ELEKTROTEHNIŠKI VESTNIK 89(3): 73-80, 2022
ORIGINAL SCIENTIFIC PAPER

Characterization of Selected Security-related Standards in the Field of Security Requirements Engineering

Damjan Fujs [1,*], Igor Bernik [2]

[1] *University of Ljubljana, Faculty of Computer and Information Science, Večna pot 113, 1000 Ljubljana, Slovenia*
[2] *University of Maribor, Faculty of Criminal Justice and Security, Kotnikova ulica 8, 1000 Ljubljana, Slovenia*
[*] *E-mail: damjan.fujs@fri.uni-lj.si*

Abstract. Security requirements are an important part of modern information systems. In the past, they have been implemented in final stages of the information systems development. Though, there are many approaches and publications in the field of security requirements engineering, there is a gap in how to find the most relevant sources. To this end, we present a novel approach to discover knowledge from academic databases. It enables a qualitative and quantitative analysis of scientific publications in the field of security requirements engineering. A special attention is paid to standards in the field of information security and other knowledge bases that create an added value in understanding the security requirements engineering. The VOSviewer software for keyword analysis in scientific publications in the academic database Web of Science Core Collection (a total of 319 scientific publications analyzed) is used. As part of this, two visualizations of clustering (a solution with five and two clusters) are highlighted. The results show that the most popular standards and methodologies in the field of information security are family of the ISO/IEC standards 27000, NIST 800-53 and Tropos. The presented approach is applicable also to other areas.

Keywords: non-functional requirements, knowledge discovery, information security, Web of Science, VOSviewer

Karakterizacija izbranih, z varnostjo povezanih standardov na področju inženirstva varnostnih zahtev

Varnostne zahteve so pomemben element sodobnih informacijskih sistemov, ki je bil v preteklosti izveden v končnih fazah razvoja informacijskih sistemov. Dandanes obstajajo številni pristopi in publikacije na področju inženirstva varnostnih zahtev, vendar kljub temu obstaja vrzel, kako ob tem velikem korpusu poiskati čim bolj relevantne vire. V ta namen je predstavljen nov pristop odkrivanja znanja iz akademskih baz podatkov. Pristop omogoča kvalitativno in kvantitativno analizo znanstvenih publikacij na področju inženirstva varnostnih zahtev. Posebna pozornost je namenjena standardom na področju informacijske varnosti in preostalim bazam znanja, ki ustvarjajo dodano vrednost pri razumevanju inženirstva informacijskovarnostnih zahtev. Uporabljena je bila programska oprema VOSviewer za analizo ključnih besed v znanstvenih publikacijah v akademski bazi podatkov Web of Science Core Collection (skupno analiziranih 319 znanstvenih publikacij). V sklopu tega sta izpostavljeni dve vizualizaciji gručenja (rešitev s petimi in rešitev z dvema gručama). Rezultati kažejo, da so najbolj priljubljeni standardi in metodologije na področju informacijske varnosti sledeči: družina ISO/IEC standardov 27000, NIST 800-53 in Tropos. Predstavljeni pristop je uporaben tudi na drugih področjih.

Ključne besede: nefunkcijske zahteve, odkrivanje znanja, informacijska varnost, Web of Science, VOSviewer

1 INTRODUCTION

The Cyber security or the information security maintains a global significance as threats to information systems are increasingly numerous and sophisticated [1]. This is also evident by the information security strategy implementation in various countries [2], the growing number of professional associations, publications in scientific journals [3], etc. In the paper, there will be no clear distinction made between the information security and the cyber security [2]. The main difference between them is that the information security ensures security with the help of the information and communication technology, but this is not necessary (e.g., protected information of the archival material). As shown in Figure 1, the term cybersecurity is becoming increasingly popular in the everyday use all over the world and in many cases replaces the term information security.

This pervasive popularity of the cyber security poses a challenge to methodologies for finding the most relevant sources. The focus of the paper is on the security requirements engineering of the cyber security. When speaking in terms of security requirements engineering, the question raised is *what should the system contain to assure security*?

Received 21 July 2021
Accepted 12 January 2022

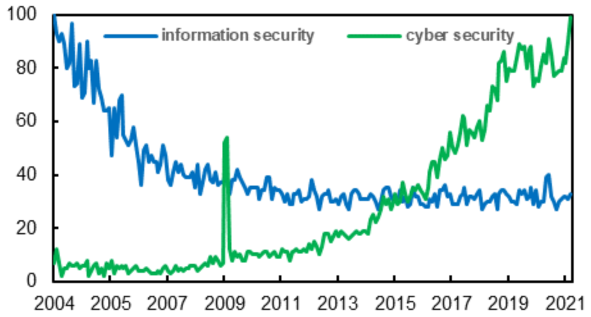

Figure 1. Popularity comparison of the two terms in 2004 – 2021 shows a growing trend in the use rate of the term cyber security. The value of 100 means the highest popularity of the term. Data source: Google Trends.

An important part of security requirements engineering are standards and security checklists that cover the requirements for a secure information system/software. Here there are several challenges. First, there are various non-universal standards needing to be adapted. Second, there are standards promoted as the "state-of-the-art" which in fact they are not. Third, though the literature offers several methodologies and approaches (body of knowledge) to the field of security requirements engineering (including standards), to the best of our knowledge, there has been no overview made of the studied areas and subfields od the scientific landscapes.

In the academic sphere, research papers (publications) are places where new knowledge and findings are written [4]. The goal of any publication is to get as many people to read and cite it as possible. However, this is not easy to achieve as different research areas are differently attractive.

To make the above possible, our paper proposes:

1) an adapted model for knowledge discovery from the literature in the field of security requirements engineering and
2) a quantitative and qualitative analysis of studies addressing information security standards in the field of security requirements engineering.

The rest of the paper is organized as follows. Chapter 2 presents the main idea of the proposed knowledge discovery model in the field of security requirements engineering. Chapter 2 describes the background of similar works is performed. Chapter 3 provides methodology of data collection and data processing. Chapter 4 presents results of our study. Chapter 5 draws conclusions and discusses theoretical and practical implications. Chapter 6 points at the work to be done in future.

1.1 Knowledge discovery model in the field of security requirements engineering

Adoption of the Fayyad et al. [5] model is used to serve as a research framework for knowledge discovery (KDD) in the field of security requirements engineering. KDD is a term used for the general knowledge discovery in data. The aim of the paper is to obtain a useful value of the data (knowledge) based on a quantitative and qualitative literature analysis. The KDD process proposed by Fayyad et al. [5] is not completely applicable for the studied case, because it also integrates "patterns" step, and as such it does not cover our entire research problem, which is of a qualitative nature.

Our focus is on the information security standards in the field of security requirements engineering. It should be noted that the terms standard and approach are sometimes used interchangeably. Security requirements belong to the field of non-functional requirements, which means that they have an imprecise quantitative and qualitative objective [6]. Speaking in terms of requirements, we are interested in the system content, i.e. its functionalities.

Therefore, based on the literature, no direct answer can be given. The analysis needs a further qualitative interpretation. We therefore suggest to use a tool to process the bibliometric data when reviewing the literature (in our case we use the VOSviewer software). In such data, we may discover useful clusters and potentially predict trends. As it is not possible to use the "*patterns*" phase directly, we replace it with the "*final set of literature*". This means that based on the results of the VOSviewer analysis, we decide which areas will be analyzed in more detail. Based on these results, the knowledge and potential theoretical and practical solutions will be made.

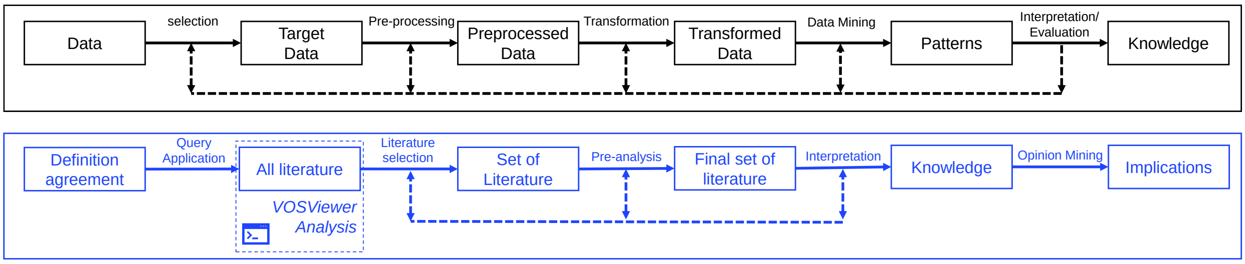

Figure 2. Model comparison of the key elements of our model for knowledge discovery in the field of security requirements engineering and the original KDD model by Fayyad et al. [5] is shown in black color. Our model is in blue. The dashed lines show potential iterative steps.

2 Related Work

In this chapter, the prior work in the field of the security requirements engineering and literature review methodologies are discussed. Chapter 2.1 describes approaches to analyzing the literature. Chapter 2.2 summarizes the state-of-the-art approaches with a particular emphasis on various knowledge bodies.

2.1 Approaches to literature analyzing

In practice, there are the following three approaches. The most common is the informal literature survey, which is mostly used in the “Related Work” sections. It is about researchers presenting relevant related works that contribute to the understanding of a topic. However, they do not define research questions and the data acquisition process [7].

The systematic literature review approach is used for a structured search and analysis of the literature with a predefined inclusion and exclusion criterion and other metrics [7]. One of the most prominent approaches is the PRISMA statement for reporting systematic reviews proposed by Liberati et al. [8] primarily for the health-related topics. PRISMA is also used in the field of security requirements engineering or in a wider topic of cyber security. Nevertheless, PRISMA is not always directly mentioned or applied but rather used by systematic literature reviews (SLR) (see for example [9]).

Other approaches are mainly of a quantitative nature, i.e. either scientometrics [3] or bibliometrics [10]. They analyze the quantitative indicators of scientific publications (e.g., the number of citations, links between citations, clustering, etc.). Each method has its advantages and disadvantages, depending on the research area. SLR are time consuming [9], but they can result in standalone publications with a clear theoretical or practical contribution.

In the paper, a hybrid approach of the three major ways of reviewing the literature is used. It provides a comprehensive insight into security requirements engineering.

2.2 Security requirements engineering body of knowledge

For the software security, there are various bodies of knowledge available that provide security-related standards. Information security bodies of knowledge refers to the information security requirements (check-lists, standards, etc.) and therefore also policies, models/approaches and other mechanisms [11]. This is because the field of security requirements engineering is complex, making it difficult to find a standard to entirely cover the security needs. There are several standards that cover the information security from various aspects, such as the needs of an organization (e.g., ISO 27001 [12], NIST SP 800-70 [13] and Common Criteria [14]), information systems (COBIT [15]) - the needs of a web application (Application Security Verification Standard - ASVS [16]). These standards include generic security requirements and can be used by software developers, cyber security professionals and researchers to explain, shape, assess and improve cyber security solutions. As most of the standards are generic, they may need to be adapted [17] to specific needs of a particular case, thus potentially improving the security yield as highlighted in ASVS [16].

Besides the above, there are various approaches to security requirements engineering used in modeling requirements engineering processes from different perspectives. Some of them are: Security Quality Requirements Engineering (SQUARE) [18], Security Requirement Engineering Process (SREP) [19], Security Requirements Engineering Framework (SREF) [20], etc.

They provide secondary data sources. However, security requirements engineering can also be formed on the basis of the primary data. In practice this means that we first perform a penetration test, and based on it we formulate security requirements. In any case, to make planning easier, it is important to have an overview of the existing solutions.

3 Characterization of Security Requirements Engineering

Our approach to analyzing the security requirements engineering is given below. In order to get visual understanding of the topic, a novel hybrid KDD model (the blue model in Figure 2) is used.

To get the widest possible picture of security requirements engineering, the following query to search for scientific publications in the Web of Science Core Collection academic database is used:

(“security requirements engineering”) OR (“security” AND “requirements engineering”).

The used query returns 319 results. They are fully used in further the analyses in the VOSviewer software. Note that no other specifications are added at this stage and that the following publications are used (regarding citation indexes): SCI-EXPANDED (1900-present), SSCI (1900-present), A&HCI (1975-present), CPCI-S (2011-present), CPCI-SSH (2011-present), BKCI-S (2011-present), BKCI-SSH (2011-present), ESCI (2015-present), CCR-EXPANDED (1985-present) and IC (1993-present). Our study was conducted in 2021 (June 20th).

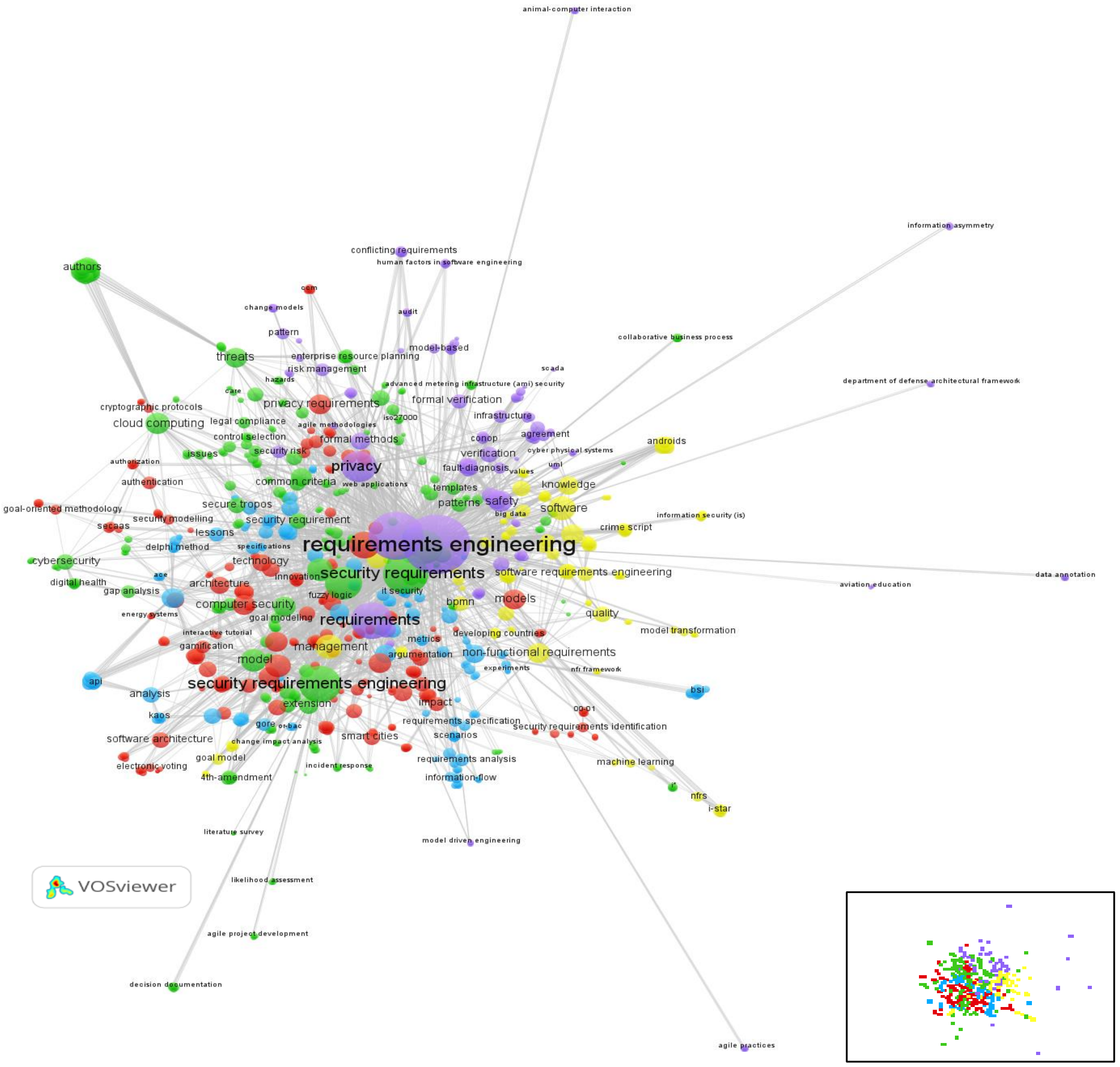

Figure 3. Visualization of the keyword map with five clusters. Each cluster is shown in a different color (blue, green, purple, yellow and red). A corpus of the keywords appearing in 319 publications is used in a novel hybrid KDD model (the blue model in Figure 2).

The VOSviewer software (developed by van Eck and Waltman [21]) is used to get an insight into the structure of publications in the field of security requirements engineering. VOSviewer is a freely available software enabling a bibliographic analysis of scientific publications. In addition, VOSviewer version 1.6.16 is used. Two visualizations of the bibliographic data are created. Clustering is performed based on the input of all 319 publications. To get an insight into the most popular keywords and their incidences, clustering on 319 publications is then made by filtering the input and displaying the links between the at least five-times appearing keywords.

4 Results

The essential part of our approach is the analysis made with the VOSviewer software. All clusters have in common the following keywords from the query: requirements engineering and security. All publications within this query are included in our analysis. The oldest publication dates from 2004 and the most recent from 2020.

Figure 3 shows a visualization of the bibliographic data based on the keywords. Each of the clusters is presented in a different color and the size of the clusters is as follows: red cluster (254 keywords), green cluster (217 keywords), blue cluster (146 keywords), yellow cluster (129 keywords) and purple cluster (120 keywords).

The red cluster in Figure 3 focuses on the business process-related topics, different types of security (e.g., cloud, risks, threats, etc.) and different privacy topics (e.g., governance, GDPR, policies, etc.). The red cluster is also the one that implements various information security standards such as ISO/IEC 2700, ISO/IEC 27001, ISO/IEC 17799 and ISO/IEC 15408. ISO/IEC 27000 is a family of information security standards [22]. It also describes the compatibility standards within the family of the ISO / IEC 27000 standards. Probably the best-known standard in the field of information security is ISO/IEC 27001, which is considered to be establishing an information security management system. ISO/IEC 27001 implements a cyclical process structure for ensuring the information security, i.e., the PDCA, Plan-Do-Check-Act model [23]. The following two standards that appear in our keyword corpus and that are devoted to security requirements are: ISO/IEC 17799 and ISO/IEC 15408. ISO/IEC 17799 describes the best information security management practices to those who manage the information security [24]. Similarly, ISO/IEC 15408 delivers security functionalities and security evaluations for IT products [25]. The Tropos methodology can be identified in this cluster as well. Namely, the Secure Tropos methodology is a model-based approach for security requirements engineering. Secure Tropos has four phases; early requirements elicitation, late requirements elicitation, architectural design and detailed design. All these steps serve to identify actors, goals processes and activities of the system [26].

The green cluster in Figure 3 focuses on technical elements of the security requirements engineering (e.g., smart things and software development in architecture). It also contains two standards as well as security requirements engineering methodologies and other relevant keywords related to requirements - either directly or indirectly. Hence, the following two standards can be found: ISO/IEC 27002 and NIST 800-53 [27]. The ISO/IEC 27002 is similar to ISO/IEC 27001, however, it describes individual safety components in more detail. NIST 800-53 is similar to the ISO/IEC information security standard, except that it originates from the United States of America. NIST 800-53 defines minimal mandatory controls to protect federal information systems (and federal information in general) [28]. Besides these standards, certification is also dealt with (for example x.509 certificate for authentication and authorization [29]). Other identified keywords that come with security requirements engineering are: Security Threat-Oriented Requirements Engineering methodology (STORE) [29], p-STORE methodology (extension of STORE and addressing the privacy) [29] and Socio-Technical Security Modeling Language (STS) [30].

The blue cluster in Figure 3 mostly includes the keywords related to security methods such as metrics and evaluations. For the information security standards, only the common criteria standard (CC) can be identified. CC is the second term for ISO/IEC 15408 [31] described in the green cluster. However, there is also a security requirements methodology, i.e. UMLSec, which is a security UML extension [32].

The yellow cluster in Figure 3 contains no direct specific information security standard in keywords. Nevertheless, some security requirement engineering-related concepts, such as certification and accreditation can be identified, i.e. the *i** framework and WebREd-Tool. The *i** framework is a methodology for security requirements elicitation [33]. WebREd-Tool is a software that helps requirements elicitation in the design of web applications. In general, the cluster includes keywords from the field of business processes, decision making, general information security and management.

The purple cluster in Figure 3 refers mainly to areas of agility, privacy and regulation compliance. In this cluster, two standards can be identified: IEC 61131 and IEC 61499. They provide a solid software architecture in the field industrial automation systems [34]. Similarly to Figure 3, Figure 4 shows the links between the keywords, yet, here there are only keywords included that appear at least five times in the used academic database. The red cluster is the largest one. It contains 32 keywords. The green cluster contains only 14 keywords.

The red cluster can be said to implement socio-technical keywords (e.g., management, safety, risks, trust, framework, etc.). The green cluster focuses on more technical elements of security requirements engineering, such as cloud computing, software, ontology, software engineering, etc. Neither of them does not contain a particular standard. The red cluster highlights the Tropos methodology, that appears in 27 publications. The keyword "security" is most present in the green cluster, next is the keyword "privacy".

5 CONCLUSIONS

Based on the results of our study, we suggest authors to use full keywords rather than abbreviations when indexing their papers in academic databases in order to avoid dichotomy. Moreover, they should also consider how to write the keywords. For example, for the ISO 27001 standard, there are three versions of the record: ISO 27001, ISO / IEC 27001, and ISO27001. Therefore, it is important to use standard terms to find the most relevant papers and consequently to enter keywords in academic databases. Also, there may be different names for two identical standards; for example, the CC standard is also known as the ISO/IEC 15408 [31].

Choosing keywords is also a matter of creativity. Care should also be taken when choosing an academic database to search for the most relevant publications. Not every scientific field and subfield is equally represented in all academic bases. The choice of a particular academic database is affected by the availability of publications and their quality, coverage and previous user experience [35].

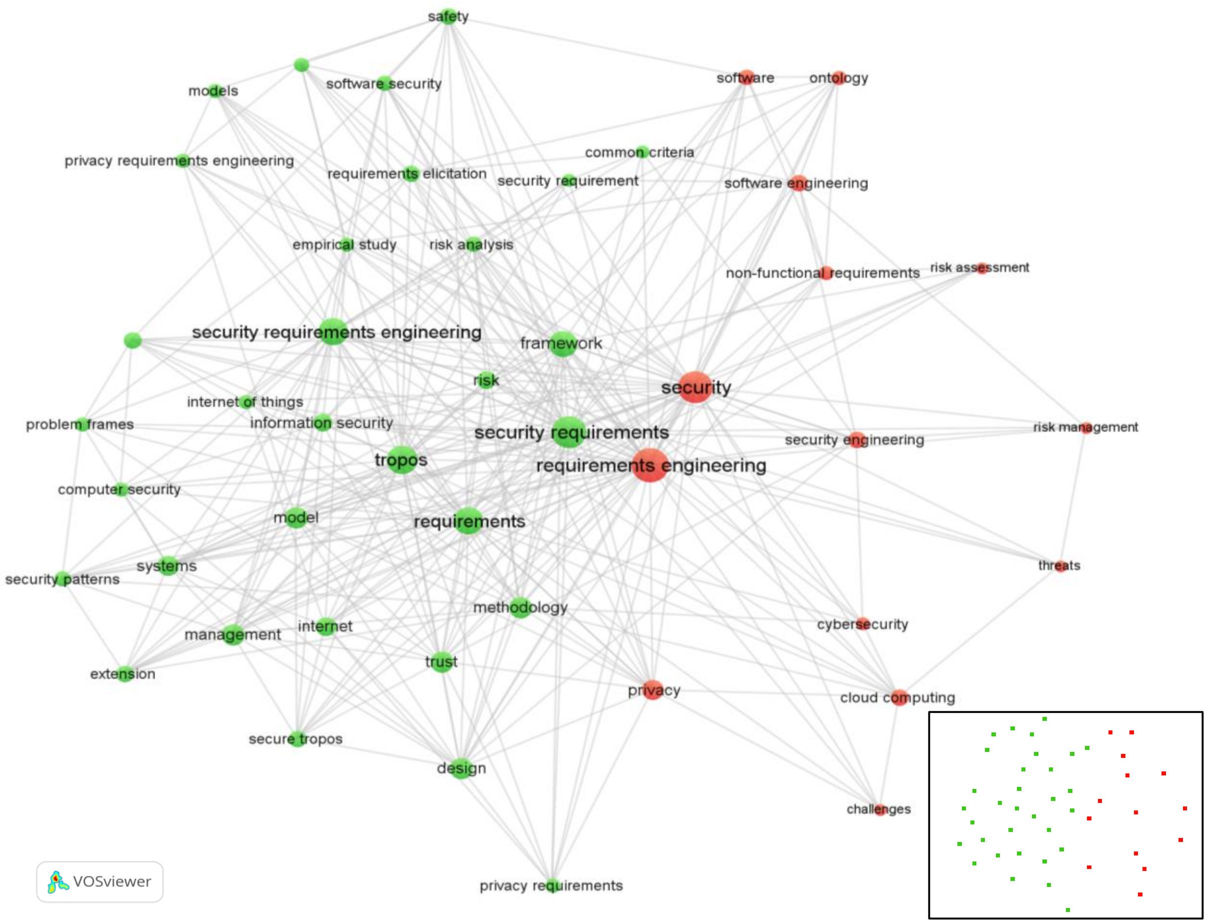

Figure 4. Visualization of the keyword map with two clusters (green and red marked). Only the keywords that appear at least five times in 319 publications are shown.

For companies and organizations, investment can be an additional challenge when applying standards. Some standards are not freely available, which means they need to be purchased, however there are also standards that are freely available (open source), such as ASVS [16]. There are also cases that some companies or organizations comply with some of the standards but have never ordered a conformity assessment or obtained a certificate.

Our approach presented in Figure 2 is applicable in other areas as well. The novelty is that we first identify the desired keywords (definition agreement) and then search for scientific publications. We then analyze all results together with other academic databases (optionally), not just in the Web of Science Core Collection. We then analyze the links between the keywords and identify the most important scientific publications. We analyze them in more detail to answer research questions. In the last phase, we provide practical and theoretical implications.

6 Limitations and Future Work

There is some further work to be done in future in order to complete our study.

The data for our analysis in the VOSviewer are obtained only from the Web of Science Core Collection academic database. In future, we shall be using also some other academic databases, such as Scopus, ACM Digital Library and IEEE Xplore Digital Library, as this will provide additional research papers and a better overview of the field. These academic databases are more suitable for the field of the security requirements engineering as they focus on the computer science. Using multiple academic databases will be useful though, as none of them is perfect [36].

According to Fujs et al., different institutions have different academic database subscriptions [10]. This can result in different results despite the same query. A solution for researchers is to connect with academic peers who also have subscriptions to earlier or multiple publications. This should provide a larger corpus of scientific publications to be included in the analysis.

Our approach is also based on the keyword analysis. However, if a publication does not mention a certain term in keywords, it does not mean that it does not mention it throughout the text. Therefore, the knowledge body should be thoroughly analyzed.

ACKNOWLEDGMENT AND STATEMENT

The information contained in the analyzed scientific publications has been exclusively used to support our academic research. No human or animal participants have been involved in it. References to the literature studied in our research are given.

The paper is partly based on the research programme Security and safety in local communities - comparison of rural and urban environments (P5-0397, 2019-2024). The project is carried out by the Faculty of Criminal Justice and Security, University of Maribor, Slovenia and is financed by the Slovenian Research Agency (ARRS).

REFERENCES

[1] D. Fujs, S. L. R. Vrhovec, and D. Vavpotič, “Inovativni model za obvladovanje informacijskovarnostnih groženj pri uporabi informacijskih sistemov,”. Elektrotehniški Vestnik, 87(3), 109-116, 2020.

[2] R. Von Solms and J. Van Niekerk, “From information security to cyber security,” *Comput. Secur.*, vol. 38, pp. 97–102, 2013.

[3] S. Wendzel, C. Lévy-Bencheton, and L. Caviglione, “Not all areas are equal: analysis of citations in information security research,” *Scientometrics*, vol. 122, no. 1, pp. 267–286, 2020.

[4] S. Vrhovec, L. Caviglione, and S. Wendzel, “Crème de la Crème : Lessons from Papers in Security Publications,” in *The 16th International Conference on Availability, Reliability and Security (ARES 2021)*, 2021, pp. 17–20.

[5] U. Fayyad, G. Piatetsky-Shapiro, and P. Smyth, “The KDD Process for Extracting Useful Knowledge from Volumes of Data,” *Commun. ACM*, vol. 39, no. 11, pp. 27–34, 1996.

[6] D. Fujs, S. Vrhovec, and D. Vavpotič, “A Novel Approach for Acquiring Training and Software Security Requirements,” in *Proceedings of the European Interdisciplinary Cybersecurity Conference*, 2020, pp. 1–2.

[7] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering - A systematic literature review,” *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009.

[8] A. Liberati *et al.*, *The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration*, vol. 62, no. 10. 2009.

[9] M. Niazi, A. M. Saeed, M. Alshayeb, S. Mahmood, and S. Zafar, “A maturity model for secure requirements engineering,” *Comput. Secur.*, vol. 95, p. 101852, 2020.

[10] D. Fujs, S. Vrhovec, and D. Vavpotič, “Bibliometric mapping of research on user training for secure use of information systems,” *J. Univers. Comput. Sci.*, vol. 26, no. 7, pp. 764–782, 2020.

[11] K. Harley, R. Cooper, and N. Brunswick, “Information Integrity : Are We There Yet ?,” *ACM Comput. Surv.*, vol. 54, no. 2, pp. 1–35, 2021.

[12] ISO 27001, “ISO 27001 Information technology-security techniques-tnformation security management systems-requirements,” 2013.

[13] S. D. Quinn, M. Souppaya, M. Cook, and K. Scarfone, *National Checklist Program for IT Products - Guidelines for Checklist Users and Developers*, vol. 4. 2018, pp. 1–52.

[14] Common Criteria, “Common Criteria for Information Technology Security Evaluation,” 2017. [Online]. Available: https://www.commoncriteriaportal.org/cc/.

[15] ISACA, *COBIT 2019 Framework Introduction and methodology*. Information Systems Audit and Control Association, 2019.

[16] OWASP, “Application Security Verification Standard 4.0.2,” 2020. https://github.com/OWASP/ASVS.

[17] S. Zareen, A. Akram, and S. A. Khan, “Security requirements engineering framework with BPMN 2.0.2 extension model for development of information systems,” *Appl. Sci.*, vol. 10, no. 14, 2020.

[18] N. R. Mead and T. Stehney, “Security Quality Requirements Engineering (SQUARE) Methodology,” *ACM SIGSOFT Softw. Eng. Notes*, vol. 30, no. 4, pp. 1–7, 2005.

[19] D. Mellado, E. Fernández-Medina, and M. Piattini, “Applying a Security Requirements Engineering Process,” in *European Symposium on Research in Computer Security*, 2006, vol. 4189 LNCS, pp. 192–206.

[20] C. B. Haley, R. Laney, J. D. Moffett, and B. Nuseibeh, “Security Requirements Engineering: A Framework for Representation and Analysis,” *IEEE Trans. Softw. Eng.*, vol. 34, no. 1, pp. 133–153, Jan. 2008.

[21] N. J. van Eck and L. Waltman, “Software survey: VOSviewer, a computer program for bibliometric mapping,” *Scientometrics*, vol. 84, no. 2, pp. 523–538, Aug. 2010.

[22] G. Disterer, “ISO/IEC 27000, 27001 and 27002 for Information Security Management,” *J. Inf. Secur.*, vol. 04, no. 02, pp. 92–100, 2013.

[23] K. Beckers, “Goal-Based Establishment of an Information Security Management System Compliant to ISO 27001,” in *SOFSEM 2014: Theory and Practice of Computer Science*, 2014, vol. 8327, pp. 102–113.

[24] D. Mellado, E. Fernández-Medina, and M. Piattini, “A common criteria based security requirements engineering process for the development of secure information systems,” *Comput. Stand. Interfaces*, vol. 29, no. 2, pp. 244–253, Feb. 2007.

[25] ISO/IEC 15408-1:2009, “Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model,” Switzerland, 2014.

[26] G. Kavallieratos, S. Katsikas, and V. Gkioulos, “SafeSec Tropos: Joint security and safety requirements elicitation,” *Comput. Stand. Interfaces*, vol. 70, p. 103429, Jun. 2020.

[27] T. D. Breaux, D. G. Gordon, N. Papanikolaou, and S. Pearson, “Mapping Legal Requirements to IT Controls,” in *6th International Workshop on Requirements Engineering and Law (RELAW)*, Jul. 2013, pp. 11–20.

[28] NIST, “NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations,” 2020.

[29] J. Lopez, J. A. Montenegro, J. L. Vivas, E. Okamoto, and E. Dawson, “Specification and design of advanced authentication and authorization services,” *Comput. Stand. Interfaces*, vol. 27, no. 5, pp. 467–478, 2005.

[30] E. Paja, M. Poggianella, F. Dalpiaz, P. Roberti, and P. Giorgini, “Security Requirements Engineering with STS-Tool,” in *Secure and Trustworthy Service Composition*, vol. 8900, A. D. Brucker, F. Dalpiaz, P. Giorgini, P. H. Meland, and E. Rios, Eds. Lecture Notes in Computer Science, Springer, 2014, pp. 95–109.

[31] B. Fabian, S. Gürses, M. Heisel, T. Santen, and H. Schmidt, “A comparison of security requirements engineering methods,” *Requir. Eng.*, vol. 15, no. 1, pp. 7–40, 2010.

[32] S. H. Houmb, S. Islam, E. Knauss, J. Jürjens, and K. Schneider, “Eliciting security requirements and tracing them to design: an integration of Common Criteria, heuristics, and UMLsec,” *Requir. Eng.*, vol. 15, no. 1, pp. 63–93, Mar. 2010.

[33] J. Trujillo, E. Soler, E. Fernández-Medina, and M. Piattini, "An engineering process for developing Secure Data Warehouses," *Inf. Softw. Technol.*, vol. 51, no. 6, pp. 1033–1051, Jun. 2009.

[34] R. Sinha, S. Patil, L. Gomes, and V. Vyatkin, "A Survey of Static Formal Methods for Building Dependable Industrial Automation Systems," *IEEE Trans. Ind. Informatics*, vol. 15, no. 7, pp. 3772–3783, 2019.

[35] J. Zhu and W. Liu, "A tale of two databases: the use of Web of Science and Scopus in academic papers," *Scientometrics*, vol. 123, no. 1, pp. 321–335, Apr. 2020.

[36] M. Gusenbauer and N. R. Haddaway, "Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources," *Res. Synth. Methods*, vol. 11, no. 2, pp. 181–217, Mar. 2020.

Damjan Fujs is currently a teaching assistant and Ph.D. student at the Faculty of Computer and Information Science, University of Ljubljana, Slovenia. His research interests include cyber security, security requirements engineering and software development methodologies.

Igor Bernik is a Professor of Information Security, head of the Information Security Lab and Vice Dean for Quality Assurance and Development at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. His research interests include cybercrime, cyberwarfare, cybernetics, decision support systems and information security. He is the author and co-author of numerous scientific papers published in renowned international journals and conferences, and the author of the book Cybercrime and Cyberwarfare, published in 2014 by Wiley.