Review Article

Multicriteria Decision and Machine Learning Algorithms for Component Security Evaluation: Library-Based Overview

Jibin Zhang ¹, Shah Nazir,² Ansheng Huang ¹ and Abdullah Alharbi³

¹Materials Corporation of Petro China Southwest Oil & Gasfield Company, Chengdu 610017, China

²Department of Computer Science, University of Swabi, Swabi, Pakistan

³Department of Information Technology, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia

Correspondence should be addressed to Ansheng Huang; huangansheng@petrochina.com.cn

Received 14 June 2020; Revised 1 July 2020; Accepted 3 July 2020; Published 10 September 2020

Academic Editor: Amir Anees

Copyright © 2020 Jibin Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Components are the significant part of a system which plays an important role in the functionality of the system. Components are the reusable part of a system which are already tested, debugged, and experienced based on the previous practices. A new system is developed based on the reusable components, as reusability of components is recommended to save time, effort, and resources as such components are already made. Security of components is a significant constituent of the system to maintain the existence of the component as well as the system to function smoothly. Component security can protect a component from illegal access and changing its contents. Considering the developments in information security, protecting the components becomes a fundamental issue. In order to tackle such issues, a comprehensive study report is needed which can help practitioners to protect their system. The current study is an endeavor to report some of the existing studies regarding component security evaluation based on multicriteria decision and machine learning algorithms in the popular searching libraries.

1. Introduction

Technology has made life easier but has exposed several security issues. Over the last few years with the development of Internet, the number of attacks has increased. Technology plays an inevitable role in human life. The Internet of Things (IoT) enables communication with different devices. The smart devices are connected to communicate, process, compute, and monitor diverse real-time scenarios. The devices are normally heterogeneous and have low memory and short power for processing. The concept of Internet of Things came with the challenges of privacy and security, as the conventional security protocol does not fit the devices of IoT. The information security of an organization is highly dependent on different types of information of the organization. Manager of the information security is not only

concerned with the relevant information but also with the interdependencies among this information. Individuals, government, and organizations are facing risks of information security. These risks can be damaged at a high level in terms of breach of confidentiality of sensitive data, financial loss, and loss of integrity and availability of data which is sensitive. Security of components plays an important role in the functionality of a system to run properly. Different studies are available for the security purpose [1–5]. The algorithms of ML have shown a considerable performance in different application fields such facial recognition, text recognition, spam detection, and so on. The applications of machine learning (ML) algorithms are obvious in different domain areas [2, 5–11].

The contribution of the proposed study is to present a comprehensive report on some of the existing state-of-the-

FIGURE 1: Relevant terminologies for security.

art research studies for component security evaluation based on multicriteria decision and machine learning algorithms. This study will support the researchers to extract the most useful insights of security to a particular domain to strengthen its existence and to avoid future hurdles.

The organization of the paper is as follows. Section 2 presents the related work to the current research, in particular to multicriteria decision and machine learning algorithm applications for component security evaluation. Section 3 briefly shows multicriteria decision and machine learning approaches to the security evaluation. Section 4 shows the library-based analysis of the existing literature from different perspectives in the most popular libraries.

2. Related Work

Different approaches are being proposed by researchers to tackle the issue of security from different perspectives. Saranya et al. [6] presented the study of comparisons of different machine learning algorithms for intrusion detection system with applications in different areas such as smart city, Internet of Things, fog computing, big data, and so on. The KDD-CUP dataset was used to test efficiency and compared with existing available research. For the information security products of cloud computing, a test evaluation system is established [1]. The security identification has a significant role in the field like Internet of Things in smart city. Manjia Tahsien et al. [8] presented an overview of the IoT architecture with a detailed review on machine learning algorithms, significance of IoT security with diverse types of attacks. The study proposed a model of the associated information management factors for the information security of organization. Firstly, they surveyed 136 articles to identify the information security factors, and secondly, a series of interviews with 19 experts from the industry to evaluate the relevancy of these factors. In third step, a complete model was developed [3]. The authors [12] conducted a detailed survey of the state-

of-the-art IoT security, deep learning, and big data technology.

Yuan and Luo [13] evaluated energy security of the Chinese provinces through analyzing the reasons and implementation of policy, with the help of MTGS and SPATOPSIS. Wijayarathna and Arachchilage [14] assessed the cognitive dimensions framework with the help of four security application programming interfaces, such as Bouncy Castle light weight Crypto API, Google Authentication API, OWASP Enterprise Security API, and Java Secure Socket Extension API. Wang et al. [9] presented a detailed overview of the security properties investigation of machine learning algorithms. They have analysed the security model of ML to build up a blueprint for multidisciplinary area of research. After that, the attack methods and the strategies of defense against them are discussed. The study presented an overview of the weaknesses and strengths of the available evaluation methods used for usability and security for the websites of electronic commerce (E-commerce). The evaluation models from 2000 to 2018 have been reviewed for E-commerce [4]. Many burning issues like untrustworthy information, insecure platform, malicious propagation, and illegal cheating exist. Security and trustworthiness play an important role for the communication among social interactions of sharing information and communication. Zhang et al. [15] proposed an approach for crowd assessing the security and trustworthiness of open social networks based on signaling theory.

Mao et al. [16] proposed a system for building security dependency to measure the significance of security of a system from a wide perspective of the system. The effect of small-world and power-law distribution for the degree for in- and out-degree in security dependency network was observed. Halabi and Bellaiche [17] proposed an approach for measuring performance and assessment of services of security for Cloud on the basis of set of assessment measures using Goal-Question-Metric. Cheah et al. [18] devised a systematic framework for security testing for interfaces of automotive Bluetooth and applied a tool of proof-of-concept

FIGURE 2: Publication type and total number.

to carry out testing on vehicle with the help of the proposed framework. Nazir et al. [19] proposed a methodology for evaluating the security of software components using the analytic network process. This technique works in the situation of complexity where dependencies exist among different nodes of network. Cherdantseva et al. presented an evaluation of a reference model of information assurance and security for summarizing the information required by the information assurance and security community [20]. Jouini et al. proposed a quantitative approach to security risk for information systems which is extendable, systematic, and modular. The study aimed to effectively evaluate security threat in a comprehensive way [21]. The study considered an approach to attack of computer modeling and security assessment which is recommended to realize in advanced Security Information and Event Management (SIEM)

systems. Subsorn and Limwiriyaikul [23] examined the security of internet banking of 16 Australian banks for finding the shortcomings which were probably affecting the confidentiality of the bank customers. Furthermore, the study investigated 12 Thai commercial banks and compared the results with those of the previous research. Kotenko and Chechulin [24] presented a framework for security assessment and attack modelling in security information and event management system.

3. Multicriteria Decision Making and Machine Learning Algorithms for Security Evaluation

Several techniques are being practiced in the literature for security evaluation [25–27]. These techniques evaluate the security from different perspectives. A number of machine

FIGURE 3: Places of conferences held.

FIGURE 4: Name and year of conferences held.

FIGURE 5: Total number of conferences held in the given year.

FIGURE 6: Article type total number of publication.

FIGURE 7: Publication title along with total number of publication.

learning algorithms are used for the detection of intrusion affecting the system of organizations. Shafiq et al. [7] proposed a novel framework and used BoT-IoT identification dataset and 44 features with the help of machine learning algorithm. After this, five effective machine learning algorithms are considered for the detection of anomaly and

malicious traffic with performance of evaluation measures of machine learning algorithm. An approach of bijective softest and its algorithm is applied to find effectiveness of machine learning algorithm. Mohanta et al. [2] reported the technology of IoT and its applications in different areas. The security issues such as integrity, availability, and

FIGURE 8: Total number of papers published in the given year.

FIGURE 9: Subjects along with the number of publications.

confidentiality and the issues are discovered. The applications of artificial intelligence, machine learning, and Blockchain for the issues of security for IoT are studied. Marwan et al. [10] proposed a ML based approach to secure the processing of data based on cloud environment. The support vector machines and fuzzy c-means clustering were used to classify the pixels of images in an efficient way. To reduce the disclosure of medical information, the module of

CloudSec into the conventional architecture of two-layered was incorporated.

Katzir and Elovic [5] presented the adversarial resilience based on supervised machine learning algorithm for detection systems. The study provides a definition of adversarial resilience with focus on system of multisensory fusion. Model robustness score was defined for evaluating the relative resilience of existing models, and then two

FIGURE 10: Subjects along with the number of publications.

FIGURE 11: Journal/magazine name and number of publication.

FIGURE 12: Proceeding/book name and number of publication.

novel feature selection algorithms for designing adversary aware classifiers were recommended. In network communication, one of the major concerns is the detection of intrusion. Different approaches are used for effective and efficient detection and prevention of intrusion and ensuring privacy and security. Four classifiers of machine learning algorithms that are, Naïve-Bayes, support vector

machine, decision tree, and Random Forest using Apache Spark were used to evaluate the performance of intrusion detection in network [11]. Apart from this, several approaches exist for security evaluation such as analytic network process, analytic hierarchy process, fuzzy logic, IoT-based security evaluation, and feature-based birthmarks [19, 28, 29].

FIGURE 13: Proceeding series and number of publication.

4. Library-Based Search for the Existing Research

Before, data security was simply a specialized concern and specialized representatives were answerable for data security issues inside an organization. Thus, in previous years, there was a shift of paradigm from the official innovation master to the obligation of administration and a more business-centred view ensuring data security. Nowadays, security supervisors are completely capable to consider and react to data security issues. Due to the move from a specialized to an administration point of view, the examination concentration additionally changed from specialized setting to investigating the administration job. Supervisors must have the option to accept specialized dangers just as different elements like human conduct into record to take the privilege

and powerful activities to moderate threats. Therefore, this examination has the reason to distinguish the key components and assess them and investigate between conditions to at last produce a thorough model to comprehend the security of data at multilevel nature and subsequently give high data security, the executive choices.

Multicriteria and machine learning algorithms plays an important role in security of information. Mostly, the security of the IoT devices is evaluated through machine learning algorithms. The purpose of this section is to identify the existing available research from different popular libraries in order to extract meaning insights for practitioners. These libraries mainly include ACM, Scienedirect, IEEE, Springer, Wiley, and Tailor & Francis. The query was considered as collection of different words. An individual word shows more materials which is very difficult to analyze.

FIGURE 14: Media format and number of publication.

FIGURE 15: Conference event and number of publication.

So the query was considered as the collection of different words with the operator “AND” and “OR” to show all the relevant materials. The mentioned libraries were searched based on the following queries:

(“software component” OR “component of software”) AND (“security evaluation OR security assessing”) AND (“multi criteria decision” OR “multi-criteria decision”) AND (“machine learning”), and/or (software component OR component of software) AND (security evaluation OR security assessing) AND (multi criteria decision OR multi-criteria decision) AND (machine learning)

The reasons behind the two queries is that entering the first query gives less amount of materials while the second query gives huge amount of materials. The study attempts to select more articles to give more detail information to the research community. These libraries were searched from different perspectives and the details are given in the following subsections. Figure 1 shows the relevant terminologies to the security.

The following subsections briefly show the details of the search process in the selected famous libraries. The reason behind the selection of these libraries is that these are the most popular and well-known libraries. Google scholar was not considered as there are more irrelevant materials and

FIGURE 16: Content type and total number of publication.

there is no authenticity to the materials that is relevant or irrelevant. It shows all the available sources, which is then difficult to analyse.

4.1. Searching Process in IEEE. The IEEE library was searched to find the relevant information regarding the applications of machine learning and multicriteria decision regarding security evaluation. Figure 2 shows the publication type and total number of publications related to the given search. These publications are categorized into different areas such as decision making, learning, fuzzy theory, genetic algorithm, and operational research.

The search process was further explored to find more relevant information of these studies. Figure 3 shows the places of conferences held.

Figure 4 shows the year of conferences held.

Figure 5 shows the total number of conferences held in the given year.

4.2. Searching Process in Sciencedirect Library. After searching the library of IEEE, it was felt that the other famous libraries should also be searched to see the relevant materials published in the literature. Figure 6 shows the article type in the form of conference, journal, book chapter, and review articles along with the total number of publications.

The publications were then checked that which paper is published in which specific journal/conference. Figure 7 shows the title of publication where the paper is published along with the total number of papers.

The searched papers were checked to show the year of publication that a paper is published in which particular

year. Figure 8 shows the total number of publications in the given year.

4.3. Searching Process in Wiley Library. The Wiley library was searched to find the relevant materials regarding particular search terms. This library does not contain more searching operations as compared to the other libraries. So, only the subjects related information along with the total number of publications is shown in Figure 9.

4.4. Searching Process in Tailor & Francis Library. The Tailor and Francis library was searched to get the most relevant information. Figure 10 shows the subjects of publication along with the total number of publication in the given library in which engineering and technology is on top followed by other disciplines.

4.5. Searching Process in ACM Library. The defined keywords were searched in the ACM library for obtaining relevant information. The ACM library contains several options to study the search results from different perspectives. These perspectives include the publication name where the paper is published, publication types, proceedings, media format, and many others. Figure 11 shows the journal/magazine name along with the total number of papers published for the search process.

Figure 12 shows the proceedings/book name along with the total number of publications in the ACM library.

Figure 13 shows the proceedings series along with the total number of publications.

The search process in this library was further explored to show the media format that which is the

FIGURE 17: Discipline and total number of publications.

particular format of publication. The media format includes, PDF, image, HTML, Archive/Zip, and video. Figure 14 shows the media format of the publication in the ACM library.

Figure 15 shows the event of the conferences along with the total number of publications.

Figure 16 shows the content type along with the number of publications in the ACM library for the search process. The content types include research article, tutorial, column, monograph, prefatory, index, section, demonstration, interview, introduction, and short paper.

4.6. Searching Process in Springer Library. The Springer library was searched to show the relevant materials published for

the given query and keywords. This library contains different options for searching a particular query of keywords. Figure 17 shows the discipline and total number of publications.

Figure 18 shows the content type and total number of publications in the Springer library.

Figure 19 shows publications type of all publications and total number.

5. Conclusion

Security of components plays an important role in a system to function properly. The components are reusable parts of a system which are reused to save time, effort, and cost of developments. Components can be reused as they are already tested, debugged, and experienced. Component

FIGURE 18: Content type and total number of publication.

FIGURE 19: All publications and total number.

security can protect a component from illegal access, use, and change of its contents. Considering the developments in information security, protecting the components becomes a fundamental issue. To tackle this issues, a comprehensive study report is needed which can help practitioners to protect their system. The present study reports some of the available research regarding component security evaluation based on multicriteria decision and machine learning algorithms in the popular searching libraries. Different perspectives of the search process are shown to show the existence of the research related to the current research. Based on the available literature summarized in this paper, researchers can take help from it as evidence and can propose new ideas. In future, the proposed research can be extended to a more detailed analysis from different perspectives such as feature-based security evaluation and real-time security evaluation.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

- [1] 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, Yunnan, China, May 2019.
- [2] 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, Article ID 100227, 2020.
- [3] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Computers & Security*, vol. 92, Article ID 101747, 2020.
- [4] 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.
- [5] 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.
- [6] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. K. A. Ahamed Khan, "Performance analysis of machine learning algorithms in intrusion detection system: a review," *Procedia Computer Science*, vol. 171, pp. 1251–1260, 2020.
- [7] 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.
- [8] S. Manjia Tahsien, H. karimipour, and P. spachos, "Machine learning based solutions for security of internet of things (IoT): a survey," *Journal of Network and Computer Applications*, vol. 161, Article ID 102630, 2020.
- [9] 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.
- [10] M. Marwan, A. Kartit, and H. Ouahmane, "Security enhancement in healthcare cloud using machine learning," *Procedia Computer Science*, vol. 127, pp. 388–397, 2018.
- [11] 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.
- [12] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin et al., "Deep learning and big data technologies for IoT security," *Computer Communications*, vol. 151, pp. 495–517, 2020.
- [13] J. Yuan and X. Luo, "Regional energy security performance evaluation in China using MTGS and SPA-TOPSIS," *Science of the Total Environment*, Article ID 133817, vol. 696, pp. 1–11, 2019.
- [14] 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.
- [15] Z. Zhang, J. Wen, X. Wang, and C. Zhao, "A novel crowd evaluation method for security and trustworthiness of online social networks platforms based on signaling theory," *Journal of Computational Science*, vol. 26, pp. 468–477, 2017.
- [16] 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.
- [17] 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.
- [18] 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.
- [19] 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, Islamabad, Pakistan, December 2013.

- [20] Y. Cherdantseva, J. Hilton, O. Rana, and W. Ivins, "A multifaceted evaluation of the reference model of information assurance & security," *Computers & Security*, vol. 63, pp. 45–66, 2016.
- [21] M. Jouini, L. B. A. Rabai, and R. Khedri, "A multidimensional approach towards a quantitative assessment of security threats," in *Proceedings of the Procedia Computer Science the 6th International Conference on Ambient Systems, Networks and Technologies*, pp. 507–514, London, UK, December 2015.
- [22] I. Kotenko and A. Chechulin, "Computer attack modeling and security evaluation based on attack graphs," in *Proceedings of the 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems*, pp. 614–619, Berlin, Germany, September 2013.
- [23] P. Subson and S. Limwiriyakul, "A comparative analysis of internet banking security in Thailand: a customer perspective," *Procedia Engineering*, vol. 32, pp. 260–272, 2012.
- [24] I. Kotenko and A. Chechulin, "Common framework for attack modeling and security evaluation in SIEM systems," in *Proceedings of the IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber*, pp. 94–101, Besançon, France, 2012.
- [25] 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, 2020.
- [26] 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, San Francisco, CA, USA, March 2019.
- [27] B. A. Sassani, M. Alkorbi, N. Jamil, M. A. Naeem, and F. Mirza, "Evaluating encryption algorithms for sensitive data using different storage devices," *Scientific Programming*, Article ID 6132312, vol. 2020, pp. 1–9, 2020.
- [28] 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, p. 1, 2020.
- [29] 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.