Arabian Journal for Science and Engineering
https://doi.org/10.1007/s13369-019-04319-2

RESEARCH ARTICLE - COMPUTER ENGINEERING AND COMPUTER SCIENCE

Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study

Mamoona Humayun[1] · Mahmood Niazi[2] · NZ Jhanjhi[3] · Mohammad Alshayeb[2] · Sajjad Mahmood[2]

Received: 9 May 2019 / Accepted: 26 December 2019

Abstract
There has been a tremendous increase in research in the area of cyber security to support cyber applications and to avoid key security threats faced by these applications. The goal of this study is to identify and analyze the common cyber security vulnerabilities. To achieve this goal, a systematic mapping study was conducted, and in total, 78 primary studies were identified and analyzed. After a detailed analysis of the selected studies, we identified the important security vulnerabilities and their frequency of occurrence. Data were also synthesized and analyzed to present the venue of publication, country of publication, key targeted infrastructures and applications. The results show that the security approaches mentioned so far only target security in general, and the solutions provided in these studies need more empirical validation and real implementation. In addition, our results show that most of the selected studies in this review targeted only a few common security vulnerabilities such as phishing, denial-of-service and malware. However, there is a need, in future research, to identify the key cyber security vulnerabilities, targeted/victimized applications, mitigation techniques and infrastructures, so that researchers and practitioners could get a better insight into it.

Keywords Cyber security · Threats · Vulnerabilities · Attack

1 Introduction

In today's world, cyber civilization has become a popular and inevitable source of information sharing and other professional activities including business, shopping, bank transactions, advertisements, services, etc. This exponential increase in the use of cyberspace has resulted in an exponential increase in cybercriminal activities. The basic reason for this increase is the excessive usage of Web applications in almost every field of life. These Web applications are not free from design faults, and cyber criminals exploit these faults to gain illegal access to systems [1, 2]. Therefore, cyber security has become an important concern for researchers and practitioners [2]. Cyber security can be defined as the collection of tools, techniques, policies, security measures, security guidelines, risk mitigation strategies, actions, training, good practices, security reassurance and latest technologies that may be used to protect cyber space and the assets of users [3]. Cyber security nowadays has become a matter of global interest and importance, and it involves securing information by detecting, preventing and responding to cyber attacks [3–5].

The defensive mechanisms used by various organizations to protect their cyber space are not sufficient to protect these cyber environments from the ever-increasing security vulnerabilities. Therefore, it is one of the important scientific challenges that has been attracting the attention of researchers and practitioners for the last decade. A number of research efforts have been made in different cyber domains, each having specific features and peculiarities to address various security breaches [1]. In the literature, various approaches and tools have been suggested for the detection and the mitigation of cyber security threats [6, 7]. However, before proceeding with further research in this area, there is a need to compile the existing work. To fill this gap, this research study aims to provide a broad

✉ NZ Jhanjhi
noorzaman.jhanjhi@taylors.edu.my

[1] Department of Information systems, College of Computer and Information Sciences, Jouf University, Al-Jouf, Saudi Arabia

[2] Information and Computer Science Department, King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia

[3] SoCIT, Taylor's University, Subang Jaya, Malaysia

Published online: 06 January 2020

and detailed landscape of cyber security vulnerabilities and the provided solutions.

The objective of this study is to conduct a systematic mapping study in order to identify and analyze the common cyber security vulnerabilities. This mapping study intends to identify the available studies on cyber security vulnerabilities and categorize these solutions against (1) commonly available security vulnerabilities, (2) victims of cyber threat, (3) vulnerability severity and (4) methods of data collection and validation approaches. Specifically, our mapping study addresses the following research questions:

RQ1 What are the common cyber security threats and vulnerabilities?

One of the main RQs is to find the key security vulnerabilities based on their frequency of occurrence in the selected studies. Finding an answer to this question will help researchers and practitioners understand the key security vulnerabilities and determine the main research areas in the field.

RQ2 What are the key venues for publications on cyber security threats and vulnerabilities?

This RQ will identify the key venues for publications on cyber security. The answer to this question will help researchers find the main conferences and journals in the field to publish their research in a relevant place.

RQ3 Who are the active researchers on cyber security threats and vulnerabilities?

This question will identify active researchers and their countries. This will help in identifying active researchers in the field.

RQ4 Who are the key victims of security vulnerabilities?

The answer to this question highlights the victims of security breaches. We classify victims into two broad categories, namely individual and organization. The answer to this question will help researchers and practitioners to gain an overview of the major victims of cyber security vulnerabilities. This will help in knowing the main trend of security vulnerability attacks.

RQ5 Which applications are the targets of cybercrimes in the selected studies?

The answer to this question will be a list of applications that were targets of cyber security in the selected studies and will provide an insight into these application users so that they can protect their applications from cyber attacks.

RQ6 What are the common cyber security mitigation techniques discussed in the literature?

The answer to this question will be a list of mitigation techniques used to overcome cyber security threats and will help researchers gain an overview of the existing techniques available so far.

The remainder of this paper is structured as follows. Section 2 describes the background knowledge. Section 3 briefly describes some existing work. Section 4 explains the research methodology. Section 5 presents the results of the study followed by Sect. 6 which presents a discussion of the results. The paper is concluded in Sect. 7 followed by Sect. 8 which discusses some open issues.

2 Background

This section provides background information on cyber security.

2.1 Cyber Security

Security is defined as "the protection against undesirable disclosure, destruction, or modification of data in a system and also the protection of systems themselves" [8]. According to ISACA "Cyber security is concerned with the security and privacy of digital assets-everything from networks to computing devices and information that is processed, stored or exchanged by internetworked information systems" [9]. According to the International Telecommunications Union, cyber security is the collection of techniques, rules, policies, best practices and approaches used to protect a user's assets and cyber organizations [9, 10]. Cyber security is defined as "preserving the integrity, confidentiality, and timely availability of information in cyberspace" [9]. The Merriam-Webster dictionary defines cyber security as protecting computer systems from unauthorized access and attacks [11]. According to [3], cyber security is defined as the processes and technologies used to protect computing devices and networks from unauthorized access and attacks over the Internet. Cyber security is the protection of physical and non-physical components of organizations from illegal access [12].

According to these definitions, researchers define cyber security in different ways. Existing definitions focus on different cyber security aspects. For example, some definitions focus on protection and privacy, while others highlight the needs for defining rules and policies for information integrity, confidentiality, and availability. In addition,

other researchers stressed the need to define processes and technologies to protect computing devices. Cyber security can be considered as a mechanism of protecting individuals' and organizations' assets from unauthorized access. These definitions also highlight the importance of the cyber environment and its protection.

2.2 Cyber Security Terminologies

Following are some definitions of important terminologies that are necessary to gain a better understanding of the key concepts related to the area under research.

Cyber space is a global domain within the information world whose distinct characteristic is the use of the electronic and electromagnetic spectrum to create, update, store, share and exploit information with the help of interconnected and dependent networks using the latest information and communication technologies [13–15].

Vulnerabilities These are the flaws in a system or its design that allows an attacker to execute malicious commands, access data in an unauthorized way and/or conduct various denial-of-service attacks [16, 17].

Threats These are actions taken to gain a benefit from security breaches in a system and negatively impact it [16, 18].

Attacks These are the actions taken to damage a system or disturb its routine operations by exploiting vulnerabilities using various tools and techniques. Attackers launch these attacks to achieve their malicious goals, either for self-satisfaction or for financial reward [18, 19].

A number of security vulnerabilities have been discussed in the literature. To assist the readers to better understand some of the common cyber security vulnerabilities, these are described as follows:

- *Denial-of-service (DoS)* This type of attack is an effort to make a machine or network resource inaccessible to its intended users. It is caused by any event that weakens or eliminates a network's capacity to perform its expected function. Owing to low memory capabilities and limited computation resources, most computing devices in the IoT environment are vulnerable to asset enervation assaults [20]. One of the reasons for a DoS attack is that various industries use similar technologies and potential attackers take advantage of this [21, 22].
- *Malware* In this attack, the attacker deploys malicious software programs to gain unauthorized access to computer systems by exploiting its security vulnerabilities. The incentive behind malware is an extraordinary financial or political reward that accelerates an attacker's motivation to compromise as many network devices they can to accomplish their malicious aims [23, 24].
- *Phishing* This is an unlawful activity which uses social engineering and technology to collect sensitive information from an Internet user. Phishing techniques utilize various methods of communication, such as email, instant messages, pop-up messages or Web pages [25, 26].
- *SQL injection attack* In this attack, an input string is injected through the application to change or manipulate the SQL statement to the attacker's advantage. This attack harms the database in several ways, including unauthorized access and manipulation of the database, and disclosure of sensitive data. This attack is risky as it can cause data loss or misuse of data by groups who are not authorized, and consequently, functionality and confidentiality are destroyed. Further, system-level commands are also executed under this category of attack, resulting in authorized users being unable to access the required information [27, 28].
- *Session hijacking and Man-in-the-Middle attacks* Man-in-the-middle (MITM, also abbreviated in the literature as MIM, MitM, MiM or MITMA) is an attack where an unauthorized third party secretly gains control of the communication channel between multiple endpoints. The MITM attacker can interrupt, manipulate or even replace the target victims' communication traffic. Further, victims are not aware of the intruder, thus believing that the communication channel is safe and protected [29, 30].
- *Cross-site scripting (XSS)* In this type of attack, a malicious attacker tries to run a JavaScript code in the client's browser in order to steal the client's sensitive data. It is a commonly used vulnerability found in recent Web sites [31, 32].

3 Existing Work

Several mapping studies and systematic literature reviews (SLR) exist in the area of the cyber environment, but these studies have not specifically targeted cyber security vulnerabilities. We discuss these studies in the following.

Lun et al. [1] performed a detailed systematic mapping study on cyber-physical system security. The review targeted various domains including network systems, smart grid, information systems and automatic control. According to study results, researchers have mainly targeted smart grid systems and their main focus is on physical-level attacks.

Nguyen et al. [33] performed a systematic mapping study on the use of model-based security engineering to address the security challenges of the cyber-physical system. The paper has three main contributions: It classifies the primary studies based on publication statistics, identifies the security concerns discussed in the selected primary studies and highlights the open issues. According to their study, only a

few security solutions exist regarding the use of model-based security engineering in the cyber-physical system. Further, there are only a few empirical studies on this topic.

Hydara et al. [34] performed a SLR to investigate the state of the art in cross-site scripting (XSS) vulnerabilities in Web applications. According to this study, the researchers found several solutions to address XSS vulnerabilities, but there is still no single solution to mitigate the XSS problem. According to the results of the SLR, there is a need for more research to address XSS removal from source code before deployment.

Muccini et al. [35] conducted a SLR on self-adaptation for the cyber-physical system (CPS). The main focus of their study is to assess the existing approaches used to handle self-adaptation in CPS at the architectural level. According to the study, self-adaptation for CPS is a cross-layer concern, where existing solutions combine various adaptation mechanisms within and across layers. Hence, there is a need for more research in the field of self-adaptation in CPS and the mapping of solutions across different layers.

Mishna et al. [36] also carried out a SLR to identify the state of the art on the existing solutions to prevent and reduce the cyber abuse of youth. The aim of the study is to check the effectiveness of cyber abuse interventions in improving safety knowledge regarding Internet usage and risky online behavior. The results show the effectiveness of cyber abuse intervention in improving safety knowledge; however, it has no significant association with risky online behavior.

Lewis and Lago [37] performed a SLR to understand the state of the art on the existing architectures that support cyber foraging. Cyber foraging is a computing technique in which low-powered devices offload their heavy work on high-powered neighborhood machines. The aim of the study was to categorize the existing architectural solutions related to what, when and where to offload data and computation for mobile devices. The authors identified the elements of existing architectures and codified them in architectural tactics that can help architectural researchers and practitioners extend their design to support cyber foraging.

Rahim et al. [38] performed a SLR to analyze the approaches used to assess cyber security awareness. According to the study findings, many approaches have been proposed in the literature to develop awareness of cyber security. However, there is still a need to combine multiple approaches for better results. Further, there is a need to promote more awareness about cyber security, especially to young people who are the key targets of cyber attacks.

Enoch et al. [39] tried to capture the possible attack scenarios for dynamic networks using Global System for Mobile Communications (GSM). A change in security metric is evaluated based on a change in network parameters. The effectiveness of each metrics was evaluated according to the persistent security challenges. This study helps the researcher and practitioner to determine the most suitable security metrics for their network. However, this study discussed security vulnerabilities in general and did not target any particular cyber security attacks.

Ramaki et al. [40] carried out a systematic mapping study on intrusion alert analysis using the SMS process. In this mapping study, 411 studies were evaluated to answer the research questions. According to the study findings, intrusion alert analysis is a rapidly growing research field. The paper gives a good insight into the current state-of-the-art regarding intrusion alert analysis.

Chockalingam et al. [41] performed a systematic review to evaluate the effectiveness of a Bayesian network model in cyber security. Seventeen Bayesian network models were identified and evaluated in this study. According to the study findings, Bayesian network models are useful for solving the problem of malicious insiders. However, these models are frequently used to address the security issues associated with the information technology environment compared to the industrial control systems. Further, no standard Bayesian network models exist which address all the issues of cyber security.

Alguliyev et al. [42] reviewed the literature on SCADA and smart gird security to highlight the persistent cyber attacks and existing solutions. The important contribution of the paper is a discussion of cyber attack approaches, consequence modeling of these attacks and the detection and design of security architecture.

Franke and Brynielsson [43] conducted a SLR on cyber situational awareness based on 102 primary studies published till 2013. They concluded that some aspects of cyber situational awareness are more mature and widely researched than others. Franke and Brynielsson study focused on cyber situational awareness area, while in our study we focused on identifying the common cyber security threats and vulnerabilities. In addition, our study is a systematic mapping study, while the study of Franke and Brynielsson is a systematic literature review. Moreover, our study includes papers published up to the end of 2018.

From the above discussion, it becomes clear that a large body of research has been conducted in the area of cyber security and cyber awareness. Systematic mapping studies and SLRs have also been conducted. However, the existing mapping studies mainly focus on cyberspace security in general and cyber awareness in particular. No systematic mapping study exists that synthesizes knowledge on the key cyber security vulnerabilities and approaches to mitigate these risks. To bridge the gap, this mapping study is conducted to provide the researchers with an overview of existing cyber security vulnerabilities and their detection and mitigation approaches.

4 Research Methodology

In this study, guidelines for conducting a systematic mapping study were followed [44–46]. The reasons for choosing this method are manifold. It is a systematic and organized way of identifying, evaluating and interpreting all the relevant studies concerning a particular research question, focus area or phenomenon of interest. A systematic mapping study is a well-defined and disciplined way to review and synthesize the empirical evidence concerning a method or technology, find out the missing areas and gaps in the current research and provide researchers or practitioners with the background knowledge to justify new research. A systematic mapping study is different from a conventional literature review as it takes more time and effort, but it provides a deeper understanding of the topic and a strong basis for establishing claims about research questions [47]. A systematic mapping study protocol contains five distinct phases as shown in Fig. 1.

A systematic mapping study protocol has been prepared, which includes the details of all steps that were followed in the current study. A brief description of the major steps is as follows:

1. Formulating research questions.
2. Defining search process and search string.
3. Defining the process of study selection including inclusion and exclusion criteria.
4. Data extraction and mapping the data with defined research questions.
5. Data analysis and result extraction.

This mapping study was undertaken by five researchers. All are academic faculty members. The protocol was developed by one author, and the other authors reviewed it critically to identify the weaknesses. All team members contributed during all the phases of the systematic mapping study. To lessen personal bias and to improve the process of the mapping study, inter-rater reliability tests were executed at the preliminary and final selection phases of this systematic mapping study process. A comprehensive search was conducted to identify the relevant articles published up end of 2018.

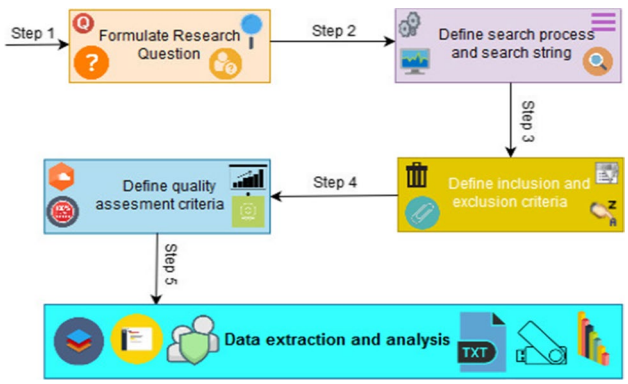

Fig. 1 Phases of a systematic mapping study

4.1 Search Strategy

Before starting the mapping study formally, the string "empirical studies on cyber security" was applied in ScienceDirect. The reason for choosing ScienceDirect is that it is a well-known library consisting of a vast collection of articles from various domains. The purpose of this initial search was two-fold: firstly, to ensure whether there are a sufficient number of empirical studies to undertake a mapping study; and secondly, to identify some primary studies that may be used later for the validation of the search string. The selected studies were exported into the Endnote software [48]. The abstracts of the retrieved papers were studied, and nine empirical studies were chosen as the primary studies, so they could be used to validate our refined string. In this informal search process, many empirical studies were found so it was decided to perform a systematic mapping study and the initial string which was defined for the search process was cyber AND security. When this initial string was applied on the ScienceDirect search engine, the retrieved results did not include all the primary studies. Further, two senior software engineering researchers from academia who have expertise in conducting SLRs were chosen as experts and they were requested to evaluate the search string and provide feedback. Based on these experts' opinions, the initial string was revised, and the main search string was split into two parts. Expert opinion is a way of quickly evaluating and validating information [49]. Below are the two parts of our defined string.

1. Cyber security.
2. Attack/threat/vulnerability.

The synonyms of both these parts of the string were considered to collect all possible relevant studies. This refined string was again validated against the list of primary studies, and the results of the validation were positive, so it was decided to use this in the future for data extraction. The results obtained from the second search string consist of all the selected primary studies, which shows the validity of our search string. The search strategy in this systematic mapping study is based on the following three key steps:

4.1.1 Constructing the Search String

First, the search terms were formed using the keywords identified from the population, the proposed solution, the outcome of relevance and context as under.

Population Set of articles describing the empirical studies on cyber security.
Intervention Solutions proposed in the literature to address cyber security issues.
The outcome of relevance Quantity and type of evidence related to cyber security.
Context Within the domain of cyber security with a focus on empirical studies.

4.1.2 Finding Synonyms of the Derived Search Terms Using Boolean Operators

The identified search terms were validated in the major academic databases. All possible relevant synonyms of the identified terms were found to construct the search string. The following synonyms have possible relevance to the topic:

Cyber security (cyber OR Privacy OR {cyber security} OR {cyber physical} OR {Network security} OR {Internet security} OR {computer security} OR {IT Security} OR {software Security}).

Attack (vulnerability OR {cyber threat} OR {cyber Crime} OR {cyber-attack} OR challenge OR risks OR violence).

4.1.3 Verification of Identified Terms in the Academic Databases

After multiple iterations and revision, the following search string was finalized for this mapping study:

Cyber OR Privacy OR{cyber security} OR {cyber physical} OR {Network security} OR {Internet security} OR {computer security} OR {IT Security} OR {software Security}) AND (vulnerability OR {cyber threat} OR {cyber Crime} OR {cyber-attack} OR challenge OR risks OR violence).

The final search string was used in the following digital libraries (the search string was also tailored according to the search mechanism provided by these libraries):

- ACM Digital Library.
- ScienceDirect.
- IEEE Explore.
- John Wiley Online Library.
- SpringerLink.

The above five databases were selected as they are the popular venues for publishing papers on cyber security. Other researchers have also used these databases in their SLR studies [35, 50, 51].

4.2 Publication Selection

This section details the inclusion and exclusion criteria used for publication selection and also highlights the process used to select relevant publications as per the research questions. The following criteria were set for inclusion:

The review period was almost a decade and includes studies published from 2007 to 2018. This starting date was chosen because most cybercrimes were reported in 2007 and later. However, the search was performed in the start of 2019, so only publications pertaining to end of 2018 were considered in the systematic mapping study.

- Empirical studies with a focus on cyber security vulnerabilities.
- Studies which focus on providing a solution to cyber security vulnerabilities.

The following exclusion criteria were used:

- Studies that do not provide detailed information on how to detect cyber security vulnerabilities.
- Duplicated studies, only the most recent one was chosen.
- Studies where the findings are not evaluated empirically.
- Studies only available as abstracts or PowerPoint presentations.
- Papers with no focus on the cyber security domain.
- Papers presenting only guidelines, recommendations or a description of cyber security.
- Introductory papers for workshops, special issues and books.
- Book chapters.
- Papers not written in English.
- Papers that are not accessible.

The process of selecting publications was automatic and twofold: Firstly, the initial selection from the search result was performed according to the selection criteria by screening the title and abstract of the publications; secondly, the papers selected in the initial phase were read completely in order to shortlist publications for final selection, based on the defined inclusion criteria.

4.3 Data Extraction

Based on our search string and the identified security vulnerabilities, we developed a data extraction form (available in "Appendix A") to extract data from the retrieved publications. This data extraction form consists of a mix of open-ended and closed-ended questions. A pilot study involving two software engineering experts was conducted to evaluate the data extraction form. The data extraction form was finalized based on the feedback from the pilot

study. The final version of the data extraction form consists of three parts: Section one collects information about the selected paper, such as paper title, list of authors, year of publication, country of publication and reference type of papers; section two includes information on the quality assessment of the paper (the results of the quality assessment are not included in this paper, as based on the mapping study guidelines, quality assessment is not essential in mapping studies [45]); and section three presents the data that were extracted from the selected publications.

5 Results

5.1 Categorization of Cyber Security Vulnerabilities

This section presents the results of the systematic mapping study. The total number of studies selected in the initial search phase was 162. Based on the inclusion and exclusion criteria, 78 articles were selected in the final iteration (as shown in "Appendix B"). The details of each iteration are shown in Table 1. These selected articles were studied and analyzed in detail to address the research questions.

Table 2 shows the main categories of cyber security threats and vulnerabilities (RQ1) identified from the systematic mapping study. Column 1 of Table 2 lists the cyber security vulnerabilities that were identified in this mapping study. Column 2 of Table 2 shows the frequency of occurrence for each vulnerability as it appeared in the selected studies, while Column 3 of Table 2 shows the percentage of occurrence for these vulnerabilities. Key vulnerabilities identified in our mapping study include malware, phishing, SQL injection attack, cross-site scripting (XSS), denial-of-service (DoS), session hijacking, man-in-the-middle attacks and credential reuse. Denial-of-service is the most addressed vulnerability in the systematic mapping study (37%). The second most discussed vulnerability in the literature is malware (21%) followed by phishing. The details of remaining vulnerabilities are shown in Table 2.

Table 1 Study selection

Source	Retrieved	Initial selection	Final selection
IEEE	3897	51	34
ACM	323	31	10
ScienceDirect	1308	50	22
SpringerLink	1445	14	8
Wiley	91	16	4
Total	7064	162	78

5.2 Analysis Based on the Venue of Publication and Source Type

The second aspect of this study focuses on the venue of the selected publication and its source type, which will help to address research question 2 (RQ2) (i.e., the key venues of publication that contribute to the area of cyber security).

For venue and source type analysis, we considered five libraries as the key venues for publications as shown in Tables 3 and 4. The selected studies from these libraries were published in three main publication types, namely conferences, journals and workshops. Table 3 shows the distribution of the selected studies with respect to the publication type. The number of studies published in conferences and journals is almost the same, and only three studies were published in workshops. The percentage of studies published in conferences, journals and workshops was 48%, 48% and 4%, respectively. The results of Table 3 show that IEEE and ACM libraries contain more conference papers than journal papers. From the publications extracted from the IEEE library, only three were published in IEEE journals and the rest all were published in IEEE conferences. For the ACM library, all the extracted papers were published in conferences and workshops (67% and 33%, respectively) and no journal paper was extracted in the domain of the area under study. However, if we analyze the statistics of the three other

Table 2 Cyber security threat and vulnerability categorization

Threat and vulnerability	Frequency	Percentage (%)
Credential reuse	1	1
Cross-site scripting (XSS)	1	1
Denial-of-service (DoS)	29	37
Malware	16	21
Phishing	7	9
Session hijacking and man-in-the-middle attacks	2	3
SQL injection attack	3	4
Other	19	24

Table 3 Distribution of studies based on publication venue

	Journal papers	Conference papers	Workshop papers	Total
IEEE	5	29	0	34
ACM	0	7	3	10
ScienceDirect	22	0	0	22
Springer	7	1	0	8
Wiley	4	0	0	4
Total	38	37	3	78

Table 4 Publication venues with more than one selected study

Venue	Library	Type	Frequency
Computers & Security	ScienceDirect	Journal	5
Information Sciences	ScienceDirect	Journal	3
Annual Cyber Security and Information Intelligence Research Workshop	ACM	Workshop	2
Annual Conference on cyber and information security research	ACM	Conference	2
Winter Simulation Conference	ACM	Conferee	2
International Conference on Advanced Communication Technology	IEEE	Conference	2
International Conference on Recent Trends in Information Technology	IEEE	Conference	2
IEEE Access	IEEE	Journal	2
Procedia Technology	ScienceDirect	Journal	2
Future Generation Computer Systems	ScienceDirect	Journal	2
Computer Networks	ScienceDirect	Journal	2
Security and Communication Networks	Wiley Online	Journal	2
International Journal of Information Security	Springer	Journal	2

libraries, namely ScienceDirect, Wiley Online and Springer, the extracted publications relevant to the current study domain were all published in journals. From these three libraries, the frequency of publication in ScienceDirect was the highest with 30% of the papers in the pool. Springer and Wiley were second and third in the pool with a frequency of 8.69% and 4%, respectively.

Table 4 shows the most common venues for the primary studies with a frequency of 2 or more. The results indicate that most of the articles are published in journals. Journal of Computer & Security by ScienceDirect has the highest frequency (5 out of 78) articles, while Information Sciences by ScienceDirect is the second with 3 out of 78 articles.

5.3 Demographic Analysis

To identify and rank the most active countries in the area of research on cyber security, the author's affiliation was used. The rationale for this ranking is to answer research question 3 (RQ3) and to determine from which countries researchers who publish in the area of cyber security come. The affiliation information provided in each paper was used, even if the author had moved to another country. If a paper was written by several authors, the country of the first author was chosen. The results are shown in Table 4 and Fig. 2.

Column 1 of Table 5 lists the authors' affiliation country as appeared in selected studies. Column 2 of Table 5 shows the frequency of authors' affiliation belonging to the country mentioned in Colum 1, and Column 3 of Table 5 shows the percentage value of Column 2. The results (for RQ3) indicate that the highest number of research articles in the area of cyber security is published by American and Indian researchers who contributed 40% (16 out of 78 each) of the selected articles. Authors from China (with 14 out of 78) were second in the ranking, and Australia and

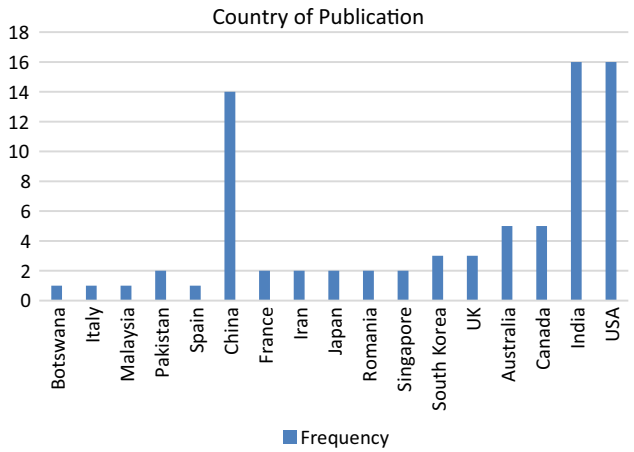

Fig. 2 Country of publication

Canada, both ranked third, contributed 6% each. The rest of the articles were published in various countries with a frequency between 2 and 4 articles.

This illustrates the need for more research in the area of cyber security from various countries to understand the effect of sociocultural differences.

Our research further identified that the more active researchers are from China with multiple publications related to the cyber security and vulnerabilities. However, the frequency shows that the active researchers mostly extend their work from conferences to the journal venues with further insight.

The selected studies were also categorized with respect to the year of publication to identify the current research trends in the area of cyber security. Figure 3 shows the distribution of studies by year. The results of Fig. 3 show that there is a significant increase in research in the area of

Table 5 Country frequency analysis

Country	Frequency	Percentage (%)
Botswana	1	1
Italy	1	1
Malaysia	1	1
Pakistan	2	3
Spain	1	1
China	14	18
France	2	3
Iran	2	3
Japan	2	3
Romania	2	3
Singapore	2	3
South Korea	3	4
UK	3	4
Australia	5	6
Canada	5	6
India	16	20
USA	16	20

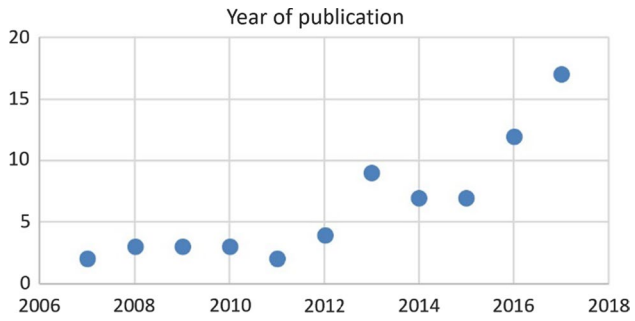

Fig. 3 Frequency of publications

Table 6 Characteristics of validation data

Option	Frequency	Percentage (%)
Academia	7	9
Industrial	23	29
Government	2	3
Mixed	46	59

cyber security to support cyber applications and to address the key security threats faced by these applications.

Data characteristics were also highlighted in order to understand which kind of data is mostly used to validate the proposed approach. Table 6 shows the characteristics of the data used to validate the proposed strategies. Most researchers used mixed data for validation which includes the mix of academia, industry, and the government with 59% of the articles in the pool. Industrial data were used by 29% of the researchers for the validation of their proposed approach, and the percentage of academia and government data was 9% and 3%, respectively.

Table 7 Study strategy used

Study types	Frequency	Percentage (%)
Case study	4	5
Experiment	46	59
Simulation	28	36

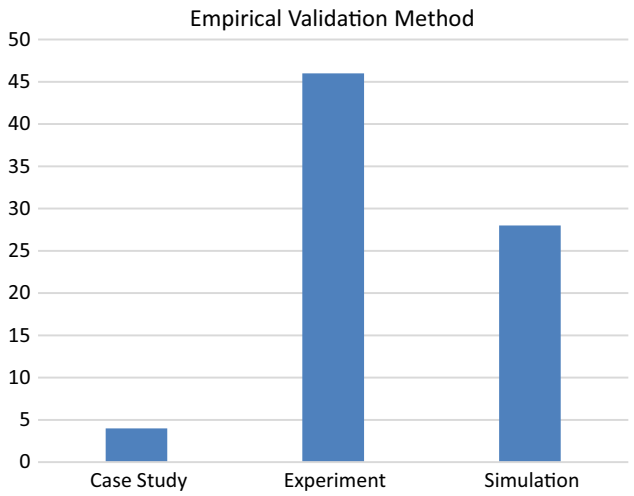

Fig. 4 Division of studies based on the used empirical method

As the focus of the study was on empirical studies only, only those studies which performed an empirical validation of the results were selected. Empirical studies were divided into three commonly used research methodologies, namely experiment, case study and simulation. The reason for selecting simulation was that it was mostly used in the selected studies for validation. The results of Table 7 show the distribution of studies with respect to the research methodology.

The results of Table 7 and Fig. 4 show that experimentation was the most commonly used method of validation with 59% or 46 of 78 of the articles in the pool using this method. The second most commonly used method of empirical validation was simulation with 36% or 28 out of 78 articles in the pool using this method, and the least used method of validation was a case study with 5% or 4 of 78 studies using this method.

5.4 Victim Analysis

The focus of the fourth research question is to identify the key victims of cyber security vulnerabilities which will help to answer RQ4, i.e., who are the key victims of these security vulnerabilities? The victims were divided into two broad categories, namely organizations and individuals, and the results are shown in Table 8. Some of the vulnerabilities affected both individuals and organizations together in the selected studies; therefore, the results are overlapping for these vulnerabilities.

5.5 Target Applications

The focus of the fifth research question (RQ5) was to pinpoint the applications that were key targets of cybercrimes in the selected studies. Although the data extracted from the selected studies regarding the targeted victims' organizations and applications were heterogeneous, we organized it into the following three categories.

5.5.1 Infrastructure That Was Targeted

According to the extracted data, the following infrastructure was a key target of cybercrimes.

- Social media.
- Smart grid.
- Mobile application.
- Industrial control systems.
- Network.
- Distributed system.
- Cloud application.
- Multiple VLAN.
- Vehicular ad hoc network (VANET).
- Information systems and Internet of things.
- Client–server application.
- Internet data.
- Collaborative working nodes interconnected through MPLS-VPN cloud.
- Enterprise network gateway.
- Cyber-physical systems.
- Application servers.
- Peer-to-peer (P2P) systems.

Table 8 Victim frequency

Victim	Response %age	Responses (%)
Individual	9	11
Organization	74	95

5.5.2 Target Applications

The following applications were the targets of cyber attacks according to our data.

- Energy-efficient neuromorphic hardware platform.
- Thunderbird 24. 8. 0.
- Libav 10.1
- Banking.
- Web application.
- Xen 4.4.0
- E-commerce.
- Hackmageddon database.

Organizations/agencies that were targeted

The following organizations were the targets of cyber attacks, according to our studies.

- DARPA.
- AhnLab Security Emergency Centre.
- Aircraft attitude sensors.

.

5.6 Attack Mitigation Techniques

The focus of our last research question (RQ6) was to identify the mitigation techniques used by various victim industries from cyber threats. Table 9 shows the frequency and percentage of the mitigation techniques that were used to protect the cyber environment from cyber security threats.

According to our extracted data, some organizations used more than one technique to protect their cyber environment; for example, a firewall and IDs were used by many cyber organizations along with other security mitigation techniques. The total frequency is more than 78 (the number of selected studies) due to the use of multiple security mitigation techniques. Further, the papers that targeted only phishing attacks mostly used antiphishing techniques to prevent the systems from a phishing attack.

Traffic analysis was also used in many papers for security attack detection. According to our mapping study, intrusion detection system and firewalls are most commonly used techniques for cyber attack mitigation with the frequency of occurrence (17 out of 78 and 13 out of 78). The second most commonly used method of cyber attack mitigation was traffic analysis with the frequency of occurrence as 7 out of 78. The third commonly used techniques of cyber attack mitigation are antiphishing and signature-based techniques with the frequency of occurrence as 6 out of 78 each. Remaining mitigation techniques and their frequency are mentioned in Table 9. Some articles mentioned more than one technique for mitigating cyber security attack; therefore,

Table 9 Attack mitigation techniques

Mitigation techniques	Frequency	Percentage (%)
Algorithm weakly supervised	5	6
VulPecker tool	1	1
Iterative approach of critical component identification	3	4
Intrusion detection systems (IDS)	17	22
Content-based spam filtering technique	3	4
MP shield	1	1
Command and control (C&C) servers	1	1
Antiphishing techniques	6	8
Firewalls	13	17
Analyzing traffic anomaly features	7	9
Anti-malware software	5	6
Automated dynamic analysis techniques	1	1
Modifying the way of accepting incoming requests	1	1
Conventional false data detection (FDD) approaches	4	5
Signature-based detection and anomaly-based detection	6	8
Darknet	2	3
Sandboxing	3	4
Not mentioned	9	12

the total frequency is more than 78. However, nine of the extracted studies did not mention the name of the mitigation technique used.

6 Discussion

In the following, we discuss our results in detail and map them according to the posed research questions to better understand the ability of the readers.

RQ1 What are the common cyber security vulnerabilities?

To answer RQ1, all the retrieved papers were thoroughly studied, and the key vulnerabilities discussed in these papers were extracted. Table 2 lists these common security vulnerabilities. Table 2 also shows the frequency with which the cyber security vulnerability has been investigated. The results of the current mapping study indicate that denial-of-service has been investigated the most frequently as many researchers have addressed this issue, as shown in Table 2. The security vulnerabilities investigated second and third most frequently are malware and phishing detection and mitigation, respectively. Only a few studies have targeted other security vulnerabilities, which shows the need for more research to address these vulnerabilities. Further, there is a need to accommodate exposure avoidance from these three common vulnerabilities during cyberspace creation. There is also a need to develop some strategies to make people aware of these vulnerabilities.

RQ2 What are the key venues for publication on cyber security? Which journals include papers on cyber security threats and vulnerabilities?

To identify the key venues for publication, five key libraries were used for data extraction, namely IEEE, ACM, ScienceDirect, Wiley Online and Springer. The extracted results from these libraries were divided into three categories, namely journals, conferences and workshops, as shown in Table 3. The results of Table 3 show that more research in the area under study was published in conferences and journals and only a few articles were published in workshops. Further, the results of Table 3 show that publications extracted from IEEE and ACM libraries are mainly conference papers, only 5 out of 34 were journal papers in the IEEE library and 3 out of 10 were workshop papers in the ACM digital library. On the other hand, all the publications retrieved from the remaining three libraries (ScienceDirect, Wiley Online and Springer) were mostly journal papers except one paper that was published in Springer conference. This shows that IEEE and ACM are the key venues for conference publications in the area under study, while ScienceDirect, Wiley Online and Springer are key venues for journal publications in the area of study. Further, to identify the key journals and conferences which publish papers on cyber security, we listed the journals and conferences which published more than one papers from the list of retrieved studies in Table 4. The results of Table 4 show that two journals of ScienceDirect, namely Computers & Security and Information Sciences,

have published more papers in the current domain with the frequency of 5 and 3, respectively.

RQ3 Researchers from which country are more active in cyber security?

During the demographic analysis, some interesting findings surfaced are as follows: USA and India are the countries which most frequently publish research in the area of cyber security vulnerability detection and mitigation, as shown in Table 5 and Fig. 2; the second observation is that the number of publications in the area of cyber security is increasing which shows the importance of research in the area of cyber security, as shown in Fig. 3.

With respect to active authors from the primary studies, we noticed that most authors published one paper; however, only six researchers, namely Anil Siani, Manoj Singh Gaur, Vijay Laxmi, Lejun Fan, Yuanzhuo Wang and Xueqi Cheng, published two or more articles.

RQ4 Who are the key victims of these security vulnerabilities?

The victims of security vulnerabilities were divided into two categories, namely individuals and organizations. The results in Table 8 show that organizations are more vulnerable to cyber threats compared to an individual. However, there are some vulnerabilities that target both individuals and organizations. This is shown by the overlapping values in Table 8.

RQ5 Which applications are the targets of cybercrimes in the selected studies?

The data obtained from the selected studies to answer research question 5 were heterogeneous and therefore were not able to be classified into specific groups. Further, most of the papers did not mention the name of the application that was the target of cybercrime. However, we divided the extracted data into the following three classifications: Firstly, we highlighted the infrastructures that were the key targets of cybercrime; secondly, we identified the applications that were targets of cybercrime; and lastly, we identified the organization/agencies that were targets of cybercrime. The results of RQ5 show that the smart grid, the Internet of things, the cyberspace and the cloud environment are the key targets of cybercrime.

RQ6 What are the common cyber security mitigation techniques discussed in the literature?

According to the data obtained from the selected studies, different organizations use different techniques to protect their cyberspace from security attacks. However, it was observed that the intrusion detection system and firewalls are the most commonly used techniques with a frequency of 17 out of 78 and 13 out of 78, respectively. Further, traffic analysis and antiphising are the third and fourth most widely used cyber attack prevention techniques.

6.1 Research and Practical Implications

This mapping study has both research and practical implications. We categorized the key security vulnerabilities and identified their frequency of occurrence in the selected studies. This will help researchers know which security vulnerabilities need more attention. In the future, researchers can target those security issues which need more research. Further, we categorized the studies with respect to country of publication. This will help researchers analyze the sociocultural impact on cyber security.

It is also anticipated that the key vulnerabilities identified and their frequency of occurrence will help practitioners develop strategies to make individuals and organization aware of these vulnerabilities and their mitigation techniques. It is a common practice to highlight frequently occurring cyber attacks, as not all attacks and vulnerabilities are equally important. It will also guide investment decisions in key security areas. Thus, this systematic mapping study and the empirical results presented in this paper will help practitioners decide where to invest while developing tools and strategies to protect the cyber environment.

Cyber organizations need to provide their clients with guidelines and training in relation to critical vulnerabilities and ways to protect themselves. Organizations should develop mechanisms to establish suitable privacy policies to protect the important assets of individuals as well as organizations. Organizations should also select attack detection strategies and tools carefully so that the client can use them easily. Organizations also need to make sure that employees do not disclose their personal information to any third party, nor should they reply to junk emails or messages.

6.2 Threats to Validity

Threats to validity for the mapping study are as follows:

Publication bias There is a possibility that some relevant studies that are published in other databases which are not included in this study have been missed. However, we believe that the selected databases cover the most relevant published literature on cyber security domain.

Missing synonyms Another possible threat might be the absence of some synonyms in the search string. Despite the fact that we have tried to cover all the synonyms, there is still a possibility that we missed or overlooked some work.

7 Conclusion

This paper presents the results of a systematic mapping study that was undertaken to identify and analyze the common cyber security vulnerabilities. A summary of the important results follows:

RQ1 A total of 134 articles were selected using a defined search string for this systematic mapping study. After all the papers had been screened, 78 articles that met our inclusion criteria were selected. Each publication was analyzed in detail, and seven key security vulnerabilities that were the most discussed in the selected publications were extracted. Based on our analysis, denial-of-service and malware were the most cited security vulnerabilities, with a frequency of 37% and 21%, respectively. The approaches most used in the detection of these vulnerabilities as detailed in the selected research include intrusion detection systems, machine learning techniques and algorithm-based solutions.

RQ2 With respect to the publication venue, we only targeted five key digital libraries, those being IEEE, ACM, ScienceDirect, Springer and Wiley Online. According to our findings, IEEE and ScienceDirect are the key publication venues in the area of cyber security. According to our findings, journals are the key publication venue representing 38 out of 78 studies; the second key venue of publication is conference representing 37 out of 78 studies, while publications in workshops only contribute 3 out of 78 studies.

RQ3 The focus of the third research question was to identify the country from which the researchers who contributed more in the area of cyber security came. To obtain an overview of the key researchers in this area, we counted the number of papers with respect to the country of publication. Our findings show that USA and India are more active in this area of research compared to other countries.

RQ4 Based on our research, organizations are more vulnerable to cyber attacks compared to individuals. However, there are some attacks that target both individuals as well as organizations. Individuals are the main target of phishing attacks, where they receive junk emails and instant messages which aim to disclose their personal credentials. There is a need for cyber awareness to provide individuals with knowledge of cyber attacks and to warn them about the disclosure of their personal information.

RQ5 Based on our analysis, the smart grid, the Internet of things, the cyberspace and the cloud environment are the key targets of cybercrime. There is a need to implement proper safety and security measures throughout the planning, design, implementation, deployment and operational cycles of these cyber environments.

RQ6 Based on our analysis, no standard measure/mitigation techniques exist that can be used by all cyber organizations to protect their cyber environments from potential cyber threats. However, organizations need to be aware of the existing vulnerability mitigation techniques. There is also a need to provide proper training to employees regarding security.

It is expected that these research findings will support cyber organizations to better understand the existing cyber security vulnerabilities and their mitigation strategies. Further, the findings provide a strong basis for researchers and practitioners to address the aforementioned cyber security issues in detail while developing new cyber security approaches.

8 Open Issues

Cyber security is a rapidly growing research area due to its wide use in almost every field of life, but it also imposes high demands on the safety and security of cyber systems from insider and outsider attacks. Fundamental research is required in this field to effectively address the key security vulnerabilities. In this paper, we highlighted important and frequently occurring cyber security vulnerabilities so that researchers can find gaps in the existing literature and new directions for research. Some future research directions are as follows:

Table 2 lists and categorizes the common cyber security vulnerabilities along with their frequency of occurrence. According to this, denial-of-service and malware are frequently occurring security vulnerabilities. There is a need to develop methods to secure the cyber environment from these vulnerabilities.

Table 8 shows the percentage of individuals and organizations who were targeted. Although the percentage of organizations suffering from security issues is very high compared to individuals, there is still a need to develop a reliable information security mechanism to keep personal information confidential. There is a need to develop a secure and transparent mechanism to save organizations from internal and external security attacks. Section 5.5 lists the infrastructure, applications and organizations that are the key targets of cybercrime. This shows the need to propose mitigation strategies to protect these environments from cyber attacks.

Acknowledgements The authors would like to acknowledge the support provided by the Deanship of Scientific Research via the project number IN161024 at King Fahd University of Petroleum and Minerals,

Saudi Arabia. In addition, we are grateful to the participants who evaluated the proposed model and recommended improvements.

Appendix A: Data Extraction Form

Section 1: Paper information	
Paper title:	
Authors:	Year of publication:
Reference type: Journal/Conference	Publisher:
Country:	

Section 2: Quality assessment	
The findings and results of study are clearly stated?	Yes No
The findings of the study are evaluated empirically?	Yes No
The study has been published in a relevant journal or conference?	Very relevant Relevant Not relevant
The study has been cited by other authors?	Yes Partially No

Section 3: Data extraction	
Questions	Possible answers
Which application is targeted for cybercrime in the given study?	Application name
Which method is used to protect the application for cyber attack?	Method name
Which cyber connection is used for committing cybercrime?	Connection name
Who are the victims of cybercrimes in the given study?	Individual Organization
Which cyber security vulnerability is discussed in the study?	Malware Phishing SQL injection attack Cross-site scripting (XSS) Denial-of-service (DoS) Session hijacking and man-in-the-middle attacks Credential reuse Others
What is the severity of discussed cyber security vulnerability?	Critical High Medium Low
Which technique is used in the study for detecting cyber threats?	Technique name
What kind of data is used for validation? Data characteristics	Academia Industrial Government Mixed
Which empirical validation methods are used in the proposed approach?	Case study Experiment Simulation Others

Appendix B: Finally Selected Papers

1. Khandpur, Rupinder Paul, et al. "Crowdsourcing cybersecurity: Cyber attack detection using social media." Proceedings of the 2017 ACM on Conference on Information and Knowledge Management. ACM, 2017.
2. Li, Zhen, Deqing Zou, Shouhuai Xu, Hai Jin, Hanchao Qi, and Jie Hu. "VulPecker: an automated vulnerability detection system based on code similarity analysis." In *Proceedings of the 32nd Annual Conference on Computer Security Applications*, pp. 201–213. ACM, 2016.
3. Cheng, Maggie, Mariesa Crow, and Robert F. Erbacher. "Vulnerability analysis of a smart grid with monitoring and control system." *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*. ACM, 2013.
4. Zanero, Stefano. "Ulisse, a network intrusion detection system." In *Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead*, p. 20. ACM, 2008.
5. Werner, Gordon, Shanchieh Yang, and Katie McConky. "Time series forecasting of cyber attack intensity." In *Proceedings of the 12th Annual Conference on cyber and information security research*, p. 18. ACM, 2017.
6. Masi, Denise, Martin J. Fischer, John F. Shortle, and Chun-Hung Chen. "Simulating network cyber attacks using splitting techniques. ACM" In *Proceedings of the Winter Simulation Conference*, pp. 3217–3228. Winter Simulation Conference, 2011.
7. Okutan, Ahmet, Shanchieh Jay Yang, and Katie McConky. "Predicting cyber attacks with bayesian networks using unconventional signals." In *Proceedings of the 12th Annual Conference on Cyber and Information Security Research*, p. 13. ACM, 2017.
8. Farraj, Abdallah, Eman Hammad, and Deepa Kundur. "Impact of Cyber Attacks on Data Integrity in Transient Stability Control." In *Proceedings of the 2nd*

Workshop on Cyber-Physical Security and Resilience in Smart Grids, pp. 29–34. ACM, 2017.

9. Kuhl, Michael E., Jason Kistner, Kevin Costantini, and Moises Sudit. "Cyber attack modeling and simulation for network security analysis." In *Proceedings of the 39th Conference on Winter Simulation: 40 years! The best is yet to come*, pp. 1180–1188. ACM Press, 2007.
10. Gudo, Munyaradzi, and Keshnee Padayachee. "SpotMal: A hybrid malware detection framework with privacy protection for BYOD." In *Proceedings of the 2015 Annual Research Conference on South African Institute of Computer Scientists and Information Technologists*, p. 18. ACM, 2015.
11. Kim, Ikkyun, Daewon Kim, Byunggoo Kim, Yangseo Choi, Seongyong Yoon, Jintae Oh, and Jongsoo Jang. "A case study of unknown attack detection against Zero-day worm in the honeynet environment." In *2009 11th International Conference on Advanced Communication Technology*, vol. 3, pp. 1715–1720. IEEE, 2009.
12. Ahmadloo, Fatemeh, and Farzad Rajaei Salmasi. "A cyber-attack on communication link in distributed systems and detection scheme based on H-infinity filtering." In *2017 IEEE International Conference on Industrial Technology (ICIT)*, pp. 698–703. IEEE, 2017.
13. Aishwarya, R., and S. Malliga. "Intrusion detection system-An efficient way to thwart against Dos/DDos attack in the cloud environment." In *2014 International Conference on Recent Trends in Information Technology*, pp. 1–6. IEEE, 2014.
14. Al-Dabbagh, Ahmad W., Yuzhe Li, and Tongwen Chen. "An intrusion detection system for cyber attacks in wireless networked control systems." *IEEE Transactions on Circuits and Systems II: Express Briefs* 65, no. 8 (2017): 1049–1053.
15. Alom, Md Zahangir, and Tarek M. Taha. "Network intrusion detection for cyber security on neuromorphic computing system." In *2017 International Joint Conference on Neural Networks (IJCNN)*, pp. 3830–3837. IEEE, 2017.
16. Aparicio-Navarro, Francisco J., Konstantinos G. Kyriakopoulos, Yu Gong, David J. Parish, and Jonathon A. Chambers. "Using pattern-of-life as contextual information for anomaly-based intrusion detection systems." *IEEE Access* 5 (2017): 22177–22193.
17. Bhadre, Parvati, and Deepali Gothawal. "Detection and blocking of spammers using SPOT detection algorithm." In *2014 First International Conference on Networks & Soft Computing (ICNSC2014)*, pp. 97–101. IEEE, 2014.
18. Bottazzi, Giovanni, Emiliano Casalicchio, Davide Cingolani, Fabio Marturana, and Marco Piu. "MP-Shield: a framework for phishing detection in mobile devices." In *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, pp. 1977–1983. IEEE, 2015.
19. Chen, Chia-Mei, Han-Wei Hsiao, Peng-Yu Yang, and Ya-Hui Ou. "Defending malicious attacks in cyber physical systems." In *2013 IEEE 1st International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA)*, pp. 13–18. IEEE, 2013.
20. Chen, Chia-Mei, Ya-Hui Ou, and Yu-Chou Tsai. "Web botnet detection based on flow information." In *2010 International Computer Symposium (ICS2010)*, pp. 381–384. IEEE, 2010.
21. Chonka, Ashley, and Jemal Abawajy. "Detecting and mitigating HX-DoS attacks against cloud web services." In *2012 15th International Conference on Network-Based Information Systems*, pp. 429–434. IEEE, 2012.
22. Devi, BS Kiruthika, G. Preetha, G. Selvaram, and S. Mercy Shalinie. "An impact analysis: Real time DDoS attack detection and mitigation using machine learning." In *2014 International Conference on Recent Trends in Information Technology*, pp. 1–7. IEEE, 2014.
23. Eslahi, Meisam, Habibah Hashim, and Nooritawati Md Tahir. "An efficient false alarm reduction approach in HTTP-based botnet detection." In *2013 IEEE Symposium on Computers & Informatics (ISCI)*, pp. 201–205. IEEE, 2013.
24. Gantsou, Dhavy. "On the use of security analytics for attack detection in vehicular ad hoc networks." In *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pp. 1–6. IEEE, 2015.
25. Hesar, Amin Danandeh, and Mahmoud Ahmadian Attari. "Simulating and analysis of cyber attacks on a BLPC network." In *2014 Smart Grid Conference (SGC)*, pp. 1–6. IEEE, 2014.
26. Hong, Junho, Chen-Ching Liu, and Manimaran Govindarasu. "Integrated anomaly detection for cyber security of the substations." *IEEE Transactions on Smart Grid* 5, no. 4 (2014): 1643–1653.
27. Hu, Xin, Jiyong Jang, Marc Ph Stoecklin, Ting Wang, Douglas L. Schales, Dhilung Kirat, and Josyula R. Rao. "BAYWATCH: robust beaconing detection to identify infected hosts in large-scale enterprise networks." In *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 479–490. IEEE, 2016.
28. Ichise, Hikaru, Yong Jin, and Katsuyoshi Iida. "Analysis of via-resolver DNS TXT queries and detection possibility of botnet communications." In *2015 IEEE Pacific Rim Conference on Communications, Comput-*

ers and Signal Processing (PACRIM), pp. 216–221. IEEE, 2015.

29. Indre, Ionut, and Camelia Lemnaru. "Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things." In *2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP)*, pp. 175–182. IEEE, 2016.
30. Jakaria, A. H. M., Wei Yang, Bahman Rashidi, Carol Fung, and M. Ashiqur Rahman. "Vfence: A defense against distributed denial of service attacks using network function virtualization." In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, vol. 2, pp. 431–436. IEEE, 2016.
31. Jin, Guang, Fei Zhang, Yuan Li, Honghao Zhang, and Jiangbo Qian. "A Hash-based Path Identification Scheme for DDoS Attacks Defense." In *2009 Ninth IEEE International Conference on Computer and Information Technology*, vol. 2, pp. 219–224. IEEE, 2009.
32. Jing, Tao, Jun Li, and Rong Xing. "Research on malicious links detection system based on script text analysis." In *2012 14th International Conference on Advanced Communication Technology (ICACT)*, pp. 439–442. IEEE, 2012.
33. Khan, Mohiuddin Ali, Sateesh Kumar Pradhan, and Huda Fatima. "Applying data mining techniques in cyber crimes." In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, pp. 213–216. IEEE, 2017.
34. Khan, Muhammad Salman, Ken Ferens, and Witold Kinsner. "A chaotic measure for cognitive machine classification of distributed denial of service attacks." In *2014 IEEE 13th International Conference on Cognitive Informatics and Cognitive Computing*, pp. 100–108. IEEE, 2014.
35. Kong, Xinling, Yonghong Chen, Hui Tian, Tian Wang, Yiqiao Cai, and Xin Chen. "A novel botnet detection method based on preprocessing data packet by graph structure clustering." In *2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 42–45. IEEE, 2016.
36. Misra, Sudip, P. Venkata Krishna, Harshit Agarwal, Antriksh Saxena, and Mohammad S. Obaidat. "A learning automata based solution for preventing distributed denial of service in internet of things." In *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, pp. 114–122. IEEE, 2011.
37. Sanchez, Fernando, and Zhenhai Duan. "A sender-centric approach to detecting phishing emails." In *2012 International Conference on Cyber Security*, pp. 32–39. IEEE, 2012.
38. Shitharth, S., and D. Prince Winston. "A novel IDS technique to detect DDoS and sniffers in smart grid." In *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, pp. 1–6. IEEE, 2016.
39. Sun, Jia-Hao, Tzung-Han Jeng, Chien-Chih Chen, Hsiu-Chuan Huang, and Kuo-Sen Chou. "MD-Miner: Behavior-Based Tracking of Network Traffic for Malware-Control Domain Detection." In *2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService)*, pp. 96–105. IEEE, 2017.
40. Velauthapillai, Thaneswaran, Aaron Harwood, and Shanika Karunasekera. "Global detection of flooding-based DDoS attacks using a cooperative overlay network." In *2010 Fourth International Conference on Network and System Security*, pp. 357–364. IEEE, 2010.
41. Sun, Cong, Jiao Liu, Xinpeng Xu, and Jianfeng Ma. "A privacy-preserving mutual authentication resisting DoS attacks in VANETs." *IEEE Access* 5 (2017): 24012–24022.
42. Fan, Lejun, Yuanzhuo Wang, Xueqi Cheng, and Shuyuan Jin. "Privacy Theft Malware Detection with Privacy Petri Net." In *2012 13th International Conference on Parallel and Distributed Computing, Applications and Technologies*, pp. 195–200. IEEE, 2012.
43. Cui, Helei, Yajin Zhou, Cong Wang, Qi Li, and Kui Ren. "Towards Privacy-Preserving Malware Detection Systems for Android." In *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*, pp. 545–552. IEEE, 2018.
44. Xu, Lei, Chunxiao Jiang, Nengqiang He, Zhu Han, and Abderrahim Benslimane. "Trust-based collaborative privacy management in online social networks." *IEEE Transactions on Information Forensics and Security* 14, no. 1 (2018): 48–60.
45. Shitharth, S., and D. Prince Winston. "A comparative analysis between two countermeasure techniques to detect DDoS with sniffers in a SCADA network." *Procedia Technology* 21 (2015): 179–186. ScienceDirect.
46. Spyridopoulos, Theodoros, G. Karanikas, Theodore Tryfonas, and Georgios Oikonomou. "A game theoretic defence framework against DoS/DDoS cyber attacks." *Computers & Security* 38 (2013): 39–50. ScienceDirect.
47. Shon, Taeshik, and Jongsub Moon. "A hybrid machine learning approach to network anomaly detection." *Information Sciences* 177, no. 18 (2007): 3799–3821. ScienceDirect.
48. Wang, Fei, Hailong Wang, Xiaofeng Wang, and Jinshu Su. "A new multistage approach to detect subtle DDoS

attacks." *Mathematical and Computer Modelling* 55, no. 1–2 (2012): 198–213. ScienceDirect.
49. Varshney, Gaurav, Manoj Misra, and Pradeep K. Atrey. "A phish detector using lightweight search features." *Computers & Security* 62 (2016): 213–228. ScienceDirect.
50. Liu, Ting, Yanan Sun, Yang Liu, Yuhong Gui, Yucheng Zhao, Dai Wang, and Chao Shen. "Abnormal traffic-indexed state estimation: A cyber–physical fusion approach for smart grid attack detection." *Future Generation Computer Systems* 49 (2015): 94–103. ScienceDirect.
51. Qiu, Yue, Maode Ma, and Shuo Chen. "An anonymous authentication scheme for multi-domain machine-to-machine communication in cyber-physical systems." *Computer Networks* 129 (2017): 306–318. ScienceDirect.
52. Kumara, Ajay, and C. D. Jaidhar. "Automated multi-level malware detection system based on reconstructed semantic view of executables using machine learning techniques at VMM." *Future Generation Computer Systems* 79 (2018): 431–446. ScienceDirect.
53. Zhao, David, Issa Traore, Bassam Sayed, Wei Lu, Sherif Saad, Ali Ghorbani, and Dan Garant. "Botnet detection based on traffic behavior analysis and flow intervals." *Computers & Security* 39 (2013): 2–16. ScienceDirect.
54. Noor, Muzzamil, Haider Abbas, and Waleed Bin Shahid. "Countering cyber threats for industrial applications: An automated approach for malware evasion detection and analysis." *Journal of Network and Computer Applications* 103 (2018): 249–261. ScienceDirect.
55. Huda, Shamsul, Suruz Miah, Mohammad Mehedi Hassan, Rafiqul Islam, John Yearwood, Majed Alrubaian, and Ahmad Almogren. "Defending unknown attacks on cyber-physical systems by semi-supervised approach and available unlabeled data." *Information Sciences* 379 (2017): 211–228. ScienceDirect.
56. Alajeely, Majeed, Robin Doss, and Vicky Mak-Hau. "Defense against packet collusion attacks in opportunistic networks." *Computers & Security* 65 (2017): 269–282. ScienceDirect.
57. Maciá-Fernández, Gabriel, Rafael A. Rodríguez-Gómez, and Jesús E. Díaz-Verdejo. "Defense techniques for low-rate DoS attacks against application servers." *Computer Networks* 54, no. 15 (2010): 2711–2727. ScienceDirect.
58. Kiss, Istvan, Piroska Haller, and Adela Bereş. "Denial of Service attack Detection in case of Tennessee Eastman challenge process." *Procedia Technology* 19 (2015): 835–841. ScienceDirect.
59. Abbaspour, Alireza, Kang K. Yen, Shirin Noei, and Arman Sargolzaei. "Detection of fault data injection attack on uav using adaptive neural network." *Procedia computer science* 95 (2016): 193–200. ScienceDirect.
60. Stevanovic, Dusan, Natalija Vlajic, and Aijun An. "Detection of malicious and non-malicious website visitors using unsupervised neural network learning." *Applied Soft Computing* 13, no. 1 (2013): 698–708. ScienceDirect.
61. Li, Beibei, Rongxing Lu, Wei Wang, and Kim-Kwang Raymond Choo. "Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system." *Journal of Parallel and Distributed Computing* 103 (2017): 32–41. ScienceDirect.
62. Yu, Wei, Sriram Chellappan, Xun Wang, and Dong Xuan. "Peer-to-peer system-based active worm attacks: Modeling, analysis and defense." *Computer Communications* 31, no. 17 (2008): 4005–4017. ScienceDirect.
63. Abdelhamid, Neda, Aladdin Ayesh, and Fadi Thabtah. "Phishing detection based associative classification data mining." *Expert Systems with Applications* 41, no. 13 (2014): 5948–5959. ScienceDirect.
64. Alazab, Mamoun. "Profiling and classifying the behavior of malicious codes." *Journal of Systems and Software* 100 (2015): 91–102. ScienceDirect.
65. Song, Jungsuk, Hiroki Takakura, Yasuo Okabe, and Koji Nakao. "Toward a more practical unsupervised anomaly detection system." *Information Sciences* 231 (2013): 4–14. ScienceDirect.
66. Saini, Anil, Manoj Singh Gaur, Vijay Laxmi, and Mauro Conti. "Colluding browser extension attack on user privacy and its implication for web browsers." *Computers & Security* 63 (2016): 14–28. ScienceDirect.
67. Choi, Sang-soo, Jungsuk Song, Seokhun Kim, and Sookyun Kim. "A model of analyzing cyber threats trend and tracing potential attackers based on darknet traffic." *Security and Communication Networks* 7, no. 10 (2014): 1612–1621. Wiley.
68. Rubio-Hernan, Jose, Luca De Cicco, and Joaquin Garcia-Alfaro. "Adaptive control-theoretic detection of integrity attacks against cyber-physical industrial systems." *Transactions on Emerging Telecommunications Technologies* 29, no. 7 (2018): e3209. Wiley.
69. Zhang, Jian, Phillip Porras, and Johannes Ullrich. "Gaussian process learning for cyber-attack early warning." *Statistical Analysis and Data Mining: The ASA Data Science Journal* 3, no. 1 (2010): 56–68. Wiley.
70. Fan, Lejun, Yuanzhuo Wang, Xueqi Cheng, Jinming Li, and Shuyuan Jin. "Privacy theft malware multi-process collaboration analysis." *Security and Communication Networks* 8, no. 1 (2015): 51–67. Wiley.

71. Wu, Yu-Sung, Vinita Apte, Saurabh Bagchi, Sachin Garg, and Navjot Singh. "Intrusion detection in voice over IP environments." *International Journal of Information Security* 8, no. 3 (2009): 153–172. Springer.
72. Deepa, G., P. Santhi Thilagam, Furqan Ahmed Khan, Amit Praseed, Alwyn R. Pais, and Nushafreen Palsetia. "Black-box detection of XQuery injection and parameter tampering vulnerabilities in web applications." *International Journal of Information Security* 17, no. 1 (2018): 105–120. Springer.
73. Gowtham, R., and Ilango Krishnamurthi. "PhishTackle—a web services architecture for antiphishing." *Cluster computing* 17, no. 3 (2014): 1051–1068. Springer.
74. Saha, Sujoy, Subrata Nandi, Rohit Verma, Satadal Sengupta, Kartikeya Singh, Vivek Sinha, and Sajal K. Das. "Design of efficient lightweight strategies to combat DoS attack in delay tolerant network routing." *Wireless Networks* 24, no. 1 (2018): 173–194. Springer.
75. Gupta, Shashank, and B. B. Gupta. "XSS-SAFE: a server-side approach to detect and mitigate cross-site scripting (XSS) attacks in JavaScript code." *Arabian Journal for Science and Engineering* 41, no. 3 (2016): 897–920. Springer.
76. Jain, Ankit Kumar, and Brij B. Gupta. "A novel approach to protect against phishing attacks at client side using auto-updated white-list." *EURASIP Journal on Information Security* 2016, no. 1 (2016): 9. Springer.
77. Ahmad, Farhan Habib, Komal Batool, and Azhar Javed. "Detection of Privacy Threat by Peculiar Feature Extraction in Malwares to Combat Targeted Cyber Attacks." In *Advanced Computer and Communication Engineering Technology*, pp. 1237–1247. Springer, Cham, 2016.
78. Saini, Anil, Manoj Singh Gaur, Vijay Laxmi, Tushar Singhal, and Mauro Conti. "Privacy leakage attacks in browsers by colluding extensions." In *International Conference on Information Systems Security*, pp. 257–276. Springer, Cham, 2014.

References

1. Lun, Y.Z.; et al.: Cyber-physical systems security: a systematic mapping study. arXiv:1605.09641 (2016)
2. Razzaq, A.; et al.: Cyber security: threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. In: 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS). IEEE (2013)
3. Von Solms, R.; Van Niekerk, J.: From information security to cyber security. Comput. Secur. **38**, 97–102 (2013)
4. Benson, V.; McAlaney, J.; Frumkin, L.A.: Emerging threats for the human element and countermeasures in current cyber security landscape. Psychological and Behavioral Examinations in Cyber Security, pp. 266–271. IGI Global, Hershey (2018)
5. Bada, M.; Sasse, A.M.; Nurse, J.R.: Cyber security awareness campaigns: why do they fail to change behaviour? arXiv :1901.02672 (2019)
6. Floyd, D.H.; Shelton, J.W.; Bush, J.E.: Systems and methods for detecting a security breach in an aircraft network. Google Patents (2018)
7. Taha, A.F.; et al.: Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs. IEEE Trans. Smart Grid **9**(2), 886–899 (2018)
8. Valeriano, B.; Maness, R.C.: International relations theory and cyber security. In: Brown, C., Eckersley, R. (eds.) The Oxford Handbook of International Political Theory, p. 259. Oxford University Press, Oxford (2018)
9. von Solms, B.; von Solms, R.: Cybersecurity and information security—what goes where? Inf. Comput. Secur. **26**(1), 2–9 (2018)
10. Ron, M.: Situational status of global cybersecurity and cyber defense according to global indicators. Adaptation of a model for ecuador. In: Developments and Advances in Defense and Security: Proceedings of the Multidisciplinary International Conference of Research Applied to Defense and Security (MICRADS 2018). Springer (2018)
11. Al Mazari, A.; et al.: Cyber terrorism taxonomies: definition, targets, patterns, risk factors, and mitigation strategies. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, pp. 608–621. IGI Global, Hershey (2018)
12. Hansen, L.; Nissenbaum, H.: Digital disaster, cyber security, and the Copenhagen School. Int. Stud. Q. **53**(4), 1155–1175 (2009)
13. Kuehl, D.T.: From cyberspace to cyberpower: Defining the problem. Cyberpower and National Security, vol. 30. National Defense University Press, Washington, D.C (2009)
14. Benedickt, M.: Cyberspace: First Steps. MIT Press, Cambridge (1991)
15. Gunkel, D.J.: Hacking Cyberspace. Routledge, Abingdon (2018)
16. Abomhara, M.; Køien, G.M.: Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J. Cyber Secur. **4**(1), 65–88 (2015)
17. Mittal, S.; et al.: Cybertwitter: using twitter to generate alerts for cybersecurity threats and vulnerabilities. In: Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. IEEE Press (2016)
18. Johnson, C.; et al.: Guide to cyber threat information sharing. NIST Spec. Publ. **800**, 150 (2016)
19. Rid, T.; Buchanan, B.: Attributing cyber attacks. J. Strateg. Stud. **38**(1–2), 4–37 (2015)
20. Banks, W.C.: Cyber espionage and electronic surveillance: beyond the media coverage. Emory L. J. **66**, 513 (2016)
21. Zhang, H.; et al.: Optimal denial-of-service attack scheduling with energy constraint. IEEE Trans. Autom. Control **60**(11), 3023–3028 (2015)
22. Kustarz, C.: et al.: System and method for denial of service attack mitigation using cloud services. Google Patents (2016)
23. Niemelä, J.; Hyppönen, M.; Kangas, S.: Malware protection. Google Patents (2016)
24. Choo, K.-K.R.: The cyber threat landscape: challenges and future research directions. Comput. Secur. **30**(8), 719–731 (2011)
25. Parmar, B.: Protecting against spear-phishing. Comput. Fraud Secur. **2012**(1), 8–11 (2012)
26. Dodge Jr., R.C.; Carver, C.; Ferguson, A.J.: Phishing for user security awareness. Comput. Secur. **26**(1), 73–80 (2007)
27. Sharma, P.; Johari, R.; Sarma, S.: Integrated approach to prevent SQL injection attack and reflected cross site scripting attack. Int. J. Syst. Assur. Eng. Manag. **3**(4), 343–351 (2012)

28. Choraś, M.; et al.: Correlation approach for SQL injection attacks detection. In: International Joint Conference CISIS'12-ICEUTE´12-SOCO´12 Special Sessions. Springer (2013)
29. Brar, H.S.; Kumar, G.: Cybercrimes: a proposed taxonomy and challenges. J. Comput. Netw. Commun. **2018**, Article ID 1798659 (2018)
30. Gill, R.S.; Smith, J.; Looi, M.H.; Clark, A.J.: Passive techniques for detecting session hijacking attacks in IEEE 802.11 wireless networks. In: Clark, A.J., Kerr, K., Mohay, G.M. (eds.) AusCERT Asia Pacific Information Technology Security Conference: Refereed R&D Stream, 22–26 May 2005, Gold Coast, Australia (2005)
31. Wassermann, G.; Su, Z.: Static detection of cross-site scripting vulnerabilities. In: Proceedings of the 30th International Conference on Software Engineering. ACM (2008)
32. Kieyzun, A.; et al.: Automatic creation of SQL injection and cross-site scripting attacks. In: Proceedings of the 31st International Conference on Software Engineering. IEEE Computer Society (2009)
33. Nguyen, P.H.; Ali, S.; Yue, T.: Model-based security engineering for cyber-physical systems: a systematic mapping study. Inf. Softw. Technol. **83**, 116–135 (2017)
34. Hydara, I.; et al.: Current state of research on cross-site scripting (XSS)—a systematic literature review. Inf. Softw. Technol. **58**, 170–186 (2015)
35. Muccini, H.; Sharaf, M.; Weyns, D.:. Self-adaptation for cyber-physical systems: a systematic literature review. In: Proceedings of the 11th International Symposium on Software Engineering for Adaptive and Self-managing Systems. ACM (2016)
36. Mishna, F.; et al.: Interventions to prevent and reduce cyber abuse of youth: a systematic review. Res. Soc. Work Pract. **21**(1), 5–14 (2011)
37. Lewis, G.; Lago, P.: Architectural tactics for cyber-foraging: results of a systematic literature review. J. Syst. Softw. **107**, 158–186 (2015)
38. Rahim, N.H.A.; et al.: A systematic review of approaches to assessing cybersecurity awareness. Kybernetes **44**(4), 606–622 (2015)
39. Enoch, S.Y.; et al.: A systematic evaluation of cybersecurity metrics for dynamic networks. Comput. Netw. **144**, 216–229 (2018)
40. Ramaki, A.A.; Rasoolzadegan, A.; Bafghi, A.G.: A systematic mapping study on intrusion alert analysis in intrusion detection systems. ACM Comput. Surv. (CSUR) **51**(3), 55 (2018)
41. Chockalingam, S.; et al.: Bayesian network models in cyber security: a systematic review. In: Nordic Conference on Secure IT Systems. Springer (2017)
42. Alguliyev, R.; Imamverdiyev, Y.; Sukhostat, L.: Cyber-physical systems and their security issues. Comput. Ind. **100**, 212–223 (2018)
43. Franke, U.; Brynielsson, J.: Cyber situational awareness—a systematic review of the literature. Comput. Secur. **46**, 18–31 (2014)
44. Budgen, D.; Brereton, P.: Performing systematic literature reviews in software engineering. In: Proceedings of the 28th International Conference on Software Engineering. ACM (2006)
45. Kitchenham, B.A.; Budgen, D.; Brereton, O.P.: The value of mapping studies-A participant-observer case study. In: EASE (2010)
46. Petersen, K.; Vakkalanka, S.; Kuzniarz, L.: Guidelines for conducting systematic mapping studies in software engineering: an update. Inf. Softw. Technol. **64**, 1–18 (2015)
47. Niazi, M.: Do systematic literature reviews outperform informal literature reviews in the software engineering domain? An initial case study. Arab. J. Sci. Eng. **40**(3), 845–855 (2015)
48. Chong, R.: Quick reference guide to endnote (2018)
49. Beecham, S.; et al.: Using an expert panel to validate a requirements process improvement model. J. Syst. Softw. **76**(3), 251–275 (2005)
50. Mohammed, N.M.; et al.: Exploring software security approaches in software development lifecycle: a systematic mapping study. Comput. Stand. Interfaces **50**, 107–115 (2017)
51. Mufti, Y.; et al.: A readiness model for security requirements engineering. IEEE Access **6**, 28611–28631 (2018)