Structure or Anarchy: A Bibliometric Analysis of Keywords in Cybersecurity Education Literature

Jason M. Pittman
Department of Cybersecurity University of Maryland Global Campus
Largo, Maryland USA
0000-0002-5198-8157

Helen G. Barker
Department of Cybersecurity University of Maryland Global Campus
Largo, Maryland USA
0000-0003-4328-0121

Shaho Alaee
George Washington University
Washington, DC USA
0000-0002-4735-6552

***Abstract*—Bibliometric analysis is essential for understanding the growth, health, and trajectory of scientific disciplines. In effect, such analyses help researchers determine if a given field is well-structured or fragmented through anarchy. Prior work examined to what extent cybersecurity education research generated a follow-up study. The goal of the work was to uncover bibliometric features and characteristics linked to overall maturity of the field. The results suggested little, if any, research follow up or extension took place based on the dearth of interlinking between citations. This work continues the line of bibliometric description by investigating if cybersecurity education papers are not extended because of discoverability issues during literature reviews. To answer this question, this work explored structural bibliometric indicators in 163 journal and conference articles. Specifically, we extracted metadata keywords and paper content keywords as input to frequency analyses of the sample articles. The results revealed 12.4% of the sample contains metadata keywords. Further, 18.03% of the sample contained educated related keywords. Lastly, four of the top five sample papers by citation count do not contain keywords at all and papers with content only keywords exhibited more frequent citation than those with only metadata keywords. Based on these results, we offer observational conclusions as well as notions for future work.**

Keywords—Cybersecurity education, pedagogy, laboratories, bibliometrics

I. INTRODUCTION

Often, scholarly research ends with ruminations on how the work might extended in the future. The presence of these ideas constitutes an implicit social contract within the academic community as statements of future work engender follow-up study. This is the way - brick by brick, study extending study - the roadwork interlinking a scientific field of knowledge is constructed. Yet, despite the assumption that literature adheres to such a social contract, and the ubiquity of future work sections in published work, nearly 80% of cybersecurity education studies do not extend existing research [1]. Comparatively, foundational work in computer science [2] discovered only 70% of 200 sample papers from the ACM catalog were extended after publication.

On one hand, according to the literature, low frequency of extension might reflect a high degree of terminal research. On the other hand, the same literature suggests low frequency of extension might indicate a young, growing field of knowledge, poor health of the field, or even an expected difference given the nature of inquiry in the field. Given the wide range of possible explanations, there is a clear call for additional bibliometric analysis. Indeed, existing research [1] quantified how often cybersecurity education literature exhibited scientific follow-up. The study suggested a potential problem driving the dramatic lack of follow-up might be researchers not being able to find relevant source research during literature searches.

One potential avenue to affect an examination of such a research problem would be to extract metadata keywords from the PDF files and measure the frequency of those keywords in the article. Keywords are intended to serve as indicators of an article's content, and have often been used in scientometrics or bibliometric analysis of literature [3]–[5]. By way of analogy, keywords ought to function similarly to keywords in Search Engine Optimization (SEO) or tags in searchable text. Yet, the literature [6] suggests keywords in PDF metadata are underutilized by common search mechanisms. As a baseline, one study [7] found 62% of papers do not include author supplied keywords. As such, the purpose of this work was to examine a sample of cybersecurity laboratory education research and utilize statistical analyses to describe structural features related to discoverability (i.e., metadata-based keywords, keyword frequencies, and citations counts).

The following sections detail the relevant background to conceptualize the current study. The related work discussion is followed by a detailing of the research design and methodology employed during this work. Finally, the results of the analyses are presented and reviewed.

II. RELATED WORKS

Scientific progress and the operative health of a field of study are intertwined. Because of the tight coupling between these concepts, it is possible to infer the latter by the quantitative assessment of the former. The established scientific methodology to explore both concepts is through bibliometrics [8]. Accordingly, the following sections describe the existing literature forming the conceptual and theoretical framework for our analysis of cybersecurity education research structural bibliometrics.

A. General Bibliometrics

Bibliometric analyses are used across a variety of scientific fields. According to [9], "bibliometrics is to

scientific papers what epidemiology is to patients" (p. 14). As a scientific method, bibliometric analysis quantitatively explores the evolution of a given discipline, reveals research gaps, and describes the structure of both individual works as well as broader fields of study [8], [10], [11]. The types of exploration are achieved by working with one of three types of bibliometric indicators: quantity indicators, performance indicators, and structural indicators [12]. While quantity and performance bibliometric indicators have found broad use across academia (e.g., impact factor, h-index), structural bibliometric analysis exclusively facilitates working with knowledge architecture.

B. Structural Bibliometrics

Trends in research structural indicators are important in establishing growth and health of knowledge domains [13]. Structural bibliometrics trace the development of a field of study through its architecture. One output of structural methods can be a map of the interconnectedness of research [10], [14]. As well, structural features of literature can statistically reveal patterns in publications [3]–[5].

Along such lines, analyzing structural indicators – specifically, keywords – is a primary methodology to uncover possible developmental issues in a growing scientific field [8]. Such changes reflect shifts in trends within a field. Moreover, structural elements such as keywords may reveal underlying field development [15]. Additionally, researchers [16], [17] have given significant attention to keywords as domain or knowledge search artifacts. Some work [17], [18] suggests structural artifacts such as the title, abstract, and keywords are indexed in combination as if those artifacts are *the* paper. Fortunately, keywords (as well as other artifacts) exist both as a defined standard for PDF file metadata [19] and are included in scientific article text.

C. Metadata Standards

There are three fundamental mechanisms for attaching metadata to scientific literature: embedded, associated, and third-party [19]. Embedded metadata is a critical source of identifiable attributes such as document title, authors, journal information, and keywords [20]. This type of metadata must be generated at the point of document creation and has the tightest coupling to the file object because it becomes part of it.

Standards exist for these PDF metadata fields [21], [22] and largely exist to enable forms of *search*. Search in this case can either be for the goal of indexing such as for libraries [23] or for end users looking to discover scientific information [24].

The PDF file format has a public specification establishing the technical details for embedded metadata [25], [26]. Specifically, the specification indicates the metadata header is to be embedded as a set of key, value pairs in the *Document Information Dictionary* [26]. Both the metadata header and individual fields within are optional. The possible metadata fields [26, 14.3.3] are as follows:

```
Def metadata_header :
   Title = str()
   Author = str()
   Subject = str()
   Keywords = str()
   Creator = str()
   Producer = str()
   CreationDate = date()
   ModDate = date()
   Trapped = name ()
```

Despite the existence of a PDF metadata standard, existing research [6], [21], [27] continually indicates reading data from PDF metadata fields is a serious challenge. To that end, much of the current literature attempts to establish metadata extraction mechanisms [6], [7], [20], [23]. At the same time, development of automated tools, techniques, and practices presupposes keyword metadata is populated with author supplied content. Based on existing research [7], a majority (62%) of papers do not have keyword metadata available. The extent to which cybersecurity education literature follows the same trend is an open question.

III. METHOD

This study was motivated by wanting to understand potential structural bibliometrics features of cybersecurity education literature related to article discoverability. In particular, we sought to answer whether cybersecurity laboratory education papers are not extended because researchers are unable to find them during literature reviews based on keyword presence in the PDF metadata. To answer this question, we identified a population and sample, developed appropriate instrumentation and a research protocol, and then conducted frequency analyses.

A. Population and Sample

We leveraged the sample from prior work [1] first establishing the lack of research extension in cybersecurity laboratory education with one modification. We used only the original type studies which totaled 163.

The rationale for doing so is twofold. Primarily, using established population and sample ensures this work carries forward the validity and quality of data in the source paper [28]. Secondarily, this study adds to the collective understanding of the research problem by addressing a different question to the original data [29].

B. Instrumentation

Bibliometric analysis tools, while not plentiful, do exist. However, structural bibliometric analysis tools are more limited, specifically instruments working with keywords. No tool exists which specifically detects metadata keywords and calculates overall document frequency of those keywords. To that end, we developed an instrument [30] consisting of four components. First, the instrument needed to load a specified

PDF file object. Second, the instrument needed to read embedded metadata. Third, the instrument needed to parse the PDF content and compute frequencies for keywords detected in the file object metadata. Lastly, the instrument needed to output data in a standardized format.

1) Pilot Study: We conducted a pilot study to assess the inter-rater reliability of the instrument developed for this research. We selected the pilot sample from a field of science with a high degree of follow up work but with adjacency to computer science and cybersecurity. Thus, based on NSF publication output trends [31], we identified *Health sciences and biological and biomedical sciences* in general and *computational biology* in specific.

The pilot sample consisted of 26 papers downloaded from academic databases and separated into two strata. One stratum consisted of literature containing keywords in the metadata field. The second stratum literature lacking keywords in the metadata field or the field itself. Overall, the pilot size was greater than 20% of the study sample ($N = 163$).

We then analyzed metadata keyword extraction for the pilot sample using two mechanisms: *exiftool* and the research instrument. We established a rating system of zero and one, corresponding to a judgment of *correct* and *incorrect*. Then, we used the Python *unittest* package to automate the rating of both step one groups and record the results. The results for metadata keyword extraction revealed a inter-rater reliability of 100%. In other words, the research instrument reliably extracted PDF metadata when such was present and did not retrieve metadata when none was available.

Lastly, we assessed the inter-rater reliability of calculating keyword frequency in the paper content. For this test, we applied the research instrument to the pilot sample strata containing keywords only. Then, we recorded keyword frequency from the instrument and the same from the native *find* feature in our text editor. Where frequency matched, we judged the outcome as zero, otherwise as one. The results for metadata keyword frequencies demonstrated 92.2% reliability. Potential explanations for these results are outlined in the *Limitations* section below.

C. Research Protocol

There is no direct measurement for article discoverability in the structural bibliometric literature. Impact factor is a similar concept but not applicable in this work because we are not interested in *influence* of authors, journal, or topic. Instead, we measured adjacent factors and infer structural attributes through descriptive and frequency and analyses. While not direct evidence for discoverability, our goal for such analyses was to peel back the bibliometric curtain somewhat obscuring potential answers to why the cybersecurity laboratory education literature is fragmented.

To achieve this, we developed the following research protocol:

- Download PDF versions of papers in the sample.
- Code sample papers according to citation key (e.g., authorYEARkeyword).
- Extract metadata using instrument.
- Extract paper content using instrument.
- Conduct frequency analysis of:
    - ...metadata keywords in paper content.
    - ...paper text keywords in paper content.
- Capture citation counts for sample papers.
- Conduct observational inference based on descriptive statistics.

D. Limitations

This research has four limitations. Foremost, we opted to only include research articles available from a journal or conference in PDF format. While doing so covers the majority of available research, some papers are available in other formats (e.g., Microsoft Word) exclusively and may exhibit different structural bibliometric characteristics. Further, a notable limitation of this study is the underlying assumption of keyword importance in cybersecurity education research relative to literature search and discovery.

The instrumentation does have some limitation as well, specifically related to keyword frequency calculation. Some PDFs are rendered with nonstandard UTF-8 character formatting which inhibits frequency analysis. Likewise, content justification forcing splitting of words or hyphenated word wrapping artificially lowers words counts. Meanwhile, counts can be inflated when keywords appear in bibliography material as part of cited research titles.

A final limitation of this work revolves around the generation of PDF documents. The end user has no control over the tools, techniques, and practices employed by authors in the generation of a document. In another way, this work is limited by the publisher. The end user has no knowledge whether the publisher employs a process which might negatively impact (i.e., remove) metadata content. Thus, all structural bibliometric analyses are limited by potentially unseen and unknown document handling procedures.

IV. RESULTS

A. Frequencies

Data were collected from 163 cybersecurity laboratory education papers previously categorized as original research articles [1]. From the 163 sample papers, 20 exhibited a populated keyword metadata field or 12.4%. We initially focused frequency analyses on this subset of the sample.

The sample papers and the frequency of the metadata keywords contained in the paper content revealed more structural bibliometric details (Appendix, Table VI). Two papers out of the subset of 20 had zero occurrence of a metadata keyword in their content. The highest frequency of an individual keyword was 81 occurrences. Meanwhile, three papers from the subset of 20 had a metadata keyword with a frequency of zero in the paper content. The high σ (standard deviation) and σ^2 (variance) values indicate extreme spread

between individual data elements (Table I). As an aside, we took a σ greater than one-third of $\bar{X}$ (Mean) to indicate *high*.

TABLE I. FREQUENCY ANALYSIS OF METADATA KEYWORDS

	Keywords	Frequency
Mean	44.95	3.95
Median	35.5	4
Mode	0	3
Std Dev	43.39	1.23
Variance	1882.99	1.52
Min	0	1
Max	153	6

1. *keywords* column is total keywords across all papers.
2. *frequency* column is number of keywords per paper.

Next, we analyzed the frequency of the keywords extracted from the content of the same 20 sample papers which had metadata keywords present (Appendix, Table VII). Three papers in this group had zero keywords. Yet, all the keywords, when present, had at least one occurrence in the paper content inclusive of the keyword itself. The highest frequency of individual keyword was 106. Notably, the σ (standard deviation) and σ^2 (variance) demonstrated higher values compared the metadata keyword dataset, meaning the spread between individual data elements was both high and comparatively greater (Table II).

TABLE II. FREQUENCY ANALYSIS OF PAPER KEYWORDS

	Keywords	Frequency
Mean	67.63	4.25
Median	67.63	4
Mode	16	5
Std Dev	53.97	1.13
Variance	2912.05	1.27
Min =	4	2
Max	191	6

1. *keywords* column is total keywords across all papers.
2. *frequency* column is number of keywords per paper.

We also performed a frequency analysis on citations (i.e., *cited by*) of the 20 papers containing metadata keywords. The per sample paper citation quantities (Appendix, Table VIII) revealed a maximum citation count of 120 and a minimum of zero. The σ (standard deviation) and σ^2 (variance) demonstrate a moderate spread in the individual data elements (Table III).

TABLE III. FREQUENCY ANALYSIS OF PAPER CITATIONS WITH METADATA KEYWORDS

	Citations
Mean	17.45
Median	8
Mode	14
Std Dev	27.20
Variance	739.94
Min	0
Max	120

The majority of the overall sample did not contain structural metadata ($N = 143$). At the same time, only 72% of this subset ($N = 103$) contained keywords in the paper content. The range of keywords exhibited by these papers was substantial: the maximum number of keywords was 17 while the minimum was two. The highest frequency of an individual keyword was 465 while the minimum was, again, zero. The standard deviation (σ) and variance (σ^2) demonstrated significant dispersion (Table IV).

TABLE IV. FREQUENCY ANALYSIS OF PAPER KEYWORDS WITHOUT METADATA

	Keywords	Frequency
Mean	78.50	4.37
Median	45.5	4
Mode	7	4
Std Dev	100.21	1.79
Variance	10042.27	3.19
Min	0	2
Max	560	17

1. *keywords* column is total keywords across all papers.
2. *frequency* column is number of keywords per paper.

Finally, we analyzed the frequency of paper citations (*N* = 143) for the sample not containing metadata keywords (Appendix, Table IX). We found a maximum citation count of 183 and a minimum citation count of zero. Data elements continued to exhibit wide dispersion (σ) and variance (σ^2). Notably, these data revealed a Median and Mode roughly inverse compared to the papers with metadata keywords (Table V).

TABLE V. FREQUENCY ANALYSIS OF PAPER CITATIONS WITHOUT METADATA KEYWORDS

	Citations
Mean	21.6
Median	11
Mode	8
Std Dev	30.21
Variance	912.56
Min	0
Max	183

V. CONCLUSIONS

Bibliometric analysis is essential for understanding the growth, health, and trajectory of scientific disciplines. One objective of such analyses is to deconflict or lessen the complexity of accumulating cybersecurity education knowledge. This is particularly true as the field is expanding at an increasing rate. To that end, prior research [1] demonstrated the cybersecurity laboratory education literature is fragmented topologically. In other words, new research is not interlinked to existing studies through citations. The prior work left open questions inquiring about reasons for such being true. This study attempted to investigate one potential answer by operationalizing structural bibliometrics, specifically metadata and keywords.

The results of this study revealed four notable factors related to the structural bibliometrics of cybersecurity laboratory education literature. We present observational interpretations for these factors, followed by ideas for future work. Our hope is the field recognizes the scientific and practical significance of the results and continued research pursue investigations into the health and growth of cybersecurity education literature.

Foremost, nearly a quarter (24.4%) of the sample did not contain any keywords whatsoever, metadata or paper content. Meanwhile, a full 87.6% did not contain metadata keywords. Significantly more cybersecurity laboratory education papers lacked metadata keywords than existing research [7] in computer science found. While we would not expect results from two different fields to be identical, it is notable such closely related fields of knowledge differ by more than 20%. Such is all the more curious when considering the two fields exhibited similar findings in terms of research extension [1].

Perhaps more revealing, we observed keywords related to *education* (e.g., training, learning, etc.) only account for 18.03% of keywords across all sample papers. In other words, more than three-quarters of keywords are not related to education per se. It is possible this factor compounds potential issues in literature discoverability given a significant quantity of papers do not include keywords at all. We also observed when a keyword such as education, training, learning, or so forth is present, the term is not the most frequently used in the paper content. Finally, we observed four of the five highest citation count papers do not have metadata or paper keywords at all. Moreover, the highest citation frequencies come from literature with paper content keywords only, not metadata keywords. Taken collectively, we wonder to what extent the literature emphasizes technical aspects of cybersecurity versus the education or training of the technical aspects of cybersecurity.

Additional future work is necessary to pursue why cybersecurity education research is so loosely related through citations. Within structural bibliometrics, future work may be necessary to develop quantitative instrumentation and measures for casual relationships. In other words, the field needs a mechanism to harness experimental designs to move beyond correlational inferences. This is certainly complex to architect but may have significant payoff to researchers, practitioners, and to the plethora of knowledge domains stagnating on the edges of maturity and growth. While this work has quantitatively described the structural bibliometrics characteristics of the cybersecurity laboratory education literature, we are not necessarily closer to understanding potential correlational and causal factors. Thus, future work is still necessary to establish which characteristics have operational relationships.

As a side note, the lack of metadata negatively impacts software tools and automation. In fact, we had to manually retrieve *bibtex* citation entries for the 163 papers comprising the data sample. This was necessary to cross-reference the literature and verify we had the correct papers in the sample. Had the metadata been populated per the PDF standard, a variety of tools could have been used to automate the work.

REFERENCES

[1] J. M. Pittman, R. Kobbe, T. Lynch, and H. G. Barker, "Cybersecurity laboratory education research: A lush ecosystem or elephant graveyard?" in *Journal of The Colloquium for Information Systems Security Education*, vol. 9, no. 1, 2022, pp. 6–6.

[2] J. Wainer and E. Valle, "What happens to computer science research after it is published? tracking cs research lines," *Journal of the American Society for Information Science and Technology*, vol. 64, no. 6, pp. 1104–1111, 2013.

[3] S. E. Fratesi and H. L. Vacher, "Scientific journals as fossil traces of sweeping change in the structure and practice of modern geology," *Journal of Research Practice*, vol. 4, no. 1, pp. M1–M1, 2008.

[4] J. Lonchamp, "Computational analysis and mapping of ijcscl content," *International Journal of Computer-Supported Collaborative Learning*, vol. 7, no. 4, pp. 475–497, 2012.

[5] S. Reinhold, C. Laesser, and D. Bazzi, "The intellectual structure of transportation management research: A review of the literature," 2015.

[6] M. W. Ahmed and M. T. Afzal, "Flag-pdfe: Features oriented metadata extraction framework for scientific publications," *IEEE Access*, vol. 8, pp. 99 458–99 469, 2020.

[7] K. Patel, C. Caragea, J. Wu, and C. L. Giles, "Keyphrase extraction in scholarly digital library search engines," in *Web Services – ICWS 2020: 27th International Conference, Held as Part of the Services Conference Federation, SCF 2020, Honolulu, HI, USA, September 18–20, 2020, Proceedings*. Berlin, Heidelberg: Springer-Verlag, 2020, p. 179–196.

[8] W. Glanzel, *Bibliometrics as a research field a course on theory and application of bibliometric indicators*, 2003.

[9] G. Lewison and M. E. Devey, "Bibliometric methods for the evaluation of arthritis research." *Rheumatology (Oxford, England)*, vol. 38, no. 1, pp. 13–20, 1999.

[10] M. K. McBurney and P. L. Novak, "What is bibliometrics and why should you care?" in *Proceedings. IEEE international professional communication conference. IEEE*, 2002, pp. 108–114.

[11] I. Zupic and T. C˘ ater, "Bibliometric methods in management and organization," *Organizational research methods*, vol. 18, no. 3, pp. 429– 472, 2015.

[12] V. Durieux and P. A. Gevenois, "Bibliometric indicators: quality measurements of scientific publication," *Radiology*, vol. 255, no. 2, pp. 342– 351, 2010.

[13] M. d. C. Giménez-Espert and V. J. Prado-Gascó, "Bibliometric analysis of six nursing journals from the web of science, 2012–2017," *Journal of advanced nursing*, vol. 75, no. 3, pp. 543–554, 2019.

[14] O. J. de Oliveira, F. F. da Silva, F. Juliani, L. C. F. M. Barbosa, and T. V. Nunhes, "Bibliometric method for mapping the state-of-the-art and identifying research gaps and trends in literature: An essential instrument to support the development of scientific projects," in *Scientometrics recent advances*. IntechOpen, 2019.

[15] Y. Song, X. Chen, T. Hao, Z. Liu, and Z. Lan, "Exploring two decades of research on classroom dialogue by using bibliometric analysis," *Computers & Education*, vol. 137, pp. 12–31, 2019.

[16] G. Chen and L. Xiao, "Selecting publication keywords for domain analysis in bibliometrics: A comparison of three methods," *Journal of Informetrics*, vol. 10, no. 1, pp. 212–223, 2016.

[17] B. Pesta, J. Fuerst, and E. O. Kirkegaard, "Bibliometric keyword analysis across seventeen years (2000–2016) of intelligence articles," *Journal of Intelligence*, vol. 6, no. 4, p. 46, 2018.

[18] T. Bekhuis, "Keywords, discoverability, and impact," *Journal of the Medical Library Association: JMLA*, vol. 103, no. 3, p. 119, 2015.

[19] E. Duval, W. Hodgins, S. Sutton, and S. L. Weibel, "Metadata principles and practicalities," *D-lib Magazine*, vol. 8, no. 4, pp. 1–10, 2002.

[20] Z. Bodo´ and L. Csato´, "A hybrid approach for scholarly information extraction," *Studia Univ. Babes-Bolyai, Inform*., vol. 62, no. 2, pp. 5– 16, 2017.

[21] F. Cave, "Article metadata standards: an historical review," *OCLC Systems & Services: International digital library perspectives*, 2003.

[22] B. Eden, "New and emerging metadata standards," *Library Technology Reports*, vol. 41, no. 6, pp. 34–44, 2009.

[23] S. T. R. Rizvi, A. Dengel, and S. Ahmed, "A hybrid approach and unified framework for bibliographic reference extraction," *IEEE Access*, vol. 8, pp. 217 231–217 245, 2020.

[24] J. Kemp, "Metadata and discoverability: A use case overview," *Information Services & Use*, vol. 38, no. 1-2, pp. 81–84, 2018.

APPENDIX

TABLE VI. SAMPLE METADATA KEYWORD AND FREQUENCIES

	Keywords & Frequencies
choi2010feasibility	exercises: 2, labs: 33, security: 81, security education: 8, virtual lab: 29
bazzaza2015using	Cloud Computing: 2, Computer Networks: 7, eLearning: 0, Education Technology: 1
mountrouidou2018cybersecurity	Cybersecurity; General Education; Liberal Arts; GENI: 0
james2020hands	Computing education: 2, Computer security: 5, Computer architecture: 1
wang2020developing	Information Security; Ethical Hacking; Course Design: 1
hu2008teaching	Security: 51, Xen: 9, Virtual Environment: 1, Project: 17
wu2010benefits	VMware workstation: 4, education: 9, information security: 4, lab assignment: 1, virtualization: 28
miloslavskaya2018developing	Information security incident: 11, Online banking services: 2, Money transfer: 4, Hands-on laboratory work: 4, Computer forensics: 10
buckley2018introducing	Cybersecurity; security education: 1, software testing; computer security; defect detection: 0, software maintenance: 1
crowley2003information	Information technology curricula; Information technology security; security: 0
zeng2013research	cross site scriping: 1, lab environment: 16, higher vocational college: 11, network security: 5, attack: 40, defense: 24
trabelsi2013hands	Information security curriculum: 6, DoS attacks: 31, Hands-on lab exercises: 21, Ethical hacking: 24, Schools and educators liability: 1
broisin2017lab4ce	Online learning environment: 1, Remote laboratory: 15, Computer science: 18
trabelsi2011hands	ARP cache poisoning: 36, Denial of Service (DoS) attack: 0, Man-in-the-Middle (MiM) attack: 2, sniffer: 4
chi2014design	Virtual Training: 1, Insider Threats: 9, Hands-on lab: 23, Information Assurance: 6, Active Learning: 4, CyberCIEGE: 25
iqbal2015conceptual	information security lab: 4, ensemble artefact: 0, design principles: 19
tunc2015claas	CLaaS: 26, virtualization: 6, cybersecurity: 28, virtual lab: 2, education: 6
pittman2013understanding	Cybersecurity laboratory: 40, laboratories: 54, system utilization: 18, literature analysis: 3 chan2004vpl
chan2004vpl	Education: 8, Virtual Programming Laboratory: 12, Distance Learning: 14, E-Learning: 3
irvine1999reference	Computer Security Education: 6

TABLE VII. PAPER CONTENT KEYWORDS AND FREQUENCIES

	Keywords & Frequencies
choi2010feasibility	Virtual lab: 38, security: 106, exercises: 2, labs: 35, security education: 10
bazzaza2015using	Computing:5; Computer Networks: 9; eLearning: 1, Education Technology: 1
mountrouidou2018cybersecurity	Cybersecurity: 68, General Education: 27, Liberal Arts: 13, GENI: 13
james2020hands	Computing education: 2, Computer security: 5, Computer architecture: 1
wang2020developing	Information Security: 11; Ethical Hacking: 12; Course Design: 3
hu2008teaching	
wu2010benefits	
miloslavskaya2018developing	information security incident: 12, online banking services: 2, money transfer: 5, hands-on laboratory work: 5, computer forensics: 14
buckley2018introducing	security education: 4, software testing: 9; computer security: 1; defect detection: 1, software maintenance: 1
crowley2003information	Information technology curricula: 1, Information technology security: 3
zeng2013research	cross site scripting: 6; lab environment: 24; higher vocational college: 18; network security: 9; attack: 48; defense: 29
trabelsi2013hands	Information security curriculum: 6, DoS attacks: 35, Hands-on lab exercises: 26, Ethical hacking: 29, Schools and educators liability: 1
broisin2017lab4ce	Online learning environment: 2. Remote laboratory: 17. Computer science: 21
trabelsi2011hands	Denial of Service (DoS) attack: 1, Man-in-the-Middle (MiM) attack: 2, ARP cache poisoning: 41, Sniffer: 7
chi2014design	Virtual Training: 1, Insider Threats: 10, Hands-on lab: 24, Information Assurance: 8, Active Learning: 5, CyberCIEGE: 28
iqbal2015conceptual	
tunc2015claas	CLaaS: 26; virtualization: 7; cybersecurity: 40; virtual lab: 2; education: 7
pittman2013understanding	Cybersecurity laboratory: 43, laboratories: 56, system utilization: 18, literature analysis: 4
chan2004vpl	Education: 8; Virtual Programming Laboratory: 13; Distance Learning: 14; E-Learning: 3
irvine1999reference	Computer Security Education: 12, Reference Monitor Concept: 48, Assurance: 12, Graduate Education: 1

TABLE VIII. WITH METADATA KEYWORDS SAMPLE CITATION FREQUENCIES

	Keywords & Frequencies
choi2010feasibility	9
bazzaza2015using	14
mountrouidou2018cybersecurity	14
james2020hands	3
wang2020developing	3
hu2008teaching	24
wu2010benefits	7
miloslavskaya2018developing	1
buckley2018introducing	5
crowley2003information	120
zeng2013research	13
trabelsi2013hands	18
broisin2017lab4ce	53
trabelsi2011hands	18
chi2014design	4
iqbal2015conceptual	2
tunc2015claas	6
pittman2013understanding	5
chan2004vpl	0
irvine1999reference	30

TABLE IX. WITHOUT METADATA KEYWORDS SAMPLE CITATIONS FREQUENCIES

Papers	F
abbott2008developing	26
abler2006georgia	67
adams2005configuring	35
aly2004cryptography	6
anantapadmanabhan2003design	16
bell2018meeting	3
beltran2018experiences	10
bhatt2018using	15
bishop1993teaching	29
bishop1997computer	11
bishop2009critical	20
bishop2013some	8
Bishop97thestate	20
brustoloni2006laboratory	33
Buchler2018	36
bullers2006virtual	124
cai2018using	7
caltagirone2006design	22
cavanagh2011goals	4
zeng2013research	7
chatmon2010active	16
chicone2018using	5
chin1997information	16
chou2018developing	8
chow2017cooperative	3
colon2018capture	2
connor2018board	1
conti2003comprehensive	15
crawford2011multi	7
cronin2013creating	4
dai2018situation	11
Dark2015	36
de2018tutorials	10
deng2018	19
di1997virtual	22
zeng2013research	13

Papers	F
dobrilovic2012usability	14
dobrilovic2012virtualization	5
dobrilovic2013expanding	17
du2010enhancing	28
du2011seed	88
elias2015design	1
eliot2018flexible	25
ezenwoye2019integrating	2
fernandez2013virtualization	3
franco2018network	5
frydenberg2020lizards	1
fundaburk2001developing	1
gephart2010design	15
graham1999monitoring	1
guild2004design	4
guler2012virtualized	8
haag2018dvcl	3
hartley2015ethical	17
hartley2017ethical	13
harvey2006virtual	6
hill2001using	165
idziorek2012security	6
irvine1997challenges	8
irvine1997naval	19
irvine1997nps	19
irvine1997teaching	8
irvine1998integrating	121
irvine1999amplifying	32
irvine1999benefits	0
irvine2003teaching	57
irvine2017labtainers	8
james2016cybersecurity	7
jardim2014u	5
Kam2020	20
king2006rapidly	3
zeng2018improving	7

Papers	F
konak2018experiential	19
kotevski2018free	10
kwon2017enriching	9
leblanc2004teaching	25
lee2010design	22
liurescue	0
lodgher2018innovative	7
lukowiak2014cybersecurity	16
mano2006case	8
marquardson2018cyber	6
marsa2013design	37
mattord2004planning	30
mayo2003tcp	3
mink2010evaluation	18
mok2012setting	6
munoz2016computing	8
murphy2014building	8
murphy2015experiences	5
naf2008two	12
o2006laboratory	54
o2017innovative	8
padman2002design	44
papanikolaou2011hacker	9
peltsverger2014bottleneck	6
pittman2020exploring	0
qu2018teaching	0
ramalingam2007practicing	11
richards2002illustrating	15
rickman2001enhancing	11
roschke2010security	8
roychoudhuritoward	0
salah2015teaching	64
schumacher2002educating	12
sharma2007teaching	64
shipman2015lab	4
zhu2015hands	12

Papers	F
siraj2014empowering	13
son2012virtual	40
spafford1997one	7
stanisavljevic2018adding	2
stefanek2017use	1
stewart2010developing	2
sun2010experiences	2
tao2010virtual	12
tao2010work	6
thibodeaux2001ethical	5
timchenko2015simple	15
trabelsi2012switch	13
trabelsi2013teaching	20
trabelsi2014enhancing	8
trabelsi2014web	4
trabelsi2016ethical	22
trabelsi2018teaching	11
tzeng2000design	14
vaughn1999integration	20
vaughn2004building	53
vigna2003teaching	90
wagner1999computer	69
wagner2004designing	69
wang2010using	58
wang2013pvee	0
wang2015hands	16
welch2001trial	32
winters2006tinkernet	14
wolf2009assessing	145
wu2014teaching	17
yang2004design	39
yasinsac2002information	24
yasinsac2003computer	183
yuan2008laboratory	9
yuan2014developing	5