Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
July-December 2023 4(2), 2263–2279

A SYSTEMATIC MAPPING STUDY OF CYBERSECURITY VULNERABILITIES, ATTACKS, AND MITIGATION STRATEGIES

Kanika Khanna [1]

[1] Assistant Professor, Department of Computer Science, SJK PG College Kalanaur, Rohtak

ABSTRACT

For the intention of fortifying cyber applications and fending off significant security hazards, cybersecurity exploration has witnessed a remarkable upsurge in recent years. Identifying and examining prevalent cybersecurity vulnerabilities is the main aim of this investigation. To reach that destination, scientists embarked on a comprehensive cartography inquiry, which led to the recognition and assessment of 69 primary investigations. We discovered the most widespread security vulnerabilities after performing an extensive examination of the selected investigation. The location of publishing, country of publication, significant targeted infrastructure, applications, etc. have all been examined and showcased through data amalgamation. The results illustrate that the previously mentioned security methods simply strive to enhance security in overall, and that additional investigation is necessary to empirically confirm and practically implement the suggested resolutions. Moreover, we discovered that the majority of the investigation we incorporated in our examination concentrated on just a handful of the most common security vulnerabilities, such as social engineering, denial-of-service assaults, and malicious software. Nevertheless, additional effort must be exerted in this domain to ensure scholars and professionals acquire an enhanced comprehension of the utmost urgent cybersecurity weaknesses, targeted/exploited applications, alleviation methods, and frameworks.

Keywords: Cybersecurity, Threats, Vulnerabilities, Attack

Corresponding Author

Kanika Khanna,
Khanna.kanika918@gmail.com

DOI
10.29121/shodhkosh.v4.i2.2023.5315

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

1. INTRODUCTION

The digital realm is presently a crucial component of daily existence, enabling interaction, trade, finance, promotion, and a diverse range of additional vocational pursuits. The pace at which cybercrime is escalating directly corresponds to the pace at which cyberspace is being utilized. The extensive utilization of internet-based applications is the main catalyst of this expansion. These internet applications are not flawless, and cybercriminals exploit weaknesses in their programming to acquire unauthorized entry to networks [1, 2]. Due to this, cyber security is emerging as a significant subject of examination and implementation [2]. It is feasible to utilize a broad array of resources, encompassing the latest technology, protocols, safeguarding measures, directives, hazard-alleviating approaches, endeavors, education, optimal methodologies, and assurance, to uphold the security of users' data and accounts in the digital realm [3]. Data security

through the identification, inhibition, and reaction to cyber assaults [3-5] has escalated to emerge as a subject of global focus and importance.

There is an expanding disparity between the security weaknesses in the digital realm and the protective measures implemented by various businesses. Scientists and experts alike have been concentrating on this matter for the majority of a decade since it embodies a noteworthy scientific obstacle. There have been numerous investigations carried out in diverse cyber domains, each with its distinct features and idiosyncrasies to tackle different security infringements [1].

There are several approaches and instruments suggested in the literature for identifying cyber security problems and addressing them [6, 7]. Nevertheless, an aggregation of the preceding research is necessary prior to proceeding with further investigation in this domain. This document endeavors to tackle that vacancy by offering a thorough synopsis of cyber security hazards and current safeguards.

The objective of this investigation is to methodically chart the widespread cyber security weaknesses so that they can be recognized and examined. This susceptibility mapping investigation aims to uncover prevailing investigations on cyber security weaknesses and categorize remedies based on (1) extensively-utilized security weaknesses, (2) cyber threat targets, (3) susceptibility intensity, and (4) data gathering and authentication approaches. The subsequent scientific concerns are directly tackled by our mapping investigation:

Question 1: What are the most common imperfections in network security?

One of the main inquiries is to recognize the utmost urgent vulnerabilities in view of their frequency across the encompassed investigation. The response to this inquiry will illuminate the utmost urgent security concerns and emphasize the most productive paths for additional investigation.

Question 2: Where do the majority of cyber security articles surface?

With this inquiry, you'll discover where to search for the finest cyber defense publications. Discovering the foremost symposiums and periodicals in the field to disseminate investigations in is simplified with the response to this inquiry.

Question 3: Which country possesses the highest number of dynamic researchers in the realm of cyber security, as per RQ3?

Question 4: Who frequently becomes a victim of security vulnerabilities?

The reply to this inquiry focuses on individuals who are affected by security vulnerabilities. We categorize victims into two groups: individuals and enterprises. Discovering the solution to this inquiry will furnish researchers and practitioners with an all-encompassing viewpoint of the prevalent objectives of cybersecurity vulnerabilities. This will assist in comprehending the overall trend of assaults that aim at security vulnerabilities.

Question 5: Which software applications have been the focal point of cybercrime in these investigations?

To tackle this problem, we will gather a compilation of applications that were the subjects of cybersecurity in the selected research, providing users of these apps with valuable insights on safeguarding themselves against cyber threats.

Question 6: In the realm of cyber security, what are the frequently mentioned safeguards?

The response to this inquiry will furnish researchers with a synopsis of the current mitigation measures by presenting a catalogue of techniques employed to combat cyber security hazards.

This document's framework will appear as such for the remaining portion of its extent. The essential background is given in Section 2. In Section 3, we briefly examine what's already available. The investigation's approach is delineated in Section 4. The investigation's discoveries are showcased in Section 5, and their elucidation is furnished in Section 6. Section 7 concludes the article, while Section 8 addresses certain unresolved inquiries.

2. BACKGROUND

In this part, we'll look at some of the history of cyber security.

2.1. CYBER SECURITY

Safeguarding data and systems against unapproved entry, utilization, or modification is what we indicate when we discuss security. [8].

Cybersecurity, as delineated by the Information Systems Audit and Control Association (ISACA), "is preoccupied with the safeguarding and confidentiality of electronic resources, encompassing networks, computing gadgets, and data that is handled, stored, or shared by interconnected information systems" [9].

The International Telecommunications Union describes cyber security as "the collection of knowledge, methods, and protocols that are employed to protect information systems and the information and data they hold" [9, 10].

Safeguarding information in the digital realm entails ensuring its confidentiality and can be retrieved as required, amidst various other aspects.[9].

Cybersecurity, as defined by Merriam-Webster, is "the act of safeguarding computer networks and information from trespass or alternative types of assault" [11].

According to [3], the phrase "cyber security" pertains to the techniques and structures implemented to avert data breaches and attacks on computer systems and networks that originate in the virtual realm.

Cyber security is the art of protecting computer networks and other digital infrastructures from invasion. [12].

Researchers utilize a multitude of vocabularies to delineate cyber security. Various aspects of cyber security are emphasized by the numerous current definitions. Some explanations highlight confidentiality and protection, while others emphasize the importance of setting up principles for maintaining information confidential, safeguarded, and reachable. Furthermore, certain academics have underscored the necessity of delineating systems and technology to protect computers. The phrase "cyber security" pertains to precautions implemented to hinder unauthorized entry to computer systems and the information they encompass. The requirement of preserving a safe digital realm is additionally underscored by these notions.

2.2. CYBER SECURITY TERMINOLOGIES

Here are some explanations of significant concepts utilized in this investigation, which will assist you in comprehending the underlying principles at work.

Knowledge that is formed, upgraded, preserved, distributed, and utilized through the utilization of interconnected and reliant networks using cutting-edge knowledge and communication technologies is said to exist in the realm of cyberspace [13-15].

Weaknesses: When a system or its blueprint possesses weaknesses, a perpetrator can exploit them to execute arbitrary code, obtain unauthorized entry to confidential information, or induce a disruption of service. [22, 23]

Actions carried out with the aim to gain from vulnerabilities in a system while also causing harm to the system itself are menaces [22, 24].

Assaults are all endeavors to cause damage to, or disturb the regular operation of, a framework through the utilization of the misuse of weaknesses utilizing any assortment of instruments and methodologies. These attacks are executed for the advantage of the assailants, who might desire personal satisfaction or monetary profit [24, 25].

There have been numerous deliberations in the literature regarding diverse security vulnerabilities. Several common cyber security vulnerabilities are delineated here to assist readers in gaining a more comprehensive understanding of the subject matter.

DoS attacks are those that aim to impede individuals from accessing a designated computer or network resource. It's triggered by anything that hinders or completely disables a network's capability to accomplish its intended goal. Numerous computer gadgets in the IoT framework are susceptible to resource exhaustion assaults [26] because of their limited memory capabilities and computational assets. One reason for a denial-of-service attack is that potential attackers take advantage of the fact that many different sectors utilize the same technologies [27, 28]. Malevolent software is an attack category in which the attacker utilizes malicious software programs to gain unauthorized access to computer systems by exploiting its security vulnerabilities. A dramatic fiscal or administrative reward is the reason behind malware, urging an attacker to infiltrate as many network devices as possible to achieve their malevolent goals [29, 30].

Phishing is an illicit practice that utilizes both technological and societal methods to pilfer personal data from Internet users. Email, instant messaging, pop-up notifications, and websites are all utilized in phishing assaults [31, 32].

A SQL infusion assault includes the incorporation of a malevolent information string into the program to change or otherwise control the SQL inquiry. The database is susceptible to numerous hazards from this attack, including disclosure of confidential information and unauthorized entry and modification of data. This assault is perilous because it might jeopardize data integrity and reveal delicate information to unauthorized entities. Furthermore, approved users are incapable of retrieving the essential information as system-wide directives are executed during this type of assault [33, 34].

Intermediary assaults and session commandeering: Man-in-the-middle assaults, additionally recognized as MIM, MitM, MiM, and MITMA, transpire when a malevolent performer covertly seizes control of a communication conduit amidst two or more entities. The transmission of the intended targets could potentially be intercepted, manipulated, or even substituted by the MITM assailant. Furthermore, as victims remain oblivious to the trespasser, they presume the pathway of correspondence is safeguarded [35, 36].

In a Cross-Site Scripting (XSS) assault, a cybercriminal endeavors to pilfer confidential data from a user by executing malevolent JavaScript code in the target's web browser. It's a recent website weakness that's been taken advantage of frequently [37, 38].

3. EXISTING WORK

The digital realm has been the topic of numerous cartography studies and comprehensive literature reviews (CLR), but these inquiries have not concentrated on cyber safety hazards. The subsequent is a discourse of diverse exploration endeavors.

[1] cybernetic physical system safety was the topic of an extensive cartography examination. The extent of the assessment was extensive, encompassing subjects such as self-governing command, intelligent power networks, data frameworks, and network structure. Scientists have primarily concentrated on bodily level attacks against intelligent grid systems, as evidenced by investigations.

[39] performed an extensive mapping examination of how model-driven security engineering is being utilized to address the security challenges of cyber-physical systems. The article's three main contributions are its classification of primary studies based on publication figures, its recognition of the security issues addressed in the selected primary research, and its clarification of the unresolved inquiries. Researchers discovered that a limited number of models-centric security engineering solutions were accessible for cyber-physical systems. Furthermore, there are scant empirical inquiries on this matter.

[40] Cyber situational consciousness was the topic of a strengths, weaknesses, opportunities, and threats (SWOT) examination. The authors selected 102 articles and categorized them into clusters. The findings imply that not all aspects of cyber situational awareness have been examined to the equal degree. Investigation endeavors are focused primarily on industrial command systems and comparatively less on communication and defense operations.

[41] an advanced investigation on cross-site scripting (XSS) weaknesses in web applications utilizing a systematic literature review (SLR). Scientists in this investigation discovered several methods to XSS weaknesses, but they couldn't agree on a solitary one as a cure-all. The SLR suggests further investigation is necessary to completely resolve the problem of XSS elimination from source code before deployment.

[42] self-teaching endeavor (SLR) on cyber-physical system (CPS) adjustment. The main objective of their investigation is to assess present approaches of managing self-adjustment in CPS structure. Current methods for self-adjustment in Cyber-Physical Systems (CPS), as discovered by the investigation, encompass a variety of diverse modification procedures both within and amidst strata. Hence, additional examination into self-adjustment in CPS and the step-by-step correlation of resolutions is necessary.

[43] additionally performed a systematic literature review (SLR) to ascertain the present degree of understanding regarding approaches for diminishing and deterring adolescent engagement in cyber-mistreatment. The objective of the investigation is to assess the effectiveness of cyber maltreatment interventions in augmenting Internet security consciousness and diminishing perilous online conduct. Digital maltreatment intervention was demonstrated to be advantageous in enhancing consciousness of internet hazards, albeit the data exhibited no association between the two.

[44] performed a systematic literature review to explore our understanding of the existing cyber foraging frameworks. Cyber foraging is a technique of computing in which low-powered devices delegate their resource-intensive

tasks to more capable nearby computers. The investigation aimed to categorize the numerous architectural methods to address the queries of what, when, and where mobile devices can unload data and processing. To support architectural researchers and practitioners in broadening their design to facilitate cyber foraging, the authors recognized the qualities of existing architectures and delineated them in architectural methodologies.

[45] performed a systematic literature review (SLR) exploration of the techniques for evaluating cyber security consciousness testing. According to the results of the research, a wide variety of strategies have been recommended in the literature to raise cyber security awareness. Nevertheless, there is still a requirement to amalgamate multiple approaches for improved efficiency. Furthermore, enhanced education is necessary concerning digital security, specifically for the youth, who are the main victims of cyber assaults.

[46] tried to document possible assault situations for GSM-dependent dynamic networks. Network parameter modifications are employed to assess the influence on security measurements. Every metric's performance was evaluated considering the constant risks to data protection. Researchers and practitioners may utilize the findings of this investigation to gain a deeper comprehension of which security indicators hold the utmost significance for their specific networks. This investigation, nonetheless, concentrated solely on generic security vulnerabilities instead of particular cyber risks.

[47] performed a comprehensive mapping investigation utilizing SMS to analyze intrusion notifications. A grand total of 411 papers were examined for the analysis of this mapping study. The investigation concluded that trespass warning examination is an emerging domain of research. Understanding of the present condition of the cutting-edge in intrusion alarm examination is given in this investigation.

[48] performed a literary investigation to ascertain if Bayesian network models are beneficial for cyber defense. In this investigation, we discovered and prioritized seventeen distinct Bayesian network frameworks. The investigation demonstrates that Bayesian network models might assist in addressing the problem of detrimental insiders. When juxtaposed with industrial control systems, these models are frequently utilized to manage the security apprehensions of the information technology milieu. Furthermore, there are no ubiquitous Bayesian network models that address each and every cyber security issue.

[49] examined the literature on SCADA and intelligent grid security, highlighting continuous cyber assaults and existing safeguards. The article's primary contribution is its examination of cyber assault techniques, simulation of possible attack consequences, and discourse on security framework identification and creation.

From what has been mentioned, it is apparent that numerous investigations have been conducted on the subject of cybersecurity and cyber consciousness. SLRs and systematic cartography inquiries have also been conducted. Current mapping studies, nonetheless, have predominantly concentrated on digital security and digital consciousness. There hasn't been an exhaustive investigation that charts out all the manners in which cyber security may be jeopardized or how most effectively to safeguard against that likelihood. This mapping exploration completes the gaps by providing researchers a panoramic view of the condition of cyber security vulnerabilities and identification techniques.

4. RESEARCH METHODOLOGY

Principles for methodical cartography investigations [50-52] were adhered to in this exploration. There are a multitude of benefits to utilizing this method. It's a systematic approach to discovering, examining, and interpreting research that is relevant to a specific subject, theme, or phenomenon of interest. To assess and amalgamate the empirical proof regarding a technique or technology, to pinpoint the absent domains and discrepancies in the present investigation, and to equip researchers or practitioners with the framework essential to validate novel research, a methodical cartography investigation is a potent and structured strategy. While a methodical cartography investigation is further time- and effort-consuming than a conventional literature examination, the outcomes are greater comprehensive understanding of the matter and a sturdy groundwork on which to establish assertions concerning research subjects [53]. Figure 1 illustrates the five stages of a customary process for a methodical charting venture.

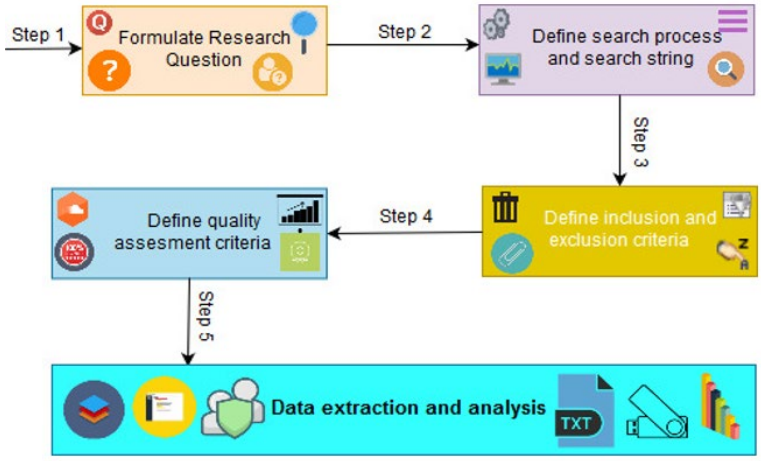

Fig. 1. Phases of a systematic mapping study

All the procedures used in this work have been documented in full in a protocol for systematic mapping. Here's a high-level breakdown of what needs to happen:

1) Developing study questions
2) Specifying the Search Methodology and the Search String
3) Outlining the steps and criteria for selecting studies to include or exclude
4) Extraction of data and correlation with research questions
5) Extracting Meaning from Analyzed Data

Two scientists worked on this mapping project. Both of them are professors in universities. One author created the procedure, while the second author evaluated it critically to point out its flaws. Each member of the team helped with some aspect of the systematic mapping research. As part of this systematic mapping study's efforts to reduce subjectivity and enhance its methodology, inter-rater reliability tests were conducted throughout both the screening and final selection stages. Articles published between January 2017 and December 2018 that fit the criteria were found using a systematic search.

4.1. SEARCH STRATEGY

Before initiating the official inquiry, the term "observational inspections on digital security" was employed in Science Direct. The justification for choosing Science Direct is because of its prestige as a well-known repository containing a vast variety of articles from various disciplines. The aim of this initial exploration was twofold: firstly, to validate whether there are a sufficient number of empirical investigations to carry out a mapping examination; and secondly, to identify some foundational studies that could potentially be employed later for the validation of the search query. The selected inquiries were migrated into the Endnote software [54]. The synopses of the acquired papers were scrutinized, and nine observational investigations were chosen as the primary studies so they could be employed to validate our enhanced expression. In this informal exploration process, countless observational inquiries were uncovered so it was decided to carry out a systematic mapping study and the preliminary phrase that was established for the exploration process was cyber AND security. When this initial string was employed on the Science Direct search engine, the acquired results did not encompass all the essential inquiries. Furthermore, two seasoned software engineering academics from the scholarly realm who have expertise in conducting methodical literature reviews were chosen as experts and they were invited to evaluate the search query and provide their perspectives. Based on these experts' perspectives, the initial string was altered, and the main search string was split into two sections. Expert perspective is a technique of rapidly evaluating and verifying information [55]. Here are the two constituents of our designated sequence.

1. Cyber Security
2. Attack/threat/vulnerability

In order to find all relevant papers, synonyms for both of these terms were evaluated. It was agreed to employ this improved string for future data extraction after it was checked once again against the list of primary research. Our search string is reliable since the results from the second search string include just the major research we specified. This systematic mapping research employs a three-pronged approach to its search strategy:

4.1.1. CONSTRUCTING THE SEARCH STRING:

The population, the suggested solution, the relevance and context results were used to first formulate the search phrases as under.

- Articles describing empirical research on cyber security constitute the population.
- Intervention: Literature-proposed solutions to cyber security problems.
- The result of importance: Cybersecurity evidence quantity and kind
- In the context of cyber security, where there has been a lot of attention paid to empirical research,

4.1.2. DISCOVERING SYNONYMS OF THE DERIVED EXPLORATION PHRASES UTILIZING BOOLEAN OPERATORS.

The selected keywords were checked against the largest scholarly indexes for accuracy. The search string was built by identifying all relevant synonyms for the given keywords. Possible related terms include the ones listed below:

- Cyber Security: (cyber 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. CONFIRMATION OF RECOGNIZED TERMS IN THE SCHOLARLY REPOSITORIES

The following search phrase was settled upon after many iterations and revisions 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
- Science Direct
- IEEE Explore
- John Wiley Online Library
- Springer Link

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 [R1][R2][42] .

4.2. PUBLICATION SELECTION

The selection criteria and methodology used to identify appropriate articles in light of the research questions are outlined in this section. The following requirements were established for consideration:

The reviewed literature spans a full decade, from 2007 to 2018. The majority of cybercrimes were not reported until after 2007, therefore that's when we'll begin looking. However, given the search was conducted in 2018, only papers from the second quarter of 2018 were included in the systematic mapping analysis.

- Empirical research on the state of cyber security

- Research aimed at finding effective countermeasures for cyber security flaws

The following conditions served as grounds for elimination:

Lacking specific instructions on how to identify potential cyber security flaws, these studies are of little use.

- Multiple studies with the most current one included for analysis.
- Research that does not include a critical evaluation of its results.
- Only PowerPoint presentations and abstracts for these studies are currently accessible.
- Articles that don't address cyber security in any way.
- Articles that only describe cyber security or provide advice and suggestions
- Workshop and special-issue pieces, as well as book prefaces.
- Sections of a book
- Non-English language papers.
- Unobtainable research papers.

Publications were first selected from the search result based on title and abstract screening according to the selection criteria, which was completed automatically. Second, we reviewed all of the articles that made it through the first round so that we could narrow down the list of publications to consider for the final round based on our predetermined inclusion criteria.

4.3. DATA EXTRACTION

To procure intelligence from the acquired documents, we devised a data extraction template (enclosed in Appendix A) founded on our search expression and the unearthed vulnerabilities. There are both expansive and restricted questions on this data gathering document. Two software developers took part in a pilot experiment to evaluate the data retrieval tool. The outcomes of the preliminary investigation influenced the ultimate iteration of the data retrieval template. The ultimate configuration for data retrieval comprises three divisions: Details about the selected document are accumulated in the initial segment; this encompasses the document's heading, writers, year of publication, nation, and citation categories of documents. The evaluation of the paper's quality is outlined in the subsequent section (the results of quality evaluation are not included in this paper because, as per the mapping study guidelines, quality assessment is not indispensable in mapping studies [51]).

5. RESULTS

5.1. CLASSIFICATION OF CYBER SECURITY WEAKNESSES

The findings of the comprehensive mapping analysis are shown here. A total of 134 studies passed muster during the primary search. In the end, 69 articles met both the inclusion and exclusion criteria (as given in Appendix B). Each iteration's data is listed in Table 1. In order to answer the study questions, careful reading and analysis of these chosen publications was conducted.

Table 1 Study selection

Source	Retrieved	Initial selection	Final selection
IEEE	3878	40	30
ACM	314	26	9
Science Direct	1299	46	21
Springer Link	1440	11	6
Wiley	85	11	3
Total	7016	134	69

The systematic mapping analysis yielded the types of cyber security vulnerabilities (RQ1) shown in Table 2. The cyber security flaws discovered in this mapping analysis are listed in column 1 of table 2. Each vulnerability's appearance rate in the included studies is shown in column 2 of Table 2, and the percentage of occurrence is displayed in column 3.

Malware, phishing, SQL injection, XSS, DoS, session hijacking, man-in-the-middle attacks, and credential reuse are just some of the major security flaws we found throughout our mapping research. The systematic mapping research focused mostly on securing against denial-of-service attacks (41%). Malware (16%) is more common than phishing (14%) as a vulnerability described in the literature. Table 2 displays the remaining vulnerabilities and their specifics.

Table 2 Cyber security vulnerability categorization

Vulnerability	Frequency	Percentage
Credential Reuse	1	1%
Cross-site Scripting (XSS)	1	1%
Denial-of-service (DoS)	28	41%
Malware	11	16%
Phishing	7	10%
Session Hijacking and Man-in-the-Middle-Attacks	2	3%
SQL Injection Attack	3	2%
Other	17	24%

5.2. EVALUATION DERIVED FROM THE LOCATION OF PUBLICATION AND TYPE OF SOURCE

To answer the second research question (RQ2) (i.e., what are the most important places to publish in cyber security?), this study will analyze the venue and source type of the chosen publication.

Table 3 shows the five libraries we focused on for our venue and source type study. Conference proceedings, academic journals, and workshop proceedings are the primary venues for the dissemination of the chosen papers from these archives. Table 3 displays the breakdown of the sampled research by method of publishing. Only three of the 69 total research were published in workshops, while the number of papers published at conferences is almost identical (33 out of 69). Workshops hosted 4% of all research presentations, whereas journals hosted 48%, and conferences hosted 4%. According to Table 3, there are more conference papers than journal publications in IEEE and ACM libraries. Three of the works were published in IEEE journals, while the other publications were all presented at IEEE conferences. No journal articles were found in the ACM database; all relevant papers were found at conferences and workshops (67% and 33%, respectively). Statistical analysis of the other three libraries reveals that all of the relevant articles found for the present research were published in journals (Science Direct, Wiley Online, and Springer). Science Direct has the largest percentage (30%) of publications published from these three collections. There were 8.69% of the pool named Springer, followed by 4% named Wiley.

Table 3 Distribution of studies w.r.t. venue of publication

Venue	Journal Papers	Conference Papers	Workshop Papers	Total
IEEE	3	27	0	30
ACM	0	6	3	9
Science Direct	21	0	0	21
Springer	6	0	0	6
Wiley	3	0	0	3
Total	33	33	3	69

5.3. DEMOGRAPHIC ANALYSIS

The author's affiliation was utilized to determine and rank the top nations engaged in cyber security research.

Table 4 Country frequency analysis

Country		Frequency	Percentage
Italy		1	1%
Malaysia		1	1%
Pakistan		1	1%
Spain		1	1%
China		2	3%
France		2	3%
Iran		2	3%
Japan		2	3%
Romania		2	3%
Singapore		2	3%
South Korea		3	4%
UK		3	4%
Australia		5	7%
Canada		5	7%
Taiwan		7	10%
India		14	20%
USA		16	23%

The objective of this ranking is to recognize the countries from which the majority of cyber security researchers compose in order to tackle research inquiry 3 (RQ3). Despite the writer having moved to an alternative country, the association particulars provided in the document were utilized. The country of the initial writer was utilized if there were multiple authors for an article. Table 4 and Figure 2 display the results. Table 4, column 1, displays the nations from which authors of pertinent studies originate. Table 4, column 2, exhibits the ratio of authors who are associated with the country mentioned in column 1, and Table 4, column 3, demonstrates the occurrence rate of this phenomenon. Based on the information (for RQ3), American scientists contributed 23% (16 out of 69) of the selected publications, establishing the United States as the nation with the highest quantity of published cyber security research papers. Australia and Canada, who shared fourth position, each contributed 7%, while authors from India and Taiwan (with 14 and 7 pieces, respectively) secured second and third places, correspondingly. The leftover fragments surfaced in newspapers and magazines in a variety of countries every couple to several instances per annum.

This highlights the necessity for further international study into cyber security to better comprehend the impact of cultural norms and practices.

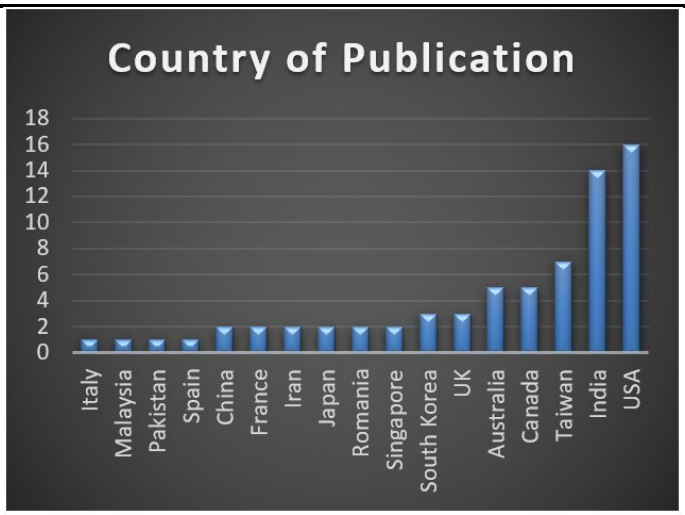

Fig.2. country of publication

Current research trends in the field of cyber security were determined by classifying the chosen papers according to their year of publication. The breakdown of research by year is shown in Figure 3. Figure 3 demonstrates the dramatic rise in cyber security studies conducted to bolster cyber applications and counter the most pressing security challenges they confront.

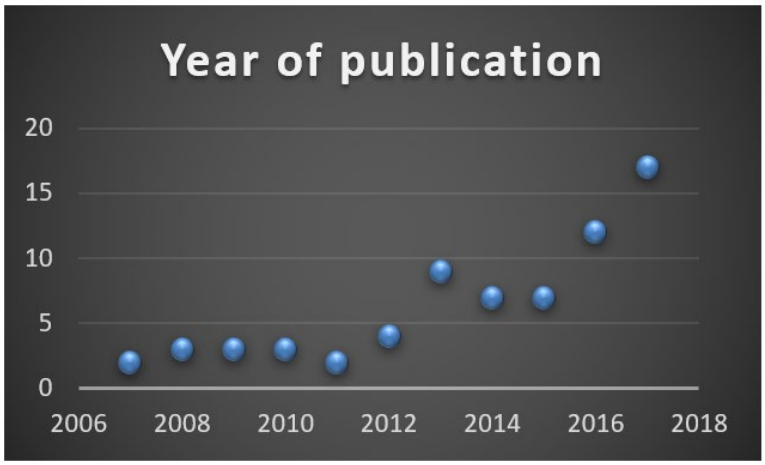

Fig.3. Year of Publication

The properties of the data used to verify the suggested method were also emphasized to help readers better grasp the data types often used. In Table 5, we can see the details of the test data that was utilized to verify the effectiveness of the methods. Most studies' validation data came from a variety of sources (44% of total papers), including scholarly journals, commercial companies, and government agencies. Thirty percent of the scientists checked their theory using data from industry, ten percent with academic data, and three percent with government data.

Table 5 Data Characteristics

Option	Frequency	Percentage
Academia	7	10
Industrial	21	30%
Government	2	3%
Mixed	39	44%

Since only empirical research were considered for inclusion, only those that validated their findings empirically were included. Experiment, case study, and simulation are the three main types of empirical research methods. The studies were chosen because they all employed simulation as a primary validation method. Table 6 summarizes the findings of the breakdown of studies by study design.

Table 6: Study strategy used

Study types	Frequency	Percentage
Case Study	4	6%
Experiment	43	62%
Simulation	28	41%

Table 6 and Figure 4 reveal that, of the 69 publications included in the sample, 62% (or 43 of them) employed experimental validation. In terms of empirical validation, case studies were employed by just 6% of the total sample size (four out of sixty-nine articles), whereas simulation was used by 41% of the pool (twenty-eight articles).

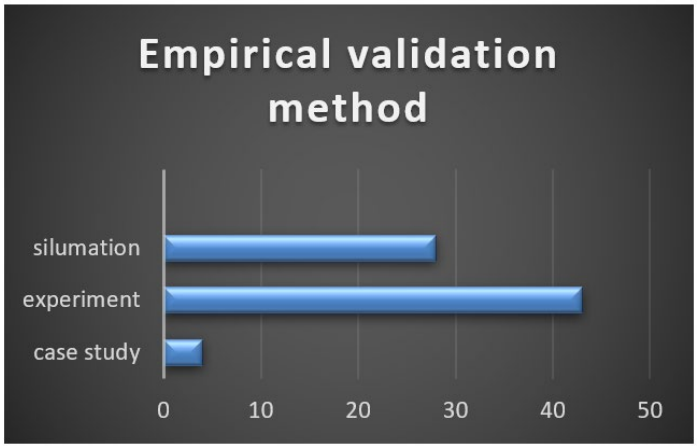

Fig.4. Classification of research based on empirical approach employed

5.4. VICTIM ANALYSIS

Research Question 4 (RQ4) seeks to address the question, "Who are the key victims of these security vulnerabilities?" by identifying these victims. Table 7 displays the breakdown of the victims into two groups: businesses and individuals. Some of the vulnerabilities in the chosen studies impacted both people and organizations, therefore the findings for these vulnerabilities overlap.

Table 7 Victim frequency

Victim	Response &age	Responses
Individual	6	9%
Organization	69	100%

5.5. TARGET APPLICATIONS

With this fifth inquiry (RQ5), we embarked on determining the software applications that were the main objectives of the cybercrimes investigated. The data we collected from the investigation we selected on the organizations and initiatives that were the targeted recipients was moderately diverse, but we managed to categorize it into the subsequent three classifications.

5.5.1. INFRASTRUCTURE THAT WAS TARGETED

The retrieved data suggests that the following infrastructure was often attacked using cyber means:

- 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

5.5.2. TARGET APPLICATIONS

According to our findings, cybercriminals specifically targeted the following software:

- 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

Our last inquiry (RQ6) looked at how different sectors were taking precautions against cyberattacks. The frequency and proportion of the mitigation measures employed to safeguard the cyber environment from cyber security risks are shown in Table 8.

Our analysis shows that many cyber firms use a combination of security measures to safeguard their network, with firewalls and user IDs being particularly common. Using a combination of security measures has increased the frequency

to more than 69 (the number of studies included in this analysis). Additionally, antiphishing strategies were widely employed in the articles that dealt only with phishing assaults.

Many publications also employed traffic analysis to spot security breaches. Our analysis of the landscape reveals that intrusion detection systems (17 out of 69) and firewalls (13/69) are the most widely deployed defensive measures against cyber attacks. Six out of a total of sixty-nine instances of cyber threat mitigation used anti-phishing or traffic analysis. Antimalware software, intended to safeguard the cyber environment from malware assault, is the third method of mitigating cyber attacks. Table 8 lists the remaining preventative measures and how often they are used. However, the names of the mitigating techniques were not included in nine of the collected papers.

Table 8: Attack mitigation techniques

Mitigation techniques	Frequency	Percentage
Algorithm weakly supervised	3	4.3%
VulPecker tool	1	1.45%
Iterative approach of Critical component identification	2	2.90%
Intrusion detection systems (IDS)	17	24.6%
Content based spam filtering technique	3	4.3%
MP shield	1	1.45%
Command and Control (C&C) servers	1	1.45%
Antiphishing techniques	6	8.69%
Firewalls	13	18.84%
Analysing traffic anomaly features	6	8.69%
Anti-malware software	5	7.25%
Automated dynamic analysis techniques	1	1.45%
Modifying the way of accepting incoming requests	1	1.45%
Conventional false data detection (FDD) approaches	4	5.80%
Signature-based detection and anomaly-based detection	3	4.3%
Darknet	2	2.90%
Not Mentioned	9	13.04%

6. DISCUSSION

This study looks in detail at cybersecurity challenges and assembles the results from 69 published studies that were released between 2007 and 2018. The purpose of this study is to examine important flaws, how sourced works emerged, major countries, key application areas and what strategies are used for defense. It is clear that Denial-of-Service (DoS) attacks are the major threat, making up 41% of all reported incidents, while malware and phishing each make up 16% and 10%. Numerous frameworks are now used to exploit these vulnerabilities such as methods used in smart grids, cloud services, IoT networks and systems controlling industry (Zhang et al., 2015; Alguliyev et al., 2018). Evidence from the analysis indicated that cyber threats were growing more complicated and that the use of Intrusion Detection Systems (IDS), firewalls and anti-malware tools was now essential (Hydara et al., 2015; Taha et al., 2018).

The research report showed that the United States is responsible for 23% of cybersecurity research, ahead of India at 20% and Taiwan at 10%. That shows a global trend of varying attention to cybersecurity research (Robinson et al., 2015; von Solms & van Niekerk, 2018). Both journals and conferences were equally important, offering 48% of the main publishing opportunities and IEEE and ScienceDirect were commonly where research could be found (Kitchenham et al., 2006; Petersen et al., 2015). Most of the empirical validation was carried out through experiments (62%), some through simulations (41%) and a minimum fraction using case studies (6%) which points to controlled settings being preferred to hands-on ones (Budgen & Brereton, 2006). While different groups tried to address the issues, only a certain number

of research focused on joins strategies. Utilized techniques for these included VulPecker, as well as weakly supervised algorithms which were described by Rahim et al., 2015 and Chockalingam et al., 2017.

In essence, the findings showed that it is crucial to investigate cybercrime more fully in developing countries and deeper understanding of the marginalised groups who are not properly covered in current cybersecurity research (Bada et al., 2019; Mishna et al., 2011). The research underlined the difference between suggested solutions and their implementation, highlighting the need for research, better structures and realistic reviews of cyberattacks on actual systems (Lewis & Lago, 2015; Enoch et al., 2018). While more is being done to spot and categorise cyber threats, a lot of current research still looks at only a few types of weaknesses. Overlooking these issues means that the more common threats of credential reuse and session hijacking which are also dangerous, will not be addressed.

7. CONCLUSION

The study covers in detail the most common cybersecurity risks, the measures used to address them and trending research topics found in 69 top studies published over the decade from 2007 to 2018. The research lists Denial-of-Service (DoS), malware, phishing and SQL injection as the main threats researchers studied. Most cybersecurity research relies on experiments, although case studies and examples from real-life vary significantly. Most cybersecurity research in fields like the United States, India and Taiwan is showcased in publications available through IEEE, ACM and ScienceDirect. Although threats are a common problem, studies do not make consistent use of strategies including intrusion detection, firewalls and anti-phishing. By looking at the numbers, it's clear that organizations are more frequently surveyed, a sign that not enough attention is given to inclusive cybersecurity solutions. The report also highlights the frequent targets within software and IT, including social media, systems that manage factories, cloud systems and web applications. Even though several advanced approaches and frameworks have been created for mitigation, their practical success or proper testing has not always been accomplished. This study emphasizes that better cybersecurity depends on global cooperation, improved facilities for testing outside environments and focusing more broadly on all types of threats to keep security fair and steady in all sectors.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Lun, Y.Z., D'Innocenzo, A., Malavolta, I., Di Benedetto, M.D.: Cyber-physical systems security: a systematic mapping study. arXiv preprint arXiv:1605.09641 (2016).

Razzaq, A., Hur, A., Ahmad, H.F., Masood, M.: Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. In: Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on 2013, pp. 1-6. IEEE

Von Solms, R., Van Niekerk, J.: From information security to cyber security. computers & security 38, 97-102 (2013).

Benson, V., McAlaney, J., Frumkin, L.A.: Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape. In: Psychological and Behavioral Examinations in Cyber Security. pp. 266-271. IGI Global, (2018)

Bada, M., Sasse, A.M., Nurse, J.R.: Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672 (2019).

Floyd, D.H., Shelton, J.W., Bush, J.E.: Systems and methods for detecting a security breach in an aircraft network. In. Google Patents, (2018)

Taha, A.F., Qi, J., Wang, J., Panchal, J.H.: Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs. IEEE Transactions on Smart Grid 9(2), 886-899 (2018).

Valeriano, B., Maness, R.C.: International Relations Theory and Cyber Security. The Oxford Handbook of International Political Theory, 259 (2018).

Von Solms, B., von Solms, R.: Cybersecurity and information security–what goes where? Information & Computer Security 26(1), 2-9 (2018).
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) 2018, p. 12. Springer
Al Mazari, A., Anjariny, A.H., Habib, S.A., Nyakwende, E.: Cyber terrorism taxonomies: Definition, targets, patterns, risk factors, and mitigation strategies. In: Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications. pp. 608-621. IGI Global, (2018)
Hansen, L., Nissenbaum, H.: Digital disaster, cyber security, and the Copenhagen School. International studies quarterly 53(4), 1155-1175 (2009).
Kuehl, D.T.: From cyberspace to cyberpower: Defining the problem. Cyberpower and national security 30 (2009).
Benedickt, M.: Cyberspace: first steps. (1991).
Gunkel, D.J.: Hacking cyberspace. Routledge, (2018)
Robinson, M., Jones, K., Janicke, H.: Cyber warfare: Issues and challenges. Computers & security 49, 70-94 (2015).
Blakemore, B.: Policing cyber hate, cyber threats and cyber terrorism. Routledge, (2016)
Taylor, R.W., Fritsch, E.J., Liederbach, J., Saylor, M.R., Tafoya, W.L.: Cyber Crime and Cyber Terrorism. (2019).
Jajodia, S., Shakarian, P., Subrahmanian, V., Swarup, V., Wang, C.: Cyber warfare: building the scientific foundation, vol. 56. Springer, (2015)
Danks, D., Danks, J.H.: Beyond machines: Humans in cyber operations, espionage, and conflict. Binary Bullets: The Ethics of Cyberwarfare, 177-197 (2016).
Libicki, M.C.: Drawing inferences from cyber espionage. In: 2018 10th International Conference on Cyber Conflict (CyCon) 2018, pp. 109-122. IEEE
Abomhara, M., Køien, G.M.: Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security 4(1), 65-88 (2015).
Mittal, S., Das, P.K., Mulwad, V., Joshi, A., Finin, T.: 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 2016, pp. 860-867. IEEE Press
Johnson, C., Badger, L., Waltermire, D., Snyder, J., Skorupka, C.: Guide to cyber threat information sharing. NIST special publication 800, 150 (2016).
Rid, T., Buchanan, B.: Attributing cyber attacks. Journal of Strategic Studies 38(1-2), 4-37 (2015).
Banks, W.C.: Cyber espionage and electronic surveillance: beyond the media coverage. Emory LJ 66, 513 (2016).
Zhang, H., Cheng, P., Shi, L., Chen, J.: Optimal denial-of-service attack scheduling with energy constraint. IEEE Transactions on Automatic Control 60(11), 3023-3028 (2015).
Kustarz, C., Huston III, L.B., Simpson, J.A., Winquist, J.E., Barnes, O.P., Jackson, E.: System and method for denial of service attack mitigation using cloud services. In. Google Patents, (2016)
Niemelä, J., Hyppönen, M., Kangas, S.: Malware protection. In. Google Patents, (2016)
Choo, K.-K.R.: The cyber threat landscape: Challenges and future research directions. Computers & Security 30(8), 719-731 (2011).
Parmar, B.: Protecting against spear-phishing. Computer Fraud & Security 2012(1), 8-11 (2012).
Dodge Jr, R.C., Carver, C., Ferguson, A.J.: Phishing for user security awareness. Computers & Security 26(1), 73-80 (2007).
Sharma, P., Johari, R., Sarma, S.: Integrated approach to prevent SQL injection attack and reflected cross site scripting attack. International Journal of System Assurance Engineering and Management 3(4), 343-351 (2012).
Choraś, M., Kozik, R., Puchalski, D., Hołubowicz, W.: Correlation approach for SQL injection attacks detection. In: International Joint Conference CISIS'12-ICEUTE´ 12-SOCO´ 12 Special Sessions 2013, pp. 177-185. Springer
Brar, H.S., Kumar, G.: Cybercrimes: A Proposed Taxonomy and Challenges. Journal of Computer Networks and Communications 2018 (2018).
Gill, R.S., Smith, J., Looi, M.H., Clark, A.J.: Passive techniques for detecting session hijacking attacks in IEEE 802.11 wireless networks. (2005).
Wassermann, G., Su, Z.: Static detection of cross-site scripting vulnerabilities. In: Proceedings of the 30th international conference on Software engineering 2008, pp. 171-180. ACM

Kieyzun, A., Guo, P.J., Jayaraman, K., Ernst, M.D.: Automatic creation of SQL injection and cross-site scripting attacks. In: Proceedings of the 31st International Conference on Software Engineering 2009, pp. 199-209. IEEE Computer Society

Nguyen, P.H., Ali, S., Yue, T.: Model-based security engineering for cyber-physical systems: A systematic mapping study. Information and Software Technology 83, 116-135 (2017).

Franke, U., Brynielsson, J.: Cyber situational awareness–a systematic review of the literature. Computers & Security 46, 18-31 (2014).

Hydara, I., Sultan, A.B.M., Zulzalil, H., Admodisastro, N.: Current state of research on cross-site scripting (XSS)–A systematic literature review. Information and Software Technology 58, 170-186 (2015).

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 2016, pp. 75-81. ACM

Mishna, F., Cook, C., Saini, M., Wu, M.-J., MacFadden, R.: Interventions to prevent and reduce cyber abuse of youth: A systematic review. Research on Social Work Practice 21(1), 5-14 (2011).

Lewis, G., Lago, P.: Architectural tactics for cyber-foraging: Results of a systematic literature review. Journal of Systems and Software 107, 158-186 (2015).

Rahim, N.H.A., Hamid, S., Mat Kiah, M.L., Shamshirband, S., Furnell, S.: A systematic review of approaches to assessing cybersecurity awareness. Kybernetes 44(4), 606-622 (2015).

Enoch, S.Y., Ge, M., Hong, J.B., Alzaid, H., Kim, D.S.: A systematic evaluation of cybersecurity metrics for dynamic networks. Computer Networks 144, 216-229 (2018).

Ramaki, A.A., Rasoolzadegan, A., Bafghi, A.G.: A systematic mapping study on intrusion alert analysis in intrusion detection systems. ACM Computing Surveys (CSUR) 51(3), 55 (2018).

Chockalingam, S., Pieters, W., Teixeira, A., van Gelder, P.: Bayesian Network Models in Cyber Security: A Systematic Review. In: Nordic Conference on Secure IT Systems 2017, pp. 105-122. Springer

Alguliyev, R., Imamverdiyev, Y., Sukhostat, L.: Cyber-physical systems and their security issues. Computers in Industry 100, 212-223 (2018).

Budgen, D., Brereton, P.: Performing systematic literature reviews in software engineering. In: Proceedings of the 28th international conference on Software engineering 2006, pp. 1051-1052. ACM

Kitchenham, B.A., Budgen, D., Brereton, O.P.: The value of mapping studies-A participant-observer case study. In: EASE 2010, pp. 25-33

Petersen, K., Vakkalanka, S., Kuzniarz, L.: Guidelines for conducting systematic mapping studies in software engineering: An update. Information and Software Technology 64, 1-18 (2015).

Niazi, M.: Do systematic literature reviews outperform informal literature reviews in the software engineering domain? An initial case study. Arabian Journal for Science and Engineering 40(3), 845-855 (2015).

Chong, R.: QUICK REFERENCE GUIDE TO ENDNOTE. (2018).

Beecham, S., Hall, T., Britton, C., Cottee, M., Rainer, A.: Using an expert panel to validate a requirements process improvement model. Journal of Systems and Software 76(3), 251-275 (2005).

R1. N. M. Mohammed, M. Niazi, M. Alshayeb, and S. Mahmood, "Exploring software security approaches in software development lifecycle: A systematic mapping study," Computer Standards & Interfaces, vol. 50, pp. 107-115, 2017/02/01/ 2017.

[R2] Y. Mufti, M. Niazi, M. Alshayeb, and S. Mahmood, "A Readiness Model for Security Requirements Engineering," IEEE Access, vol. 6, pp. 28611-28631, 2018