Taxonomy and Literature Survey of Security Pattern Research

Conference Paper · November 2018

DOI: 10.1109/AINS.2018.8631465

Hironori Washizaki
Waseda University
321 PUBLICATIONS **1,592** CITATIONS

Yoshiaki Fukazawa
Waseda University
327 PUBLICATIONS **1,311** CITATIONS

Hideyuki Kanuka
Hitachi, Ltd.
11 PUBLICATIONS **29** CITATIONS

Takao Okubo
Institute of Information Security
43 PUBLICATIONS **138** CITATIONS

Taxonomy and Literature Survey of Security Pattern Research

Hironori Washizaki, Tian Xia,
Natsumi Kamata, Yoshiaki Fukazawa
Waseda University
Tokyo, Japan, washizaki@waseda.jp

Hideyuki Kanuka, Dan Yamaoto,
Masayuki Yoshino
Hitachi, Ltd.
Kanagawa, Japan

Takao Okubo
Institute of Information Security
Kanagawa, Japan

Shinpei Ogata
Shinshu University
Nagano, Japan

Haruhiko Kaiya
Kanagawa University
Kanagawa, Japan

Takehisa Kato
Toshiba Digital Solutions Corporation
Kanagawa, Japan

Atsuo Hazeyama
Tokyo Gakugei University
Tokyo, Japan

Takafumi Tanaka
Tokyo University of Agriculture and Technology
Tokyo, Japan

Nobukazu Yoshioka
National Institute of Informatics
Tokyo, Japan

G Priyalakshmi
PSG College of Technology
Coimbatore, India

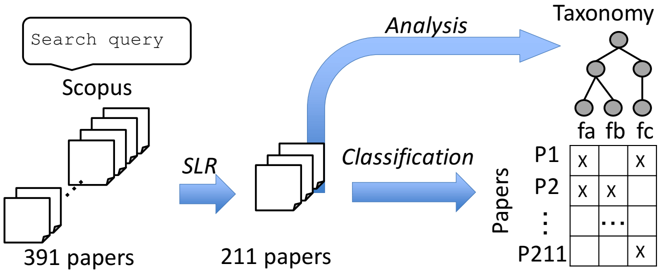
***Abstract*—Security patterns encapsulate security-related problems and solutions that recur in certain contexts for secure software system development and operations. Almost 500 security patterns have been proposed since the late 1990s. Technical investigations on their applications have advanced implementation, but the direction, overall picture, and significant technical challenges remain unclear. In this study, we propose a taxonomy for security pattern research by conducting a systematic literature review. Over 200 papers are categorized based on the taxonomy. The taxonomy is expected to guide practitioners to choose existing security pattern methods and tools. In addition, the taxonomy and the survey results should support communications among practitioners and researchers, and improve the quality of security pattern research and the effectiveness of security patterns.**

***Index Terms*—Security patterns, Systematic Literature Review**

I. Introduction

Security patterns, which are a level of abstraction, encapsulate security-related problems and solutions that recur in certain contexts for secure software system development and operations [1]. Many security patterns including concrete patterns [2]–[4] and abstract ones [5] have been proposed since the late 1990s. Implementing security patterns appropriately in software development is not trivial. Although technical investigations on their applications have advanced implementation, the direction, overall picture, and significant technical challenges remain unclear. In this study, we propose a taxonomy for security pattern research by conducting a systematic literature review (SLR) [6][1] to categorized the contents of over 200 studies.

The remainder of this paper is organized as follows. Section II shows the construction of our taxonomy and the SLR process. Section III outlines our taxonomy. Section IV describes the analysis results. Finally, our conclusion and future work are summarized in Section V.



	fa	fb	fc
P1	x		x
P2	x	x	
⋮		...	
P211			x

Fig. 1. Taxonomy construction process

II. Taxonomy Construction

We identified various characteristics to distinguish existing security pattern studies. A comprehensive taxonomy is proposed to classify security pattern research in the form of feature diagrams. In this study, we adopt a top-down approach to design the taxonomy of security pattern research. Figure 1 outlines the process.

Firstly, we clearly defined the purpose of the taxonomy. Our intent is to support stakeholders in classifying, comparing, reusing, and extending security pattern research. Additionally, the taxonomy should support communications among stakeholders and improve the accessibility of the research results.

Secondly, we conducted a SLR, which aims to aggregate existing evidence to address research questions and to support the development of evidence-based guidelines for researchers and practitioners [8]. We searched for papers about security pattern research using Scopus [2], which

[1] Although a systematic mapping study on security pattern research targeting only 30 papers has been reported [7], this is the first report of a rigorous SLR targeting more than 200 papers.

[2] https://www.scopus.com/

978-1-5386-6925-9/18/$31.00 ©2018 IEEE

is Elsevier's abstract and citation database by using the following search query: TITLE-ABS-KEY("security pattern") AND (LIMIT-TO(SUBJAREA,"COMP") OR LIMIT-TO(SUBJAREA,"ENGI")). Our query returned 391 papers. Then we applied the inclusion and exclusion criteria to verify the relevance of the returned papers. We included studies published in journals or conference proceedings in the form of papers employing security patterns for software and systems engineering. We excluded studies that propose or introduce security patterns without any further engineering activities such as analysis and application. For each paper, one author conducted the initial check, while another author confirmed the result of the initial check. In the case of disagreement, all authors discussed until a consensus was reached. Applying these criteria reduced the number of papers to 211 [3].

Thirdly, we merged the identified characteristics in existing security pattern research, existing standards (such as CVSS [9] and CWE [10]) as well as key concepts in the Security and Privacy Metamodel [11] into one structure in the form of feature diagrams [12]. Feature diagrams are trees that visualize the following relationships between a parent feature and its subfeatures (i.e., child features): "Mandatory", "Optional", "Or", and "Alternative". Mandatory means that a subfeature is required. Optional indicates a subfeature do not have to be selected. Or implies that at least one subfeature must be selected. Alternative denotes only one subfeature must be selected. A feature diagram essentially defines a taxonomy [13].

Finally, the taxonomy is validated in terms of its orthogonality by using it to classify the existing security pattern research identified in the SLR.

III. Taxonomy

We built the taxonomy (Fig. 2) to include five features as facets of categorization for security pattern research.

- Purpose: This includes the topics addressed by the security pattern research, phases of the targeted system and software lifecycle, and intended users.
- Research implementation: This includes the platform to realize the results of security pattern research, whether the results are automated and encapsulated as a tool, and whether case studies or experiments are conducted to evaluate the results relevant to the original research purpose.
- Quality: This includes categories related to quality characteristics such as vulnerability 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.
- Pattern: This includes the types of patterns addressed in the security pattern research such as security patterns, attack patterns, and misuse patterns.

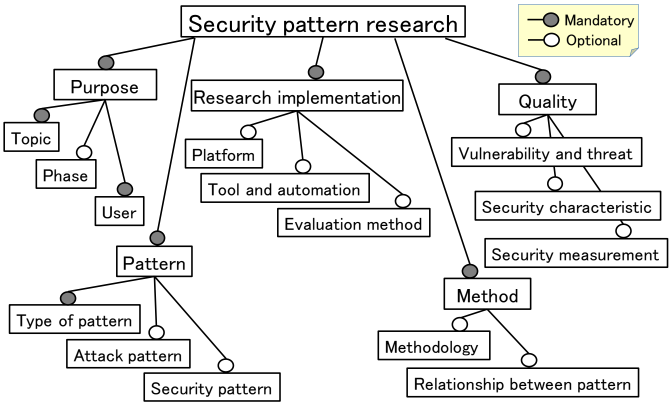


Fig. 2. Feature diagram of the taxonomy

- Method: This include methodology and modeling methods, which may or may not handle pattern relationships.

A taxonomy can be validated by demonstrating the orthogonality of its classification features, benchmarking against existing classification schemes, or demonstrating its utility to classify existing knowledge [14]. In our case, 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.

The taxonomy is expected to guide practitioners and researchers in the following possible usecases UC1 and UC2:

UC1: To choose existing security pattern methods and tools: When engineers want to reuse and eventually extend existing security pattern methods and tools, they must compare and then select the appropriate one according to how the methods and tools meet their objectives. The taxonomy can help by comparing criteria and the methods and tools according to the characteristics defined in the taxonomy.

UC2: To communicate and research security pattern methods and tools: The taxonomy can serve as a reference for the security pattern engineering community, including practitioners and researchers. It can be extended by peers, providing the community with an important body of knowledge to guide future communications and research on security pattern methods and the corresponding tools since it incorporates the characteristics of security pattern research into a single structure. For example, the taxonomy can serve as the basis to build an open repository of information of existing security pattern research methods (and corresponding tools) by accumulating classification results. Moreover, the taxonomy should support the security community by improving the quality of security pattern research and the effectiveness of security patterns that are addressed by research.

IV. Survey results

We successfully classified 211 research papers from the SLR according to the facets defined in the taxonomy. Below, how the taxonomy helps classify security pattern research papers is summarized. Because the classification yields one category for each characteristic fitting, the orthogonality of the classification features is confirmed.

[3] The 211 papers and details of the analysis results are available at http://www.washi.cs.waseda.ac.jp/security/ .

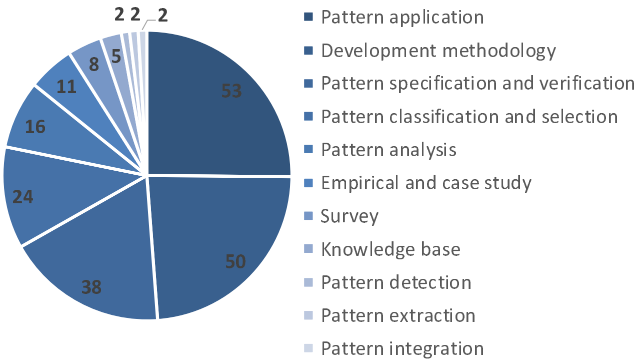


Fig. 3. Breakdown of Topics

A. Purpose

1) Topic: Figure 3 shows the breakdown of the research topics. The majority consists of security pattern applications during development, abstract development methodologies, and proposals for processes. On the other hand, the number of papers on case studies and demonstrations is limited.

These findings indicate that additional case studies and experiments on applications and methodologies are needed. Since the late 1990's, new proposals for security patterns have been actively presented at conferences such as PLoP (Pattern Language of Programs). However, patterns are identified manually. Systematic methods have yet to be established. In terms of evaluating security and vulnerability, it is desirable to automatically identify the necessity of the attack and security patterns prior to determining the requirements and designing in coding. Although a mechanism to identify and extract security patterns is anticipated, the problem is that such studies barely exist in reality.

2) Phase of lifecycle: Figure 4 shows the results after categorizing the patterns into 16 phases. In this analysis, each paper is categorized in zero or more phases. In addition, the categories have a hierarchy. For example, "any" can produce phases with a higher granularity compared to the "design" phase. Hence, the analysis results include some ambiguities. Whether "evolution" is included in "any" has to be determined individually. Various phases from "analysis" to "evolution" can be research targets. Each paper is classified into the highest granularity as possible.

The number of targeted phases for the patterns is highest in "design" followed by "analysis" and "implementation". Hence, targets are skewed towards the earlier phases. Few papers target phases after implementation such as "maintenance" and "evolution", suggesting that security pattern research in later phases may be a frontier field. Cutting-edge topics include pattern classification, pattern extraction from the source code, improvement of legacy systems using security patterns, and security patterns for operation dynamics. The following topics require further investigations: pattern classification for the system lifecycle, defining patterns that respond to dynamic behaviors, and utilization of defined patterns in existing systems.

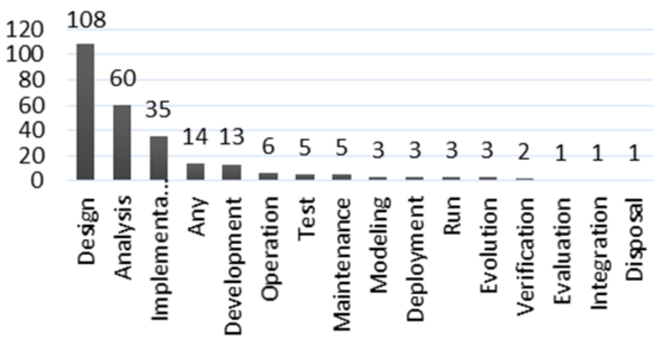


Fig. 4. Phases Targeted by Security Patterns

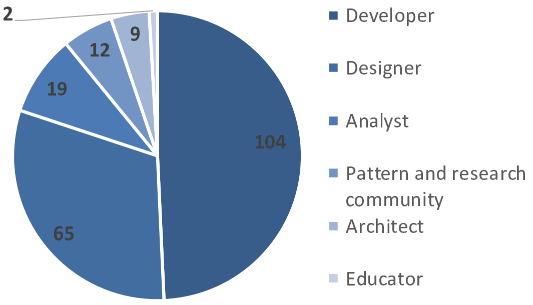


Fig. 5. Users of the Research Results

3) User of research results: Figure 5 shows the target users. "Designers", "analysts", and "architects" refer to users who are clearly described in the literature as designer of the system or software, analysts for processes, security requirements, and policy review, and architects for the system or software architecture and evaluation, respectively. On the other hand, "developers refers to users that are not clearly described, but the results may be used by developers in general. "Pattern and research community" refers to the results used by research communities or pattern researchers. About half of the target users are developers and another 30% are designers. However, analysts and community are not typically the target users.

Because most security patterns addressed in research deal with design, we hypothesize that a large number of target users are designers. Research results targeting developers in general should clarify the usage and target users, except for studies involving methodology and lifecycle. One threat to validity is that we analyzed the target users by sharing tasks with multiple individuals. Therefore, the categorization may depend on the individual when the target user is not clearly indicated.

B. Research implementation

1) Computing platform: Among the 211 papers, 49 (23%) are based on certain platforms (Fig. 6). The majority uses web, cloud, and distributed systems, but BPM (business process management) and MAS (multi-agent systems) are also mentioned. About 77% do not mention a specific platform. Considering the development of systems involving IoT, the cloud, and their applications, the research results should use IoT or embedded and controlled platforms.

2) Tool and automation: Of the 211 papers, 73 (35%) mention tools or automation (Fig. 7). Many use tools and

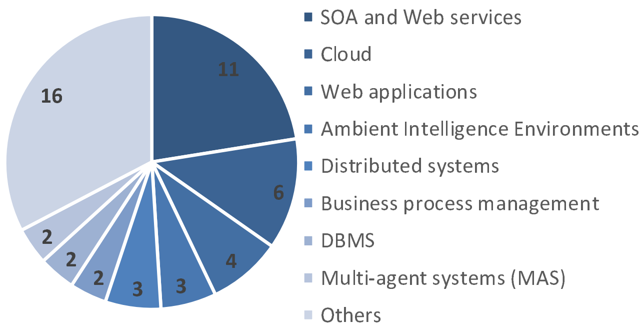


Fig. 6. Breakdown of Computing Platforms

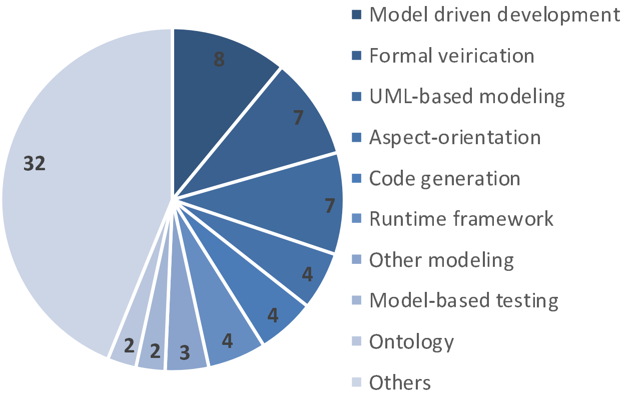


Fig. 7. Breakdown of Tools and Automation

approaches that involve modeling. However, formal methods, verification, aspect-oriented approaches, and code generation are also mentioned. Because the majority of studies create their own tools, many tools exist for modeling, analysis, and design.

Security should be handled in all phases. Thus, it is desirable to directly incorporate tools for security patterns in the implementation, testing, and operation phases. In other words, the entire security lifecycle should be covered.

3) Evaluation method: Of the 211 papers, 100 (47%) conduct some form of evaluation. The most common method is a case study (39, 18%) followed by referencing examples (33, 16%), and experiments (7, 3%). Ten papers (5%) claim to use an evaluation but the method is not specified. On the other hand, one paper reports using 11 different evaluation methods (argumentation, classification, critique, discussion, examination, measurement, modularity, scenario, risk assessment, validation, and observation study).

Evaluations related to security pattern usages are immature. Only about half of the papers implemented an evaluation. Even if an evaluation is conducted, it is limited to case studies and references to examples. Employing a stricter evaluation method such as a control experiment is extremely rare. Hence, more rigorous evaluation methods are expected in the future.

C. Quality

1) Vulnerability and threat: Of 211 papers, 61 (29%) mention vulnerability or threats. As for the analysis process of the vulnerability and threats, some (16, 8%) refer to STRIDE [15], which is advocated by Microsoft. A total of 12 papers (6%) reference publicly available information regarding vulnerability and threats. Of these, three reference CVSS [9], which summarizes risk information, and seven reference more tangible vulnerability information such as CWE [10] and CVE [16]. Furthermore, three reference CAPEC [17], which categorizes actual attacks.

Security measures involve addressing a system vulnerabilities and threats. Research patterns should clearly address how to deal with vulnerabilities and threats. Hence, the fact that only 29% of the papers mention vulnerabilities or threats is disconcerting. Additionally, research needs to collect theoretical and actual relationships on vulnerabilities to realize practical uses of security patterns. Currently, only 6% of papers mention the relation to publicly available information. In the future, more studies should focus on how to utilize such information along with increasing awareness of security patterns.

2) Security characteristic: To determine the trends in security pattern research, we focus on the security characteristics mentioned in the literature. Over half (121, 57%) mention at least one security characteristics. Of these 121 papers, 112 (93%) reference CIA characteristics, which stand for confidentiality, integrity, and availability as defined by ”information security is to maintain CIA” in ISO/IEC 27002. Of those referring to CIA characteristics, 94 (84%), 72 (64%), and 63 (56%) reference confidentiality, integrity, and availability, respectively (Fig. 8).

Another 31 (26%) of papers reference security characteristics other than CIA. Specifically, they mention access control, accountability, authenticity, authentication, authorization, and nonrepudiation. Of these, 22 (18%) mention both CIA and non-CIA characteristics, while 9 (7%) only mention non-CIA characteristics.

The findings show that many studies examine security characteristics based on the CIA characteristic security patterns. Confidentiality, which allows only individuals with permission access to information, is especially important in patterns involving privacy and confidentiality such as RBAC (Role-Based Access Control).

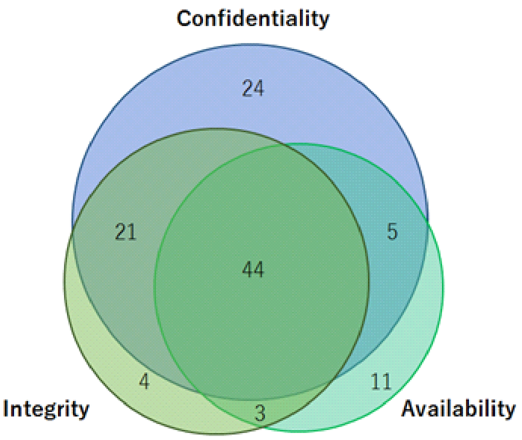


Fig. 8. Breakdown of the Security Characteristics

TABLE I
TYPES OF SECURITY PATTERNS

Security Pattern Type	Number of Papers
Security pattern	179
Design pattern	13
Dependability pattern	9
Misuse pattern	6
Attack pattern	6
Architecture pattern	6
Requirement pattern	3
Usability pattern	1
Privacy pattern	1

3) Security measurement: Of the 211 papers, 17 (8%) evaluate patterns. Of these, two use STRIDE [15]. [18] evaluates the handling of potential threats using a graph and indicates the categories of attacks against non-secure and secure systems accordingly. [19] uses STRIDE to evaluate the system against security attacks. In an evaluation using fuzzy logic, five levels for the main five events, which correspond to the category in STRIDE, are defined. The number of levels/categories and how each level/category is defined may differ slightly between these two evaluation models. However, 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 the security patterns.

Individual evaluation categories in a research paper make it difficult to judge the reasonableness of the evaluation results. In the future, research should evaluate qualities against a standard index such as STRIDE. Below is a summary of other measurements in the literature.

D. Security related patterns

1) Types of patterns: There are two common types of patterns: security patterns and misuse or attack patterns. While 179 papers (85%) deal with security patterns only 11 papers (5%) focus misuse or attack patterns, which is negligible in comparison. Research on attack patterns tends to focus on solving actual problems. Currently, we have collected papers dealing with security patterns. However, other patterns that address non-functional requirements such as dependability and usability are also observed (Table I). For security patterns targeting the development phase, 3 papers reference “requirements” and 13 (6%) reference “design”.

Relative to studies on security patterns, few examine attack patterns. This may be a consequence of our search method. However, the smaller proportion of studies on attack and misuse patterns suggests that more active investigations are necessary. Similarly, only a few works focus on a phase on other than the design or development phase. In the future, pattern research on requirement analysis and testing should be more active.

2) Attack pattern: Of the 211 papers, 33 (16%) mention some form of attack pattern. Table II summarizes patterns that appear in multiple papers. Compared to security patterns, this is extremely low. Abstraction of patterns also varies. Some are about abstract patterns in STRIDE, which is a categorization of attack patterns, while other write about CIA security characteristics. One paper investigates illegal money transfers specific to a certain application. As for the number of appearances, many attack patterns appear in one paper only. Attack patterns appearing in multiple studies include spoofing (six times) followed by DoS (five times), tampering (four times), information disclosure (four times), injection (three times) and misuse (three times). Additionally, the following appear in two papers: repudiation, integrity, message secrecy violation, session state poisoning, attack, malicious virtual machine migration, and threat. These observations reveal that categories related to the characteristics of attack patterns and security characteristics frequently appear, but few reports employ specific examples.

TABLE II
NUMBER OF APPEARANCES OF ATTACK PATTERNS IN THE LITERATURE

Attack Pattern Name	#Appearances
Spoofing	6
DoS	5
Information disclosure	4
Tampering	4
Misuse	3
Injection	3
Attack	2
Session state poisoning	2
Message secrecy violation	2
Malicious Virtual Machine Migration	2
Threat	2
Repudiation	2
Integrity	2
Elevation of privilege	2

3) Security pattern: Among 211 papers, 166 (79%) mention a specific security pattern by name. Pattern names are mentioned 1063 times, which is an average of 6.4 patterns per paper. However, there are only 466 unique pattern types. Of these, 172 patterns (37%) are mentioned in at least two papers. Table III lists the 14 pattern names mentioned in ten or more papers. Many are related to access control, authorization, and authentication.

Surprisingly, over 20% of the papers do not mention specific pattern names. This is an issue because it is difficult to explain proposed ideas and methods without mentioning a specific pattern. Although specific names may not be mentioned, it is possible that the papers outline a specific pattern. Our results reveal about one-third of the patterns are common and can be easily described using a directed graph structure represented by a class diagram. Therefore, patterns may be used in many research papers. In the future, we expect that more research will use patterns to express features that are difficult to express by a structural description such as availability.

E. Method

1) Methodology: Among the 211 papers, 87 (41%) describe a development methodology. Many (21, 10%) mention a methodology related to a model-driven approach or an aspect-oriented approach (10, 5%). Figure 9 shows the breakdown of the main methodologies. Although various development methodologies are observed, few focus on security. As we enter into the IoT generation, more studies on the methodology that consciously focus on security by design are needed.

TABLE III
SECURITY PATTERN NAMES MENTIONED IN AT LEAST 10 OR MORE PAPERS

Security Pattern Name	Number of Appearances
RBAC	45
Authorization	31
Access control	23
Authentication	20
Authenticator	18
Check point	18
Reference monitor	16
Secure logger	14
Secure pipe	13
Single access point	13
Authentication enforcer	11
Replicated system	10
ABAC	10
XACML	10

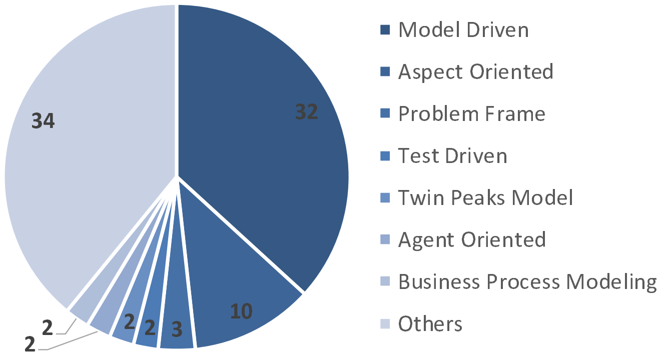


Fig. 9. Number of Papers Referencing the Intended Development Methodology

2) Relationship between patterns: There are two types of security patterns: those that describe methods to reduce security risks and those that describe methods to reduce misuse or attack patterns by detailing security risks from the attackers viewpoint. Therefore, there are two types of relationships between patterns: between security patterns (relationship A) and between a misuse or attack pattern and a security pattern to reduce risks (relationship B). Relationships between security patterns (relationship A) are dealt in 85 (40%) papers and 12 (6%) papers mention relationship B.

Many security patterns are applied in combination. Thus, the relationships between patterns need to be clarified. Of these papers, 40% consider some kind of relationship between patterns because security patterns are often applied in combination. However, the relationship between misuse or attack patterns, which are required in security risk analysis and security measure patterns are mentioned in only 6% of all research papers. 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.

V. CONCLUSION AND FUTURE WORK

Since the taxonomy was successfully used to classify and analyze the contents of over 200 security pattern research papers through a SLR, it should be useful to classify, compare, reuse, and extend security pattern research. In addition, the taxonomy is also expected to support communications among stakeholders.

In the future, we plan to examine the details of each facet as well as the relationships among the facets. These results will be used to elucidate the future outlook of security pattern research.

REFERENCES

[1] N. Yoshioka, H. Washizaki, and K. Maruyama, "A survey on security patterns," *Progress in Informatics*, pp. 35–48, 3 2008.

[2] E. Fernandez, N. Yoshioka, and H. Washizaki, "Patterns for security and privacy in cloud ecosystems," in *Proceedings of the 2nd International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE 2015)*, 2015.

[3] A. Nhlabatsi, A. Bandara, S. Hayashi, C. Haley, J. Jurjens, H. Kaiya, A. Kubo, R. Laney, H. Mouratidis, B. Nuseibeh, T. Tun, H. Washizaki, N. Yoshioka, and Y. Yu, "Security patterns: Comparing modeling approaches," in *Software Engineering for Secure Systems: Industrial and Research Perspectives*, 2010.

[4] E. Fernandez, N. Yoshioka, H. Washizaki, J. Jurjens, M. VanHilst, and G. Pernul, "Using security patterns to develop secure systems," in *Software Engineering for Secure Systems: Industrial and Research Perspectives*, 2010.

[5] E. Fernandez, H. Washizaki, and N. Yoshioka, "Abstract security patterns," in *Proceedings of the 15th Conference on Pattern Languages of Programs (PLoP'08)*, 2008.

[6] M. Babar and H. Zhang, "Systematic literature reviews in software engineering: Preliminary results from interviews with researchers," in *Proceedings of the Third International Symposium on Empirical Software Engineering and Measurement, ESEM 2009, October 15-16, 2009, Lake Buena Vista, Florida, USA*, pp. 346–355, 2009.

[7] Y. Ito, H. Washizaki, M. Yoshizawa, Y. Fukazawa, T. Okubo, H. Kaiya, A. Hazeyama, N. Yoshioka, and E. Fernandez, "Systematic mapping of security patterns research," in *Proceedings of the 22nd Conference on Pattern Languages of Programs Conference 2015 (PLoP 2015)*, 2015.

[8] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic Literature Reviews in Software Engineering - A Systematic Literature Review," *Information and Software Technology*, vol. 51, no. 1, pp. 7–15, 2009.

[9] FIRST.Org, "Common Vulnerability Scoring System v3.0: Specification Document," https://www.first.org/cvss/, 2015.

[10] The MITRE Corporation, "Common Weakness Enumeration Version 3.1," https://cwe.mitre.org/, 2018.

[11] T. Xia, H. Washizaki, T. Kato, H. Kaiya, S. Ogata, E. Fernandez, H. Kanuka, M. Yoshino, D. Yamamoto, T. Okubo, N. Yoshioka, and A. Hazeyama, "Cloud security and privacy metamodel: Metamodel for security and privacy knowledge in cloud services," in *MODELSWARD 2018 - Proceedings of the 6th International Conference on Model-Driven Engineering and Software Development*, SciTePress, 2018.

[12] K. C. Kang, S. G. Cohen, J. A. Hess, W. E. Novak, and A. S. Peterson, "Feature-Oriented Domain Analysis (FODA) Feasibility Study," *Technical Report CMU/SEI-90-TR-21*, pp. 1–148, 1990.

[13] K. Czarnecki and S. Helsen, "Classification of Model Transformation Approaches," in *Proceedings of the OOPSLA Workshop on Generative Techniques in the Context of Model-Driven Architecture*, pp. 1–17, 2003.

[14] D. Smite, C. Wohlin, Z. Galvina, and R. Prikladnicki, "An Empirically Based Terminology and Taxonomy for Global Software Engineering," *Empirical Software Engineering*, vol. 19, no. 1, pp. 105–153, 2014.

[15] A. Shostack, ed., *Threat Modeling: Designing for Security*. Wiley, 1 ed., 2014.

[16] The MITRE Corporation, "Common Vulnerability and Exposures," https://cve.mitre.org/, 2018.

[17] The MITRE Corporation, "Common Attack Pattern Enumeration and Classification," https://capec.mitre.org/, 2018.

[18] S. Halkidis, N. Tsantalis, A. Chatzigeorgiou, and G. Stephanides, "Architectural risk analysis of software systems based on security patterns," in *IEEE Transactions on Dependable and Secure Computing*, 2008.

[19] S. Halkidis, A. Chatzigeorgiou, and G. Stephanides, "Quantitative evaluation of systems with security patterns using a fuzzy approach," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2006.