Proc. of the Intl. Conf. on Advances In Information Processing And Communication Technology - IPCT 2014.

ISBN: 978-1-63248-021-7 doi: 10.15224/ 978-1-63248-021-7-90

Semantically Enhanced Cyber Security over Clouds: Methodological Approach

Ramo Šendelj, Ivana Ognjanović

***Abstract*—Cloud computing is achieving increased popularity among both, researchers and practitioners; while security is one of the major issues which reduces its growth and complications with data privacy and data protection continue to plague the market. Stimulated by the promising solutions of Semantic Web (also known as Web 3.0) for addressing the problems of management and monitoring of services shared by different parties (with different semantics and interests), the service-oriented transformations over cloud-computing processes are today a rapidly growing demand. In this paper we go one step further and propose methodology for increasing cyber security over cloud services by using Semantic Web technology, hierarchical ontology and intelligent reasoning techniques.**

***Keywords*—cyber security, cloud computing, semantic technologies, intelligent reasoning**

I. Introduction

Nowadays, we are witnessing that cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. The term 'cloud computing' is popular and suddenly everywhere, with government leaders, industry executives, and the press all talking excitedly about this new concept [1]. The basic idea behind cloud computing is replacing computing as a personal commodity by computing as a public utility (from storing data to community via e-mail to collaborating on documents or crunching numbers on large data sets). As defined in [12] it is '*an emerging computing paradigm that promotes delivery of applications to users as services over the Internet while keeping the hardware, systems software and system maintenance away from her*'.

Despite of all the hype surrounding the cloud, enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. The main concern that is beginning to grow is about just how safe an environment it is, as more and more information on individuals and companies (hereinafter, participant) are placed in the cloud. Each participant has a different business strategy and thereby may stress some specific security aspects over others, and the implications of security breaches are confounded by the dynamics of communications and collaborations that occur throughout the network in the normal course of business. Furthermore, each participant operates autonomously and has legal and business control over its internal operations, data and other resources, and it is hardly to be expected that there exist homogeneity and compatibility between all parties. Traditional methods for collaboration between distributed systems include static and centralized approaches, trusted third party approaches and dynamic negotiation, which obviously expressed weaknesses associated with maintaining the security of the central security policy repository.

Stimulated by the promising solutions of Semantic Web (also known as Web 3.0) for addressing the problems of management and monitoring of services shared by different parties (with different semantics and interests), the service-oriented transformations over cloud-computing processes are today a rapidly growing demand in almost all sectors. Recent research is focused on making synergistic solutions for sevice-oriented applications over clouds in the form of Business Process Families (BPFs) that are being configured for each participant independently [11]. Methods with tool support for semi-automated integration are proposed in [13], that heavily uses ontologies [14] and Semantic Web technologies [15] for semantic annotation of BPFs.

In this paper we go one step further, and extend proposed model in [13] by addressing cyber security issues [16] and using intelligent reasoning techniques to maximize usability, efficiency, legal foundations and the security of a service-oriented architecture of clouds. However, we provide knowledge and methods to design and implement semi-automated semantically-enabled cyber-security system over cloud-computing environment (and its instances).

II. Proposed Model

Cloud computing is an emerging computing paradigm that promotes delivery of applications to users as services over the Internet [1, 2, 3] while each service is customized to each specific participant and its requirements. Therefore, each BPF in the cloud is specified with Business Process Family Models (BPFMs) (as proposed in [17]) and specific BPF is configured by selecting the desired features of the family. The BPFM is composed of feature models (FM) (representing all possible features of family members), Business Process Model Template (BPMT) (representing all business process variants) and corresponding mapping between two models. In the context of BPFs in the cloud, FM, BPMT and mapping models

RamoŠendelj
University of Donja Gorica
Montenegro
ramo.sendelj@gmail.com

Ivana Ognjanović
University Mediterranean, Faculty of Information technology
Montenegro
ivana.ognjanovic@unimediteran.net

Proc. of the Intl. Conf. on Advances In Information Processing And Communication Technology - IPCT 2014.

ISBN: 978-1-63248-021-7 doi: 10.15224/ 978-1-63248-021-7-90

are deployed to an external location on the Internet, while each instance has his own customized configuration of the family.

The requirements (functional, non-functional, security) of the new application are investigated through the analysis phase. Business processes are developed by reviewing business goals and objectives and addressing security issues. In the analysis phase, business processes and services are identified and specified in a stepwise manner [41].
By following the same conceptual approach, we consider family model of cyber security issues over BPMFs as overall general model of artefacts specifying the security concerns in cloud computing environment. Many researchers have recently analyzed cyber security information that should be identified, exchanged and measured [16, 18, 19]. Ontological approach has been shown as the most promising, giving holistic perspective of cyber security operations and providing categories of cyber security operational information [20]. The complexity of ontological structure is imposed by abstracting the heterogeneity in semantics, technical, legal and other aspects and additional issues of providing the non-functional characteristics that should be used for measuring security thresholds.

On the other side, since all cloud computing deployment approaches are not the same, while different, they are still considered to have models that are possible to be integrated. For the purpose of this paper, motivated by promising results in BPFMs [21, 22], we will assume that one integral hierarchical structure (hereinafter, Cyber Security Model-CSM) could heavily cover all semantic diversity in characteristics, relationships and dependencies between cloud computing models and all involved parties. It builds upon the framework proposed in [23], and illustrated in Figure 1.

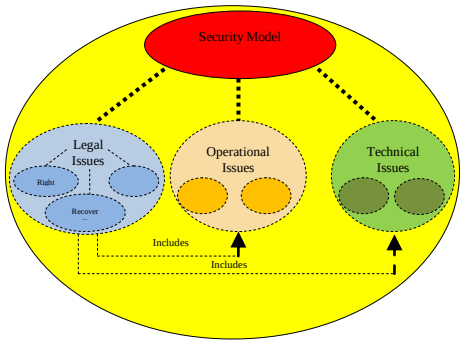

Figure 1. Hierachical ontological structure (Cyber Security Model-CSM)

Similarly to BPFM, these ontologies and hierarchical structure of CSM are deployed to an external location on the Internet, while each instance has his own customized configuration of the family, i.e. each ontological concept is assigned the value characterizing selected feature in the model.

Furthermore, as shown in [24], by having specific vales for each ontological concept, aggregation operations should be used in order to provide overall values of cyber security concerns for each instanced BPF. Quantitative measures are provided in [18], enabling rationalization of related decision making.

Methodologically, integration of CSM simultaneously to integration of BPFM is depicted in Figure 2. It is built as extension of the framework proposed in [13], and upon the framework proposed in [21, 22] representing common practice in BPMFs. In our methodology, final result of *Requirement Engineering*, *Domain Design and Realisation* and *Application Engineering* phases, is integrated and configured BPF (in addition to [13] which does not address *Application Engineering* phase) with assigned cyber security values for all constitutive elements (e.g. services, platforms, applications, etc.) and the model as a whole.

In the Requirement engineering phase we propose the following activities (as extension to those proposed in [13]):

- *Examination* of relationships between features of independent families by employing ontologies and Semantic Web technologies. For example, considered on clouds, the same business process by intention may have different actual realizations (e.g. some services and/or sub-processes should be executed before the other one, etc). It imposes relations between hierarchies in CSM and/or among them.
- *Verification and Validation* of relationships in FM and concepts and relations in CSM (validation with both, target customers and developers, and their legal and operational issues, while verification mechanisms [25] should be applied for checking inconsistencies).
- *Integration selection* is an activity where an integration approach is decided among each specific relations between features in FM, and appropriate aggregation approaches are decided at each level in CSM hierarchy by respecting constraints and relations in FM (mostly often by provision on bottom-up approach [24])
- *Transformation* is the final activity resulting with FM of the integrated family and CSM over it. Furthermore, mapping between FM and CSM is specified enabling assigning values specific to concrete FM realisation with services, as follows in the next phase.

In the next phase of *Domain design and implementation*, the same activities are proposed, finally resulting with BPMT and annotated CSM. The following activities are proposed:

- *Examination* of relationships between business processes in BPM
- *Verification and validation* of relationships for semantic and well-formedness
- *Integration selection*, i.e. the selection of predefined integration options and extension of aggregating approaches over CSM hierarchy in accordance with relations and constraints in BPMT

Proc. of the Intl. Conf. on Advances In Information Processing And Communication Technology - IPCT 2014.

ISBN: 978-1-63248-021-7 doi: 10.15224/ 978-1-63248-021-7-90

- *Transformation* from input BPMTs to the integrated BPMT with assigned CSM.

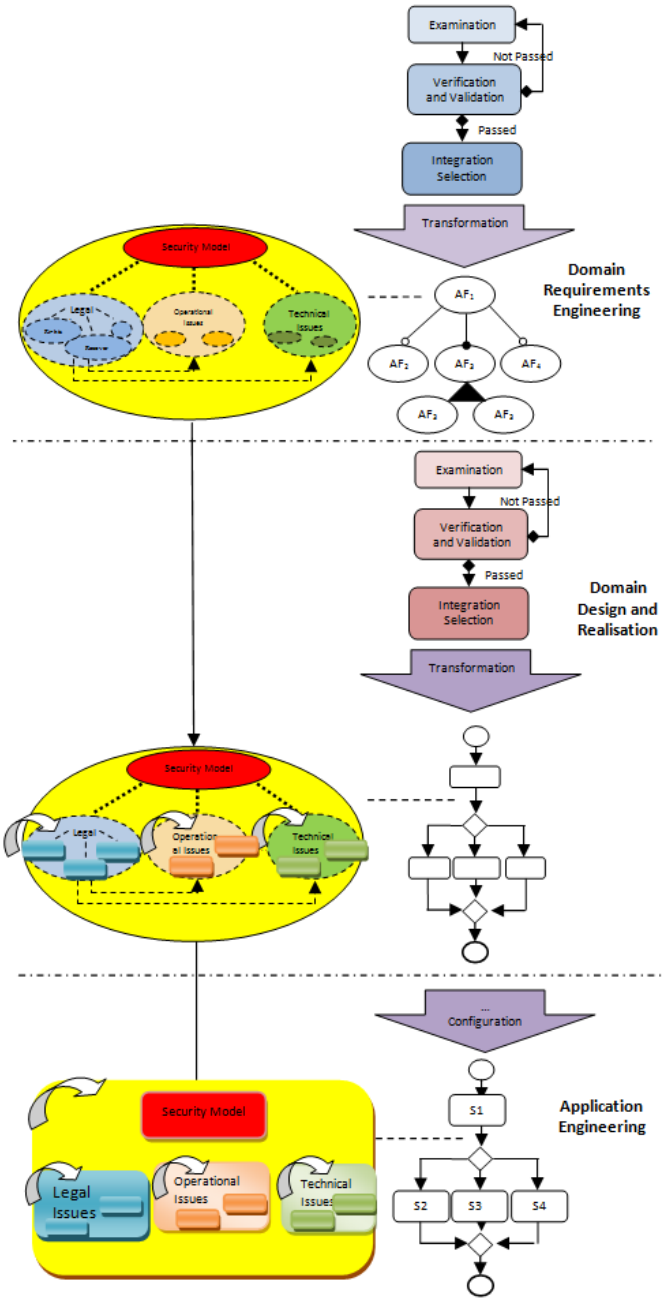

Figure 2.Integration of cyber security model with business process families over cloud

Finally, during *Application Engineering* phase, specific features are selected (by respecting all defined relations and constraints) and configured (by selection of appropriate services from available). It imposes final configuration of CSM, generated in two steps:

- *Configuration* by selection of appropriate services in BPMT and corresponding values of security concerns in CSM at the lowest level of the hierarchy
- *Propagation of values* in configured CSM, by application of specified aggregation rules having inputs of specific values at the lowest values of the hierarchy.

This paper is not focused on making analyses of requirements by which fulfilment the set of appropriate services is selected in the model. Its selection directly gives security values in CSM, which implicitly put security requirements as additional group of requirements that should define selection process.

III. Foundations

A. *Ontology over Clouds*

Use of ontology toward cyber security in cloud computing is recently analysed by considering and analysing actual cyber security operations in the context of non-cloud computing [20]. Ontology proposed in [20] can be used for providing a framework for sharing and reutilizing cyber security operational information over clouds. It analyses three domains of cyber security operations: IT Asset Management (with entities Administrator and IT Infrastructure Provider), Incident Handling (with entities Response Team and Coordinator) and Knowledge Accumulation (with entities Researcher, Product & Service Provider, and Registrar).

On the other side, hierarchical structure of security ontology is proposed in [28], by specifying three sub-ontologies at first level: security, enterprise, and location. Security sub-ontology further has five concepts: attribute, threat, rating, control and vulnerability, etc.

Information security ontology proposed in [29] integrates aspects of human-behavioural implications resulting from information security management decisions, before security controls are deployed.

In [26], a security management framework is proposed for an arbitrary information system, by developing security ontology with reusable security knowledge interoperability, aggregation and reasoning exploiting security knowledge from diverse sources. It also addresses the separation of security requirements from their technical implementations facilitates the security management.

Also related to our approach, [27] proposes vulnerability-centric approach for constructing security ontology since weaknesses can be identified in the requirements, design and implementation phases. This ontology gives a framework for integration of vulnerabilities into the security requirements and their relationships.

The viewpoint proposed in this paper is on integration of actual ontologies having different concerns and viewpoints, while the promising solution is on creation of hierarchical structure with relations and constraints often used in semantic technology environment [23].

Proc. of the Intl. Conf. on Advances In Information Processing And Communication Technology - IPCT 2014.

ISBN: 978-1-63248-021-7 doi: 10.15224/ 978-1-63248-021-7-90

B. *Intelligent Reasoning*

An aspect of intelligent reasoning techniques used in this paper is focused on making sophisticated analyses over hierarchical ontological structure, making aggregation operations (respecting defined constraints and relations) and making predictions and estimations of security threshold values in the model.

There is a variety of methods and techniques primary developed in other fields, such as data mining, operational research, databases etc. As shown in [7], there is no general best fitting approach, and the most appropriate one should be selected in accordance with domain characteristics and semantic structure. In the following we outline just a few methods in beneficial domains, but not limiting on them.

- *Data mining techniques* [40] can be used for revealing patterns among collected data; on what basis clustering techniques (k-means, hierarchical clustering, rule generation, etc.)[39, 38] can be applied for classifying security concerns and determination of their threshold values;
- Methods for quantitative and qualitative analyses of requirements, among which the most well-known and widely used are AHP [9], TCP-nets and CP-nets [5], cp-theory [6], etc. These methods can be applied in order to prioritize available services by defined requirements
- Mostly related to our work, the aggregation scheme of non-functional characteristics over BPMs proposed in [10] is extended by respecting variability in BPMFs giving an aggregation model for QoS computation which takes both variability and composition patterns into account [24]. Similar approach should be applied over CSM by taking into account patterns in BPMT and relations and constraints among and over hierarchies in CSM.

C. *Legal and Operational Issues over Clouds*

Legal issues over clouds include consideration of jurisdictional issues, an understanding and the evaluation of cloud stakeholder rights, and technical approaches to addressing the associated legal and jurisdictional issues. More specifically, legislatives and legal procedures should arrange the following [4, 36, 16, 18]: (i) compliance with laws and industry regulation and its requirement (i.e. laws, technical, legal, compliance, risk, and security); (ii) Understand the contractual responsibilities of each party; (iii) Determine how existing compliance requirements will be impacted by the use of cloud services, for each workload (i.e., set of applications and data), in particular as they relate to information security; (iv) Specialized compliance requirements for highly regulated industries (e.g., finance, health care); (v) make agreement between customers and providers how to collect, store, and share compliance evidence (e.g., audit logs, activity reports, system configurations), etc.

IV. The proposed Highly Secured Support for Cloud Computing

As shown on Figure 3, benefits of using hierarchical ontological approach of cyber security issues over clouds integrated with semantically enabled service families, are multiple and may be applied for each instance of the family.

More specifically, proposed CSM should be constructed during Domain Engineering and Domain Design and Realisation phases, and later configured during Application Engineering phase. Additionally, after obtaining the final instance of family (i.e. final software system on clouds), the same model can be used for monitoring security values of its each component during the whole cyber life-cycle activities (i.e. prevention, detection, (re-)action, retrieval, etc.).

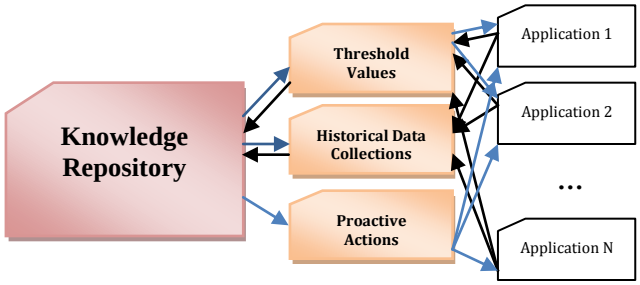

Figure 3. Knowledge Repository

More specifically, the following activities are recognised:

- *Continual support to checking threshold values* aimed on periodical measuring all security values in CSM, their aggregation and identification of potential violation of the permitted thresholds;
- *Creation of Knowledge Repository* representing stored historical data of security values over the model. The repository should contain records of each periodical measuring of security values over CSM for each individual instance. In this paper we do not address the issue of legal and ownership issues over the Repository since several providers may existing and each customer is sharing the resources.
- Dynamic changes in CSM and individual instances (for the aspect of security issues) imposed by constant changes and enriches in cyber attacks and threats, but identified, extracted and integrated from meaningful information from Knowledge Repository.

Theoretically, proposed CSM with Knowledge Repository should be self-adapted and semi-automated for processing meaningful information and generating security mechanisms and activities. Data mining and intelligent reasoning techniques are promising solutions, and the whole approach is built upon solutions and results presented in [40, 21, 22].

Proc. of the Intl. Conf. on Advances In Information Processing And Communication Technology - IPCT 2014.

ISBN: 978-1-63248-021-7 doi: 10.15224/ 978-1-63248-021-7-90

V. Related Work

Cloud computing is recently one of major challenges for researchers and scientific community in general. Several groups and organization are interested in developing security solutions and standards for the cloud. The potentials of semantic technologies in this filed are recognized by Cloud Computing Alliance [30]. Yet, the technological and legal realization of the vision is still in its infancy. There is no general framework for addressing this issue.

Some researchers are focused on development of tough security architecture (e.g. [31] proposes four-tier framework for web-based development), and making separate considerations of different deployment models of clouds [32, 33]. [33] proposes a cloud service broker model to serve as a trusted interface between the enterprise, cloud service providers and other organizations collaborating in a value network. Furthermore, a Trusted Third Party is proposed in [16] with defined specific tasks aimed on assuring specific security characteristics within a cloud environment. They make identification of user-specific security requirements and make categorization of threats accordingly. Proposed trusted third party has potentials to be relied upon for: (i) Low and High level confidentiality; (ii) Server and Client Authentication; and (iii) generating Security Domains; (iv) cryptographic Separation of Data, and (v) Certificate-Based Authorization.

The issue of providing security measurements over clouds is also partially addressed by many researchers, enabling analyses of cloud computing as a business model. [18] gives a quantitative model of security measurements that enables cloud service providers and cloud subscribers to quantify the risks they take with the security of their assets. Also, quantitative measurements can be used as a basis for making security related decisions in cloud environment. On the another side, [34] proposes division of security metrics between protective metrics and behavioral metrics. To this end, three security metrics are proposed, namely the MTTF (Mean Time to Failure), MTTCF (Mean Time to Catastrophic Failure) and MTTR (Mean Time of Repair). MTTF-metrics are also discussed in [35] defining the following metrics: mean time to incident discovery, incident rate; mean time between security incidents; vulnerability scan coverage; percentage of systems without known severe vulnerabilities, and many others.

To the best of our knowledge, there is no comprehensive approach enabling integration of all cyber security issues in one integral framework with defined metrics (quantitative and qualitative). Legal issues are also widely recognized and analyzed [32], supply chain security [37], economics, incentives and risks [36]. Our work is perfectly compatible with these works since we proposed hierarchical structure to integrate different security issues (presented with specific ontology due to its complexity, heterogeneity and shared parts).

VI. Conclusions and Future Work

In this paper, we have described a semantically enabled approach for improving security over service families in the Cloud. This approach has promising potentials due to proven benefits of using semantic Web technologies, and current trends in dynamic deploying of service process in the Cloud. Ontologies are also used to overcome heterogeneity and complexity in security over clouds, while semantic web technologies and intelligent reasoning techniques are proposed for making automatic identification, estimations and proactive security actions.

This model can be used as a solid basis for future work in this direction, which should include (i) verification and formal validation of the whole approach, (ii) development of tool support, and (iii) evaluation of the approach by applying it on realistic case studies.

References

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing." Communications of the ACM, 2010, 53(4), pp. 50-58

[2] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, and I. Brandic "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility." Future Generation computer systems, 2009, 25(6), pp. 599-616

[3] N.Daniel, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov "The eucalyptus open-source cloud-computing system", CCGRID, 2009

[4] D. C. Wyld, and R. Maurin, “Moving to the Cloud: An Introduction to Cloud Computing in Government”, IBM Centre for The Business of Government, 2009

[5] C. Boutilier, R. I, Brafman, C. Domshlak, H. H, Hoos, and D. Poole, “CP-nets: a tool for representing and reasoning with conditional ceteris paribus preference statements”, J.of AI Research,2004,21(1), pp.135-191

[6] C. Domshlak, “A Snapshot on Reasoning with Qualitative Preference Statements in AI”, In G. Riccia, D. Dubois, H. J. Lenz, and R. Kruse (Eds.), “Preferences and similarities”, 2008, Vol. 504, pp. 265-282

[7] I.Ognjanović, D.Gašević, and E.Bagheri, "A Stratified Framework for Handling Conditional Preferences: an Extension of the Analytic Hierarchy Process", Expert Systems with Applications, 2013, 40(4), pp.1094-1115

[8] M. McGeachie, and J. Doyle, “The local geometry of multiattribute tradeoff preferences”, Artificial Intelligence, 2011, 175(7-8), 1122-1152.

[9] T. L. Saaty, “The Analytic Hierarchy Process”. McGraw-Hill, New York, 1980

[10] J. Cardoso, A. P. Sheth, J. A. Miller, J. Arnold, J., and K. Kochut, “Quality of service for workflows and web service processes”,. J. Web Sem., 2004, pp. 281–308

[11] W. van der Aalst, “Configurable services in the cloud: Supporting variability while enabling cross-organizational process mining”, In: On the Move to Meaningful Internet Systems: OTM, Vol.6426 of LNCS, Springer, 2010, pp. 8-25

[12] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A View of Cloud Computing”, Communications of ACM, 53 (4), 2010, pp.50-58

[13] M. Bošković, E. Bagheri, G.grossmann, D. Gašević, and M. Stumptner, „Towards Integration of Semanticallz Enabled Service Families in the Cloud“, CSWS 2011, Vol. 774, pp.58-69

[14] T. R. Gruber, „Toward principles for the design of ontologies used for knowledge sharing“, Int. Journal on Human-Computer Studeis, Vol.43, 2010, pp.62-81

ISBN: 978-1-63248-021-7 doi: 10.15224/ 978-1-63248-021-7-90

[15] T. Berners-Lee, J. Hendler, and O. Lassila, „The semantic web“, Scientific American, 2001, pp. 29-37

[16] Z. Dimitrios, and L. Dimitrios, „Addressing cloud computing security issues“, Future Generation Computer Systems, 2012,Vol.28, pp.583-592

[17] K. Czarnecki, and U. W. Eisenecker, „Generative programming: methods, tools, and applications“, ACM Press/Addison-Wesley Pub.Co. 2000

[18] L. B. A. Rabai, M. Jouini, A. B. Aissa, and A. Mili, „A cybersecurity model in cloud computing environments“, J. of King Saud University-Computer and Information Sciences, 2013, vol. 25, pp.63-75

[19] S. Subashini, and V. Kavitha, „A survey on security issues in service delivery models of cloud computing“, J.of Network and Computer Applications, 2011, Vol.34, pp.1-11

[20] T. Takahashi, Y. Kadobayashi, and H. Fujiwara, „Ontological Approach toward Cybersecurity in Cloud Computing“, SIN 2010, pp.7-11

[21] M. Asadi, B. Mohabbati, D. Gasevic, E. Bagheri, and M.Hatala, “Developing Semantically-Enabled Families of Method-Oriented Architectures”, IJISMD, 2012, 3(4), pp. 1-26

[22] M. Boskovic, D. Gasevic, B. Mohabbati, M. Asadi, M. Hatala, N. Kaviani, J. J. Rusk, and E. Bagheri, “Developing Families of Software Services: A Semantic Web Approach”, Journal of Research and Practice in Information Technology, 2011, 43(3), pp. 179-208

[23] V. Schickel-Zuber, and B. Faltings, “OSS: A Semantic Similarity Function based on Hierarchical Ontologies”, IJCAI, 2007, pp.551-556

[24] B. Mohabbati, D. Gasevic, M. Hatala, M. Asadi, E. Bagheri, and M. Boskovic, “A Quality Aggregation Model for Service-Oriented Software Product Lines Based on Variability and Composition Patterns”, ICSOC 2011, pp. 436-451

[25] G. Gröner, C. Wende, M. Boskovic, F. S. Parreiras, T. Walter, F. Heidenreich, D. Gasevic, and S. Staab, “Validation of Families of Business Processes”, CAiSE 2011, pp. 551-565

[26] B. Tsoumas, D. Gritzalis, “Towards an Ontology-based Security Management”, AINA 2006, pp. 985-995

[27] G. Elahi, E. Yu, and N. Zannone, “A Modeling Ontology for Integrating Vulnerabilities into Security Requirements Conceptual Foundations”, Conceptual Modeling - ER 2009, Lecture Notes in Computer Science Vol. 5829, 2009, pp. 99-114

[28] S. Fenz, and A. Ekelhart, “Formalizing information security knowledge”, ASIACCS 2009, pp.183-194

[29] S. E. Parkin, A. van Moorsel, and R. Coles, “An information security ontology incorporating human-behavioural implications”, SIN 2009, pp. 46-55

[30] Cloud Security Alliance, Report: Security Guidance for Critical Areas of Focus in Cloud Computing V3.0

[31] W. Tsai, Z. Jin, and X. Bai, “Internetware computing: issues and perspectives”, 1st Asia-pacific symposium on Internetware, China, 2009, pp.1-10

[32] B. Hay, K. Nance, M. Bishop, “Storm Clouds Rising: Security Challenges for Iaas Cloud Computing”, 44th Hawaii Int. Conf. On System Scieneces, 2011

[33] H. Demirkan, M. Goul, “Taking value-network to the cloud services: security services, semantics and service level agreemnets”, Inf. Syst E-Bus Manage, 2013, Vol.11, pp.51-91

[34] E. Jonsson, L. Pirzadeh, “A framework for security metrics based on operational system attributes”, MetriSec2011

[35] B. B. Madana, K. Goševa-Popstojanovab, K. Vaidyanathanc, K. S. Trivedia, “A method for modeling and quantifying the security attributes of intrusion tolerant systems”, Performance Evaluation, 2004, Vol. 56, pp.167–186

[36] K. W. Hamlen, and B. Thuraisingham, “Data security services, solutions and standards for outsourcing”, Computer Standards and Interfaces, 2013, Vol.35, pp.1-5

[37] B. Thuraisingham, “Data supply chain management: supply chain management for incentive and risk-based assured information sharing”, UTD Technical Report, 2010

[38] N. Blaikie, “Analyzing Quantitative Data”, London: Sage, 2003

[39] M. Kaur, and U. Kaur, “Comparison Between K-Mean and Hierarchical Algorithm Using Query Redirection”, Int. J. of Advanced Research in Computer Science and Software Engineering, 2013, 3(7), pp.1454-1459

[40] S. K. Pal, and P. Mitra, “Pattern Recognition Algorithms for Data Mining”, Chapman and Hall/CRC, 2004

[41] M. Papazoglou, and W. Van Den Heuvel, “Service-oriented design and development methodology”, Int. J. of Web Engineering and Technology, 2006, 2(4), pp.412-442

About Author (s):

Ramo Šendelj, PhD is a Research Chair in field of Cyber Security at University of Donja Gorica, Montenegro. He was a Dean of Faculty of information technology, in period 2006-2013. He is Montenegrin Delegate in „European Strategy Forum on Research Infrastructures” and FP7 expert for Ethics reviewing.

Ivana Ognjanović, PhD has completed his PhD thesis in software engineering field at University of Belgrade, Serbia. She is a member of Semantic technologies group in Canada, led by Prof. Dragan Gašević. Currently she is working on several international and national projects.