future internet

MDPI

Article

Modeling cloud ecosystems

Eduardo B. Fernandez[1], Nobukazu Yoshioka[2] , Hironori Washizaki[3], and Madiha H. Syed[1]

Received: date; Accepted: date; Published: date
Academic Editor: name

1 Dept. of Comp, and Elect. Eng. and Comp. Sci, Florida Atlantic University, Boca Raton, FL 33431, USA fernande|msyed@fau.edu

2 GRACE Center, National Institute of Informatics, Tokyo, Japan, nobukazu@nii.ac.jp

3 Waseda University, Tokyo, Japan, washizaki@waseda.jp

Correspondence: fernande@fau.edu

Abstract: Clouds do not work in isolation but interact with other clouds and with a variety of systems either developed by the same provider or by external entities with the purpose to interact with them; forming then an ecosystem. A software ecosystem is a collection of software systems that have been developed to coexist and evolve together. The stakeholders of such a system need a variety of models to give them a perspective of the possibilities of the system, to evaluate specific quality attributes, and to extend the system. A powerful representation when building or using software ecosystems is the use of architectural models, which describe the structural aspects of such a system. These models have value for security and compliance, are useful to build new systems, can be used to define service contracts, find where quality factors can be monitored, and to plan further expansion. We have described a cloud ecosystem in the form of a pattern diagram where its components are patterns and reference architectures. A pattern is an encapsulated solution to a recurrent problem. We have recently expanded these models to cover fog systems and containers. Fog Computing is a highly virtualized platform that provides compute, storage, and networking services between end devices and Cloud Computing Data Centers; a Software Container provides an execution environment for applications sharing a host operating system, binaries, and libraries with other containers. We intend to use this architecture to answer a variety of questions about the security of this system as well as a reference to design interacting combinations of heterogeneous components. We defined a metamodel to relate security concepts which is being expanded.

Keywords: Software ecosystems, architecture patterns, cloud computing, reference architectures, security patterns, systems security.

1. Introduction

Because of their convenience and relative low cost cloud computing systems have become very successful in attracting small and medium businesses and academic institutions. Their emergence has brought a variety of products or services that complement or extend their basic services. Some clouds are also connected to other (maybe more specialized) clouds and may support cyber-physical systems as well as a variety of user devices or intelligent machines. We have now what is called a software ecosystem. Ecosystems were initially defined from a biological perspective: systems formed by the interaction of a community of organisms with their physical environment[1]. The term was later

[1] http://wordnetweb.princeton.edu/perl/webwn

applied to software systems: "a collection of software systems, which are developed and co-evolve in the same environment" [Lun09]. For software product lines: "An ecosystem is the expansion of a software product line architecture to include systems outside the product which interact with the product" [Bos09]. Software ecosystems are advantageous to suppliers who can offer a larger variety of products or services and to consumers who can find more products to help them reach their business goals. Companies such as Microsoft and Apple have been building ecosystems around their products for many years and more recently telecommunications companies such as Cisco [Cis14], Ericsson [Bas14], and others, have been building extensive software ecosystems.

Software ecosystems include also economic and socio-technical aspects [Jan09]; but those aspects are not considered here. In cloud ecosystems their complementary systems may not be produced by the same vendor and may use different protocols although able to interact with other products in the ecosystem. These complementary systems are a growing set, where new types of products or services constantly appear and provide some useful functions for some types of users. Some of those products may be housed in real devices but they also can be virtualized and executed in any system, including standard processors or cyber-physical systems.

Several authors, e.g. [Bou09, Jan09, Maz12] have indicated that the lack of reference architectures or other abstract models inhibit the wider adoption of software ecosystems and deny the possibility of exploiting their full potential. This need motivates our work: Architectural models based on patterns are a powerful representation when building or using cloud ecosystems and similar complex systems [Fer13]. A pattern is an encapsulated solution to a software problem. We started by describing models for clouds [Fer15a] and then expanded them to describe cloud ecosystems [Fer15d]. After a careful search we have not found similar models (see Section 4). We have expanded our initial ecosystem to cover fog systems [Sye15b] and containers [Sye15a]. Most of the components of this system have been already modeled as patterns by ourselves but some are missing, we identify here the new patterns we need. We present here a systematic method to build ecosystem models for clouds, using patterns and reference architecures, which is our main contribution. We discuss the value of these models with respect to several objectives, which are useful for understanding and analyzing significant aspects of the ecosystem.. We do not claim completeness, an ecosystem is open-ended and our model will continue growing when we identify more functions and their patterns.

As indicated, an important value of our model is for analyzing security aspects of an ecosystem and we intend to answer several security questions with it. Our long term objective is to develop a holistic security view across all the elements of the ecosystem and we are starting with security in a fog controlling a variety of devices. In particular, we intend to define policies on what data from the cloud can be sent to the devices or what data from the devices can be sent to the cloud. Devices may contain sensitive data whose disclosure would affect the privacy of users. The fog platform itself contains data and the access of that data should conform with cloud policies as well as device policies; that is, security constraints in the cloud and devices should propagate across up and down levels. Without a unified view it is very difficult to integrate systems which may have their own security policies. As part of this emphasis we show a security metamodel that is being extended to include more concepts.

This work is organized as: Section 2 defines some necessary concepts; Section 3 presents related work on ecosystems and fog security, while Section 4 describes the cloud ecosystem as a pattern diagram, followed by a description of three of its patterns to illustrate their contents. Section 5 considers the use of security metamodels to complement our architectural models when dealing with security aspects. Validation of the models is discussed in Section 6, which also emphasizes possible applications for them. Section 7 considers some security issues. We end with conclusions in Section 8.

2. Background

A *pattern* is a solution to a recurring problem in a specific context. Software patterns are categorized as analysis [Fow97], design [Gam94], architecture [Bus96], and security patterns [Fer13]. *Abstract patterns* describe a basic semantic aspect while *Abstract Security patterns* (ASPs), realize one or more security policies able to control (stop or mitigate) a threat or comply with a security-related regulation or institutional policy [Fer14]. Patterns are described using a template composed of a set of sections. A problem section describes a problem and the forces that constrain and define guidelines for its solution, e.g. "overhead must be reasonable". Pattern solutions are usually described using modeling languages such as the Unified Modeling Language (UML), maybe combined with formal languages such as the Object Constraint Language (OCL). UML diagrams may include class, sequence, state, and activity diagrams. A set of consequences indicate how the pattern solved the specific problem and what are the advantages and disadvantages of using it; i.e., how well the forces were satisfied by the solution. An implementation section provides hints on how to use the pattern in an application. A section on "Known uses" lists real systems where this solution has been used previously, i.e., a pattern is an abstraction of a good practice. A section on related patterns indicates patterns that complement or provide alternative solutions to the one in this pattern. A pattern embodies the knowledge and experience of software developers and can be reused in new applications; carefully-designed patterns implicitly apply good design principles. Patterns are also good for communication between designers and to evaluate and reengineer existing systems. While initially developed for software, patterns can describe hardware, physical entities, and combinations of these. Pattern solutions are suggestions, not plug-ins or software components. A *compound* pattern is composed of two or more simpler patterns.

A *Reference Architecture* (RA) is an abstract software architecture, based on one or more domains, with no implementation aspects [Avg03, Ang12]. An RA should define the fundamental concepts of a system expressed as ASPs and the interactions among these units. An RA should be reusable, extendable, and configurable; that is, it is a kind of composite pattern for whole architectures and it can be instantiated into a concrete software architecture by adding platform aspects [Avg03]. In addition to class and sequence diagrams, an RA may include a set of use cases (UC), and a set of Roles (R) corresponding to its stakeholders (actors). Types of RAs include those for the technology domain (describe platforms and other design artifacts [Ang12]), application domain (describe different types of applications), and problem domain (similar to DMs, but oriented to software). After adding security patterns to neutralize identified threats in an RA we have a *Security Reference Architecture* (SRA), and we have just produced a SRA for clouds [Fer15a]. We can also add compliance patterns to produce a *Compliance Reference Architecture* [Yim15].

Policies are high-level guidelines defining how an institution conducts its activities in its business, professional, economic, social, and legal environment. The institution security policies include laws, rules, and practices that regulate how an institution uses, manages and protects resources. *Regulations* are local or government policies that must be reflected in the implemented system. Industry regulations are called *standards*. Policies, regulations, and standards can be described using UML models.

We describe the relationships between patterns using a *pattern diagram* [Bus96]. In a pattern diagram rounded rectangles represent patterns and arrows indicate the contribution of a pattern to another, e.g., a Container provides virtual enviroenments to PaaS in Figure 1.

3. Related work

As indicated earlier, the word ecosystem has a variety of interpretations. [Maz12] discusses an IoT ecosystem from a business perspective. A business ecosystem is "the network of buyers, suppliers and makesr of related products or services plus the socio-economic environment, including the institutitonal and regulatory framework." Our definition is more restricted focusing on the products themselves but also considering policies defining institution or regulations as well as industry standards that apply to the products. [Maz12] indicates that ecosystems ususally have a *hub,* or central product or service; we have a similar concept in our ecosystem. A specialized type of ecosystem is the *learning ecosystem* [Gar13, Gar15a, Gar15b]. This type of ecosystem is quite different from ours in that it is a set of homogeneous units with a predefined purpose and a well-defined architecture; ours are heterogeneous systems with an evolving architecture. These ecosystems do not use our definition of pattern and do not use UML models to describe them. The only paper with more abstract models of ecosystems is [Bou09], which presents a model oriented to the business (functional) aspects of ecosystems; in contrast our models emphasize the structural aspects of the interconnection of products.

While there is a good amount of work on ecosystems from the point of view of software architecture, e.g. [Bos09], we have found only a few examples of cloud ecosystems. NIST described an ecosystem for its Cloud Reference Architecture [NIS11] and later an ecosystem for its Security Reference Architecture [NIS13]. However, they included only a Broker to let users access multiple clouds, an Auditor to check compliance with regulations, and a Communications Provider; that is, theirs is a rather meager set of external functions. They describe their models with words and block diagrams, which we consider not precise enough to guide developers and researchers. The Open Group has a web site with their cloud model [OPE]. This includes a UML model for the main blocks and a table describing the components involved. There are no UML models for the components and they consider the same main components of the NIST model. A blog presents some ideas about models for cloud ecosystems [Cho11]; however, the models are loose and shown as block diagrams. OSGi also has some general ideas about ecosystems [OSG12] but nothing specific about clouds. Ecosystems can also be seen as systems of systems and work on that topic may apply to them. Work on software product line architectures is also relevant [Mel10], as well as work on cloud security requirements [She15], but these works do not attempt to model a complete ecosystem.

Given the novelty of fog computing there is little work on its security aspects. Three papers survey general security aspects:

[Axe15] evaluates business, professional, and government structures and practices for improving IoT security, proposing some structures and rules. The paper focuses mainly in economic and political aspects and does not provide any technical details.

[Sto14] surveys fog applications and general security issues. They analyze in detail a man-in-the-middle attack, where gateways used as fog devices may be replaced by fake ones.

[Sad15] considers industrial IoT systems, which are cyber-physical systems where attacks can have very serious effects. The paper surveys some of these attacks and provides a few solutions.

The only paper that discusses fog computing security models and architectures is [Dso14]. The paper proposes a policy-driven security management approach, considering the implementation of a policy enforcement system (Reference Monitor [Fer13]) that can enforce XACML rules; however, they do not consider rights inheritance or propagation of rights in the ecosystem. We see our work as expanding this work across the ecosystem.

Some work considers the use of cloud computing to support cyberphysical systems (CPSs) [Tah14]. This work is more general than fog computing but some of their ideas are clearly related to this architecture. Along these lines, our work on modeling and finding generic threats for CPSs is

relevant and we will apply it to fog computing [Fer16]. It is clear that the security of the combination cloud/Internet of Things is an area that requires more work and where our models appear promising.

4. A model for a cloud ecosystem

We show first the complete ecosystem in the form of a pattern diagram that relates the contributions of the patterns with respect to each other. After building this pattern diagram we need to build detailed models for the components. We show three examples of the patterns in the ecosystem and a part of the SRA. None is shown completely, the idea is to show their main functions, the complete descriptions can be found in their respective references. These descriptions follow the standard pattern template of [Bus96]. Missing parts include sections on Problem, Forces, Consequences, Implementation, Known uses, and Related Patterns. The idea here is that we can build patterns for every participant in the ecosystem, which provides a unified view of the complete system.

4.1 Pattern diagram of the ecosystem

Figure 1 shows our current cloud ecosystem. The Cloud Reference Architecture (Cloud RA) is the main pattern that defines the ecosystem (the hub) [Fer15a]. As indicated, this can be converted into a Cloud Security RA (Cloud SRA) by adding security patterns to control its identified threats. The Cloud SRA includes, among others, patterns for Authentication, Authorization, and Logging [Fer13]. We just defined a cloud HIPAA-compliant RA [Yim15]. Threats can be enumerated in several ways and we use an approach based on activities in an activity diagram describing its use cases [Fer13]. Cloud Web Application Firewalls and Security Group Firewalls provide filtering functions that can be provided as services through NFVs (see below) or on their own.

The service layers of a cloud are themselves compound patterns and we have written patterns for IaaS, PaaS, and SaaS [Has12]. They describe the services sold by the cloud provider. Telecommunication companies have discovered that they can provide services to their customers by building their networks as services rented from some cloud provider [Bas14]. The provision of network functions using virtualization, Network Functions Virtualization (NFV), is a network architecture where functions such as load balancers, firewalls, IDS, and accelerators are built in software and offered as services. Each Virtualized Network Function (VNF) may use one or more virtual machines or containers running different software. Typically, NFVs come with some security mechanisms but which ones depend on the vendor. To make the model more flexible we have a pattern for the NFV without security and a derived pattern for the Secure NFV [Fer15c].

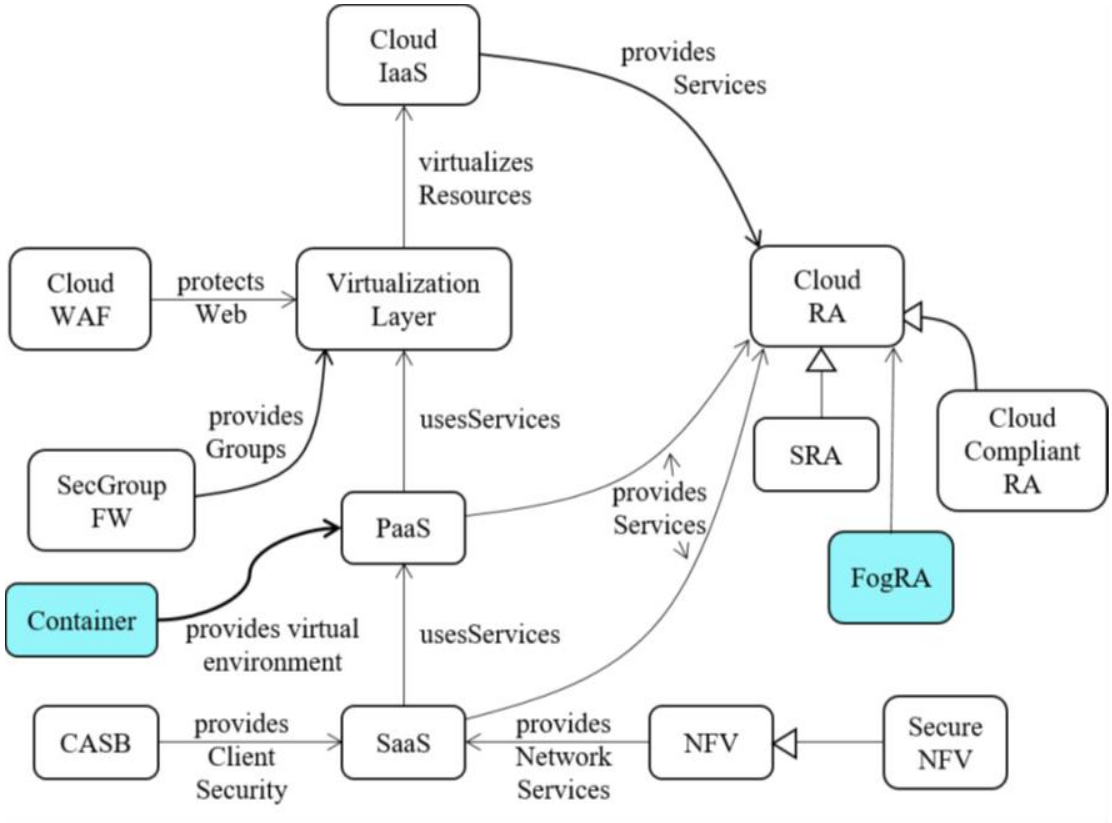
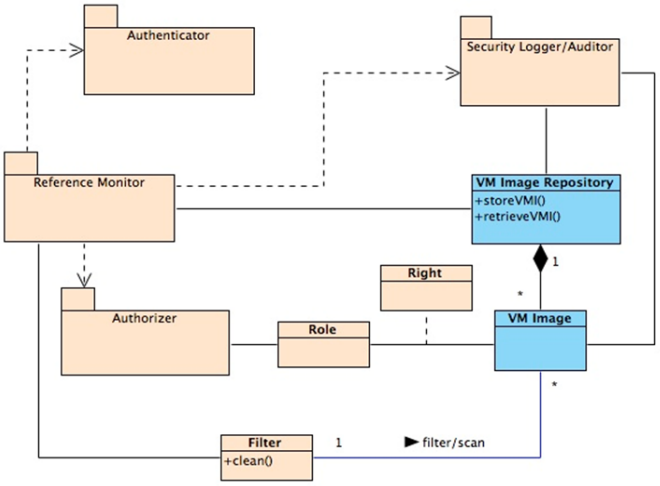


Fig. 1. A cloud ecosystem

Cloud Access Security Brokers (CASBs) are security enforcement points between consumers and service providers that apply security controls to access cloud services, usually SaaS services [Fer15b]. They may also control access to internal company resources. Security controls may include authentication (credentials and passwords), authorization policy enforcement, intrusion prevention, antimalware filters, security logging/auditing, and encryption. There is no pattern yet for the Virtualization Layer, although we defined a pattern for a Virtual Machine Operating System [Fer13]. An important lower-level pattern for this function is an OpenStack pattern, part of a hierarchy of IaaS patterns [Fer15e].

As indicated, analyzing threats and neutralizing them with patterns we arrived to secure units of the SRA. Figure 2 shows a class model for the secure VM image repository system. The Virtual Machine Image Repository holds a set of Virtual Machine Images (VMI) that can be used to instantiate virtual machines. The Reference Monitor uses a Filter that scans all VM images before being published or retrieved. The Authenticator is an instance of the Authenticator Pattern that allows the Reference Monitor to authenticate the users who can publish or retrieve images if the Authorizer authorizes them. The Reference Monitor pattern enforces the authorization rights defined in the Authorizer. The Security Logger/Auditor keeps track of accesses to the repository. Our latest additions are the Container and the Fog Reference Architecture, described below.



. Fig. 2. Secure VMI Repository System

4.2. Some of the patterns in the ecosystem

4.2.1. Cloud Access Security Broker [Fer15b]

Intent

Cloud Access Security Brokers (CASBs) are security enforcement points between consumers and service providers that apply security controls to the consumer's users to access cloud services, usually SaaS services. They may also control access to internal company resources. Security controls may include authentication (credentials and passwords), authorization policy enforcement, intrusion prevention, antimalware filters, security logging/auditing, and encryption.

Solution

Use an intermediary system, called a CASB, which provides security controls (authentication and authorization), can monitor the use of services by users, and can perform malware detection when users access cloud applications. Additionally, other services such as performance, identity, and search can be provided. Figure 3 shows the class diagram of the CASB. Consumers (users) request services through the Broker, which in turn gets them from one of the Service Providers. The Broker includes a set of security mechanisms such as a SecurityLogger/Auditor, an Authorizer, an Authenticator, an Encryptor, and maybe others. Consumers and CASBs can be mutually authenticated. The CASB enforces rights for the consumers when they try to access an application. Internal Resources (applications) can also be controlled by the CASB. An Identity Federation provides identifiers for consumers and SPs to support authentication. Figure 4 shows the sequence diagram for the use case "Access an application service": a consumer requests a service to the CASB, which invokes an authentication protocol, when authenticated the consumer can access the service if authorized for it; this interaction is logged.

The CASB enforces institution policies in any access as well as protecting against malware. In other words, the CASB is an extended Reference Monitor [Fer13].

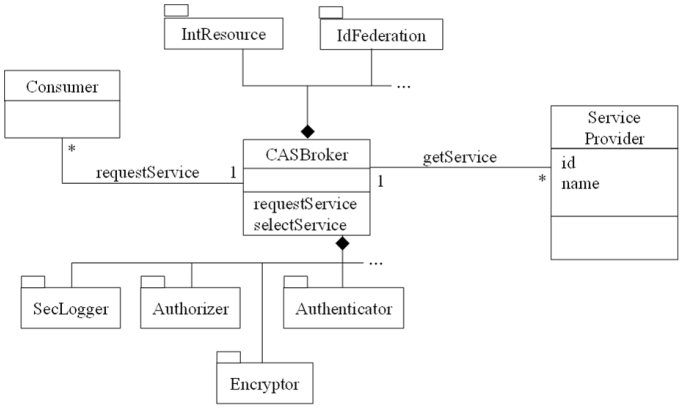


Fig.3 Class diagram of the CASB pattern

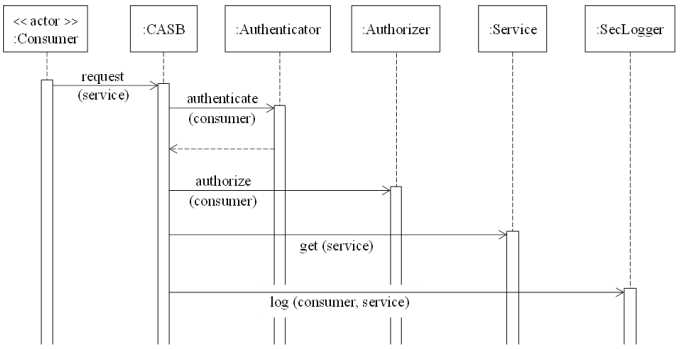


Fig. 4 Sequence diagram for the use case "Access an application service"

4.2.2. The Software Container

Intent

A Software Container provides an execution environment for applications sharing a host operating system, binaries, and libraries with other containers. Containers are lightweight, portable, extensible, reliable, and secure.

Solution

Provide a runtime environment that can support the isolated execution of applications on a shared Host OS, this is a Software Container (Figure 5). They also may share binaries and libraries with other containers. Containers provide isolated execution and extensible services to the application.

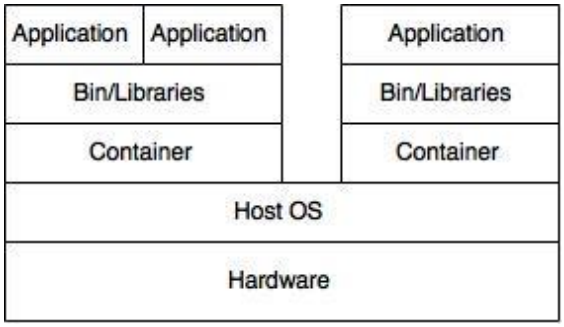


Fig. 5 Two containers sharing one OS

Figure 6 shows the class diagram for this pattern. A Container controls a set of Applications sharing a Host OS that provides a set of Resources. An Interceptor mediates the services provided to the application by the container. Applications hosted in containers can be accessed remotely through Proxies, where the Container acts as a broker. The client interacts with the Application Proxy, which represents the application. The application interacts with the Client Proxy, which represents the client. The Container provides a set of Services to the applications. Container Images are stored in image repositories.

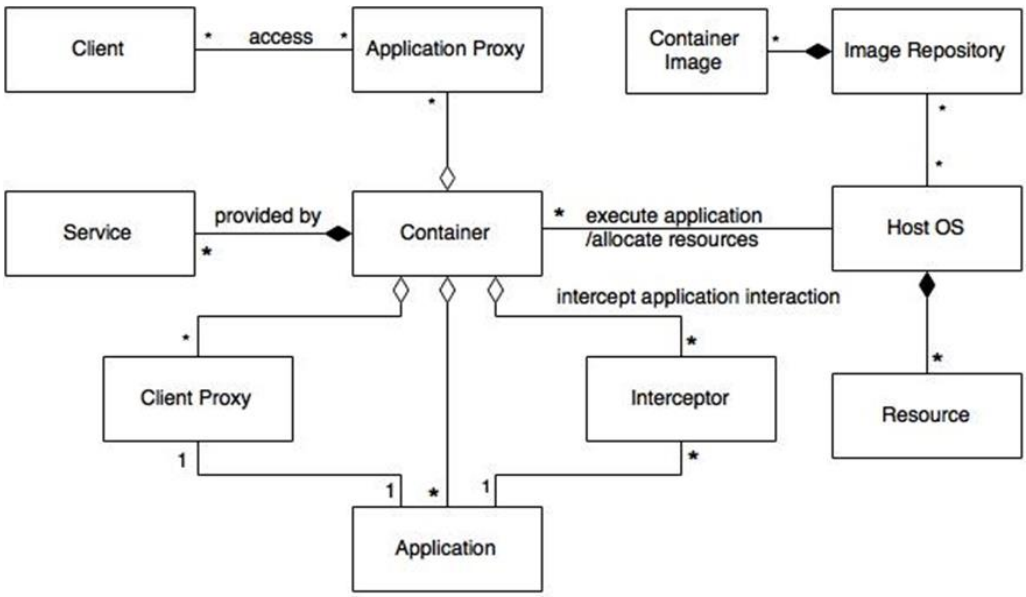


Fig. 6 Class diagram of the container pattern

4.2..3. Fog computing

Our current work also includes modeling fog computing. Fog Computing is a highly virtualized platform that provides compute, storage, and networking services between end devices and Cloud Computing Data Centers [Bon12, Bon14, YiS15]. Fog computing systems are key systems for the Internet of Things, they can control for example smart grids or traffic lights [Rag15, Sto14]. We have completed a pattern for fog computing [Sye15b]. Figure 7 shows its class diagram. The Fog is a collection of several distributed tiny clouds called Fog Nodes. They can be resource-rich servers,

routers, access points, mobile devices, etc. A Fog Node has resources which include hardware (compute, networking and storage) capabilities. The nodes provide real-time analytics using an Analytics Engine. Applications can be hosted in the fog nodes using virtualization, provided by a Virtual Machine Monitor (VMM), which can create virtual machines (VMs), and/or Containers. A Distributed Database stores both application data and necessary metadata for service orchestration; it also has information about the hardware and software capabilities of nodes, information about the status of fog nodes and services, policies for security, filtering, and configuration. Fog computing uses policy-based service orchestration. A Policy Manager is triggered by service requests and a Decision Maker Engine (Reference Monitor) gathers relevant policies and metadata to decide about requests. Data is transferred between fog nodes, the decision maker, and the various components of the Fog. The Fog also provides Authentication and Authorization services. In addition, services like filtering, aggregation of data, logging, etc., can be provided.

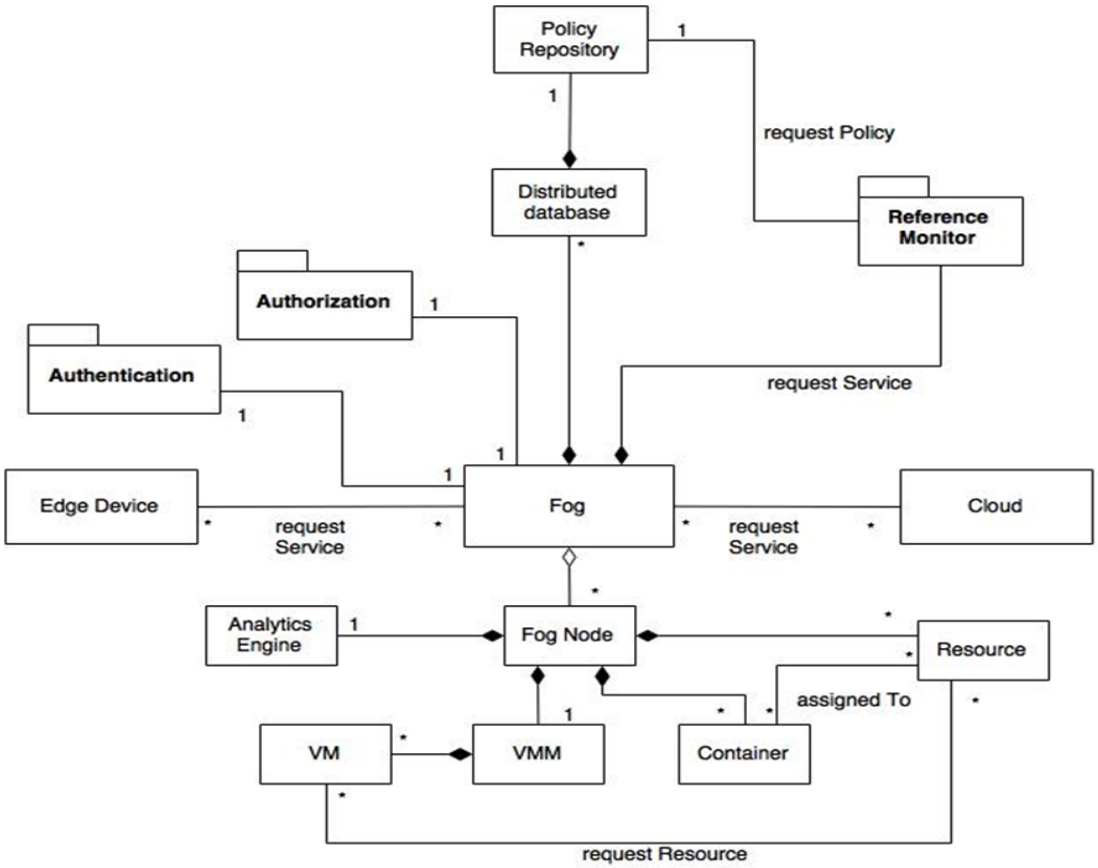


Fig. 7. Class diagram of the Fog Computing pattern

5. Metamodels for security concepts

The metamodel of Figure 8 relates the security concepts we are using in the ecosystem. *Threats* take advantage of *Vulnerabilities* that can exist in any cloud service level. Threats come from analysis of Use Cases or from published Threat Lists. Each use case has a set of Roles that describe the participants in the use case. We can stop a threat by removing the initial vulnerability or by controlling its propagation (by removing other vulnerabilities) through the use of a *Security Pattern*.

The security pattern to use can be selected from the countermeasures defined in the *Misuse Pattern* which describes the threat. Threats that lead to misuses are the goals of the attacker and are performed through low-level threats in the *Threat List* or directly through a use case operation. Use cases include the roles that participate in the use case. Some threats can happen in all service levels. For example, buffer overflow is a language problem and allows escalation of privilege by the attacker operating at any level. Other threats are specific to the level; for example, a financial application can be attacked by taking advantage of lack of proper authentication in remote access to accounts. If the threat takes advantage of a flaw in an application, it may compromise the security of that application. If the threat affects the IaaS level it affects all the cloud computations, and if it happens at the PaaS level it can affect all the applications developed or deployed in the cloud.

We have started to expand this metamodel by integrating and extending existing cloud security metamodels together with newly added concepts. Figure 9 shows how the metamodel would be used in cloud services development and maintenance. Our metamodel provides a basis for describing and accumulating security and privacy-related knowledge over different layers so that it becomes much easier to select and combine the right patterns and related knowledge for addressing these issues in cloud services. Moreover, designers could refer to the metamodel for designing high-level architectures of cloud service systems in efficient and effective manner. To confirm the usefulness and feasibility of the metamodel, we conducted a case study that describes a cloud security pattern based on the metamodel [Was15].

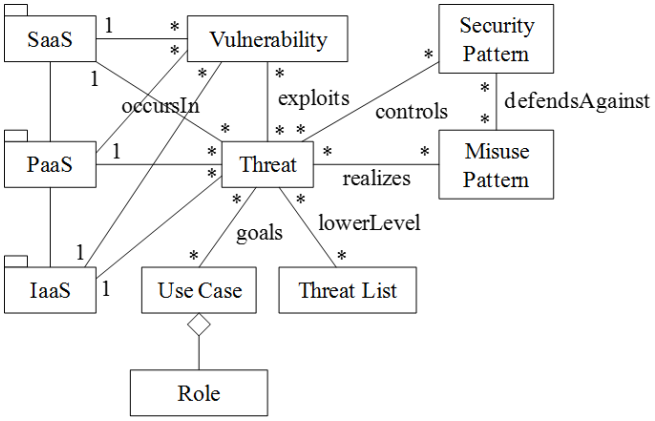


Fig. 8. Metamodel for security concepts

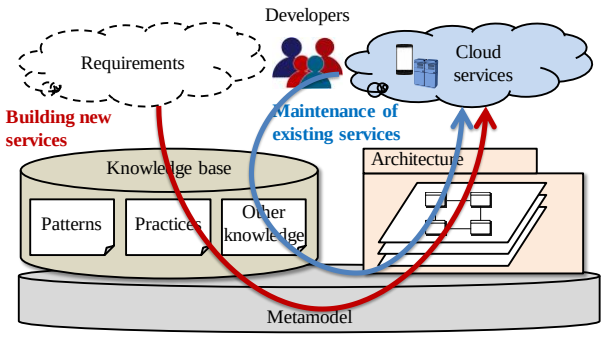


Fig. 9. Metamodel and cloud services

6 Validation of the models

Ecosystem model validation requires first to validate the patterns used in its construction; then RAs and SRAs must also be validated, followed by the complete ecosystem.

Specific patterns are normally evaluated by submitting them to some pattern conference, e.g., Pattern Languages of Programs (PLoP) or EuroPLoP. In these conferences, a pattern paper is developed with the help of a shepherd and then discussed in a workshop by about ten people. The pattern is then published and exposed for criticism. We have followed this route for all our patterns. Of course, the ultimate evaluation comes when developers use them in their designs but the patterns shown here are too new for this to have happened.

RAs are abstract models and cannot be evaluated with respect to security or performance through experimentation or testing. An RA is similar to a pattern, and it has a similar use; it is a paradigm to guide implementation of new systems or evaluation of existing systems as well as other uses described below. Their evaluation must be based on how well they represent the relevant concepts of the systems they describe, how well they handle potential threats, how complete they are, how precise they are, how they can be applied to the design or evaluation of systems, and how useful they are for other relevant functions. Again, their final validation comes from practitioners who can find them useful and convenient to build concrete architectures. In this respects, we showed in [Fer15a] that our SRA included all the functions found in the SRAs of commercial and experimental clouds.

A type of validation (or at least justification) of our ecosystem models comes from describing their advantages:

Control of heterogeneity: The involved components come from different vendors and follow a variety of standards and protocols. An abstract model can unify this heterogeneity and provide a way to understand and analyze global aspects of these systems.

A *holistic security view*. Many authors, e.g. [Bro12, Fer11], emphasize the need to develop secure systems in a holistic way. Systems built piecemeal omit important interactions that may result in vulnerabilities. Enterprises have started to realize of the value of holistic approaches to security [Cis14, Cis15]. An ecosystem provides such a holistic view by indicating the places where security mechanisms can be attached and their effect on the functional parts of the architecture. As we did in Figure 2, we can extend the UML model of the functional ecosystem by indicating all the points where threats are neutralized with corresponding security patterns. We can trace the propagation of attacks and study where to place defenses for greater effect. Many threats result of the interaction of different units and cannot be discovered by analyzing each unit in isolation. Privacy rules are defined in the clouds and in devices but we need to make sure that interactions with the components still respect these rules. We elaborate on other security aspects in Section 7.

Other quality factors: Holistic views are useful to combine quality factors such as safety or reliability with security.

Compliance with standards and regulations. An RA can be used to support security standards and regulations, which can be described as policies which in turn can be implemented as patterns and made part of the SRA. The ecosystem helps architects or designers to identify what components of the cloud system are associated with the standard and can be used to comply with the specific rules of the standard. Relating specific regulations to specific security mechanisms can be used to demonstrate compliance [Yim15].

Support for software development [Sye15c]. DevOps is an increasingly popular agile process to build software that relies heavily on containers. We explored the use of our Container pattern [Sye15a] for this purpose.

Support for virtualization. It is possible to assign the software processes of the ecosystem to a variety of hardware platforms, some or all of which can be virtualized. For example, one can build a virtual drone implemented using two physical devices.

Support for service contracts. In an ecosystem users or institutions may want to rent services involving more than one product. This requires a service level agreement indicating the obligations ot providers and consumers. An ecosystem model can make these services transparent and indicate where compliance would be monitored.

7. Security issues of ecosystems

We intend to develop a holistic security view across all the elements of the ecosystem. In particular, we intend to define policies on what data from the cloud can be sent to the devices or what data from the devices can be sent to the cloud. Devices may contain sensitive data whose disclosure would affect the privacy of users. The fog platform itself contains data and the access of that data should conform with cloud policies as well as device policies; that is, security constraints in the cloud and devices should propagate across levels. We intend to perform a systmatic analysis of threats, keeping in mind that the introduction of new products may bring new vulnerabilities; each use case of a new product or service must be analyzed to consider possible attacker goals related to it.

Each component may have its own set of policy rules or may inherit from other components; in the latter case there can be conflicts [Woo79]. Fog platforms may communicate with other fogs and may need authorizations to perform actions in remote fog systems. Some of this work has already been done in isolated fogs [Dso14], but it is not clear how these results apply to the new context defined by the components of a cloud ecosystem.

We need to define policies on how data from the cloud can be used in the devices or what data can be sent from devices to the cloud. The fog also sends commands to the devices and devices may send events to the cloud. The fog itself has a database and operations that can be accessed from the cloud or the devices. We need to require that devices have a basic separation of computing environments as using two virtual machines or two separated environments. We need to build a detailed security architecture to provide these functions, express it using XACML rules and build several examples. We have developed patterns for XACML [Fer13], which can be applied to describe precisely these rights.

Consider a set of rights for cloud resources (R, O, t), where R is a set of roles, O is a set of objects, and t is an access type. Each right represents what a given actor or role can do with specific resources; for example, in fog managing traffic lights, "Role 'Traffic Light Controller' can activate traffic lights". Those rights can be defined in the fog itself or can be inherited from higher-level rights defined in the cloud. We may need to add new constraints in the form of predicates to the rights in the fog to access devices, e.g. rights such as "Role Traffic Light Maintenance Worker" can activate or deactivate only the lights in a specific zone". The fog may have also new roles. We need to add rights in devices to access fog resources; this may give device users rights to access cloud data and it is related to the BYOD problem.

An important security need is management. The functions of such a system include determination of assets, assignment of rights, consideration of regulations, policy definition, and privacy. The metamodel of Section 5 is valuable for this purpose. A model oriented to fulfill the ISO 27000 security regulations in clouds is given in [Bec13], but there is no such a model for ecosystems.

8. Conclusions

Clouds require a variety of complementary components to be effective and cloud ecosystems are starting to become widespread. Some are implicit ecosystems like the combination of clouds and

wireless devices. New components such as containers and fog computing platforms are appearing. We believe that a holistic, unified treatment is fundamental to handle the complexity of cloud-based systems and allow different kinds of users to analyze the synergy of the total ecosystem. Patterns provide a unified way of representing all the components of the ecosystem and can represent both functional and non-functional aspects. Pattern models are especially useful for handling security and privacy, a unified approach reduces complexity, one of the most important weaknesses used by attackers and can enable analysis of the propagation of threats and data leaks. We show that we can start from patterns, combine them to produce reference architectures, and aggregate those two concepts to build models for complete ecosystems. While we presented these models in terms of clouds the methodology is general and can be used to build other types of ecosystems. We have defined architectures for all the current components and we are using this architecture to analyze security and related aspects. We identified several other directions where this ecosystem appears valuable and we intend to study some of them. In the immediate future we are concentrating in security aspects of the fog systems as part of a cloud ecosystem.

Acknowledgements

We thank our reviewers who provided valuable suggestions and references. Part of this work was performed during the visit of Dr. Fernandez to Tokyo in March of 2015, supported by the National Institute of Informatics of Japan.

References

[Ang12] S. Angelov, P. Grefen, and D. Greefhorst, A framework for analysis and design of software reference architectures", *Inf. and Soft. Technology*, vol. 54, 2012, 417-431.

[Avg03] P. Avgeriou, "Describing, Instantiating and Evaluating a Reference Architecture: A Case Study," *Enterprise Architect Journal*, Fawcette Technical Publications, Jun. 2003.

[Axe15] C.W.Axelrod, "Enforcing security, safety and privacy for the Internet of Things", *Systs., Apps., and Technology Conf.* (LISAT), 2015.

[Bas14] H. Basilier, M. Darula, and J. Wilke, "Virtualization network services—the telecom cloud", *Ericsson Review*, March 28, 2014, 2-9.

[Bec13] K. Beckers, I. Coté, S. Fassbender, M. Heisel, and S. Hofbauer, "A pattern-based method for establishing a cloud-specific information security management system", *Requirements Eng*. vol. 18, 2013, 343-395.

[Bon12] F. Bonomi, R. Milito, J. Zhu., S. Addepalli, "Fog computing and its role in the Internet of Things", *MCC'12,* ACM, Aug. 17, 2012, Helsinki, Finland.

[Bon14] F. Bonomi, R. Milito, P. Natarajan and J. Zhu, "Fog Computing: A Platform for Internet of Things and Analytics", 2014. DOI: 10.1007/978-3-319-05029-4_7

[Bos09] J. Bosch, "From software product lines to software ecosystems", *Procs. 13thInt. Software Product Line Conf.* (SPLC'09), August 2009, 111-119.

[Bou09] V. Boucharas, S. Jansen, S. Brinkkemper, "Formalizing software ecosystem modeling", *IWOCE'09*, Aug. 24, 2009, Amsterdam, The Netherlands.

[Bro12] A. Brown, B. Apple, J.B. Michael, and M. Schumann, "Atomic-level security for web applications in a cloud environment", *Computer,* Dec. 2012, IEEE, 80-83.

[Bus96] F. Buschmann, R. Meunier, H. Rohnert, P. Sommerland, and M. Stal, *Pattern-Oriented Software Architecture Volume 1: A System of Patterns*, Wiley, 1996.

[Cho11] D. Chou, "Rise of the cloud ecosystems", http://blogs.msdn.com/b/dachou/archive/2011/03/16/rise-of-the-cloud-ecosystems.aspx

[Cis14] Cisco Corp., "Cisco cloud strategy for cloud providers", 2014.

[Cis15] Cisco white paper, "Security everywhere", http://www.cisco.com/web/offers/pdfs/security-everywhere-whitepaper.pdf

[Dso14] C. Dsouza, G.J.Ahn, M. Taguinod, "Policy-driven security management for fog computing: Preliminary framework and a case study", *Procs. IEEE International Conference on Information Reuse and Integration* (IRI 2014), San Francisco, CA, Aug. 2014, 16-23.

[Fer11] E. B. Fernandez, N. Yoshioka, H. Washizaki, and M. VanHilst, "An approach to model-based development of secure and reliable systems", *Sixth International Conference on Availability, Reliability and Security (ARES 2011)*, August 22-26, Vienna, Austria.

[Fer13] E.B.Fernandez, *Security patterns in practice: Building secure architectures using software patterns*, Wiley Series on Software Design Patterns, 2013.

[Fer14] E. B.Fernandez, N. Yoshioka, H. Washizaki, and J.Yoder, "Abstract security patterns for requirements specification and analysis of secure systems", *Procs. of the WER 2014 Conference*, a track of the 17th Ibero-American Conf. on Soft. Eng.(CIbSE 2014), Pucon, Chile, April 2014

[Fer15a] E.B.Fernandez, Raul Monge, and Keiko Hashizume, "Building a security reference architecture for cloud systems", *Requirements Engineering*, 2015. DOI: 10.1007/s00766-014-0218-7

[Fer15b] E.B. Fernandez, Nobukazu Yoshioka, Hironori Washizaki, "Cloud Access Security Broker (CASB): A pattern for accessing secure cloud services", *Procs. of 4th AsianPLoP (Pattern Languages of Programs) 2015*, Tokyo, Japan, March 2015.

[Fer15c] E.B.Fernandez and B. Hamid, "A pattern for Networks Functions Virtualization", *Procs. EuroPLoP 2015*.

[Fer15d] E.B. Fernandez, N. Yoshioka, and H. Washizaki, "Patterns for Security and Privacy in Cloud Ecosystems", *Procs. 23rd IEEE Int. Requirements Eng. Conf.*, August 24-28, Ottawa, Canada.

[Fer15e] E. B. Fernandez, H. Washizaki, N. Yoshioka, "Patterns for Secure Cloud IaaS", *Procs. AsianPLoP* 2016

[Fer16] E.B. Fernandez, "Preventing and unifying threats in cyberphysical systems", *17th IEEE High Assurance Systems Engineering Symposium* (HASE), Orlando, Jan. 7-9, 2016.

[Fow97] M. Fowler, *Analysis patterns – Reusable object models*, Addison-Wesley, 1997.

[Gam94] E. Gamma, R. Helm, R. Johnson, J. Vlissides. *Design Patterns: Elements of Reusable Object-Oriented Software*, Addison-Wesley, Boston, Mass., 1994.

[Gar13] García-Holgado, A., & García-Peñalvo, F. J. (2013). The evolution of the technological ecosystems: An architectural proposal to enhancing learning processes. In F. J. García-Peñalvo (Ed.), *Procs of the First International Conference on Technological Ecosystems for Enhancing Multiculturality (TEEM'13)* (Salamanca, Spain, November 14-15, 2013) (pp. 565-571). New York, NY, USA: ACM.

[Gar15a] García-Holgado, A., García-Peñalvo, F. J., & Rodríguez-Conde, M. J. (2015). Definition of a Technological Ecosystem for Scientific Knowledge Management in a PhD Programme. In G. R. Alves & M. C. Felgueiras (Eds.), *Procs.*

of the Third International Conference on Technological Ecosystems for Enhancing Multiculturality (TEEM'15) (Porto, Portugal, October 7-9, 2015) (pp. 695-700). New York, NY, USA: ACM.

[Gar15b] García-Peñalvo, F. J., Hernández-García, Á., Conde-González, M. Á., Fidalgo-Blanco, Á., SeinEchaluce Lacleta, M. L., Alier-Forment, M., Llorens-Largo, F., & Iglesias-Pradas, S. (2015). Learning services-based technological ecosystems. In G. R. Alves & M. C. Felgueiras (Eds.), *Procs. of the Third International Conference on Technological Ecosystems for Enhancing Multiculturality (TEEM'15*) (Porto, Portugal, October 7-9, 2015) (pp. 467-472). New York, USA: ACM.

[Has12] Keiko Hashizume, E.B.Fernandez, and Maria M. Larrondo-Petrie, "A pattern for Software-as-a-Service in Clouds", *RISE'12, Workshop on Redefining and Integrating Security Engineering*, part of the ASE Int. Conf. on Cyber Security, Washington, DC, December 12-14, 2012.

[Jan09] Slinger Jansen, Anthony Finkelstein, Sjaak Brinkkemper, "A Sense of Community: A Research Agenda for Software Ecosystems", *31st Int. Conference on Software Engineering, New and Emerging Research Track*, 2009

[Lun09] M. *Lungu, Reverse Engineering Software Ecosystems* (Ph.D. Dissertation). University of Lugano, Switzerland, 2009.

[Maz12] O. Mazhelis, E. Luoma, H. Warma, "Defining an Internet-of-Things ecosystem", *Procs. of NEW2AN/ruSMART* 2012, LNCS 7469, 1-14, Springer-Verlag, 2012.

[Mel10]Daniel Mellado, Eduardo Fernández-Medina, Mario Piattini: Security requirements engineering framework for software product lines. *Information & Software Technology* 52(10): 1094-1117 (2010)

[NIS11] NIST, *Cloud Computing Reference Architecture*. 2011:
http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

[NIS13] NIST, *Cloud Computing Security Reference Architecture*, NIST Special Publication 500-299.

[OPE] The Open Group Cloud Ecosystem Reference Model, http://www.opengroup.org/cloud/cloud.htm

OSG, http://www.osgi.org/wiki/uploads/CommunityEvent2012. pdf

[Rag15] D. Ragget, "The web of things: Challenges and opportunities", *Computer*, IEEE, May 2015, 28-32.

[Sad15] A.R.Sadeghi, C.Wachsmann, M. Waidner, "Security and privacy challenges in industrial Internet of Things", *ACM DAC'15*, June 2015, San Francisco, CA.

[She15] Shaun Shei, Luis Márquez Alcañiz, Haralambos Mouratidis, Aidan Delaney, David G. Rosado, Eduardo Fernández-Medina: Modelling secure cloud systems based on system requirements. *ESPRE 2015:* 19-24

[Sto14] I. Stojmenovic and S. Wen, "The Fog Computing paradigm: Scenarios and security issues", *Procs. of the 2014 Fed. Conf. on Comp. Sci. and Info. Systs, (*ACSIS), 1-8.

[Sye15a] Madiha H. Syed and E. B. Fernandez, "The Software Container pattern", *22nd Conference on Pattern Languages* of Programs 2015, Pittsburgh, PA, October 24-26, 2015.

[Sye15b] Madiha H. Syed, E.B.Fernandez and M. Ilyas, "A Pattern for Fog Computing", *Procs. VikingPLoP* 2016.

[Sye15c] Madiha H. Syed and E.B.Fernandez, "Cloud ecosystems support for Internet of Things and DevOps using patterns", *First International Workshop on Interoperability, Integration, and Interconnection of Internet of Things Systems (I4T)*, part of the IEEE Int. Conf. on Cloud Engineering (IC2E), Berlin, Germany, April 4-8, 2016.

[Tah14] A. Taherkordi and F. Eliassen Towards Independent in-Cloud Evolution of Cyber-Physical Systems, *The 2nd IEEE International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA 2014*), Hong Kong, China, Aug. 2014.

[Was15] H. Washizaki, S. Fukumoto, M. Yamamoto, M. Yoshizawa, Y. Fukazawa, T. Okubo, S. Ogata, E.B. Fernandez, H. Kaiya, T. Kato, A. Hazeyama, N. Yoshioka , "A Metamodel for Security and Privacy Knowledge in Cloud Services", submitted for publication.

[Woo79] C. Wood, R. Summers, and E. B. Fernandez, ``Authorization in Multilevel Database Models," *Information Systems*, Vol 4, pp. 155-161, 1979.

[Yim15] D. Yimam and E. B. Fernandez, "Building Compliance and Security Reference Architectures for Cloud Systems", *IEEE Int. Conf. On Cloud Engineering (IC2E) 2016*, Berlin, April 4-8, 2016.

[YiS15] S. Yi, Z. Hao, Z.Qin, Q. Li, "Fog computing: Platform and applications", *2015 Third Int. IEEE Workshop on Hot Topics in Web Systems and Technologies*, 2015, 73-78.