Hindawi
Security and Communication Networks
Volume 2021, Article ID 6677867, 22 pages
https://doi.org/10.1155/2021/6677867

Review Article

Assessing Security of Software Components for Internet of Things: A Systematic Review and Future Directions

Zitian Liao,[1] **Shah Nazir**,[2] **Habib Ullah Khan**,[3] **and Muhammad Shafiq**[4]

[1] *University of Sydney, School of Architecture Design & Planning, New South Wales 2006, Sydney, Australia*
[2] *Department of Computer Science, University of Swabi, Swabi, Khyber Pakhtunkhwa, Pakistan*
[3] *Department of Accounting & Information Systems, College of Business & Economics, Qatar University, Doha, Qatar*
[4] *Cyberspace Institute of Advance Technology, Guangzhou University, Guangzhou, China*

Correspondence should be addressed to Zitian Liao; zitianliao@sina.com and Shah Nazir; snshahnzr@gmail.com

Received 7 December 2020; Revised 14 January 2021; Accepted 4 February 2021; Published 15 February 2021

Academic Editor: Shehzad Chaudhry

Software component plays a significant role in the functionality of software systems. Component of software is the existing and reusable parts of a software system that is formerly debugged, confirmed, and practiced. The use of such components in a newly developed software system can save effort, time, and many resources. Due to the practice of using components for new developments, security is one of the major concerns for researchers to tackle. Security of software components can save the software from the harm of illegal access and damages of its contents. Several existing approaches are available to solve the issues of security of components from different perspectives in general while security evaluation is specific. A detailed report of the existing approaches and techniques used for security purposes is needed for the researchers to know about the approaches. In order to tackle this issue, the current research presents a systematic literature review (SLR) of the present approaches used for assessing the security of software components in the literature by practitioners to protect software systems for the Internet of Things (IoT). The study searches the literature in the popular and well-known libraries, filters the relevant literature, organizes the filter papers, and extracts derivations from the selected studies based on different perspectives. The proposed study will benefit practitioners and researchers in support of the report and devise novel algorithms, techniques, and solutions for effective evaluation of the security of software components.

1. Introduction

The role of component-based software engineering (CBSE) is obvious in software development. Software is designed according to previous experiences and component reusability which can save a lot of time, effort, and resources [1, 2]. Its effort is to bring commercial, cost-effective, and quality system by integrating the existing components. A system is designed using available components which is cheap, already tested, and error-free [1, 3–6]. An individual component is a single part of a software system and is a unit to facilitate reputable functionality in the system. The functionality of such components is combined which forms a complete software system. Two types of interfaces are used in a component such as provided and required interfaces. Both of these interfaces are a source of communication inside the software system. A component can be replaced, modified, and changed according to the requirements of the system. The developments with the use of existing components can save about half of the complete developed software [7]. Compositional approaches have many benefits in the development of software systems from the appearance of development of components which has accordingly produced substantial attention in research and developments in business standards for architectures of domain-specific, component interaction, toolkits, and numerous other applicable fields.

A number of approaches exist for the security of systems [8–12]. The elementary prerequisites of security are demarcated in Availability, Integrity, and Confidentiality

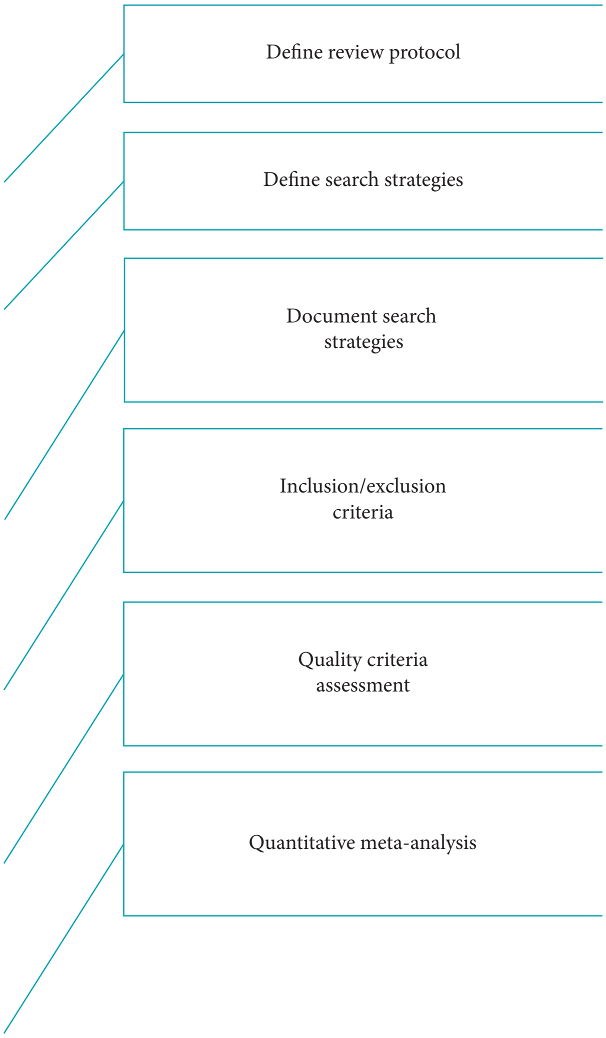

Define review protocol
Define search strategies
Document search strategies
Inclusion/exclusion criteria
Quality criteria assessment
Quantitative meta-analysis

Figure 1: Process of conducting a systematic literature review.

[10, 13–17]. Diverse reviews, frameworks, surveys, models, and analysis affecting the IoT security for security investigation are in use. Tekeoglu and Tosun [18] offered a framework of layer-based packet capturing for inspecting IoT devices' privacy and security. Mazhelis and Tyrväinen [19] assessed platforms of IoT from application provider perceptions. Machine learning (ML) algorithms have exposed a substantial enactment in diverse applications and fields such as text recognition, facial recognition, and detection of spam. These applications of ML have understandable performance in different areas and domains [9, 12, 20–25]. The devices of the Internet of Medical Things (IoMT) are susceptible to quite a lot of security threats, attacks, and liabilities. IoMT devices are suffering commencing massive threats of security due to little costs and power, unlike typical mobile and desktop devices. The malware reproduces itself by negotiating the joining that links the devices of IoT [26]. Mao et al. [27] planned an approach for structuring dependencies of security to measure the implication of system security from an extensive perception. The consequence of small-world and power-law distribution for in- and out-degree in security dependence networks was observed. The authors in [28] planned a method to measure the performance and services' evaluation of security for the cloud on the ground of a set of evaluation measures using Goal-Question-Metric. The authors in [29] conceived a framework for testing the security of interfaces of automotive Bluetooth with the help of a proof-of-concept tool for carrying out a test on a vehicle with the support of a planned framework. Nazir et al. [1] presented an approach for assessing software security of components via the analytic network process (ANP). The approach of ANP can work in a complex situation where the dependence arises among diverse network nodes.

The proposed research presents an SLR of the existing approaches used by practitioners to protect software systems. The protocol followed for conducting the proposed study is based on [3]. The study searches the literature in the popular and well-known libraries, filters the relevant literature, organizes the filter papers, and extracts derivations from the selected studies based on different perspectives. The following key contributions are achieved by the proposed study:

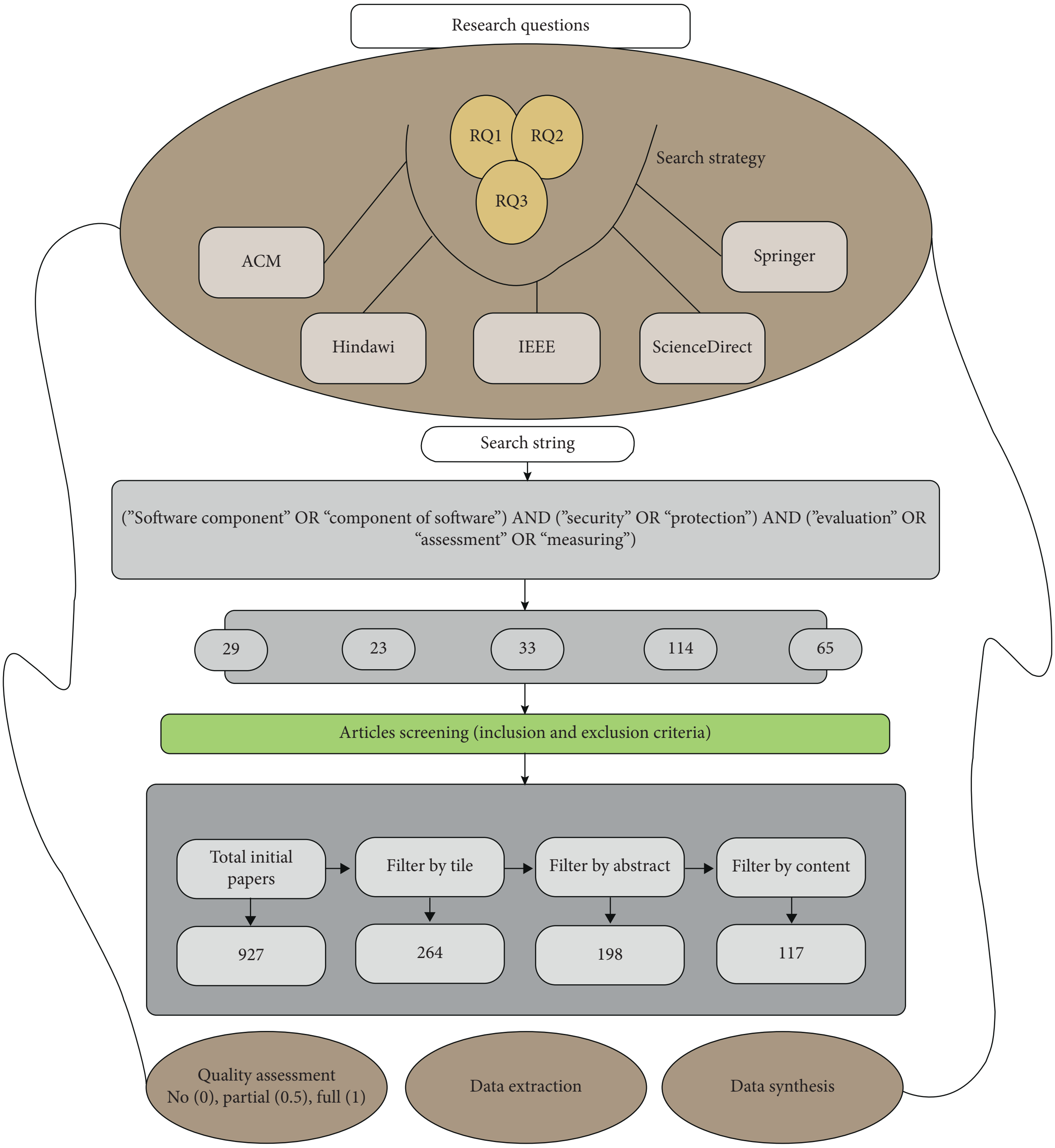


Figure 2: Protocol process and the libraries.

(i) To study the security measures for assessing software security of components

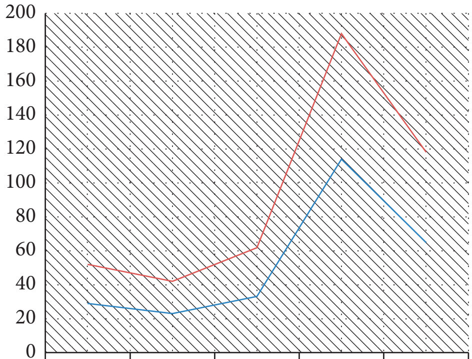
(ii) To identify the techniques and methods available for assessing software security of components

(iii) To show how these techniques efficiently work for evaluating the security of components

The paper is structured as follows. Section 2 shows the research method focusing on SLR for showing the analysis of the current study. Section 3 shows the results and discussions of the paper with answers to the research questions. The conclusion is presented in Section 4.

2. Methodology

2.1. Research Plan and Process. The SLR is a formal way of searching the keywords, identifying the relevant materials associated with the research, organizing in an efficient way, and deriving meaningful information and derivations from the studies selected. Figure 1 represents the steps followed for the proposed research where firstly the review protocol is defined, then the search strategies are defined for the research, then the search strategies are documented, the relevant materials are included while the rest of the materials are excluded, the quality assessment is done for the selected



	ACM	Hindawi	IEEE	Science Direct	Springer
Abstract	23	19	29	74	53
Title	29	23	33	114	65

Figure 3: Overall search results.

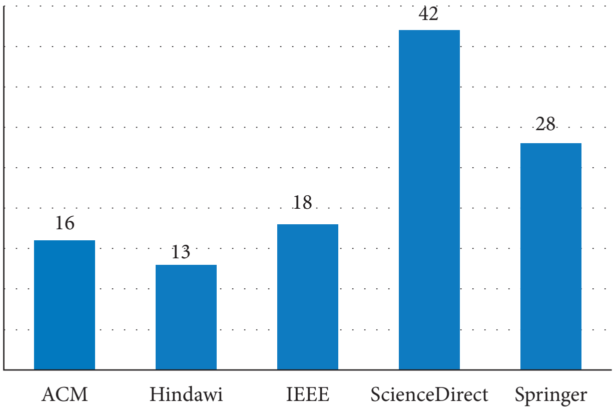


Figure 4: Final filtered papers by contents.

papers, and lastly the data analysis is extracted from the included papers.

2.2. Research Questions. Below are the questions which were defined for the current study:

(1) What can be the security measures for assessing software security of components?

(2) What are the techniques and methods available for assessing the security of software components?

(3) How efficiently the techniques work for evaluating component security?

2.3. Keywords and Libraries. The keywords ("Software components" OR "components of software") AND ("security" OR "protection") AND ("evaluation" OR "assessment" OR "measuring") were defined to search the libraries. The following libraries were adopted for the process of search. Other libraries were skipped due to the reason that these libraries are publishing materials which are peer-reviewed, while Google Scholar has all of the materials.

(i) ACM

(ii) Hindawi

(iii) IEEE

(iv) ScienceDirect

(v) Springer

The following are the details of the process of the search for each of the selected library.

(i) ACM: [[[All: "software components"] OR [All: "components of software"]] AND [[All: "security"] OR [All: "protection"]] AND [All: (]] OR [All: (] OR [All: "evaluation"] OR [All: "assessment"] OR [All: "measuring"]

(ii) Hindawi: "("Software components" OR "components of software") AND ("security" OR "protection") AND ("evaluation" OR "assessment" OR "measuring")"

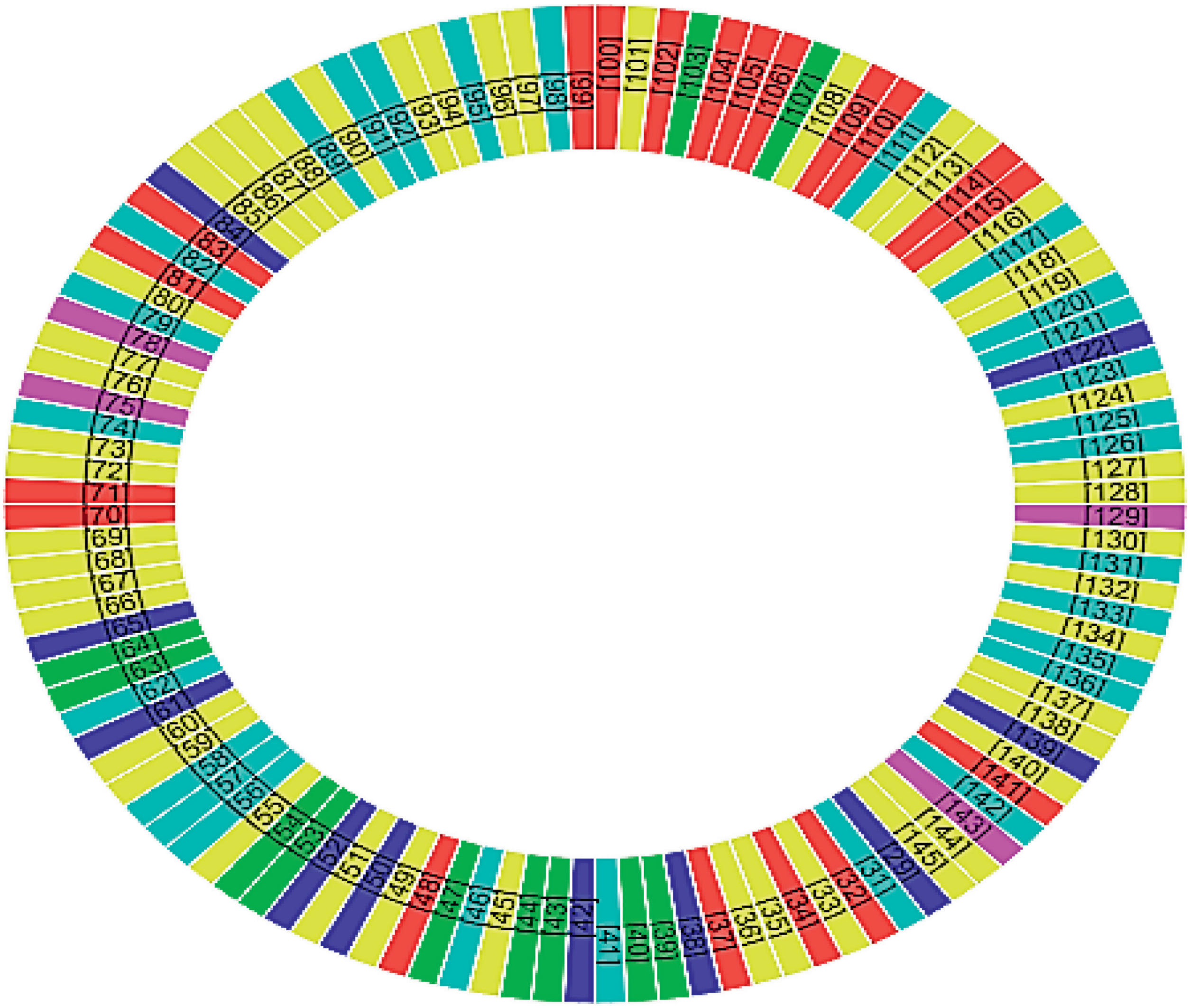


Figure 5: Selected articles.

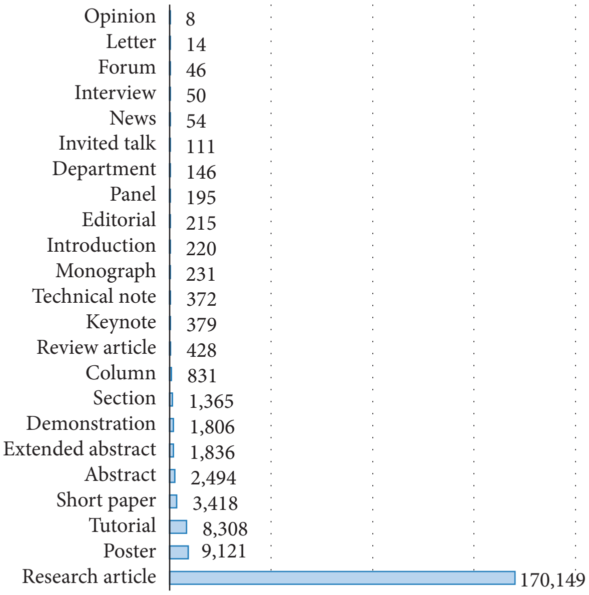


Figure 6: Article types and the number of papers.

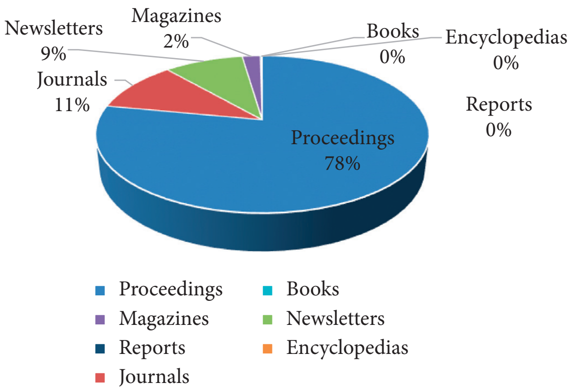


Figure 7: Article types and publications.

(iii) IEEE: ("All Metadata":Software components) OR "All Metadata":components of software) AND "All Metadata":security) OR "All Metadata":protection) AND "All Metadata":evaluation) OR "All Metadata": assessment) AND "All Metadata":measuring)

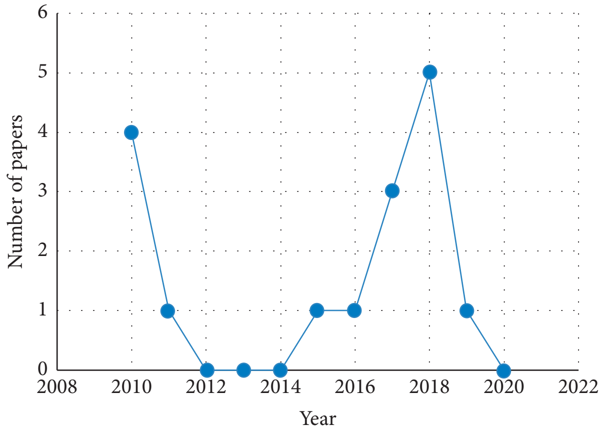


Figure 8: Year and number of papers published.

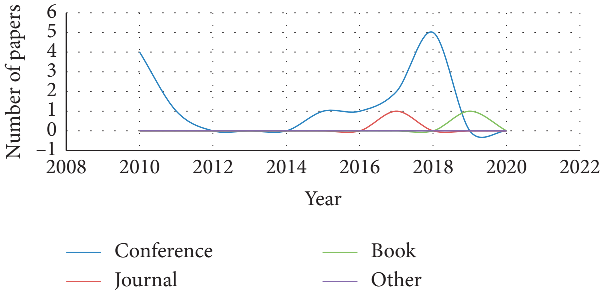


Figure 9: Year and number along with the type of paper published.

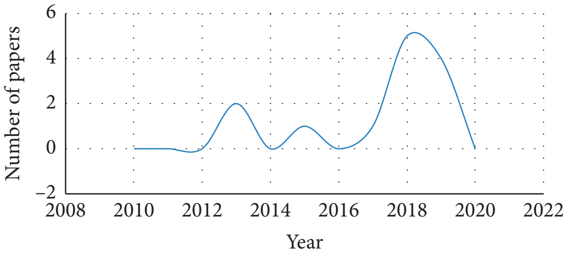


Figure 10: Year and total of articles.

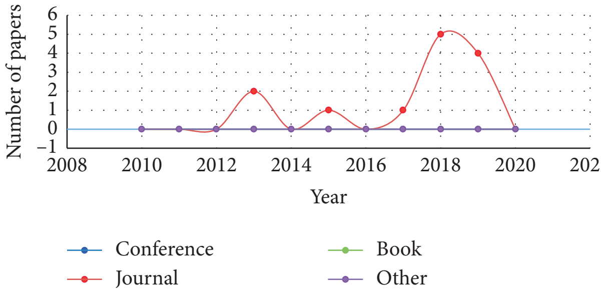


Figure 11: Year and number along with the type of paper published.

(iv) ScienceDirect: "("Software components" OR "components of software") AND ("security" OR "protection") AND ("evaluation" OR "assessment" OR "measuring")"

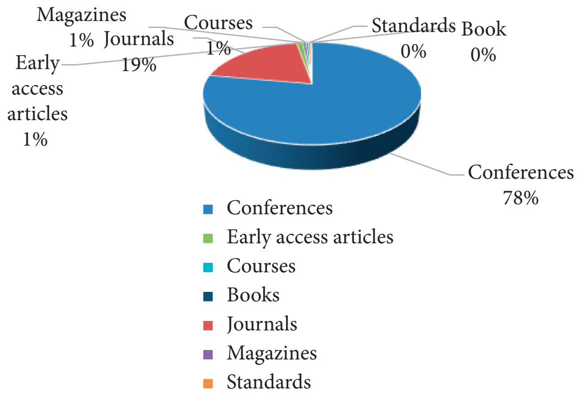


Figure 12: Number of publications along with the type of publication.

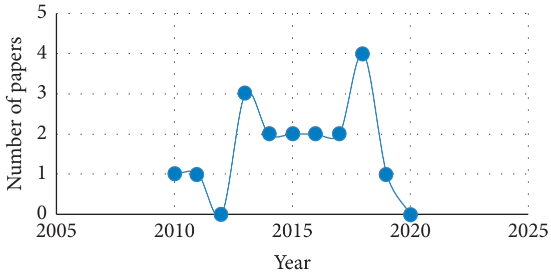


Figure 13: Year and the total number of articles.

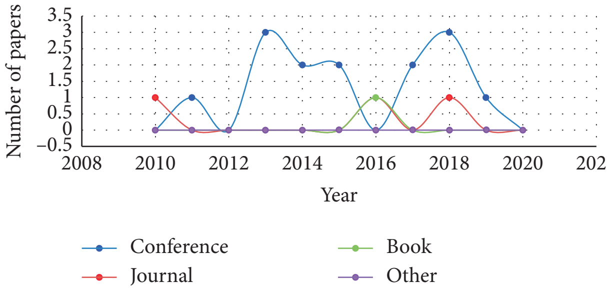


Figure 14: Year and number along with the type of paper published.

(v) Springer: "("Software components" OR "components of software") AND ("security" OR "protection") AND ("evaluation" OR "assessments" OR "measuring")"

Figure 2 shows the process of searching the keywords in the given libraries with the results of the search obtained. The filtering process of papers by title, abstract, and finally contents is also shown in the figure. The figure is initially based on the research questions defined and then the search process in the given libraries with the use of Boolean operators "AND" and "OR."

Figure 3 shows the number of papers filtered by title and then by an abstract in the given libraries. Initially, huge

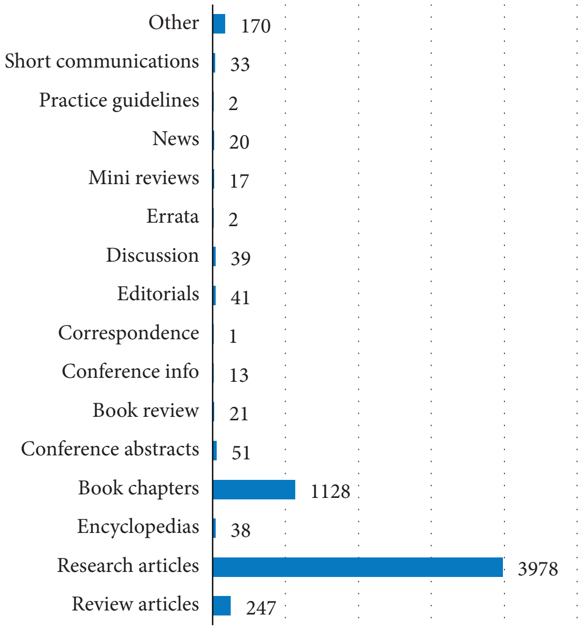


Figure 15: Publication type and the number of papers published.

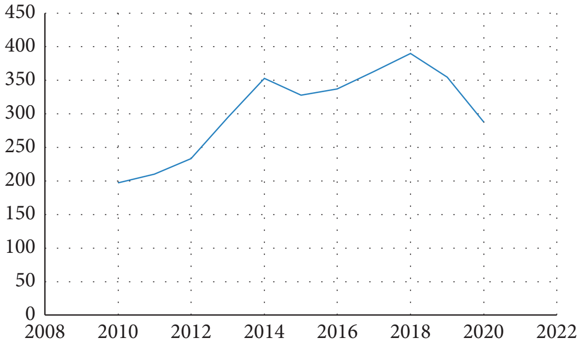


Figure 16: Number of publications in the given year.

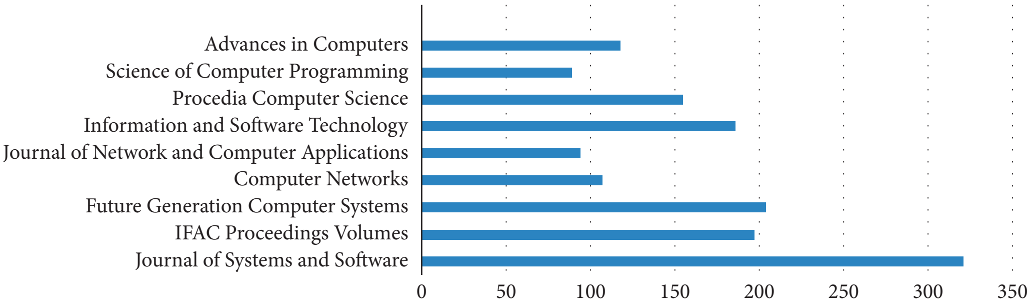


Figure 17: Publication title and number of papers.

numbers of papers were obtained during the search process. It was considered that the analysis of all the searched papers was difficult, so due to this reason, the papers were filtered by title for obtaining the relevant papers. After this, a total of 264 papers were obtained which was also difficult to analyze in one process, so these articles were then filtered by abstract, and a total of 198 articles were achieved.

The articles were filtered based on content, and a total of 117 articles were achieved for the given libraries which are shown in Figure 4.

The articles selected are shown in Figure 5.

After this, the details of each library were analyzed which are given hereinafter. The library of ACM was analyzed in the first step for the research article type and content type. This search was for the initial results of the search which is shown in Figure 6.

The article type for the ACM library is shown in Figure 7.

After the initial search process, the materials were filtered to extract only relevant studies. Figure 8 shows the articles published in the mentioned years.

The article types were viewed in the given year. Figure 9 depicts article types and the total number of articles in given years.

After searching the ACM library, the library of the Hindawi publisher was checked for relevant materials related to the proposed study. Figure 10 presents year-wise publication numbers in the library of Hindawi.

Figure 11 represents the total number of articles published in given years based on the types of publications.

The library of IEEE was searched for identifying relevant studies to the proposed research. Figure 12 shows initial search results for publications with publication types in the IEEE library.

The obtained papers from the searched process in the IEEE were then filtered to extract only relevant papers. Figure 13 shows the total number of articles in given years in the IEEE library.

Figure 14 presents publication types with publication numbers in given years in the same library.

The library of ScienceDirect was considered to find the relevant materials to the proposed research. During the initial search process, the publication types were checked which is shown in Figure 15.

The total number of articles was checked in given years. The total number of articles with the year of articles is presented in Figure 16.

The publication titles were also checked that where the papers are published. Figure 17 presents the titles of the articles with a total number of articles.

After filtering the process of papers in the ScienceDirect library, the number of articles in given years was reviewed. The details are given in Figure 18.

Figure 19 presents the total number of articles with the types of publications in given years.

Finally, the library of Springer was searched to obtain the associated material to the proposed research. The initial search results for the number of publications with article types are shown in Figure 20.

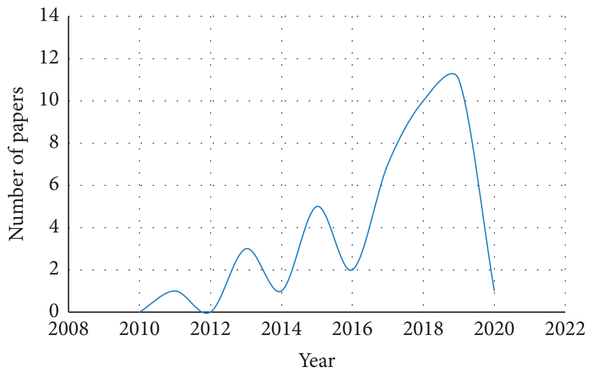


FIGURE 18: Number of publications in the given years.

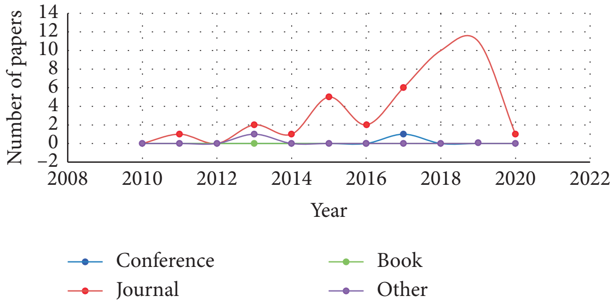


FIGURE 19: Article type with the total number of articles.

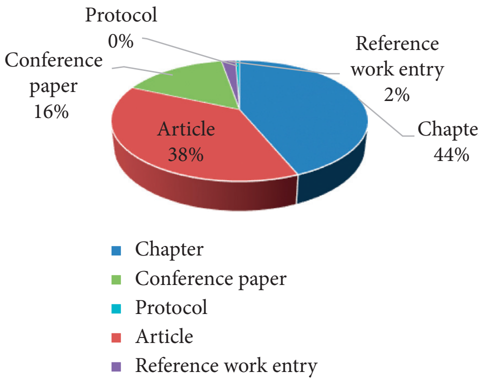


FIGURE 20: Articles with the type of papers.

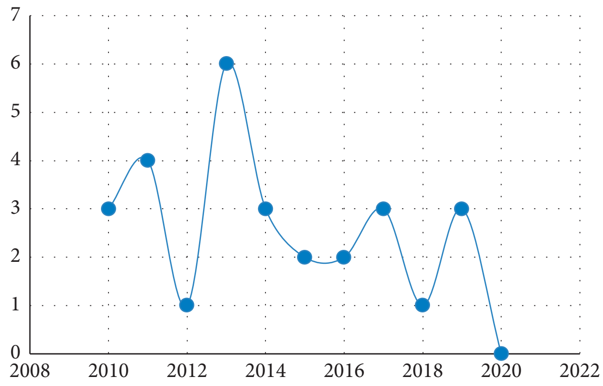


FIGURE 21: Number of publications in the given year.

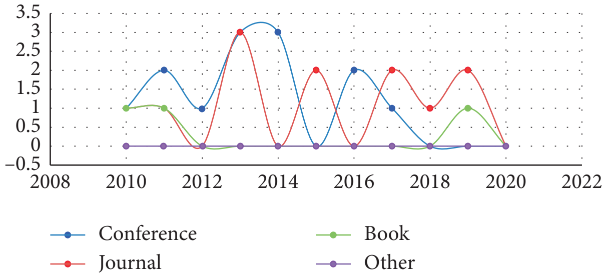


Figure 22: Article type with the total number of papers in the given year.

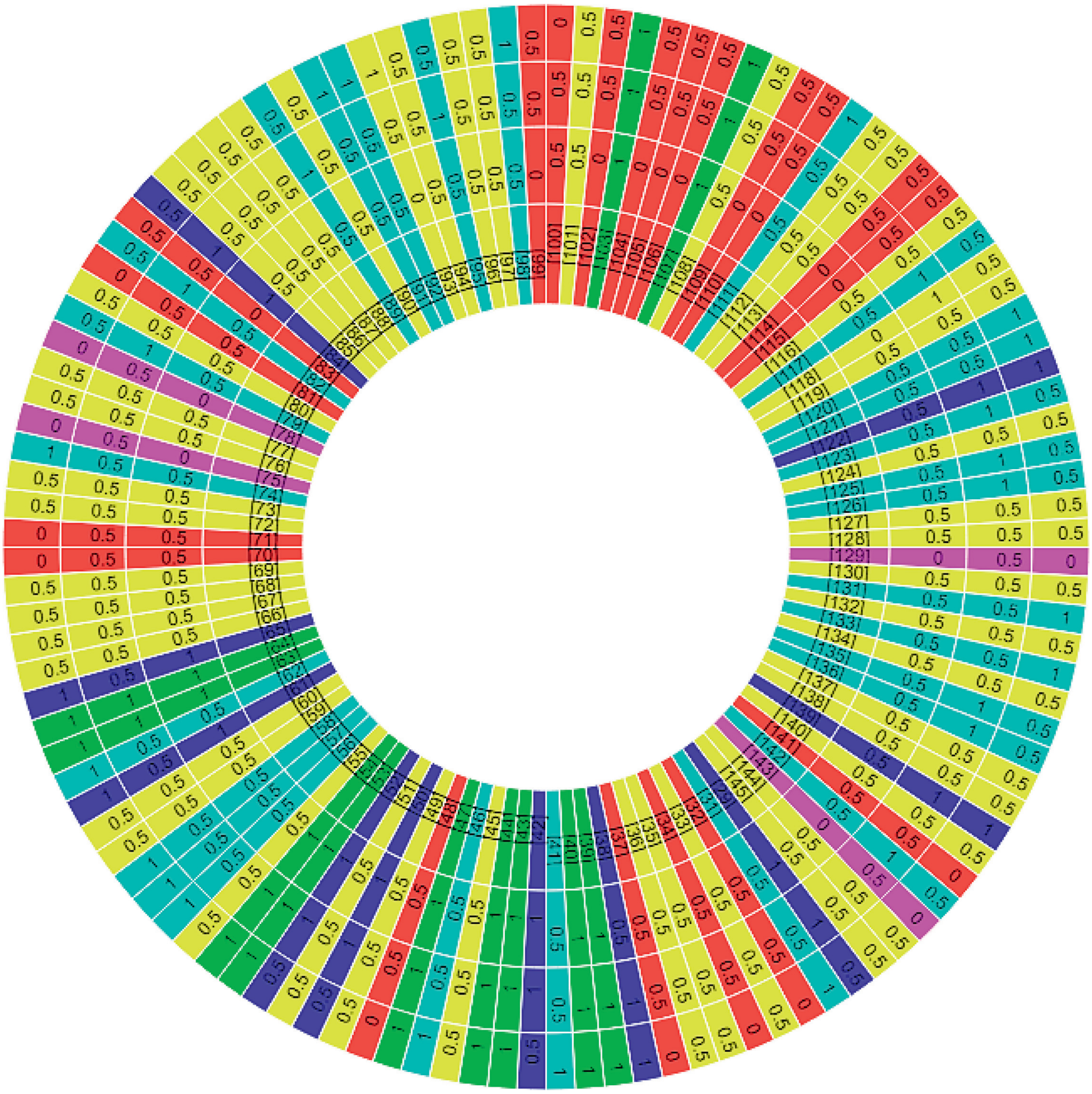


Figure 23: Score of research questions for each paper.

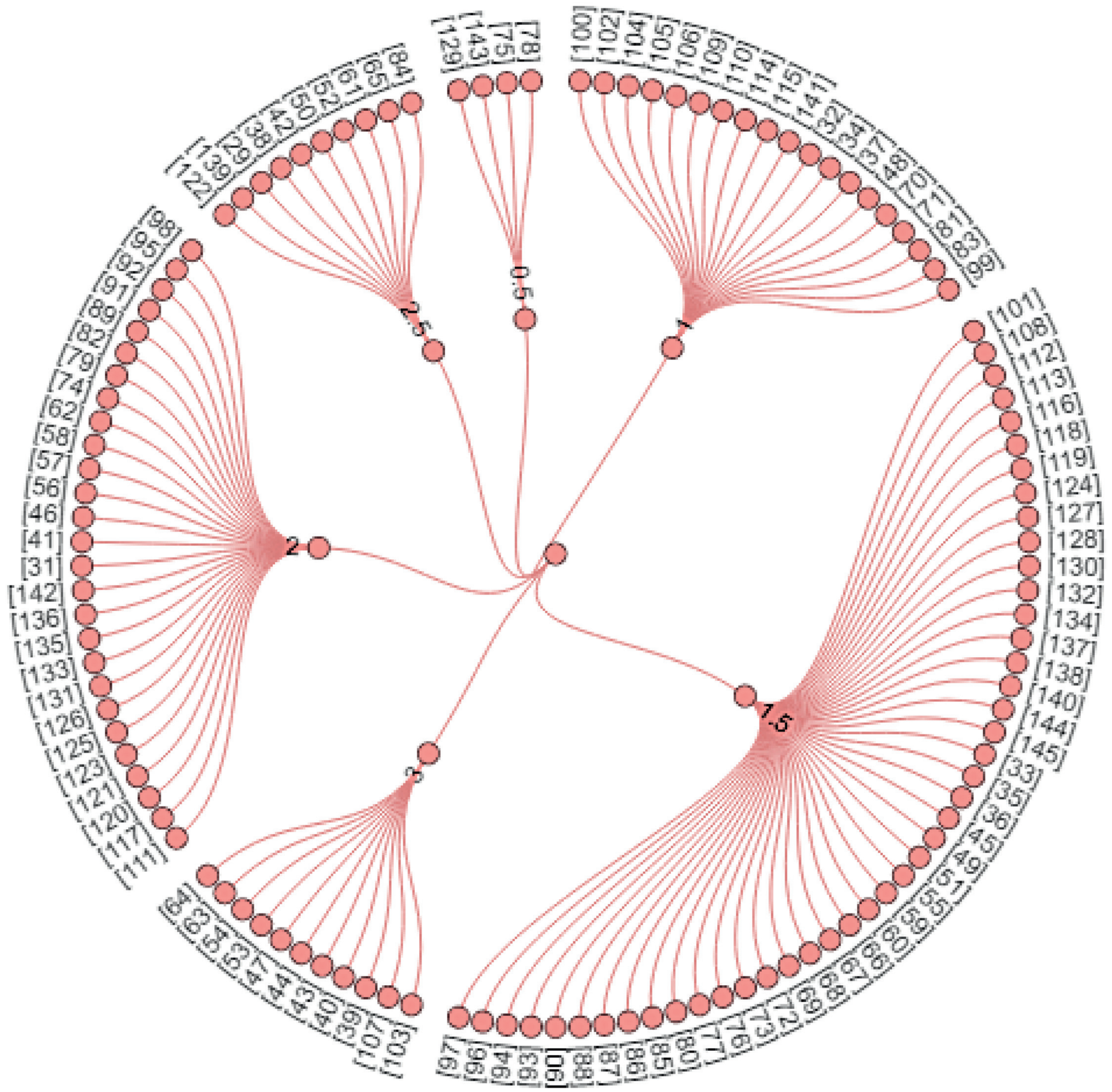


Figure 24: Sum of scores for each paper.

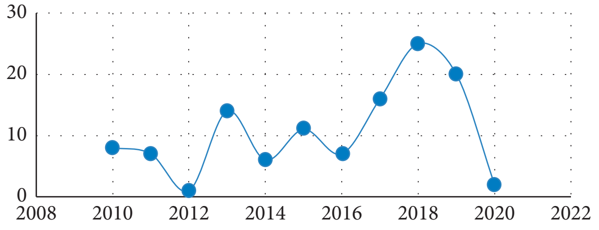


Figure 25: Overall number of papers in all the libraries in the given years.

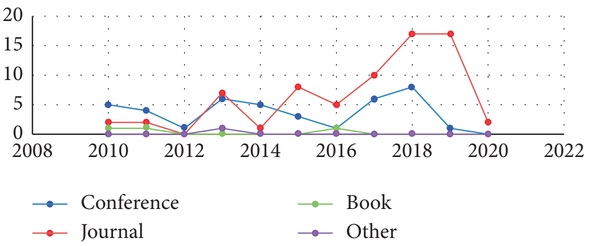


Figure 26: Overall number of papers and type of papers in all libraries in the given years.

Table 1: Identified list of security features presented by researchers.

References	Features
[30]	Maximum signal range Variety of network topologies Safety and security of data transfer Reliability and dependability of WCT Throughput and data rate Applicability of WCT Wireless power transfer Minimum latency
[17]	Confidentiality Availability Integrity Authentication Access control Authorization Auditing Trust Privacy Reputation metering Accountability Replay protection Anonymization Resilience to attacks Fault tolerance Nonrepudiation
[31]	Confidentiality Integrity Availability Fault tolerance Accountability System trust
[32]	Privacy and security Technology Communication Culture Job Legal regulation
[33]	Privacy protection Node information certificate Secure cloud computing Encryption mechanism Anti-DDoS Platform security Secure multiparty computation Information application security Antiattack security Heterogeneous network recognition

After filtering the process of papers, the results were analyzed to obtain meaningful results related to the proposed research. Figure 21 represents article numbers in the given year in the library of Springer.

Figure 22 represents the total number of publications with the type of publications in the given year in the Springer library.

2.4. Quality Assessment of the Selected Papers. The quality assessment process of the carefully chosen articles was done in order to know how much the paper is related to the proposed study. A score of “1” was given to the research paper which completely fulfills the research question, “0.5” was given to the paper somewhat satisfying the research question, and “0” was given to the paper not satisfying the research question. Figure 23 shows the quality score for each paper based on the defined research questions.

Figure 24 shows the sum of the overall score for each paper. The assigned values of the selected papers for all the research questions were summed and the total score is shown in the figure.

3. Results and Discussion

After individual analysis of the libraries, all the references were merged into a single Endnote file to analyze them. It was found that there is an increase in the year-wise number of publications related to the proposed research. Figure 25 shows the number of publications in the given years for the overall libraries collectively.

Figure 26 shows the number of publications along with the type of publications in the given years for all the libraries collectively.

3.1. What Can Be the Security Measures for Assessing the Security of Software Components? Security features can play a significant role in the smooth running of a particular system. A number of features were identified from the literature based on which the security is evaluated. Table 1 shows the identified list of features from the literature presented by different researchers.

3.2. What Are the Techniques and Methods Available for Assessing the Security of Software Components? Diverse approaches are presented by the researchers to tackle the issue of security evaluation of software and its components. These approaches work from different perspectives. Table 2 shows the summary of the existing techniques available for security evaluation.

3.3. How Efficiently the Techniques Work for Assessing the Security of Components? There is high need of effective security evaluation techniques which can efficiently evaluate the security of software system. Such techniques

Table 2: Existing approaches for evaluating security.

Citation	Technique	Description
[34]	Quantitative assessment approach	This approach evaluates the component security level quantitatively and identifies efficiently the component security vulnerabilities.
[35]	Secure multiparty computation (SMC)	This paper revisits the history of developments to SMC that completed the years and studies the opportunity of coupling reliable hardware with SMC.
[36]	Software-defined networking (SDN)	The analysis demonstrated that SDN appears to be the most attractive developmental structure for upcoming networks.
[37]	Conventional security mechanisms	They focus on emerging security threats aiming at vulnerabilities, human errors, and defects of a mobile device structure in existing schemes.
[38]	Abstract network model	The analysis shows that the abstract network model is a valuable method for attack graph-based assessments.
[39]	Logic programming	In this article, model-based testing and logic programming was introduced for detecting accessible SQL injection (SQLI) and cross-site scripting (XSS) of web applications.
[40]	Cognitive dimensions questionnaire	Results revealed that the usability issues of security application programming interfaces (APIs) may be determined using this methodology with significantly good reliability and validity.
[28]	Goal-question-metric (GQM) method	The proposed assessment methodology might help cloud service providers (CSPs) to practice a security self-evaluation and is suitable for the level of their security services within the cloud market.
[29]	Threat model	This model is helpful for the evaluation of the Bluetooth interface on a range of built-in automotive infotainment systems.
[41]	Security assessment	This study presents the cybersecurity associated principles for the smart grid which address the issue in different ways and to various extents.
[42]	Semantic model	In this paper, a semantic model for structuring and risk visualization implemented into the metric visualization system (MVS) was presented.
[43]	NIST national vulnerability database (NVD) combined with EBIOS risk analysis and evaluation methodology	The finding of this research has demonstrated that virtual networks, SDN controllers, and hypervisors continue to present new attack capabilities that are continually being exposed, further escalating the security risk of modern data centers.
[44]	Security behavior	The research findings show that psychological ownership, descriptive norm, response cost, self-efficacy, and perceived vulnerability all were significant in determining personal computing security intentions and behavior for both the mobile device and home computer users.
[45]	Countermeasure-cantered approach	In this article, a prototype implementing such a security management system is described.
[46]	Threat model	This work presents a quantitative study on the security solutions for communication quality used in robotics, while security capabilities are enabled.
[47]	Supervisory control and data acquisition (SCADA) systems security	This provides an insight into developing a framework that can be used to assist critical infrastructure sectors.
[48]	Innovative ontology and graph-based approach	For network security evaluation, an innovative approach that uses ontology was proposed. The ontology is intended to illustrate security knowledge such as that of attacks, vulnerabilities, assets, and the relationships between them.
[49]	Information-theoretic model	For the computer systems security analysis, the entropy concept was utilized and a quantitative model was derived. The assessment process consists of dynamic and static phases.
[50]	International symposium on formal methods (FM 2012)	This short paper is intended to accompany a talk at the 18th international symposium (FM 2012). It discusses software security with a highlight on formal aspects, defenses, and low-level attacks.
[51]	Security metrics and risk analysis	In this work, formal analysis of associations between risk and security metrics and formal definition of risk were provided.
[52]	Security information and event management (SIEM) systems	The article proposed a general framework for the visualization of SIEM which permits integration of different visualization approaches and expands simply the application functionality.

Table 2: Continued.

Citation	Technique	Description
[53]	Big data framework	A framework for big data in this work was proposed to build up the security capability of small enterprises.
[54]	Usability of security software	This article addresses the usability of security alerts across a wider range of security products.
[55]	Security evaluation using Bayesian belief networks	This article demonstrates parts of the gap, in particular the challenges associated with variable quality of information, lack of empirical information, limited budget, short time-to-market, and lack of resources.
[56]	Multimetrics approach for security	This article presents a multimetric approach jointly with a methodology to estimate the system security, privacy, and dependability (SPD) level throughout both the running and design process.
[57]	Ontology-based model for security assessment	In this article, the ontology-based framework was classified in five dimensions for assessing attack effect; they are defense, vulnerability, attack target, attack vector, and attack impact.
[58]	Vulnerability-centric requirements engineering framework	This paper gives an engineering framework to maintain the elicitation of security requirements and analysis based on vulnerabilities.
[59]	Evaluation and assessment of the security of wearable devices	This paper examined the usefulness and design of SecuWear platform for recognizing vulnerabilities in these areas and assists wearable security research to mitigate them.
[60]	Assessment of platforms	This paper explains how the PRIME platform trust can enhance trust and manager operates.
[61]	Software-defined security framework	For protecting the distributed cloud, a software-defined security framework was proposed in this paper.
[62]	Software-defined mobile network security	This article gives a survey of software-defined mobile network (SDMN) and its related security issues.
[63]	Reputation model	In this article, the most critical as well as essential security threats for a utility-based reputation model in grids were assessed.
[64]	IoT monitoring solution	A monitoring tool based on the extension of the Montimage network monitoring tools for IoT systems was presented in this paper.
[65]	A comprehensive pattern-driven security methodology	ASE—a comprehensive pattern-driven security methodology intended particularly for (common) distributed systems—focuses on the early life cycle phases and particularly the design phase.
[66]	Contract-based security assertion monitoring	This article demonstrates how in a live environment on Linux a contract-based security assertion monitoring can be attained.
[67]	Network security visualization	For the security visualization systems evaluation such as ranking and rating, a framework was proposed in this paper.
[68]	Empirical study	This article empirically examines how refactoring can progress the security of an application by removing code bad smells.
[69]	Computational approach	For the standardization of the software development process, a computational approach was proposed in this work.
[70]	Multitarget approach	In this paper, for the estimation of scores and vulnerability characteristics from the technical description, a model of the combination of multitarget classification and text analysis approaches was created.
[71]	A new threat identification approach	In this paper, for the assessment of security threats quantitatively, a new approach was adopted, which is modular, extendable, and systematic.
[72]	Regression model	For the identification of security requirements, a linear based approach was proposed in this work.
[73]	Problem-oriented security patterns	Based on the problem frames technique, a systematic approach was proposed in this work for the iterative development of software architectures and requirements analysis.
[74]	A framework for semiautomated coevolution	For the security maintenance and support, a model-based framework was addressed in this paper for a software system during the long-term evolution.
[75]	A manual approach	The legal and security risks were discussed in this paper which arise from reuse.
[76]	A coarse approach to quantitative modeling and analysis	For the integrated vulnerability assessment, a methodology using a coarse approach to quantitative analysis and modeling was discussed in this paper.

Table 2: Continued.

Citation	Technique	Description
[77]	Cyberdefense and cloud vulnerability assessment	In order to decrease, evaluate, and assess the vulnerability level of distributed computing systems (DCIs), an IT security audit framework was created in this paper.
[1]	Analytic network process (ANP)	For the component security evaluation, an ANP was proposed in this paper.
[78]	Distributed security systems	Distributed security systems were examined in this paper with devoted server modules that perform client modules' monitoring and managing.
[79]	Threatened-based software security evaluation method	In software security literature, for the software security assessment, a new concept was introduced in this paper: the threatened-based method.
[80]	Measurement frameworks	This paper reports a measurement framework for software development.
[81]	A cloud data monitoring system	Based on autonomic computing, a data security monitoring approach was proposed in this paper for the feasibility verification through simulation.
[82]	Hybrid reputation model	Based on both explicit definition of reputation and implicit reputation calculation, a hybrid reputation model is presented in this article.
[83]	Security architecture	In this paper, the implementation and design of a security framework to FPGA-based heterogeneous systems developed on top of MAC-based OS/Hypervisors was presented.
[84]	Website security analysis	A model-based website security testing method was proposed in this paper.
[85]	Methodology for enhancing software security	For enhancing software security in the development life cycle, a methodology was proposed in this paper.
[86]	Dynamic disassembly of machine instructions	This paper talks about a novel concept RECSRF, consisting of the runtime execution complexity (REC) and its evaluation method security risk factor (SRF).
[87]	Protection of IoT devices using Berkeley packet filters	This paper reports a practical approach which is an easy-to-use framework to protect IoT devices against attacks.
[88]	Software security knowledge	For the secure software development that incorporates an artifact and a knowledge-based management system, a case-based management system (CBMS) was proposed in this work.
[89]	Security analysis of android applications	This paper addresses a mobile app security investigation tool StaDART that merges dynamic and static examination to present the existence of dynamic code update.
[90]	Surveys and overviews	This paper summarizes the field of software vulnerability examination and discovery that uses machine learning and data mining approaches.
[91]	Security and privacy	This paper talks about safe patch fingerprinting.
[92]	Text mining	This paper focuses on text mining approaches and their different classification techniques (support vector machines, neural networks, and decision trees).
[93]	Software security engineering	This paper described an attempt to benchmark and baseline the state of company software and also incorporates state of software reliability data across the company's products.
[94]	Quantitative measurement	In this paper, for software engineering service bus (EngSB) platform assessment, a set of quantitative metrics was proposed.
[95]	Common vulnerability scoring system	This article reports which information cues decrease or increase vulnerability evaluation by humans.
[96]	Automatic approach	In this article, an automatic approach was proposed for detecting the software vulnerabilities on multiple systems using/sharing API libraries or similar code.
[97]	Software and application security	This paper talks about the software vulnerabilities by means of descriptions only via deep learning and word embedding approaches.
[98]	Threat analysis	This paper talks about the threat agent approach.
[99]	Machine learning techniques	This paper reports a lightweight dynamic and static features approach for the software vulnerability testing detection by means of machine learning methods.
[100]	Models of computation	In this paper, a cryptographically secure attestation scheme was proposed, which detects direct memory access (DMA) attacks.
[101]	Understanding security requirements and challenges	This work describes the state-of-the-art efforts in ensuring security in the IoT network.

Table 3: Summary of the existing techniques for evaluating security.

Citation	Technique	Description
[102]	A framework for the comparison of security adaptation approaches	Five security adaptations were compared in this framework. The framework includes three perspectives that are life cycle, security, and adaptation. The evaluation illustrated that in each adaptation approach the monitor and analysis phase is described.
[103]	Information security risk assessment	The analysis showed that this method gets more scientific evaluation and reliable and stable results on the evaluation of the risk of the control systems of industry.
[104]	State fusion finite state machine model	In this paper, an SF-FSM model was proposed to recognize a legitimate application to evaluate its vulnerabilities and illegal behavior of unauthorized parties for an industrial control system.
[105]	Core unified risk framework (CURF)	This approach is suitable for the qualitative comparison of activities and processes in each method of information security risk assessment (ISRA) and presented a measure of completeness.
[106]	Complexity metrics for software security improvement	For the security level of computer-based systems, improving software security is essential.
[107]	Security vulnerability assessment, prevention, and prediction (SVAPP)	The proposed SVAPP methodology exploits an active security barrier approach and adapts it to suit the security facet.
[108]	Security quality requirements engineering (SQUARE) method	In this paper, SQUARE effectiveness was evaluated in terms of its artifacts (attack tree, security templates, system architecture diagram and use-case diagram, and scenarios), a set of security goals, vulnerabilities, threats, and prioritized and categorized security requirements.
[109]	SODA	In this paper, SODA was introduced, which leverages integrate virtual network functions (VNFs) and software-defined networking (SDN) to realize service management and security policy for IoT environments.
[110]	Evaluating of security risks framework	In this article, the security risks for IEC 61850 network, intelligent electronic devices (IEDs), and distributed denial of service (DDoS) attack assessment within an SDN-enabled smart grid communication network.
[111]	Security analysis and security rules	This analysis investigates four in-app payments' implementation and also summarizes a series of security rules.
[112]	Formal framework	In this paper, a formal framework for the strength of software obfuscation evaluation was proposed. It is used for the protection of secret data or control-flow graphs (CFGs) of a program.
[113]	Machine learning methods	The contribution of this paper is a methodology for analyzing features from C source code to classify functions as vulnerable or nonvulnerable.
[114]	UML or SysML language	In this article, the state of the art associated with quantification, verification, and security specification for systems and software that are modeled by means of UML or SysML language is reviewed.
[115]	Security diagnosis as a service (SDaaS)	The scalability, performance, and accuracy of the framework were evaluated. The results of the evaluation reveal that SDaaS demonstrates information flow vulnerabilities with not merely scalability, performance, and accuracy, but furthermore lightweight footprint on resource utilization.
[116]	Calculus IoT-LySa	This article presents a methodology, based on the process calculus IoT-LySa, to infer quantitative measures on the evolution of systems.
[117]	Framework for modeling and assessing the security of the Internet of Things (IoT)	The IoT is facilitating innovative applications in a variety of domains. The key contributions of this article were to assess the framework using three scenarios, including environment monitoring, wearable healthcare monitoring, and smart home.
[118]	Broadcasting service	This article describes and records all probable threats to broadcasting services
[119]	Security in software evolution	In this chapter, four challenges including relevant knowledge, the impact of available knowledge, reestablishing, and reactions of security were addressed.
[120]	Framework for security testing	In this article, the proposed framework is used for security testing subsequent to the system implementation.
[121]	Multiperspective security management	The projected modeling approach for managing and designing IT security in institution account used for diverse perceptions is based on multiperspective enterprise modeling.
[122]	Embedded device design and verification	This paper focused on the approaches for verification and design of information systems with embedded devices.

Table 3: Continued.

Citation	Technique	Description
[123]	Automotive security assurance	In this article, a systematic security assessment to specify undesirable behaviors, enabling the assignment of severity ratings in a (semi-) automated manner was explored.
[124]	Pattern-based method	In this paper, for establishing a cloud-specific information security management system (PACTS), a pattern-based method was presented.
[125]	Temporal hierarchical attack representation model	In this article, network changes were systematically formalized and categorized on the basis of their causes of the change.
[126]	Stochastic modeling	For the security metrics quantitative assessment, a state-based stochastic model was proposed in this paper.
[127]	Experimental assessment	In the presence of denial of service (DoS) attacks for the assessment of the security of web service frameworks, an experimental approach was proposed in this article.
[128]	Hash power distribution analysis model	In this article, a hash power distribution analysis model for the profitability of miner measurement was proposed based on various incentives toward an evaluation of Bitcoin security.
[129]	mHealth apps security framework (MASF)	To secure the execution of mHealth apps and their users' data, the mHealth apps security framework (MASF) was proposed in this article.
[130]	Abstract model	In this article, for the support of single sign-on (SSO) development, an abstract model was provided.
[131]	A proactive approach	To quantitatively assess the security of network systems, a proactive approach was addressed in this paper for validating, formulating, and identifying a number of essential features that mostly affect its security.
[132]	Trust modeling and evaluation	For a component-based software system, an autonomic trust management solution was introduced in this paper.
[133]	Static analysis	For the security static analysis tools, an evaluation framework was introduced in this paper.
[134]	SecuWear platform	This paper presents a multicomponent research platform, called SecuWear, for mitigating, analyzing, and testing vulnerabilities in software and hardware.
[135]	One-to-many bilateral e-trade negotiation framework	A mobile agent-based secure one-to-many bilateral e-trade negotiation framework was presented in this paper.
[136]	Model integrated computing	For rapidly deploying cyberphysical system (CPS) attack experiments, a model-based software development framework integrated with a hardware-in-the-loop (HIL) testbed was presented in this work.
[137]	Concise binary object representation (CBOR)	This paper reports instantiated architecture for verification and secure measurement of dynamic runtime information for Linux-based OS.
[138]	Multidomain networks	In this article, a framework was proposed for leveraging service function chaining (SFC) and software-defined networking (SDN) to improve collaboration among security service functions (SSFs).
[139]	Security-informed safety	This paper talks about security-informed safety.
[140]	Trust model	In this article, for cloud-edge-based data-sharing infrastructure, a 5 level trust model was proposed.
[141]	Security and risk assessment	This paper gives suggestions about unmasking the uncertainty of risk assessment and facilitating oversight of its practice by public actors, judicial and legislative.
[142]	Software security vulnerabilities	In this work, for recurring software vulnerabilities, an empirical study was reported.
[143]	Self-destructive tamper response	In this paper, a method for tamper-resistant software was created, so as to be resistant to dynamic analysis as well as static analysis.
[144]	Model of virtual machine (VM)	Based on memory introspection, a model of VM security monitoring was proposed in this article.
[145]	Software-defined networking (SDN)	This paper reports the NOSArmor, which contains various security mechanisms, such as a security building block (SBB), into a consolidated SDN controller.
[146]	Binary-level patch analysis framework	SPAIN which is a patch analysis framework was proposed in this paper for summarizing patch patterns, security patches identification, and their corresponding vulnerability patterns.

can be useful for the success of software from a business perspective. Table 3 shows the summary of the efficiently used techniques for evaluating the security of software systems.

4. Conclusion

Components of software play an important role in the functionality of the activities of software systems. Components are considered to be reused due to the properties that are already tested, debugged, and experienced in practice. The security of components is important for its nature due to avoidance of happening of illegal or malicious activities that can harm the success of the software system. The security of component can be high if it has a higher level of security. Security of software components can save the software from the harm of illegal access and damages of its contents. Diverse approaches are available to tackle the issues of security of components from diverse perceptions. A detailed report of the existing approaches and techniques used for security purposes is needed through which the researchers should know the in-depth knowledge of approaches, tools, and techniques. The proposed research presents an SLR of the approaches used by practitioners to protect software systems for IoT. The study has searched the literature in the popular and well-known libraries, filters the relevant literature, organizes the filter papers, and extracts derivations from the selected studies based on different perspectives. The proposed research will help practitioners and researchers in presenting new algorithms, techniques, and solutions for efficient assessment of the software components from security perspectives.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. Nazir, S. Shahzad, M. Nazir, and H. U. Rehman, "Evaluating security of software components using analytic network process," in *Proceedings of the 11th International Conference on Frontiers of Information Technology (FIT)*, pp. 183–188, IEEE, Islamabad, Pakistan, December 2013.

[2] P. S. Sandhu and H. Singh, "A neuro-fuzzy based software reusability evaluation system with optimized rule selection," in *Proceedings of the 2006 International Conference on Emerging Technologies*, pp. 664–669, Peshawar, Pakistan, November 2006.

[3] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security analysis of IoT devices by using mobile computing: a systematic literature review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020.

[4] M. Li, S. Nazir, H. U. Khan, S. Shahzad, and R. Amin, "Modelling features-based birthmarks for security of end-to-end communication system," *Security and Communication Networks*, vol. 2020, Article ID 8852124, 9 pages, 2020.

[5] H. U. Rahman, A. U. Rehman, S. Nazir, I. U. Rehman, and N. Uddin, "Privacy and security—limits of personal information to minimize loss of privacy," in *Proceedings of the Future of Information and Communication Conference*, pp. 964–974, 2019.

[6] S. Nazir, S. Shahzad, S. Mahfooz, and M. N. Jan, "Fuzzy logic based decision support system for component security evaluation," *International Arab Journal of Information and Technology*, vol. 15, pp. 1–9, 2015.

[7] A. Rawashdeh and B. Matalkah, "A new software quality model for evaluating COTS components," *Journal of Computer Science*, vol. 2, no. 4, pp. 373–381, 2006.

[8] H. H. Song, "Testing and evaluation system for cloud computing information security products," in *Proceedings of the 3rd International Conference on Mechatronics and Intelligent Robotics (ICMIR-2019)*, pp. 84–87, Kunming, China, May 2019.

[9] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, 2020.

[10] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Computers & Security*, vol. 92, p. 101747, 2020.

[11] N. A. B. Mohd and Z. F. Zaaba, "A review of usability and security evaluation model of ecommerce website," in *Proceedings of the Fifth Information Systems International Conference 2019*, pp. 1199–1205, Surabaya, Indonesia, July 2019.

[12] Z. Katzir and Y. Elovici, "Quantifying the resilience of machine learning classifiers used for cyber security," *Expert Systems with Applications*, vol. 92, pp. 419–429, 2018.

[13] S. Alam, M. M. R. Chowdhury, and J. Noll, "Interoperability of security-enabled internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 567–586, 2011.

[14] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: the case study of a smart home," in *Proceedings of the 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, pp. 618–623, Kona, HI, USA, March 2017.

[15] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: current status, challenges and prospective measures," in *Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 336–341, London, UK, December 2015.

[16] A. W. Atamli and A. Martin, "Threat-based security analysis for the internet of things," in *Proceedings of the 2014 International Workshop on Secure Internet of Things*, pp. 35–43, Wroclaw, Poland, September 2014.

[17] K. C. Park and D.-H. Shin, "Security assessment framework for IoT service," *Telecommunication Systems*, vol. 64, no. 1, pp. 193–209, 2017.

[18] A. Tekeoglu and A. Ş. Tosun, "An experimental framework for investigating security and privacy of IoT devices," in *Proceedings of the International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments*, pp. 63–83, Vancouver, Canada, November 2017.

[19] O. Mazhelis and P. Tyrväinen, "A framework for evaluating Internet-of-Things platforms: application provider viewpoint," in *Proceedings of the 2014 IEEE World Forum on*

Internet of Things (WF-IoT), pp. 147–152, Seoul, South Korea, March 2014.

[20] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. K. A. A. Khan, "Performance analysis of machine learning algorithms in intrusion detection system: a review," *Procedia Computer Science*, vol. 171, pp. 1251–1260, 2020.

[21] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," *Future Generation Computer Systems*, vol. 107, pp. 433–442, 2020.

[22] S. Manjiatahsien, Hadiskarimipour, and Petrosspachos, "Machine learning based solutions for security of Internet of Things (IoT): a survey," *Journal of Network and Computer Applications*, vol. 161, 2020.

[23] X. Wang, J. Li, X. Kuang, Y.-A. Tan, and J. Li, "The security of machine learning in an adversarial setting: a survey," *Journal of Parallel and Distributed Computing*, vol. 130, pp. 12–23, 2019.

[24] M. Marwan, A. Kartit, and H. Ouahmane, "Security enhancement in healthcare cloud using machine learning," *Procedia Computer Science*, vol. 127, pp. 388–397, 2018.

[25] M. Belouch, S. El Hadaj, and M. Idhammad, "Performance evaluation of intrusion detection based on machine learning using Apache Spark," *Procedia Computer Science*, vol. 127, pp. 1–6, 2018.

[26] C. Hosmer, "IoT vulnerabilities," in *Defending IoT Infrastructures with the Raspberry Pi: Monitoring and Detecting Nefarious Behavior in Real Time*, pp. 1–15, Apress, Berkeley, CA, USA, 2018.

[27] W. Mao, Z. Cai, D. Towsley, Q. Feng, and X. Guan, "Security importance assessment for system objects and malware detection," *Computers & Security*, vol. 68, pp. 47–68, 2017.

[28] T. Halabi and M. Bellaiche, "Towards quantification and evaluation of security of cloud service providers," *Journal of Information Security and Applications*, vol. 33, pp. 55–65, 2017.

[29] M. Cheah, S. A. Shaikh, O. Haas, and A. Ruddle, "Towards a systematic security evaluation of the automotive bluetooth interface," *Vehicular Communications*, vol. 9, pp. 8–18, 2017.

[30] I. Sidenko, "Multi-Criteria selection of the wireless communication technology for specialized IoT network," in *Proceedings of the CEUR Workshop*, Rome, Italy, November 2014.

[31] B. Uslu, T. Eren, Ş. Gür, and E. Özcan, "Evaluation of the difficulties in the internet of things (IoT) with multi-criteria decision-making," *Processes*, vol. 7, no. 3, p. 164, 2019.

[32] A. Hinduja and M. Pandey, "An ANP-GRA-based evaluation model for security features of IoT systems," in *Advances in Intelligent Systems and Computing,Intelligent Communication, Control and Devices*, pp. 243–253, Springer, Berlin, Germany, 2020.

[33] I. Cvitić and M. Vujić, "Classification of security risks in the IoT environment," *Annals of DAAAM & Proceedings*, vol. 26, no. 1, 2015.

[34] J. Chen, Y. Lu, H. Wang, and C. Mao, "A quantitative assessment approach to COTS component security," *Mathematical Problems in Engineering*, vol. 2013, Article ID 165029, 11 pages, 2013.

[35] J. I. Choi and K. R. B. Butler, "Secure multiparty computation and trusted hardware: examining adoption challenges and opportunities," *Security and Communication Networks*, vol. 2019, Article ID 1368905, 28 pages, 2019.

[36] H. Zhang, Z. Cai, Q. Liu, Q. Xiao, Y. Li, and C. F. Cheang, "A survey on security-aware measurement in SDN," *Security and Communication Networks*, vol. 2018, Article ID 2459154, 14 pages, 2018.

[37] X. Su, Z. Wang, X. Liu, C. Choi, and D. Choi, "Study to improve security for IoT smart device controller: drawbacks and countermeasures," *Security and Communication Networks*, vol. 2018, Article ID 4296934, 14 pages, 2018.

[38] S. Zhang, X. Ou, and J. Homer, "Effective network vulnerability assessment through model abstraction," in *Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 17–34, Amsterdam, Netherlands, July 2011.

[39] P. Zech, M. Felderer, and R. Breu, "Knowledge-based security testing of web applications by logic programming," *International Journal on Software Tools for Technology Transfer*, vol. 21, no. 2, pp. 221–246, 2019.

[40] C. Wijayarathna and N. A. G. Arachchilage, "Using cognitive dimensions to evaluate the usability of security APIs: an empirical investigation," *Information and Software Technology*, vol. 115, pp. 5–19, 2019.

[41] R. Leszczyna, "Standards on cyber security assessment of smart grid," *International Journal of Critical Infrastructure Protection*, vol. 22, pp. 70–89, 2018.

[42] O.-M. Latvala, J. Toivonen, A. Evesti, M. Sihvonen, and V. Jordan, "Security risk visualization with semantic risk model," *Procedia Computer Science*, vol. 83, pp. 1194–1199, 2016.

[43] F. Munodawafa and A. I. Awad, "Security risk assessment within hybrid data centers: a case study of delay sensitive applications," *Journal of Information Security and Applications*, vol. 43, pp. 61–72, 2018.

[44] N. Thompson, T. J. Mcgill, and X. Wang, ""Security begins at home": determinants of home computer and mobile device security behavior," *Computers & Security*, vol. 70, pp. 376–391, 2017.

[45] B. Robisson, M. Agoyan, P. Soquet et al., "Smart security management in secure devices," *Journal of Cryptographic Engineering*, vol. 7, no. 1, pp. 47–61, 2017.

[46] F. Martín, E. Soriano, and J. M. Cañas, "Quantitative analysis of security in distributed robotic frameworks," *Robotics and Autonomous Systems*, vol. 100, pp. 95–107, 2018.

[47] S. Ismail, E. Sitnikova, and J. Slay, "Towards developing scada systems security measures for critical infrastructures against cyber-terrorist attacks," in *Proceedings of the IFIP International Information Security Conference*, pp. 242–249, Marrakech, Morocco, June 2014.

[48] S. Wu, Y. Zhang, and W. Cao, "Network security assessment using a semantic reasoning and graph based approach," *Computers & Electrical Engineering*, vol. 64, pp. 96–109, 2017.

[49] J. Almasizadeh and M. Abdollahi Azgomi, "Mean privacy: a metric for security of computer systems," *Computer Communications*, vol. 52, pp. 47–59, 2014.

[50] M. Abadi, "Software security: a formal perspective," in *Proceedings of the International Symposium on Formal Methods*, pp. 1–5, Paris, France, August 2012.

[51] L. Krautsevich, F. Martinelli, and A. Yautsiukhin, "Formal analysis of security metrics and risk," in *Proceedings of the IFIP International Workshop on Information Security Theory and Practices*, pp. 304–319, Crete, Greece, June 2011.

[52] I. Kotenko and E. Novikova, "Vissecanalyzer: a visual analytics tool for network security assessment," in *Proceedings of the International Conference on Availability, Reliability, and*

Security, pp. 345–360, Regensburg, Germany, September 2013.

[53] H.-K. Kim, W.-H. So, and S.-M. Je, "A big data framework for network security of small and medium enterprises for future computing," *The Journal of Supercomputing*, vol. 75, no. 6, pp. 3334–3367, 2019.

[54] T. Ibrahim, S. M. Furnell, M. Papadaki, and N. L. Clarke, "Assessing the usability of end-user security software," in *Proceedings of the International Conference on Trust, Privacy and Security in Digital Business*, pp. 177–189, Bilbao, Spain, August 2010.

[55] S. H. Houmb, I. Ray, I. Ray, and S. Chakraborty, "Trust-based security level evaluation using Bayesian belief networks," in *Transactions on Computational Science X*, pp. 154–186, Springer, Berlin, Germany, 2010.

[56] I. Garitano, S. Fayyad, and J. Noll, "Multi-metrics approach for security, privacy and dependability in embedded systems," *Wireless Personal Communications*, vol. 81, no. 4, pp. 1359–1376, 2015.

[57] J.-B. Gao, B.-W. Zhang, X.-H. Chen, and Z. Luo, "Ontology-based model of network and computer attacks for security assessment," *Journal of Shanghai Jiaotong University (Science)*, vol. 18, no. 5, pp. 554–562, 2013.

[58] G. Elahi, E. Yu, and N. Zannone, "A vulnerability-centric requirements engineering framework: analyzing security attacks, countermeasures, and requirements based on vulnerabilities," *Requirements Engineering*, vol. 15, no. 1, pp. 41–62, 2010.

[59] M. L. Hale, K. Lotfy, R. F. Gamble, C. Walter, and J. Lin, "Developing a platform to evaluate and assess the security of wearable devices," *Digital Communications and Networks*, vol. 5, no. 3, pp. 147–159, 2019.

[60] S. Crane and S. Pearson, "Security/trustworthiness assessment of platforms," in *Digital Privacy*, pp. 457–483, Springer, Berlin, Germany, 2011.

[61] M. Compastié, R. M. Badonnel, O. Festor, R. He, and M. Kassi-Lahlou, "Towards a software-defined security framework for supporting distributed cloud," in *Proceedings of the IFIP International Conference on Autonomous Infrastructure, Management and Security*, pp. 47–61, Zurich, Switzerland, July 2017.

[62] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Software-defined mobile networks security," *Mobile Networks and Applications*, vol. 21, no. 5, pp. 729–743, 2016.

[63] O. Kussul, N. Kussul, and S. Skakun, "Assessing security threat scenarios for utility-based reputation model in grids," *Computers & Security*, vol. 34, pp. 1–15, 2013.

[64] V. Casola, A. De Benedictis, A. Riccio, D. Rivera, W. Mallouli, and E. M. De Oca, "A security monitoring system for internet of things," *Internet of Things*, vol. 7, p. 100080, 2019.

[65] A. V. Uzunov, E. B. Fernandez, and K. Falkner, "ASE: a comprehensive pattern-driven security methodology for distributed systems," *Computer Standards & Interfaces*, vol. 41, pp. 112–137, 2015.

[66] A. M. Hoole, I. Traore, and I. Simplot-Ryl, "Application of contract-based security assertion monitoring framework for telecommunications software engineering," *Mathematical and Computer Modelling*, vol. 53, no. 3-4, pp. 522–537, 2011.

[67] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "An evaluation framework for network security visualizations," *Computers & Security*, vol. 84, pp. 70–92, 2019.

[68] H. Mumtaz, M. Alshayeb, S. Mahmood, and M. Niazi, "An empirical study to improve software security through the application of code refactoring," *Information and Software Technology*, vol. 96, pp. 112–125, 2018.

[69] A. K. Srivastava and S. Kumar, "An effective computational technique for taxonomic position of security vulnerability in software development," *Journal of Computational Science*, vol. 25, pp. 388–396, 2018.

[70] G. Spanos and L. Angelis, "A multi-target approach to estimate software vulnerability characteristics and severity scores," *Journal of Systems and Software*, vol. 146, pp. 152–166, 2018.

[71] M. Jouini, L. B. A. Rabai, and R. Khedri, "A multidimensional approach towards a quantitative assessment of security threats," *Procedia Computer Science*, vol. 52, pp. 507–514, 2015.

[72] W. Wang, K. R. Mahakala, A. Gupta, N. Hussein, and Y. Wang, "A linear classifier based approach for identifying security requirements in open source software development," *Journal of Industrial Information Integration*, vol. 14, pp. 34–40, 2019.

[73] A. Alebrahim and M. Heisel, "Towards developing secure software using problem-oriented security patterns," in *Proceedings of the International Conference on Availability, Reliability, and Security*, pp. 45–62, Fribourg, Switzerland, September 2014.

[74] J. Bürger, D. Strüber, S. Gärtner, T. Ruhroth, J. Jürjens, and K. Schneider, "A framework for semi-automated co-evolution of security knowledge and system models," *Journal of Systems and Software*, vol. 139, pp. 142–160, 2018.

[75] J. Davies, "Measuring subversions: security and legal risk in reused software artifacts," in *Proceedings of the 33rd International Conference on Software Engineering*, pp. 1149–1151, Honolulu, HI, USA, April 2011.

[76] D. Macdonald, S. L. Clements, S. W. Patrick et al., "Cyber/physical security vulnerability assessment integration," in *Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, pp. 1–6, Washington, DC, USA, February 2013.

[77] M. S. Kozlovszky, "Cloud security monitoring and vulnerability management," in *Critical Infrastructure Protection Research*, pp. 123–139, Springer, Berlin, Germany, 2016.

[78] S. Panasenko, "Evaluation of distributed security systems server modules peak workload," in *Proceedings of the 2013 International Conference on Anti-Counterfeiting, Security and Identification (ASID)*, pp. 1–4, Shanghai, China, October 2013.

[79] M. R. Razian and H. M. Sangchi, "A threatened-based software security evaluation method," in *Proceedings of the 2014 11th International ISC Conference on Information Security and Cryptology*, pp. 120–125, Tehran, Iran, September 2014.

[80] P. Morrison, "A security practices evaluation framework," in *Proceedings of the 2015 IEEE/ACM 37th IEEE International Conference on Software Engineering*, pp. 935–938, Florence, Italy, May 2015.

[81] J. Zhang, Q. Wu, R. Zheng, J. Zhu, M. Zhang, and R. Liu, "A security monitoring method based on autonomic computing for the cloud platform," *Journal of Electrical and Computer Engineering*, vol. 2018, Article ID 8309450, 9 pages, 2018.

[82] B. Bordel, R. Alcarria, D. M. De Andres, and I. You, "Securing Internet-of-Things systems through implicit and explicit reputation models," *IEEE Access*, vol. 6, pp. 47472–47488, 2018.

[83] F. Hategekimana, J. M. Mbongue, M. J. H. Pantho, and C. Bobda, "Inheriting software security policies within

hardware IP components," in *Proceedings of the 2018 IEEE 26th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*, pp. 53–56, Boulder, CO, USA, April 2018.

[84] I. Alsmadi and F. Mira, "Website security analysis: variation of detection methods and decisions," in *Proceedings of the 2018 21st Saudi Computer Society National Computer Conference (NCC)*, pp. 1–5, Riyadh, Saudi Arabia, April 2018.

[85] A. R. S. Farhan and G. M. M. Mostafa, "A methodology for enhancing software security during development processes," in *Proceedings of the 2018 21st Saudi Computer Society National Computer Conference (NCC)*, pp. 1–6, Riyadh, Saudi Arabia, April 2018.

[86] A. Wanniarachchi and C. Gamage, "RECSRF: novel technique to evaluate program security using dynamic disassembly of machine instructions," in *Proceedings of the 2019 21st International Conference on Advanced Communication Technology (ICACT)*, pp. 545–551, PyeongChang, South Korea, February 2019.

[87] B. Cruz, S. Gómez-Meire, D. Ruano-Ordás, H. Janicke, I. Yevseyeva, and J. R. Méndez, "A practical approach to protect IoT devices against attacks and compile security incident datasets," *Scientific Programming*, vol. 2019, Article ID 9067512, 11 pages, 2019.

[88] M. Saito, A. Hazeyama, N. Yoshioka et al., "A case-based management system for secure software development using software security knowledge," *Procedia Computer Science*, vol. 60, pp. 1092–1100, 2015.

[89] M. Ahmad, V. Costamagna, B. Crispo, F. Bergadano, and Y. Zhauniarovich, "StaDART: addressing the problem of dynamic code updates in the security analysis of android applications," *Journal of Systems and Software*, vol. 159, p. 110386, 2020.

[90] S. M. Ghaffarian and H. R. Shahriari, "Software vulnerability analysis and discovery using machine-learning and data-mining techniques: a survey," *ACM Computing Surveys*, vol. 50, no. 4, pp. 1–36, 2017.

[91] N. Schagen, K. Koning, H. Bos, and C. Giuffrida, "Towards automated vulnerability scanning of network servers," in *Proceedings of the 11th European Workshop on Systems Security*, pp. 1–6, Porto, Portugal, April 2018.

[92] G. Spanos, L. Angelis, and D. Toloudis, "Assessment of vulnerability severity using text mining," in *Proceedings of the 21st Pan-Hellenic Conference on Informatics*, pp. 1–6, Larissa, Greece, September 2017.

[93] P. Rotella, "Software security vulnerabilities: baselining and benchmarking," in *Proceedings of the 1st International Workshop on Security Awareness from Design to Deployment*, pp. 3–10, Gothenburg, Sweden, June 2018.

[94] C. Fruehwirth, S. Biffl, A. Schatten, D. Winkler, and W. D. Sunindyo, "Quantitative software security measurement in an engineering service bus platform," in *Proceedings of the 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement*, p. 1, Bozen, Italy, September 2010.

[95] L. Allodi, S. Banescu, H. Femmer, and K. Beckers, "Identifying relevant information cues for vulnerability assessment using CVSS," in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, pp. 119–126, Tempe, AZ, USA, March 2018.

[96] N. H. Pham, T. T. Nguyen, H. A. Nguyen, X. Wang, A. T. Nguyen, and T. N. Nguyen, "Detecting recurring and similar software vulnerabilities," in *Proceedings of the 2010 ACM/IEEE 32nd International Conference on Software Engineering*, pp. 227–230, Cape Town, South Africa, May 2010.

[97] S. E. Sahin and A. Tosun, "A conceptual replication on predicting the severity of software vulnerabilities," in *Proceedings of the Evaluation and Assessment on Software Engineering*, pp. 244–250, Copenhagen, Denmark, April 2019.

[98] T. Casey, P. Koeberl, and C. Vishik, "Threat agents: a necessary component of threat analysis," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, pp. 1–4, Oak Ridge, TN, USA, April 2010.

[99] G. Grieco, G. L. Grinblat, L. Uzal, S. Rawat, J. Feist, and L. Mounier, "Toward large-scale vulnerability discovery using machine learning," in *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, pp. 85–96, New Orleans, LA, USA, March 2016.

[100] Y. Lu, K. Mitropoulos, R. Ostrovsky, A. Weinstock, and V. Zikas, "Cryptographically secure detection of injection attacks," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2240–2242, Toronto, Canada, October 2018.

[101] S. Hameed, F. I. Khan, and B. Hameed, "Understanding security requirements and challenges in Internet of Things (IoT): a review," *Journal of Computer Networks and Communications*, vol. 2019, no. 11, pp. 1–14, 2019.

[102] A. Evesti and E. Ovaska, "Comparison of adaptive information security approaches," *International Scholarly Research Notices*, vol. 2013, Article ID 482949, 18 pages, 2013.

[103] W. Shang, T. Gong, C. Chen, J. Hou, and P. Zeng, "Information security risk assessment method for ship control system based on fuzzy sets and attack trees," *Security and Communication Networks*, vol. 2019, Article ID 3574675, 11 pages, 2019.

[104] J. Xu and D. Feng, "Identification of ICS security risks toward the analysis of packet interaction characteristics using state sequence matching based on SF-FSM," *Security and Communication Networks*, vol. 2017, Article ID 2430835, 17 pages, 2017.

[105] G. Wangen, C. Hallstensen, and E. Snekkenes, "A framework for estimating information security risk assessment method completeness," *International Journal of Information Security*, vol. 17, no. 6, pp. 681–699, 2018.

[106] S. Moshtari, A. Sami, and M. Azimi, "Using complexity metrics to improve software security," *Computer Fraud & Security*, vol. 2013, no. 5, pp. 8–17, 2013.

[107] M. A. V. Staalduinen, F. Khan, and V. Gadag, "SVAPP methodology: a predictive security vulnerability assessment modeling method," *Journal of Loss Prevention in the Process Industries*, vol. 43, pp. 397–413, 2016.

[108] H. Suleiman and D. Svetinovic, "Evaluating the effectiveness of the security quality requirements engineering (SQUARE) method: a case study using smart grid advanced metering infrastructure," *Requirements Engineering*, vol. 18, no. 3, pp. 251–279, 2013.

[109] Y. Kim, J. Nam, T. Park, S. Scott-Hayward, and S. Shin, "SODA: a software-defined security framework for IoT environments," *Computer Networks*, vol. 163, p. 106889, 2019.

[110] H. Maziku, S. Shetty, and D. M. Nicol, "Security risk assessment for SDN-enabled smart grids," *Computer Communications*, vol. 133, pp. 1–11, 2019.

[111] W. Yang, J. Li, Y. Zhang, and D. Gu, "Security analysis of third-party in-app payment in mobile applications," *Journal of Information Security and Applications*, vol. 48, p. 102358, 2019.

[112] S. Banescu, M. Ochoa, and A. Pretschner, "A framework for measuring software obfuscation resilience against automated attacks," in *Proceedings of the 2015 IEEE/ACM 1st International Workshop on Software Protection*, pp. 45–51, Florence, Italy, May 2015.

[113] B. Chernis and R. Verma, "Machine learning methods for software vulnerability detection," in *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics*, pp. 31–39, Tempe, AZ, USA, March 2018.

[114] S. Ouchani and M. Debbabi, "Specification, verification, and quantification of security in model-based systems," *Computing*, vol. 97, no. 7, pp. 691–711, 2015.

[115] M. Elsayed and M. Zulkernine, "Offering security diagnosis as a service for cloud SaaS applications," *Journal of Information Security and Applications*, vol. 44, pp. 32–48, 2019.

[116] C. Bodei, S. Chessa, and L. Galletta, "Measuring security in IoT communications," *Theoretical Computer Science*, vol. 764, pp. 100–124, 2019.

[117] M. Ge, J. B. Hong, W. Guttmann, and D. S. Kim, "A framework for automating security analysis of the internet of things," *Journal of Network and Computer Applications*, vol. 83, pp. 12–27, 2017.

[118] J. H. Lee and S. J. Kim, "Analysis and security evaluation of security threat on broadcasting service," *Wireless Personal Communications*, vol. 95, no. 4, pp. 4149–4169, 2017.

[119] J. Jürjens, K. Schneider, J. Bürger et al., "Maintaining security in software evolution," in *Managed Software Evolution*, pp. 207–253, Springer, Cham, Switzerland, 2019.

[120] D. Gupta, K. Chatterjee, and S. Jaiswal, "A framework for security testing," in *Proceedings of the International Conference on Computational Science and Its Applications*, pp. 187–198, Cagliari, Italy, July 2013.

[121] A. Goldstein and U. Frank, "Components of a multi-perspective modeling method for designing and managing IT security systems," *Information Systems and E-Business Management*, vol. 14, no. 1, pp. 101–140, 2016.

[122] V. Desnitsky and I. Kotenko, "Expert knowledge based design and verification of secure systems with embedded devices," in *Proceedings of the International Conference on Availability, Reliability, and Security*, pp. 194–210, Fribourg, Switzerland, September 2014.

[123] M. Cheah, S. A. Shaikh, J. Bryans, and P. Wooderson, "Building an automotive security assurance case using systematic security evaluations," *Computers & Security*, vol. 77, pp. 360–379, 2018.

[124] K. Beckers, I. Côté, S. Faßbender, M. Heisel, and S. Hofbauer, "A pattern-based method for establishing a cloud-specific information security management system," *Requirements Engineering*, vol. 18, no. 4, pp. 343–395, 2013.

[125] S. Y. Enoch, M. Ge, J. B. Hong, H. Alzaid, and D. S. Kim, "A systematic evaluation of cybersecurity metrics for dynamic networks," *Computer Networks*, vol. 144, pp. 216–229, 2018.

[126] J. Almasizadeh and M. A. Azgomi, "A stochastic model of attack process for the evaluation of security metrics," *Computer Networks*, vol. 57, no. 10, pp. 2159–2180, 2013.

[127] R. A. Oliveira, N. Laranjeiro, and M. Vieira, "Assessing the security of web service frameworks against Denial of service attacks," *Journal of Systems and Software*, vol. 109, pp. 18–31, 2015.

[128] A. R. Sai, J. Buckley, and A. Le Gear, "Assessing the security implication of Bitcoin exchange rates," *Computers & Security*, vol. 86, pp. 206–222, 2019.

[129] M. Hussain, A. Al-Haiqi, A. A. Zaidan et al., "A security framework for mHealth apps on Android platform," *Computers & Security*, vol. 75, pp. 191–217, 2018.

[130] G. Sciarretta, R. Carbone, S. Ranise, and A. Armando, "Anatomy of the facebook solution for mobile single sign-on: security assessment and improvements," *Computers & Security*, vol. 71, pp. 71–86, 2017.

[131] M. S. Ahmed, E. Al-Shaer, M. Taibah, and L. Khan, "Objective risk evaluation for automated security management," *Journal of Network and Systems Management*, vol. 19, no. 3, pp. 343–366, 2011.

[132] Z. Yan and C. Prehofer, "Autonomic trust management for a component-based software system," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 6, pp. 810–823, 2010.

[133] H. H. Albreiki and Q. H. Mahmoud, "Evaluation of static analysis tools for software security," in *Proceedings of the 2014 10th International Conference on Innovations in Information Technology (IIT)*, pp. 93–98, Al Ain, UAE, November 2014.

[134] M. L. Hale, D. Ellis, R. Gamble, C. Waler, and J. Lin, "Secu Wear: an open source, multi-component hardware/software platform for exploring wearable security," in *Proceedings of the 2015 IEEE International Conference on Mobile Services*, pp. 97–104, New York, NY, USA, June 2015.

[135] R. Al-Jaljouli, J. Abawajy, M. M. Hassan, and A. Alelaiwi, "Secure multi-attribute one-to-many bilateral negotiation framework for e-commerce," *IEEE Transactions on Services Computing*, vol. 11, no. 2, pp. 415–429, 2016.

[136] B. Potteiger, W. Emfinger, H. Neema, X. Koutosukos, C. Tang, and K. Stouffer, "Evaluating the effects of cyber-attacks on cyber physical systems using a hardware-in-the-loop simulation testbed," in *Proceedings of the 2017 Resilience Week (RWS)*, pp. 177–183, Wilmington, DE, USA, September 2017.

[137] K.-O. Detken, M. Jahnke, T. Rix, and A. Rein, "Software-design for internal security checks with dynamic integrity measurement (DIM)," in *Proceedings of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, pp. 367–373, September 2017, Bucharest, Romania.

[138] D. Migault, M. A. Simplicio, B. M. Barros et al., "A framework for enabling security services collaboration across multiple domains," in *Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pp. 999–1010, Atlanta, GA, USA, June 2017.

[139] R. Bloomfield, K. Netkachova, and R. Stroud, "Security-informed safety: if it's not secure, it's not safe," in *Proceedings of the International Workshop on Software Engineering for Resilient Systems*, pp. 17–32, Kiev, Ukraine, October 2013.

[140] D. W. Chadwick, W. Fan, G. Costantino et al., "A cloud-edge based data security architecture for sharing and analysing cyber threat information," *Future Generation Computer Systems*, vol. 102, pp. 710–722, 2020.

[141] P. Doty, "U.S. homeland security and risk assessment," *Government Information Quarterly*, vol. 32, no. 3, pp. 342–352, 2015.

[142] N. H. Pham, T. T. Nguyen, H. A. Nguyen, and T. N. Nguyen, "Detection of recurring software vulnerabilities," in *Proceedings of the IEEE/ACM International Conference on Automated Software Engineering*, pp. 447–456, Antwerp, Belgium, September 2010.

[143] K. Oishi and T. Matsumoto, "Self destructive tamper response for software protection," in *Proceedings of the 6th ACM Symposium on Information, Computer and*

Communications Security, pp. 490–496, Hong Kong, China, March 2011.

[144] S. Zhang, X. Meng, L. Wang, L. Xu, and X. Han, "Secure virtualization environment based on advanced memory introspection," *Security and Communication Networks*, vol. 2018, Article ID 9410278, 16 pages, 2018.

[145] H. Jo, J. Nam, and S. Shin, "NOSArmor: building a secure network operating system," *Security and Communication Networks*, vol. 2018, Article ID 9178425, 14 pages, 2018.

[146] Z. Xu, B. Chen, M. Chandramohan, Y. Liu, and F. Song, "Spain: security patch analysis for binaries towards understanding the pain and pills," in *Proceedings of the 2017 IEEE/ACM 39th International Conference on Software Engineering (ICSE)*, pp. 462–472, Buenos Aires, Argentina, May 2017.