A Systematic Mapping Study on Approaches for AI-Supported Security Risk Assessment

Gencer Erdogan, Enrique Garcia-Ceja, Åsmund Hugo, Phu H. Nguyen, and Sagar Sen
SINTEF, Oslo, Norway
firstname.lastname@sintef.no

***Abstract*—Effective assessment of cyber risks in the increasingly dynamic threat landscape must be supported by artificial intelligence techniques due to their ability to dynamically scale and adapt. This article provides the state of the art of AI-supported security risk assessment approaches in terms of a *systematic mapping study*. The overall goal is to obtain an overview of security risk assessment approaches that use AI techniques to identify, estimate, and/or evaluate cyber risks. We carried out the systematic mapping study following standard processes and identified in total 33 relevant primary studies that we included in our mapping study. The results of our study show that on average, the number of papers about AI-supported security risk assessment has been increasing since 2010 with the growth rate of 133% between 2010 and 2020. The risk assessment approaches reported have mainly been used to assess cyber risks related to intrusion detection, malware detection, and industrial systems. The approaches focus mostly on identifying and/or estimating security risks, and primarily make use of Bayesian networks and neural networks as supporting AI methods/techniques.**

***Index Terms*—security, risk assessment, cyber risk, artificial intelligence, mapping study**

I. Introduction

Public and private organizations highlight the need to develop and improve threat and risk management approaches supported by artificial intelligence (AI) [1]. This view is substantiated by Gartner, who report that "the general increase in information will mean artificial security intelligence is necessary" [2]. Moreover, Gartner states that "more information security decisions need to move toward a real-time assessment of risk and trust at the point in time that the security decision is made, using relevant context to enrich and inform the decision-making process and to enable real-time, adaptive, risk-based responses for access enablement and protection from threats and attacks" [3]. Thus, to successfully identify, estimate, and evaluate current and future cyber risks in the increasingly dynamic threat landscape, cyber risk assessment must be supported by artificial intelligence techniques.

This paper presents the results of our systematic mapping study addressing security risk assessment (SRA) approaches that are supported by artificial intelligence techniques. The overall contribution is an overview of security risk assessment approaches that use AI techniques to identify, estimate, and/or evaluate cyber risks. We obtain this overview by answering the following research questions:

RQ1. How much activity has there been in AI supported security risk assessment (AIS-SRA) since 2010?

RQ2. In which domain has AI supported security risk assessment been applied?

RQ3. Which security risk assessment tasks have been supported by AI methods?

RQ4. What types of AI methods have been used in security risk assessment?

The remainder of this paper is organized as follows. In Section II, we provide the background necessary to understand the terms we use in the mapping study. In Section III, we describe the systematic mapping process used in our study, while in Section IV we provide our findings with respect to the research questions. We discuss related work in Section V and finally conclude the paper in Section VI.

II. Background and Terminology

This section describes the technical terms related to AI-supported security risk assessment used in the mapping study.

A. Security Risk Assessment

Security refers to the preservation of confidentiality, integrity and availability of information [4]. Security risk assessment consists of three consecutive steps: risk identification, risk estimation, and risk evaluation [5]. The following paragraphs explain each step.

Risk identification is the process of finding, recognizing and describing risks. This involves identifying sources of risk, areas of impact, events (including changes in circumstances), their causes and their potential consequences. Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs [5].

Risk estimation is the process of comprehending the nature of risk and determining the level of risk. Risk estimation provides the basis for risk evaluation and decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods [5].

Risk evaluation is the process of comparing the results of risk estimation with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation assists in the decision about risk treatment [5].

B. Artificial Intelligence

Artificial intelligence can be defined as "the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings" [6]. There are two fields that are strongly related with AI: i) machine learning

978-1-6654-2463-9/21/$31.00 ©2021 IEEE
DOI 10.1109/COMPSAC51774.2021.00107

and ii) deep learning. Machine learning can be thought of as a sub-field of AI and deep learning as a sub-field of machine learning. Machine learning refers to the set of algorithms that automatically find useful patterns and relationships from data. Machine learning methods can be categorized into two main groups based on the presence or absence of labels: *Supervised learning* and *Unsupervised learning*. In the former, the data point's labels are available at training time whereas in the latter there are no labels. In our systematic mapping study, most of the work fell into the category of supervised learning.

Deep learning consists of a set of methods and architectures primarily based on artificial neural networks (ANNs). Artificial neural networks are learning methods inspired by the brain. However, it does not mean that ANNs actually work as their biological counterpart. In the early days of ANNs it was difficult to train artificial neural networks due to computational constraints, even for moderate-sized networks. New technological advancements such as graphical processing units (GPUs) and more efficient methods to estimate the optimal network weights have allowed to build larger networks with more hidden layers. Even though it is not a strict rule, ANNs with more than two hidden layers are already considered to be deep learning models. Deep learning does not only mean more hidden layers, but it also encompasses different network architectures being some of the most common Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Autoencoders. CNNs are mainly used for computer vision tasks. RNNs are suitable for sequential data such as time series, text, video, and voice. Autoencoders are neural networks trained to produce as output the same data as their input. Autoencoders have several applications such as dimensionality reduction, denoising, and compression.

III. Systematic mapping process

The process applied in this systematic mapping study is based on the approach suggested by Kitchenham et al. [7]. Section III-A presents the selected keywords and the constructed query string. Section III-B describes the inclusion and exclusion criteria. In Section III-C, we describe our search strategy, and in Section III-D we present the classification scheme used to group and analyze the primary studies.

A. Keywords and Query String

The keywords for Security risk assessment (SRA) and AI were divided into the following general and specific terms. **SRA general terms:** security, threat, risk, assessment, management, cybersecurity. **SRA specific terms:** malware, adversary, hacker. **AI general terms:** AI, artificial intelligence, machine learning. **AI specific terms:** deep learning, neural network, convolutional neural network, recurrent neural network, generative adversarial network, bayesian network, genetic algorithm, expert system. Based on these keywords, the following query string was constructed:

((risk OR security OR threat OR cybersecurity OR malware OR adversary OR hacker) AND (assessment OR management)) AND (AI OR artificial intelligence OR machine learning OR deep learning OR neural network OR convolutional neural network OR recurrent neural network OR generative adversarial network OR bayesian network OR genetic algorithm OR expert system)

The query string was formed by joining the security related terms with AI related terms using a conjunction. The first clause (security) was formed by joining the security related keywords (risk, security, threat, etc.) with OR. Next, this clause was joined with an AND to the two keywords assessment and management. This was done to cover different commonly used combinations such as "security risk assessment", "threat management", "risk management", etc. The second clause (AI) was formed by joining the general AI terms with the AI method terms using an OR. The rationale behind this is that some work can use AI methods without explicitly mentioning the broader field. For example, an article using neural networks may not mention the word AI or machine learning but neural networks belong to those two broader fields.

B. Inclusion and Exclusion Criteria

We defined five inclusion criteria and six exclusion criteria. The inclusion criteria were: i) the paper is written in English, published in a peer-reviewed journal or as part of the proceedings from a conference/workshop, ii) papers from 2010 and onwards, iii) the approach must use at least one AI method, iv) the paper is among the first 1000 results and, v) the paper tackles at least one specific cybersecurity issue.

The six exclusion criteria were: i) papers having less than four pages double column or six pages single column, ii) papers that do not provide technical details, iii) papers that do not provide any quantitative evaluation for the proposed approach, iv) surveys or literature reviews, v) the paper appears after 40 consecutive non-included search entries, and vi) papers that do not explicitly support security risk assessment.

C. Search Strategy and Selection Process

Fig. 1 shows the steps of the search and selection process. In our study, we considered five scientific databases namely, IEEE Xplore[1], ACM DL[2], Springer[3], Science Direct[4], and Scopus[5]. We adapted the query string (presented in Section III-A) for the input format required by each of the databases. From the results, we analysed each paper and determined if it should be included according to the inclusion/exclusion criteria. First, we reviewed the title and abstract of each paper. If these two pieces of information were not enough to make a decision then, the content of the paper was skimmed. Each database was assigned to one of the authors of this study and the search was conducted independently.

Since some databases may contain papers included in others, we looked for duplicates and removed them. To be more specific, we kept the selected papers from IEEE Xplore

[1]http://ieeexplore.ieee.org
[2]https://dl.acm.org
[3]https://link.springer.com
[4]https://www.sciencedirect.com
[5]https://www.scopus.com

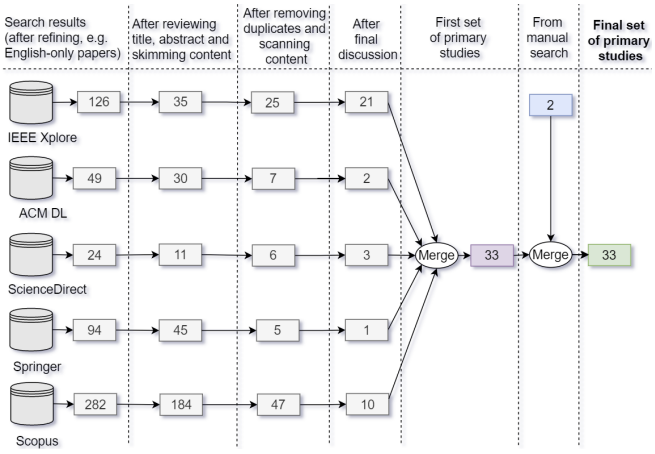

Fig. 1. Overview of the search and selection steps. Numbers inside boxes indicate number of papers.

and removed the duplicates from the other sources. This is why the primary studies mostly come from IEEE Xplore, as illustrated in Fig. 1. There are significant drops of candidate papers between skimming and scanning steps in some sources like ACM DL and Scopus. Besides the reason of removing duplicates, the drops also show the different strategies in removing candidate papers by each reviewer. There were many papers about malware detection using AI but not really having risk assessment aspects. Some reviewers decided to remove them right after skimming through the content. Others only decided to remove such papers after scanning the content. We held group discussions between reviewers to synchronize on the selection in the following step.

If additional information was needed to decide whether to include a paper, the paper was scanned in more detail and some key data was extracted. Next, we had rounds of group discussions (cross-check) where we decided by majority vote if papers in doubt should be included. At this step, we also removed any paper that already had a more extensive version covering its content. For example, we removed a conference paper when we already included its journal version. In the end, the database search and selection process yielded the first set of 33 primary studies.

We also performed backward snowballing [8] by manually checking the references of the 33 selected papers to find other primary studies. We found two papers that were complementary to two existing selected papers and did not count them as new primary studies. After this process, we finalized with a set of 33 primary studies in which two primary studies were presented in more than one paper.

D. Classification Scheme

We addressed our RQs by extracting information from the selected papers based on the following three categories.

Security Risk Assessment: risk identification, risk estimation, risk evaluation (steps supported by the approach).

Machine Learning & AI: Type of machine learning approach: supervised, semi-supervised, and unsupervised learning. Deep learning methods: ANNs, CNNs, RNNs, and Autoencoders. Other methods like genetic algorithms and Bayesian networks. Input features: The features extracted from preprocessing phases and used for training machine learning models, such as images, byte code, and emails. Target: The target is the output prediction of the model. It could be the individual classes that the input variables may be mapped to in case of a classification problem or the output value range in a regression problem. Some examples are malware signatures, URL injection, and anomalies.

General Aspects: Application domains (authentication, government, human resources, industrial, IoT, malware, mobile apps, network, risk management, and social network), publication year, published in conference proceedings or journals, authors' affiliation (industry/academia/mixed).

IV. Results

Table I shows the complete list of primary studies included in our study. In total, 33 papers were included in our study where we considered papers published in the year range 2010 to 2020. The majority of the papers were produced by academia (29 papers), while 4 papers were produced by joint academia and industry. Moreover, with respect to publication type, there are 20 conference papers and 13 journal papers. In the following, we present the results grouped with respect to our research questions RQ1–RQ4.

A. RQ1: How much activity has there been in AI supported security risk assessment (AIS-SRA) since 2010?

Fig. 2 shows the number of publications per year. On average, there were three papers per year. We found the highest number of published primary studies (eight) for the year 2020 even though we stopped our search and selection process in October 2020. Fig. 2 also shows the linear trend over time. On average, the number of papers about AIS-SRA has been increasing since 2010 with the growth rate of 133% between 2010 and 2020 with a cumulative total of 33 articles published in 10 years. However, due to the small sample size we cannot make strong conclusions about this trend.

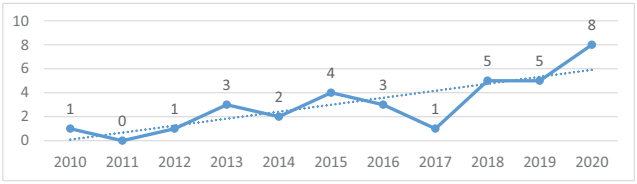

Fig. 2. Number of papers in the study per year.

B. RQ2: In which domain has AI supported security risk assessment been applied?

Fig. 3 shows the paper counts for the domains in which AI supported security risk assessment has been applied.

TABLE I
PRIMARY STUDIES

#	Year	Full Title	v	f
[S1]	2020	Risk Assessment Scheme for Mobile Applications Based on Tree Boosting	J	A
[S2]	2020	Classifying network abnormalities into faults and attacks in IoT-based cyber physical systems using machine learning	J	M
[S3]	2020	TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data	J	A
[S4]	2020	Cybersecurity threats based on machine learning-based offensive technique for password authentication	J	A
[S5]	2020	A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model	J	M
[S6]	2020	Dynamic Expert System-Based Geographically Adapted Malware Risk Evaluation Method	J	A
[S7]	2020	Dynamic Attack Scoring Using Distributed Local Detectors	C	A
[S8]	2020	Bayesian Network Based C2P Risk Assessment for Cyber-Physical Systems	J	A
[S9]	2019	Learning about risk: Machine learning for risk assessment	J	A
[S10]	2019	Decision-Making Method for Estimating Malware Risk Index	J	A
[S11]	2019	Cyberthreat detection from twitter using deep neural networks	C	A
[S12]	2019	Deep Learning Analytics for IoT Security over a Configurable BigData Platform: Data-Driven IoT Systems	C	M
[S13]	2019	I-HMM-Based Multidimensional Network Security Risk Assessment	J	A
[S14]	2018	Classifying IoT security risks using Deep Learning algorithms	C	A
[S15]	2018	Risk assessment of autonomous vehicles using bayesian defense graphs	C	M
[S16]	2018	An improved information security risk assessments method for cyber-physical-social computing and networking	J	A
[S17]	2018	A model-data integrated cyber security risk assessment method for industrial control systems	C	A
[S18]	2018	Intelligent Risk Management Framework for BYOD	C	A
[S19]	2017	Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks	C	A
[S20]	2016	Droidscribe: Classifying android malware based on runtime behavior	C	A
[S21]	2016	S.A.V.I.O.R: security analytics on asset vulnerability for information abstraction and risk analysis	C	A
[S22]	2015	Cyber security risk assessment using an interpretable evolutionary fuzzy scoring system	C	A
[S23]	2015	Risk Assessment of Public Safety and Security Mobile Service	C	A
[S24]	2015	Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems	J	A
[S25]	2015	Information Risk Analysis in a Distributed MOOC Based Software System Using an Optimized Artificial Neural Network	C	A
[S26]	2015	Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops	C	A
[S27]	2014	Biologically inspired risk assessment in cyber security using neural networks	C	A
[S28]	2014	Towards automated risk assessment and mitigation of mobile applications	J	A
[S29]	2013	The e-government system risk assessment model based on dynamic threat and fuzzy neural network	C	A
[S30]	2013	Risk assessment and analysis through population-based attack graph modelling	C	A
[S31]	2013	A Genetic Algorithm Approach for the Most Likely Attack Path Problem	C	A
[S32]	2012	A multi-objective genetic algorithm for minimising network security risk and cost	C	A
[S33]	2010	Implementation and comparison of machine learning classifiers for information security risk analysis of a human resources department	C	A

[v] Venue type: J = Journal (13), C = Conference (20)
[f] Authors' affiliations: I = Industry (0), A = Academia (29), M = Mixed Academia & Industry (4)
* sorted by year of publication

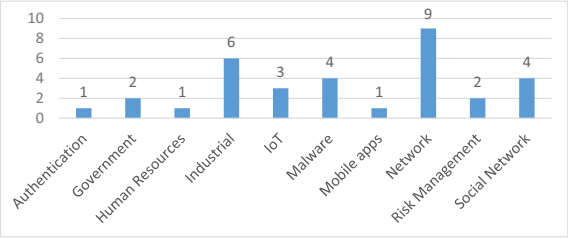

Fig. 3. AI supported security risk assessment applied in domains.

We see that the domains are very diverse and the most popular one is *network*. In the network domain, AIS-SRA has been used mainly for intrusion detection [S2], [S7], [S18]. AIS-SRA has also been applied in the *malware* domain particularly, for malware detection in mobile technologies [S1], [S20] and risk evaluation [S6].

Industrial systems are attractive targets for attackers due to the potential of illegally obtaining benefits (e.g., by stealing credential information), but also because of the high impact that can be caused by disrupting the system. Thus, it comes at no surprise that several works have addressed these issues in industrial settings, specifically for industrial control systems [S17], [S19], [S24].

C. RQ3: Which security risk assessment tasks have been supported by AI methods?

The Sankey diagram in Fig. 5 shows on the right-most lane the number of approaches supporting one or more steps of the security risk assessment process. In total, nine approaches support security risk identification only, nine approaches support security risk estimation only, seven approaches support both security risk identification and estimation (I and E), and finally, eight approaches support security risk identification, estimation, and evaluation (All).

Moreover, Fig. 5 indicates that most approaches use AI methods to either identify or estimate security risks, or both identify and estimate security risks. Approaches that use AI methods to support risk evaluation has received the least attention in the literature.

D. RQ4: What types of AI methods have been used in security risk assessment?

We discovered that 31 out of the 33 primary studies use a supervised learning approach. Unsupervised learning is used in one paper [S26] and another paper uses both semi-supervised and unsupervised learning [S7].

Fig. 4 shows the most commonly used AI methods. The diagram shows only the methods that are used by more than one study. Note that some studies use more than one method as well. Bayesian networks and neural networks are the most used methods. However, we note that some of these methods are included in the query string as part of our search process described earlier (e.g., *bayesian network*, *neural network*) thus making papers covering these methods more likely to appear in the search results. From the top five used methods, four of them are part of the query string except support vector machine (SVM). Other methods like self-organizing maps, Dagging, auto-encoders, expert system rules, topic clustering, Monte Carlo, K-nearest neighbors (KNN), and random forest were reported in at most one paper.

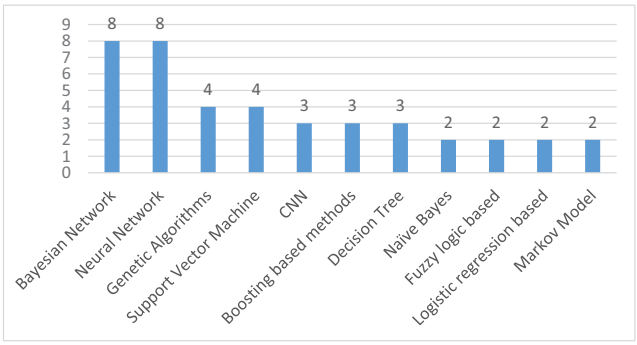

Fig. 4. Most commonly used AI methods for SRA.

In the last years, deep learning methods have gained a lot of attention due to their flexibility and performance results. To this extent, we wanted to investigate how deep learning methods have been used over time. From the primary studies list, the first occurrence of such a paper was in 2018, and it increased to 5 occurrences in 2019 and 2020.

E. Summary of Results

We present the cross-cutting flow of research in the period 2010-2020 to preferences of AI models, applications domains, and the supporting risk assessment tasks in Fig. 5. Five lanes in Fig. 5 represent (L1) total number of articles (L2) publication year (L3) AI model (L4) risk assessment domain (L5) risk assessment task, when read from left to right. Risk assessment domains in L4 are **Networks** on attacks and intrusion on networks, **CPS** on cyber-physical systems, Internet of things, industrial control systems, autonomous vehicles, and smart home settings, **Social** on social networks such as Twitter and hacker forums, **General** on cybersecurity risk without addressing a specific application domain, **Software** on mobile software and password authentication in web applications, **Malware** on malware classification and detection, **People Services** on IT-based services interfacing people for human resource management, education on Massive Open Online Courses (MOOCs) and e-governance platforms, **Oil and Gas** on safety and security risks in the Oil and Gas sector.

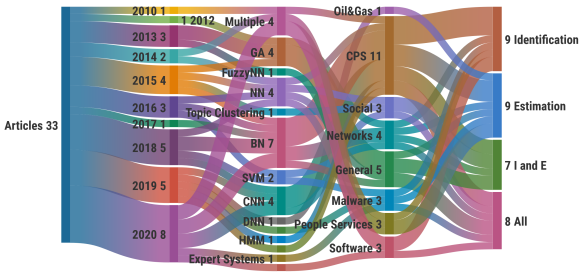

Fig. 5. Sankey diagram of AI approaches and the risk assessment tasks supported over the years.

We observe that there is a growing interest in security risk assessment over the years (L2). Bayesian networks and deep learning models such as CNNs have been quite popular after 2015 shifting from genetic algorithms (GA) and standard neural networks (NNs) (L2,L3). There has been considerable focus on using Bayesian networks and CNNs to support risk assessment in CPS and Computer Networks. However, there is lack of research for risk assessment in software despite Marc Andreessen's famous quote "Software is eating the world". AI models to learn human factors such as cyber-attacks originating in hacker chat forums or communication of attacks on Twitter to minimize impact are in their infancy. Malware classification has been thoroughly investigated, however, not many take the next step to perform security risk assessment. Articles performing risk assessment for malware rely traditionally on explainable approaches such as SVMs, expert systems, and Markov models instead of deep learning. Risk assessment in critical infrastructures such as Oil and Gas has only been explored in one article using DNNs [S9]. IT-based people services have little work on risk assessment, although they form the foundation of our post COVID-19 remote work society. Risk identification and risk estimation in isolation and in combination are equally well explored as shown in L5. However, risk evaluation, the step where risks are evaluated and deemed acceptable or unacceptable, is largely ignored. It can be seen that as we go further away from the technical systems (CPS, Networks, Software) to terminology that is more domain specific such as Oil and Gas and People services there is practically not much research that perform a full risk assessment.

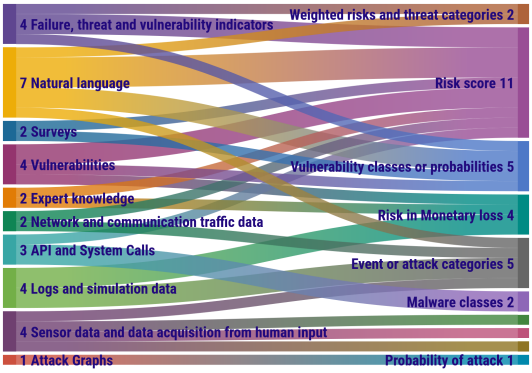

Fig. 6. Sankey diagram of Inputs and Outputs in AI models.

We present input artifacts we encountered in the study (Lane LI) and the output variables (Lane LO) in Fig. 6. Most observed outputs in LO are *numerical values of risk* such as change in risk, and cumulative risk in order to estimate risk. Input artifacts include surveys, natural language, logs and simulation data, vulnerabilities, API and system calls, expert knowledge, indicators of failure/threat/vulnerabilities, and network traffic data (LI). Many research articles predict classes and probabilities of vulnerabilities and events/attacks, threat classes and probabilities, and malware classes from almost all types of input artifacts. Research shows that the growing trend on the Internet of Things has resulted in the prediction of risk categories from patterns in sensor data. Unsupervised learning and semi-supervised learning is underexplored in security risk assessment.

V. Related Work

Security risk assessment is a proliferating field and several surveys and literature reviews have been published with the objective of summarising and categorising the advancements across the vast landscape of work within this field [9], [10]. There have been several surveys that aim to provide an overview of different industrial aspects with respect to risk assessment. For instance, Knowles et al. [11] conducted a survey about methodologies and research for measuring and managing risk in industrial control systems and with an

emphasis on metrics. Cherdantseva et al. [12] conducted a similar study in the context of Supervisory Control and Data Acquisition (SCADA) systems.

Hegde et al. [13] report on a literature survey in which they review applications of machine learning methods for engineering risk assessment, and Baryannis et al. [14] report on a systematic mapping study in which they review supply chain literature that addresses supply chain risk management using approaches that fall within the AI spectrum. Both of these literature surveys are similar to the systematic mapping study we report in this paper considering approaches using artificial intelligence methods for risk assessment. However, while Hegde et al. [13] report on approaches specifically for *safety* risk assessment and Baryannis et al. [14] report on approaches specifically for *supply chain* risk assessment, we report on approaches for *cybersecurity* risk assessment. Thus, our systematic mapping study complements the literature surveys carried out by Baryannis et al. [14] and Hegde et al. [13] addressing different domains.

Other cybersecurity risk assessment surveys and reviews have been published in the last years covering specific domains such as smart grids [15] and Internet of Things [16], to name a few. Even though, some of those reviews sporadically mention some AI methods, it is not their primary focus. As opposed to previous reviews, the present work explicitly studies the intersection between AI and security risk assessment including the utilised machine learning methods and the supported tasks.

VI. Conclusions

We present a systematic mapping study with the objective to obtain an overview of security risk assessment approaches that use AI techniques to identify/estimate/evaluate cyber risks.

Our final set of 33 primary studies is not very large for drawing many conclusions. However, we find that the set shows a high-level landscape of the research work in this direction so far, which can give us a glimpse of the trend. Moreover, we mitigate the risk of missing out important primary studies by defining inclusion and exclusion criteria in advance and discussing in plenum the papers in doubt. Finally, we adapted our search string to fit each of the five search engines we used as well as carrying out backward snowballing on the primary studies included in our study.

The study shows that on average, the number of papers about AI-supported security risk assessment has been increasing since 2010 with the growth rate of 133% between 2010 and 2020. AI-supported security risk assessment has mainly been used to assess cyber risks related to intrusion detection, malware detection, and industrial systems. Moreover, 25 of 33 approaches focus mainly on using AI methods to either identify or estimate security risks, or both identify and estimate security risks. Approaches that use AI methods to support risk evaluation have received the least attention in the literature. Finally, the most commonly used AI techniques to support security risk assessment are Bayesian networks and neural networks, and in terms of learning methods we discovered that 31 out of 33 approaches use supervised learning.

The usage of AI techniques for cyber risk assessment, as well as within the cybersecurity domain, is relatively new. The points above show that the usage of AI to support security risk assessment is in fact increasing, but that the domain is still in its infancy.

Acknowledgment

This work was supported by the SINTEF project AISRA, funded by the basic funding through Research Council of Norway, as well as CyberSec4Europe (830929) funded by the European Commission within the H2020 Programme.

References

[1] *European Cybersecurity Strategic Research and Innovation Agenda (SRIA) for a contractual Public-Private Partnership (cPPP)*, European Cyber Security Organization, 2016, accessed December 9, 2020. [Online]. Available: http://ecs-org.eu/documents/ecs-cppp-sria.pdf

[2] *Gartner's top cybersecurity trends cover the skills shortage, cloud and a shift to detection and response*, Gartner, 2017, accessed December 9, 2020. [Online]. Available: https://www.gartner.com/smarterwithgartner/5-trends-in-cybersecurity-for-2017-and-2018/

[3] *Gartner: Cybersecurity Needs to Become More Continuous, Adaptable and Risk-Based*, Gartner, 2017, accessed December 9, 2020. [Online]. Available: https://haystax.com/gartner-cybersecurity-needs-to-become-more-continuous-adaptable-\and-risk-based/

[4] *ISO/IEC 27000:2018(en) Information technology – Security techniques – Information security management systems – Overview and vocabulary*, International Organization for Standardization, 2018.

[5] *ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management*, International Organization for Standardization, 2018.

[6] B. Copeland, "Artificial intelligence," in *Encyclopædia Britannica*. Encyclopædia Britannica, 2020. [Online]. Available: https://www.britannica.com/technology/artificial-intelligence

[7] B. A. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Keele University and Durham University Joint Report, Tech. Rep. EBSE 2007-001, 2007. [Online]. Available: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf

[8] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proceedings of the 18th international conference on evaluation and assessment in software engineering*. ACM, 2014, p. 38.

[9] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (isra)," *Computers & security*, vol. 57, pp. 14–30, 2016.

[10] S. Chockalingam, D. Hadžiosmanović, W. Pieters, A. Teixeira, and P. van Gelder, "Integrated safety and security risk assessment methods: a survey of key characteristics and applications," in *International Conference on Critical Information Infrastructures Security*. Springer, 2016, pp. 50–62.

[11] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *International journal of critical infrastructure protection*, vol. 9, pp. 52–80, 2015.

[12] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for scada systems," *Computers & security*, vol. 56, pp. 1–27, 2016.

[13] J. Hegde and B. Rokseth, "Applications of machine learning methods for engineering risk assessment – a review," *Safety Science*, vol. 122, p. 104492, 2020.

[14] G. Baryannis, S. Validi, S. Dani, and G. Antoniou, "Supply chain risk management and artificial intelligence: state of the art and future research directions," *International Journal of Production Research*, vol. 57, no. 7, pp. 2179–2202, 2019.

[15] T. Hecht, L. Langer, and P. Smith, "Cybersecurity risk assessment in smart grids," *Tagungsband ComForEn 2014*, vol. 39, 2014.

[16] I. Lee, "Internet of things (iot) cybersecurity: Literature review and iot cyber risk management," *Future Internet*, vol. 12, no. 9, p. 157, 2020.