IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 19, 2022, accepted May 27, 2022, date of publication June 2, 2022, date of current version June 23, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3179822

Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach

ABDUL WAHID KHAN[1], SHAH ZAIB[1], FAHEEM KHAN[2], ILHAN TARIMER[3], JUNG TAEK SEO[2], AND JIHO SHIN[4]

[1]Department of Computer Science, University of Science and Technology Bannu, Khyber Pakhtunkhwa 28100, Pakistan
[2]Department of Computer Engineering, Gachon University, Seongnam 13120, South Korea
[3]Department of Information Systems Engineering, Mugla Sitki Kocman University, 48000 Mugla, Turkey
[4]Police Science Institute, Korea National Police University, Asan 31539, South Korea

Corresponding authors: Faheem Khan (faheem@gachon.ac.kr) and Jung Taek Seo (seojt@gachon.ac.kr)

This work was supported in part by the Nuclear Safety Research Program through the Korea Foundation of Nuclear Safety (KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission (NSSC), Republic of Korea, under Grant 2101058; in part by the Institute of Information and Communications Technology Planning and Evaluation (IITP) through the Korea Government (MSIT) under Grant 2021-0-00493; and in part by the 5G Massive Next Generation Cyber Attack Deception Technology Development.

ABSTRACT Security is the protection from various kinds of threats and most organizations engage in the challenge of security especially cyber-attacks. The attacks are increasing rapidly, due to which cyber security does not now change on supervised and pattern-based detection algorithms which assure continuous security observing. There are many kinds of problems in vendor organizations like cyber theft, which is the most common attack in cyberspace. This research study is developing a Cyber Security Challenges Model (CSCM) that will facilitate vendors' organizations to identify challenges of cyber security during the development of software in a vendor organization. To find cyber security issues/challenges, a Systematic Literature Review (SLR) is conducted on 44 relevant research publications by developing a search string based on research questions. As the final selected research publications were less in number and did not complete our aim, therefore, snow bowling technique is applied to 67 relevant research publications. This relevant data was comprised of different databases/sources e.g., Google Scholar, IEEE Explore, SpringerLink, ACM Digital Library, anFffid ScienceDirect. Furthermore, for the distinctive literature review, we've carried out all of the steps in SLR, for example, improvement of SLR protocol, initials, and a very last collection of the applicable information, data extraction, data quality assessment, and data synthesis. Thirteen (13) critical cyber security challenges are identified which are; "Security issues/Access of Cyberattacks", "Lack of Right Knowledge", "Framework", "Lack of Technical Support", "Disaster Issues", "Cost Security issues", "Lack of Confidentiality and Trust", "Lack of Management", "Unauthorized Access issues", "Lack of Resources", "Lack of Metrics", "Administrative Mistakes during Development" and "Lack of Quality, Liability, and Reliability". The findings of our analysis study signify the similarities and dissimilarities in the recognized cybersecurity challenges in different decades, companies/firms, continents, databases, and methodologies.

INDEX TERMS Cybersecurity, challenges, SLR, vendor, software development, SPSS.

I. INTRODUCTION

In the digital world, the identification of security threats is the most important issue and it needs thorough information related to security-based technologies [1]. For companies and organizations, security can be discussed in various forms like computer security, information security, cyber security, etc. [2]. Information security is defined as "the preservation of particulars/information and its analytic components, comprising of the systems and hardware that use, reserve, and impart that particulars/information" [3]. Information Security is a process neither a technology nor a product [4].

The associate editor coordinating the review of this manuscript and approving it for publication was Porfirio Tramontana.

Either more and more information security is not an undisputed idiom [5]. Hardly any of the documentation appears to formulate a difference between the theory of cyber security and information security or the correlation between them. For Small and Medium Enterprises (SMEs) ''information security'' can turn out to be an important matter and many times used as cyber security [6].

Nowadays organizations encounter difficulty to protect themselves from potential cyber-attacks [7]. The International Telecommunications Union (ITU) defines cyber security as:

Cyber Security is the collection of instruments, strategies, security concepts, suggestions, measures, instructions, and technologies that could be useful while safeguarding the cyber environment, firm, and user resources. Cyber Security [8] is turning out to be important stuff of worldwide attentiveness and significance. The cyber violations that took place at Small Medium Enterprises (SMEs) are nearly 72%. This is why at some layers SMEs require security services [9]. With obvious and shared characteristics, IT security commonly concentrated on guarding networked computer resources/assets [10]. To oppose the threats of cyber-attacks Cyber security advocates, try to encourage security top applications and the acquisition of security technology [11].

Cybersecurity is a computing-based discipline that in the presence of challenges and threat line up resources of the network and human and processes to corroborate ''Assured Operation''. Nowadays, cybersecurity has turned out to be one of the most severe financial and nationwide security issues [12]. Due to the fact, that the internet provides the phantasm – and, every so often, the fact – of anonymity, those wishing to pursue criminal hobbies discover the net as a secure and resourceful ground for their efforts. One of these activities enabled through the Internet and the modern-day World Wide Web (from time to time cited as ''internet 2.0''), is cyberstalking [13].

DoS transmissions also can be applied to execute far-flung records spoofing from random factors. An attacker should assemble malicious streams of message records to shape all subscriber pastimes that could be dispatched to the DCS service event for advertising. Subsequent subscribers might then unknowingly take delivery of the malicious packets through relied-on DCS event services. The 2007 cyber assaults on Estonia consisted of DDoS assaults that crippled the country's banks and parliament capabilities. The assaults concerned ping floods and the ''botnet'' era such that the DDoS assault technique changed into a complexity now no longer visible before. Researchers and navy planners concur that the coaching at the back of the DDoS assaults has been the second-biggest example of state-backed cyber warfare [14].

In a hit attack, the loss to the victim (the metropolis and its citizens) and the advantage to the hacker may be notably asymmetric, with the loss in large part exceeding the advantage [15]. According to records from the Russian facts protection certification system, approximately one 1/3 of the portions of the software program examined exhibited vulnerabilities at some stage in a two-12 months study [16]. The vulnerability might be a code flaw this is intentional or unintended and won't appear to be malicious code [17].

Instead of seeking to create whole completely proven PC systems, maximum developers simply recognize on verifying smaller, vulnerable, or important portions of a system. As long as those people stay careless and unaware approximately their position in enhancing cybersecurity, the country of cybersecurity will stay weak [18].

Based on the survey performed with the aid of using Symantec which interviewed 20,000 humans throughout 24 countries, 69% mentioned being the sufferer of a cyber-attack in their lifetime. Symantec calculated those 14 adults come to be the sufferer of a cyberattack each second or greater than a million assaults each day, and not limited to geography and distance [19].

The international availability of the Internet permits cyber-criminals to release attempts on each machine additive from anywhere, at any place, at any time. Nevertheless, one of the maximum complex elements of cybersecurity is the quick and continuously evolving nature and due to this fact cyberattacks have become greater in the capacity to unfold in a rely of seconds [20].

To deal with cyber security issues/challenges, a research question is designed as:

RQ1. What are the cyber security issues faced by vendor organizations in software development that have a negative impact on the software industry?

Keeping in view the above research question, we find out 13 critical cybersecurity challenges from the final selected 67 research articles for the proposed SLR study. The results validate the resemblances and differences in the identified critical cybersecurity challenges in different periods, continents, organizations, databases, and methods.

This paper consists of the following sections: Section II describes the related work of cyber security challenges to vendor organization; Section III describes the SLR methodologies with primary, secondary, and final selection; Section IV describes the findings of the SLR and the analysis of results. Section V describes the limitations of this study and Section VI describes the conclusion of this paper.

II. RELATED WORK

The characteristics of threats, vulnerabilities, and resources in cyber security are different from information security. All security is concerned with numerous risks of resources [8]. Technical knowledge and skills are important in cyber security but in addition to these two, a successful cyber security promoter is the one who should be aware of the context [11].

The authors [7] suggest a model having distinct information about cyber security that could be executed whichever vulnerability is stated. Cyber security must be related to information or resources but also a person(s) who is using these resources in the cyber environment [8]. Common reasons for cyber-attacks are; ease to access, capacity to store data in comparatively small space, loss of evidence, etc. The existing models are signature-based, which is easy for the attacker to launch an attack by minor changes in this syntactical illustration of the signature [21]. In 2016, at least 255,100 phishing attacks occurred worldwide [22].

If every enterprise ensures its security to maximize its internet benefit, then the distribution of charges and benefits may be distributed [23]. Organizations create a secure system that helps to improve and preserve the behavior of the professional workers and employees who lack an organizational system due to poor performance in daily progress [24].

Many incidents have concerned the removal of malware rights, along with the unencrypted USB tool, or violating processes concerning outside email. Cyber-attackers have often penetrated well-designed, steady user structures by taking benefit of the carelessness of individuals, or with the aid of using intentionally deceiving them, for example with the aid of using pretending to be the gadget administrator and inquiring for passwords [25].

On the internet, a vast scale of possible unlawful activities is included through cyber security threats. Primarily ''cybercrimes'' are split into three main groups: (i) cybercrimes against the person (ii) against all property formations and (iii) against Government. A vast range of law activities is encompassed through [8]–[21] Cyber Theft, Software Piracy, Cyber Terrorism, Spam, Stealing Credit Card information, Denial of service, Cyber Bullying, Digital media. Computer as the Target: theft of property, theft of advertising facts (e.g., purchaser list, pricing data, or advertising plan), and blackmail primarily based on facts received from automated files (e.g., clinical facts, non-public history, or sexual preference) [26]. One of the problems that managing safety is to offer a proper assessment of various safety plans, and estimate expenses and benefits of technology while not having real data [27].

Cybercrimes are divided into three basic classifications like emails that bother someone, the use of different kinds of spyware software to break into other's computers unlawfully, and plagiarizing confidential data, due to its government suffering like violations into the website. It causes the loss of millions of dollars to organizations. After reviewing the literature on this area, there may be no category of attacks or the underlying techniques to execute the attacks [28].

To perform an attack, the attacker wishes to understand little professional behavior to understand the protocols used to transfer the messages [29]. If clients can't distinguish between a well-built and a secure product, the enterprise product gets to the marketplace first, and feature an advantage [30]. It is not possible to react timely if the response does not know the nature of the attack [31].

If this problem is not corrected timely, then the abnormal effects of cybercrimes will the whole society, businesses, and research community [32]–[34].

III. METHODOLOGY

In SLR, the searching of relevant issued composition is done with the support of a pre-defined search string that's grounded on the study questions. For the analysis of gathered data, a pre-defined criterion of SLR for insertion/removal has been used. As per Kitchenham [35], the Systematic Literature Review (SLR) has three phases i.e. planning, conducting, and reporting. The trustworthiness of the SLR outcomes is higher than the common literature review because SLR imitates an approach of organized assessment. To recognize the cyber security issues/challenges by SLR, a step-by-step process has been followed. In this process, a paper is selected on its relation to the subject matter or search string. To eliminate the unimportant articles from selected research papers of our search systematically, an inclusion/exclusion criterion has been applied. Next, the relevant data is extracted from the selected papers through the data extraction process and then the quality of the publication process is carried out. This article aims to highlight all the cybersecurity issues/challenges with the help of SLR that are faced by vendors organizations during software development.

Through SLR, we have found thirteen (13) critical issues/barriers as shown in Table 2, confronted by vendor organizations in software development in the shape of cyber security, and these challenges are identified through SLR.

A. SEARCH PROCESS

We follow the following procedure to make the search string for SLR.

- Identification of outcomes, population, and intervention for a search string.
- To identify synonym words for the search string.
- Validation and verification for keywords in the relevant literature.
- Use of Boolean operators for precise output.

Initially, a search string is designed on a trial basis to apply to different digital libraries/search engines to recognize the related research papers. The trial search was conducted on five databases/search engines i.e., Google Scholar, ACM, IEEE Explore, SpringerLink, and ScienceDirect. Different results are collected from different databases through trial search but their precision is less. The trail search string is given below:

((''Software development'') AND (''Cybersecurity'') AND (vendor) AND (Challenges) AND (practices))

The results of the trial search string were not satisfactory; therefore, we have developed a final search.

The final search string mentioned above was short in length for ScienceDirect to search relevant papers because ScienceDirect does not support lengthy strings. The final search string for ScienceDirect is mentioned below: ((''Software development'' OR ''software evolution'' OR ''software maturing'') AND (''Cybersecurity'' OR ''cyber risks'' OR ''IT security'') AND (supplier OR trader) AND (issues OR problems)).

TABLE 1. Period wise list of challenges.

Name of Database	Search Result	Primary Selection	Final Selection
Google Scholar	13900	81	37
IEEE	55	02	00
SpringerLink	2074	33	03
ACM	398	22	00
ScienceDirect	4795	31	04
Total	**21222**	**169**	**44**
After selecting 23 papers in Snow Bowling Technique (Total)			**67**

The exploration outcomes of related papers are developed by applying the concluded search string are shown in Table 1.

An insertion/removal criterion has been used in the conclusive selection of the research papers as demonstrated in Table 1, we have used the inclusion/exclusion criterion. In this process, we have selected the relevant articles on quality of paper and verification through reading.

IV. FINDINGS

This segment shows the results thoroughly acquired through SLR.

A. CHALLENGES/BARRIERS/ISSUES FIND THROUGH SYSTEMATIC LITERATURE REVIEW

To answer RQ.1, we have recognized critical cybersecurity challenges for vendors companies by expository analyzing research articles reviewed via SLR as shown in Table 1. ‘‘Security issues/access of cyber-attacks’’ means that cyber-attacks and cyber-crimes are increasing day by day and fatally defecting the systems. Each year cyber-attacks are growing continuously and cyber threats are turning out to be harmful, diverse, and troublesome [12].

Another critical challenge in a study is the ‘‘lack of right knowledge’’−48%. ‘‘Lack of right knowledge’’ means a lack of knowledge about intellectual property rights/property right acts, products, and policies of the software. Azeez Nureni Ayofe and Osunade Oluwaseyifunmitan stated the nature of cybercrime for citizen’s privacy breaches [36].

Another critical challenge is ‘‘framework’’−48%. ‘‘Framework’’ means lack of network computer protection, the vulnerability of network, web browsers, and framework illustrated to attacks. Vagoun and Strawn [37] discussed that ‘‘At the onset, to achieve transformational results, the research framework not only had to focus on root causes, but it also had to unite expertise from a range of disciplines that would reflect technological and social aspects of cybersecurity’’.

Another identified critical challenges are the ‘‘lack of technical support’’ whose frequency percentage is equal to 43%. ‘‘Lack of technical support’’ means deficiency or lack of professional and training skills e.g., one person who is developing software but doesn’t have professional skills of development then must perform extreme mistakes in development which makes the software vulnerable to cyber-attacks. Cao and Ajwa [12] suggested that it is helpful to get essential training on cybersecurity issues for those who work in business or government with information systems.

‘‘Disaster issues’’−40% is identified as another critical challenge. ‘‘Disaster issues’’ means that the system/software causes disaster and is unable to protect, prevent and detect cyber-attacks/vulnerabilities. Chinese Academy of Cyberspace Studies [22] stated that the malfunction may become disastrous for e-government, e-commerce, and online business [13].

Another critical challenge is ‘‘cost security issues’’−39%. ‘‘Cost security issues defines as’’ the serious economic, investment, and financial issues faced by any vendor organization. In [38], almost 431 million users are victimized and their financial lost increases to 388 billion dollars.

‘‘Lack of confidentiality and trust’’−37% is another critical challenge identified by us. ‘‘Lack of confidentiality and trust’’ means that lack of human trust, confidentiality, integrity, and noncompliance makes the vendor organizations more vulnerable to attacks. In [39] stated that the increase in security vulnerabilities and hacking attacks are causing the loss of human trust.

Another critical challenge, we identified is ‘‘lack of management −33%. ‘‘Lack of management’’ means a lack of focus on requirements, management problems, protection from vulnerabilities during software development, and the careless and unconstrained behavior of the developer. It [40], is argued that during software development processes an unintentional information security threat can be caused by the software developer due to incompetent actions or negligence.

Our results also identified ‘‘unauthorized access issues’’ 31% as a critical challenge. This challenge can get access to information without authentication or a necessary process, and also there is a lack of detection of the source from where this unauthorized action is taking place. In [39] it is compared to an outside attacker but the malicious attacker is more harmful to an organization and has the advantage to give more potential damage to that organization.

‘‘Lack of resources’’ is another critical challenge, we identified i.e., 28%. ‘‘Lack of resources’’ means non-availability of the right resources at the time of emergency and or not used at the right place and time. Vagoun and Strawn [37] stated that misallocation of resources may be happened because of economically stable decision-making in security.

In our findings, another critical challenge is the ‘‘Lack of metrics’’− 28%. By this challenge, we mean meaningful metrics, proactive cybersecurity measures, and lack of impact or bad impact issues on software or in software development. Chinese Academy of Cyberspace Studies [22] discussed that DDoS attacks may be small in number but they have a greater impact. This paper [41] argued that ‘‘The cause of DoS could be something simple; for instance, a DoS attack could interrupt an Internet-facing server that feeds data to a couple

TABLE 2. List of identified challenges based on organization size.

S.No	Challenges in CSCM	Frequency (N=67)	Percentage of factors occurrence
A	Security Issues/Access of Cyber Attacks	39	58
B	Lack of Right Knowledge	32	48
C	Framework	32	48
D	Lack of Technical Support	29	43
E	Disaster Issues	27	40
F	Cost Security Issues	26	39
G	Lack of Confidentiality and Trust	25	37
H	Lack of Management	22	33
I	Unauthorized Access Issues	21	31
J	Lack of Resources	19	28
K	Lack of Metrics	19	28
L	Administrative Mistakes during Development	18	27
M	Lack of Quality, Liability, and Reliability	17	25

of systems and this would have a big impact on regular city services and activities''.

''Administrative mistakes during development''–27% is one more critical challenge in the identified list of challenges. ''Administrative mistakes during development lead to loss of reputation of an organization. One foremost cause for poor cybersecurity is extant vulnerabilities in popular software products [18].

The last critical challenge in the identified list of challenges is ''lack of quality, liability, and reliability''–25%. By this challenge, we mean non-availability of quality, liability, and reliability in vendor organizations during software development. Li and Liao [15] suggested that two major characteristics are involved in the quality of a product i.e., its resistance to cyber-attacks and its functionality to provide reliable services. It is found that in the early stages of product development, most of the vulnerabilities are functional, then management functionalities start to appear and finally become the mainstream.

B. ANALYSIS OF THE CYBER SECURITY CHALLENGES IDENTIFIED THROUGH SLR FOR VENDOR ORGANIZATIONS

The findings of SLR are presented on different variables through statistical analysis of the identified challenges. These variables consist of continents, period, and size of the organization. This analysis shows whether the mentioned thirteen challenges remain stable throughout the continent, period, and organization size.

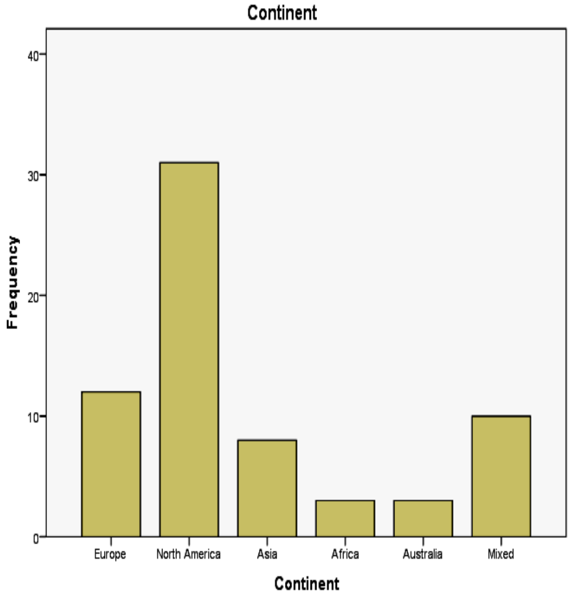

FIGURE 1. Conclusive number of articles among different continents recognized through SLR.

1) ANALYSIS OF THE CYBER SECURITY CHALLENGES IDENTIFIED THROUGH SLR FOR CONTINENTS

Different challenges in different continents through SLR [41]–[43] are shown in Table 3. The number of research papers found in various continents is shown in Figure 1. In this research, challenges have been identified after a comparison of six continents/categories i.e., Europe, North America, Asia, Africa, Australia, and Mixed. The goal of our research is to find whether these identified challenges are different from one another in various continents or remain the same/constant/uniform. We had created the data set in SPSS, which contains the data type as ordinal. To find the significant difference in various continents between the identified challenges, we have used Chi-square Test (linear by linear association). This [45] stated the comparison of Chi-square linear by linear association with Pearson Chi-square and shows that the former is more effective than the latter and therefore the fore is preferred for testing the significant difference between ordinal variables.

In Table 3, the result shows more similarities than differences amongst the challenges over various continents. As shown in Table 3, the total number of challenges cited in various continents are cited in Europe, North America and Mixed is 13, challenges cited in Asia & Africa are 11, and challenges cited in Australia are 10. ''Lack of quality, liability, and reliability'' is the only challenge that has zero occurrences in three continents i.e., Asia, Africa, and Australia, while the other challenges have no occurrences in one continent i.e., ''lack of resources'' in Asia, ''disaster issues'' in Africa and ''cost security issues'' and

TABLE 3. continents wise list of challenges.

Challenges	Sample Size find through SLR (N=67)											Chi-Square Test (Linear-by-Linear Association) α = .05			
	Europe (N=12)		North America (N=31)		Asia (N=8)		Africa (N=3)		Australia (N=3)		Mixed (N=10)	X^2		df	P
	Fr eq.	%	Freq.	%	Freq.	%	Fre q.	%	Freq.	%	Freq.	%	Freq.		
Security Issues of Cyber Attacks	6	50	19	61	5	62.5	2	67	2	67	5	50	.011	1	.918
Lack of Right Knowledge	6	50	15	48	1	12.5	3	100	1	33	6	60	.291	1	.590
Framework	7	58	14	45	4	50	2	67	2	67	3	30	.629	1	.428
Lack of Technical Support	6	50	16	52	2	25	1	33	1	33	3	30	1.834	1	.176
Disaster Issues	**4**	**33**	**11**	**36**	**2**	**25**	**0**	**0**	**1**	**33**	**9**	**90**	**6.148**	**1**	**.013**
Cost Security Issues	2	17	14	45	4	50	1	33	0	0	5	50	.408	1	.523
Lack of Confidentiality and Trust	4	33	9	29	5	62.5	2	67	1	33	4	40	.577	1	.447
Lack of Management	4	33	9	29	2	25	1	33	1	33	5	50	.970	1	.325
Unauthorized Access Issues	2	17	10	32	3	37.5	1	33	1	33	4	40	.919	1	.338
Lack of Resources	1	8	12	39	0	0	2	67	2	67	2	20	.173	1	.677
Lack of Metrics	1	8	11	36	2	25	1	33	0	0	4	40	.554	1	.457
Administrative Mistakes during Development	3	25	9	29	2	25	1	33	1	33	2	20	.081	1	.777
Lack of Quality, Liability, and Reliability	5	42	8	26	0	0	0	0	0	0	4	40	.109	1	.742

'lack of metrics' in Australia. A single difference in "disaster issues" throughout the six continents is identified in Table 3. This challenge has the following percentages in six continents/categories i.e., Europe (33%), North America (36%), Asia (25%), Africa (0%), Australia (33%), and Mixed (90%). According to Table 3, this challenge has zero percentage/occurrence in continent Africa while having the highest percentage in Mixed continents, which means that "disaster issues" are considered more critical for Mixed continents than the other five continents.

2) ANALYSIS OF THE CYBER SECURITY CHALLENGES IDENTIFIED THROUGH SLR, BASED ON PERIODS

Table 4 presents a list of challenges period-wise. The variation of challenges is shown over time and considered in two periods from 2001-2010 and 2011 to 2020. To understand the significant difference between the two periods, a linear-by-linear association chi-square test is used. The number of research papers found in two decades is represented in Figure 2.

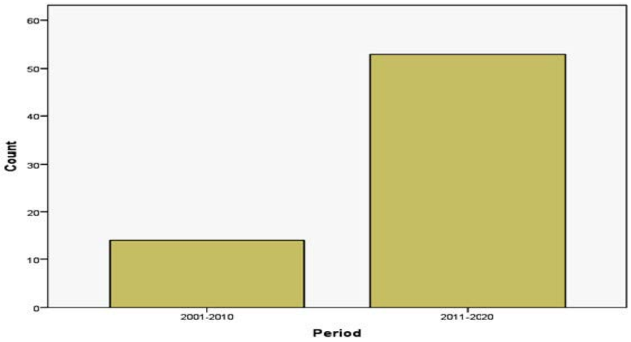

FIGURE 2. Conclusive number of articles from two decades, recognized through SLR.

A total of 13 challenges have been identified for both periods. As both periods present 13 challenges, hence no changes occur in all the challenges over two periods as represented in Table 4. However, the identified challenges have variations in their frequencies as shown in Table 4. As we have identified 13 challenges based on critical challenges identification criteria, so, the challenge "security issues/access of cyber-attacks" (43%,62%) is considered the most critical challenge in both periods. A sudden increase is observed in the second period, it shows that software vendor organizations have not taken it seriously and do not take any profitable steps to overcome this challenge. Due to this non-serious behavior of the software vendors' organizations, this challenge is now critical and needs to be considered as a serious issue to overcome its rapid increase. Nathaniel J. Fuller and Greg Simco [14] identified that in 2003, a DDoS attack was launched by hackers against eBay's web services. About 20,000 computers or 'bots' control has been acquired by the hackers and the attacks were launched from different locations and identities. The "lack of right knowledge" (71%,42%) is also considered a critical challenge in cybersecurity challenges in the two periods. The decrease in challenges in the second period shows the seriousness and priority of software vendor organizations towards the second period.

This paper [46] argued that "This is problematic because any business that wants to have a competitive edge in today's global marketplace should adopt a comprehensive security policy in consultation with partners, suppliers, and distributors".

TABLE 4. Period wise list of challenges.

Challenges	Sample Size find through SLR (N=67)				Chi-Square Test (Linear-by-Linear Association) α = .05		
	Period						
	2001-2010 (N=14)		2011-2020 (N=53)		X^2	df	P
	Freq.	%	Freq.	%			
Security Issues/Access of Cyber Attacks	6	43	33	62	1.689	1	.194
Lack of Right Knowledge	10	71	22	42	3.914	1	.048
Framework	6	43	26	49	.168	1	.682
Lack of Technical Support	3	21	26	49	3.392	1	.066
Disaster Issues	**10**	**71**	**17**	**32**	**7.022**	**1**	**.008**
Cost Security Issues	8	57	18	34	2.469	1	.116
Lack of Confidentiality and Trust	4	29	21	40	.570	1	.450
Lack of Management	3	21	19	36	1.029	1	.310
Unauthorized Access Issues	6	43	15	28	1.074	1	.300
Lack of Resources	2	14	17	32	1.699	1	.192
Lack of Metrics	4	29	15	28	.000	1	.984
Administrative Mistakes during Development	4	29	14	26	.026	1	.872
Lack of Quality, Liability, and Reliability	**8**	**57**	**9**	**17**	**9.293**	**1**	**.002**

Some of the challenges are considered critical challenges within the two periods by vendors organizations during software development i.e., "disaster issues" (71%, 32%), "cost security issues" (57%, 34%), "unauthorized access issues" (43%,28%), "lack of metrics" (29%, 28%), "managerial blunders" (29%, 26%). The decrease in challenges in the second period shows the seriousness and priority of software vendor organizations towards the second period. This is the reason that vendors organizations/software industry has learned to handle (avoid/mitigate) these challenges for successful software development without any cybersecurity issues. This paper [15] identified that it is a great achievement that lifestyle in cities is changing by using smart technologies but the main drawback is that these technologies have made the cities possible victims of cyberattacks. This paper [38] stated that in 2011, approximately US$114 billion of cybercrime is performed in 24 different countries. This paper [47] stated that an exceptional skill of cyberattacks affects user or business systems very badly and it was suggested that those organizations have also taken strict actions to prevent and detect attacks.

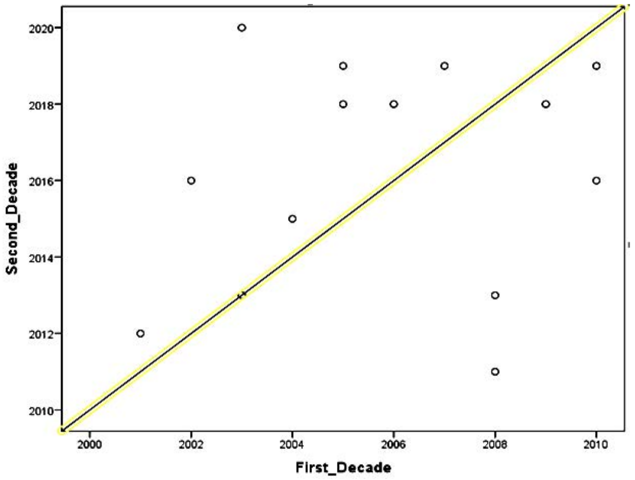

FIGURE 3. Scatter diagram.

While the other challenges i.e., "framework" (43%, 49%), "lack of technical support" (21%, 49%), "lack of confidentiality and trust" (29%,40%), "lack of management" (21%, 36%) and "lack of resources" (14%, 32%) have increased in the second period which means that these challenges have not been considered as critical in the first period due to which it has emerged as critical in the second period. Roman L. Hund, Lt Col, USAF [17] suggested that to acquire further restrictive information, the attacker may use a keylogger that records passwords, access bank accounts or log into virtual private networks. This paper [13] suggested that in cyberspace the wide usage of social networking sites in which communication can turn out to be very private even though the actors have never met individual.

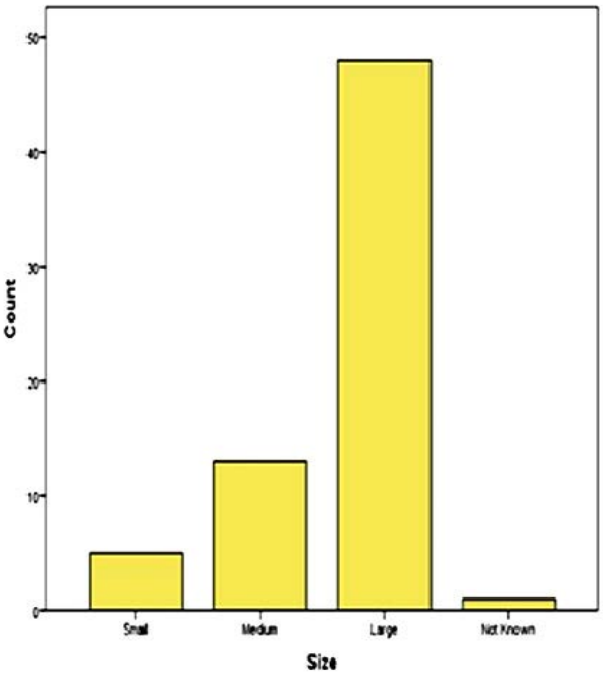

FIGURE 4. The final collection of papers from different organizations sized.

We have found that two challenges "disaster issues" and "lack of quality, liability, and reliability" were significantly different between the two periods. Both the challenges have a high percentage of occurrence in the first period and then it was reduced to a low level in the second period. That might be the reason that software vendors organizations have taken these challenges very seriously and it was reduced to such a level in the second period. A Spearman's rank [47] correlation coefficient is performed to compare the relationship between the first and second periods. it is found that the correlation coefficient between the first and second periods is 0.157 and shows a strong relationship. This relationship is represented in Figure 3 by using a scatter diagram.

3) SUBFIGURE LABELS IN MULTIPART FIGURES AND TABLES

In this research paper, a sample size of 67 papers is used and in 66 papers organization size is shown in Table 5 and Figure 4. For finding the organization size, the Australian Bureau of Statistics is followed. According to this categorization, an organization with <=19 employees will be considered as a small size organization and with greater than 19 but less than 199 will be considered a medium-size organization. An organization that has greater than 199 employees will be considered a large size organization. One more category is named 'Not Known'.

The challenges of cybersecurity with high-frequency percentages >=38 are a total of 06 in numbers. Our analysis reveals that for medium-sized organizations total of four barriers are cited in >=46% of papers with 13 cybersecurity issues. These four cybersecurity challenges are "lack of right knowledge –54%", "disaster issues –54%", "cost security issues –54%", and "security issues/access of cyberattacks –46%". Cybersecurity challenges for medium-sized organizations are "lack of right knowledge", "disaster issues", "cost security issues" and "security issues/access of cyberattacks" which have the highest percentages (54, 54, 54, and 46) respectively. For sustainability and good relationships with the clients, the medium-size organization should concentrate on the following challenges.

The results show that 09 challenges are cited in >=40% of papers with 13 cybersecurity challenges in small-size organizations. These nine challenges are "lack of right knowledge –80%", "security issues/access of cyber-attacks – 60%", "administrative mistakes during development –60%", "framework –40%", "lack of technical support –40%", "disaster issues –40%", "cost security issues –40%", "lack of management –40%" and "lack of quality, liability, and reliability –40%".

The results show that the challenges with the highest percentages for small size organizations are "lack of right knowledge", "security issues/access of cyber-attacks", "administrative mistakes during development", "framework", "lack of technical support", "disaster issues", "cost security issues", "lack of seriousness" and "lack of quality, liability, and reliability" (80%, 60%, 60%, 40%, 40%, 40%, 40%, 40%, 40%) respectively. For sustainability and good relationships with the clients, medium-size organizations should concentrate on the following challenges.

Our results specify that "security issues/access of cyber-attacks", "lack of right knowledge" and "disaster issues" are the critical challenges for all large, medium, and small size organizations. There is no significant difference among all 13 identified challenges. Amongst the various organization sizes, the linear-by-linear Chi-square test has been used for the recognition of statistically notable variations. Chi-square linear-by-linear association test acquires considerable divergences amongst all 13 identified cybersecurity challenges based on various organization sizes. As revealed by the Literature this test is desired to be the best and more dominant than the Pearson chi-square test when testing the differences between ordinal variables [45].

The statistical comparison of different organization sizes has been got through Anova One Way Factor, which is shown in Table 6 and its graph is illustrated in Figure 5.

V. LIMITATIONS

As far as limitation is concerned, the authors of a lot of these studies research have been now not purported to report the sincere reasons why these cybersecurity challenges/issues are faced by way of vendor organizations and also have a negative impact on the software program enterprise in the context of software program development. It may be that most people of research studies were literature assessment, surveys, and case research which may be similarly concern to publication bias. Google Scholar shows 13900 search results but very few are accessible only.

TABLE 5. List of identified challenges based on organization size.

Challenges	Sample Size find through SLR (N=67)								Chi-Square Test (Linear-by-Linear Association) α = .05		
	Organization Size										
	Small (N=05)		Medium (N=13)		Large (N=48)		Not Known (N=01)		X^2	df	P
	Freq.	%	Freq.	%	Freq.	%	Freq.	%			
Security Issues/Access of Cyber Attacks	3	60	6	46	29	60	1	100	.658	1	.417
Lack of Right Knowledge	4	80	7	54	21	44	0	0	3.206	1	.073
Framework	2	40	5	39	25	52	0	0	.138	1	.711
Lack of Technical Support	2	40	5	39	21	44	1	100	.576	1	.448
Disaster Issues	2	40	7	54	18	38	0	0	.867	1	.352
Cost Security Issues	2	40	7	54	16	33	1	100	.099	1	.753
Lack of Confidentiality and Trust	1	20	3	23	21	44	0	0	1.113	1	.291
Lack of Management	2	40	5	39	13	27	0	0	.650	1	.420
Unauthorized Access Issues	1	20	4	31	16	33	0	0	.051	1	.821
Lack of Resources	1	20	3	23	14	29	1	100	1.392	1	.238
Lack of Metrics	0	0	5	39	14	29	0	0	.145	1	.703
Administrative Mistakes during Development	3	60	2	16	13	27	0	0	.917	1	.338
Lack of Quality, Liability, and Reliability	2	40	5	39	10	21	0	0	2.306	1	.129

TABLE 6. Anova one way factor statistical comparison of different organization sizes.

ANOVA						
		Sum of Squares	df	Mean Square	F	Sig.
Small	Between Groups	114.133	2	57.067	6.114	0.141
	Within Groups	18.667	2	9.33		
	Total	132.800	2			
Medium	Between Groups	114.731	3	38.244	2.287	0.147
	Within Groups	150.500	9	16.722		
	Total	265.231	12			
Large	Between Groups	76.242	3	25.414	1.181	0.329
	Within Groups	882.336	4	21.520		
	Total	958.578	44			

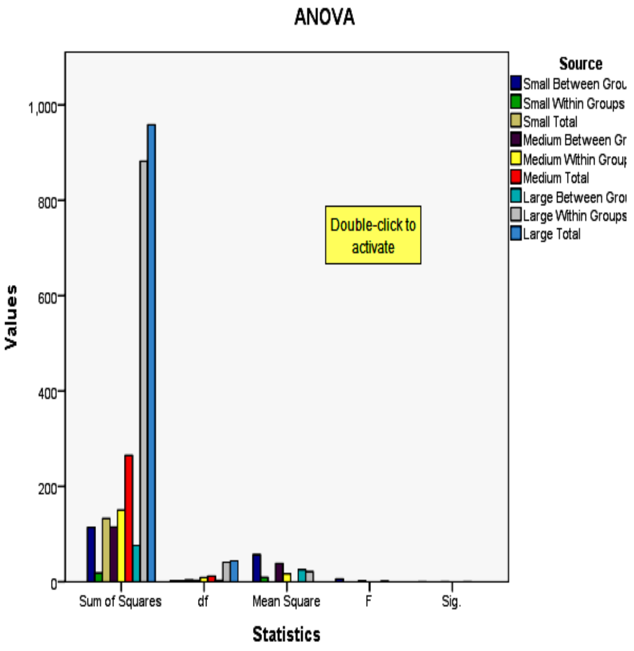

FIGURE 5. Graph representation of anova one way factor.

As there is a small ratio of work done in the field, we are doing research that's why we have found only 44 papers as our final sample for the data extraction in this study, which is very low in numbers and we were not able to get our required results. So, we have conducted a snow bowling technique and got 67 papers as our final sample for data extraction which is nearly an appropriate number to get our required results.

VI. CONCLUSION AND FUTURE WORK

Through SLR, we have identified a list of 13 challenges which are all marked as critical challenges for vendor organization during software development in CSCM as shown in Table 2. These 13 challenges are "A (58%)", "B (48%)", "C (48%)", "D (43%)", "E (40%)", "F (39%)", "G (37%)", "H (33%)", "I (31%)", "J (28%)", "K (28%)", "L (27%)" and "M (25%)". The vendor organizations need to give proper attention to these critical challenges to avoid any risk of failure by addressing these challenges.

We have further analyzed the identified challenges across the continents, periods, and organization size which are discussed above in detail.

Furthermore, we also intended to find the practices for these critical cyber security challenges and will try to help the vendor organizations through these identified practices.

REFERENCES

[1] W. A. Conklin, R. E. Cline, and T. Roosa, "Re-engineering cybersecurity education in the U.S.: An analysis of the critical factors," in *Proc. 47th Hawaii Int. Conf. Syst. Sci.*, Jan. 2014, pp. 2006–2014.

[2] M. Kazemi, "Evaluation of information security management system success factors: Case study of municipal organization," *Afr. J. Bus. Manage.*, vol. 6, no. 14, pp. 4982–4989, Apr. 2012.

[3] M. E. Whitman and H. J. Mattord, *Principles of Information Security*. Boston, MA, USA: Cengage Learning, 2011.

[4] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*, 2002.

[5] M. Schaake and M. Vermeulen, "Towards a values-based European foreign policy to cybersecurity," *J. Cyber Policy*, vol. 1, no. 1, pp. 75–84, Jan. 2016.

[6] F. Giubilo, A. Sajjad, M. Shackleton, D. W. Chadwick, W. Fan, and R. de Lemos, "An architecture for privacy-preserving sharing of CTI with 3rd party analysis services," in *Proc. 12th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2017, pp. 293–297.

[7] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decision Support Syst.*, vol. 86, pp. 13–23, Jun. 2016.

[8] R. von Solms and J. van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013.

[9] P. H. Meland, I. A. Tondel, and B. Solhaug, "Mitigating risk with cyberinsurance," *IEEE Secur. Privacy*, vol. 13, no. 6, pp. 38–43, Nov. 2015.

[10] L. Maglaras, K. H. Kim, H. Janicke, M. A. Ferrag, S. Rallis, P. Fragkou, A. Maglaras, and T. J. Cruz, "Cyber security of critical infrastructures," *ICT Exp.*, vol. 4, no. 1, pp. 42–45, 2018.

[11] J. M. Haney and W. G. Lutters, "Skills and characteristics of successful cybersecurity advocates," in *Proc. SOUPS*, 2017.

[12] P. Y. Cao and I. A. Ajwa, "Enhancing computational science curriculum at liberal arts institutions: A case study in the context of cybersecurity," *Proc. Comput. Sci.*, vol. 80, pp. 1940–1946, Jan. 2016.

[13] P. R. Stephenson and R. D. Walter, "Toward cyber crime assessment: Cyberstalking," in *Proc. 6th Annu. Symp. Inf. Assurance (ASIA)*, 2011.

[14] N. J. Fuller and G. Simco, "Software and CyberSecurity: Attack resistant secure software development survivable distributed communication services (DCS)," in *Proc. IEEE Conf. Technol. Homeland Secur.*, May 2008, pp. 599–602.

[15] Z. Li and Q. Liao, "An economic alternative to improve cybersecurity of E-government and smart cities," in *Proc. 17th Int. Digit. Government Res.*, Jun. 2016, pp. 455–464.

[16] R. Ruiz, "A study of the U.K. Undergraduate computer science curriculum: A vision of cybersecurity," in *Proc. IEEE 12th Int. Conf. Global Secur., Saf. Sustainability (ICGS3)*, Jan. 2019, pp. 1–8.

[17] R. L. Hund, "Acquisition regulations and offshore software development: Implications for cybersecurity of DOD networks," Air War College Air Univ., Maxwell AFB, AL, USA, Tech. Rep., 2013.

[18] R. Sen, "Challenges to cybersecurity: Current state of affairs," *Commun. Assoc. Inf. Syst.*, vol. 43, no. 1, pp. 22–44, 2018.

[19] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, 2013.

[20] D. P. Möller and R. E. Haas, "Automotive cybersecurity," in *Guide to Automotive Connectivity and Cybersecurity*. Springer, 2019, pp. 265–377.

[21] A. Razzaq, A. Hur, H. F. Ahmad, and M. Masood, "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications," in *Proc. IEEE 11th Int. Symp. Auton. Decentralized Syst. (ISADS)*, Mar. 2013, pp. 1–6.

[22] *Development of the World Cyber Security*, CAOC Studies, World Internet Develop. Report, Translated by Peng Ping, 2019, pp. 89–117.

[23] R. Rue, S. L. Pfleeger, and D. Ortiz, "A framework for classifying and comparing models of cyber security investment to support policy and decision-making," in *Proc. WEIS*, 2007.

[24] J. A. Cowley and F. L. Greitzer, "Organizational impacts to cybersecurity expertise development and maintenance," in *Proc. Hum. Factors Ergonom. Soc. Annu. Meeting*. Los Angeles, CA, USA: SAGE, 2015.

[25] J. Nixon and B. McGuinness, "Framing the human dimension in cybersecurity," *ICST Trans. Secur. Saf.*, vol. 1, no. 2, p. e2, May 2013.

[26] H. Jahankhani, A. Al-Nemrat, and A. Hosseinian-Far, "Cybercrime classification and characteristics," in *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Amsterdam, The Netherlands: Elsevier, 2014, pp. 149–164.

[27] M. Cremonini and P. Martini, "Evaluating information security investments from attackers' perspective: The return-on-attack (ROA)," in *Proc. WEIS*, 2005.

[28] M. R. Stytz and S. B. Banks, "Issues and requirements for cybersecurity in network centric warfare," Air Force Res. Lab., Wright-Patterson AFB, OH, USA, Tech. Rep., 2004.

[29] T. Moore, "The economics of cybersecurity: Principles and policy options," *Int. J. Crit. Infrastruct. Protection*, vol. 3, nos. 3–4, pp. 103–117, Dec. 2010.

[30] A. Shostack, "Avoiding liability: An alternative route to more secure products," in *Proc. WEIS*, 2005.

[31] D. Klaper and E. Hovy, "A taxonomy and a knowledge portal for cybersecurity," in *Proc. 15th Annu. Int. Conf. Digit. Government Res.*, 2014.

[32] J. Fonseca, M. Vieira, and H. Madeira, "The web attacker perspective—A field study," in *Proc. IEEE 21st Int. Symp. Softw. Rel. Eng.*, Nov. 2010, pp. 299–308.

[33] S. W. Brenner, *Cybercrime: Criminal Threats From Cyberspace*. Santa Barbara, CA, USA: ABC-CLIO, 2010.

[34] M. Theoharidou and D. Gritzalis, "Common body of knowledge for information security," *IEEE Security Privacy*, vol. 5, no. 2, pp. 64–67, Mar. 2007.

[35] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Tech. Rep., 2007.

[36] A. N. Ayofe and O. Oluwaseyifunmitan, "Towards ameliorating cybercrime and cybersecurity," *Int. J. Comput. Sci. Inf. Secur.*, vol. 3, no. 1, pp. 1–11, 2009.

[37] T. Vagoun and G. O. Strawn, "Implementing the federal cybersecurity R&D strategy," *Computer*, vol. 48, no. 4, pp. 45–55, 2015.

[38] A. McGettrick, "Toward effective cybersecurity education," *IEEE Secur. Privacy*, vol. 11, no. 6, pp. 66–68, Nov. 2013.

[39] A. Rastogi and K. E. Nygard, "Cybersecurity practices from a software engineering perspective," in *Proc. Int. Conf. Softw. Eng. Res. Pract. (SERP)*, 2017.

[40] A. V. Barabanov, A. S. Markov, M. I. Grishin, and V. L. Tsirlov, "Current taxonomy of information security threats in software development life cycle," in *Proc. IEEE 12th Int. Conf. Appl. Inf. Commun. Technol. (AICT)*, Oct. 2018, pp. 1–6.

[41] C. Cerrudo, "An emerging U.S. (and world) threat: Cities wide open to cyber attacks," *Securing Smart Cities*, vol. 17, pp. 137–151, Oct. 2015.

[42] S. U. Khan, A. W. Khan, F. Khan, M. A. Khan, and T. K. Whangbo, "Critical success factors of component-based software outsourcing development from vendors' perspective: A systematic literature review," *IEEE Access*, vol. 10, pp. 1650–1658, 2022.

[43] M. S. Khan, A. W. Khan, F. Khan, M. A. Khan, and T. K. Whangbo, "Critical challenges to adopt DevOps culture in software organizations: A systematic review," *IEEE Access*, vol. 10, pp. 14339–14349, 2022.

[44] A. W. Khan, G. Yaseen, M. I. Khan, and F. Khan, "AHP-based prioritization framework for software outsourcing human resource success factors in global software development," in *Evolving Software Processes: Trends and Future Directio*, 2022, pp. 151–173.

[45] M. Bland, "An introduction to medical statistics," in *An Introduction to Medical Statistics*, 3rd ed., 2000.

[46] S. Kabanda, M. Tanner, and C. Kent, "Exploring SME cybersecurity practices in developing countries," *J. Org. Comput. Electron. Commerce*, vol. 28, no. 3, pp. 269–282, Jul. 2018.

[47] S. L. Pfleeger and R. Rue, "Cybersecurity economic issues: Clearing the path to good practice," *IEEE Softw.*, vol. 25, no. 1, pp. 35–42, Jan. 2008.

ABDUL WAHID KHAN received the Ph.D. degree in computer science from the University of Malakand. He is currently working as an Assistant Professor with the University of Science and Technology Bannu, Pakistan.

SHAH ZAIB is currently pursuing the M.S. degree in computer science from the University of Science and Technology Bannu, Pakistan. His research interest includes software engineering.

FAHEEM KHAN received the Ph.D. degree in computer science from the University of Malakand, KPK, Pakistan. He served four years in Pakistan as an Assistant Professor and supervised many papers and students. Since April 2021, he has been an Assistant Professor with the Department of Computer Engineering, Gachon University, South Korea.

ILHAN TARIMER received the master's and Ph.D. degrees from the Gazi University Institute of Science and Technology Electrical and Electronics Education. He has supervised many master's and Ph.D. students. He is currently working with Mugla Sitki Koccman University, Turkey. He has published many quality articles in reputed journals.

JUNG TAEK SEO received the M.S. degree in computer engineering from Ajou University, South Korea, in 2001, and the Ph.D. degree in information security engineering from Korea University, South Korea, in 2006. He was a Senior Researcher with the National Security Research Institute and an Associate Professor with the Department of Information Security Engineering, Soonchunhyang University. He is currently an Associate Professor with the Department of Computer Engineering, Gachon University. His research interests include CPS security, ICS cybersecurity, smart grid security, nuclear power plant security, smart factory security, smart city security, and automotive cybersecurity.

JIHO SHIN received the M.S. degree in digital forensics from Korea University, South Korea, in 2015, and the Ph.D. degree in information security engineering from Soonchunhyang University, South Korea, in 2022. He is currently a Research Officer with the Science and Technology Research Division, Police Science Institute, Korean National Police University. His research interests include digital forensics, cybercrime response, OT security, industrial control systems, and information security.