**Software Engineering**
2019; 7(2): 30-38
http://www.sciencepublishinggroup.com/j/se
doi: 10.11648/j.se.20190702.12
ISSN: 2376-8029 (Print); ISSN: 2376-8037 (Online)

# Model Driven Security: A Systematic Mapping Study

**Omar Masmali, Omar Badreddin**

Department of Computer Science, The University of Texas, El Paso, USA

**Email address:**
oamasmali@miners.utep.edu (O. Masmali), obbadreddin@utep.edu (O. Badreddin)

**To cite this article:**
Omar Masmali, Omar Badreddin. Model Driven Security: A Systematic Mapping Study. *Software Engineering.* Vol. 7, No. 2, 2019, pp. 30-38. doi: 10.11648/j.se.20190702.12

**Received**: June 24, 2019; **Accepted**: July 15, 2019; **Published**: August 5, 2019

**Abstract:** Model Driven Software Engineering (MDSE) promotes the use of models, rather than code, as the primary development artifacts. Models tend to be more understandable than code and can represent systems are variable levels of abstraction. MDSE promises improved code quality and engineers' productivity. Many of those benefits have been well examined and evaluated. However, the potential implications of MDSE on software security and reliability is not well understood. Model-Driven Security (MDS) is an approach that can support the process of modeling security requirements at a high level of abstraction in the early stage of software development. In this paper, we conduct a systematic study on MDS methodologies and concepts. The scope of the review is ten years from 2008 to 2018. The study reports on the frequencies of publication over this time period to identify the MDS forums based on seven classifications: online databases, year of publications, type of publication (journal or conference paper), the geographical distribution of the researchers, the main contribution of each paper, MDS approaches, and the security concepts. The majority of studies focused on extensions to existing UML languages suggesting some limitations in the current UML standard support for security. Most studies report on empirical evaluations, and UML Class Diagrams were the most extended language.

**Keywords:** Model-Driven Security, Model Based Security, MDS, UML, Systematic Mapping Study

## 1. Introduction

Software security has become an essential topic in Software Engineering. The emergence of new platforms such as the Internet of Things (IoT) and distributed and embedded systems have meant that the implications of software vulnerabilities could be catoptric. As more software codes are reused across platforms and systems, exploitation of software vulnerabilities could have magnified cross-platform effects. Many recent studies of software vulnerabilities suggest that code reviews are not effective in identifying and removing vulnerabilities. In the current studies, more code reviews did not improve software security or vulnerabilities. One reason is that code complexities tend to obscure vulnerabilities. That has motivated researchers to investigate Model Driven Development methodologies. Models tend to be more abstract and more understandable. Moreover, models facilitate generative programming where many code elements are automatically generated from code.

This paper reports on a systematic mapping study to uncover trends in Model Driven Software Security research. This paper is organized as follows. In the next Section, we provide an overview of the Model-Driven Security. In Section 3, we introduce the design of our systematic study methodology starting with the research questions and the search strings, databases, and steps. In Section 4, we report on the results and analysis. In Section 5, we came across some of the related works. Finally, we conclude the paper in the last section.

## 2. Model-driven Security

Model-Driven Security is an approach that can support the process of modeling security requirements at a high level of abstraction in the early stage of software development before the transaction process and generate codes. In fact, there are many definitions for MDS such as Levi L´ucio and others when they describe it as a specialization of Model-Driven Engineering (MDE) for supporting the development of security-critical applications which can make the use of the conceptual approach of MDE as well as its associated techniques and tools to propose methods for the engineering of security-critical applications [1]. D. G. Firesmith in his

paper “Engineering safety and security-related requirements for software-intensive systems” [2] found that MDS can decrease the risk of unauthorized harm to the valuable assets of the system to a certain level that is acceptable to the system’s stakeholders by preventing and reacting to malicious damage, misuse, threats, and security risks. Moreover, R. Breu explains MDS based upon MDA in the sense that security requirements are integrated into the design models which can lead to security design models [3]. In the end, all the definitions agree to the point that MDS is applying security requirements in the system modeling to increase the level of system quality.

Levi L´ucio et al. follow some historical steps for development of MDS [1]. Model-Driven Security has emerged in the early 2000s as a specialized Model-Driven Engineering approach to support the development of security terms of the systems. Jan Jurjens in 2001 started working in the domain of MDS. He uses a method based on UML extensions which is UMLsec. UMLsec contains some diagrams for modeling and analyzing systems such as class diagrams and interaction diagrams to enforce security in the target platform. In 2002, Lodderstedt and Basin found that the models in the MDA approach allow the direct manipulation of business domain’s concepts [4]. Besides, model transformations enable the automatic generation of executable systems with fully configured security infrastructures. The idea of SecureUML started in 2003 by Basin to demonstrate the feasibility and efficiency of an MDA approach. In 2008 Lang and Schreiner introduced the Domain-Specific Languages (DSLS) for capturing requirements at higher levels of abstraction and generating code automatically. And finally, in 2011 Basin applied SecureUML to various application domains showing that models are powerful enough to document security requirements and design [5].

The Model Driven Security approach has many advantages. First, it naturally gives rise to models that are technology independent, reusable, and evolvable. Second, it can integrate security and system design models and generate “security aware” applications that can have some options to the user with the formalized security policy. Third, it uses UML-notation which make it easier for most users to understand and apply since UML is a widely-used language that developers are familiar with and many tools are available for processing UML models. Further, by using MDS, it is possible to formally analyze both the models and the transformation process [6]. Also, MDS provides a way for software engineers to bridge the gap between security requirements and design the system. Also, it helps to implement security from the early stage of software development. Finally, it Increases the level of system quality and helps to reduce maintenance cost for run-time systems.

# 3. Systematic Study Method

The goal of this study is to provide a mapping of the MDS research area in the last ten years. The study reports on the frequencies of publication over this time period to identify the MDS forums based on seven classifications: online databases, year of publications, type of publication whether is it an article from a journal or a conference paper, the geographical distribution of the researchers, the main contribution of each paper, MDS approaches, and the security concepts. The methodology steps of our systematic mapping study start with a definition of research questions, then searching for relevant papers from specific online databases. The next step is screening papers, keywords and abstracts and finally, inclusion and extraction of relevant data.

### *3.1. Research Questions*

Our study has the following research questions.

RQ1: What are the characteristics of the Model-Based Security methodologies that are reported over the study period?

RQ2: How effective are Model-Based approached in improving software security and reliability?

RQ3: What aspects of security being addressed using model-based approaches?

### *3.2. String Search*

Our search strings are "Model-driven security", "Model based security" and MDS. We also included additional optional strings as follows: "SecureUML", "UMLsec", "SecureMDD", "SECTET", and "Secure Data Wearhouse". In general, the string that we apply was as follows with some adaptation needed for each search engine:

("Model-driven security" OR "Model based security" OR MDS), ("SecureUML" OR "UMLsec" OR "SecureMDD" OR "SECTET").

### *3.3. Online Databases*

We performed the search by using three of database search engines: IEEE Xplore, ACM Digital Library, and SpringerLink, by using the search strings with focusing on a range of ten years (2008 to 2018). The following is are the specifications for the search for each database.

#### *3.3.1. IEEE Xplore*

We used the command search in IEEE Xplore by applying the two searches:

"Document Title": “model-driven security” OR "Document Title": “model based security” OR "Document Title": MDS.

"Document Title": “Secure data warehouses” OR "Document Title": “UMLsec” OR "Document Title": "secureUML" OR "Document Title": "secureMDD" OR "Document Title": "SECTET".

#### *3.3.2. ACM Digital Library*

In this database we used the advanced search tool to perform the following two searches in table 1 and table 2:

***Table 1.*** *ACM Digital library first search.*

| | | |
|---|---|---|
| Title | matches all | "model-driven security" |
| Title | matches all | "model based security" |
| Publication year | in the range | 2008 to 2018 |

***Table 2.*** *ACM Digital library second search.*

| | | |
|---|---|---|
| Title | matches any | "Secure data warehouses" |
| Title | matches any | "UMLsec" |
| Title | matches any | "secureUML" |
| Title | matches any | "secureMDD" |
| Title | matches any | "SECTET" |
| Publication year | in the range | 2008 to 2018 |

#### *3.3.3. Springer Link*

In SpringerLink online database we firstly browse by Computer Science discipline. Secondly, in the subdiscipline, we select Software Engineering. Then, we set up the range for date published to be between 2008 and 2018. Finally, we apply those two searches:

"model-driven security" OR "model based security" OR MDS.

"Secure data warehouses" OR "UMLsec" OR "secureUML" OR "secureMDD" OR "SECTET".

### *3.4. Search Steps*

The search has gone through the following five steps. In step one, we started by conducting the search on the three online databases using the strings that described on the earlier step. In step two after finding the papers from the first step, we selected only journal articles and conference papers to reduce the number of papers. Then in step three, we started to read titles and keywords for each publication. The next step was going deep throw papers to decide which one we can include it and is not relevant to our research by reading abstract and skimming and scanning papers. Finally, the last step was removing any duplication that can be found in Figure 1.

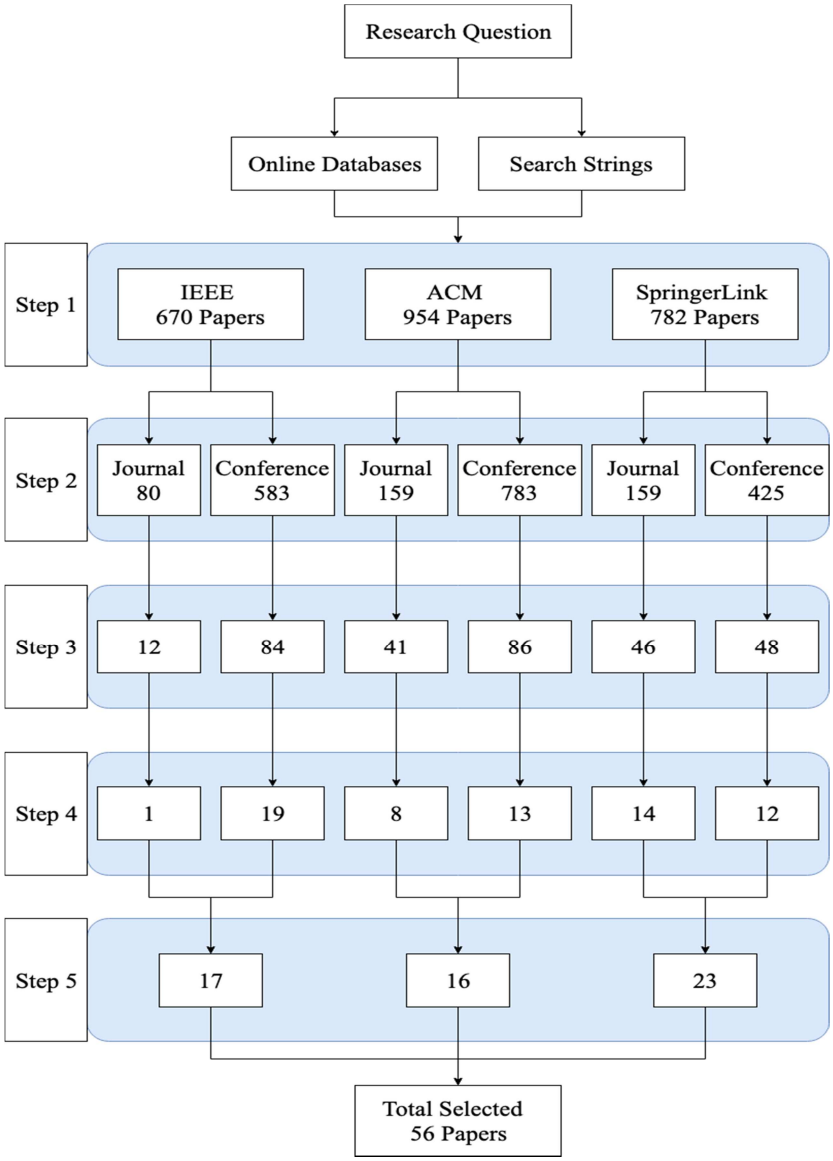


***Figure 1.*** *The five steps of search and number of publications after each step.*

### 3.5. Inclusion and Exclusion

When we reviewed the papers, we considered the criteria that we were focused. According to these criteria we include and exclude some papers depending on the following:

1. Papers that less than five pages in two columns are eliminated and we include papers that are five pages or more.
2. Papers organized in one column that are fewer than seven pages has been excluded.
3. Papers that do not explore or discuss MDS approaches are excluded from this investigation. Only the papers that study MDS are considered.
4. Papers not written in English are excluded.
5. We include papers from the last decade starting from 2008 to 2018.

## 4. Results and Analysis

### 4.1. Search and Selection Results

The overall results, which are based on the steps presented above starting from research questions and then choosing search strings to use it in specific online databases and going through all excluding steps are classified in each of the following sub-classifications.

#### 4.1.1. Classifications by Online Database

The three online databases that we used in this research are IEEE Xplore, ACM digital library, and Springer Link. In those databases, we selected only the journal papers and conference papers.

*Table 3. Databases classifications.*

| Database | Step 1 | Step 2 | Step 3 | Step 4 | Step 5 |
|---|---|---|---|---|---|
| IEEE Xplore | 670 | 663 | 96 | 20 | 17 |
| ACM digital library | 954 | 942 | 127 | 21 | 16 |
| Springer Link | 782 | 633 | 94 | 26 | 23 |
| Total | 2406 | 2238 | 317 | 67 | 56 |

In total, we select 17 papers from the IEEE Xplore database which is 30% of the overall selected papers, and 16 papers from ACM digital library as shown in table 3 which is 29%. Most of the selected papers are from Springer Link database as shown in figure 2 which shows that 41% of the articles are chosen from SpringerLink.

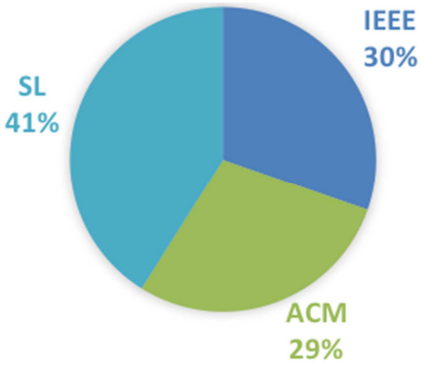


*Figure 2. Percentage of the selected papers from every database.*

#### 4.1.2. Classifications by Publication Year

*Table 4. This Year classification.*

| Year | Number of papers | Percentage |
|---|---|---|
| 2008 | 4 | 7.14% |
| 2009 | 2 | 3.57% |
| 2010 | 5 | 8.93% |
| 2011 | 7 | 12.50% |
| 2012 | 5 | 8.93% |
| 2013 | 5 | 8.93% |
| 2014 | 7 | 12.50% |
| 2015 | 9 | 16.07% |
| 2016 | 7 | 12.50% |
| 2017 | 4 | 7.14% |
| 2018 | 1 | 1.79% |

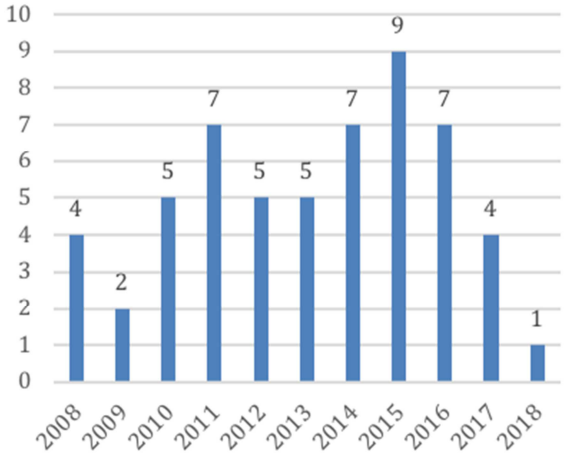


*Figure 3. Distribution of publication in ten years.*

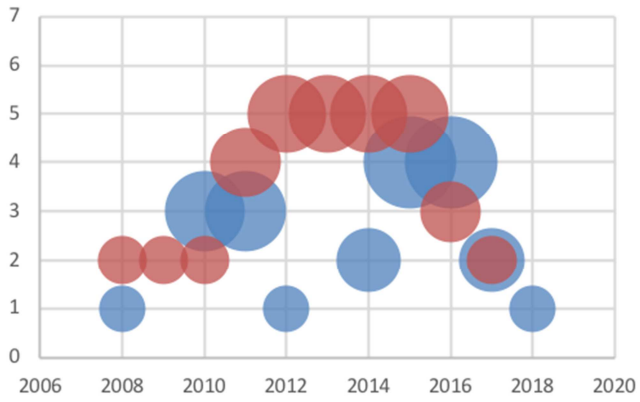


*Figure 4. Distribution of the publication type (journal articles in blue and conference papers in red).*

The results for publication year as shown in table 4 shows that years 2014, 2015 and 2016 are the years of highest number of researches been conducted in the area of MDS with 41%. 9 papers are selected in the year 2015 and 7 papers from each of the years 2011, 2014 and 2016 (figure 3). In each of the years 2010, 2012, and 2013, we found five papers which are about 9% for each year. The chart in figure 4 shows the distribution of the publication type (journals in blue and conference papers in red) and the size over the years, and the chart in figure 5 shows the distribution of size

number of the selected articles from each online database (IEEE in blue, ACM in red and sprigerlike in green) over the last ten years.

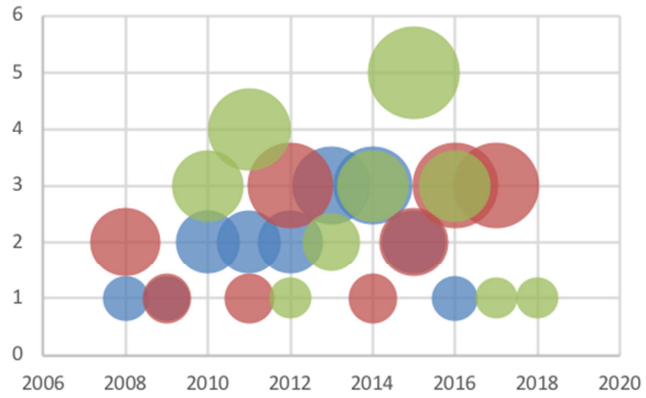


***Figure 5.*** *Size number of the selected papers from every database.*

### *4.1.3. Classifications by Publication Year*

The selected study was published as a conference paper or journal article. The study distribution of the selected studies over publication type is shown in table 5, in which about two third of the selected papers was a conference paper with 35 articles. Meanwhile, 37.5% of the selected papers was journal papers which is almost one third.

***Table 5.*** *Publication type classification.*

| Database | Journal Article | Conference Paper |
|---|---|---|
| IEEE Xplore | 1 | 16 |
| ACM digital library | 7 | 9 |
| Springer Link | 13 | 19 |
| Total | 21 (37.5%) | 35 (62.5%) |

### *4.1.4. Classifications by Author Geographic*

***Table 6.*** *This Authors geographic classification.*

| Continent | Country | Authors | | |
|---|---|---|---|---|
| | | Primary | Others | Total |
| Europe | Germany | 16 | 5 | 21 |
| | France | 11 | 2 | 13 |
| | Luxembourg | 2 | | 2 |
| | Norway | 3 | | 3 |
| | Netherlands | 1 | | 1 |
| | Austria | 2 | | 2 |
| | Sweden | | 1 | 1 |
| | UK | 1 | 1 | 2 |
| | Italy | 1 | | 1 |
| | Hungary | 1 | | 1 |
| | Belgium | 1 | 1 | 2 |
| North America | USA | 1 | | 1 |
| | Canada | 3 | 1 | 4 |
| Africa | Morocco | 1 | | 1 |
| | Tunisia | | 1 | 1 |
| Asia | Malaysia | 2 | | 2 |
| | Japan | 2 | | 2 |
| | Bangladesh | 1 | | 1 |
| | India | 2 | | 2 |
| | Pakistan | 1 | | 1 |
| | Iran | 1 | | 1 |
| Australia | Australia | 1 | | 1 |
| Total | | 56 | 14 | 70 |

We can see from table 6 the detailed nations of the authors and co-authors of the selected publications. Germany came first with 16 authors and five co-authors and in total 21.

Then France with 11 authors and two co-authors and in total 13 researchers. Figure 6 shows that 70% of all primary authors are from Europe then Asia with 9% of the researchers.

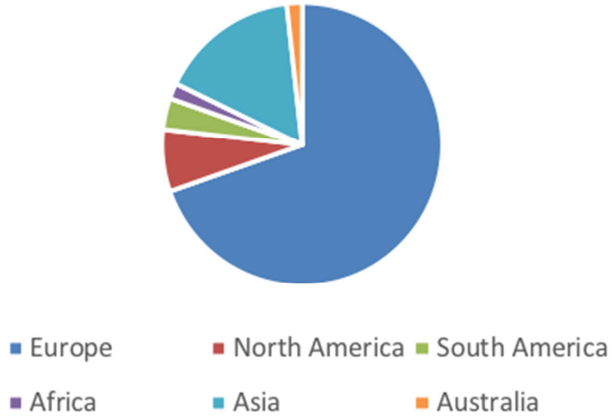


***Figure 6.*** *Classification of the author's primary author.*

### *4.1.5. Classifications by Main Contribution*

Table 7 shows that seven papers provided a new model. Those models can be a textual model or visual model or even a combination of both. Besides, the central contribution of about 29 of the selected papers was empirical. In more details, there are 11 case study papers as shown in figure 7, seven systematic mapping studies, five experiment research papers, three surveys and another three papers focusing on comparison and evaluation of MDS approaches. Furthermore, 39% of the found publications concentrating on extensions. UML extension was expressed by 20 papers, while three publications found talking about OCL extension.

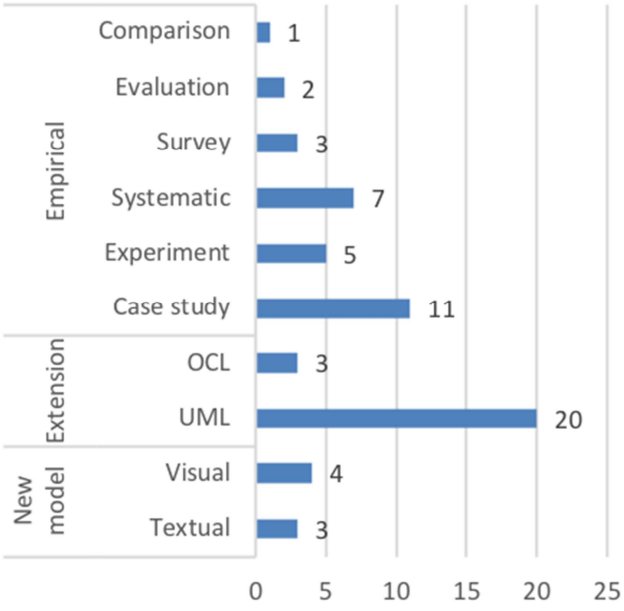


***Figure 7.*** *Paper's main contribution.*

***Table 7.*** *Main contribution.*

| Main contribution | | Papers | Percentage |
|---|---|---|---|
| New Model | Textual | 3 | 5.08 % |
| | Visual | 4 | 6.78 % |
| Extension | UML | 20 | 33.90 % |
| | OCL | 3 | 5.08 % |
| Empirical | Case study | 11 | 18.64 % |
| | Experiment | 5 | 8.47 % |
| | Systematic | 7 | 11.86 % |
| | Survey | 3 | 5.08 % |
| | Evaluation | 2 | 3.39 % |
| | Comparison | 1 | 1.69 % |

In more detail, 46% of the found publications that are focusing on the UML extension, there was 16 paper extending the class diagram. State machine diagram came next with six papers as shown in table 8. The next UML extension with five publications was a sequence diagram which is about 14%.

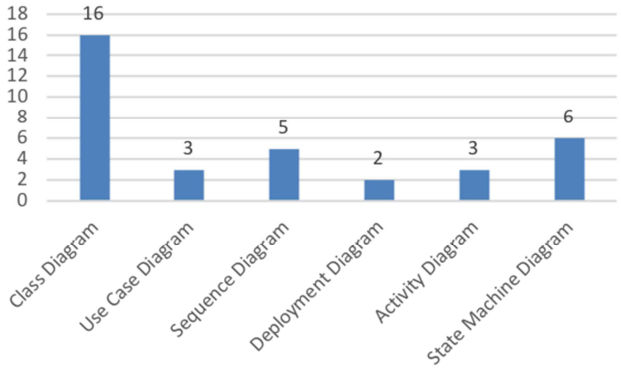


***Figure 8.*** *UML Extensions distribution.*

Moreover, it can be seen from figure 8, that each of use case diagram and activity diagram was explored on three papers for each. Finally, there are only two papers we found were focusing on a deployment diagram.

***Table 8.*** *UML Extensions.*

| UML Extension | Number of papers | Percentage |
|---|---|---|
| Class Diagram | 16 | 45.71 % |
| Use Case Diagram | 3 | 8.57 % |
| Sequence Diagram | 5 | 14.29 % |
| Deployment Diagram | 2 | 5.71 % |
| Activity Diagram | 3 | 8.57 % |
| State Machine Diagram | 6 | 17.14 % |

### *4.2. Application Domain Results*

As shown in figure 9, MDS approaches are mentioned, used, and proposed mostly for embedded systems with 19.64%, followed by Information systems with 14.29%, and the web applications with 10.71%. That can give us an impression that embedded systems such as smart-cards are inherently security-critical [7], which make it in top research concern in MDS area. In the same direction, web applications play a central role in our society and are necessary for most organizations to access data outside their information systems or to provide services for customers [8]. Therefore, web application security is a great challenge as well. Cloud computing was one of the application domains that some of the papers has focused on lately. We found that 7.14% of the selected papers studying MDS on cloud systems. SOA, also, has the same amount of papers with 7.14% of all publications. Also, we found that 12 articles, which amounts to 21.43%, are explaining the use of MDS in two or more application domains. About 16% of the found papers were discussing MDS in general without examining it on any application domain as shown in table 9.

***Table 9.*** *Application domain distribution.*

| Application Domain | Papers | Percentage |
|---|---|---|
| Information System | 8 | (14.29%) |
| Web Application | 6 | (10.71%) |
| Embedded System | 11 | (19.64%) |
| Data Warehouse | 2 | (3.57%) |
| SOA | 4 | (7.14%) |
| Cloud Computing | 4 | (7.14%) |
| Unspecified | 9 | (16.07%) |
| More than one | 12 | (21.43%) |

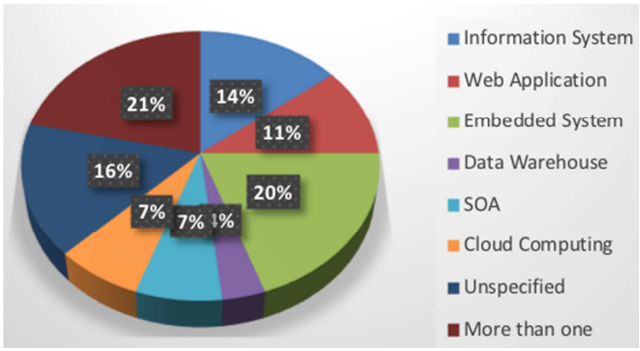


***Figure 9.*** *Classification of the application domain.*

### *4.3. MDS Approaches Results*

From table 10 we can recognize that UMLsec along with secureMDD are the most MDS approaches been studied in the last ten years. Firstly, UMLsec, which is 19.64% of the publications, which is an extension of UML [9] for recurring security requirements and security assumptions on the system environment. UMLsec can be specified either within UML specifications or within the source code as annotations. The second approach, with 11 papers as well, is secureMDD. SecureMDD [10] is another model-driven approach to develop secure applications which can be designed from a UML application model using a predefined UML profile and a platform independent and domain-specific language.

***Table 10.*** *MDS approaches.*

| MDS Approach | Number of Papers |
|---|---|
| UMLsec | 11 (19.64%) |
| secureUML | 6 (10.71%) |
| secureMDD | 11 (19.64%) |
| SECTET | 3 (5.36%) |
| Secure Data Warehouses | 2 (3.57%) |
| Security Patterns | 5 (8.93%) |
| EBIOS | 2 (3.57%) |
| Two or more | 11 (19.64%) |

| MDS Approach | Number of Papers |
|---|---|
| Security Testing | 3 (5.36%) |
| Model checking | 1 (1.79%) |
| ISOAS | 1 (1.79%) |

In this study, we found that also another 11 papers are discussing more than one MDS approach which contains about 19.64% of the overall found publications. Moreover, from the selected papers, we saw that 10.71% of the recent researches is talking about secureUML. SecureUML [11, 12] is a support tool for specifying authorization constraints based on role-based access control, and it defines a vocabulary for annotating UML models to expresses different aspects of access control, such as role, role permission, and user-role assignment.

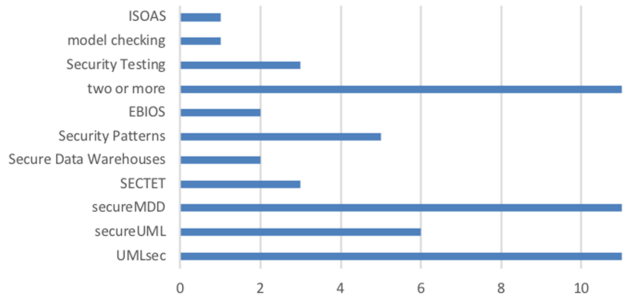


***Figure 10.*** *MDS approaches.*

Figure 10 is shown that there are three publications found for each of SECTET and security testing. Secure data warehouse and EBIOS approaches we found two papers for each one of them, and finally, only one paper discussing ISOAS and another one about model checking approach.

### *4.4. Security Concepts Results*

Our approach to evaluating the selected publication in security matter was based on the three traditional CIA triad security concepts, Confidentiality, Integrity, and Availability. The CIA [13] triad is a security model that designed to guide policies for information security. Confidentiality [14] is to make sure that access to information is restricted to only authorized people and to prevent any unauthorized person to access the system. Integrity means that the information should not be modified illegally. Availability, the data must be available 100% of the time to authorized parties when it is needed.

***Table 11.*** *CIA Security concerns.*

| Security concerns | Number of papers |
|---|---|
| Confidentiality | 44 (78.6%) |
| Integrity | 24 (42.9%) |
| Availability | 20 (35.7%) |

Researchers have studied confidentiality as the most security concept with 78.6% as described in table 11. Integrity has been the second most security concern with 24 papers, and lastly, 35.7% of the selected papers were focusing on availability as shown in figure 11.

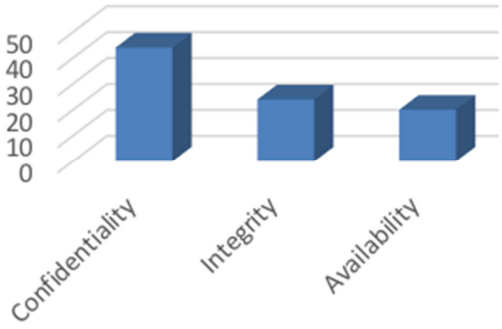


***Figure 11.*** *Security concerns distribution.*

Table 12 explains the combination of security concerns that found on the selected papers in this research. Only four papers are focusing on integrity and availability concerns (IA).

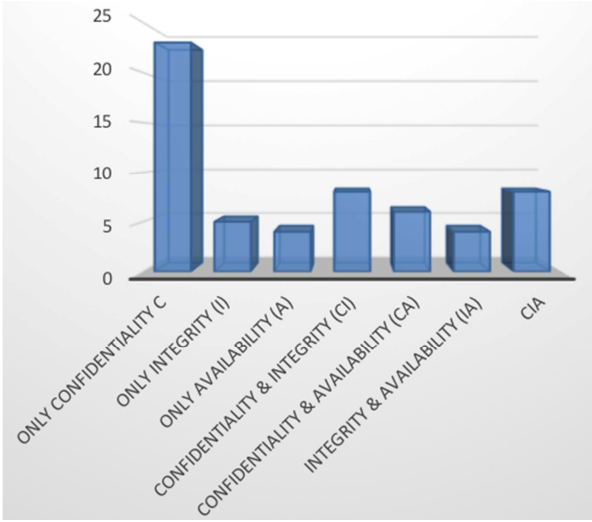


***Figure 12.*** *Distribution of the combinations of security concerns.*

***Table 12.*** *Security Concerns Combination.*

| Security Concerns Combination | Papers |
|---|---|
| Only Confidentiality (C) | 23 (41.1%) |
| Only Integrity (I) | 5 (8.93%) |
| Only Availability (A) | 4 (7.14%) |
| Confidentiality & Integrity (CI) | 8 (14.3%) |
| Confidentiality & Availability (CA) | 6 (10.7%) |
| Integrity & Availability (IA) | 4 (7.14%) |
| CIA | 8 (14.3%) |

Meanwhile, as figure 12 explicate, the concepts of confidentiality and availability (CA) were found on six papers which are about 10%. The combination of confidentiality and integrity concerns (CI) were found expressed in eight articles. Finally, all three CIA triad security concepts were spotted together in 14.3% of the publications which is eight papers.

## 5. Related Work

Although the importance of MDS, still there is not enough research exploring this area. R. Abdallah presented a

framework for model-driven based security to analyze the process that begins from the design phase of the system architecture [15]. Meanwhile, T. Lodderstedt in his paper "secureUML: A UML-Based Modelling Language for Model-Driven Security" presented a new modeling language called secureUML for the model-driven development of secure systems based on the Unified Modelling Language UML [4]. A new tool has been used by J. ürjens which is UMLsec for extending UML for secure system development [16]. Furthermore, M. Zhendong examined model-driven security for Web services in e-Government system, and he realized that MDS is a promising approach to reduce complexity and increase efficiency in the development of systems security [17].

In term of systematic mapping and literature studies, there are no quite enough publications in MDS. J. Jensen [18] in 2011 tried to answer the questions "What are the major scientific initiatives describing automatic code generation from design models within the context of security in MDD? What empirical studies exist on the topic of security within MDD/MDA? What are the strengths of the evidence showing that security aspects successfully can be modeled as an inherent property and transformed to more secure code?". This study expressed the need for more empirical studies on the security within MDD/MDA. In 2013, P. Nguyen studied MDS in his systematic review with focus on many evaluation criteria such as security concerns (Confidentiality, Integrity, Availability, Authenticity, and Authorization), type of models (structural or behavioural), transformations level (endogenous or exogenous), code generation tools, application domains (IS, embedded systems, distributed systems, ect.), and type of validation such as case studies [19]. In this paper, they found that most approaches focus on authorization and confidentiality; meanwhile, the other security concerns such as authentication and integrity, comes with only a few publications.

Furthermore, another systematic classification by M. Felderer in 2016 presented a taxonomy for model-based security testing. It also provides an overview of state of the art in the field of model-based security testing [20]. Finally, in 2017, a systematic literature review by A. Berghe to investigate and characterize the existing notations and associated techniques in the area of designing secure software. In their study, they realized that not all security concerns are supported equally by the current notations, and also, most notations are evaluated using only illustrations without case studies [21].

# 6. Conclusion

This paper has reported the results of a systematic mapping we conducted in the field of model-driven security. We have systematically scanned the publications over three online databases for the past ten years from 2008 to 2018. From over 2400 publications dealing with MDS, we selected 56 research. Research studies were selected based on journal articles and conference papers. The results were classified by the three online databases chosen, published year, publication type, authors and co-authors nationalities and the distribution of their continents, and the main contribution. In addition, we tracked the main domain applications that the researchers use it to apply MDS. We also classified MDS approaches studied by authors in their papers. Further, we quantified the security concerns based on the CIA triad security concepts that the publications were focusing on.

# References

[1] L´ucio, L., Zhang, Q., Nguyen, P., Amrani, M., Klein, J., Vangheluwe, H., Traon Y., 2014. Advances in Model-Driven Security. Advances in Computers, Chapter 3, Volume 93, Elsevier.

[2] Firesmith, D., 2007. Engineering safety and security related requirements for software intensive systems. In 29th International Conference on Software Engineering. ICSE.

[3] Breu, R., Hafner, M., Weber, B., Novak A., 2005. Model Driven Security for Inter-Organizational Workflows in e-Government. E-Government: Towards Electronic Democracy.

[4] Lodderstedt, T., Basin, D., Doser, J., 2002. SecureUML: A UML-based modeling language for model-driven security. In Model Engineering, Concepts, and Tools 5th International Conference.

[5] Basin, D., Clavel, M., Egea, M., 2011. A Decade of Model-Driven Security. In 16th ACM symposium on Access control models and technologies. SACMAT.

[6] Basin, D., Doser J., 2006. Model Driven Security: from UML Models to Access Control Infrastructures. ACM Transactions on Software Engineering and Methodology (TOSEM), Volume 15 Issue 1.

[7] Moebius, N., Stenzel, K., Grandy, H., Reif, W., 2009. SecureMDD: A Model-Driven Development Method for Secure Smart Card Applications. In International Conference on Availability, Reliability and Security.

[8] Idani, A., 2017. Model Driven SecureWeb Applications The SeWAT platform. In the Fifth European Conference on the Engineering of Computer-Based Systems.

[9] Fourneret, E., Ochoay, M., Bouquet, F., Botellaz, J. Jürjensy, J., Yousefi, P., 2011. Model-Based Security Verification and Testing for Smart-cards. In Sixth International Conference on Availability, Reliability and Security.

[10] Borek, M., Stenzel, K., Katkalov, K., Reif, W., 2015. Integration and Exchangeability of External Security-Critical Web Services in a Model-Driven Approach. In International Conference on Conceptual Modeling.

[11] Chowdhury, M., 2014. Security Risk Modelling Using SecureUML. In 16th International Conference Computer and Information Technology.

[12] Matulevičius, R., Lakk, H., 2015. A Model-driven Role-based Access Control for SQL Databases. Complex Systems Informatics and Modeling Quarterly. CSIMQ.

[13] Rawat, D., Bajracharya, C., 2015. Cyber Security for Smart Grid Systems: Status, Challenges and Perspectives. In the IEEE Southeast Conference.

[14] Kumar, P., Raj, P., Jelciana, P., 2017. Exploring Data Security Issues and Solutions in Cloud Computing. In the 6th International Conference on Smart Computing and Communications.

[15] Abdallah, R., Yakymets, N., Lanusse, A., 2015. Towards a Model-driven based Security Framework. In 3rd International Conference on Model-Driven Engineering and Software Development. MODELSWARD.

[16] Jurjens, J., Schreck, J., Yu, Y., 2008. Automated Analysis of Permission-Based Security Using UMLsec. In International Conference on Fundamental Approaches to Software Engineering.

[17] Ma, Z., Wagner, C., Bleier, T., 2011. Model-driven security for Web services in e-Government system: ideal and real. In 7th International Conference on Next Generation Web Services Practice.

[18] Jensen, J., Jaatun, M., 2011. Security in Model Driven Development: A Survey. In Sixth International Conference on Availability, Reliability and Security.

[19] Nguyen, P., Klein, J., Traon, Y., Kramer M., 2013. A Systematic Review of Model-Driven Security. In 20th Asia-Pacific Software Engineering Conference.

[20] Felderer, M., Zech, P., Breu, R., Büchler, M., Pretschner, A., 2016. Model-based security testing: a taxonomy and systematic classification. Software Testing Verification and Reliability, Volume 26, Issue 2. Chichester, UK.

[21] Berghe, A., Scandariato, R., Yskout, K., Joosen, W., 2017. Design notations for secure software: a systematic literature review. Software and Systems Modeling, Volume 16, issue 3.