











Article

# Systematic Literature Review of Security Pattern Research

Hironori Washizaki<sup>1</sup> , Tian Xia<sup>1</sup> , Natsumi Kamata<sup>1</sup>, Yoshiaki Fukazawa<sup>1</sup> , Hideyuki Kanuka<sup>2</sup> , Takehisa Kato<sup>2</sup> , Masayuki Yoshino<sup>2</sup>, Takao Okubo<sup>3</sup> , Shinpei Ogata<sup>4</sup> , Haruhiko Kaiya<sup>5</sup> , Atsuo Hazeyama<sup>6</sup> , Takafumi Tanaka<sup>7</sup>, Nobukazu Yoshioka<sup>8</sup>  and G Priyalakshmi<sup>9</sup>

<sup>1</sup>Waseda University; washizaki@waseda.jp

<sup>2</sup>Hitachi, Ltd.; hideyuki.kanuka.dv@hitachi.com

<sup>3</sup>Institute of Information Security; okubo@iisec.ac.jp

<sup>4</sup>Shinshu University; ogata@cs.shinshu-u.ac.jp

<sup>5</sup>Kanagawa University; kaiya@kanagawa-u.ac.jp

<sup>6</sup>Tokyo Gakugei University; hazeyama@u-gakugei.ac.jp

<sup>7</sup>Tamagawa University; tanaka\_t@eng.tamagawa.ac.jp

<sup>8</sup>National Institute of Informatics; nobukazu@nii.ac.jp

<sup>9</sup>PSG College of Technology; priya.venky2001@gmail.com



**Abstract:** Security patterns encompass security-related issues in secure software system development and operations that often appear in certain contexts. Since the late 1990s about 500 security patterns have been proposed. Although the technical components are well investigated, the direction, overall picture, and barriers to implementation are not. Here, a systematic literature review of 240 papers is used to devise a taxonomy for security pattern research. Our taxonomy and the survey results should improve communications among practitioners and researchers, standardize the terminology, and increase the effectiveness of security patterns.

**Keywords:** Security patterns, software patterns, systematic literature review (SLR)

## 1. Introduction

Security patterns encapsulate security-related problems and solutions that recur in certain contexts for secure software system development and operations [1]. Although both concrete and abstract security patterns have been proposed since the 1990s, they are still difficult to apply appropriately. Most studies have focused on technical aspects and implementation, but few have examined the direction, overall picture, and significant technical challenges. One study systematically mapped security patterns using 30 papers [2].

In this paper, we propose a taxonomy for security pattern research by conducting a systematic literature review (SLR) [3]. Based on the taxonomy, we categorize and analyze 240 papers [4–243] to clarify state-of-the-art and future directions of security pattern research in terms of 13 facets including topics and security characteristics<sup>1</sup>. Our taxonomy and the survey results should improve communications among practitioners and researchers, standardize the terminology, and increase the effectiveness of security patterns.

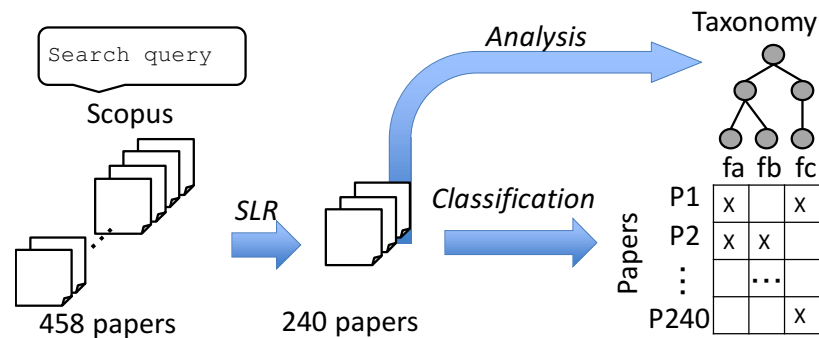


Figure 1. Taxonomy construction process

The rest of this paper is organized as follows. Section 2 overviews our SLR process and taxonomy. Section 3 outlines our taxonomy. Sections 4 show the survey results of the facets in the taxonomy. Finally, Section 5 provides the conclusion and future directions.

## 2. Taxonomy Construction

Figure 1 outlines how various characteristics are identified to distinguish existing security pattern studies to realize a comprehensive taxonomy, which classifies security pattern research as feature diagrams. A top-down approach is used by having four steps: determining the scope, conducting an SLR, analyzing the results, and validating the results.

1. To determine the scope, we first defined our purpose and goals. The purpose is to support the classification, comparison, reuse, and extension of security pattern research. Our goals are to improve not only communications about security software stakeholders such as researchers, developers, and users but also to improve the availability of research results. Thus, we aimed to develop a taxonomy to classify security patterns and standard terminology.
2. Next, we conducted a SLR, which aims to aggregate existing evidence to achieve the research goal and to support the development of evidence-based guidelines for researchers and practitioners [245]. The SLR used Scopus<sup>2</sup>, which is Elsevier's abstract and citation database, to search for papers about security pattern research. The search query was the following.

```
TITLE-ABS-KEY("security pattern") AND ( LIMIT-TO(SUBJAREA,"COMP")
OR LIMIT-TO(SUBJAREA,"ENGI"))
```

Scopus was chosen because its effectiveness as a software engineering SLR has been demonstrated [246–249]. In addition, the results can be easily exported. On October 23, 2018, our query returned 484 papers published between 1992–2017. The following inclusion and exclusion criteria were subsequently used to compile research on security patterns:

- The publication is a paper in a journal or conference proceeding. (Inclusion)
- The topic must propose or employ security patterns for software and systems engineering. (Inclusion)
- It does not include further engineering activities such as analysis and application. (Exclusion)

Each paper was initially read by one author to determine if it was within the scope of this study. Then a second author confirmed the assessment. If these classifications conflicted, all authors discussed until a consensus was reached. This procedure returned 240 papers<sup>3</sup>.

3. Afterwards, the identified characteristics in existing security pattern research were merged using existing methods such as CVSS [250] and CWE [251] as well as key concepts in the Security and Privacy Metamodel [252] to form a feature diagram [253]. A feature diagram is a tree to visualize four types of relationships between a parent feature and its child features (subfeatures): The first is "Mandatory," which indicates a required subfeature. The second is "Optional," which denotes a voluntary feature. The third is "Or," which requires at least one of the subfeatures. The fourth is "Alternative," which means only one subfeature can be selected. Since a feature diagram essentially defines a taxonomy, feature diagrams have been used for defining taxonomies to classify papers and documents in literature review [254,255].
4. Finally, the taxonomy was validated by classifying existing security pattern research identified in the SLR.

### 3. Taxonomy

Figure 2 shows our taxonomy, which includes five features as facets of categorization for security pattern research. The first feature is "Purpose," which includes topics addressed by security pattern research, phases of the targeted system, and the software lifecycle. The second is "Research Implementation," which includes the platform to realize the results of security pattern research, whether the results are automated or encapsulated as a tool, and whether case studies or experiments are performed to evaluate the results relevant to the original research purpose. The third is "Quality," which includes items related to quality characteristics such as vulnerabilities and threats toward a specific security problem; security characteristics such as privacy, integrity, and availability; and whether a measurement system is incorporated to detect changes in security by introducing or applying the results. The fourth is "Pattern," which includes the types of patterns addressed in the research. Patterns that address security concerns can be classified into two types: security patterns and attack patterns. The former addresses both of recurring security problems and corresponding solutions from the viewpoint of defenders to security risks, while the later addresses only security problems from the viewpoint of malicious attackers by detailing security risks. The fifth is "Method," which includes the methodology, pattern modeling notations, and pattern relationships.

There are multiple methods to validate a taxonomy. Examples include demonstrating the orthogonality of its classification features, benchmarking against existing classification schemes, or confirming its utility to classify existing knowledge [256]. Herein orthogonality means that a security pattern research paper can be classified as only one category of possible combinations of concrete features in the feature diagram.

Our taxonomy should guide practitioners and researchers in the two use cases (UCs).

- **UC1** is to help practitioners choose existing security pattern methods and tools. When engineers want to reuse and eventually extend existing security pattern methods and tools, security patterns must be compared prior to selecting the most appropriate one for the scenario. Selection should be based on how the methods and tools meet the intended objectives. Our taxonomy helps compare criteria to assess methods and tools according to their characteristics.
- **UC2** is to communicate and research security pattern methods and tools. In this case, the taxonomy serves as a resource for the security pattern engineering community, which includes practitioners and researchers. By incorporating the characteristics of security pattern research into a single structure, our taxonomy can serve as a framework to guide future communications and research on security pattern methods and the corresponding tools. For example, our taxonomy

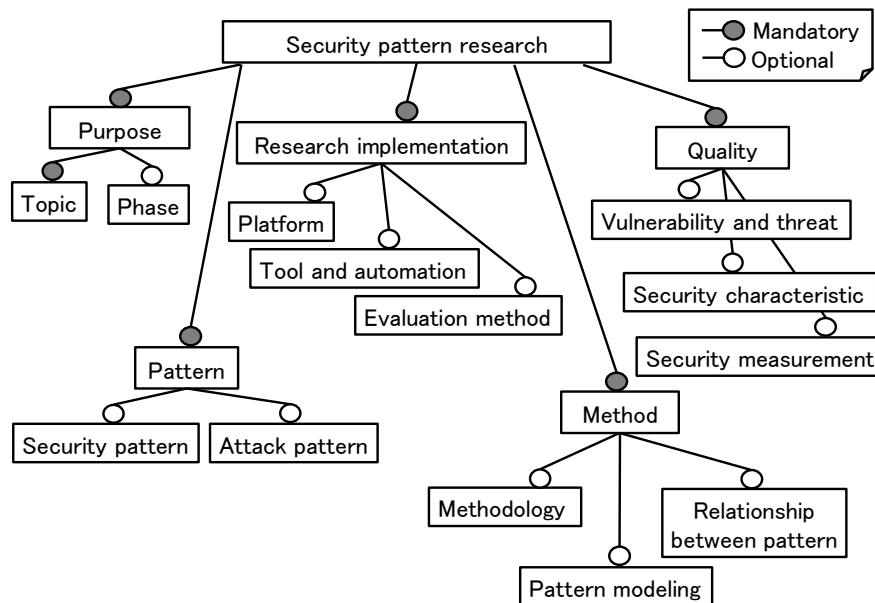


Figure 2. Feature diagram of the taxonomy

can serve as the basis to build an open repository of information of existing security pattern research methods and their corresponding tools. Moreover, our taxonomy should improve the quality of security pattern research and the effectiveness of security patterns by serving as a unifying resource.

#### 4. Survey results

The 240 papers identified in the SLR are classified by the 13 facets defined in the taxonomy to clarify state-of-the-art approaches and future research directions. Because each characteristic fitting gives only one classification category, the classification features are orthogonal. Below, how the taxonomy helps classify security pattern research papers is summarized.

##### 4.1. Purpose

###### 4.1.1. Topic

Figure 3 divides the 240 papers by research topic. Most papers report security pattern applications during development, abstract development methodologies, and pattern classification. Empirical and case study reports are limited, indicating that future research should consider case studies, methodologies, and applied experiments.

Although security patterns have been presented at conferences such as PLoP (Pattern Language of Programs)<sup>4</sup> since the late 1990s, patterns are still manually identified. Pattern extraction is rarely reported (i.e., 1%) [11,13]. Mechanisms to identify and extract security patterns are highly anticipated, but in reality, research is not being conducted on this topic. Similarly, automatically identifying critical attack and security patterns is desired to determine coding requirements and design, but these topics are not extensively researched as only 8% of papers report pattern specifications and verifications. Hence, more research on these topics should be conducted in the future.

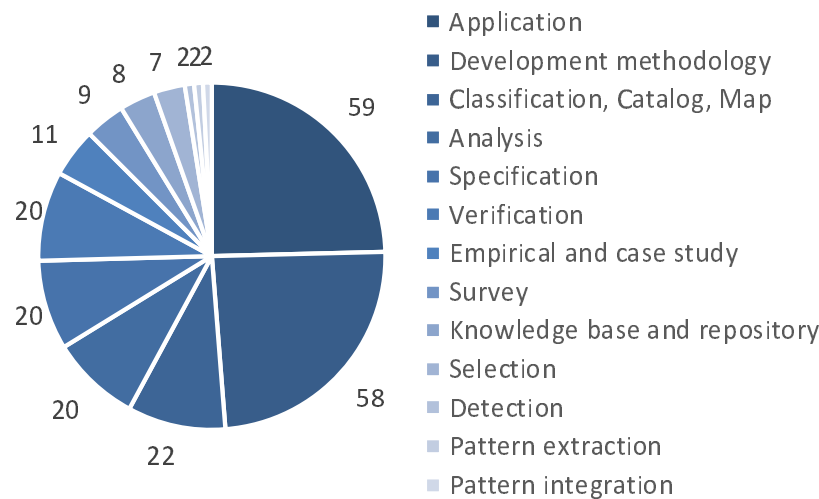


Figure 3. Breakdown of topics

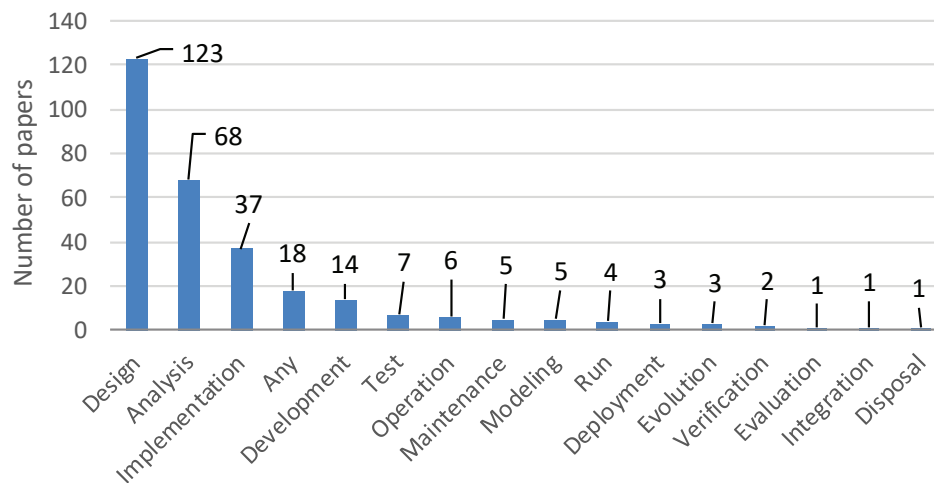


Figure 4. Phases targeted by security patterns

#### 4.1.2. Phase of lifecycle

Figure 4 shows the results after categorizing the papers into 16 phases. Each paper is categorized in zero or more phases. In addition, the categories have a hierarchical order. For example, because "Any" can produce phases with a higher granularity compared to the "Design" phase, the analysis results include some ambiguities. Whether "Evolution" is included in "Any" must be determined individually. Numerous phases from "Analysis" to "Evolution" can be research targets. Each paper should be classified into the highest granularity as possible.

The most commonly investigated phases are "Design" followed by "Analysis" and "Implementation." Hence, research targets are skewed towards the earlier phases. Few report post-implementation phases such as "Maintenance" and "Evolution," suggesting that security pattern research in later phases may be a frontier field. Cutting-edge topics include pattern classification [16], pattern detection from the source code [41], improvement of legacy systems using security patterns [10], and security patterns for operation dynamics [181]. In contrast, classifying patterns for the system lifecycle, defining patterns that respond to dynamic behaviors, and utilizing defined patterns in existing systems are topics that should be further examined.

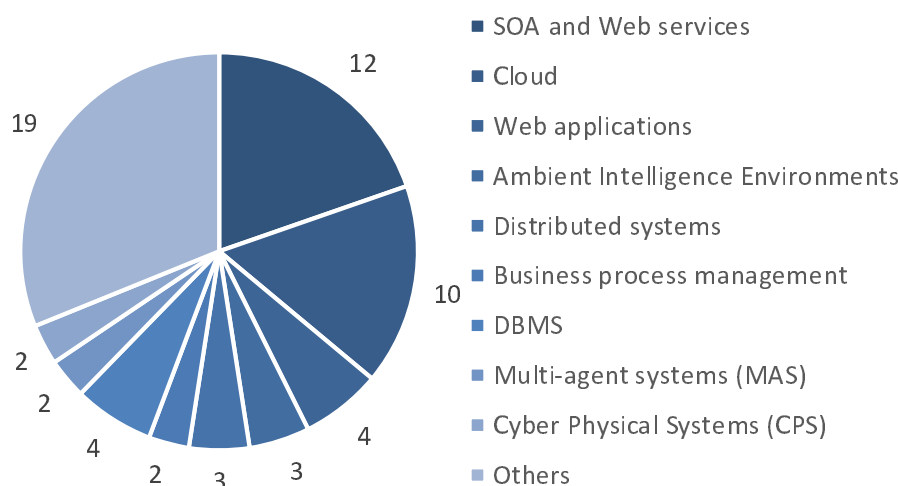


Figure 5. Breakdown of computing platforms

## 4.2. Research implementation

### 4.2.1. Computing platform

Among the 240 papers, 25% (61) are platform specific (Fig. 5), including Ambient Intelligence Environments, Business Process Management (BPM), and Multi-Agent Systems (MAS). Most reports use general platforms like the web, cloud, and distributed system.

A few papers address Cyber Physical Systems (CPS) and the Internet of Things (IoT) [227,233]. However, various IoT security patterns are emerging. About 75% do not refer to a specific platform. Considering the development of systems involving IoT, the cloud, and their applications, active research on such platforms is desirable.

### 4.2.2. Tool and automation

About 34% (82 papers) mention tools or automation (Fig. 6). Many use tools and approaches that involve modeling. A few also include formal verification, aspect-oriented approaches, and code generation. Because the majority of reports create a unique tool, there are many tools for modeling, analysis, design, and implementation. However, few studies propose testing tools (such as model-based testing [179,209]) and operating tools (such a runtime framework [40,171,173,199]).

Tools should span the entire lifecycle because security issues appear in all phases. Hence, future studies should develop tools that directly incorporate security patterns in the testing and operation phases.

### 4.2.3. Evaluation method

About half (51.6%, 124 papers) incorporate an evaluation by implementing a case study (19.5%), referencing examples (15%), and conducting experiments (4.1%). Additionally, 12.9% report using an evaluation without specifying the method.

The findings indicate that evaluations of security pattern usage are an immature research area. Even if an evaluation is conducted, it is often limited to a case study or referencing an example. Stricter evaluation methods (e.g., a control experiment) are almost non-existent. Hence, more rigorous evaluation methods are expected in the future.

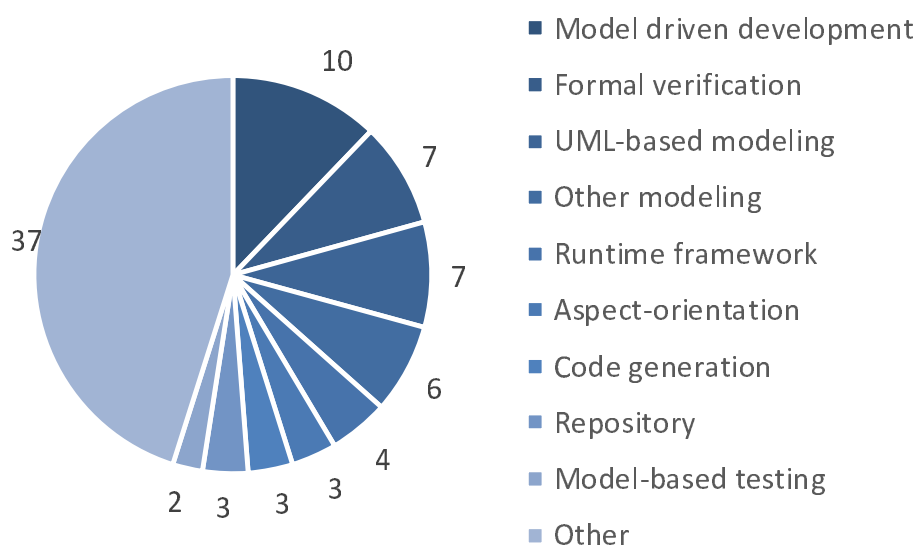


Figure 6. Breakdown of tools and automation

### 4.3. Quality

#### 4.3.1. Vulnerability and threat

Vulnerabilities or threats are mentioned in 29.5% (71) of the papers. Only 1.2% (3) refer to STRIDE [257], which is advocated by Microsoft, while another 2.5% (6) refer to other publicly available information regarding vulnerabilities and threats. Of these, one [10] references CVSS (the Common Vulnerability Scoring System) [250], which summarizes risk information. Four papers reference more tangible vulnerability information such as CWE (Common Weakness Enumeration) [251] and CVE (Common Vulnerability and Exposures) [258]. Furthermore, one paper [214] refers to CAPEC (Common Attack Pattern Enumeration and Classification) [259], which categorizes actual attacks.

Because security measures often involve addressing system vulnerabilities and threats, research patterns should clearly explain how to deal with them. Thus, the fact that only 29% of the papers mention vulnerabilities or threats is troublesome. Future research should collect both the theoretical and actual relationships on vulnerabilities to realize practical uses of security patterns. Currently, only 6% of papers are related to publicly available information. Consequently, future research should investigate how to utilize such information along with increasing the awareness of security patterns.

#### 4.3.2. Security characteristic

The security characteristics mentioned in the literature are used to identify the trends in security pattern research. Over half (58.8%, 141) mention security characteristics. Of the 141 papers, 91.5% (129) reference CIA characteristics, which stand for confidentiality, integrity, and availability as defined by "information security is to maintain CIA" in ISO/IEC 27002. In these papers, there are 109, 84, and 71 references to confidentiality, integrity, and availability, respectively (Fig. 7).

Another 37 papers reference non-CIA security characteristics of access control, accountability, authenticity, authentication, authorization, and nonrepudiation. Of these, 25 mention both CIA and non-CIA characteristics, while 12 only mention non-CIA characteristics.

Many studies examine security characteristics, especially those based on CIA characteristic security patterns. Confidentiality, which allows only individuals with granted permission to access information, is especially important. One example involving privacy and confidentiality is RBAC (Role-Based Access Control).



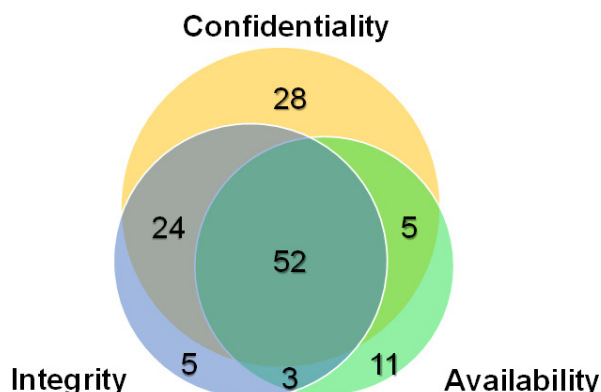


Figure 7. Breakdown of the security characteristics

#### 4.3.3. Security measurement

Only a few papers (10.8%, 26) adopted security measurements to evaluate patterns. Two used STRIDE [257]. [57] evaluated the handling of potential threats via a graph and indicated attack categories against non-secure and secure systems accordingly. [141] used STRIDE to evaluate the system against security attacks. Their evaluation using fuzzy logic defined five levels for the five main events, where the levels correspond to a category in STRIDE. Although the number of levels/categories and how each level/category is defined may differ slightly between these two evaluation models, both employ an approach to evaluate three to five discrete levels for the likelihood of exposing vulnerabilities and their effects on the system associated with security patterns.

Because each research paper used its own evaluation categories, assessing the applicability of the evaluation results is challenging. In the future, a standard index such as STRIDE should be used to evaluate results to create comparable and standard security patterns. The following list summarizes other measurements in the literature.

- In [5], security patterns found in 23 papers are grouped into 14 categories. Then the categories are evaluated using nine levels of quality standard classifications.
- In [26], forces and Solution are used to evaluate attribute, risk reduction frequency, risk reduction consequence, annual number of attacks, cost per attack, and cost solution. Furthermore, XSS (Cross Site Scripting) is evaluated as a case study.
- In [29], seven levels of security criteria are used to compare and evaluate nine security patterns. In addition, performance gain and loss is compared. The implementation cost and degree of security are also evaluated in three levels.
- In [37], the following three categories are used for evaluating security pattern description elements (problem and forces, structure description, structure image, behavior description, behavior image, consequences, and example): not provided, minimal, and satisfactory.
- In [39], measures against possible threats are evaluated using a graph.
- In [59], resource access restrictions granted to different roles are evaluated in terms of four operations: C (create), R (retrieve), U (update), and D (delete).
- [76] supports an aspect-oriented approach and proposes an evaluation using Object Constraint Language (OCL) for Account Lockout with Selective Logging (ALSEL) and IMAP system.
- In [116], nine levels of quality are used to evaluate nine concerns such as threats and attacks to be avoided, an attack pattern to be applied, threats to be passed, and security requirements.
- In [125], security patterns of eight categories such as accountability, confidentiality, and integrity are evaluated.
- In [152], security patterns of a distributed system are categorized and five quality indicators are evaluated.
- In [155], using the  $6\sigma$  approach, 12 security patterns are evaluated by 6 categories of undesirable properties.



**Table 1.** Security pattern names in at least ten papers

Security Pattern Name	Number of Appearances
RBAC	49
Authorization	34
Authentication	23
Access control	21
Authenticator	21
Secure logger	19
Check point	17
Reference monitor	15
Secure pipe	14
Single access point	13
Authentication enforcer	11
Replicated system	10
ABAC	10
Encrypted Storage	10
Firewall	10

- In [200], using its own unique evaluation formula, the applicability of patterns is calculated as rate.
- In [202], three indices (completeness, isolation, and verifiability) are used as the engineering principles of security kernel.
- [203] is related to security patterns of a grid system. Password and digital signature are expressed as graphic extension of Backus normal form (a.k.a. Backus–Naur form) in the authentication pattern.
- In [204], using an example of an ATM terminal, security objects, and patterns are described and evaluated in eight matrices.
- [205] categorizes patterns into three layers and evaluates them.

#### 4.4. Security related patterns

##### 4.4.1. Security pattern

Most papers (77.9%, 187) mention a specific security pattern by name. On average, each paper mentions 4.9 patterns. Although there are 1179 references to a pattern name, only 558 are unique patterns. Of these, 31.5% (176 patterns) are mentioned in at least two papers. By the definition of the word “pattern,” a software pattern should be used by many practitioners. However, this study reveals that the majority of patterns (70%) are not actually shared. Only 16 patterns are mentioned in at least 10 papers (Table 1). These patterns are related to access control, authorization, and authentication.

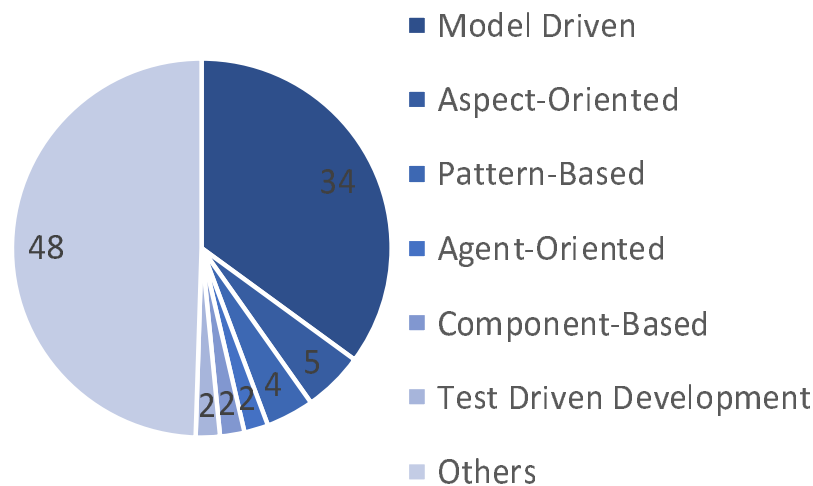
Ironically, over 22% of the papers on security patterns do not mention a specific pattern by name. Without a pattern name, it is difficult to explain a new idea or method. Our results reveal about one-third of the patterns are common and can be easily described using a directed graph structure represented by a UML class diagram. Although many research papers express patterns without specific names, this will become more challenging in the future as research expands to include concepts that are difficult to express by a structural description such as availability.

##### 4.4.2. Attack pattern

Attack patterns are much less prevalent than security patterns. Only 17.0% (41) papers mention attack patterns. Many patterns are mentioned in only one paper. Table 2 summarizes patterns mentioned in multiple papers. These include spoofing (six times), denial-of-service (five times), misuse (five times), tampering (four times), information disclosure (four times), injection (four times), and malicious virtual machine migration (three times).

**Table 2.** Appearances of attack patterns in at least two papers

Attack Pattern Name	Number of Appearances
Spoofing	6
Denial-of-service (DoS)	5
Misuse	5
Tampering	4
Information disclosure	4
Injection	4
Malicious Virtual Machine Migration	3
Repudiation	2
Integrity	2
Message secrecy violation	2
Session state poisoning	2
Elevation of privilege	2
Theft of services	2
Resource usage monitoring	2

**Figure 8.** Papers referencing the intended development methodology

Moreover, the abstraction varies widely. Some refer to abstract patterns in STRIDE, which is a categorization of attack patterns. Others discuss CIA security characteristics. One is specific to illegal money transfers in a certain application. Although attack patterns and security characteristics are common, specific examples are rare.

#### 4.5. Method

##### 4.5.1. Methodology

97 papers (40.4%) describe a development methodology (Fig. 8). Some discuss a methodology related to a model-driven approach (14.2%) or an aspect-oriented approach (2.1%). Although many development methodologies are reported, few examine security. As IoT becomes ubiquitous, studies on the methodology should intentionally focus on security by design.

**Table 3.** Pattern modeling notation

Group	Example	Number of Papers
UML	Class/Activity diagram	104 (43.3%)
Goal oriented	i*, KAOS, threat tree	13 (5.4%)
Formal	Z notation, formula	12 (5.0%)
Natural language	Text, structured document	12 (5.0%)
Original	Original notations	6 (2.5%)
Others	Process model, XML, OWL	65 (27.1%)
Not specified		77 (32.1%)

#### 4.5.2. Pattern modeling notation

The types of modeling notations used in security-pattern research are examined. About two-third of the papers represent the notations of security patterns, which can be categorized into six groups. Table 3 shows the groupings, where multiple groups indicate papers using multiple notations. The "UML" group includes UML diagrams and UML based notations. The "Goal-oriented," "Formal," and "Natural language" groups include models used in goal-oriented methods, formal notations, and natural language notations, respectively.

Security patterns are mostly UML, which is reasonable since UML is generally accepted for modeling software and systems. In papers that address specific development methods or tools, formal, goal-oriented, and natural language notations are used in 13, 12, and 12 papers, respectively. Moreover, about one-third of papers do not describe the notations of security patterns. In the future, the notation should be described to clarify security patterns.

#### 4.5.3. Relationship between patterns

Because security patterns are often applied as combinations, their relationships must be clarified. There are two types of relationships between patterns: between security patterns (relationship A) to enhance described security methods by combination, and between an attack pattern and a security pattern to reduce risks (relationship B).

Of the 240 papers, 98 papers (40.8%) focus on relationship A. Only 5.8% (14) mention relationship B. These results demonstrate that security pattern combinations are often not considered. In the future, pattern research on analysis and development processes to understand specific security risks, to reduce such risks, and to identify security pattern relationships needs to be conducted with an emphasis on relationship B.

### 5. Conclusion and Future Work

In this paper, a new taxonomy for security pattern research is devised via an SLR. To clarify the state-of-the-art and future directions of security pattern research from various facets including topics and security characteristics, this taxonomy categorized 240 papers.

This taxonomy analyzed the contents of 240 security pattern research papers identified through an SLR, demonstrating its usefulness in security pattern research. This taxonomy should also support communications among researchers, practitioners, and stakeholders. Hence, it should improve the not only the quality but also the effectiveness of security patterns. The results show that a taxonomy can be developed to provide evidence-based guidelines for researchers and practitioners. Herein 13 facets are used to define the taxonomy. There are two types of security patterns, but most focus on security patterns and not attack patterns.

Future efforts include experimentally verifying our taxonomy using the two use cases (UC1 and UC2) in Section 3. We will implement a collaborative Wiki so that the community can refine and modify the taxonomy online. In addition, we intend to enhance our SLR to include other databases and

additional categories and datasets. Our findings will be shared with the public so that our taxonomy can be validated and revised by the community and standard terminology can be defined.

**Author Contributions:** Conceptualization and methodology, Hironori Washizaki.; literature review and analysis, all authors. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was supported by the SCAT Research Grant, the MEXT enPiT-Pro Smart SE: Smart Systems and Services innovative professional Education program, the JSPS KAKENHI grant number 16H02804, and the JSPS KAKENHI grant number 17K00475.

**Acknowledgments:** The authors thank Dr. Dan Yamamoto and Dr. Takafumi Komoto for their helps.

## References

1. Yoshioka, N.; Washizaki, H.; Maruyama, K. A survey on security patterns. *Progress in Informatics* **2008**, pp. 35–48. doi:10.2201/NiiPi.2008.5.5.
2. Ito, Y.; Washizaki, H.; Yoshizawa, M.; Fukazawa, Y.; Okubo, T.; Kaiya, H.; Hazeyama, A.; Yoshioka, N.; Fernandez, E. Systematic Mapping of Security Patterns Research. Proceedings of the 22nd Conference on Pattern Languages of Programs Conference 2015 (PLoP 2015), 2015.
3. Babar, M.; Zhang, H. Systematic literature reviews in software engineering: Preliminary results from interviews with researchers. Proceedings of the Third International Symposium on Empirical Software Engineering and Measurement, ESEM 2009, October 15-16, 2009, Lake Buena Vista, Florida, USA, 2009, pp. 346–355.
4. Bouaziz, et al., R. A collaborative process for developing secure component based applications. Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE, 2014.
5. Alvi, et al., A. A comparative study of software security pattern classifications. Proceedings - 2012 7th International Conference on Availability, Reliability and Security, ARES 2012, 2012.
6. Uzunov, et al., A. A comprehensive pattern-driven security methodology for distributed systems. Proceedings of the Australian Software Engineering Conference, ASWEC, 2014.
7. Uzunov, et al., A.F. A comprehensive pattern-oriented approach to engineering security methodologies. *Inf Softw Technol*, 2015.
8. Bouaziz, et al., R. A decision support map for security patterns application. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015.
9. Balopoulos, et al., T. A framework for exploiting security expertise in application development. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2006.
10. Guan, et al., H. A framework for security driven software evolution. ICAC 2014 - Proceedings of the 20th International Conference on Automation and Computing: Future Automation, Computing and Manufacturing, 2014.
11. Singpant, et al., P. A method for web security context patterns development from user interface Guidelines based on structural and textual analysis. *Lecture Notes in Electrical Engineering*, 2015.
12. Abramov, et al., J. A methodology for integrating access control policies within database development. *Computers and Security*, 2012.
13. Ryoo, et al., J. A methodology for mining security tactics from security patterns. Proceedings of the Annual Hawaii International Conference on System Sciences, 2010.
14. Fernandez, et al., E. A methodology to develop secure systems using patterns. *Integrating Security and Software Engineering: Advances and Future Visions*, 2006.
15. Hamid, et al., B. A modeling and formal approach for the precise specification of security patterns. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014.
16. VanHilst, et al., M. A multi-dimensional classification for users of security patterns. *Journal of Research and Practice in Information Technology*, 2009.
17. Alvi, et al., A. A natural classification scheme for software security patterns. Proceedings - IEEE 9th International Conference on Dependable, Autonomic and Secure Computing, DASC 2011, 2011.

18. Mourad, et al., A. A novel approach for the development and deployment of security patterns. Proceedings - SocialCom 2010: 2nd IEEE International Conference on Social Computing, PASSAT 2010: 2nd IEEE International Conference on Privacy, Security, Risk and Trust, 2010.
19. Abramov, et al., J. A pattern based approach for secure database design. Lecture Notes in Business Information Processing, 2011.
20. Benameur, et al., A. A pattern-based general security framework : AAAAn ebusiness case study. 2009 11th IEEE International Conference on High Performance Computing and Communications, HPCC 2009, 2009.
21. Schnjakin, et al., M. A pattern-driven security advisor for service-oriented architectures. Proceedings of the ACM Conference on Computer and Communications Security, 2009.
22. Delessy, et al., N. A pattern-driven security process for SOA applications. Proceedings of the ACM Symposium on Applied Computing, 2008.
23. Ratchakom, et al., M. A process model design and tool support for information assets access control using security patterns. Proceedings of the 2011 8th International Joint Conference on Computer Science and Software Engineering, JCSSE 2011, 2011.
24. Halkidis, et al., S. A qualitative analysis of software security patterns. Computers and Security, 2006.
25. Rui, et al., J. A security engineering process for systems of systems using security patterns. 8th Annual IEEE International Systems Conference, SysCon 2014 - Proceedings, 2014.
26. Varela-Vaca, et al., A. A security pattern-driven approach toward the automation of risk treatment in business processes. Advances in Intelligent Systems and Computing, 2013.
27. Fernandez, et al., E. A Security Reference Architecture for cloud systems. ACM International Conference Proceeding Series, 2014.
28. Tekbacak, et al., F. A semantic based certification and access control approach using security patterns on SEAGENT. 20th International Conference on Software Engineering and Knowledge Engineering, SEKE 2008, 2008.
29. Rosado, et al., D. A study of security architectural patterns. Proceedings - First International Conference on Availability, Reliability and Security, ARES 2006, 2006.
30. Uzunov, A. A survey of security solutions for distributed publish/subscribe systems. Computers and Security, 2016.
31. Ahmed, et al., N. A taxonomy for assessing security in business process modelling. Proceedings - International Conference on Research Challenges in Information Science, 2013.
32. Bergmann, et al., G. A tool for managing evolving security requirements. Lecture Notes in Business Information Processing, 2012.
33. Fernandez, et al., E. A UML-based methodology for secure systems: The design stage. Proceedings of the 3rd International Workshop on Security in Information Systems, WOSIS 2005, in Conjunction with ICEIS 2005, 2005.
34. Fernandez, E.; Washizaki, H.; Yoshioka, N. Abstract security patterns. Proceedings of the 15th Conference on Pattern Languages of Programs (PLoP'08), 2008.
35. Fernandez, et al., E. Abstract security patterns for requirements specification and analysis of secure systems. CIBSE 2014: Proceedings of the 17th Ibero-American Conference Software Engineering, 2014.
36. Busnel, et al., P. Achieving socio-technical confidentiality using security pattern in smart homes. Proceedings of the 2008 2nd International Conference on Future Generation Communication and Networking, FGCN 2008, 2008.
37. Heyman, et al., T. An analysis of the security patterns landscape. Proceedings - ICSE 2007 Workshops: Third International Workshop on Software Engineering for Secure Systems, SESS'07, 2007.
38. Bouaziz, et al., R. An approach for security patterns application in component based models. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2014.
39. Fernandez, et al., E. An approach to model-based development of secure and reliable systems. Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011, 2011.
40. Serrano, et al., D. An architecture for secure ambient intelligence environments. Advances in Soft Computing, 2009.

41. Bunke, et al., M. An architecture-centric approach to detecting security patterns in software. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2011.
42. Mouheb, et al., D. An aspect-oriented approach for software security hardening: From design to implementation. *Proceedings of 8th International Conference on New Trends in Software Methodologies, Tools and Techniques, SoMeT 09*, 2009.
43. Mourad, et al., A. An aspect-oriented approach for the systematic security hardening of code. *Computers and Security*, 2008.
44. Alebrahim, et al., A. An aspect-oriented approach to relating security requirements and access control. *CEUR Workshop Proceedings*, 2012.
45. He, et al., K. An attack scenario based approach for software security testing at design stage. *Proceedings - International Symposium on Computer Science and Computational Technology, ISCSCT 2008*, 2008.
46. Bouaziz, et al., R. An engineering process for security patterns application in component based models. *Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE*, 2013.
47. Alakula, et al., M.L. An experience report of improving business process compliance using security risk-oriented patterns. *Lecture Notes in Business Information Processing*, 2015.
48. Noel, et al., R. An exploratory comparison of security patterns and tactics to harden systems. *CIBSE 2014: Proceedings of the 17th Ibero-American Conference Software Engineering*, 2014.
49. El, et al., K.P. An ontological interface for software developers to select security patterns. *Proceedings - International Workshop on Database and Expert Systems Applications, DEXA*, 2008.
50. Guan, et al., H. An ontology-based approach to security pattern selection. *International Journal of Automation and Computing*, 2016.
51. Hwang, et al., G.H. An operational model and language support for securing XML documents. *Computers and Security*, 2004.
52. Ortiz, et al., R. Analysis of application of security patterns to build secure systems. *Lecture Notes in Business Information Processing*, 2011.
53. Li, et al., T. Analyzing and enforcing security mechanisms on requirements specifications. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015.
54. Ortiz, et al., R. Applicability of security patterns. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2010.
55. Changadwech, et al., C. Applying information retrieval technique for security requirements verification based on security patterns. *Lecture Notes in Engineering and Computer Science*, 2016.
56. Bouaziz, et al., R. Applying security patterns for component based applications using UML profile. *Proceedings - 15th IEEE International Conference on Computational Science and Engineering, CSE 2012 and 10th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, EUC 2012*, 2012.
57. Halkidis, S.; Tsantalis, N.; Chatzigeorgiou, A.; Stephanides, G. Architectural risk analysis of software systems based on security patterns. *IEEE Transactions on Dependable and Secure Computing*, 2008.
58. Uzunov, et al., A. ASE: A comprehensive pattern-driven security methodology for distributed systems. *Computer Standards and Interfaces*, 2015.
59. Steinegger, et al., R. Attack surface reduction for web services based on authorization patterns. *SECURWARE 2014 - 8th International Conference on Emerging Security Information, Systems and Technologies*, 2014.
60. Warschofsky, et al., R. Automated security service orchestration for the identity management in Web Service based systems. *Proceedings - 2011 IEEE 9th International Conference on Web Services, ICWS 2011*, 2011.
61. Dong, J. Automated verification of security pattern compositions. *Information and Software Technology*, 2010.
62. Gunawan, et al., L. Behavioral singletons to consistently handle global states of security patterns. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2012.



63. Tatsubori, et al., M. Best-practice patterns and tool support for configuring secure web services messaging. Proceedings - IEEE International Conference on Web Services, 2004.
64. Fernandez, et al., E. Building a security reference architecture for cloud systems. Requirements Engineering, 2016.
65. Rimba, P. Building high assurance secure applications using security patterns for capability-based platforms. Proceedings - International Conference on Software Engineering, 2013.
66. Fernandez, et al., E. Building secure systems: From threats to security patterns. Proceedings - International Conference of the Chilean Computer Science Society, SCCC, 2011.
67. Bayley, I. Challenges for a formal framework for patterns. Cyberpatterns: Unifying Design Patterns with Security and Attack Patterns, 2014.
68. Slavin, et al., R. Characterizations and boundaries of security requirements patterns. 2012 2nd IEEE International Workshop on Requirements Patterns, RePa 2012 - Proceedings, 2012.
69. Fernandez, et al., E. Classifying security patterns. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2008.
70. Rimba, et al., P. Composing Patterns to Construct Secure Systems. Proceedings - 2015 11th European Dependable Computing Conference, EDCC 2015, 2015.
71. Alzahrani, et al., A. Conformance checking of single access point pattern in JAAS using codecharts. 2015 World Congress on Information Technology and Computer Applications, WCITCA 2015, 2015.
72. Schmidt, et al., H. Connecting security requirements analysis and secure design using patterns and UMLsec. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2011.
73. Ouedraogo, et al., W. Context-aware Security@run.time deployment. CLOSER 2015 - 5th International Conference on Cloud Computing and Services Science, Proceedings, 2015.
74. Bouaziz, et al., R. C-SCRIP: Collaborative security pattern integration process. International Journal of Information Technology and Web Engineering, 2015.
75. Li, et al., T. Dealing with security requirements for socio-technical systems: A holistic approach. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2014.
76. Tian, et al., K. Defining re-usable composite aspect patterns: An FDAF based approach. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2008.
77. Rosado, et al., D. Defining security architectural patterns based on viewpoints. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2007.
78. Rosado, et al., D. Defining viewpoints for security architectural patterns. SECRIPT 2006 - International Conference on Security and Cryptography, Proceedings, 2006.
79. Fernandez, et al., E. Designing secure SCADA systems using security patterns. Proceedings of the Annual Hawaii International Conference on System Sciences, 2010.
80. Gymnopoulos, et al., L. Developing a security patterns repository for secure applications design. 5th European Conference on Information Warfare and Security 2006, ECIW 2006, 2006.
81. Serrano, et al., D. Development of applications based on security patterns. Proceedings - 2009 2nd International Conference on Dependability, DEPEND 2009, 2009.
82. Yskout, et al., K. Do security patterns really help designers? Proceedings - International Conference on Software Engineering, 2015.
83. Yskout, et al., K. Does organizing security patterns focus architectural choices? Proceedings - International Conference on Software Engineering, 2012.
84. Gandhi, et al., R. Early security patterns: A collection of constraints to describe regulatory security requirements. 2012 2nd IEEE International Workshop on Requirements Patterns, RePa 2012 - Proceedings, 2012.
85. Okubo, et al., T. Effective security impact analysis with patterns for software enhancement. Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011, 2011.
86. Mathew, G. Elements of application security in the cloud computing environment. 2012 IEEE Conference on Open Systems, ICOS 2012, 2012.



87. Braz, et al., F. Eliciting security requirements through misuse activities. Proceedings - International Workshop on Database and Expert Systems Applications, DEXA, 2008.
88. Solinas, et al., M. Embedding security patterns into a domain model. Proceedings - International Workshop on Database and Expert Systems Applications, DEXA, 2009.
89. Yu, et al., Y. Enforcing a security pattern in stakeholder goal models. Proceedings of the ACM Conference on Computer and Communications Security, 2008.
90. Khoury, et al., P. Enforcing security in smart homes using security patterns. International Journal of Smart Home, 2009.
91. Uzunov, et al., A. Engineering Security into Distributed Systems: A Survey of Methodologies. Journal of Universal Computer Science, 2012.
92. Katt, et al., B. Enhancing model driven security through pattern refinement techniques. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2013.
93. Supaporn, et al., K. Enterprise assets security requirements construction from ESRMG grammar based on security patterns. Proceedings - Asia-Pacific Software Engineering Conference, APSEC, 2007.
94. Moral-Garcia, et al., S. Enterprise security pattern: A model-driven architecture instance. Computer Standards and Interfaces, 2014.
95. Moral-Garcia, et al., S. Enterprise security pattern: A new type of security pattern. Security and Communication Networks, 2014.
96. Faily, et al., S. Evaluating the implications of attack and security patterns with premortems. Cyberpatterns: Unifying Design Patterns with Security and Attack Patterns, 2014.
97. Abramov, et al., J. Evaluation of the Pattern-based method for Secure Development (PbSD): A controlled experiment. Information and Software Technology, 2012.
98. Dalai, et al., A. Evaluation of web application security risks and secure design patterns. ACM International Conference Proceeding Series, 2011.
99. Hafiz, et al., M. Evolution of the MTA architecture: The impact of security. Software - Practice and Experience, 2008.
100. Van, et al., V.A. Exploring information security issues in public sector inter-organizational collaboration. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2011.
101. Savic, et al., D. Extended software architecture based on security patterns. Informatica, 2010.
102. Robinson, P. Extensible security patterns. Proceedings - International Workshop on Database and Expert Systems Applications, DEXA, 2007.
103. Munoz, et al., A. Facilitating the use of TPM technologies using the serenity framework. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2011.
104. Near, et al., J. Finding security bugs in web applications using a catalog of access control patterns. Proceedings - International Conference on Software Engineering, 2016.
105. Ruamjinda, et al., P. Framework for information security standards storage and retrieval using security patterns. Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS, 2013.
106. Horvath, et al., V. From security patterns to implementation using Petri nets. Proceedings - International Conference on Software Engineering SESS2008, 2008.
107. Hafiz, et al., M. Growing a pattern language (for security). SPLASH 2012: Onward! 2012 - Proceedings of the ACM International Symposium on New Ideas, New Paradigms, and Reflections on Programming and Software, 2012.
108. Dikanski, et al., A. Identification and implementation of authentication and authorization patterns in the spring security framework. SECURWARE 2012 - 6th International Conference on Emerging Security Information, Systems and Technologies, 2012.
109. Patu, et al., V. Identifying and implementing security patterns for a dependable security case - From security patterns to D-case. Proceedings - 16th IEEE International Conference on Computational Science and Engineering, CSE 2013, 2013.

110. Yoshizawa, et al., M. Implementation support of security design patterns using test templates. Information (Switzerland), 2016.
111. Edge, et al., C. Improving security design patterns with aspect-oriented strategies. Proceedings of the Annual Southeast Conference, 2012.
112. Washizaki, et al., H. Improving the classification of security patterns. Proceedings - International Workshop on Database and Expert Systems Applications, DEXA, 2009.
113. Netter, et al., M. Integrating security patterns into the electronic invoicing process. Proceedings - International Workshop on Database and Expert Systems Applications, DEXA, 2009.
114. Li, et al., T. Integrating security patterns with security requirements analysis using contextual goal models. Lecture Notes in Business Information Processing, 2014.
115. Schaeffer-Filho, et al., A. Management patterns for network resilience: Design and verification of policy configurations. Cyberpatterns: Unifying Design Patterns with Security and Attack Patterns, 2014.
116. Fernandez, et al., E. Measuring the level of security introduced by security patterns. ARES 2010 - 5th International Conference on Availability, Reliability, and Security, 2010.
117. Dong, et al., J. Model checking security pattern compositions. Proceedings - International Conference on Quality Software, 2007.
118. Shiroma, et al., Y. Model-driven security patterns application based on dependences among patterns. ARES 2010 - 5th International Conference on Availability, Reliability, and Security, 2010.
119. Nguyen, et al., P. Model-driven security with a system of aspect-oriented security design patterns. ACM International Conference Proceeding Series, 2014.
120. Li, et al., T. Modeling and applying security patterns using contextual goal models. CEUR Workshop Proceedings, 2014.
121. Dai, et al., L. Modeling and performance analysis for security aspects. Science of Computer Programming, 2006.
122. Asnar, et al., Y. Modeling design patterns with description logics: A case study. Beijing Daxue Xuebao (Ziran Kexue Ban)/Acta Scientiarum Naturalium Universitatis Pekinensis, 2011.
123. Fernandez, et al., E. Modeling misuse patterns. Proceedings - International Conference on Availability, Reliability and Security, ARES 2009, 2009.
124. Mouratidis, et al., H. Modeling secure systems using an agent-oriented approach and security patterns. International Journal of Software Engineering and Knowledge Engineering, 2006.
125. Weiss, M. Modelling security patterns using NFR analysis. Integrating Security and Software Engineering: Advances and Future Visions, 2006.
126. Halkidis, et al., S. Moving from requirements to design confronting security issues: A case study. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2009.
127. Mourad, et al., A. New Approach Targeting Security Patterns Development and Deployment. Information Security Journal, 2011.
128. Fernandez, et al., E. On building secure SCADA systems using security patterns. ACM International Conference Proceeding Series, 2009.
129. Bunke, M. On the description of software security patterns. ACM International Conference Proceeding Series, 2014.
130. Hafiz, et al., M. Organizing security patterns. IEEE Software, 2007.
131. Dove, R. Pattern qualifications and examples of next-generation agile system-security strategies. Proceedings - International Carnahan Conference on Security Technology, 2010.
132. Rrenja, et al., A. Pattern-based security requirements derivation from secure tropos models. Lecture Notes in Business Information Processing, 2015.
133. Fernandez, et al., E. Patterns and pattern diagrams for access control. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2008.
134. Fernandez, E.; Yoshioka, N.; Washizaki, H. Patterns for security and privacy in cloud ecosystems. Proceedings of the 2nd International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE 2015), 2015.
135. Hafiz, et al., M. Patterns transform architectures. Proceedings - 9th Working IEEE/IFIP Conference on Software Architecture, WICSA 2011, 2011.

136. Thomsen, D. Practical policy patterns. CODASPY'11 - Proceedings of the 1st ACM Conference on Data and Application Security and Privacy, 2011.
137. Hazeyama, et al., A. Preliminary evaluation of a software security learning environment. *Studies in Computational Intelligence*, 2015.
138. Fernandez, E. Preventing and unifying threats in cyberphysical systems. *Proceedings of IEEE International Symposium on High Assurance Systems Engineering*, 2014.
139. Romanosky, et al., S. Privacy patterns for online interactions. *PLoP 2006 - PLoP Pattern Languages of Programs 2006 Conference Proceedings*, 2006.
140. Alebrahim, et al., A. Problem-oriented security patterns for requirements engineering. *ACM International Conference Proceeding Series*, 2014.
141. Halkidis, S.; Chatzigeorgiou, A.; Stephanides, G. Quantitative evaluation of systems with security patterns using a fuzzy approach. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2006.
142. Hafner, et al., M. Realizing model driven security for inter-organizational workflows with WS-CDL and UML 2.0 bringing web services, security and UML together. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2005.
143. Netter, et al., M. Refining the pattern-based reference model for electronic invoices by incorporating threats. *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*, 2010.
144. Heyman, et al., T. Reusable formal models for secure software architectures. *Proceedings of the 2012 Joint Working Conference on Software Architecture and 6th European Conference on Software Architecture, WICSA/ECSA 2012*, 2012.
145. Fernandez, et al., E. Revisiting architectural tactics for security. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015.
146. Bouaziz, et al., R. SCRISTUDIO: A security pattern integration tool. *2016 International Conference on Information Technology for Organizations Development, IT4OD 2016*, 2016.
147. Bergmann, et al., G. SeCMER: A tool to gain control of security requirements evolution. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2011.
148. Hafner, et al., M. Sectet: An extensible framework for the realization of secure inter-organizational workflows. *Internet Research*, 2006.
149. Bouaziz, et al., R. Secure component based applications through security patterns. *Proceedings - 2012 IEEE Int. Conf. on Green Computing and Communications, GreenCom 2012, Conf. on Internet of Things, iThings 2012 and Conf. on Cyber, Physical and Social Computing, CPSCoM 2012*, 2012.
150. Ruiz, et al., J. Secure engineering and modelling of a metering devices system. *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, 2013.
151. Fernandez, et al., E. Securing analysis patterns. *Proceedings of the Annual Southeast Conference*, 2007.
152. Uzunov, et al., A. Securing distributed systems using patterns: A survey. *Computers and Security*, 2012.
153. Sohn, et al., J.W. Securing web applications with better 'Patches': An architectural approach for systematic input validation with security patterns. *Proceedings - 10th International Conference on Availability, Reliability and Security, ARES 2015*, 2015.
154. Armenteros, et al., A. Security and dependability in ambient intelligence scenarios: The communication prototype. *ICEIS 2009 - 11th International Conference on Enterprise Information Systems, Proceedings*, 2009.
155. Laverdiere, et al., M.A. Security design patterns: Survey and evaluation. *Canadian Conference on Electrical and Computer Engineering*, 2007.
156. Memon, et al., M. Security modeling for service-oriented systems using security pattern refinement approach. *Software and Systems Modeling*, 2014.
157. Duncan, et al., I. Security pattern evaluation. *Proceedings - IEEE 8th International Symposium on Service Oriented System Engineering, SOSE 2014*, 2014.
158. Sarmah, et al., A. Security Pattern Lattice: A formal model to organize Security Patterns. *Proceedings - International Workshop on Database and Expert Systems Applications, DEXA*, 2008.

159. Moral-Garcia, et al., S. Security pattern mining: Systematic review and proposal. Proceedings of the 8th International Workshop on Security in Information Systems, WOSIS 2011, in Conjunction with ICEIS 2011, 2011.
160. Fernandez, E. Security patterns and a methodology to apply them. *Advances in Information Security*, 2009.
161. Rosado, et al., D. Security patterns and requirements for internet-based applications. *Internet Research*, 2006.
162. Fernandez, E. Security patterns and secure systems design. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2007.
163. Cuevas, et al., A. Security patterns for capturing encryption-based access control to sensor data. Proceedings - 2nd Int. Conf. Emerging Security Inf., Systems and Technologies, SECURWARE 2008, Includes DEPEND 2008: 1st Int. Workshop on Dependability and Security in Complex and Critical Inf. Sys., 2008.
164. Mouratidis, et al., H. Security patterns meet agent oriented software engineering: A complementary solution for developing secure information systems. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2005.
165. Hamid, et al., B. Security patterns modeling and formalization for pattern-based development of secure software systems. *Innovations in Systems and Software Engineering*, 2016.
166. Yoshioka, et al., N. Security patterns: A method for constructing secure and efficient inter-company coordination systems. Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOC, 2004.
167. Nhlabatsi, A.; Bandara, A.; Hayashi, S.; Haley, C.; Jurjens, J.; Kaiya, H.; Kubo, A.; Laney, R.; Mouratidis, H.; Nuseibeh, B.; Tun, T.; Washizaki, H.; Yoshioka, N.; Yu, Y. Security patterns: Comparing modeling approaches. *Software Engineering for Secure Systems: Industrial and Research Perspectives*, 2010.
168. Menzel, et al., M. Security requirements specification in service-oriented business process management. Proceedings - International Conference on Availability, Reliability and Security, ARES 2009, 2009.
169. Uzunov, et al., A. Security solution frames and security patterns for authorization in distributed, collaborative systems. *Computers and Security*, 2015.
170. Hasheminejad, et al., S. Selecting proper security patterns using text classification. Proceedings - 2009 International Conference on Computational Intelligence and Software Engineering, CiSE 2009, 2009.
171. Serrano, et al., D. SERENITY Aware System Development Process. *Advances in Information Security*, 2009.
172. Sanchez-Cid, et al., F. SERENITY pattern-based software development life-cycle. Proceedings - International Workshop on Database and Expert Systems Applications, DEXA, 2008.
173. Sanchez-Cid, et al., F. Software engineering techniques applied to AmI: Security patterns. *Developing Ambient Intelligence - Proceedings of the First International Conference on Ambient Intelligence Developments, AmID 2006*, 2006.
174. Tryfonas, et al., T. Standardising business application security assessments with pattern-driven audit automations. *Computer Standards and Interfaces*, 2008.
175. Alzahrani, et al., A. Structural analysis of the check point pattern. Proceedings - IEEE 8th International Symposium on Service Oriented System Engineering, SOSE 2014, 2014.
176. Babar, et al., M. Supporting security sensitive architecture design. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2005.
177. Hazeyama, A. Survey on body of knowledge regarding software security. Proceedings - 13th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, SNPD 2012, 2012.
178. Porekar, et al., J. Technical patterns for long term trusted archiving. Proceedings of the 3rd International Conference on Digital Society, ICDS 2009, 2009.
179. Kobashi, et al., T. TESEM: A tool for verifying security design pattern applications by model testing. 2015 IEEE 8th International Conference on Software Testing, Verification and Validation, ICST 2015 - Proceedings, 2015.
180. Morrison, et al., P. The credentials pattern. *PLoP 2006 - PLoP Pattern Languages of Programs 2006 Conference Proceedings*, 2006.

181. Ciria, et al., J. The history-based authentication pattern. *ACM International Conference Proceeding Series*, 2014.
182. Alkussayer, et al., A. The ISDF framework: Integrating security patterns and best practices. *Communications in Computer and Information Science*, 2009.
183. Hafiz, et al., M. The nature of order: From security patterns to a pattern language. *SPLASH'12 - Proceedings of the 2012 ACM Conference on Systems, Programming, and Applications: Software for Humanity*, 2012.
184. Gutierrez, et al., C. The practical application of a process for eliciting and designing security in web service systems. *Information and Software Technology*, 2009.
185. Shahzad, et al., A. The security survey and analysis on supervisory control and data acquisition communication. *Journal of Computer Science*, 2014.
186. Heyman, et al., T. The Security Twin Peaks. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2011.
187. De, et al., M.H.J. Thinking towards a pattern language for predicate based encryption crypto-systems. *Proceedings of the 2012 IEEE 6th International Conference on Software Security and Reliability Companion, SERE-C 2012*, 2012.
188. Okubo, et al., T. Threat and countermeasure patterns for cloud computing. *2014 IEEE 4th International Workshop on Requirements Patterns, RePa 2014 - Proceedings*, 2014.
189. Anand, et al., P. Threat assessment in the cloud environment - A quantitative approach for security pattern selection. *ACM IMCOM 2016: Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication*, 2016.
190. Bouaziz, et al., R. Towards a better integration of patterns in secure component-based systems design. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2011.
191. Graziano, et al., A. Towards a classification framework for security patterns. *Proceedings of the 6th International Network Conference, INC 2006*, 2006.
192. Blackwell, C. Towards a conceptual framework for security patterns. *Cyberpatterns: Unifying Design Patterns with Security and Attack Patterns*, 2014.
193. Fuchs, et al., A. Towards a generic process for security pattern integration. *Proceedings - International Workshop on Database and Expert Systems Applications, DEXA*, 2009.
194. Hafner, et al., M. Towards a MOF/QVT-based domain architecture for model driven security. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2006.
195. Ortiz, et al., R. Towards a pattern-based security methodology to build secure information systems. *Proceedings of the 8th International Workshop on Security in Information Systems, WOSIS 2011, in Conjunction with ICEIS 2011*, 2011.
196. Fernandez, et al., E. Towards compliant reference architectures by finding analogies and overlaps in compliance regulations. *SECURITY 2015 - 12th International Conference on Security and Cryptography, Proceedings; Part of 12th International Joint Conference on e-Business and Telecommunications, ICETE 2015*, 2015.
197. Kozlovs, et al., D. Towards continuous information security audit. *CEUR Workshop Proceedings*, 2016.
198. Alebrahim, et al., A. Towards developing secure software using problem-oriented security patterns. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014.
199. Serrano, et al., D. Towards precise security patterns. *Proceedings - International Workshop on Database and Expert Systems Applications, DEXA*, 2008.
200. Ferreira, et al., A. Usability and security patterns. *Proceedings of the 2nd International Conferences on Advances in Computer-Human Interactions, ACHI 2009*, 2009.
201. Fernandez, et al., E. Using patterns to understand and compare Web services security products and standards. *Proceedings of the Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services, AICT/ICIW'06*, 2006.
202. Heckman, et al., M. Using proven Reference Monitor patterns for security evaluation. *Information (Switzerland)*, 2016.



203. Aziz, et al., B. Using security patterns for modelling security capabilities in grid systems. Proceedings - IEEE 8th International Symposium on Service Oriented System Engineering, SOSE 2014, 2014.
204. Heyman, et al., T. Using security patterns to combine security metrics. ARES 2008 - 3rd International Conference on Availability, Security, and Reliability, Proceedings, 2008.
205. Fernandez, E.; Yoshioka, N.; Washizaki, H.; Jurjens, J.; VanHilst, M.; Pernul, G. Using security patterns to develop secure systems. Software Engineering for Secure Systems: Industrial and Research Perspectives, 2010.
206. Wagner, et al., R. Using security patterns to tailor software process. SEKE 2011 - Proceedings of the 23rd International Conference on Software Engineering and Knowledge Engineering, 2011.
207. Fernandez, et al., E. Using UML and security patterns to teach secure systems design. ASEE Annual Conference and Exposition, Conference Proceedings, 2005.
208. Kobashi, et al., T. Validating security design patterns application using model testing. Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013, 2013.
209. Yoshizawa, et al., M. Verifying implementation of security design patterns using a test template. Proceedings - 9th International Conference on Availability, Reliability and Security, ARES 2014, 2014.
210. Anand, et al., P. Vulnerability-based security pattern categorization in search of missing patterns. Proceedings - 9th International Conference on Availability, Reliability and Security, ARES 2014, 2014.
211. Okubo, et al., T. Web security patterns for analysis and design. PLoP08 - 15th Conference on Pattern Languages of Programs, Proceedings, 2008.
212. King, et al., A. Wireless Information security system via role based access control pattern use case design. Proceedings of the 2008 International Conference on Computing, Communication and Networking, ICCCN 2008, 2008.
213. Barhoom, et al., T. XML context's security patterns language: Description and syntax. Information Technology Journal, 2007.
214. Regainia, et al., L. A classification methodology for security patterns to help fix software weaknesses. Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA, 2017.
215. Trubiani, et al., C. Exploiting traceability uncertainty between software architectural models and extra-functional results. Journal of Systems and Software, 2017.
216. Motii, et al., A. Guiding the Selection of Security Patterns for Real-Time Systems. Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, ICECCS, 2017.
217. Anand, et al., P. Addressing Security Challenges in Cloud Computing - A Pattern-Based Approach. Proceedings - 2015 1st International Conference on Software Security and Assurance, ICSSA 2015, 2017.
218. Regainia, et al., L. A methodology of security pattern classification and of attack-defense tree generation. ICISSP 2017 - Proceedings of the 3rd International Conference on Information Systems Security and Privacy, 2017.
219. Amorim, et al., T. Systematic pattern approach for safety and security co-engineering in the automotive domain. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2017.
220. Nafees, et al., T. Idea-caution before exploitation: The use of cybersecurity domain knowledge to educate software engineers against software vulnerabilities. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2017.
221. Shin, et al., M. Model-based design of reusable secure connectors. CEUR Workshop Proceedings, 2017.
222. Salva, et al., S. Using data integration for security testing. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2017.
223. Argyropoulos, et al., N. Supporting secure business process design via security process patterns. Lecture Notes in Business Information Processing, 2017.
224. Ruiz, et al., J. Security knowledge representation artifacts for creating secure IT systems. Computers and Security, 2017.
225. Sheta, et al., M. Anti-spyware security design patterns. Proceedings - 2016 6th International Conference on Instrumentation and Measurement, Computer, Communication and Control, IMCCC 2016, 2016.
226. Mazo, et al., R. Framework for engineering complex security requirements patterns. 2016 6th International Conference on IT Convergence and Security, ICITCS 2016, 2016.

227. Fernandez, E. Threat Modeling in Cyber-Physical Systems. Proceedings - 2016 IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, DASC 2016, 2016 IEEE 14th International Conference on Pervasive Intelligence and Computing, PICom 2016, 2016 IEEE 2nd International Conference on Big Data Intelligence and Computing, DataCom 2016 and 2016 IEEE Cyber Science and Technology Congress, CyberSciTech 2016, DASC-PICom-DataCom-CyberSciTech 2016, 2016.
228. Ur-Rehman, et al., O. Secure design patterns for security in smart metering systems. Proceedings - EMS 2015: UKSim-AMSS 9th IEEE European Modelling Symposium on Computer Modelling and Simulation, 2016.
229. Washizaki, et al., H. A Metamodel for Security and Privacy Knowledge in Cloud Services. Proceedings - 2016 IEEE World Congress on Services, SERVICES 2016, 2016.
230. Fernandez, E. Building secure cloud architectures using patterns. Proceedings - 2016 IEEE International Conference on Cloud Engineering Workshops, IC2EW 2016, 2016.
231. Ponde, et al., P. An analytical study of security patterns. ACM International Conference Proceeding Series, 2016.
232. Fernandez, et al., E. Modeling and security in cloud ecosystems. Future Internet, 2016.
233. He, et al., X. Modeling and analyzing security patterns using high level petri nets. Proceedings of the International Conference on Software Engineering and Knowledge Engineering, SEKE, 2016.
234. Motii, et al., A. Towards the integration of security patterns in UML Component-based Applications. CEUR Workshop Proceedings, 2016.
235. Motii, et al., A. Model-based real-time evaluation of security patterns: A SCADA system case study. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2016.
236. Horcas, et al., J.M. Automatic enforcement of security properties. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2016.
237. Lee, et al., K.H. Adaption of integrated secure guide for secure software development lifecycle. International Journal of Security and its Applications, 2016.
238. Bunke, M. Software-security patterns: Degree of maturity. ACM International Conference Proceeding Series, 2015.
239. Motii, et al., A. Guiding the selection of security patterns based on security requirements and pattern classification. ACM International Conference Proceeding Series, 2015.
240. Atymtayeva, et al., L. Improvement of security patterns strategy for information security audit applications. BMSD 2015 - Proceedings of the 5th International Symposium on Business Modeling and Software Design, 2015.
241. Rimba, et al., P. Building Secure Applications Using Pattern-Based Design Fragments. Proceedings of the IEEE Symposium on Reliable Distributed Systems, 2015.
242. Yoshioka, et al., N. A survey on security patterns. Progress in Informatics, 2008.
243. Kearney, et al., B. Security patterns for automated continuous auditing. Information Security Journal, 2008.
244. Washizaki, H.; Xia, T.; Kamata, N.; Fukazawa, Y.; Kanuka, H.; Yamaoto, D.; Yoshino, M.; Okubo, T.; Ogata, S.; Kaiya, H.; Kato, T.; Hazeyama, A.; Tanaka, T.; Yoshioka, N.; Priyalakshmi, G. Taxonomy and Literature Survey of Security Pattern Research. Proceedings of the IEEE Conference on Applications, Information and Network Security (AINS). IEEE Computer Society, 2018, pp. 87–92.
245. Kitchenham, B.; Brereton, O.P.; Budgen, D.; Turner, M.; Bailey, J.; Linkman, S. Systematic Literature Reviews in Software Engineering - A Systematic Literature Review. *Information and Software Technology* **2009**, *51*, 7–15.
246. dos Santos Marques, A.B.; Rodrigues, R.; Conte, T. Systematic Literature Reviews in Distributed Software Development: A Tertiary Study. 2012 IEEE Seventh International Conference on Global Software Engineering, Porto Alegre, Rio Grande do Sul, Brazil, August 27-30, 2012. IEEE Computer Society, 2012, pp. 134–143.
247. Dadwal, A.; Washizaki, H.; Fukazawa, Y.; Iida, T.; Mizoguchi, M.; Yoshimura, K. Prioritization in Automotive Software Testing: Systematic Literature Review. Proceedings of the 6th International Workshop on Quantitative Approaches to Software Quality co-located with 25th Asia-Pacific Software Engineering Conference (APSEC 2018), Nara, Japan, December 4, 2018, pp. 52–58.



248. Washizaki, H.; Uchida, H.; Khomh, F.; Guéhéneuc, Y. Studying Software Engineering Patterns for Designing Machine Learning Systems. 10th International Workshop on Empirical Software Engineering in Practice, IWSEEP 2019, Tokyo, Japan, December 13-14, 2019. IEEE, 2019, pp. 49–54.
249. Washizaki, H.; Ogata, S.; Hazeyama, A.; Okubo, T.; Fernandez, E.B.; Yoshioka, N. Landscape of Architecture and Design Patterns for IoT Systems. *IEEE Internet Things J.* **2020**, *7*, 10091–10101.
250. FIRST.Org. Common Vulnerability Scoring System v3.0: Specification Document. <https://www.first.org/cvss/>, 2015.
251. The MITRE Corporation. Common Weakness Enumeration Version 3.1. <https://cwe.mitre.org/>, 2018.
252. Xia, T.; Washizaki, H.; Kato, T.; Kaiya, H.; Ogata, S.; Fernandez, E.; Kanuka, H.; Yoshino, M.; Yamamoto, D.; Okubo, T.; Yoshioka, N.; Hazeyama, A. Cloud Security and Privacy Metamodel: Metamodel for Security and Privacy Knowledge in Cloud Services. MODELSWARD 2018 - Proceedings of the 6th International Conference on Model-Driven Engineering and Software Development. SciTePress, 2018.
253. Kang, K.C.; Cohen, S.G.; Hess, J.A.; Novak, W.E.; Peterson, A.S. Feature-Oriented Domain Analysis (FODA) Feasibility Study. *Technical Report CMU/SEI-90-TR-21* **1990**, pp. 1–148.
254. Czarnecki, K.; Helsen, S. Classification of Model Transformation Approaches. Proceedings of the OOPSLA Workshop on Generative Techniques in the Context of Model-Driven Architecture, 2003, pp. 1–17.
255. Washizaki, H.; Guéhéneuc, Y.; Khomh, F. ProMeTA: a taxonomy for program metamodels in program reverse engineering. *Empir. Softw. Eng.* **2018**, *23*, 2323–2358.
256. Smite, D.; Wohlin, C.; Galvina, Z.; Prikładnicki, R. An Empirically Based Terminology and Taxonomy for Global Software Engineering. *Empirical Software Engineering* **2014**, *19*, 105–153.
257. Shostack, A., Ed. *Threat Modeling: Designing for Security*, 1 ed.; Wiley, 2014.
258. The MITRE Corporation. Common Vulnerability and Exposures. <https://cve.mitre.org/>, 2018.
259. The MITRE Corporation. Common Attack Pattern Enumeration and Classification. <https://capec.mitre.org/>, 2018.