J. Basic. Appl. Sci. Res., 4(1)90-96, 2014
© 2014, TextRoad Publication

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

A Decade of Domain Specific Modelling Languages for Model-Driven Security

Muhammad Qaiser Saleem

Assistant Professor, College of Computer Sciences and Information Technology, Al Baha University, Al Baha, Kingdom of Saudi Arabia

Received: October 18 2013
Accepted: December 3 2013

ABSTRACT

In Model-Driven development software system design is represented through models which are created using general purpose modelling languages e.g. UML. Later on system artefacts are automatically generated from these models. Model-Driven Security is a specialization of Model-Driven paradigm towards the domain of security, where security objectives are modelled along the system models and security infrastructures are directly generated from these models. Currently available general purpose modelling languages like UML do not have capability to model the security objectives along the system models. Over the past decade, many researchers are trying to address these limitations of the general purpose modelling languages and come up with several Domain Specific Modelling Languages for Model Driven Security. In this paper, we survey the progress made by these researchers in the area of Model Driven Security and discusses different security Domain Specific Modelling Languages presented by the most prominent researchers for the development of secure system.

KEYWORDS: Model Driven Architecture, Model Driven Security, Security Goals, Domain Specific Language, Software Modelling Languages.

1. INTRODUCTION

Many software engineering approaches are used for the development of software systems, among them; Model Driven Software Development (MDSD) is one of the most promising approaches. Object Management Group (OMG) has presented a framework known as Model Driven Architecture (MDA) [1], which is considered as implementation of Model Driven Engineering (MDE). In MDA framework, software systems are modeled using general purpose modeling language like UML, as a Platform Independent Model (PIM) and then it is transformed to Platform Specific Model (PSM) or Implementation Specific Model (ISM). In MDA framework, rather than just a visual aid, models are considered as essential part of software definition [2, 3].

During software modelling, concentration is towards modelling the functional correctness in the model; usually notion of security is often neglected. It may happen due to many reasons, one of the prominent reason is that the currently available software system modelling languages do not have ability to capture security objectives [4]. In practice security objectives are specified in a non-formalize way by the business department normally as an unstructured text. If these security specification are not understood by the IT security department; a complicated and error prone coordination process between both departments arises; resulting loss of requirement sovereignty by the business department which is owner of the application [5]. General purpose modelling languages like UML or BPMN; do not have capability of modelling the security objectives along modelling of the software system. To model the security objectives related to different aspects of software system; different security extensions are proposed by several authors.

Model Driven Security (MDS) is a specialization of MDSD towards the domain of security. The crucial part of this specialization is concern with the modeling language [6] for modelling security during designing the system which provides syntax and semantic as provided by the UML and BPMN. To fulfill the security requirements in modelling languages, many researchers have proposed several security Domain Specific Modeling Languages (DSMLs) or simply called as Domain Specific Languages (DSLs) by extending existing modeling languages like UML or BPMN, focusing different aspects of software development. Automatically developing software applications enriched with security configuration is a topic of interest among the research community and many research groups are trying to address the security problems for software applications [7-13]. This survey paper presents the work in the area of MDS and discusses different domain specific languages presented by the most prominent researchers in this area.

Composition of the paper is that, section two illustrates in detail the two basic concepts of background literature i.e. MDS and DSL. Section three describes in detailed the different prominent DSLs presented by different researchers in the area of MDS modeling. Finally the work is concluded in section four.

2. Foundation Concepts

Understanding of the concepts of MDS and DSL are necessary for the whole discussion, which are presented in this section

Corresponding author: Muhammad Qaiser Saleem, College of Computer Sciences and Information Technology, Al-Baha University, Al-Baha, Kingdom of Saudi Arabia: muhammad.qaiser.saleem@gmail.com

2.1 Model Driven Security

"*Model driven security is an engineering paradigm that specializes Model Driven Software Development towards Information Security*" [14]. The MDS is based on the MDSE and MDA where security requirements are realized at the model level and kept separate from the underlying security architecture. The MDS is an engineering discipline which is concerned with the integration of security requirements in all system development phases e.g. analysis, design, implementation, testing etc. [2]. The vision of the MDS is to provide a way for software engineers to bridge the gap between the system design requirements and security requirements by taking a model-centric approach. This in turn necessitated bridging the gap between security modelling languages and design modelling languages, leading to the notion of security-design modelling languages, such as the SecureUML [6].

In the MDS, security requirements are defined as a model during the designing phase and concrete security configuration files can be generated by the model transformation e.g. security concepts are modelled side by side with the business process modelling at the PIM level of abstraction and step-wise refined to further levels of abstraction i.e. PSM and ISM [10, 14-17]. Figure 1 illustrates the whole process.

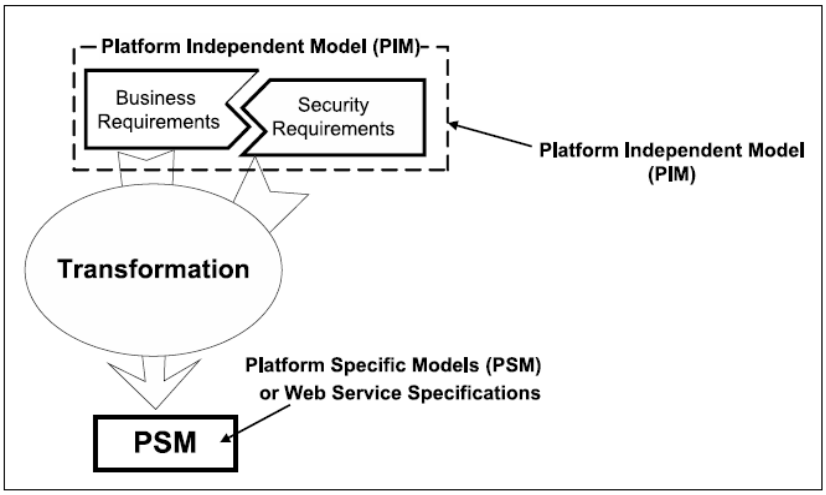

Fig 1. MDA Pattern with Security Extension [2]

These security objectives are defined in the model with the help of a DSL and transformed into enforceable security rules with a little human intervention. The MDS is a critical component of future Information Assurance (IA) architectures, especially for agile IT environments such as SOA [18].

2.2 Domain Specific Modelling Languages

Application structure, requirements and behavior according to a specific domain are formalized in the form of a DSL which is one of the components of the MDSD. A domain can be defined as " *a field of application delimitated by a specific area of interest*" [14]. A DSL is defined as " *A concise, precise and processable description of a viewpoint, concern or aspect of a system, given in a notation that suits the people who specify that particular viewpoint, concern or aspect.*" [14]. A DSL consists of constructs that capture information regarding the domain it describes[19]. A DSL may also be called a Domain Specific Modelling Language (DSML) [20].

There is a considerable body of accumulated theories and experience to assist programming language designers; however, this is not the case for the designers of modelling languages, which is still an emerging field with very few proven and established guidelines and patterns [21].

2.2.1 Importance of Domain Specific Language

General purpose modeling languages like UML do not raise the productivity to a sufficient level because they lake the domain-specific concepts [20]. General purpose modelling languages have a broader scope and there may be a situation where it is not appropriate for modelling of some specific domain e.g. security, real-time etc. Furthermore, there may be a situation when the syntax and semantics of the elements of the general purpose modelling language are not able to express the specific concepts of particular systems or there may be a situation when these element may be customized or restricted which is normally too general and too abundant [22].

For modeling a specific domain, general purpose modelling languages have three main limitations: lack of semantics, lack of visualization and lack of abstraction while preparing a model [23]. Same is case for the security i.e. these general purpose modelling languages do not support the specification of the domain of security [4, 13].

During the recent years, an important goal of the software researchers is to develop techniques where domain concepts are model in terms of design intent rather than the underlying implementation environment [2]. Extending a general purpose modelling language according to a particular domain and defining DSL is a common practice e.g. UML extensions according to specific business domains like data warehousing [24], business intelligence [25] and real-time systems [26], system aspect like security [12, 27] or concrete technologies like API (Application Programme Interface) for

different programming languages [28] etc. DSL is one the key concept in MDE [2]. DSL development requires language development expertise as well as domain knowledge [28]

As compared to the general purpose modelling languages, DSLs offer substantial gain in ease of use and expressiveness according to the specific domain according to which they are developed. DSLs results in several benefits such as considerable gain in productivity, reduction in maintenance cost and reducing the required domain specific expertise. DSLs are also called application oriented, special purpose, specialized or task specific languages. Appropriate notions related to the specific domain are usually beyond the notation offered by general purpose modelling language. General purpose modelling languages do not render the superfluous of DSLs and it is very clumsy for tasks that can benefits from the integration of the domain-specific restrictions [29].

2.2.2 Basic Concepts of DSL

A DSL consists of following three concepts [14].

1. *Abstract syntax:* defines the basic concepts, their relationships and the integrity constraints of a DSL[30] e.g. in the OMG's metamodel architecture, the UML Class diagram at the M2 level of abstraction [31]. Normally abstract syntax is defined through a metamodel [14].
2. *Concrete syntax:* defines the notion of the language, which will be used during modelling i.e. the front end of the DSL. These notions may be visual or textual [14]. For example UML notations [31].
3. *Semantic:* of a modeling language defines its meaning in context. Semantics are either defined formally or should at least be documented in an informal way [14]. For example, the natural language specification [31].

2.2.3 Definition Mechanisms/Types of DSL

The specification of a DSL that allows the software products to be represented without ambiguity at a conceptual level is one of the most important concerns when elaborating a Model-Driven development solution [32]. One of the major challenges, an architect of the MDE modelling languages faces is the abstraction challenge: " How can one provide support for creating and manipulating problem-level abstractions as first-class modelling elements in a language?" [19]. To tackle this challenge, two schools of thought have emerged in the MDE community: 1) The Extensible General-Purpose Modelling language School and 2) the Domain Specific Modelling Language School [19, 33, 34].

2.2.4 Current practice of defining MDS DSLs

There is no universal approach for the integration of security and design modelling languages [35-37]. The current practice of defining a DSL by different researchers [4, 16, 21, 27, 37-39] is that the abstract syntax of the DSL is represented by a metamodel and the concrete syntax is represented by a UML Profile.

3 Domain Specific Modeling Languages for Model-Driven Security

There is a plenty of interesting work, among them few of important related approaches presented by the prominent researchers are discussed below.

1. Basin David et al. [12, 16]; first time introduced the term Model Driven Security. They have presented "SecureUML" to model the security requirements for modelling static structure of the system. Basically it is a separate language based on Role Based Access Control (RBAC) protocol and its focus is to generate Access Control Policies from Abstract Authorization Constraints. They have presented a meta-model for abstract syntax and used UML profile for concrete syntax and security constraints are added through Object Constraints Language (OCL). The approach is flexible and afterwards SecureUML provides a schema to create other languages addressing different security aspects. Instead of adopting one-language-fit-for-all, they have proposed a general schema for integrating security requirements into system design models. In their work, they combined the SecureUML with a design modeling language based on class diagrams, known as Componenet UML, and later on with a language based on state diagram, known as ControllerUML [40]. Afterwards they combined the SecureUML with the language for modeling Graphical User Interfaces and given it name Action GUI [41]. They have considered two phases for the Model Driven Security; 1) Definition of abstract access control policies; and 2) Transformation to J2EE Deployment Descriptor Configuration. They have extended the system model with security stereotypes, which means the domain expert must have knowledge of security patterns to be used in a particular access control scenario.
2. Jan Jürjens et al. [42, 43] have extended the UML and presented a UML profile for the modelling of safety critical systems known as "UML-Sec". Their main idea is that the aspect of security should be considered throughout the whole system development process. They have used different UML models at various levels to capture security requirements like UML Class diagram for defining security for class attributes and functions, UML Sequence diagram for defining message security to exchange cryptographic data and UML Deployment diagram for defining security for physical components. Their work mostly focus the formal definition and validation of security by the developer, who already have knowledge of security, however they did not address how business department will address the security.
3. Michael Hafner and Ruth Breu have worked along the area of work-flow security and have proposed a MDS framework known as SECTET [7, 14, 44]. For their framework they have presented the two languages, SECTET-DSL (a DSL used to model the inter-organizational workflows) and SECTET-PL (a policy language used to define the abstract security policies). For SECTET-DSL, they have presented security stereotypes in UML activity diagram. In SECTET

framework, modelling is performed to represent two kind of views; workflow-view and interface-view. Basically in their work they are focusing work-flow security. M. Alam [2, 15, 45, 46] have also worked along the same direction and presented Role Based Access Control (RBAC) policy for distributed system. M. Memon [8, 47] have presented an enhanced form of SECTET framework and named it as SECTTISSIMO framework. In SECTTISSIMO framework; after PIM; a new layer is added naming Abstract Security Service Model to further elaborate the security requirements. He has extended the SECTET-DSL and used it in his framework. In their approach; abstract security policy is directly converted into code requiring the domain expert to have enough expertise to incorporate security pattern at early stages of system development.

4. Rodriguez A. et al. have created a meta-model for their security extensions and defined security stereotypes. They have assigned the different symbols to these security stereotypes. They used the same meta-model and security stereotypes for extending the two popular modelling languages i.e. BPMN [38] as well as UML [39]. They are working along the area of business process modelling. Most of their work remains at descriptive level and they only model the system with security annotation. Later on Rodríguez A. et al.[48] propose the generation of use-case views out of business process models which are examined for security requirements. They are defining security in term of general security and using MDA approach for defining security at PIM level of abstraction.

5. Christian Wolter et al. [4, 10] have introduced high-level security policies for different security objectives like confidentiality, integrity, authentication, authorization, availability and audit. For each security objective; they have presented a generic security policy model which captures the relations between basic entities like objects, attributes, their interactions and effects of these interactions. The model includes views on the enterprise architectural space which allows connecting elements from different perspectives. The security policy model maps the security goals to security constraints model, which are elaborated in the next phases. Michael Menzel et al. have worked along the same direction, [13] they have presented a meta-model for the model-driven generation of security policies for the SOA system. Meta-model describe the basic entities, their relations and associated roles (such as service and service consumer) in SOA environment and provide the foundation to model interactions and the exchange of information. They have introduced the security constraints on the security policies described by Christian Wolter et al. [10]. In [49] they proposed an approach to describe security requirements at the business process layer and their translation to concrete security configuration for SOA based system. They have introduced security objectives for business process modelling such as authentication, authorization, trust, data integrity and data confidentiality, system integrity and system availability. These security objectives are to be modeled in a business process model. These security objectives evaluate the trustworthiness of participants based on a rating of enterprise assets. Later on they tried to address the problems of security in services composition by providing a solution based on modeling concepts, semantic technologies and trust levels to express manage and negotiate security requirements in a technology-independent way [50]. They have mentioned the security pattern; however did not define anything how these patterns would be selected and used. In [36] they defined a modelling language for modelling security at system design level for SOA applications and named it as “SecureSOA”, it is an extension to the “SecureUML” by David Basin et al. [12, 16] for the service-based systems. They are not focusing some specific diagram rather discussing Fundamental Modeling Concepts (FMC) which can be used to model the structure of a system, processes in a system, and value domains of a system.

6. Saleem M. Q. et al [37] proposed a DSL named “UML-SOA-Sec” for the modelling of security objectives along business process modelling of SOA Applications. The metamodel of the proposed DSL is based on the essential security objectives for an SOA environment. Afterwards, a UML profiling mechanism is used for the definition of these security objectives as stereotypes in a modelling language. After the definition of the domain specific UML-profile, general-purpose modelling tool is specialized and these domain specific stereotypes are made available at the modelling level in the form of annotation. In their work they have tried to facilitate the business process expert in modeling the security objectives along the business process modeling of SOA applications. Business process expert is not a security expert; he/she is familiar with the basic security concepts through which he/she model the security in the business process model. Later on it’s the responsibility of the architecture team to realize these security objectives present in the business process model and choose potentially better security solutions.

The whole discussion is summarized in table 1.

Table 1. Model Driven Security Modeling Languages Presented by the Most Prominent Researcher

S/No	Researchers	Phenomenon Focused in related Work					
		Security Objectives Focused	**Proposed Work**	**Target Architecture**	**Focused Modelling Language**	**Focused System Aspect**	**Focused Professional**
1	David Basin et al.	Role Based Access Control	Security Policies SecureUML (UML profile)	Not Mentioned	UML	Static System Aspect e.g. UML Class diagram	Business Domain Expert having Strong Security Knowledge
2	Jan Jürjens et al.	Covering Different Mechanism for Distributed Systems	UML-Sec (UML Profile)	Distributed Systems	UML	Whole System Development Process	Developer/Security Expert
3	Michal Hafner and Ruth Breu	Role Based Access Control	SECTET-DSL	SOA	UML	Work-Flow Security (UML Activity Diagram)	None
4	M. Memon	Authentication, Non-repudiation	Security Pattern	SOA	UML	Work-Flow Security (UML Activity Diagram)	Business Domain Expert having Strong Security Knowledge
5	Alfonso Rodríguez et al.	Non-repudiation, Attack harm detection, Integrity, Privacy, Access control	Domain Specific Language	Not Mentioned	UML and BPMN	Business Process Modelling (UML Activity diagram and BMPN)	Business Department
6	Christian Wolter et al.	Confidentiality, Integrity, Authentication and Authorization, Availability and Auditing	Security Policy, Policy Constraint Model	SOA	No Specific Language	Business Process Model	Business Domain Expert
7	Michal Menzel et al.	Authentication, Authorization, Trust, Data Integrity and Data Confidentiality, System Integrity and System Availability	Security Policies.	SOA	BPMN	Business Process Model	None
8	Michal Menzel et al.	User Authentication, Non-repudiation, Identity Provisioning, Data Authenticity, Data Confidentiality, Trust	A DSL Called SecureSOA	SOA	Fundamental Modelling Concepts (FMC), Compositional Structure Diagrams	Business Process Model	None
9	Saleem M. Q. et al.	Confidentiality, Integrity, Availability, Auditing, Non-repudiation, Authentication, Authorization	A DSL called "UML-SOA-Sec"	SOA	UML	Business Process Model	Business Process Expert

4 Conclusion

This work have tried to compile the work of different researchers which are working in the area of MDS and presented different DSLs for security modeling along the modeling of the different aspect of software systems. We believe our efforts will facilitate the practitioners in selecting the most suitable DSL for their work. Furthermore, our efforts will facilitate the beginners in this area to get a picture of already presented work which will serve him/her as a basis for understanding the area of MDS and DSL and provide basis for further improvements in the said areas.

Acknowledgment

The authors declare that they have no conflicts of interest in this research.

REFERENCES

[1] OMG, "OMG Model Driven Architecture," *http://www.omg.org/mda/ (Date Accesed 30-10-2011).*

[2] M. Alam, "Model Driven Realization of Dynamic Security Requirements in Distributed Systems," *Phd Dissertation, University of Insbruck, Austria,* 2007.

[3] A. Rodríguez, *et al.*, "Towards CIM to PIM Transformation: From Secure Business Processes Defined in BPMN to Use-Cases," in *Business Process Management*, ed, 2007, pp. 408-415.

[4] M. M. Christian Wolter, Christoph Meinel, "Modelling Security Goals in Business Processes," *Proc. GI Modellierung 2008, GI LNI 127, Berlin, Germany,* vol. pp. 197 - 212, March 2008.

[5] H. Klarl, *et al.*, "Identity Management in Business Process Modelling: A Model-Driven Approach," in *Konzepte, Technologien, Anwendungen: 9. Internationale Tagung Wirtschaftsinformatik, Wien, 25 -27. Februar 2009. Teil 1*, H. R. Hansen, *et al.*, Eds., ed Wien: Ã–sterreichische Computer Gesellschaft, 2009, pp. 161-170.

[6] M. C. David Basin, Marina Egea, "A decade of model-driven security," presented at the Proceedings of the 16th ACM symposium on Access control models and technologies, Innsbruck, Austria, 2011.

[7] R. B. Michal Hafner, Berthold Agreiter, "SECTET: an extensible framework for the realization of secure inter-organizational workflows," *Emeral, Internet Research,* vol. Vol.16 No. 5 pp. pp.491-506, 2006.

[8] M. H. Mukhtiar Memom, Ruth Breu, "SECTISSIMO: A Platform-independent Framework for Security Services," *MODSEC08 Modeling Security Workshop,* 2008.

[9] M. T. Yuichi Nakamura, Takeshi Imamura, and Koichi Ono, "Model-driven security based on a Web services security architecture," in *IEEE International Conference on Services Computing, 2005*, 2005, pp. 7-15 vol.1.

[10] M. M. Christian Wolter, Christoph Meinel, Andreas Schaad, Philip Miseldine, "Model-driven business process security requirement specification," *J. Syst. Archit.*, vol. 55, pp. 211-223, 2009.

[11] J. Jurjens, "UMLsec: Extending UML for Secure Systems Development- Tutorial," presented at the Proceedings of the 5th International Conference on The Unified Modeling Language, 2002.

[12] D. B. Torsten Lodderstedt, Jürgen Doser, "SecureUML: A UML-Based Modeling Language for Model-Driven Security," presented at the Proceedings of the 5th International Conference on The Unified Modeling Language, 2002.

[13] C. M. Michael Menzel, "A Security Meta-model for Service-Oriented Architectures," in *IEEE International Conference on Services Computing, SCC '09'.* , 2009, pp. 251-259.

[14] R. B. Michal Hafner, "Security Engineering for Service-Oriented Architectures," *Springer-Verlag Berlin Heidelberg,* 2009, .

[15] M. Alam, "Model Driven Security Engineering for the Realization of Dynamic Security Requirements in Collaborative Systems," *MoDELS 2006 Workshops, LNCS 4364, pp. 278–287. Springer-Verlag Berlin Heidelberg,* 2007.

[16] D. Basin, *et al.*, "Model driven security: From UML models to access control infrastructures," *ACM Trans. Softw. Eng. Methodol.*, vol. 15, pp. 39-91, 2006.

[17] Y. N. Fumiko Satoh, Nirmal K. Mukhi, Michiaki Tatsubori, Kouichi Ono, "Methodology and Tools for End-to-End SOA Security Configurations," in *IEEE Congress on Services - Part I, 2008.*, 2008, pp. 307-314.

[18] R. S. Ulrich Lang, "Top SOA Security Concerns & OpenPMF Model-Driven Security," *ObjectSecurity white-paper, Topics Cloud Computing and Security Management,* 2009.

[19] R. France and B. Rumpe, "Model-driven Development of Complex Software: A Research Roadmap," in *Future of Software Engineering, FOSE '07*, 2007, pp. 37-54.

[20] M. M. Tomaž Lukman, "Model-Driven Engineering and its introduction with metamodeling tools," *9th International PhD Workshop on Systems and Control: Young Generation Viewpoint, Izola, Slovenia,* October 2008.

[21] B. Selic, "A Systematic Approach to Domain-Specific Language Design Using UML," in *10th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing, ISORC '07.* , 2007, pp. 2-9.

[22] A. V.-M. Lidia Fuentes-Fernández, "An Introduction to UML Profiles," *UPGRADE, the European Journal for the Informatics Professional,* vol. V, No. 2, April 2004.

[23] S. Brahe and K. Østerbye, "Business Process Modeling: Defining Domain Specific Modeling Languages by Use of UML Profiles," in *Model Driven Architecture – Foundations and Applications,* ed, 2006, pp. 241-255.

[24] S. Luján-Mora, Trujillo, Juan, Song, Il-Yeol, "Extending the UML for Multidimensional Modeling," in *UML 2002, LNCS 2460, pp. 290-304, 2002,* ed: Springer-Verlag Berlin Heidelberg 2002, 2002, pp. 265-276.

[25] V. L. Stefanov, Beate Korherr, Birgit, "Extending UML 2 Activity Diagrams with Business Intelligence Objects," in *Data Warehousing and Knowledge Discovery*, ed, 2005, pp. 53-63.

[26] R. D. Passerone, W. Ben Hafaiedh, I. Graf, S. Ferrari, A. Mangeruca, L. Benveniste, A. Josko, B. Peikenkamp, T. Cancila, D. Cuccuru, A. Gerard, S. Terrier, F. Sangiovanni-Vincentelli, "Metamodels in Europe: Languages, Tools, and Applications," *Copublished by the IEEE CS and the IEEE CASS,* vol. 26, pp. 38-53, 2009.

[27] J. Jürjens, "UMLsec: Extending UML for Secure Systems Development," in *«UML» 2002 — The Unified Modeling Language,* ed, 2002, pp. 1-9.

[28] M. Mernik, *et al.*, "When and how to develop domain-specific languages," *ACM Comput. Surv.*, vol. 37, pp. 316-344, 2005.

[29] J. u. D. Achim D. Brucker, "Metamodel-based UML Notations for Domain-specific Languages," *4th International Workshop on Language Engineering (atem 2007), pp. 1-{??}*, 2007.

[30] J. S. Kai Chen, Sandeep Neema, "Toward a semantic anchoring infrastructure for domain-specific modeling languages," *in 5th International Conference on Embedded Software, EMSOFT 2005, pp. 35-43*, 2005.

[31] C. Atkinson and T. Kuhne, "Model-driven development: a metamodeling foundation," *Software, IEEE*, vol. 20, pp. 36-41, 2003.

[32] B. Selic, "The pragmatics of model-driven development," *Software, IEEE*, vol. 20, pp. 19-25, 2003.

[33] B. M. GIOVANNI GIACHETTI, OSCAR PASTOR, "INTEGRATION OF DOMAIN-SPECIFIC MODELING LANGUAGES AND UML THROUGH UML PROFILE EXTENSION MECHANISM," *International Journal of Computer Science and Applications, © Technomathematics Research Foundation*, vol. Vol. 6, No. 5, pp 145-174, 2009.

[34] K. H. James Bruck, "Customizing UML: Which Technique is Right for You?," *IBM , http://www.eclipse.org/modeling/mdt/uml2/docs/articles/Customizing_UML2_Which_Technique_is_Right_For_You/article.html (Date Accesed 18-11-2008)*, 2008.

[35] T. Lodderstedt, "Model driven security: from UML models to access control architectures," *PhD Disertation, Albert-Ludwig University of Freiberg, Germany*, March 2004.

[36] C. M. Michael Menzel, "SecureSOA Modelling Security Requirements for Service-Oriented Architectures," in *IEEE International Conference on Services Computing (SCC)*, 2010, pp. 146-153.

[37] M. Q. Saleem, Jafreezal. Jaafar, M. Fadzil Hassan., "Secure Business Process Modelling of SOA Applications using UML-SOA-Sec," *International Journal of Innovative Computing, Information and Control (IJICIC),*, vol. 8, No. 4, pp 2729-2746, April 2012.

[38] F.-M. E. Rodríguez Alfonso, Piattini Mario, "A BPMN Extension for the Modeling of Security Requirements in Business Processes," *IEICE - Trans. Inf. Syst.*, vol. E90-D, pp. 745-752, 2007.

[39] A. Rodríguez, Fernández-Medina, Eduardo, Piattini, Mario, "Towards a UML 2.0 Extension for the Modeling of Security Requirements in Business Processes," in *Trust and Privacy in Digital Business*, ed, 2006, pp. 51-61.

[40] J. D. David Basin, Torsten Lodderstedt, "Model driven security: From UML models to access control infrastructures," *ACM Trans. Softw. Eng. Methodol.*, vol. 15, pp. 39-91, 2006.

[41] C. M. Basin David, Egea Marina, Schläpfer Michael, "Automatic Generation of Smart, Security-Aware GUI Models " *Springer-Verlag Berlin Heidelberg, ESSoS 2010, LNCS* vol. 5965, pp. 201-217, 2010.

[42] J. Jürjens, "UMLsec: Extending UML for Secure Systems Development," in *«UML» 2002 — The Unified Modeling Language*. vol. 2460, J.-M. Jézéquel, *et al.*, Eds., ed: Springer-Verlag Berlin Heidelberg, 2002, pp. 1-9.

[43] J. J. Bastian Best, Bashar Nuseibeh, "Model-Based Security Engineering of Distributed Information Systems using UMLsec," *ICSE '07 Proceedings of the 29th international conference on Software Engineering , IEEE Computer Society Washington, DC, USA ©2007* pp. 581-590, 2007.

[44] K. B. Ruth Breu, Michael Hafner, Jan, Jürjens, Guido Wimmel,Volkmar Lotz, "Key Issues of a Formally Based Process Model for Security Engineering," *In Proceedings of the 16th International Conference on Software & Systems Engineering and their Applications (ICSSEA03)*, 2003.

[45] B. R. Alam M. M., Breu M., "Model driven security for Web services (MDS4WS)," in *8th International Multitopic Conference, 2004. Proceedings of INMIC 2004.* , 2004, pp. 498-505.

[46] M. H. M. Alam, M. Memon, and P. Hung, "Modeling and Enforcing Advanced Access Control Policies in Healthcare Systems with SECTET.," *In MOTHIS '07: MODELS 2007, Nashville, USA*, 2007.

[47] M. Memon, "Security Modeling with Pattern Refinement for Security-as-a-Service Architecture," *Phd Dissertation, University of Insbruck, Austria, ,* January 2011.

[48] F.-M. E. Rodríguez Alfonso, Piattini Mario, "Towards CIM to PIM Transformation: From Secure Business Processes Defined in BPMN to Use-Cases," in *Business Process Management*, ed, 2007, pp. 408-415.

[49] I. T. Michael Menzel, Christoph Meinel, "Security Requirements Specification in Service-Oriented Business Process Management," in *International Conference on Availability, Reliability and Security, ARES '09.*, 2009, pp. 41-48.

[50] I. T. Michael Menzel, Christian Wolter, Christoph Meinel, "SOA Security - Secure Cross-Organizational Service Composition," *Proc. Stuttgarter Softwaretechnik Forum (SSF), Fraunhofer IRB-Verlag, Stuttgart, Germany, pp. 41 - 53*, November 2007. .