business infrastructure.

2.3.9. Legal compliance

Legal compliance is a significant challenge for cloud-based systems. Although a large number of information security and data privacy laws exist, depending on the country and location, there is no single, comprehensive legal framework in which the legal rights, liabilities, and obligations of cloud providers and cloud users are formulated (Islam et al., 2011). Both providers and customers need to comply with existing regulatory requirements and service level agreements (SLAs). SLA should be complete as well as well structured, taking into consideration the right to audit such as quality of service attributes should monitor continuously and enforced by SLA (Dawoud et al., 2010). On the one hand, customers may have to give their private data and important processes into the hands of personnel and out of their control. On the other hand, providers may be obliged to search the data due to national security or to comply with local jurisdiction. The law is enforced at the place the data is stored as well as the place from where data are transmitted. Customers should take note of the jurisdictions in which their data may be stored or processed in. Therefore, it is necessary to identify and analyse issues such as legal rights and alignment of SLA with legal obligations, protection and enforcement requirements before deploying a cloud computing solution.

2.4. Security and privacy threats

Security and privacy threats are one of the main primary concerns in cloud computing and present strong barrier for cloud adaption. Threats relating to insecure API, session or service hijacking, authentication and identity management, privacy protection, malicious insiders, and service management should be identified and controlled through a systematic risk management method (Cloud Threat, 2010; Takabi et al., 2010). Vulnerabilities can arise from unique cloud properties such as Ubiquitous network access and On-demand self-service, cloud infrastructure and technology such as virtualisation, software environment, and computational resource (Grobauer et al., 2011). When security of cloud infrastructure gets compromised, the provider should react quickly and prevent further unauthorised access; patch security holes as soon as possible and almost immediately inform clients. Letting clients know about the breach will allow them to take appropriate actions to protect their data even if their system and data were not affected. Privacy risks such as data leakage, and policy breach can be controlled if the appropriate policies and agreement are used for ensuring accountability of the every activity. Providers must initiate or offer help in the breach investigation and prosecution. Like security, privacy is an important issue in cloud computing in terms of both legal compliance and trust. Customers pay more attention to the privacy issues in cloud because customer data stored in the cloud often contains sensitive information (Islam et al., 2012b). Customers have less control over this data and the overall cloud infrastructure may not be trustworthy.

2.4.1. Loss of physical control

Organisations are worried about losing physical control over their data and business processes. The idea of the cloud computing is to outsource them increasing business performance and decreasing costs. But this means that data and processes are no longer in the total control of the organisation, someone else will be dealing with them and both data and processes might reside on different physical locations. Provider on their side must ensure organisation has maximum control possible over the data and business processes.

2.4.2. Vulnerabilities in virtualisation

Virtualisation is one of the base components in the cloud infrastructure. It allows the cloud infrastructure to be shared among multiple users but logically separated area through hypervisor technology. If security laid in virtualisation technology is vulnerable it could cause major security breaches from both organization's and provider's perspective. Attacker or a malicious user might exploit vulnerability in virtualisation layer and get access to other instances or virtual machines running on the same physical machine or to underlying system running virtualised environment itself. For instance, an attacker can exploit side-channel attack to instantiate new VMs of a target VM, so that new VM can monitor the cache of the physical machine. A path traversal vulnerability was discovered in one of the leading virtualisation vendor's – Vmware – solution: it allowed attacker to break out of isolated guest system and compromise underlying host system. Such vulnerability has high impact on the cloud environment. If host system, running several applications and guest virtual systems is compromised, multiple tenants, users might be affected: data stolen, new virtual machines launched to raise attack to the higher level (e.g. for the Denial-of-service attack (DDoS)). To prevent this happening virtualisation system should run on lowest permissions possible and be extra hardened and patched frequently. Furthermore, user privilege to access the system should be need basis and privileged users access needs cloud monitoring and control.

3. Framework

3.1. Overview of the framework

The proposed framework consists of a language and a process that is focused on the requirements engineering stage. The language employs concepts from the requirements, security and privacy engineering domains, and it is based on our previous work on security requirements engineering, and in particular Secure Tropos (Mouratidis, 2004; Mouratidis and Giorgini, 2007) and privacy requirements engineering, and in particular PriS (Kalloniatis et al., 2008). However, the language is enriched with new concepts, such as cloud actor, measure, and mechanisms, which are necessary to support the selection of the cloud provider. The process follows the typical cycle of a requirements engineering process where we have the requirements elicitation and the requirements analysis phases. Elicitation is focused on ensuring that a system's requirements are elicited and understood, while analysis focuses on ensuring that requirements are specified and modelled. To support the proposed framework, a tool has been developed using the Open Models Initiative (OMI) Platform (www.openmodels.at). The proposed framework demonstrates an important set of unique characteristics:

- Its metamodel unifies requirements, security and privacy concepts.
- The process introduces a structure approach to the elicitation and analysis of security and privacy requirements.
- It supports the selection of a cloud service provider based on the security and privacy mechanisms required by the system.
- It uses the same concepts throughout the process to support common understanding. This is particularly important since using different techniques and methods usually results in misunderstandings due to the differences on concepts and terminology used by the different approaches.
- It enables the analysis of security, privacy and system requirements under one uniform framework, which results in the identification of conflicts that usually exist between these types of requirements and enables the resolution of such conflicts and the identification of security and privacy mechanisms that satisfy the relevant requirements.

3.2. Language

The language of the proposed framework is based on concepts that have been defined in the requirements engineering discipline, and in particular in the i* framework (Yu, 1995), combined with concepts from the security requirements engineering literature, and in particular Secure Tropos (Mouratidis, 2004), and enhanced with concepts from security engineering and privacy engineering, and in particular PriS (Kalloniatis et al., 2008). In particular, our metamodel, illustrated in Fig. 1, defines the concept of an *Actor* as an entity that has strategic goals and intentions within the system or within an organisational setting (Yu, 1995). An actor can be human, a system, or an organisation. We also define a special class of an actor, a *cloud actor*. A cloud actor is an actor that demonstrates two unique characteristics, it provides a deployment model and it supports a service model. It is worth stating that as an actor, a cloud actor also inherits all the attributes and associations of the actor, for example it has goals, capabilities and it requires resources. We also differentiate a special class of an actor, a *malicious actor*. A malicious actor's intention is to introduce threats to the system, which exploit vulnerabilities. *Vulnerabilities* are defined as weaknesses or flaws, in terms of security and privacy that exists from a resource, an actor and/or a goal. Vulnerabilities are exploited by threats, as an attack or incident within a specific context. It is worth stating that legitimate actors might unintentionally introduce vulnerabilities to a system due to failure or mistakes. *Threats* pose potential loss or indicate problems that can put the system at risk. On the other hand, actors within the system environment have single or multiple goals A *Goal* represents an actors' strategic interests (Yu, 1995). Higher level strategic goals may be decomposed in simpler operational goals forming AND/OR goals hierarchy. Our meta-model differentiates between organisational, security and privacy goals, These goals introduce security and privacy constraints. A *Constraint* is used to represent a set of restrictions that do not permit specific actions to be taken, restrict the way that actions can be taken or prevent certain system objectives from being achieved (Mouratidis, 2004). Security and privacy constraints are clearly defined as separate concepts to support a clear and well-structured elicitation and analysis of security and privacy requirements. When a constraint is introduced, further analysis is required to establish if and how that constraint can be satisfied. Within the context of our metamodel, a constraint is satisfied by a measure. A *measure* represents a generic, implementation independent form of control that indicates how a constraint will be achieved. Measures are operationalised by relevant plans. A *plan* defines a specific way of operationalising a measure, i.e. the details and conditions under which a specific measure is operationalised. Plans are implemented by relevant mechanisms. A mechanism is defined as a technical solution that realises one or more plans. Mechanisms are software products developed already or customised software tools for realizing plans for the specific organisation. Mechanisms require resources and they are supported by capabilities. An actor has *capabilities*, which enable her to support the implementation of *mechanisms*. It is worth mentioning that the types of measures, plans, mechanisms follow the type of the constraint that the measure satisfies. For example, a security constraint is satisfied by a security measure, which is operationalised by a security plan, which is implemented by a security mechanism.

3.3. Stakeholders

We have identified a number of stakeholders who take part in the development process of the presented framework. These are briefly described below:

- *System owner*: This represents an entity, such as an organisation or individual, who owns the system under development.
- *Requirements engineer*: The Requirements Engineer is responsible for eliciting and analysing the requirements of the system. She/he might be part of the organisation that owns the system, or she/he might be an external consultant.
- *Security engineer*: The security engineer is responsible for supporting the elicitation, analysis and implementation of security requirements. She/he might be part of the organisation that owns the system, or she/he might be an external consultant.
- *Privacy engineer*: The privacy engineer is responsible for supporting the elicitation, analysis and implementation of security requirements. She/he might be part of the organisation that owns the system, or she/he might be an external consultant.
- *Cloud expert*: The Cloud Expert is responsible for providing cloud computing related expertise to the project and for supporting the cloud provider selection by analysing the cloud providers, and weight their contribution.

It is worth stating that most of the times, the roles of Privacy and Security Engineer will be played by the same expert.

3.4. Process

The process supported by the framework is iterative and it is based on the development of a set of models that are incrementally refined to include further details. It provides a structured way of eliciting and analysing security and privacy requirements, identifying relevant security and privacy mechanisms and of selecting an appropriate cloud service provider based on these mechanisms. It comprises of three main activities: *the Security and Privacy Cataloguing*, the *Security and Privacy Analysis*, and the *Selection of Cloud Service Provider*. Each one of these activities has specific inputs and it results in specific outputs. It is worth mentioning that only two of these activities, i.e. the security and privacy requirements analysis, and the selection of cloud service provider are compulsory. The security and privacy cataloguing is an optional activity, which can assist in identifying relevant security and privacy issues during the security and privacy requirements Analysis. This means that depending on the structure of an organisation, its resources and the team allocated to carry out the process, some organisations will make use of the security and privacy cataloguing to develop a catalogue of security and privacy issues to support their security and privacy requirements elicitation and analysis and the identification of relevant security and privacy mechanisms, while others will not use the cataloguing activity.

To support easier understanding and to better enhance communication of the presented process, we make use of the OMG standard Software and Systems Process Engineering Metamodel

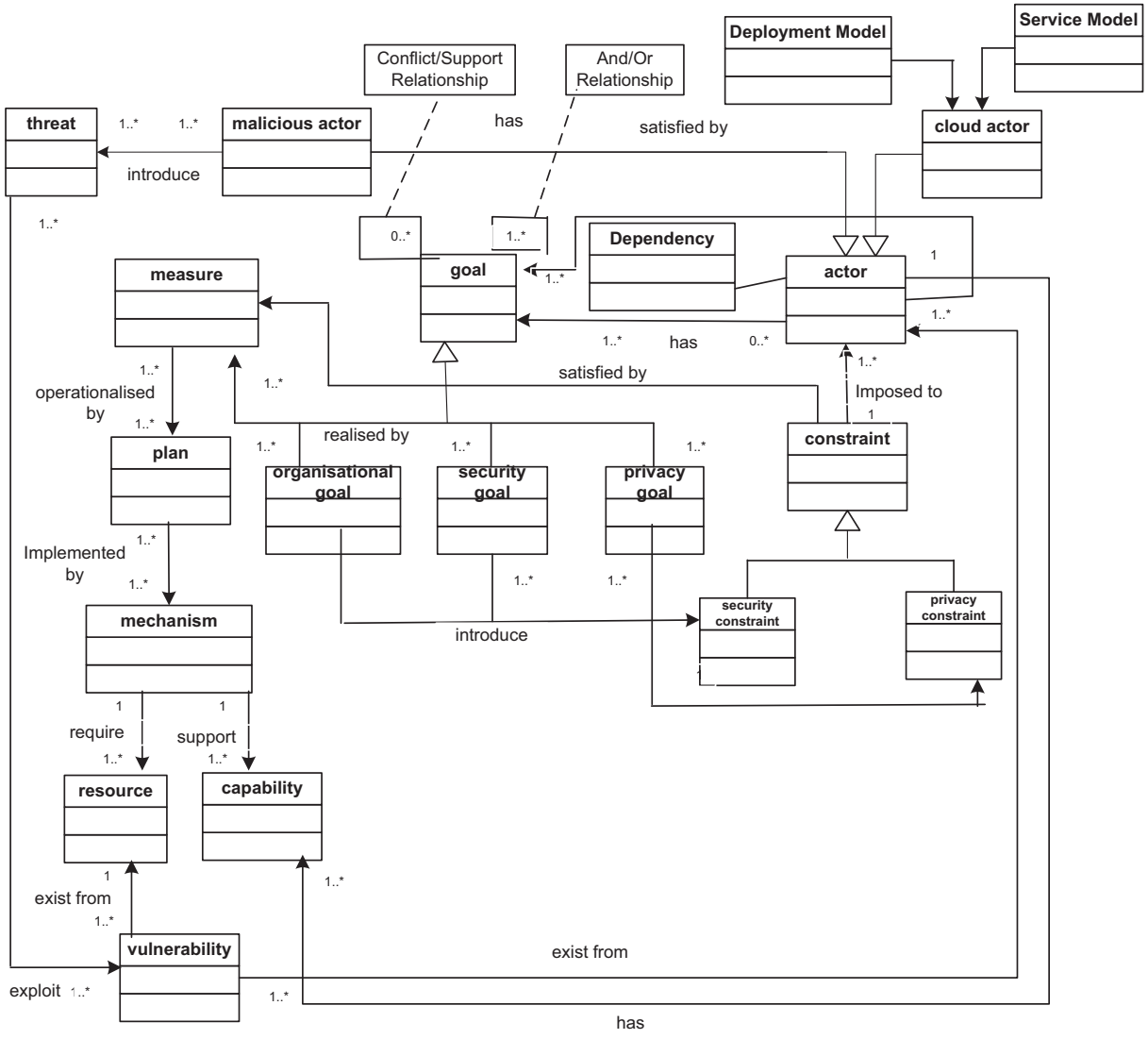

Fig. 1. Meta model for security and privacy concepts.

(SPEM) version 2.0 (OMG, 2008). SPEM is a process meta-model, which is used to describe a concrete software development process or a family of related software development processes. The SPEM specification is structured as a UML profile, and provides a complete MOF-based meta-model. This meta-process modelling is a type of metamodelling used in software engineering to support the effort of creating flexible process models. In accordance with SPEM, we specify the process with its activities and inputs/outputs as shown in Fig. 2 and furthermore we describe (in the corresponding section) each activity by specifying: the WorkProduct as both input and output respectively; the roles that perform or participate in this RoleUse activity; the collection of Steps defined for a TaskUse that represents all the work that should be carried out to achieve the overall development goal of the Activity; and the Guidance that specifies the practices, techniques or standards to consider when performing the TaskUse.

3.4.1. Security and privacy cataloguing

The security and privacy cataloguing activity assists in identifying and cataloguing security and privacy issues. Such information can be employed in later activities of the process to support the elicitation and analysis of security and privacy requirements and the identification of relevant security and privacy measures and mechanisms. In fact the main aim of this activity is to develop a reference catalogue model that can be employed not just for the project for which it was initially developed but to work as a reference model for any projects that demonstrate similar characteristics. Therefore the security and privacy cataloguing activity aims to help the development of a reference point that is based on previous experience and support the modification and/or extension of that reference based on an individual software system needs. It is expected that the security and privacy catalogue will be developed by security and privacy experts with input for relevant domain experts. For instance, a security and privacy catalogue for cloud computing requires significant input of cloud computing experts. In some cases, the knowledge represented needs to be focused on specific organisational processes and procedures, and in that case an organisational expert is needed. As mentioned above, this activity is optional and whether it is needed or not depends on a number of factors:

- *Previous knowledge:* There are organisations that might already have developed catalogues not just for security and privacy but for any factor related to potential systems development in which they are involved. Such catalogues might be represented in

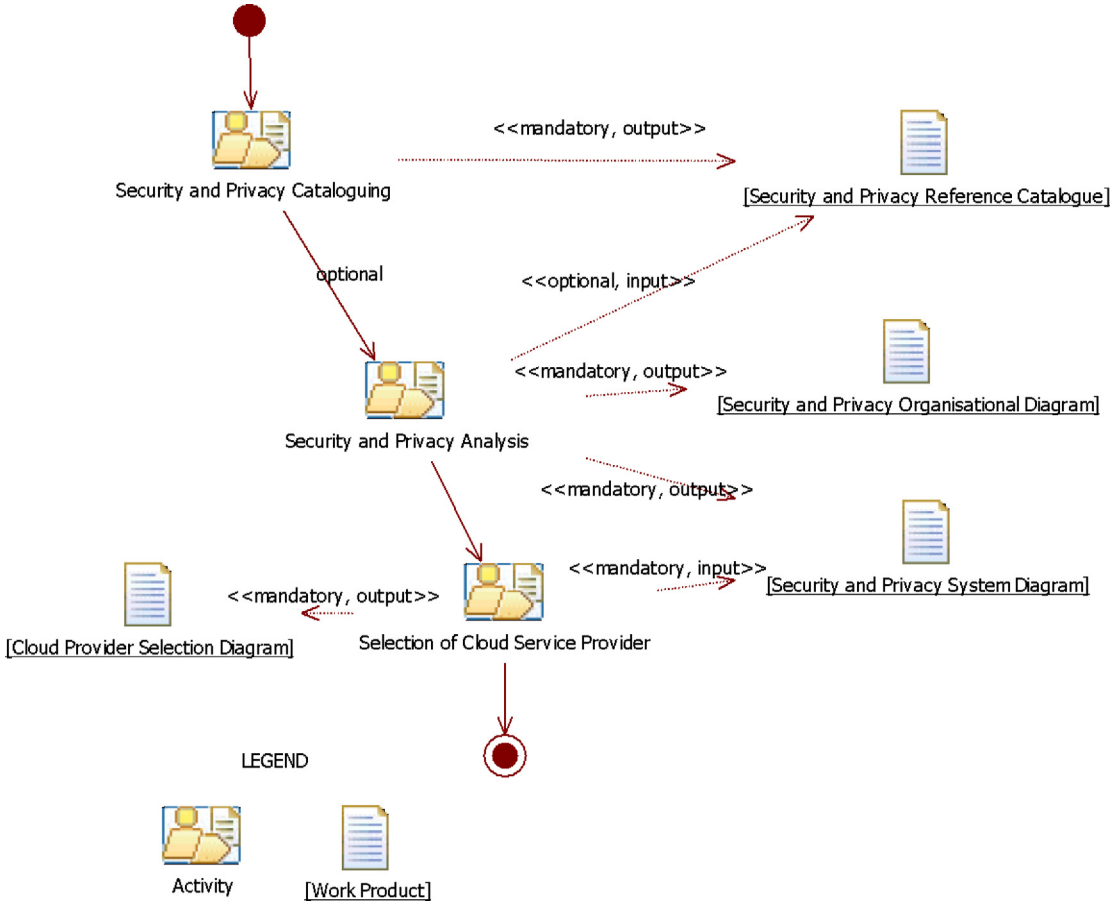

Fig. 2. Process definition in SPEM.

various forms, such as software repositories, patterns, open archival information system (OAIS) models, or just simple textual catalogues.

- *Development team organisation:* In projects where the main development effort during the requirements engineering process depends involves only requirements engineers, who might not have relevant security and privacy expertise, then a catalogue would be useful for the requirements engineers to be able to understand and analyse security and privacy issues. On the other hand, in projects where security and privacy experts are involved during the requirements analysis and elicitation process, a catalogue might not be necessary.
- *Constraints:* Depending on the constraints, in terms of time, cost, resources, that might be imposed to a project, the development of a reference catalogue for security and privacy might not be feasible.

When a catalogue is employed, it can be useful for the later activities of our process since it can support the elicitation of security and privacy requirements, identification of relevant measures and definition of relevant security and privacy mechanisms. For example, a requirements engineer might not be familiar what privacy mechanisms are needed for implementing a specific privacy plan. The catalogue can be used in that case to guide the engineer.

As stated above, our framework does not restrict the form that the artefact from the security and privacy cataloguing activity takes. This is important in order to allow usage of existing catalogues. However, as part of our framework we have developed a diagram that can be employed to model the results of the security and privacy cataloguing. Usage of that diagram introduces an important advantage for the system developers, since the proposed security and privacy cataloguing diagram uses the same concepts as the rest of our process. As such, a direct transfer of information between the security and privacy reference catalogue and the rest of the diagrams of the proposed process is possible. Moreover, support is provided by the framework's tool to develop the cataloguing diagram. Table 1 illustrates the definition of the security and reference cataloguing in SPEM.

3.4.2. Security and privacy analysis

The next main activity in our process is the security and privacy analysis activity, which aims to assist developers during the

Table 1
Security and privacy reference analysis activity define in SPEM.

Security and privacy reference cataloguing
Activity {**kind: phase**}**:** Security and privacy reference cataloguing
ProcessPerformer {**Kind: optional**}
RoleUse: Security Expert{**Kind: in**}
RoleUse: Privacy Expert {**Kind: in**}
RoleUse: Domain Expert {**Kind: in**}
WorkDefinitionParameter {**Kind: in**}
WorkProductUse: Oganization Security Knowledge
WorkProductUse: Oganization Privacy Knowledge
WorkProductUse: Security/Privacy Features Catalogues
WorkProductUse: Security/Privacy Threats Catalogues
Work DefinitionParameter {**Kind: out**}
WorkProductUse: Security and Privacy Reference Catalogue Diagram
Steps
Step: Identify Security and Privacy Goals
Step: Identify threats
Step: Identify Security and Privacy Measures
Step: Identify Security and Privacy Mechanisms

Table 2
Security and privacy requirements elicitation SPEM definition.

Security and privacy requirements analysis
Activity {**kind: phase**}**:** Security and Privacy Requirements Analysis
ProcessPerformer {**Kind: primary**}
RoleUse: Requirements Engineer {**Kind: in**}
RoleUse: Security Expert {**Kind: in**}
RoleUse: Privacy Expert {**Kind: in**}
RoleUse: Cloud Expert {**Kind: in**}
WorkDefinitionParameter {**Kind: in**}
WorkProductUse: Oganization Policies
WorkProductUse: Security and Privacy Reference Catalogue {**kind: optional**}
WorkProductUse: Oganization Requirements
Work DefinitionParameter {**Kind: out**}
WorkProductUse: Security and Privacy Organisational Diagram
WorkProductUse: Security and Privacy System Diagram
Steps
Step: Define Organisational Context
Step: Define Security and Privacy Concerns

software system development cycle to identify relevant security and privacy requirements of the system along with relevant measures and protection mechanisms. That information is then used on the last activity of the proposed framework to support the selection of a suitable cloud provider. The activity consists of two main sub-activities, each with a number of steps. A definition of the overall activity, using SPEM, is shown in Table 2.

3.4.2.1. Define organisational context. This is the first sub-activity, which triggers the whole process for security and privacy requirements engineering. It allows understanding of the organisational context and in particular identification of organisational goals, actors, their plans, resources and a set of security and privacy goals. The output of this activity provides an overview of the organisation, which is necessary to identify, and analyse the relevant security and privacy needs. The main output of this activity is a set of organisational goals, actors, goals, plans, resources, security and privacy goals. As shown in Fig. 3, it consists of four main steps: *Identification of Organisational Goals*, *Identification of Actors and Dependencies*, *Identification of Plans and Resources*, *Identification of Security and Privacy Goals*.

3.4.2.2. Identification of organisational goals. In our work, we consider an organisation has a set of actors who have some common goals. These are the organisational goals that support the overall objective and business needs of the organisation. These goals can be initially high level goals that can be refined to provide more explicit goals. Such explicit lower level sub-goals contribute to meet the parent goal. Goal refinement is achieved using relevant goal-oriented requirements engineering techniques, such as AND/OR hierarchies. In identifying organisational goals, the organisational business plan plays an important role, as the various main stakeholders related to the organisation.

Identification of actors and dependencies: This step considers identification of the entities related to the organisation in terms of actors. Actors can be identified both from within the organisation and from outside the organisation and they can be, as indicated earlier in the paper, humans as well as systems. It is worth mentioning that it is important to identify, not just actors that directly contribute to the goals of the organisation, but also actors that indirectly make some kind of contribution. For instance, in cases where an organisational actor depends on a non-organisational actor for the achievement of a goal, or plan or the provision of a resource, the latter should be included in the set of relevant actors. As part of that step, relevant dependencies between the various actors are also identified.

Identification of plans and resources: Generally an actor within an organisation has goals, executes plans to fulfil those goals, and uses (informational or physical) resources to achieve plans. Such plans and resources required from the identified actors to fulfil their goals (both individual goals as well as organisational) need to be identified. The main concern when dealing with resources is whether the resource is available and who is responsible for its delivery. It is also important, during this step, to make sure that plans and resources that an actor needs to satisfy any dependencies are also being identified.

Identification of security and privacy goals: The relevant security and privacy goals need to be elicited. In doing so, the Security and Privacy catalogue can be employed, if it exists, but it is important to make use of relevant laws and regulations as well as any previous experience that the development team might have. If the organisation has a security policy, this would be an important source of information. It is worth stating that the main aim of this step is not to "blind" use all the security and privacy goals that exist in the literature, but to identify those that are relevant to the system. For example, there might be that all security goals might be relevant, i.e. Confidentiality, integrity and availability, while only unlicability is the relevant privacy goal.

3.4.2.3. Define security and privacy concerns. Once the organisational context is defined, the next sub-activity focuses on the identification of security and privacy requirements. As stated previously, we introduce the term security and privacy constraints to enable developers to adequately capture security and privacy requirements. As illustrated in Fig. 4, this sub-activity consists of the following three steps: *Identify Security and Privacy Requirements*, *Identify Security and Privacy Measures*, *Identify Security and Privacy Mechanisms*.

Identify security and privacy requirements: This step identifies the relevant security and privacy constraints. In the context of our work we define a constraint as a restriction, related to the security and privacy issues, imposed to one or more actors, which restricts the actor from performing certain actions (Mouratidis, 2004). Constraints aim to support the security and privacy goals and they are elicited from various sources such as organisational goals, stakeholder needs, respective laws and directives, security policies, possible threats identified from risk analysis methods etc. Generally actors perform specific plans by respecting the constraints imposed to them and they require certain resources to accomplish the relevant plans in order to fulfil their goals. Actors might depend on other actors for plans they cannot accomplish themselves. As part of that activity, relevant threats and vulnerabilities are also identified and security constraints are introduced to the system to enable protection from such threats and vulnerabilities. The security and privacy reference catalogue can play an important aspect on the identification of threats and vulnerabilities, since developers are able to input directly identified threats to this activity.

Identify security and privacy measures: This step aims to identify security and privacy measures that support the satisfaction of relevant security and privacy constraints. Measures are identified with the support of security and privacy experts as well as cloud experts. Moreover, plans are identified for each actor to support the operationalization of the identified measures.

Identify security and privacy mechanisms: This step aims to identify security and privacy mechanisms that support the implementation of the relevant plans. Similarly to measures, mechanisms can be identified with the support of security and privacy experts as well as cloud experts and usage can be made of the security and privacy catalogue, if such catalogue exists.

3.4.3. Selection of cloud service provider

Once all the security and privacy mechanisms have been identified, the next activity includes the selection of an appropriate service provider based on the degree of satisfaction of these

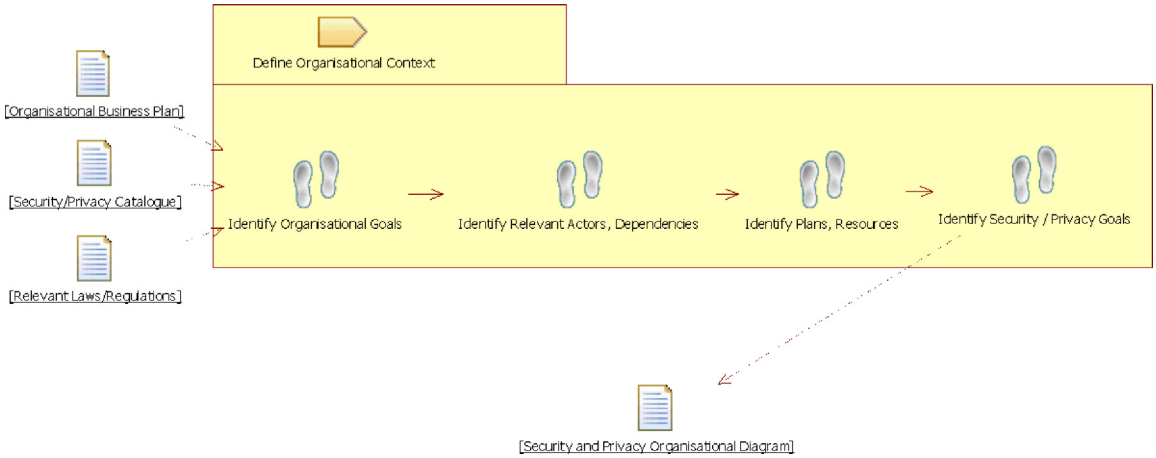

Fig. 3. Define organisational context steps.

mechanisms by potential cloud providers. For this reason, we have developed an analysis technique to enable developers to select among alternative cloud providers using as criteria the security and privacy mechanisms of the software system under development.

The proposed technique is similar to the evaluation process for organisational styles proposed by Kolp et al. (2001). The main difference is that Kolp's process is based on a qualitative reasoning, while the technique proposed by this research is based on an independent probabilistic model, which uses the measure of *satisfiability* proposed by Giorgini et al. (2002). In our work, satisfiability represents the probability that the security and/or privacy mechanism will be satisfied. Thus, the evaluation results in contribution relationships from the cloud provider to the probability of satisfying the security and/or privacy mechanisms of the system identified in the previous activity of our process.

To express the contribution of each provider to the satisfiability of each security/privacy requirement of the system, a weight is assigned. Weights take a value between 0 and 1. The allocation of such weights is performed by the security, privacy and cloud experts after studying the required security and privacy mechanisms and the various characteristics and provisions that a potential cloud provider has in place to support these mechanisms. To assist the allocation of the weights, we have developed a four points scale, which needs to be used by the experts for each provider and their provision for each of the mechanisms. That scale is as follows:

- When the provider has no provision to support the required security and/or privacy mechanism, then a weight of 0.25 is allocated.
- When the provider has limited provision to support the required security and/or privacy mechanism, then a weight of 0.5 is allocated.
- When the provider has provision to support the required security and/or privacy mechanism, but such provision has not been tested, then a weight of 0.75 is allocated.
- When the provider has a fully tested provision to support the security and/or privacy mechanism, then a weight of 1 is allocated.

In order to understand the level of provisions provided by each provider, experts might perform different techniques such as questionnaires, interviews. Our framework assumes that any final decision made on the estimate of the satisfiability is based on expert judgments or through the use of a procedure for reaching consensus in the event of disagreements amongst the experts.

Once a consensus has been reached and the various satisfiability weights have been recorded, the overall satisfiability level is calculated for each provider. The overall satisfiability level is calculated by summing up all the satisfiability values of an individual cloud provider and dividing that sum by the number of security and privacy mechanisms required by the system. The cloud provider with the highest satisfaction level is the preferred provider. If one or more providers achieve the same satisfaction level, then relevant security and privacy mechanisms are prioritised and a prioritisation weight is allocated to the satisfiability levels. The provider with the highest satisfability level is the preferred provider. Table 3 illustrates the SPEM definition for this activity.

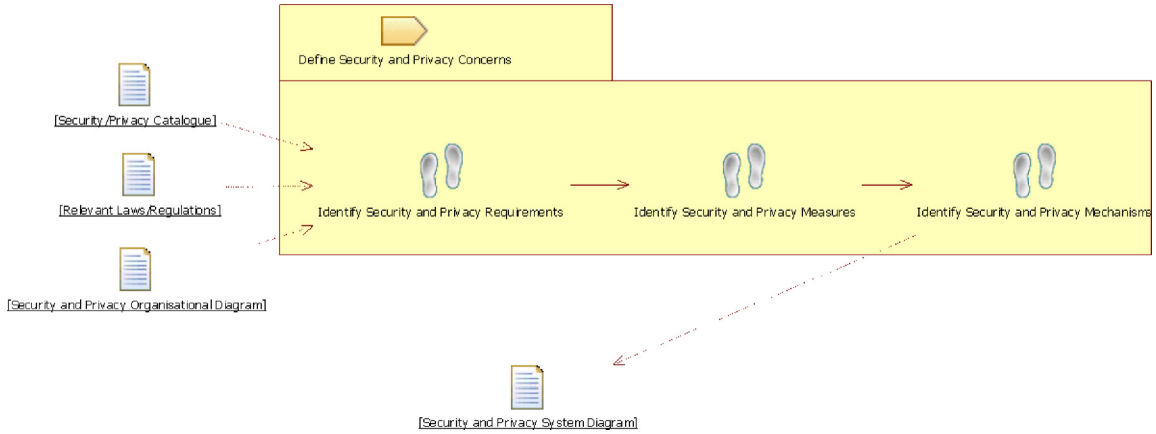

Fig. 4. Define security and privacy concerns steps.

Table 3
SPEM definition for selection of cloud provider selection.

Selection of cloud service provider
Activity {**kind: phase**}**:** Selection of Cloud Service Provider
ProcessPerformer {**Kind: primary**}
RoleUse: Requiremetns Engineer {**Kind: in**}
RoleUse: Cloud Expert {**Kind: in**}
WorkDefinitionParameter {**Kind: in**}
WorkProductUse: Security and Privacy Requirements Analysis
Work DefinitionParameter {**Kind: out**}
WorkProductUse: Cloud Provider Selection Diagram {**Kind:out**}
WorkProductUse: Preferred Service
Steps
Step: List Security and Privacy Mechanisms
Step: Identify Relevant Cloud Service Providers
Step: Analyse Service Providers based on satisfiability weights

3.5. Tool support and diagrams

The framework is supported by a tool that has been developed based on the Open Models Initiative ADOxx Platform (www.openmodels.at). ADOxx is a platform, similar to Eclipse, developed specifically to support the creation of tools for modelling methods based on the methods metamodel. The tool provides an environment for developers to create a number of diagrams that support the described process. In particular, the process described in the previous section results in the development of four artefacts represented in terms of four diagrams. These are the *Security and Privacy Reference Catalogue Diagram*, the *Security and Privacy Organisational Diagram*, *the Security and Privacy System Requirements Diagram* and the *Cloud Provider Selection Diagram* respectively.

3.5.1. Security and privacy reference catalogue diagram

For the construction process of the security and privacy reference catalogue diagram the team of developers, requirements engineer, security, privacy and cloud experts, consider security and privacy goals, security and privacy measures, and security and privacy mechanisms, along with security and privacy threats. A graphical representation of the above mentioned concepts of the security reference diagram is depicted in Fig. 5.

Please note that although the graphical representation of security and privacy goals, the two can be differentiated by the prefix [S] or [P] before the goal description. The same is true for the graphical representation of security and privacy measures and Security and Privacy mechanisms. The above-mentioned nodes of the diagram are associated with the aid of two types of links: positive and negative contribution links. A positive contribution link associates two nodes when one node helps in the fulfilment of the other. Consider, for instance, a security measure that contributes positively to the satisfaction of a security objective. A negative contribution link, on the other hand, indicates that a node contributes towards the denial of another node. As an example, consider the contribution of a privacy threat to a privacy objective. As a result, in every security and privacy reference catalogue diagram, each security/privacy objective identified receives positive contributions from different measures and negative contributions from different threats. Graphically a positive contribution link is modelled as an arrow, which points towards the node that is satisfied, with a plus (+) whereas a negative contribution link is represented as an arrow with a minus (−).

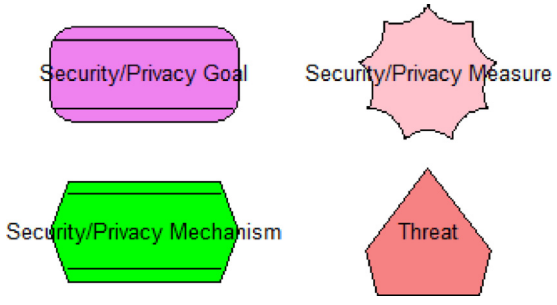

Fig. 5. Graphical representation of nodes used in the security and privacy reference diagram.

3.5.2. Security and privacy organisational diagram model

This diagram is the output of the define organisational context activity. The diagram is constructed using a defined set of concepts (actor, dependency, goal, constraint, plan, and resource), presented in the metamodel illustrated in the previous section. The construction of the diagram follows an iterative refinement-based process, where a higher level diagram is first developed that is constantly refined to better illustrate the organisational actors along with their goals, plans and resource and the relevant constraints. Although there are no specific rules on how the diagram can be constructed, i.e. which concepts need to be introduced first, second and so on in the diagram, a useful guidance is the following:

- Identify all actors with their high level goals.
- Identify those high level goals that the actors cannot achieve on their own and they depend on other actors.
- Define the dependencies for those goals.
- For each actor on the diagram, refine their goals in terms of sub-goals, plans and resources.
- Identify new dependencies if required (new sub-goals, plans, resources which the actor cannot achieve on their own) and model those new dependencies.
- Identify security and privacy goals and modelled those goals.

The above steps, follow an iterative process until a satisfactory diagram has been constructed. Fig. 6 illustrates the notation employed by the diagram.

3.5.3. Security and privacy system diagram

This diagram is the output of the define security and privacy concerns activity. It makes use of a defined set of concepts (actor, dependency, goal, constraint, measure, plan, protection mechanism, resource, threat, vulnerability), presented in the metamodel illustrated in the previous section. Similarly to the security and privacy organisational diagram an iterative process is followed. The security and privacy system diagram receives as input the analysis of the security and privacy organisational diagram and in particular the information related to the system actor of the previous diagram. As such the system actor, together with its goals, plans, resources and security and privacy goals represents the starting point for the security and privacy system diagram. Although it depends on the developers how the diagram will be constructed, we have found the following steps useful:

- Identify threats and vulnerabilities relate to the goals, plans and resources of the system actor based on the identified security and privacy goals.
- Introduce one or more security and privacy constraints for every threat and vulnerability in order to support the system's relevant security and privacy goals.
- Identify one or more security and privacy measures for every security and privacy constraints of the system actor.
- Identify one or more security and privacy plans for every security and privacy measures of the system actor.
- Analyse whether the system actor can operationalise all the identified security and privacy plans or if dependencies are required. In case dependencies are required, model those dependencies.

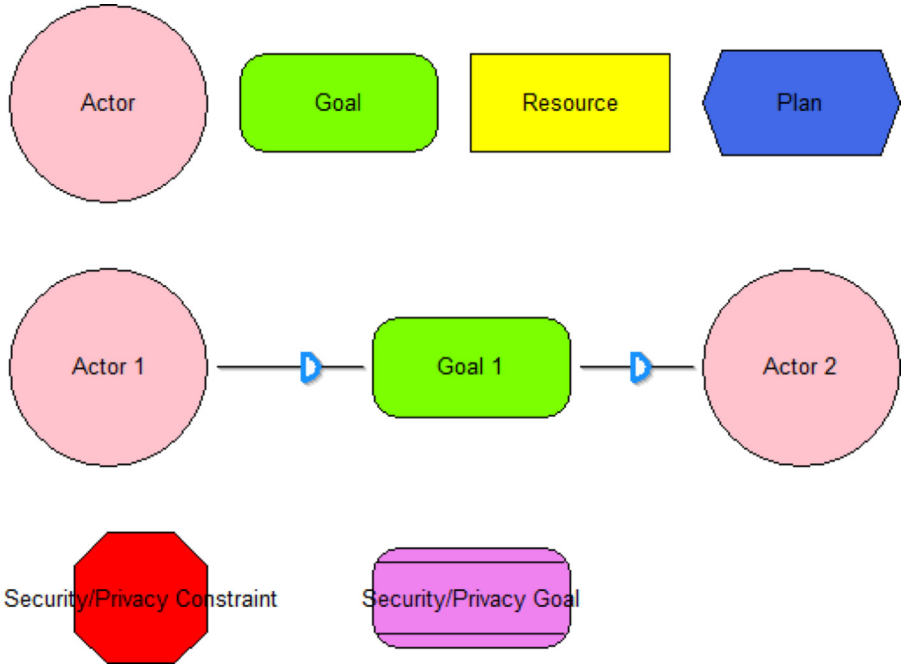

Fig. 6. Security and privacy organisational diagram notation.

- Introduce mechanisms to support the security and privacy plans identified in the previous step.
- Analyse whether the system actor can implement all the identified mechanisms, or if dependencies are required. In case dependencies are required model those dependencies.
- Fig. 7 illustrates the notation of the concepts used in the diagram.

3.5.4. Cloud provider selection diagram

The selection of cloud service provider activity results in a cloud provider selection diagram. The diagram makes use of a defined set of concepts (cloud actor, deployment model, service model, security and privacy mechanisms) from the metamodel illustrated in the previous section. The diagram also makes use of satisfiability

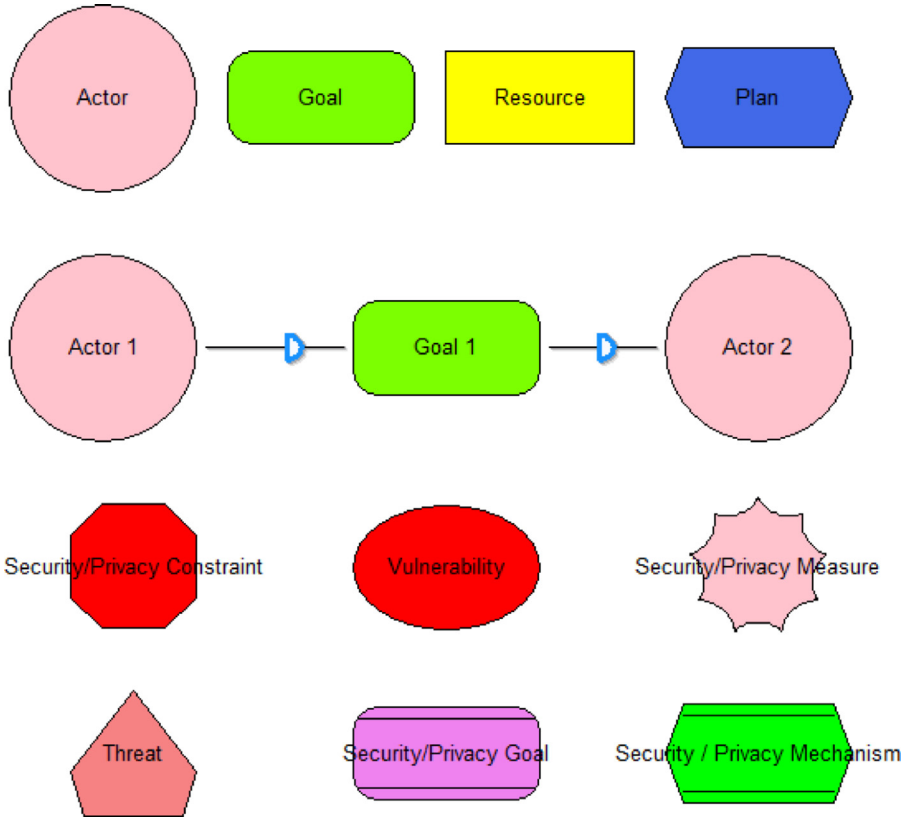

Fig. 7. Security and privacy system diagram notation.

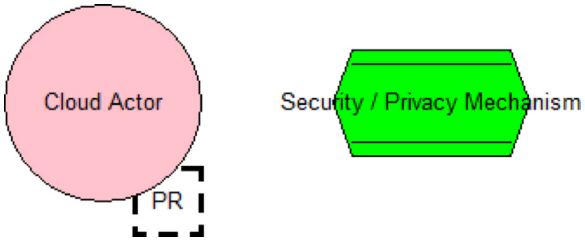

Fig. 8. Graphical representation of the service selection diagram nodes.

links to represent the satisfaction of the cloud actor to the relevant security and privacy mechanisms. It includes the following components: Security and Privacy mechanisms, service providers, satisfiability links, and satisfiability weights. A graphical representation of those concepts is shown in Fig. 8.

The construction of the diagram follows the following rules:

- First the security and privacy mechanisms are modelled on the top of the diagram. In case that a prioritisation of such mechanisms has taken place, the most "important" mechanisms are modelled on the left hand side of the diagram and the least "important" on the right hand side.
- Once the mechanisms have been modelled, cloud actors, representing cloud service providers, are modelled on the bottom of the diagram. Although there is no specific provision on how service providers should be depicted in terms of a sequence on the diagram, an alphabetical sequence is usually advised.
- For each cloud actor, relevant deployment and service models are identified.
- For each cloud actor, satisfiability links, together with the relevant satisfiability weights, are introduced for every mechanism modelled on the diagram.

4. Case study

To demonstrate the applicability of the proposed framework, we employ the proposed approach in a real-world case study based on the development of a cloud-based solution for the domain of electronic-point-of-sale (EPOS). The case study reported is part of a knowledge exchange project that took place between April and August 2012 between the School of Architecture, Computing and Engineering at the University of East London and a company specialising at the provision of EPOS solutions.[1] EPOS Ltd is a U.K. based company that provides both software (e.g. cash registers software, sales and stock analysis) and hardware (e.g. PC based cash registers, scanners, printers) solutions for EPOS. The aim of the project was to develop a cloud based solution that will enable the company to distribute its EPOS software over the cloud and also manage remotely issues such as licensing and maintenance. EPOS Ltd anticipates that a cloud-based solution will reduce their costs (especially maintenance costs), will attract more customers due to the flexibility that can be applied on licensing agreements, and improve their green credential. They also hope that they will be able to expand to different markets and utilise different (mobile) platforms to provide their customers an all-around solution. However, they recognise that security and privacy issues are very important in such scenario and they want to make sure that they have a good understanding of their security and privacy requirements and that they select a provider for their envisaged system that fulfils those requirements.

EPOS Ltd provides EPOS solutions to different types of clients, ranging from supermarkets to pubs to night clubs. Although the business objectives and aims of EPOS Ltd remain the same, irrespective of the type of client, the solutions provided are slightly different due to the unique characteristics that each type of client demonstrates. For the purposes of this paper, we focus on the application of our work to a scenario that involves a Night Club as a client.[2] Good Time Ltd operates a number of venues across the U.K., ranging from relatively small, in terms of EPOS, venues with 4 tills to rather large ones, with 30 tills. However, these tills are not all used on a daily basis. Most of these venues use all their tills during Fridays and Saturdays, while only use some of the tills during the rest of the week and they are closed on Sundays. EPOS Ltd aimed to develop a cloud based system that would enable Good Time Ltd venues to use EPOS software and pay licensing according to their true usage. In other words, EPOS Ltd aims to provide Software as a Service (SaaS) functionality to their clients. However, to be able to provide such service, EPOS Ltd requires the support of a cloud provider. As part of the project, using our framework, EPOS Ltd security and privacy requirements were elicited and analysed and a cloud provider was selected based on the EPOS Ltd requirements and the cloud provider characteristics that better matched those requirements. Such analysis is described in the following sections.

4.1. Security and privacy cataloguing

As discussed in the previous section, the main idea behind the security and privacy cataloguing and the construction of the security and privacy reference catalogue diagram is two-fold. On one hand, it allows a project team to create a reference point based on existing knowledge and previous experience, which can be used to save time and effort and transfer knowledge from one project member (e.g. security expert) to another (e.g. requirements engineer). On other hand, it supports a better understanding of the relationships between security and privacy goals, threats, security and privacy measures, and security and privacy mechanisms. This supports a clear common understanding of those concepts from all team members.

In the presented case study, EPOS Ltd had already developed a security document, where they had documented the main, according to their analysis, threats, security objectives and relevant security mechanisms. As such, it was decided not to construct a cataloguing diagram from scratch but to make use of the existing information. However, the security document that EPOS Ltd had constructed was a textual description of the relevant security issues. Therefore, the first step was to construct the security and privacy cataloguing diagram based on the EPOS Ltd security document. The output of that activity is shown in Fig. 9. It is worth mentioning that we decided not to make any changes to the security document even though there was limited consideration for privacy and some of the security analysis was different than what we expected.

4.2. Security and privacy analysis

As discussed in the previous section, the first part of this activity is to define the organisational context and in particular organisational goals, relevant actors, their plans, resources and security and privacy goals.

Focusing on our case study, we have identified five actors that are relevant to the case study presented in this paper as shown in Fig. 10. EPOS Ltd, Night Club Ltd, EPOS Software, Cashier, and Card Payment System. The main organisational goal for EPOS Ltd

[1] For confidentiality reasons we are not allowed to disclose the name of the company so we use the name "EPOS Ltd" to refer to it throughout the paper.

[2] Similarly to the EPOS Confidentiality agreement, we are not allowed to disclose the name of the Night Club, so we use the name Good Time Ltd.

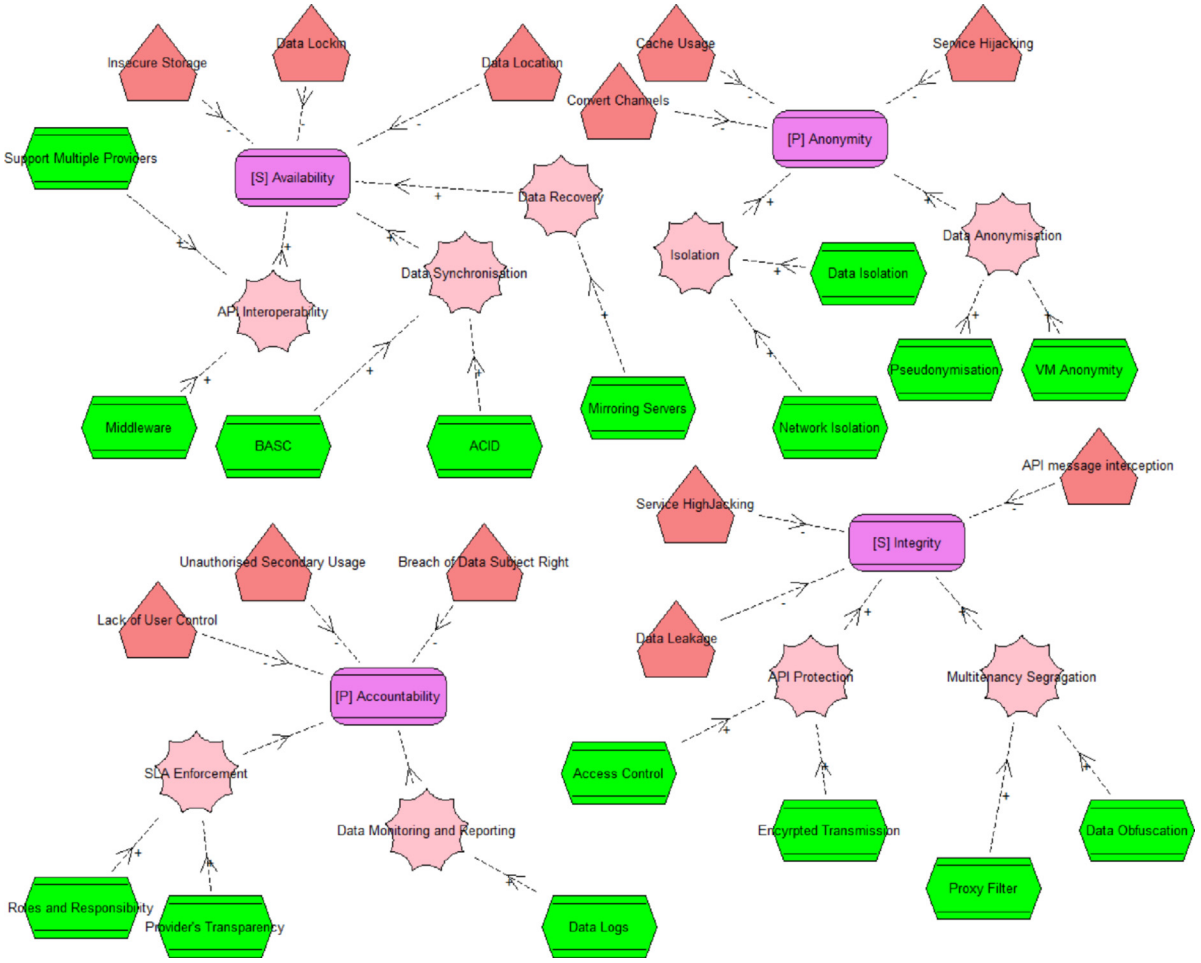

Fig. 9. Partial illustration of security and privacy catalogue reference diagram.

is to provide clients with EPOS infrastructure, as part of that Night Club Ltd depends on EPOS Ltd to *Manage Tills* and *Receive Licence*. In doing so, EPOS needs to *Provide Sales Management* and *Provide Licencing*, two goals for which EPOS Ltd depends on the EPOS Software. To achieve these dependency goals, EPOS Software has three main goals, *Manage Sales Transactions*, *Manage Licence* and *Manage Inventory*.

To Satisfy the achievement of the manage sales transaction goal, a number of sub-goals need to be satisfied such as *Log Sale*, *Record Sale Item*, *Manage Payment Type*, *Record Sale Quantity*, *Generate Receipt*, *Calculate Sale Price*. Some of these goals can be furthered refined to include relevant plans. For example, the manage payment type goal is decomposed to three plans, *Cash Payment*, *Voucher Payment*, and *Card Payment*. For the first two plans, the *EPOS Software* actor depends on the *Cashier* to record the cash and voucher transactions, while for the last plan the *EPOS Software* actor depends on the *Card Payment System* to authorise the card payment.

Once all the relevant actors, plans, resources and dependencies have been identified, relevant security and privacy goals are identified and modelled. Going back to the EPOS Ltd case study, a number of security (i.e. confidentiality, integrity and availability) and privacy (i.e. identification, unobservability, and unlikability) goals have been identified as shown in Fig. 10.

The next part of the process focuses on analysing the security and privacy needs for a cloud based EPOS Ltd provision. As shown in Fig. 11, EPOS Ltd depends on the Cloud Provider to *Provide EPOS Software as Service*, *Manage EPOS Software Licencing* and *Provide Cloud Services*.

In the rest of the section we focus on the analysis of one of these goals, i.e. *Provide EPOS Software as Service*. The first step involves identification of relevant threats to that goal. As discussed in the previous section, the security and privacy cataloguing can contribute to such identification. For example, threats such as Insecure APIs, Service Highjacking that have been identified in the catalogue reference diagram, are introduced to the Cloud Service Provider actor analysis. In the presented analysis, we consider two more threats Data Leakage and Lack of Transparency. On the other hand, our analysis identified a number of security constraints that restrict the *Provide EPOS Software as Service* goal of the *Cloud Provider* actor. To avoid lengthy discussions and to keep the paper to an acceptance level, we focus on two security constraints (Ensure Availability of Software, Ensure Data Confidentiality) and one privacy constraint (Ensure Data Residency). For each one of these security constraints, relevant security and privacy measures and mechanisms are identified. Again, from the reference catalogue, availability can be supported by data synchronisation and data recovery measures. These have been added to the analysis of the cloud service provider actor as shown in Fig. 11. Data synchronisation can be implemented by ACID (Atomicity, consistency, isolation, durability) properties mechanism or BASC (basically available, soft state, eventual consistency) properties mechanisms. Data recovery, on the other hand, can be implemented by mirroring services. Nevertheless, additional measures and resources are identified according to the case study. For example, in the EPOS Ltd case study, a number of measures and mechanisms were identified that were not catalogued in the reference diagram. For example, the Retain Sensitive Data

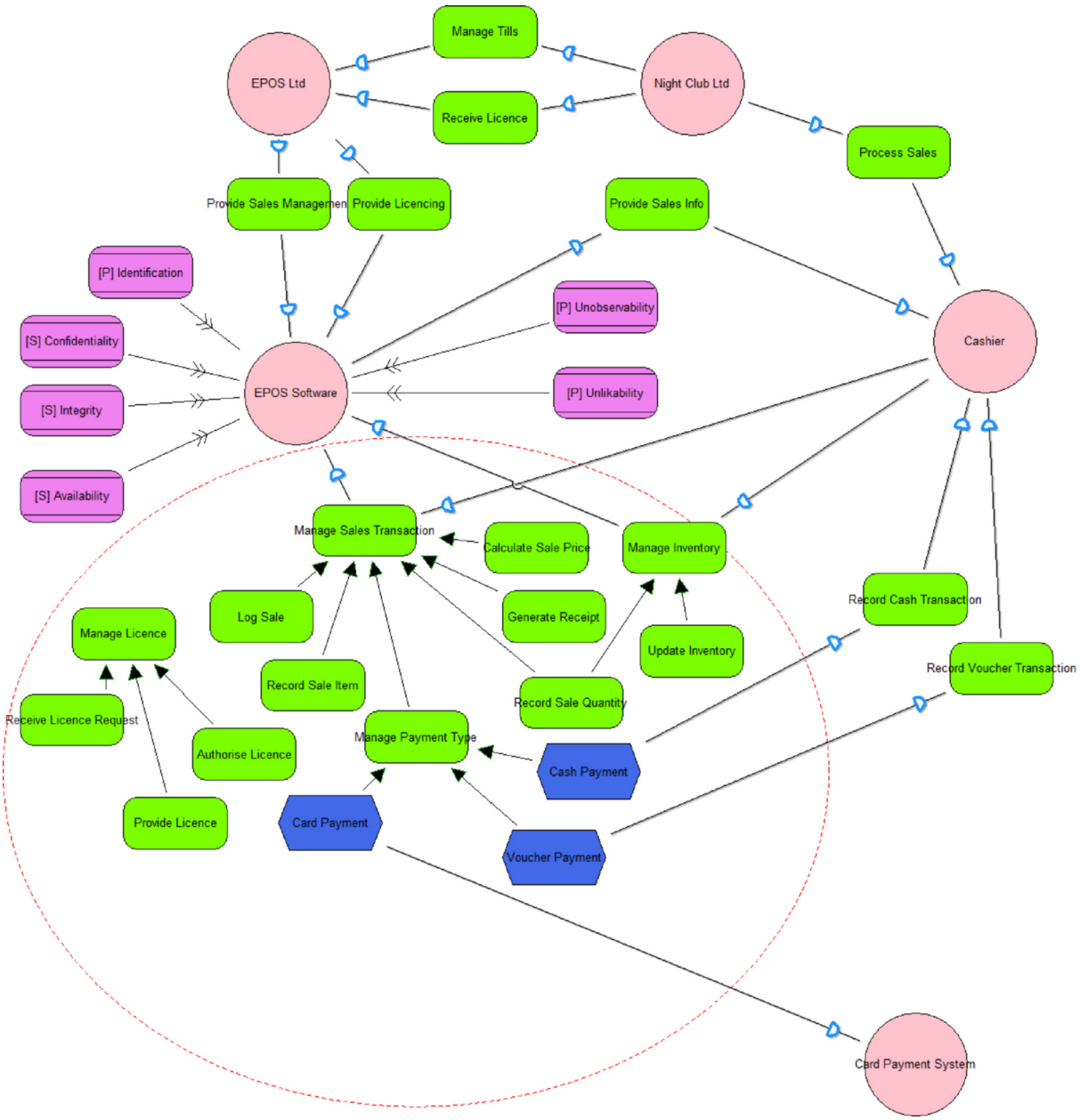

Fig. 10. Security and privacy organisational diagram.

measure can be employed to satisfy the Ensure Data Residency privacy constraints. Two relevant mechanisms have been identified that can implement that measure, i.e. data tokenisation and encryption. Relevant measures and mechanisms have been identified for all the security and privacy constraints as shown in Fig. 11.

4.3. Selection analysis

The next activity includes the selection of appropriate cloud service providers based on the security and privacy requirements identified in the previous step. In particular, as described in previous section, we evaluate how specific service providers satisfy the security and privacy mechanisms identified in the previous step. In particular, our analysis consisted of the evaluation of three cloud providers for different three different types of cloud deployments models, i.e. public, private and hybrid cloud. In this paper we focus our case study on the privacy model evaluation, since that model scored the most (i.e. overall score of all providers was higher for private than public or hybrid) in our analysis across all three providers.[3] Fig. 12 illustrates the relevant satisfability scores for each provider for 5 security and privacy mechanisms identified in the previous step. Following the steps of the selection activity, as described in previous section, for each of the providers an overall score is calculated as shown below:

$$CP1 = \frac{1 + 0.75 + 0.5 + 0.75 + 1}{5} = 0.8$$

$$CP2 = \frac{1 + 1 + 1 + 1 + 1 + 1}{5} = 1$$

$$CP3 = \frac{1 + 0.5 + 0.5 + 0.75 + 1}{5} = 0.75$$

[3] For confidentiality reasons, we are not able to reveal the true identities of the analysed cloud providers. We report however, the real satisfability scores.

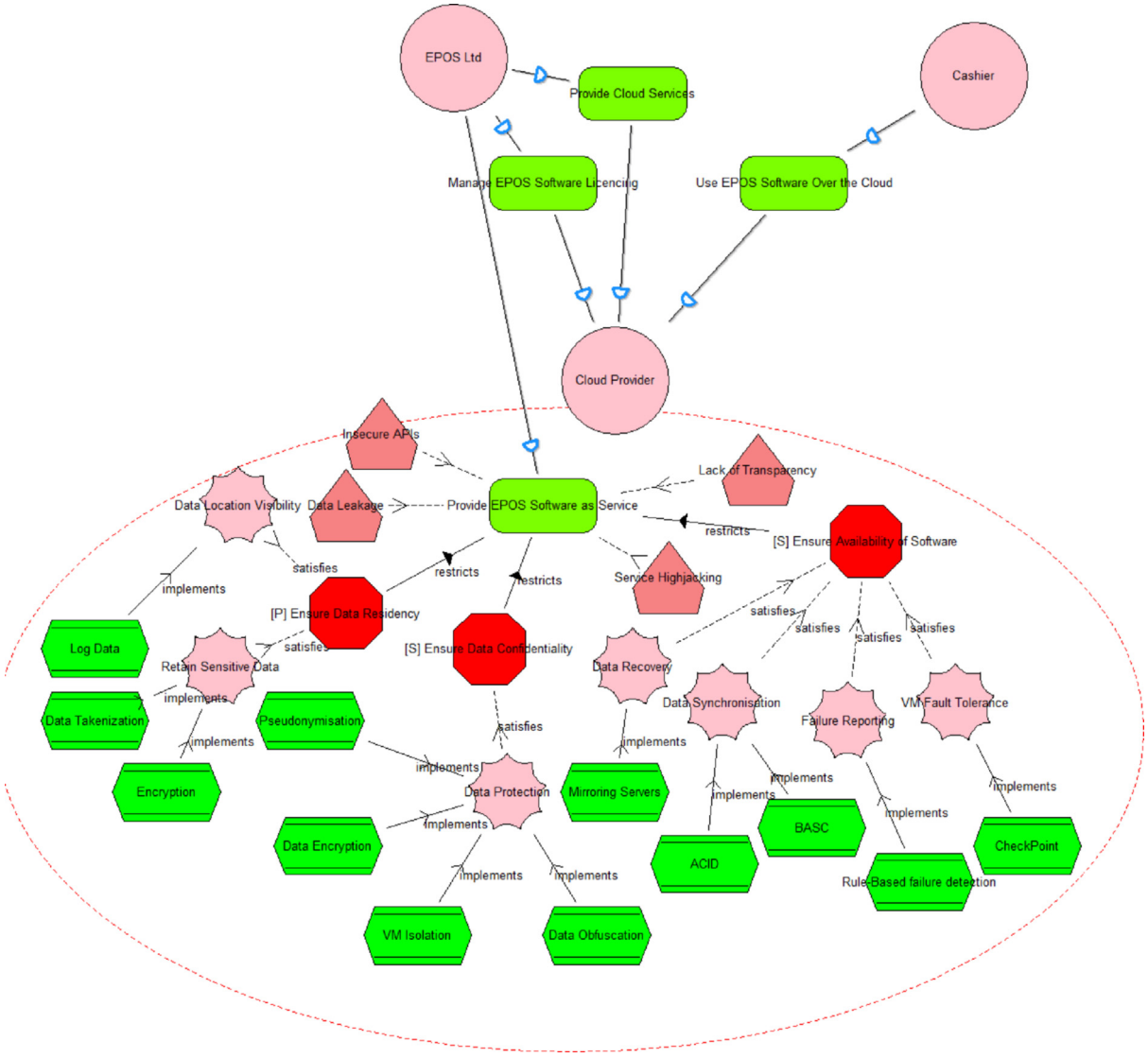

Fig. 11. Security and privacy system diagram.

The provider with the highest score, and therefore preferred, is provider 2.

5. Related work

This section discusses related work. In particular, we first discuss literature related to security and privacy requirements elicitation and analysis and then works that focus on security and privacy issues within the cloud computing domain.

5.1. Security and privacy requirements elicitation and analysis

The literature provides quite few examples of research that focus on the identification and analysis of security and privacy properties for the development of software systems.

Mouratidis and Giorgini (2007) propose Secure Tropos, an extension of the Tropos methodology. The approach is based on the concept of security constraint to analyse security requirements from the early stages of the development process. Similar to that work, Giorgini et al. (2003) have extended the i*/Tropos requirements engineering framework to deal with security requirements. Mellado et al. (2007) introduced the security requirements engineering process (SREP), which is based on several common criteria constructs, i.e., security functional components, protection profile, and security assurance components to elicit and analysis security requirements. The security quality requirement engineering methodology (SQUARE) is another security requirements engineering approach similar to SREP (Mead and Steheny, 2005). Both SREP and SQUARE are asset-based and risk-driven methods that follow a number of steps, for eliciting, categorising, and prioritising security requirements. However, SREP integrates knowledge and experience from the Common Criteria and Information Security Standards, such as ISO/IEC 27001, while eliciting security requirements. Sindre and Opdahl (2005) have developed a misuse case driven approach to establish visual link between use cases and misuse cases for eliciting security requirements at an early stage of the development. These links guide analysis of functional requirements against security requirements and the threat environment. Chung argues about a process-oriented approach to represent security requirements as potentially conflicting or harmonious goals (Chung, 1993). The proposed NFR (non-functional requirements) framework represents and uses security requirements as a class of non-functional requirements and it allows developers to

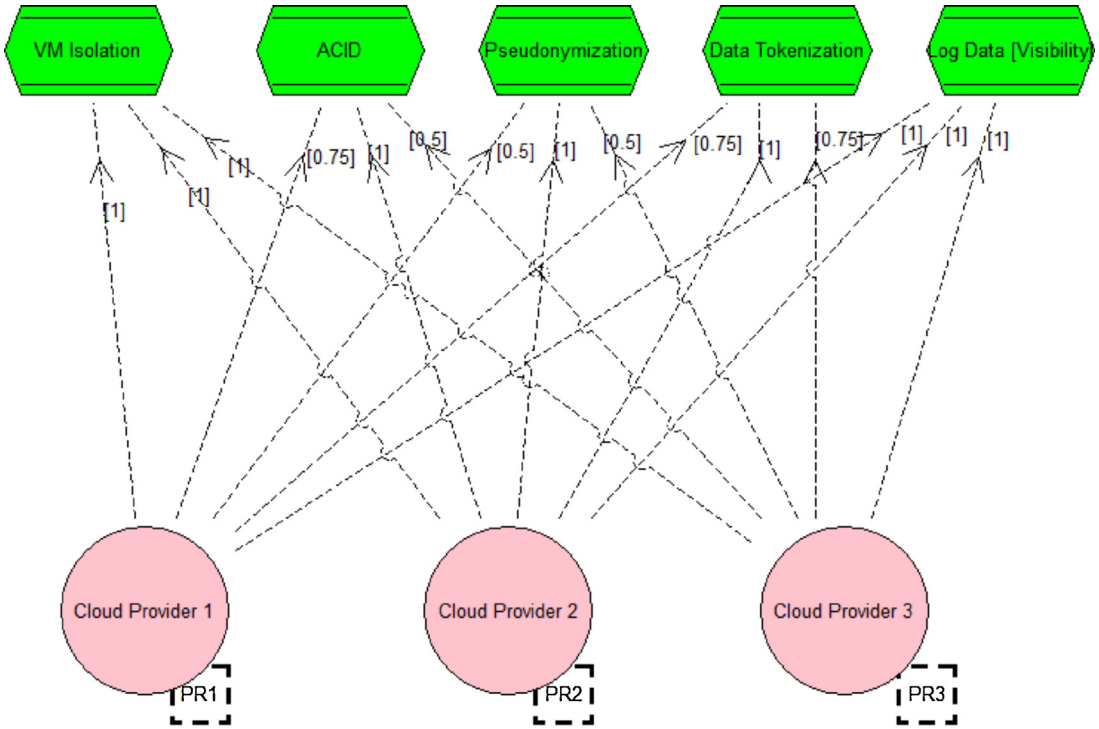

Fig. 12. Cloud provider selection diagram.

consider design decisions and relate these decisions to the represented non-functional requirements. On the other hand, prism provides a security risk management framework that is applicable to any organisational context (PRISM). It considers asset based risk management process based on strategic planning, asset environment to define risk and performance context. However the approach is mostly focused to national critical infrastructure. Houmb et al. (2010) introduce the SecReq approach to elicit, analyse and trace security requirements from the requirements engineering phase to design. Van Lamsweerde and Letier (2000) introduce the KAOS goal modelling language where goals are considered as satisfaction of a statement of intent, and obstacles are obstructions to the goals. KAOS introduces the concept of an anti-goal as the intention of an attacker to satisfy a malicious goal. These goals are finally refined as requirements, which are operationalised by agents. Pavlidis et al. (2012) use trust based concepts such as resolution, trust, trust relationship, and entailment to support analysis and modelling of security. Rosado et al. (2010) demonstrate an activity for elicitation, analysis and modelling of security and functional requirements (Rosado et al., 2010), where Security is considered as sub -factor of software quality. The work systematically uses SPEM 2.0 to define the tasks and integrate the artefacts for the security analysis.

On the other hand, the literature provides examples of works that focus on elicitation and analysis of privacy requirements. PriS is a requirements engineering method that incorporates privacy requirements early in the system development process (Kalloniatis et al., 2008). The approach considers privacy requirements as organisational goals that need to be satisfied and it adopts the use of privacy process patterns as a way to: (a) describe the effect of privacy requirements on business processes; and (b) facilitate the identification of the system architecture that best supports the privacy-related business processes. May et al. (2006) extract privacy requirements from legal text using access control techniques, while Islam et al. (2010, 2011) use natural language patterns with the Hohfeld legal taxonomy to extract security requirements from laws, combine them with the ISO/IEC policies and finally trace the identified requirements into a secure system design. Deng et al. (2011) present the LINDDUN methodology to elicit privacy requirements that consider both hard and soft privacy properties. Privacy threats are identified, categorised, and analysed through risk management methods. Finally privacy enhancing technologies are identified to address these threats. A goal based framework is presented by He and Antón (2003) for modelling privacy requirements. Organisational specific context and constraints are used to model the privacy requirements through goal based requirements engineering techniques. Legal texts are analysed using activity, purpose patterns and a set of rules to extract rights, obligations and constraints (Breaux and Antón, 2008). Rights and obligations are the actions that stakeholders are permitted and required to perform and in that work they are treated as requirements.

All of the above works, focus either on security or privacy. However, the literature provides a small number of works that consider both security and privacy. A model based process is proposed to support security and privacy requirements engineering using a set of concepts such as goal, actor, constraint, and threat (Islam et al., 2012a). Massey et al. (2010) proposed four methodological activities to evaluate existing security and privacy requirements for legal compliance. The approach in particular prioritises the requirements and establishes traceability links from requirements to legal texts. Bellotti and Sellen (1993) developed a framework for privacy-aware design in the field of ubiquitous computing. This framework proposes a procedure that designers may follow through a set of questions in order to evaluate a system. The evaluation is accomplished by identifying a set of new requirements, which must be implemented by the developers. A variation of this framework is proposed by Hong et al. (2004). In spite of the fact, that these frameworks are inexpensive to use and relatively fast to implement, a number of disadvantages exist. Firstly, they do not address/suggest any implementation techniques for realizing the identified requirements. A gap between design and implementation exists since they do not suggest a way for guiding the developer from the design to the implementation level.

5.2. Security and privacy issues in cloud computing

The literature is rich with research efforts that consider security and privacy issues within the context of cloud computing. Pearson and Benameur (2010) argued that privacy threats differ depending on the type of cloud scenario. They also argued that lack of user control, potential unauthorised secondary usage, and data proliferation are more dominate in public clouds. Gong et al. showed that using a side-channel attack, an attacker can instantiate new VMs of a target virtual machine so that the new VM can potentially monitor the cache hosted on the same physical machine (Gong et al., 2010). Grobauer et al. (2011) identified four possible places where faults can occur in cloud computing: provider-inner, provider-across, provider user and user-across. Mulazzani et al. (2011) showed that attackers can exploit data duplication techniques to access customer data by obtaining hash code of the stored file. An approach incorporates quality of service into cloud service level agreement (SLA); in particular the work measures QoS to predict availability, quantify risk, and consider liability in case of failure (Gillam et al., 2012). A goal-drivel approach is introduced to analyse security and privacy risks of cloud based system (Islam et al., 2012b). Goals, threats and risks are consider from three main components: data, service/application, and technical and organisational measure. Wenzel et al. (2012) consider security and compliance analysis of outsourcing services in the cloud computing context. The work initially considers risk analysis of business processes that are planned to be outsourced and if the process is outsourced then compliance issues are checked. The final part of the approach involves security analysis of the physical distribution of the process and communication among the entities. Khajeh-Hosseini et al. (2011) introduce cost and benefits and risk tool as decision support for public IaaS cloud migration. The cost modelling tool enables user to model IT infrastructure using UML. Risks are considered from organisational, legal, security, technical and financial perspectives. Khajeh-Hosseini et al. (2010) present a case study of an SME that migrates into the cloud. The result shows that despite of many benefits of cloud adaption, organisations should pay attention to socio-technical issues such as decrease job satisfaction, overall service quality, deterioration of customer care, and departmental downsizing.

The presented works provide solid contribution to the respected domain. However, they demonstrate a number of limitations. Some of the methods, such as Secure Tropos, SREP, SQUARE, and SEcReq, focus explicitly on security issues, while others, such as LINDDUN, focus on privacy issues. Most of the works related to security focus on the requirements stage. For instance, SREP and SQUARE follow a systematic process for elicitation and analysis of security requirements, KAOS focus on security analysis through anti-goal and obstacles. These works do not consider design issues that could realise the identified requirements. On the other hand, the methods that consider both security and privacy, treat privacy as a subset of security. Moreover, none of these works considers cloud computing. On the other hand, the works that have been developed based on the idea of cloud computing, mostly focus on implementation concerns related to security and privacy in the cloud, and they do not provide a methodology to support the elicitation and analysis of security and privacy requirements and the selection of an appropriate cloud provider based on such requirements.

The work presented here differs from these approaches in that the proposed framework provides explicit support for elicitation and analysis of security and privacy requirements within the context of cloud computing. To our knowledge based on the systematic literature review (as stated previously), there is no work in the literature that considers security and privacy issues at the requirements stage within the context of cloud computing. The closest effort to our work is the work presented by Zardari and Bahsoon (2011) on developing a requirements engineering methodology for the cloud, based on the goal-oriented requirements engineering (GORE) paradigm. We consider that work complimentary to our work, especially since we share the view that GORE represents an important paradigm for supporting software engineering activities for the cloud. However, our work has an important difference with that effort. It is focused on security and privacy requirements and it introduces a unified framework that supports the elicitation and selection of suitable service providers based on security and privacy requirements.

6. Conclusions

Despite the recent research interest in developing software engineering techniques to support systems based on the cloud, the literature fails to provide a systematic and structured approach that enables software engineers to identify security and privacy requirements and select a suitable cloud service provider based on such requirements. In this paper we have presented a novel framework that fills this gap by providing a process to support elicitation of security and privacy requirements and selection of a cloud service provider based on the satisfiability of the cloud provider to identified security and privacy mechanisms. Our framework supports understanding of the organisational context by identifying goals, actors, tasks, resources, and plans. Understanding the organisational context helps to identify and analyse security, privacy constraints, security and privacy goals, threats and vulnerabilities relevant to a cloud based system.

Through the application of our work to the real case study, we identified a number of limitations of our framework. First of all, threats, measures and mechanisms might be specific to one deployment or service model and not applicable or applicable in a different way to the other models. However, our framework does not allow for such differentiation. Moreover, our process does not indicate how the reference catalogue can be updated through information gained during a project. For instance, in the application of our work to the EPOS case study, a number of measures, mechanisms and threats were identified that were not modelled on the reference catalogue that was employed when we started the project.

Future work will focus on improving the framework with respect to the above limitations. Moreover, our efforts will focus on further extending the language to include concepts that are relevant to security and privacy, such as trust and also to include the ability to identify and select cloud providers based on legal constraints. We also envisage that we will extend the applicability of our framework to later stages of the development process, i.e. from requirements engineering that is currently applicable to design and implementation, where different issues need to be considered when selecting cloud service providers. Last but not least we aim to enhance the CASE tool used to support our framework.

References

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinsk, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M., 2010. Above the clouds: a berkeley view of cloud computing. Communications of the ACM 53 (4), 50–58.

Bellotti, V., Sellen, A., 1993. Design for privacy in ubiquitous computing environments. In: Michelis, G., Simone, C., Schmidt, Kjeld (Eds.), Proceedings of the Third European Conference on Computer Supported Cooperative Work (ECSCW), 930, pp. 93–108.

Bruening, P.J., Treacy, B.C., 2009. Cloud computing: privacy, security challenges, Bureau of Nat'l Affairs, www.hunton.com

Breaux, T.D., Antón, A.I., 2008. Analyzing regulator rules for privacy and security requirements. IEEE Transactions on Software Engineering 34 (1 (Jan–Feb)).

Cachin, C., Schunter, M., 2011. A cloud you can trust – how to ensure that cloud computing's problems—data breaches, leaks, service outages—don't obscure its virtues. In: IEEE Spektrum, 2011 December, pp. 28–51.

Chen, Y., Paxson, V., Katz, R.H., 2010. What's new about cloud computing security, technical report, Dept., Univ. of California, www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

Choo, K.R., 2010. Cloud computing: challenges and future directions, trends & issues in crime and criminal justice. Australian Institute of Criminology 400.
Chung, L., 1993. Dealing with security requirements during the development of information systems. In: 5th International Conference of Advanced Information Systems Engineering (CAiSe), Paris, France, pp. 234–251.
Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W., 2011. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering Journal 16 (1), 3–32.
Dawoud, W., Takouna, I., Meinel, C., 2010. Infrastructure as a service security: challenges and Solutions. In: Proceeding of the 7th International Conference on Informatics and Systems (INFOS). IEEE Computer Society.
Erdogmus, H., 2009. Cloud computing: does nirvana hide behind the nebula? IEEE Software 26 (2), 4–6.
Ferretti, S., Ghini, V., Panzieri, F., Pellegrini, M., Turrini, E., 2010. QoS–aware Clouds. In: Proceeding of 3rd IEEE International Conference on Cloud Computing.
Gellman, R., 2009. Privacy in the clouds: risks to privacy and confidentiality from cloud computing. http://www.worldprivacyforum.org/pdf/WPFCloud_Privacy_Report.pdf
Giorgini, P., Mylopoulos, J., Nicchiarelli, E., Sebastiani, R., 2002. Reasoning with goal models. In: Proceedings of the 21st International Conference on Conceptual Modeling (ER), Tampere, Finland, October.
Gong, C., Liu, J., Zhang, Q., Chen, H., Gong, Z., 2010. The characteristics of cloud computing. In: Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, IEEE Computer Society, Washington, DC, USA.
Grobauer, B., Walloschek, T., Stocker, E., 2011. Understanding cloud computing vulnerabilities. IEEE Security & Privacy Magazine 9 (2), 50–57.
Giorgini, P., Massacci, F., Mylopoulos, J., 2003. Requirement engineering meets security: a case study on modelling secure electronic transactions by VISA and Mastercard. In: 22nd International Conference On Conceptual Modeling (ER 2003), vol. 2813 of Lecture Notes in Computer Science, Springer, pp. 263–276.
Gillam, L., Li, B., O'Loughlin, J.,2012. Adding cloud performance to service level agreements. In: 2nd International Conference on Cloud Computing and Services Science (CLOSER). SciTePress, Portugal.
Hong, J.I., Ng, D., J Lederer, S., Landay, J.A., 2004. Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems. Designing Interactive Systems, Boston, MA.
He, Q., Antón, A.I., 2003. A framework for modelling privacy requirements in role engineering. In: Proceedings of the 9th International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'03), Austria, 2003.
Houmb, S.H., Islam, S., Knauss, E., Jürjens, J., Schneider, K., 2010. Eliciting security requirements and tracing them to design: an integration of common criteria, heuristics, and UMLsec. Requirements Engineering Journal 15 (1 (Mar)), 63–93.
Islam, S., Dong, W.,2008. Human factors in software security risk management. In: Proceedings of the First International Workshop on Leadership and Management in Software Architecture (LMSA). ACM, New York, NY, USA, pp. 13–16.
Islam, S., Mouratidis, H., Wagner, S., 2010. Toward a framework to elicit and manage security and privacy requirements from laws and regulation. In: Proceeding of Requirements Engineering: Foundation for Software Quality (REFSQ), Lecture Notes in Computer Science, vol. 6182/2010, pp. 255–261.
Islam, S., Mouratidis, H., Jürjens, J., 2011. A framework to support alignment of secure software engineering with legal regulations. Journal of Software and Systems Modelling (SoSyM) 10 (3), 369–394.
Islam, S., Mouratidis, H., Kalloniatis, C., Hudic, A., Zechner, L., 2012a. Model based process to support security and privacy requirements engineering. International Journal of Secure Software Engineering (IJSSE) 3 (3).
Islam, S., Mouratidis, H., Weippl, E., 2012b. A goal-driven risk management approach to support security and privacy analysis of cloud-based system. In: Security Engineering for Cloud Computing: Approaches and Tools. IGI Global Publication, United States of America by (an imprint of IGI Global) 701 E. Chocolate Avenue, Hershey, PA 17033.
Khajeh-Hosseini, A., Sommerville, I., Bogaerts, J., Teregowda, P., 2011. Decision support tools for cloud migration in the enterprise. In: Proceeding of IEEE 4th International Conference on Cloud Computing, IEEE Computer Society.
Khajeh-Hosseini, A., Greenwood, D., Sommerville, I., 2010. Cloud migration: a case study of migrating an enterprise IT system to IaaS. In: Proceeding of IEEE 3rd International Conference on Cloud Computing, IEEE Computer Society.
Kalloniatis, C., Kavakli, E., Gritzalis, S., 2008. Addressing privacy requirements in system design: the PriS method. Requirements Engineering Journal 13 (3), 241–255.
Kolp, M., Giorgini, P., Mylopoulos, J., 2001. A goal-based organizational perspective on multi-agent architectures. In: Proceedings of the 8th International Workshop on Agent Theories, Architectures, and Languages (ATAL-2001), Seattle, USA.
Kitchenham, B., Charters, S., 2007. Guidelines for Performing Systematic Literature Reviews in Software Engineering, Version 2.3. EBSE Technical Report. University of Keele and Durham University.
Massey, A.K., Otto, P.N., Hayward, L.J., Antón, A.I., 2010. Evaluating existing security and privacy requirements for legal compliance. Requirements Engineering Journal 15 (1).
Mouratidis, H., 2004. A security oriented approach in the development of multiagent systems: applied to the management of the health and social care needs of older people in England. PhD Thesis, University of Sheffield.
Mouratidis, H., Giorgini, P., 2007. Secure tropos: a security-oriented extension of the tropos methodology. International Journal of Software Engineering and Knowledge Engineering 17 (2), 285–309.
May, M.J., Gunter, C.A., Lee, I., 2006. Privacy APIs: access control techniques to analyse and verify legal privacy policies. In: Proceedings of the 19th Computer Security Foundations Workshop, July.
Mead, N.R., Steheny, T., 2005. Security quality requirements engineering (SQUARE) methodology. SIGSOFT Software Engineering Notes 30 (4), 1–7.
Mellado, D., Fernández-Medina, E., Piattini, M., 2007. A common criterion based security requirements engineering process for the development of secure information system. Computer Standard and Interfaces 29, 244–253.
Mulazzani, M., Schrittwieser, S., Leithner, M., Huber, M., Weippl, E., 2011. Dark clouds on the horizon: using cloud storage as attack vector and online slack space. In: Proceedings of Usenix Security.
OMG Software & Systems Process Engineering Meta-Model Specification v.2.0. 2008. http://www.omg.org/spec/SPEM
Pavlidis, M., Mouratidis, H., Islam, S., 2012. Modelling security using trust based concepts. International Journal of Secure Software Engineering 3 (2).
Pearson, S., Benameur, A., 2010. Privacy, Security and Trust Issues Arising from Cloud Computing. In: 2nd IEEE International Conference on Cloud Computing Technology and Science, IEEE Computer Society. PRISM, UK, pp. 693–702 http://www.prismworld.org/en/what-is-prism/what-does-it-deliver
Rosado, D.G., Fernández-Medina, E., López, J., Piattini, M., 2010. Analysis of secure mobile grid systems: a systematic approach. Information & Software Technology 52 (5), 517–536.
Rosado, D.G., Gomez, R., Mellado, D., Fernández-Medina, E., 2012. Security analysis in the migration to cloud environments. Future Internet 4 (2).
Rosenberg, J., Mateos, A., 2011. The Cloud at Your Service. Manning Publication, Shelter Island, NY.
Subashini, S., Kavitha, V., 2011. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34 (1).
Sindre, G., Opdahl, A.L., 2005. Eliciting security requirements with misuse cases. Requirements Engineering Journal 10 (1), 34–44.
Sriram, I., Khajeh-Hosseini, A., 2010. Research Agenda in Cloud Technologies, CoRR, CoRR abs/1001.3259:(2010).
Takabi, H., Joshi, J., Ahn, G., 2010. Security and privacy challenges in cloud computing environments. In: IEEE Computer And Reliability Societies, November/December, IEEE Computer Society.
Cloud Threat. 2010. Top Threats to Cloud Computing Vr. 1.0, Cloud Security Alliance, https://cloudsecurityalliance.org/research/top-threats/
Van Lamsweerde, A., Letier, E., 2000. Handling obstacles in goal-oriented requirements engineering. IEEE Transactions on Software Engineering 26, 978–1005.
Wenzel, S., Wessel, C., Humberg, T., Jürjens, J.,2012. Securing processes for outsourcing into the cloud. In: 2nd International Conference on Cloud Computing and Services Science. SciTePress.
Yu, E., 1995. Modelling strategic relationships for process reengineering. Ph.D. thesis, Department of Computer Science, University of Toronto, Canada.
Zardari, S., Bahsoon, R.,2011. Cloud adoption: a goal-oriented requirements engineering approach. In: Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing (SECLOUD 2011). ACM, New York, NY, USA, pp. 29–35.