

EXTENSION SPECIFICATION

***A framework to support selection of cloud providers based
on security and privacy requirements (Revisited)***

Researchers: <i>Enyo Gonçalves</i>
Email: ejtg@cin.ufpe.br

Summary

1	ANALYSE THE NEED FOR EXTENSION PROPOSAL.....	3
1.1	Study a domain/application area	3
1.2	Identify the concepts to be introduced by the extension	4
1.3	Model an example with the identified concepts using iStar	5
1.4	Search if there is an extensions related to the new proposal in iStar extensions catalogue	6
2	CONCEPTUALISE THE ISTAR EXTENSION.....	7
2.1	Search and select constructs to be reused.	7
2.2	Define extension's concepts	8
2.3	Analyse how the extension constructs can be integrated with the iStar constructs .	11
3	DEVELOP ISTAR EXTENSION.....	12
3.1	Define metamodel of extension	12
3.2	Define validation rules of extension	12
3.3	Define concrete syntax of extension.....	13
3.4	Check completeness, consistency and conflicts	14
3.5	Apply the extension to a modelling tool	16
4	EVALUATE AND VALIDATE ISTAR EXTENSION.....	16
4.1	Use the iStar extension proposed to model a system	16
4.2	Evaluate the iStar extension	17

PRESENTATION OF THE ISTAR EXTENSION: A framework to support selection of cloud providers based on security and privacy requirements (Revisited)

This document specifies the following iStar extension: A framework to support selection of cloud providers based on security and privacy requirements (Revisited). The list of constructs included, their descriptions and representations are presented following. The metamodel is also presented.

A general description should be introduced here to present an overview of the iStar extension proposed. The iStar extension metamodel should be presented and described here.

We selected the iStar extension Mouratidis, H., Islam, S., Kalloniatis, C., Gritzalis, S. A framework to support selection of cloud providers based on security and privacy requirements." Journal of Systems and Software 86.9 (2013): 2276-2293. It was choice because it has conflict, incompatibility between syntaxes, partially defines the extension and it did not consider part of iStar nodes and links.

1 Analyse The Need For Extension Proposal

1.1 Study a domain/application area

It was not necessary contact experts in domain/application area in this task. We just did a survey of the article references, which are probably what the author used to extract the concepts added by the extension. The following list of references follows:

ID_reference	Reference
REF_SPCP1	Bruening, P.J., Treacy, B.C., 2009. Cloud computing: privacy, security challenges, Bureau of Nat'l Affairs, www.hunton.com
REF_SPCP2	Cloud Threat. 2010. Top Threats to Cloud Computing Vr. 1.0, Cloud Security Alliance, https://cloudsecurityalliance.org/research/top-threats/
REF_SPCP3	Erdogmus, H., 2009. Cloud computing: does nirvana hide behind the nebula? IEEE Software 26 (2), 4–6.
REF_SPCP4	Grobauer, B., Walloschek, T., Stocker, E., 2011. Understanding cloud computing vulnerabilities. IEEE Security & Privacy Magazine 9 (2), 50–57.
REF_SPCP5	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.
REF_SPCP6	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.
REF_SPCP7	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. - Restrictions
REF_SPCP8	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.
REF_SPCP9	Rosado, D.G., Gomez, R., Mellado, D., Fernández-Medina, E., 2012. Security analysis in the migration to cloud environments. Future Internet 4 (2).
REF_SPCP10	Sriram, I., Khajeh-Hosseini, A., 2010. Research Agenda in Cloud Technologies, CoRR, CoRR abs/1001.3259:(2010)
REF_SPCP11	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.
REF_SPCP12	Mouratidis, Haralambos, and Paolo Giorgini. Secure tropos: a security-oriented extension of the tropos methodology. International Journal of Software Engineering and Knowledge Engineering 17.02 (2007): 285-309.

1.2 Identify the concepts to be introduced by the extension

We identified 17 concepts to be introduced by the extension, being 11 nodes and 6 links. Some concepts are an entity's specializations for security and privacy as a security and privacy measure.

ID_concept	Name of the Concept	Reference
<i>Nodes</i>		
CON_DEC_01	Security goal	REF_SPCP5
CON_DEC_02	Privacy goal	REF_SPCP5
CON_DEC_03	Security Measure	REF_SPCP5, REF_SPCP10
CON_DEC_04	Privacy Measure	REF_SPCP5, REF_SPCP10
CON_DEC_05	Security Mechanism	REF_SPCP9, REF_SPCP10
CON_DEC_06	Privacy Mechanism	REF_SPCP9, REF_SPCP10
CON_DEC_07	Security Constraint	REF_SPCP5, REF_SPCP12
CON_DEC_08	Privacy Constraint	REF_SPCP5, REF_SPCP12
CON_DEC_09	Cloud Actor	REF_SPCP5, REF_SPCP9
CON_DEC_10	Threat	REF_SPCP2, REF_SPCP10
CON_DEC_11	Vulnerability	REF_SPCP2, REF_SPCP4, REF_SPCP10
<i>Links</i>		
CON_DEC_12	Implements	REF_SPCP9

CON_DEC_13	Satisfies	REF_SPCP9
CON_DEC_14	Restricts	REF_SPCP9
CON_DEC_15	Satisfaction	REF_SPCP9

1.3 Model an example with the identified concepts using iStar

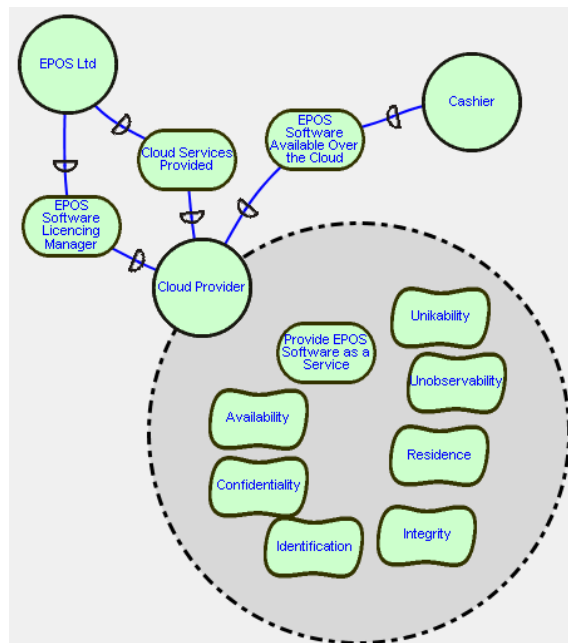
We did not have any doubts about the domain/application area, so we did not contact these experts. However, we were in doubt if it was possible to model some concepts, such as security goals and privacy goals, with the iStar without doing the extension. Consequently, we tried to model part of the example presented in the original proposal of this extension and wrote some observations.

The main goal of this task is to try identifying the domain concepts which is possible to represent with iStar without creating new representations and what is not possible to identify with iStar.

EPOS is the reduced form of the company Electronic Point Of Sales. We have identified three actors that are relevant to this example: EPOS Ltd, EPOS Software and Cashier. The EPOS Ltd depends on cloud services be provided and EPOS software Licencing is managed. The Cashier depends the EPOS software be available.

In doing so, the Cloud actor has the goal of Provide EPOS Software as a service and ensure the Data confidentiality, Data residence and Availability of Software. Furthermore, the security and privacy properties of Availability, Confidentiality, Identification, Integrity, Residence, Unobservability and Unikability are required to this actor.

The partial modelling of the System follows below. Then follows the report of the experience of how to model the system.



1.1.1 Observations

The Security and Privacy goals should be specializations of softgoal (Quality). Quality restrictions were modeled when trying to use iStar without the extension as softgoal, since they were linked to characteristics such as confidentiality and availability, for example. Difficulty in modeling threats,

measure and relationships. The modeling of direct dependence linking EPOS Ltd to the objective Provide EPOS as Service is not possible in iStar, it lacks dependum. Although vulnerability has been inserted into the actual syntax of the extension, it has not been used in the examples. I felt the need to specialise the actors that represent cloud actor, I believe that the property indicated by the researcher is ok. I consider that Security / Privacy Mechanism should not specialise task, since the description of these mechanisms are not similar to tasks (see the example of ACID mechanisms, Log data and checkPoint ... I do not see them as being a type of task). Modelling relationships is necessary as a specialization of the contribution relationship. The modelling of security and privacy objectives is necessary to be done through a textual mark, however these should be softgoals (Qualities). Is there a need to create a relationship between these properties and the cloud actor? I consider that only adding inside the boundary makes it part of the cloud ...

There is need to extend.

1.4 Search if there is an extensions related to the new proposal in iStar extensions catalogue

It was searched in the repository for some terms and some extensions were found. As we are revisiting an existing iStar extension, we added the year to publication to identify the papers published after the extension selected. The list is presented following.

Search Term	Extensions	Year
Cloud	A framework to support selection of cloud providers based on security and privacy requirements	2013
	Security Requirements Engineering for Cloud Computing: The Secure Tropos Approach	2016
Security	A framework to support selection of cloud providers based on security and privacy requirements	2013
	A vulnerability-centric requirements engineering framework: analysing security attacks, countermeasures, and requirements based on vulnerabilities	2010
	Improving Risk-Based Security Analysis with i*	2011
	Integrating Security Patterns with Security Requirements Analysis Using Contextual Goal Models	2014
	Model Based Process to Support Security and Privacy Requirements Engineering	2012
	Modelling security requirements through ownership,	2005

	permission and delegation	
	Secure Tropos: A Security-Oriented Extension of the Tropos Methodology	2007
	Security and privacy requirements analysis within a social setting	2003
	Security and Trust Requirements Engineering	2005
	Security Requirements Engineering for Cloud Computing: The Secure Tropos Approach	2016
	Security requirements engineering via commitments	2011
Privacy	A framework to support selection of cloud providers based on security and privacy requirements	2013
	Model Based Process to Support Security and Privacy Requirements Engineering	2012
	Privacy-Aware Trust Negotiation	2016
	Security and privacy requirements analysis within a social setting	2003
Service	A new service-based approach for enterprise modelling	2013
	Considering Technology Representation in Service-Oriented Business Models	2011
	Exploring Web Services from a Business Value Perspective	2005
	Modelling and Reasoning about Service-Oriented Applications via Goals and Commitments	2010

I have not considered the paper itself and papers after 2013 at this stage. Thus, we can conclude that, excluding these articles, there is no extension proposed for this purpose.

For the next process gateways the flow is: To Is there an extension suitable for your need? - Is not the extension related to a domain / application area? - Y. Thus, activity 1.2. Study a domain / application area is started.

2 Conceptualise the iStar extension

2.1 Search and select constructs to be reused.

The list of found constructors is shown below:

ID_concept	Name of the Concept	Reference of Extension to be reused
<i>Nodes</i>		
CON_DEC_01	Security goal	Integrating Security Patterns with Security Requirements Analysis Using Contextual Goal Models
CON_DEC_07	Security Constraints	Secure Tropos framework for software product lines requirements engineering
CON_DEC_10	Threat	Model Based Process to Support Security and Privacy Requirements Engineering
CON_DEC_11	Vulnerability	Há duas possibilidades: A vulnerability-centric requirements engineering framework: analyzing security attacks, countermeasures, and requirements based on vulnerabilities Improving Risk-Based Security Analysis with i*
<i>Links</i>		
CON_DEC_15	Satisfaction	Secure Tropos framework for software product lines requirements engineering

We found some constructors with the name of measurement, but they are not conceptually equivalent to the measurement to be added by the extension. I believe he reused the existing threat representation as a basis, however, withdrew the textual markup (s).

2.2 Define extension's concepts

The definition of the extension's concepts is presented in following table.

ID_concept	Name of the Concept	Definition	Reference
<i>Nodes</i>			
CON_DEC_01	Security goal	The main focus of security goals is to ensure critical security properties such as confidentiality, integrity, availability, authenticity, and non-repudiation as well as the privacy goals within the overall system environment. They are classified based on a	REF_SPCP5

		privacy taxonomy.	
CON_DEC_02	Privacy goal	It defines the goals of the privacy legislation. It is based in a taxonomy proposed by Hohfeld.	REF_SPCP5
CON_DEC_03	Security Measure	It is a measure to ensure security protection.	REF_SPCP5
CON_DEC_04	Privacy Measure	It is a measure to ensure privacy protection and to protect from any accidental and unlawful activities.	REF_SPCP5
CON_DEC_05	Security Mechanism	They are the most appropriate mechanisms used to implement certain security services for the Cloud	REF_SPCP9
CON_DEC_06	Privacy Mechanism	They are the most appropriate mechanisms used to implement certain privacy services for the Cloud	REF_SPCP9
CON_DEC_07	Security Constraint	Constraints can represent a set of restrictions that do not permit specific actions to be taken or prevent certain objectives from being achieved and more often are integrated in the specification of existing textual descriptions. This concept is related to constraints of security	REF_SPCP12
CON_DEC_08	Privacy Constraint	Constraints can represent a set of	REF_SPCP12

		restrictions that do not permit specific actions to be taken or prevent certain objectives from being achieved and more often are integrated in the specification of existing textual descriptions. This concept is related to constraints of security	
CON_DEC_09	Cloud Actor	It is a concept to represent the providers of cloud services	-
CON_DEC_10	Threat	A loss event occurs when a vulnerability is successfully exploited.	REF_SPCP4
CON_DEC_11	Vulnerability	Vulnerability is a prominent factor of risk. ISO 27005 defines risk as “the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization,” measuring it in terms of both the likelihood of an event and its consequence	REF_SPCP4
Links			
CON_DEC_12	Implements	Relationships between mechanism and measure, where a mechanism implements a measure	REF_SPCP9
CON_DEC_13	Satisfies	Relationships between measures and constraints, where a measure satisfies a constraint	REF_SPCP9

CON_DEC_14	Restricts	A constraint restricts a goal	REF_SPCP9
CON_DEC_15	Satisfaction	Relationships between security goals or privacy goals and cloud providers, where a goal satisfies cloud provider	REF_SPCP9

2.3 Analyse how the extension constructs can be integrated with the iStar constructs

We tried to relate the concepts to be introduced with the iStar standard concepts. So, we concluded that we could specialise six iStar constructs. Cloud Actor represents companies which provide cloud services, so it is a kind of Actor. Security and privacy goals are kinds of goal. Finally, Satisfies, Restricts and Implements are similar to values help, make, break and hurt which add information about the kind of contribution established between two intentional elements. The list of the relation between extension and iStar constructs is given in Table VI.

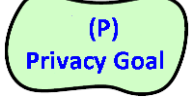
Measure and Constraint can be represented as a kind of Intentional elements. The Other constructs to be introduced by this extension (Threat, Vulnerability and Satisfaction) are represented with new metaclasses without specialising iStar nodes or links and they are not intentional elements.

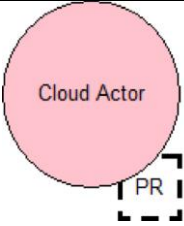
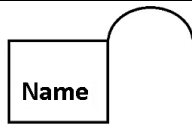
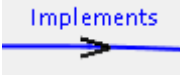
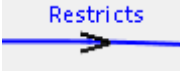
ID_concept	Name of the Concept	Relation with iStar constructs
Nodes		
CON_DEC_09	Cloud Actor	<i>Specialises Actor</i>
CON_DEC_05 and CON_DEC_06	Mechanism	<i>Specialises Task</i>
CON_DEC_07 CON_DEC_08	Security and Privacy goal	<i>Specialises Softgoal (Quality)</i>
Links		
CON_DEC_12 CON_DEC_13 CON_DEC_14	Implements, Satisfies and restricts specialise Contribution link.	Specialise Contribution link

3.1 Define metamodel of extension

3.3 Define concrete syntax of extension

The representations of extension's constructs are presented in next table. We used the iStar extensions catalogue to identify the representation of reused constructs. We considered the results of prioritization experiment to help the choice of vulnerability representation, once there were two representations. We proposed a new graphical representation to measure and specialised some iStar constructs with textual representation. The results are presented in table following.

ID_concept	Name of the Concept	Representation	Explanation about the graphical representation	Reused?
<i>Nodes</i>				
CON_DEC_01	Security goal		The Quality was specialised to represent security goals.	Yes
CON_DEC_02	Privacy goal		The Quality was specialised to represent privacy goals.	No
CON_DEC_03	Security Measure		The Figure was proposed as a polygon with many concavities to represent the measurement. The security is represented with (S) to differentiate of privacy.	No
CON_DEC_04	Privacy Measure		The Figure was proposed as a polygon with many concavities to represent the measurement. The privacy is represented with (P) to differentiate of privacy.	No
CON_DEC_05	Security Mechanism		Task was specialised to represent Security Mechanism.	No
CON_DEC_06	Privacy Mechanism		Task was specialised to represent Privacy Mechanism	No
CON_DEC_07	Security Constraint		Constraint of secure tropos was reused	Yes
CON_DEC_08	Privacy Constraint		Constraint of secure tropos was reused	Yes

CON_DEC_09	Cloud Actor		Actor was specialised to represent Cloud Actor. PR represents provider.	No
CON_DEC_10	Threat		It is a pentagon that represents the tip of a spear. The color purple was used also to represent the threat.	Yes
CON_DEC_11	Vulnerability		It was represented as square with an arch (such as a padlock opened) to represent the <i>Vulnerability</i> .	No
Links				
CON_DEC_12	Implements		We added a label to contribution link to represent implements relationship	No
CON_DEC_13	Satisfies		We added a label to contribution link to represent satisfies relationship	No
CON_DEC_14	Restricts		We added a label to contribution link to represent Restricts relationship	No
CON_DEC_15	Satisfaction		It represents the satisfaction relationship by the representation of the text ok from the <i>Quality</i> satisfied to the <i>Cloud Actor</i> .	No

3.4 Check completeness, consistency and conflicts

Completeness

Which level the iStar extension was applied

☒ [X] Concepts definition ☒ [X] Metamodel ☐ [] Well-formedness rules (optional) ☒ [X] Concrete syntax

Consistency

List following the concepts in each level			
Concept	Concept's definition	Metamodel	Concrete syntax
Security goal	[X]	[X]	[X]
Privacy goal	[X]	[X]	[X]
Security Measure	[X]	[X]	[X]
Privacy Measure	[X]	[X]	[X]
Security Mechanism	[X]	[X]	[X]
Privacy Mechanism	[X]	[X]	[X]
Security Constraint	[X]	[X]	[X]
Privacy Constraint	[X]	[X]	[X]
Cloud Provider Actor	[X]	[X]	[X]
Threat	[X]	[X]	[X]
Implements	[X]	[X]	[X]
Satisfies	[X]	[X]	[X]
Restricts	[X]	[X]	[X]
Implements	[X]	[X]	[X]

Presence of nodes and links of iStar default syntax			
Construct		Metamodel	Concrete syntax
Goal		[X]	[X]
Quality		[X]	[X]
Resource		[X]	[X]
Task		[X]	[X]
Actor		[X]	[X]
Agent		[X]	[X]
Role		[X]	[X]
Refinement		[X]	[X]
Qualification		[X]	[X]
Contribution (make, help, break, hurt)		[X]	[X]
NeededBy		[X]	[X]
Dependency		[X]	[X]
Association links	is-a	[X]	[X]
	Participates-in	[X]	[X]

Conflicts				
List the concepts and verify the occurrence of conflicts between the constructs of the extension and the existing extensions.				
Concept	Conflicts			
	One construct with	Two	of more	Wrong Construct

	two or more Symbols	constructs with only one Symbol	representation of iStar constructs	which is not part of the extension
Security goal	[0]	[0]	[0]	[0]
Privacy goal	[0]	[0]	[0]	[0]
Security Measure	[0]	[0]	[0]	[0]
Privacy Measure	[0]	[0]	[0]	[0]
Security Mechanism	[0]	[0]	[0]	[0]
Privacy Mechanism	[0]	[0]	[0]	[0]
Security Constraint	[0]	[0]	[0]	[0]
Privacy Constraint	[0]	[0]	[0]	[0]
Cloud Provider Actor	[0]	[0]	[0]	[0]
Threat	[0]	[0]	[0]	[0]
Implements	[0]	[0]	[0]	[0]
Satisfies	[0]	[0]	[0]	[0]
Restricts	[0]	[0]	[0]	[0]
Implements	[0]	[0]	[0]	[0]
Details about the problem(s): Problems were not identified.				

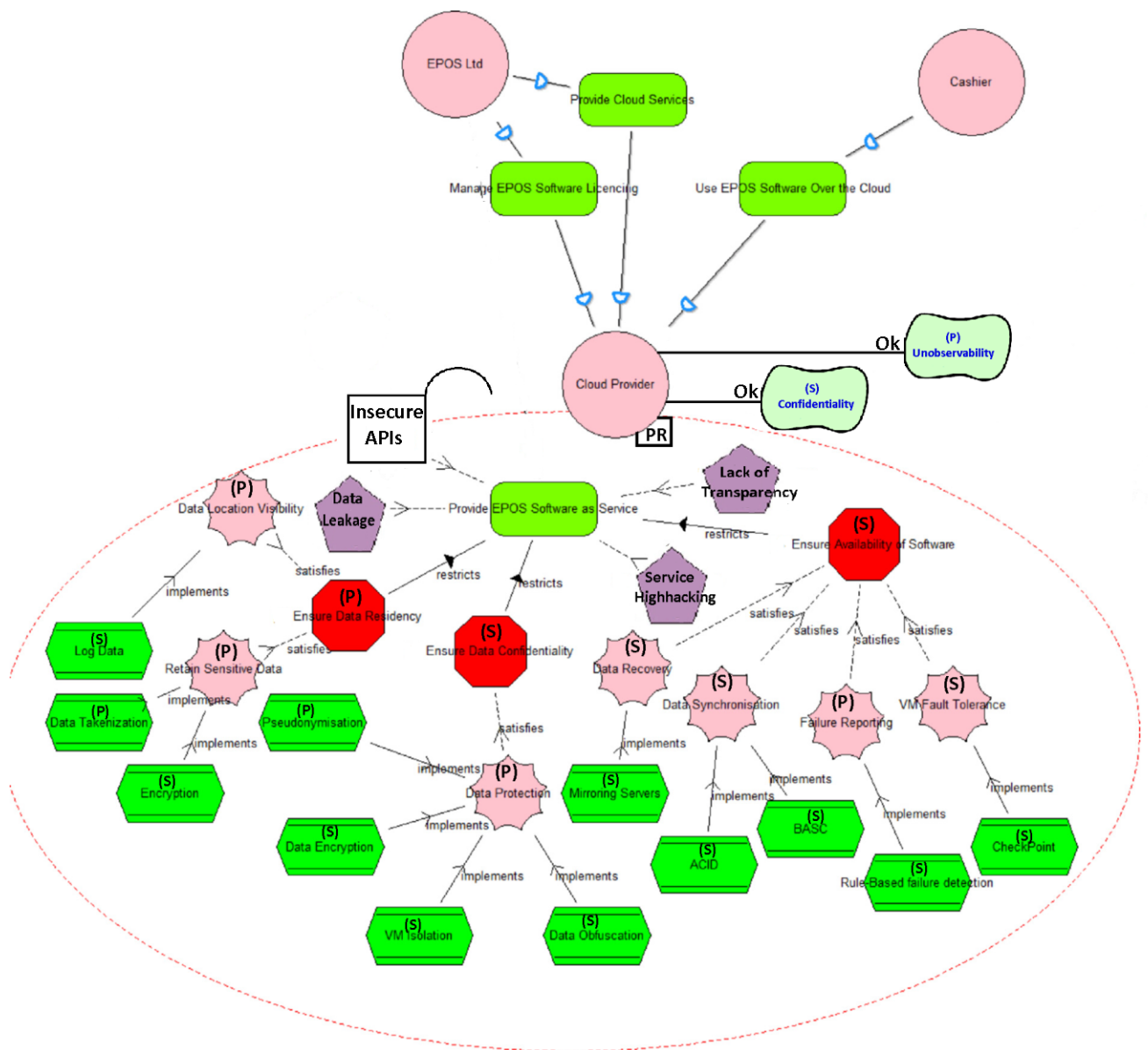
3.5 Apply the extension to a modelling tool

We did not propose a modelling tool. So, the flow goes to 4. Evaluate and validate iStar extension.

4 Evaluate and validate iStar extension

4.1 Use the iStar extension proposed to model a system

You should to relate the security and privacy qualities with the cloud providers by satisfaction relationship. The threats and vulnerabilities should be represented and related with the goals. Next, the constrains of security and privacy should be represented in model and related with existing goals by restriction. Privacy and security measure should be represented and related with the existing constraints. Finally, security and privacy mechanisms should be represented and related with the measures.



4.2 Evaluate the iStar extension

We did not perform the evaluation of the iStar extension because we are only revisiting one existing iStar extension. We will propose a new extension using all tasks of the PRISE.