IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 21, 2020, accepted July 14, 2020, date of publication July 30, 2020, date of current version August 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3013145

Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature

ISAAC WIAFE[1], FELIX NTI KORANTENG[2], EMMANUEL NYARKO OBENG[3], NANA ASSYNE[4], ABIGAIL WIAFE[5], AND STEPHEN R. GULLIVER[6]

[1]Department of Computer Science, University of Ghana, Accra, Ghana
[2]Department of Information Technology Education, University of Education, Kumasi Campus, Winneba, Ghana
[3]KPMG-Ghana, Accra, Ghana
[4]Faculty of Information Technology, University of Jyväskylä, 40014 Jyväskylä, Finland
[5]School of Computing, University of Eastern Finland, 70211 Kuopio, Finland
[6]Henley Business School, University of Reading, Reading RG6 6UR, U.K.

Corresponding authors: Stephen R. Gulliver (s.r.gulliver@henley.ac.uk) and Isaac Wiafe (iwiafe@ug.edu.gh)

ABSTRACT Due to the ever-increasing complexities in cybercrimes, there is the need for cybersecurity methods to be more robust and intelligent. This will make defense mechanisms to be capable of making real-time decisions that can effectively respond to sophisticated attacks. To support this, both researchers and practitioners need to be familiar with current methods of ensuring cybersecurity (CyberSec). In particular, the use of artificial intelligence for combating cybercrimes. However, there is lack of summaries on artificial intelligent methods for combating cybercrimes. To address this knowledge gap, this study sampled 131 articles from two main scholarly databases (ACM digital library and IEEE Xplore). Using a systematic mapping, the articles were analyzed using quantitative and qualitative methods. It was observed that artificial intelligent methods have made remarkable contributions to combating cybercrimes with significant improvement in intrusion detection systems. It was also observed that there is a reduction in computational complexity, model training times and false alarms. However, there is a significant skewness within the domain. Most studies have focused on intrusion detection and prevention systems, and the most dominant technique used was support vector machines. The findings also revealed that majority of the studies were published in two journal outlets. It is therefore suggested that to enhance research in artificial intelligence for CyberSec, researchers need to adopt newer techniques and also publish in other related outlets.

INDEX TERMS Artificial intelligence and cybersecurity, information security, machine learning, systematic reviews.

I. INTRODUCTION

The rapid evolution of information and communication technologies, including the Internet has bred positive implications to organizations and social lives. The Internet provides a platform that facilitates communication and networking. It supports knowledge sharing [1] and social interaction [2] which are important ingredients for human development. Amidst all the benefits, it has a dark side. Its increase in reliance on third party and/or cloud-based data storage and applications, make it extremely difficult for organizations to provide ''total'' security to their information systems.

For instance, current cloud infrastructure is characterized by a three-layer architecture. Each layer is arguably at risk from a range of vulnerabilities introduced either by programmers or service providers. The disparate handling of data makes crimes such as cybertheft and cyber-fraud more complex to track within cyberspaces [3]. More worryingly, ubiquitous distributed computing eliminates the importance of geographical boundaries, and this also makes it possible for criminal activities to originate from any part of the World [4]. Hence, organizations are increasingly challenged by a wide range of cyber-attacks [5], [6]. These attacks are characterized by a high level of sophistication that calls for the need of adopting Artificial Intelligence (AI) or intelligent agents to combat them.

Accordingly, cyber defense mechanisms must be i) increasingly intelligent, ii) more flexible, and iii) robust enough to detect a variety of threats and mitigate against them. To achieve these requirements, organizations are adopting AI techniques to effectively monitor and combat cyber-attacks and cybercrimes. This, in addition, calls for the need for

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

researchers and practitioners to be familiar with current state of the art on the use of AI methods for cyber safety. Although some existing studies have summarized and discussed issues impacting cybersecurity (CyberSec), to the best of our knowledge none has, in a systematic manner, focused on AI applications in CyberSec. Thus, this paper aims to systematically review existing studies on the use of AI techniques for combating cyber-attacks.

The next section provides a brief background on how AIs are used in combating CyberSec issues. This is followed by a discussion on existing related works and the current knowledge gap. The method used for conducting the study, the findings, discussions and conclusions are also presented.

II. BACKGROUND LITERATURE

A. ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY

Information and communication technology researchers agree that information security (InfoSec) is of primary importance [7]. Consequently, a number of studies have attempted to address this by adopting improved techniques and technological artifacts; including the use of malware detectors, intrusion detection and prevention systems (IDPS), sophisticated firewall setups and data encryption algorithms. Although some studies have argued that InfoSec issues can be effectively managed by focusing on human behavior [10], others have argued that focusing on human behavior alone is not sufficient [3]. For example, the quantum of information handled by most organizations necessitates considerable automation [12]. Hence, there is the need for an appropriate balance between humans, technology and policy management in organizational security activities.

Conventional CyberSec prevention technologies use fix algorithms and physical devices (such as sensors and detectors), thus they are ineffective at containing new cyberspace threats [10]. For instance, the first generation of antivirus systems were designed to identify viruses by scanning its bit signature. The fundamental assumption of this concept is that a virus has the same structure and bit pattern in all instances. These signatures and algorithms are therefore fixed. Although the catalog of signatures is updated on a daily basis (or whenever the device is connected to the Internet), the sophistication and regular release of vast malware make this approach ineffective. However, the introduction of signature-less approaches that are capable of detecting and mitigating malware attacks using newer methods such as behavioral detections and AIs have been argued to be more effective [12], [13].

This suggests that advancement in AI applications have made it possible to design relatively effective and efficient systems that automatically identify and prevent malicious activities within cyberspaces [3]. They have been adopted to support existing technological methods as they provide effective standards and mechanisms to better control and prevent cyber-attacks [14]. Despite all the benefits AI provides, the rapid evolution of approaches makes it extremely difficult for researchers to identify the most efficient technique and its impact on cyberspace security. There is no ambiguity that the general perception amongst InfoSec and CyberSec researchers and practitioners suggest that AI has improved organizational information security, yet to the best of our knowledge, these claims are speculative and have not been empirically substantiated. Most existing studies have either demonstrated how their innovation outperform a selection of existing methods or surveyed a sample of systems and assess their performance in comparison to theirs. In all cases, the level of selection biases is relatively high. Accordingly, there is the need for an aggregated literature that provide summaries on issues, challenges and future research directions within the domain.

B. RELATED WORK

As mentioned earlier, existing studies have attempted to review literature on CyberSec. For instance, Al-Mhiqani et al [15] reviewed cases and incidents in cyber-physical systems by describing a range of security breaches and provided solutions for curtailing such breaches. Although their study provides meaningful insights to researchers, it failed to address issues regarding AI advances in the domain. It is limited and did not present discussions on techniques and algorithms that are dominating the domain Li [16] provided a summary of how AI has been used to combat cyber-attacks. However, the study was arguably not systematic: the method used for selecting literature was not defined, and disputably open to researcher bias. Furthermore, Li [16] failed to provide discussions concerning the patterns and trends impacting the performance of existing algorithms.

Other researchers focused their reviews in specific domains, maintaining that CyberSec research is biased towards intrusion detection and industrial control systems [19] Lun *et al.* [20], for instance, identified, classified and analyzed cyber-physical security systems and concluded that majority of CyberSec studies focus on approaches that detect and protect power grids. Leszczyna [21] reviewed standards of CyberSec requirements for smart grids and augmented existing studies by providing evidence to consolidate and compare current standards. Coventry and Branley [22] and Kruse *et al.* [23] reviewed patterns of attacks within healthcare cyberspace, and identified that information theft and ransomware attacks were increasingly prevalent within healthcare institutions. They concluded that systems and measures for ensuring CyberSec within the healthcare industries are deficient Dilek *et al.* [3] reviewed AI applications and techniques for combating cybercrime, yet their study cannot claim to be 'systematic' when critically compared with systematic review guidelines as proposed by Kitchenham and Charters [18]. Specifically, they failed to detail the methods adopted for study selection (i.e. inclusion and exclusion criteria, search terms and phrases), the databases which were queried, and the data extraction method used. In addition, although they reported and explained existing AI methods

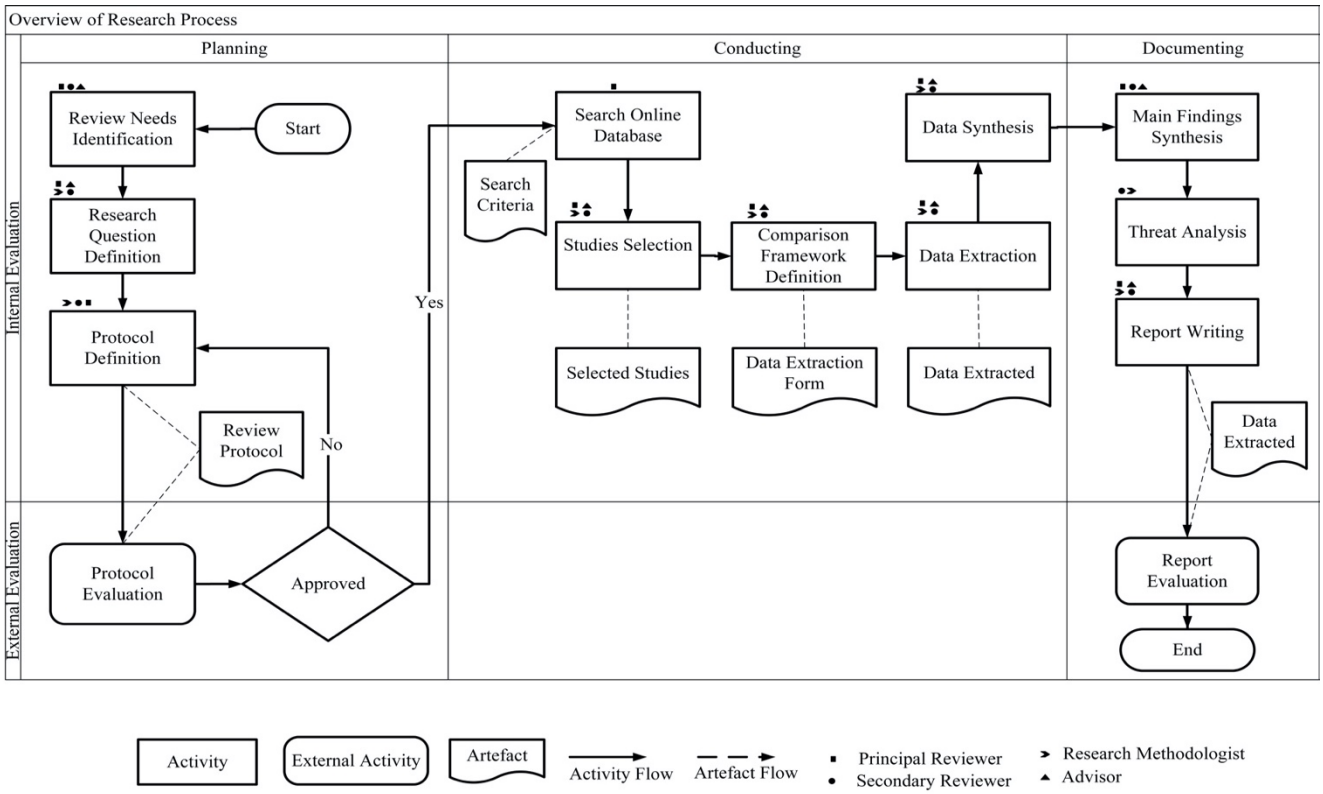


FIGURE 1. Diagrammatic representation of the review process.

that are used in combating cybercrimes, they failed to provide an overview of research trends in the domain.

Although the studies discussed above is not an exhaustive list of all literature relating to cybersecurity review research, a search from academic electronic libraries for systematic review studies on cybersecurity failed to provide studies that summarizes trends for AI methods in cybersecurity. Yet, information on publication trends, dominant AI methods and its impact on cybersecurity is crucial. This is because, such information will provide the knowledge gaps and potential opportunities or prospects in the domain: this is pertinent for researchers and practitioners. This, therefore, makes it imperative to conduct investigations in the domain using a systematic approach. It is however emphasized that, although systematic reviews do not guarantee bias-free literature investigations, it reduces biasness and also provides auditable findings.

III. REVIEW METHODOLOGY

To ensure a rigorous and auditable review, a comprehensive review protocol was developed. Review protocols reduce researcher's biasness and provide a framework that guides the review process. This study adopted an existing systematic review method used in software engineering research as proposed by Kitchenham and Charters [18]. The main review process, consists of three phases, i.e. planning, conducting and documenting phases. The protocol detailed the rationale for the study, defined the review questions, search strategy, databases, inclusion and exclusion criteria, data extraction and synthesis. Figure 1 is a diagrammatic presentation of the review process grouped into the three main phases, as suggested by Kitchenham and Charters [18].

As suggested by Brereton *et al.* [24], review questions were formulated during the planning stage to elicit the study goals, which in turn formed the foundation of the study. The Goal-Question-Metric approach (see Table 1) [25] was adopted. This approach has been demonstrated by Lun *et al.* [20] to be effective for eliciting objectives of systematic reviews.

TABLE 1. Goal-Question-Metric adopted from [25].

Purpose	This study analyses
Issues	Publication trends, domain of application, methods and future direction
Object	Existing artificial intelligence approaches used in combating cybersecurity
Viewpoint	Between 2008 and 2018

Within CyberSec domain, questions concerning the most used AI methods and its effectiveness, directions of current and future research among others remain unanswered. Accordingly, this study seeks to explore existing studies in the domain to address these knowledge gaps. Table 2 is a list of

TABLE 2. Review questions and rationale.

	Research Question	*Motivation*	*Method*
RQ1	What are the publication trends of AI methods in cybersecurity?	To classify studies and assess interests, dominating venues, and contributions. Depending on the number of studies, trends can be assessed over a period. This information will provide the research community with shortfalls within the domain.	Quantitative
RQ2	What AI methods are used in cybersecurity and what type of issues are they applied for?	To identify various AI methods currently used in cybersecurity. This will identify the most dominant method used. It will also determine why it is the most preferred method. This information will provide researchers with the potentials and/or lack of concentration in the various AI methods.	Quantitative
RQ3	What impacts have these AI methods had on cybersecurity?	To identify current impact of AI on cybersecurity and to analyze and classify existing AI approaches for cybersecurity with respect to specific concerns they seek to address.	Qualitative
RQ4	What is the future research direction?	This question seeks to identify future aspirations of AI for cybersecurity researchers and practitioners. It provides novice researchers with information on current areas of interest within the domain.	Qualitative

review questions, which this study addressed and the rationale or motivation for posing the questions.

The search terms, keywords, databases, search engines, and the scope (time frame) were all considered and defined. The inclusion and exclusion criteria were also defined. To reduce biasness, a review protocol was developed separately by four members of the research team (i.e. one principal reviewer, two secondary reviewers, and a research methodologist).

In all instances, the members performed preliminary searches to select the most appropriate databases and keywords. The individual protocols were amalgamated to address the study's need, and the combined protocol was redefined and reviewed by the fifth member (the advisor). The agreed protocol was sent to an external reviewer with CyberSec expertise for comments and amendments. After subsequent corrections, the final protocol was developed.

The keywords or phrases considered appropriate were made up of two categories; i.e. those relating to intelligence systems (Artificial intelligence, Machine learning and Deep learning) and those relating to security (Cybersecurity, information security, internet security and network security). The words from both categories were combined to form search phrases including Artificial intelligence and/or Cybersecurity, Machine learning and/or Cybersecurity, Deep learning and/or Cybersecurity, Artificial intelligence and/or information security, Machine learning and/or information security, Deep learning and/or information security, Artificial intelligence and/or internet security, Machine learning and/or internet security, Deep learning and/or internet security, Artificial intelligence and/or network security, Machine learning and/or network security, Deep learning and/or network security. The search timeframe was limited to studies published from 2008 to 2018: this allows consideration of the research patterns over a substantial period of time. Institute of Electrical and Electronics Engineers (IEEE) and Association for Computing Machinery (ACM) digital libraries were deemed the most appropriate databases for the review, since the preliminary search indicated that other scholarly databases have limited related studies in the domain. Arguably, IEEE and ACM scholarly databases are considered as the two main computer science research databases.

The search produced a total of 1145 studies. Eight hundred and fifty-seven (857) studies were from IEEE research database and the remainder (277) was from ACM Digital Library. All studies were subjected to the inclusion and exclusion criteria. Only peer-reviewed journal articles were selected. Tutorials, short papers, conference proceedings, etc. were excluded. This ensured that all selected studies had undergone consistent revision and/or had been peer-reviewed by more than one external stakeholders as being of good quality. Studies that did not suggest within the title, that its content is related to the application of AI in an area of CyberSec were discarded. Next, studies with abstracts that did not discuss an AI application for CyberSec were discarded. This reduced biasness and researcher subjectivity in the selection process.

In total, 131 studies were selected. Data were extracted from the selected studies, and 3 members of the team (i.e. the principal and secondary reviewers) performed data extraction separately. All members met and discussed their findings in order to address any disparity between analysis. Studies that produced contradictory classifications were resolved in a group meeting attended by all members of the team. A resolution was driven by the other two members (i.e. the advisor and the research methodologist) who assessed the articles. If required, a vote was taken by team members to support or refute any final decision.

During the data extraction process, the relevant information needed were recorded from all the selected primary studies (131 articles) to answer the review questions stated in table 2. The resultant information was tabulated to find trends and patterns in the selected studies. The extracted data was analyzed and summarized.

IV. REVIEW RESULTS

Information regarding the year of publication, the corresponding author's address and country and the publication outlet, were recorded. In addition, for each article the AI method used, and the type of security application discussed was recorded. Studies that discussed improvement of existing approaches were also analyzed and summarized. Below is a discussion on the findings from the study.

A. PUBLICATION TRENDS

It was evident from the results (see Figure 2) that the number of research publications on AI methods for ensuring cybersecurity have increased considerably in recent years. AI techniques in CyberSec started gaining attention after 2015. Articles from 2008 to 2015 accounted for 26% of the total selected primary studies. Since 2016, publications in the domain have increased by a margin of almost 100% and this forms the steepest slope of the graph. Publications in the domain increased from seven to fourteen in 2015 and doubled again in 2017. In 2018, fifty-seven studies were recorded: this indicates a little more than twice what was published in the previous year.

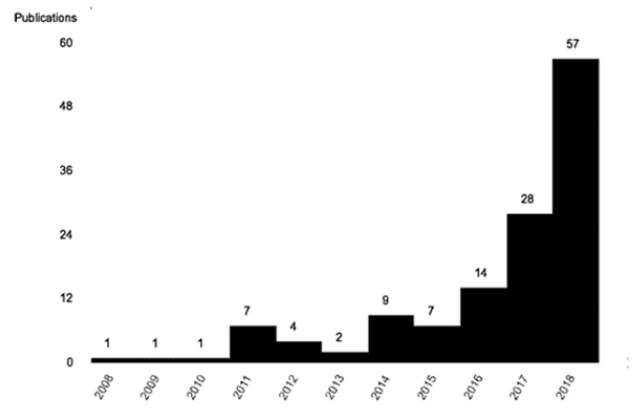


FIGURE 2. Trends in primary studies from 2008 to 2018.

The findings indicated that publications were also skewed among publishing houses/outlets. Out of the 131 journal articles studied, 32 of the articles were published in IEEE Access Journal and 26 were published at IEEE Transactions on Information Forensics and Security Journal. These two outlets accounted for 45% (59 publications of the total number. See figure 3 for the chart of publication distribution according to publication outlets). The chart indicates outlets with more than 2 publications. The next publication outlet that recorded the most articles was the IEEE Transactions on Industrial Informatics and IEEE transaction on Network and Service Management. They both recorded five studies. The rest of the publishing outlets recorded either three or less studies.

Similarly, research in the domain was observed to be skewed geographically. The addresses of corresponding authors revealed that majority of the studies originated from countries in Asia. A total of 68 articles out of the 131

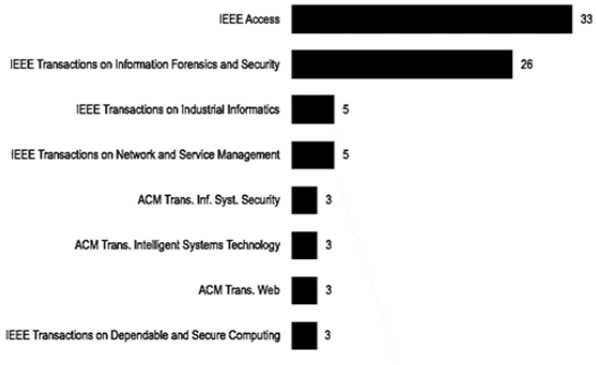


FIGURE 3. Publications outlets with more than 2 articles on AI/ in Cybersecurity.

(i.e. 52%) originated from Asia. South America and Africa recorded one publication each. In terms of countries, China recorded the highest publication followed by the United States of America. See figure 4 for the distribution of articles studied in terms of country of origin.

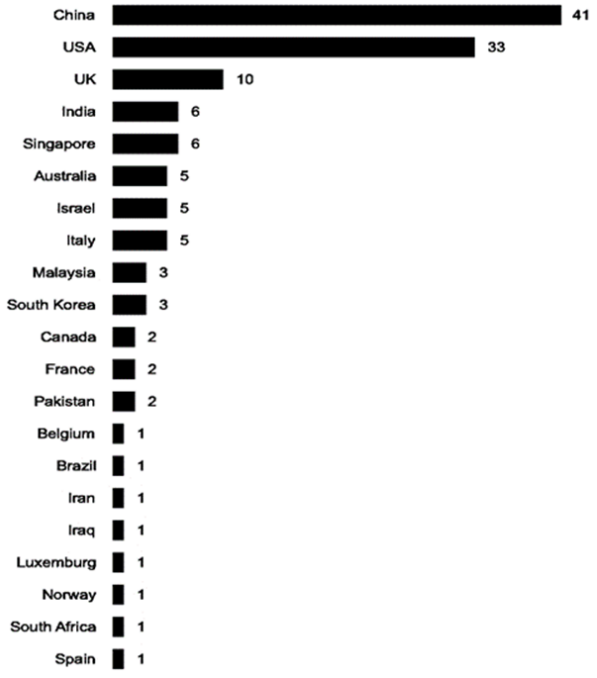


FIGURE 4. Distribution of publications by country of origin of the corresponding author.

B. AI METHODS AND DOMAIN OF APPLICATION IN CYBERSECURITY

Over 50 different algorithms were identified from the various studies that were used in the review. The dominant algorithms were: Artificial Neural Networks (ANN), Convolution Neural Networks (CNN), Decision Trees (DT), K-Means, K-Nearest Neighborhood (KNN), Adaptive Boosting (AdaBoost), Q-Learning (QL), Random Forest (RF),

Recursive Neural Networks (RNN) and Support Vector Machines (SVM) – see Table 3.

TABLE 3. AI algorithms in cybersecurity (2008 to 2018).

	AdaBoost	CNN	SVM	KNN	ANN	K-Means	Q-Learning	Random Forest	RNN	Decisions Trees	Other	Not Specified
2008	1										1	
2009											1	
2010											1	
2011			3					3		1	6	
2012					1						2	1
2013			1			1						
2014	1		1		1	1		1		1	4	1
2015		1	1			1		1			1	
2016		1	4	2	1	1	1	1			2	2
2017		4	4	1		2	3	1	4	1	13	4
2018	2	8	10	3	7	2	2	2	1	4	16	6
Total	**4**	**14**	**24**	**6**	**10**	**8**	**6**	**9**	**5**	**7**	**47**	**14**

Fourteen studies did not explicitly specify the algorithm used for implementing the security measure. The most used algorithm was SVM (24 studies) followed by CNN (14). ANN was used in 10 studies, whereas Random forest, K-means and Decision trees were recorded in 9, 8 and 7 studies respectively.

For convenience and simplicity, domains of application were grouped into six: (i) intrusion detection and prevention systems (IDPS), (ii) traffic classification systems, (iii) imaging and captcha, (iv) Encryption and certification, (v) Denial-of-service attack, and (vi) malware, virus, phishing, etc.

The study revealed that intrusion detection and prevention systems (IPDS) have attracted more research attention compared to other domains. Thirty-eight studies (i.e. 41%) addressed issues relating to IDPS (see table 4), followed by issues on malware, virus, phishing, etc. that recorded 27 studies (21%).

TABLE 4. Publication and applications domains (2008 to 2018).

	Intrusion Detection	Encryption & Certification	Imaging & Captcha	Phishing, Malware, etc.	Traffic classification	DoS	Other	
2008	1							1
2009		1						1
2010				1				1
2011	2			3			2	7
2012	2						2	4
2013					1		1	2
2014	1	1		2	2		3	9
2015			1	1	1	1	3	7
2016	5	1		3			5	14
2017	8		3	8			9	28
2018	20	3	2	9		1	22	57
Total	**38**	**6**	**6**	**27**	**4**	**3**	**47**	**131**

TABLE 5. Application domains vs AI algorithms (2008 to 2018).

	Intrusion Detection	Encryption & Certification	Imaging & Captcha	Phishing, Malware, etc.	Traffic classification	DoS	Other
Not specified	3	1		4			6
Other	17	5		8	4	1	14
Decision Trees	1			3			3
RNN	4			1			
Random forest	2			3	1		3
Q-Learning				1			5
K-Means	4				3		
ANN	4			2			4
KNN	5					1	
SVM	8		2	5		1	7
CNN	2		4	3	1		5
AdaBoost	3						1

Studies that focused on power systems security assessment, covert channels, security games, fingerprint liveness detection, biometric verification (including facial verification), malicious webpages, cyberbullying, false data injection, online deception review, information risk assessment, iris recognition were all classified as others, since they were not identified in more than 2 studies. The total number of studies that fell under this category was 47 (i.e. 36%). To understand how various algorithms have been used for different areas of application, the various methods were mapped to different domains of application. The results indicated that IDPS and malware, virus, phishing, etc. mostly adopt ensemble techniques (i.e. uses a combination of two or more AI algorithms). It was also observed that studies that focused on Encryption & Certification, DoS, and Imaging and Captcha do not prefer ensemble methods.

C. IMPACT OF AI METHODS ON CYBERSECURITY

The most significant contribution of AI in the domain is the improvement in false alarm rates for IDPS. All studies on IDPS reported improvement in false alert rates. For instance, Aminanto *et al.* [26] explained that their approach to IDPS recorded a remarkable false alarm rate of values around 0.012%, which is the current lowest value for impersonation attack detection.

Computational complexity was identified as a key challenge in IDPS. Almost all studies that sought to address issues on IDPS identified it as a challenge. It can be inferred that this challenge has been inherited from generic AI methods

(particularly relating to issues in machine learning). This is because computational complexity is one of the most challenging issues in machine learning algorithms [27], [28]. It impacts computational speed and adversely affects the performance of applications. Yet, a number of studies reported some form of reduction in computational complexities. The use of genetic algorithm-based feature selection is effective for reducing computational complexities in IDPS. This was demonstrated by studies conducted by Ahmed *et al.* [29]. With regard to network intrusion, the ability to detect new traffic patterns and anomalies using ensembles was identified to be one of the most effective methods. In addition, higher IDPS accuracies, with lower rates of false positives and lower energy consumption were observed.

Other contributions include the successful detection of both known and unknown Controller Area Network (CAN) attacks by Wang *et al.* [31]. The review revealed that AI methods have provided effective ways of detecting malicious users. The use of clickstream models, which does not require prior knowledge or assumptions of user categories was observed to be effective for capturing unexpected or previously known behaviors.

Currently, systems are capable of detecting malicious accounts through identification and coloring of similar clickstreams. Improved correctness of certification classifications, using ANN was demonstrated by Dong *et al.* [32]. Again, an improvement in accuracy, and computational efficiency for image privacy protection, is currently possible using deep CNN [33] and SVM [34]. Better image manipulation detection algorithms have been developed by Bayar and Stamm [35], and Cui *et al.* [37]. They improved manipulation detection and malware image detection results respectively using CNN. In addition, Ben Neria *et al.* [38] have improved malicious webpage detection using spectral clustering.

D. FUTURE DIRECTIONS OF AI METHODS IN CYBERSECURITY

Research directions in AI applications for cyber security were recorded to be broad and diverging since 2008. This divergence can be attributed to the larger spectrum of areas of application. As explained earlier, challenges in cyber issues continue to evolve. This makes it a challenge for studies to focus on a specific domain. Studies within similar areas of applications are currently experimenting with different AI techniques and machine learning algorithms. From table 4, algorithms that were classified as ''other'' formed 36% of the sampled studies. These are algorithms that were identified to have been used in less than two applications. Hence, it can be inferred that researchers are adopting newer, and perhaps more innovative techniques. Accordingly, future studies may opt for novel techniques from other domains. However, it must be emphasized that the need for applications to be computationally efficient, reduce computational complexity and improve performance accuracy are key issues that majority of researchers in the domain advocate for. Particularly, in IDPS the need for improvement in algorithms in complex systems by reducing model training time was observed to be paramount. Also, advocacy on proactive measures towards CyberSec is dominant. Other issues such as the ability to generalize intrusion detection models, the development of self-tuning methods for automated network anomaly detections and advocacy for a significant reduction in detection times were observed in most of the studies. Next is a discussion of the implications of the findings from this study.

V. IMPLICATION AND DISCUSSION

A. RESEARCH TRENDS

The skewness in publication trends is visible in the various forms of the analysis (i.e. publication vendors, year of publication, areas of applications and algorithms used). In particular, two outlets dominated publications. This suggests a critical issue that needs to be addressed. Although there are a number of good publication outlets that seek to discuss issues concerning CyberSec and AI, they were not adequately represented in this study. It is intriguing to observe that IEEE Access had 31 studies published between 2017 and 2018, yet IEEE Access started publishing papers in 2013. This raises questions as to why some outlets are failing to attract studies from researchers in the domain: especially outlets that started publishing in this area but are no longer seemingly attractive/support researcher contributions. This trend also suggests the need for other related outlets to consider issues in the domain. Perhaps a call for a special issue in a related journal to draw researchers' attention to the relevance of the matter in their outlet. Again, no outlet was identified with sole interest in AI application for CyberSec. All identified outlets publishing AI and CyberSec issues were multidisciplinary journals. Considering the relevance of the domain with respect to the current advancement in quantum computing and its implications on CyberSec, there is the need for an intensified focus on AI for cybersecurity research.

It can be argued that IDPS is currently the major challenge in CyberSec. Accordingly, majority of the studies geared towards addressing challenges associated with IDPS. This supports Franke and Brynielsson's [19] assertion but refutes that of Lun *et al.* [20]. Issues on IDPS are vast as they span across physical human intrusion to virtual attacks. In addition, it is associated with other CyberSec issues since most attackers start their attack processes by intruding into systems. Hence, addressing issues on intrusion will reduce a myriad of CyberSec issues.

A considerable number of the studies analyzed focused on malware, phishing and virus-related issues. This finding supports Arshad *et al.* [43] argument that there is an increase in the number of malware attacks; especially on Android devices. Accordingly, the study found a number of malware detection solutions that were designed for Android devices. Out of 14 applications that were designed for malware detection, eight (8) focused on android devices. Denial of Service attack was one of the least favored areas of interest. This raises some concerns, considering that studies have argued

that DoS has devastating effects on Information Technology systems [44]. These findings, however contradict earlier studies [20] that argued that majority of CyberSec studies focus on approaches that detect information theft and ransomware attacks [23]. Also, even though some researchers have argued that DoS attacks is one of the frightening CyberSec issues that needs attention [45], the study showed that the use of AI methods for addressing DoS issues is currently one of the areas that is attracting less attention.

B. AI METHODS AND TECHNIQUES

As observed, support vector machine is the most preferred algorithm for intrusion detection and preventive systems. This supports arguments by Peker [46] that it is a robust algorithm for classification. From the study, the application of SVM grew exponentially between 2013 and 2018. SVMs are capable of solving problems with small samples that are nonlinear and also support high dimensionality. They have become known to be a state-of-the-art algorithm for IDPS.

The study also confirmed suggestions that ensemble techniques are effective for addressing IDPS [39], [40], malware, virus, and phishing [41], [42] as most studies adopted this technique. However, ensembles are less used in Encryption & Certification, DoS, and Imaging and Captcha. Thus, there is the need for investigations to ascertain why ensembles are not preferred in Encryption & Certification, DoS, and Imaging and Captcha, especially considering its success in other cybersecurity issues as observed.

It was also observed that, algorithms that were preferred previously are becoming unpopular. For instance, AdaBoost (one of the early used algorithms) is becoming unpopular (see table 3). Hence, although AdaBoost is considered to be a robust algorithm [47], it is not gaining attention in cybersecurity issues. Other AI algorithms and techniques were not considerably present in the studies reviewed. Artificial neural network and its related algorithms, for example, have not been adequately explored for addressing cybersecurity issues. Yet, existing studies in machine learning have argued that ANN and its related methods are effective [48], [49]. This calls for investigations into the prospects of ANN in cybersecurity issues.

C. SECURING THE CYBERSPACE

AI applications for CyberSec have been generally successful. Notable contributions have been made on combating cybercrime: predominantly issues linked to IDPS. Newer systems demonstrated improvements over previous systems: with impacts on a range of issues including energy efficiency, improved accuracy in predictions, reduction in computational complexities, reduced computational speed and a reduction in model training times.

The domain, however, faces a number of challenges. The divergent nature of current research suggests a promising future, yet some threats that need addressing. A significant number of the studies sampled did not state clearly the algorithm used or the domain of application. This does not demonstrate a lack of focus on specific matters, but rather propositions of generic methods. CyberSec issues are mostly domain-specific, hence the provision of generic solutions may be neither adequate nor effective. Also, the variety of algorithms (almost 50) identified, suggests that researchers are not accepting newer methods that are being introduced. Even though it can be argued that these newer methods do not outperform existing ones (hence less patronage), it is necessary for researchers to investigate and improve them. The spectrum of security issues is broad; thus, it is imperative to consider newer algorithms to address newer challenges. So, there is the need to investigate the reasons for not adopting these techniques and how researchers may be persuaded to incorporate new AI approaches?

Again, although some researchers have argued that the use of single classifiers or algorithms are not effective in CyberSec issues and thus proposed the use of ensemble and hybrid methods [50], this study reveals that these methods are not preferred. Ensemble techniques such as AdaBoost are used less frequently. Accordingly, there is the need to develop interest and attention in the use of hybrid and ensemble classifiers to improve existing CyberSec measures.

VI. RESEARCH VALIDITY, LIMITATION AND CONCLUSION

This paper has presented an overview of existing research on the application of AI for cybersecurity. To the best of our knowledge, it is the first systematic review that considered the entire span of AI activities and its implications in CyberSec.

As in all studies, the need to validate the methods used is paramount. The first threat impacting the validity of this study is the possible omission of papers in the selection process and biasness in the data extraction process. Two scholarly databases were considered. However, there are a number of databases that may have related studies. Thus, the findings of the study cannot be generalized. Yet, it provides an indication of patterns in the domain, particularly considering that the initial search demonstrated that IEEE and ACM digital libraries contain a vast majority of papers required. In addition, to ensure that biasness in selection was minimized, Kitchenham and Charter's [18] guidelines were applied. The search phrases, databases, and scope of the review were performed by multiple individuals. Furthermore, the protocol was reviewed by an external reviewer with expertise in CyberSec to eliminate biases. To reduce the number of omitted articles, two categories of search keywords relating to intelligence systems and security were considered to facilitate a concise research scope.

Although the use of journal articles for the review process may present some biasness, it ensured that the studies selected are of good quality and have been peer-reviewed. This ensured that studies selected for this investigation are of good quality: this is paramount. Even though the omission of conference proceedings may present some biasness, the ability to identify quality conference proceedings (particularly those that are peer-reviewed) from the vast number of available proceedings is a challenge. Quality assessments on

conference proceedings are based on researcher's assessment of paper quality and this would have introduced additional biases.

In conclusion, the study suggests that the application of AI in the CyberSec domain has been promising with IDPS showing improvement. AI has facilitated a reduction in computational complexity and reduced model training times. It was also observed that there is a considerable skewness within the domain. Moreover, researchers have focused on fewer algorithms and as such newer algorithms are not popular. This stands as both a challenge and also an opportunity for researchers.

It is believed that AI applications will continue to offer opportunities for cybersecurity. However, research must never stand still, and researchers need to start adopting and adapting new approaches and publish more widely.

APPENDIX
LIST OF REVIEWED STUDIES

[S1] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) Fully Homomorphic Encryption without Bootstrapping," *ACM Trans. Comput. Theory*, vol. 6, no. 3, pp. 1–36, 2014.

[S2] M. Ben Neria, N.-S. Yacovzada, and I. Ben-Gal, "A Risk-Scoring Feedback Model for Webpages and Web Users Based on Browsing Behavior," *ACM Trans. Intell. Syst. Technol.*, vol. 8, no. 4, pp. 1–21, 2017.

[S3] S. Calzavara, G. Tolomei, A. Casini, M. Bugliesi, and S. Orlando, "A Supervised Learning Approach to Protect Client Authentication on the Web," *ACM Trans. Web*, vol. 9, no. 3, pp. 1–30, 2015.

[S4] A. Kleinmann and A. Wool, "Automatic Construction of Statechart-Based Anomaly Detection Models for Multi-Threaded Industrial Control Systems," vol. 8, no. 4, pp. 1–21, 2016.

[S5] Y. S. Dai, Y. P. Xiang, and Y. Pan, "Bionic Autonomic Nervous Systems for Self-Defense against DoS, Spyware, Malware, Virus, and Fishing," *ACM Trans. Auton. Adapt. Syst.*, vol. 9, no. 1, pp. 1–20, 2014.

[S6] G. Xiang, J. Hong, C. P. Rose, and L. Cranor, "Cantina+," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 2, pp. 1–28, 2011.

[S7] G. Wang, X. Zhang, S. Tang, C. Wilson, H. Zheng, and B. Y. Zhao, "Clickstream User Behavior Models," *ACM Trans. Web*, vol. 11, no. 4, pp. 1–37, 2017.

[S8] D. Codetta-Raiteri and L. Portinale, "Decision Networks for Security Risk Assessment of Critical Infrastructures," *ACM Trans. Internet Technol.*, vol. 18, no. 3, pp. 1–22, 2018.

[S9] L. Bauer, S. Garriss, and M. K. Reiter, "Detecting and resolving policy misconfigurations in access-control systems," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–28, 2011.

[S10] Z. Dong, K. Kane, and L. J. Camp, "Detection of Rogue Certificates from Trusted Certificate Authorities Using Deep Neural Networks," *ACM Trans. Priv. Secur.*, vol. 19, no. 2, pp. 1–31, 2016.

[S11] F. Angiulli, L. Argento, and A. Furfaro, "Exploiting Content Spatial Distribution to Improve Detection of Intrusions," *ACM Trans. Internet Technol.*, vol. 18, no. 2, pp. 1–21, 2018.

[S12] L. Bigle, S. Sen, D. Balzarotti, E. Kirda, and C. Kruegel, "EXPOSURE: A Passive DNS Analysis Service to Detect and Report Malicious Domains," vol. 16, no. 4, 2014.

[13] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Learning to detect malicious URLs," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3, pp. 1–24, 2012.

[S14] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, pp. 1–40, 2009.

[S15] D. Ippoliti, C. Jiang, Z. Ding, and X. Zhou, "Online Adaptive Anomaly Detection for Augmented Network Flows," *ACM Trans. Auton. Adapt. Syst.*, vol. 11, no. 3, pp. 17:1–17:28, 2016.

[S16] A. Kulkarni, Y. Pino, M. French, and T. Mohsenin, "Real-Time Anomaly Detection Framework for Many-Core Router through Machine-Learning Techniques," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 13, no. 1, pp. 1–22, 2016.

[S17] C. X. Lu *et al.*, "Snoopy: Sniffing Your Smartwatch Passwords via Deep Sequence Learning," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. Artic.*, vol. 1, no. 152, 2017.

[S18] A. Squicciarini, C. Caragea, and R. Balakavi, "Toward Automated Online Photo Privacy," *ACM Trans. Web*, vol. 11, no. 1, pp. 1–29, 2017.

[S19] N. Sabar, X. Yi, and A. Shong, "A Bi-objective Hyper-Heuristic Support Vector Machines for Big Data Cyber-Security NASSER," *IEEE Access*, vol. 56, no. 5, pp. 280–287, 2018.

[S20] Y. Gao, A. Choudhary, and G. Hua, "A comprehensive approach to image spam detection: From server to client solution," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 4, pp. 826–836, 2010.

[S21] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," vol. 5, 2017.

[S22] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 2, no. 1, pp. 41–50, 2018.

[S23] H. Peng, Z. Sun, X. Zhao, S. Tan, and Z. Sun, "A Detection Method for Anomaly Flow in Software Defined Network," *IEEE Access*, vol. 6, pp. 27809–27817, 2018.

[S24] C. Wang, Z. Zhao, L. Gong, L. Zhu, Z. Liu, and X. Cheng, "A Distributed Anomaly Detection System for In-Vehicle Network Using HTM," *IEEE Access*, vol. 6, pp. 9091–9098, 2018.

[S25] Y. Han, T. Alpcan, J. Chan, C. Leckie, and B. I. P. Rubinstein, "A Game Theoretical Approach to Defend Against Co-Resident Attacks in Cloud Computing?:

Preventing Co-Residence Using Semi-Supervised Learning,'' *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 3, pp. 556–570, 2016.

[S26] L. Dritsoula, P. Loiseau, and J. Musacchio, ''A Game-Theoretic Analysis of Adversarial Classification,'' vol. 12, no. 12, pp. 3094–3109, 2017.

[S27] A. Barth, B. I. P. Rubinstein, M. Sundararajan, J. C. Mitchell, D. Song, and P. L. Bartlett, ''A Learning-Based Approach to Reactive Security,'' *IEEE Trans. Dependable Secur. Comput.*, vol. 9, no. 4, pp. 482–493, 2012.

[S28] Y. Zhu and Y. Tan, ''A local-concentration-based feature extraction approach for spam filtering,'' *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 2, pp. 486–497, 2011.

[S29] M. H. Kamarudin, C. Maple, T. Watson, and N. S. Safa, ''A LogitBoost-Based Algorithm for Detecting Known and Unknown Web Attacks,'' *IEEE Access*, vol. 5, pp. 26190–26200, 2017.

[S30] V. T. Alaparthy and S. D. Morgera, ''A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory,'' *IEEE Access*, vol. 6, pp. 47364–47373, 2018.

[S31] M. H. Ali, B. Abbas, D. Al, A. Ismail, and M. F. Zolkipli, ''A New Intrusion Detection System Based on Fast Learning Network and Particle Swarm Optimization,'' *IEEE Access*, vol. 6, pp. 20255–20261, 2018.

[S32] P. Feng, J. Ma, C. Sun, and Y. Ma, ''A Novel Dynamic Android Malware Detection System With Ensemble Learning,'' *IEEE Access*, vol. 6, pp. 30996–31011, 2018.

[S33] D. Hu, L. Wang, W. Jiang, and S. Zheng, ''A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks,'' *IEEE Access*, vol. 6, pp. 38303–38314, 2018.

[S34] Y. Gao, Y. U. Liu, Y. Jin, J. Chen, and H. Wu, ''A Novel Semi-Supervised Learning Approach for Network Intrusion Detection on Cloud-Based Robotic System,'' *IEEE Access*, vol. 6, pp. 50927–50938, 2018.

[S35] Y. Xu, Z. Y. Dong, J. H. Zhao, P. Zhang, and K. P. Wong, ''A reliable intelligent system for real-time dynamic security assessment of power systems,'' *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1253–1263, 2012.

[S36] Y. Ma, L. Wu, X. Gu, J. He, and Z. Yang, ''A Secure Face-Verification Scheme Based on Homomorphic Encryption and Deep Neural Networks,'' vol. 5, no. 1, 2017.

[S37] L. Fernandez Maimo, A. L. Perales Gomez, F. J. Garcia Clemente, M. Gil Perez, and G. Martinez Perez, ''A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks,'' *IEEE Access*, vol. 6, pp. 7700–7712, 2018.

[S38] Z. Tang, X. Ding, Y. Zhong, L. Yang, and K. Li, ''A self-adaptive bell-lapadula model based on model training with historical access logs,'' *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 8, pp. 2047–2061, 2018.

[S39] P. L. Shrestha, M. Hempel, F. Rezaei, and H. Sharif, ''A Support Vector Machine-Based Framework for Detection of Covert Timing Channels,'' *IEEE Trans. Dependable Secur. Comput.*, vol. 13, no. 2, pp. 274–283, 2016.

[S40] W. Hu, S. Member, W. Hu, and S. Maybank, ''AdaBoost-Based Algorithm for Network,'' *Ieee Trans. Syst. Man, Cybern. B Cybern.*, vol. 38, no. 2, pp. 577–583, 2008.

[S41] M. A. Javed, E. Ben Hamida, A. Al-fuqaha, and B. Bhargava, ''Adaptive Security for Intelligent Transport System Applications,'' *IEEE Intell. Transp. Syst. Mag.*, vol. 10, no. April, pp. 110–120, 2018.

[S42] K. Khanna, B. K. Panigrahi, and A. Joshi, ''AI-based approach to identify compromised meters in data integrity attacks on smart grid,'' 2018.

[S43] N. Nissim, A. Cohen, and Y. Elovici, ''ALDOCX: Detection of Unknown Malicious Microsoft Office Documents Using Designated Active Learning Methods Based on New Structural Feature Extraction Methodology,'' *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 3, pp. 631–646, 2017.

[S44] H. Sedjelmaci and S. M. Senouci, ''An Accurate Security Game for Low-Resource IoT Devices,'' vol. 66, no. 10, pp. 9381–9393, 2017.

[S45] Y. Du, J. Wang, and Q. Li, ''An android malware detection approach using community structures of weighted function call graphs,'' *IEEE Access*, vol. 5, pp. 17478–17486, 2017.

[S46] J. Zhang, C. Chen, Y. Xiang, W. Zhou, and A. V. Vasilakos, ''An effective network traffic classification method with unknown flow detection,'' *IEEE Trans. Netw. Serv. Manag.*, vol. 10, no. 2, pp. 133–147, 2013.

[S47] L. Li, Y. Yu, S. Bai, Y. Hou, and X. Chen, ''An Effective Two-Step Intrusion Detection Approach Based on Binary Classification and k -NN,'' *IEEE Access*, vol. 6, pp. 12060–12073, 2018.

[S48] A. Sahi, D. Lai, Y. A. N. Li, and M. Diykh, ''An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment,'' *IEEE Access*, vol. 5, pp. 6036–6048, 2017.

[S49] A. L. I. S. Sadiq, B. Alkazemi, S. Mirjalili, N. Ahmed, S. Khan, and I. Ali, ''An Efficient IDS Using Hybrid Magnetic Swarm Optimization in WANETs,'' *IEEE Access*, vol. 6, pp. 29041–29053, 2018.

[S50] K. Huang, Q. Zhang, C. Zhou, N. Xiong, S. Member, and Y. Qin, ''An Efficient Intrusion Detection Approach for Visual Sensor Networks Based on Traffic Pattern Learning,'' vol. 47, no. 10, pp. 2704–2713, 2017.

[S51] T. Thongkamwitoon, H. Muammar, and P. L. Dragotti, ''An image recapture detection algorithm based on learning dictionaries of edge profiles,'' *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 5, pp. 953–968, 2015.

[S52] S. Li, F. Bi, W. Chen, X. Miao, J. Liu, and C. Tang, ''An improved information security risk assessments method for cyber-physical-social computing and networking,'' *IEEE Access*, vol. 6, pp. 10311–10319, 2018.

[S53] P. Tao, Z. H. E. Sun, and Z. Sun, ''An Improved Intrusion Detection Algorithm Based on GA and SVM,'' *IEEE Access*, vol. 6, pp. 13624–13631, 2018.

[S54] Z. Liu, T. Qin, X. Guan, H. Jiang, and C. Wang, ''An integrated method for anomaly detection from massive system logs,'' *IEEE Access*, vol. 6, pp. 30602–30611, 2018.

[S55] H. Liu, Y. Wang, J. Liu, J. Yang, Y. Chen, and H. V. Poor, "Authenticating Users Through Fine-Grained Channel Information," *IEEE Trans. Mob. Comput.*, vol. 17, no. 2, pp. 251–264, 2018.

[S56] M. S. Parwez, D. B. Rawat, and M. Garuba, "Big data analytics for user-activity analysis and user-anomaly detection in mobile wireless network," *IEEE Trans. Ind. Informatics*, vol. 13, no. 4, pp. 2058–2065, 2017.

[S57] B. B. Zhu, J. Yan, G. Bao, M. Yang, and N. Xu, "Captcha as Graphical Passwords — A New Security Primitive Based on Hard AI Problems," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 6, pp. 891–904, 2014.

[S58] S. Kalyani and K. Shanti Swarup, "Classification and assessment of power system security using multiclass SVM," *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.*, vol. 41, no. 5, pp. 753–758, 2011.

[S59] L. Xiao, S. Member, D. Xu, C. Xie, N. B. Mandayam, and H. V. Poor, "Cloud Storage Defense Against Advanced Persistent Threats?: A Prospect Theoretic Study," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 3, pp. 534–544, 2017.

[S60] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2018.

[S61] L. Xiao, S. Member, Y. Li, X. Huang, X. Du, and S. Member, "Cloud-Based Malware Detection Game for Mobile Devices with Offloading," vol. 16, no. 10, pp. 2742–2750, 2017.

[S62] M. N. Napiah, M. Y. I. Bin Idris, R. Ramli, and I. Ahmedy, "Compression Header Analyzer Intrusion Detection System (CHA - IDS) for 6LoWPAN Communication Protocol," *IEEE Access*, vol. 6, pp. 16623–16638, 2018.

[S63] B. Bayar and M. C. Stamm, "Constrained Convolutional Neural Networks: A New Approach Towards General Purpose Image Manipulation Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 11, pp. 2691–2706, 2018.

[S64] A. Narayanan, M. Chandramohan, L. Chen, and Y. Liu, "Context-aware, Adaptive and Scalable Android Malware Detection through Online Learning (extended version)," *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 1, no. 3, pp. 157–175, 2017.

[S65] A. D. Pozzolo, G. Boracchi, O. Caelen, and C. Alippi, "Credit Card Fraud Detection?: A Realistic Modeling and a Novel Learning Strategy," *IEEE Trans. Neural Networks Learn. Syst.*, vol. 29, no. 8, pp. 3784–3797, 2018.

[S66] G. Lin *et al.*, "Cross-Project Transfer Representation Learning for Vulnerable Function Discovery," *IEEE Trans. Ind. Informatics*, vol. 14, no. 7, pp. 3289–3297, 2018.

[S67] R. Zhao and K. Mao, "Cyberbullying Detection Based on Semantic-Enhanced Marginalized Denoising Auto-Encoder," *IEEE Trans. Affect. Comput.*, vol. 8, no. 3, pp. 328–339, 2017.

[S68] O. Y. Al-jarrah *et al.*, "Data Randomization and Cluster-Based Partitioning for Botnet Intrusion Detection," *IEEE Trans. Cybern.*, vol. 46, no. 8, pp. 1796–1806, 2016.

[S69] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, S. Member, and K. Kim, "Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 3, pp. 621–636, 2020.

[S70] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep Learning for RF Device Fingerprinting in Cognitive Communication Networks," *IEEE J. Sel. Top. Signal Process.*, vol. 12, no. 1, pp. 160–167, 2018.

[S71] Z. Wang, "Deep Learning-Based Intrusion Detection With Adversaries," *IEEE Access*, vol. 6, pp. 38367–38384, 2018.

[S72] D. Menotti *et al.*, "Deep Representations for Iris, Face, and Fingerprint Spoofing Detection," vol. 10, no. 4, pp. 864–879, 2015.

[S73] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, "Design of Cognitive Fog Computing for Intrusion Detection in Internet of Things," *J. Commun. Networks*, vol. 20, no. 3, pp. 291–298, 2018.

[S74] S. Wang, Q. Yan, Z. Chen, and B. Yang, "Detecting Android Malware Leveraging Text Semantics of Network Flows," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 5, pp. 1096–1109, 2018.

[S75] M. Esmalifalak, S. Member, L. Liu, and S. Member, "Machine Learning in Smart Grid," vol. 11, no. 3, pp. 1644–1652, 2017.

[S76] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu, and J. Hu, "Detection of Denial-of-Service Attacks Based on Computer Vision Techniques," *IEEE Trans. Comput.*, vol. 64, no. 9, pp. 2519–2533, 2015.

[S77] Z. Cui, F. Xue, X. Cai, Y. Cao, and G. Wang, "Detection of Malicious Code Variants Based on Deep Learning," *IEEE Trans. Ind. Informatics*, vol. 14, no. 7, pp. 3187–3196, 2018.

[S78] Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796–808, 2011.

[S79] T. Zhang and Q. Zhu, "Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs," *IEEE Trans. Signal Inf. Process. over Networks*, vol. 4, no. 1, pp. 148–161, 2018.

[S80] Z. Yuan, Y. Lu, and Y. Xue, "DroidDetector?: Android Malware Characterization and Detection Using Deep Learning," vol. 21, no. 1, pp. 114–123, 2016.

[S81] H. Dong, C. Wu, Z. Wei, and Y. Guo, "Dropping Activation Outputs With Localized First-Layer Deep Network for Enhancing User Privacy and Data Security," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 3, pp. 662–670, 2018.

[S82] C. J. Fung, J. Zhang, and R. Boutaba, "Effective Acquaintance Management based on Bayesian Learning for Distributed Intrusion Detection Networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 9, no. 3, pp. 320–332, 2012.

[S83] T. Alves, R. Das, and T. Morris, "Embedding Encryption and Machine Learning Intrusion Prevention

Systems on Programmable Logic Controllers," *IEEE Embed. Syst. Lett.*, vol. 10, no. 3, pp. 99–102, 2018.

[S84] T. J. De Carvalho, C. Riess, E. Angelopoulou, H. Pedrini, and A. D. R. Rocha, "Exposing digital image forgeries by illumination color classification," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 7, pp. 1182–1194, 2013.

[S85] G. Goswami, M. Vatsa, and R. Singh, "Face Verification via Learned Representation on Feature-Rich Video Frames," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 7, pp. 1686–1698, 2017.

[S86] X. He, H. Dai, and P. Ning, "Faster Learning and Adaptation in Security Games by Exploiting Information Asymmetry," *IEEE Trans. Signal Process.*, vol. 64, no. 13, pp. 3429–3443, 2016.

[S87] S. Ahmed, Y. Lee, S. Hyun, and I. Koo, "Feature Selection – Based Detection of Covert Cyber Deception Assaults in Smart Grid Communications Networks Using Machine Learning," *IEEE Access*, vol. 6, pp. 27518–27529, 2018.

[S88] R. F. Nogueira, R. D. A. Lotufo, and R. C. Machado, "Fingerprint Liveness Detection Using Convolutional Neural Networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 6, pp. 1206–1213, 2016.

[S89] X. Chen, L. Qing, X. He, J. I. E. Su, and Y. Peng, "From Eyes to Face Synthesis?: a New Approach for Human-Centered Smart Surveillance," *IEEE Access*, vol. 6, pp. 14567–14575, 2018.

[S90] S. Y. Yerima, S. Sezer, and I. Muttik, "High accuracy android malware detection using ensemble learning," pp. 313–320, 2015.

[S91] W. E. I. Wang *et al.*, "HAST-IDS?: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection," *IEEE Access*, vol. 6, pp. 1792–1806, 2018.

[S92] N. Ahmadi and G. Akbarizadeh, "Hybrid robust iris recognition approach using iris image pre-processing, two-dimensional gabor features and multi-layer perceptron neural network / PSO," vol. 7, pp. 153–162, 2018.

[S93] C. Thomas and N. Balakrishnan, "Improvement in Intrusion Detection using advances in sensor Fusion," vol. 4, no. 3, pp. 542–551, 2012.

[S94] Y. Wang, Y. Xiang, J. Zhang, W. Zhou, G. Wei, and L. T. Yang, "Internet traffic classification using constrained clustering," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 11, pp. 2932–2943, 2014.

[S95] X. Wang, C. Zhang, and K. Zheng, "Intrusion Detection Algorithm Based on Density, Cluster Centers, and Nearest Neighbors," *China Commun.*, vol. 13, pp. 24–31.

[S96] J. Yu, B. Zhang, Z. Kuang, D. Lin, and J. Fan, "iPrivacy?: Image Privacy Protection by Identifying Sensitive Objects via Deep Multi-Task Learning," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 5, pp. 1005–1016, 2017.

[S97] A. Shifa *et al.*, "Joint Crypto-Stego Scheme for Enhanced Image Protection With Nearest-Centroid Clustering," *IEEE Access*, vol. 6, pp. 16189–16206, 2018.

[S98] H. Li *et al.*, "Learning Generalized Deep Feature Representation for Face Anti-Spoofing," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 10, pp. 2639–2652, 2018.

[S99] J. Li, Z. Zhao, and R. Li, "Machine learning-based IDS for software-defined 5G network," *IET Networks*, vol. 7, no. 2, pp. 53–60, 2018.

[S100] L. Wei, W. Luo, J. Weng, Y. Zhong, X. Zhang, and Z. Yan, "Machine Learning-Based Malicious Application Detection of Android," vol. 5, pp. 25591–25601, 2017.

[S101] M. Yousefi-azar, L. G. C. Hamey, V. Varadharajan, and S. Chen, "Malytics?: A Malware Detection Scheme," *IEEE Access*, vol. 6, pp. 49418–49431, 2018.

[S102] H. Zhang, J. Wang, and J. Huang, "Markov Differential Game for Network Defense Decision-Making Method," *IEEE Access*, vol. 6, pp. 39621–39634, 2018.

[S103] W. Li and J. Huang, "Mobile physical layer spoofing detection based on sparse representation," pp. 1709–1713, 2018.

[S104] M. Osadchy, J. Hernandez-castro, S. Gibson, O. Dunkelman, and D. Pérez-cabo, "No Bot Expects the DeepCAPTCHA?! Introducing Immutable Adversarial Examples, With Applications to CAPTCHA Generation," vol. 12, no. 11, pp. 2640–2653, 2017.

[S105] W. Hu, J. Gao, Y. Wang, O. Wu, and S. Maybank, "Online Adaboost-Based Parameterized Methods for Dynamic Distributed Network Intrusion Detection," vol. 44, no. 1, pp. 66–82, 2014.

[S106] S. Mondal and P. Bours, "Person Identification by Keystroke Dynamics Using Pairwise User Coupling," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 6, pp. 1319–1329, 2017.

[S107] C. Pham, L. A. T. Nguyen, N. H. Tran, E. Huh, and C. S. Hong, "Phishing-Aware?: A Neuro-Fuzzy Approach for Anti-Phishing on Fog Networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 15, no. 3, pp. 1076–1089, 2018.

[S108] S. Marchal, J. Francois, R. State, and T. Engel, "Phish storm: Detecting phishing with streaming analytics," *IEEE Trans. Netw. Serv. Manag.*, vol. 11, no. 4, pp. 458–471, 2014.

[S109] N. Wang, T. Jiang, S. Lv, L. Xiao, and S. Member, "Physical-Layer Authentication Based on Extreme Learning Machine," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1557–1560, 2017.

[S110] R. Jiang, A. Bouridane, D. Crookes, M. E. Celebi, and H. L. Wei, "Privacy-Protected Facial Biometric Verification Using Fuzzy Forest Learning," *IEEE Trans. Fuzzy Syst.*, vol. 24, no. 4, pp. 779–790, 2016.

[S111] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-Learning-Based Vulnerability Analysis of Smart Grid Against Sequential Topology Attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 1, pp. 200–210, 2017.

[S112] Y. He, G. J. Mendis, and J. Wei, "Real-Time Detection of False Data Injection Attacks in Smart Grid?: A Deep Learning-Based Intelligent Mechanism," vol. 8, no. 5, pp. 2505–2516, 2017.

[S113] M. Tang, H. Gao, Y. Zhang, Y. Liu, P. Zhang, and P. Wang, "Research on Deep Learning Techniques in Breaking Text-Based Captchas and Designing Image-Based Captcha," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 10, pp. 2522–2537, 2018.

[S114] J. K. Rout, A. Dalmia, K. K. R. Choo, S. Bakshi, and S. K. Jena, "Revisiting semi-supervised learning for online deceptive review detection," *IEEE Access*, vol. 5, pp. 1319–1327, 2017.

[S115] J. Zhang, X. Chen, Y. Xiang, W. Zhou, and J. Wu, "Robust Network Traffic Classification," *IEEE/ACM Trans. Netw.*, vol. 23, no. 4, pp. 1257–1270, 2015.

[S116] X. Qiu and T. Jiang, "Safeguarding multiuser communication using full-duplex jamming receivers," *IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC*, vol. 2017-Octob, pp. 1–5, 2018.

[S117] S. Arshad *et al.*, "SAMADroid?: A Novel 3-Level Hybrid Malware Detection Model for Android Operating System," *IEEE Access*, vol. 6, pp. 4321–4339, 2018.

[S118] L. Caviglione, M. Gaggero, J. F. Lalande, W. Mazurczyk, and M. Urbański, "Seeing the unseen: Revealing mobile malware hidden communications via energy consumption and artificial intelligence," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 4, pp. 799–810, 2016.

[S119] L. Xiao, X. Wan, C. Dai, X. Du, X. Chen, and M. Guizani, "Security in Mobile Edge Caching with Reinforcement Learning," *IEEE Wirel. Commun.*, vol. 25, no. June, pp. 116–122, 2018.

[S120] L. Grimaudo, M. Mellia, E. Baralis, and R. Keralapura, "SeLeCT?: Self-Learning Classifier for Internet Traffic," *IEEE Trans. Netw. Serv. Manag.*, vol. 11, no. 2, pp. 144–157, 2014.

[S121] J. Li, L. Sun, Q. Yan, Z. Li, W. Srisa-An, and H. Ye, "Significant Permission Identification for Machine-Learning-Based Android Malware Detection," *IEEE Trans. Ind. Informatics*, vol. 14, no. 7, pp. 3216–3225, 2018.

[S122] L. Nie and Y. Li, "Spatio-Temporal Network Traffic Estimation and Anomaly Detection Based on Convolutional Neural Network in Vehicular Ad-Hoc Networks," *IEEE Access*, vol. 6, pp. 40168–40176, 2018.

[S123] C. Chen *et al.*, "Statistical Features-Based Real-Time Detection of Drifted Twitter Spam," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 4, pp. 914–925, 2017.

[S124] N. Z. Gong, S. Member, M. Frank, and P. Mittal, "SybilBelief?: A Semi-Supervised Learning Approach for Structure-Based Sybil Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 6, pp. 976–987, 2014.

[S125] H. Zhang, G. Liu, T. W. S. Chow, S. Member, W. Liu, and S. Member, "Textual and Visual Content-Based Anti-Phishing?: A Bayesian Approach," *IEEE Trans. Neural Networks*, vol. 22, no. 10, pp. 1532–1546, 2011.

[S126] S. Jin, Z. Zhang, K. Chakrabarty, and X. Gu, "Toward Predictive Fault Tolerance in a Core-Router System: Anomaly Detection Using Correlation-Based Time-Series Analysis," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. 37, no. 10, pp. 2111–2124, 2018.

[S127] E. Van Der Walt and J. Eloff, "Using Machine Learning to Detect Fake Identities: Bots vs Humans," *IEEE Access*, vol. 6, pp. 6540–6549, 2018.

[S128] Z. Zheng, Y. Yang, X. Niu, H. N. Dai, and Y. Zhou, "Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids," *IEEE Trans. Ind. Informatics*, vol. 14, no. 4, pp. 1606–1615, 2018.

[S129] L. K. Shar, L. C. Briand, and H. B. K. Tan, "Web Application Vulnerability Prediction Using Hybrid Program Analysis and Machine Learning," *IEEE Trans. Dependable Secur. Comput.*, vol. 12, no. 6, pp. 688–707, 2015.

[S130] H. Li, W. Li, H. Cao, S. Wang, F. Huang, and A. C. Kot, "Unsupervised Domain Adaptation for Face Anti-Spoofing," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 7, pp. 1794–1809, 2018.

[S131] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-Layer Spoofing Detection with Reinforcement Learning in Wireless Networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10037–10047, 2016.

REFERENCES

[1] F. N. Koranteng and I. Wiafe, "Factors that promote knowledge sharing on academic social networking sites: An empirical study," *Edu. Inf. Technol.*, vol. 24, no. 2, pp. 1211–1236, Mar. 2019, doi: 10.1007/s10639-018-9825-0.

[2] F. N. Koranteng, I. Wiafe, and E. Kuada, "An empirical study of the relationship between social networking sites and students' engagement in higher education," *J. Educ. Comput. Res.*, vol. 57, no. 5, pp. 1131–1159, Sep. 2019, doi: 10.1177/0735633118787528.

[3] S. Dilek, H. Cakár, and M. Aydán, "Applications of artificial intelligence techniques to combating cyber crimes: A review," *Int. J. Artif. Intell. Appl.*, vol. 6, no. 1, pp. 21–39, Jan. 2015, doi: 10.5121/ijaia.2015.6102.

[4] R. Apau and F. N. Koranteng, "Impact of cybercrime and trust on the use of E-commerce technologies?: An application of the theory of planned behavior," *Int. J. Cyber Criminol.*, vol. 13, no. 2, pp. 228–254, 2019, doi: 10.5281/zenodo.3697886.

[5] N. Aldaraani and Z. Begum, "Understanding the impact of ransomware: A survey on its evolution, mitigation and prevention techniques," in *Proc. 21st Saudi Comput. Soc. Nat. Comput. Conf. (NCC)*, Apr. 2018, pp. 1–5, doi: 10.1109/NCG.2018.8593029.

[6] M. J. Roberts, "The Cyber Threat and Globalization: The Impact on US National and International Security. By Jack A. Jarmon and Pano Yannakogeorgos. Lanham, MD: Rowman & Littlefield, 2018," *J. Strateg. Secur.*, vol. 11, no. 4, p. 5, 2019.

[7] M. Karjalainen, S. Sarker, and M. Siponen, "Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective," *Inf. Syst. Res.*, vol. 30, no. 2, pp. 351–710, 2019, doi: 10.1287/isre.2018.0827.

[8] S. Pahnila, M. Siponen, and A. Mahmood, "Employees' behavior towards IS security policy compliance," in *Proc. 40th Annu. Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2007, p. 156b.

[9] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from habit and protection motivation theory," *Inf. Manage.*, vol. 49, nos. 3–4, pp. 190–198, May 2012, doi: 10.1016/J.IM.2012.04.002.

[10] P. Patil, "Artificial intelligence in cybersecurity," *Int. J. Res. Comput. Appl. Robot.*, vol. 4, no. 5, pp. 1–5, 2016.

[11] E. Tyugu, "Artificial intelligence in cyber defense," in *Proc. 3rd Int. Conf. Cyber Conflict*, 2011, pp. 1–11.

[12] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, "Andromaly: A behavioral malware detection framework for Android devices," *J. Intell. Inf. Syst.*, vol. 38, no. 1, pp. 161–190, Feb. 2012.

[13] P. S. Deng, J.-H. Wang, W.-G. Shieh, C.-P. Yen, and C.-T. Tung, "Intelligent automatic malicious code signatures extraction," in *Proc. IEEE 37th Annu. Int. Carnahan Conf. Secur. Technol.*, May 2003, pp. 600–603, doi: 10.1109/CCST.2003.1297626.

[14] J.-X. Wu, J.-H. Li, and X.-S. Ji, "Security for cyberspace: Challenges and opportunities," *Frontiers Inf. Technol. Electron. Eng.*, vol. 19, no. 12, pp. 1459–1461, Dec. 2018, doi: 10.1631/FITEE.1840000.

[15] M. N. Al-Mhiqani, "Cyber-security incidents: A review cases in cyber-physical systems," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, pp. 499–508, 2018.

[16] J.-H. Li, "Cyber security meets artificial intelligence: A survey," *Frontiers Inf. Technol. Electron. Eng.*, vol. 19, no. 12, pp. 1462–1474, Dec. 2018, doi: 10.1631/FITEE.1800573.

[17] B. Kitcheman and S. Charters, "Guidelines for performing systematic literature review in software engineering," Keele Univ., Univ. Durham, Durham, U.K., EBSE Tech. Rep. EBSE-2007, 2007.

[18] B. Kitchenham and S. Charters, *Procedures for Performing Systematic Literature Reviews in Software Engineering*. Keele, U.K.: Keele Univ., 2007.

[19] U. Franke and J. Brynielsson, "Cyber situational awareness—A systematic review of the literature," *Comput. Secur.*, vol. 46, pp. 18–31, Oct. 2014, doi: 10.1016/J.COSE.2014.06.008.

[20] Y. Zacchia Lun, A. D'Innocenzo, F. Smarra, I. Malavolta, and M. D. Di Benedetto, "State of the art of cyber-physical systems security: An automatic control perspective," *J. Syst. Softw.*, vol. 149, pp. 174–216, Mar. 2019, doi: 10.1016/j.jss.2018.12.006.

[21] R. Leszczyna, "A review of standards with cybersecurity requirements for smart grid," *Comput. Secur.*, vol. 77, pp. 262–276, Aug. 2018, doi: 10.1016/J.COSE.2018.03.011.

[22] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018, doi: 10.1016/j.maturitas.2018.04.008.

[23] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technol. Health Care*, vol. 25, no. 1, pp. 1–10, Feb. 2017, doi: 10.3233/THC-161263.

[24] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *J. Syst. Softw.*, vol. 80, no. 4, pp. 571–583, Apr. 2007, doi: 10.1016/j.jss.2006.07.009.

[25] V. R. Basili, G. Caldiera, and H. D. Rombach, "The goal question metric approach," *Encycl. Softw. Eng.*, vol. 2, pp. 528–532, 1994,

[26] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 3, pp. 621–636, Mar. 2018, doi: 10.1109/TIFS.2017.2762828.

[27] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science*, vol. 349, no. 6245, pp. 255–260, Jul. 2015, doi: 10.1126/science.aaa8415.

[28] G. I. Webb, M. J. Pazzani, and D. Billsus, "Machine learning for user modeling," *User Model. User-Adapted Interact.*, vol. 11, nos. 1–2, pp. 19–29, 2001, doi: 10.1023/A:1011117102175.

[29] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Feature selection–based detection of covert cyber deception assaults in smart grid communications networks using machine learning," *IEEE Access*, vol. 6, pp. 27518–27529, 2018, doi: 10.1109/ACCESS.2018.2835527.

[30] Y. Gao, Y. Liu, Y. Jin, J. Chen, and H. Wu, "A novel semi-supervised learning approach for network intrusion detection on cloud-based robotic system," *IEEE Access*, vol. 6, pp. 50927–50938, 2018, doi: 10.1109/ACCESS.2018.2868171.

[31] C. Wang, Z. Zhao, L. Gong, L. Zhu, Z. Liu, and X. Cheng, "A distributed anomaly detection system for in-vehicle network using HTM," *IEEE Access*, vol. 6, pp. 9091–9098, 2018, doi: 10.1109/ACCESS.2018.2799210.

[32] Z. Dong, K. Kane, and L. J. Camp, "Detection of rogue certificates from trusted certificate authorities using deep neural networks," *ACM Trans. Privacy Secur.*, vol. 19, no. 2, pp. 1–31, Sep. 2016, doi: 10.1145/2975591.

[33] J. Yu, B. Zhang, Z. Kuang, D. Lin, and J. Fan, "IPrivacy: Image privacy protection by identifying sensitive objects via deep multi-task learning," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1005–1016, May 2017, doi: 10.1109/TIFS.2016.2636090.

[34] A. Squicciarini, C. Caragea, and R. Balakavi, "Toward automated online photo privacy," *ACM Trans. Web*, vol. 11, no. 1, pp. 1–29, Apr. 2017, doi: 10.1145/2983644.

[35] B. Bayar and M. C. Stamm, "Constrained convolutional neural networks: A new approach towards general purpose image manipulation detection," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2691–2706, Nov. 2018, doi: 10.1109/TIFS.2018.2825953.

[36] M. A. Bayero, "Effects of cashless economy policy on financial inclusion in nigeria: An exploratory study," *Procedia—Social Behav. Sci.*, vol. 172, pp. 49–56, Jan. 2015.

[37] Z. Cui, F. Xue, X. Cai, Y. Cao, G.-G. Wang, and J. Chen, "Detection of malicious code variants based on deep learning," *IEEE Trans. Ind. Informat.*, vol. 14, no. 7, pp. 3187–3196, Jul. 2018, doi: 10.1109/TII.2018.2822680.

[38] M. B. Neria, N.-S. Yacovzada, and I. Ben-Gal, "A risk-scoring feedback model for Web pages and Web users based on browsing behavior," *ACM Trans. Intell. Syst. Technol.*, vol. 8, no. 4, pp. 1–21, Jul. 2017, doi: 10.1145/2928274.

[39] M. E. Locasto, K. Wang, A. D. Keromytis, and S. J. Stolfo, "FLIPS: Hybrid adaptive intrusion prevention," in *Recent Advances in Intrusion Detection* (Lecture Notes in Computer Science), vol. 3858. Berlin, Germany: Springer 2006, pp. 82–101, doi: 10.1007/11663812_5.

[40] G. Giacinto, R. Perdisci, M. Del Rio, and F. Roli, "Intrusion detection in computer networks by a modular ensemble of one-class classifiers," *Inf. Fusion*, vol. 9, no. 1, pp. 69–82, Jan. 2008, doi: 10.1016/j.inffus.2006.10.002.

[41] E. Menahem, A. Shabtai, L. Rokach, and Y. Elovici, "Improving malware detection by applying multi-inducer ensemble," *Comput. Statist. Data Anal.*, vol. 53, no. 4, pp. 1483–1494, Feb. 2009.

[42] B. Zhang, J. Yin, J. Hao, D. Zhang, and S. Wang, "Malicious codes detection based on ensemble learning," in *Autonomic and Trusted Computing* (Lecture Notes in Computer Science), vol. 4610. Berlin, Germany: Springer, 2007, pp. 468–477, doi: 10.1007/978-3-540-73547-2_48.

[43] S. Arshad, M. A. Shah, A. Wahid, A. Mehmood, H. Song, and H. Yu, "SAMADroid: A novel 3-Level hybrid malware detection model for Android operating system," *IEEE Access*, vol. 6, pp. 4321–4339, 2018.

[44] R. Maciel, J. Araujo, J. Dantas, C. Melo, E. Guedes, and P. Maciel, "Impact of a DDoS attack on computer systems: An approach based on an attack tree model," in *Proc. Annu. IEEE Int. Syst. Conf. (SysCon)*, Apr. 2018, pp. 1–8.

[45] M. Woániak, M. Graña, and E. Corchado, "A survey of multiple classifier systems as hybrid systems," *Inf. Fusion*, vol. 16, pp. 3–17, Mar. 2014.

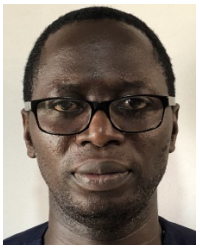
[46] M. Peker, "A decision support system to improve medical diagnosis using a combination of k-medoids clustering based attribute weighting and SVM," *J. Med. Syst.*, vol. 40, no. 5, p. 116, May 2016.

[47] T. W. Parsons, T. W. Jackson, R. Dawson, and others, "Usage and impact of ICT in education sector: A study of Navi Mumbai colleges," in *Proc. PIG*, vol. 3, Dec. 2015, pp. 1–7.

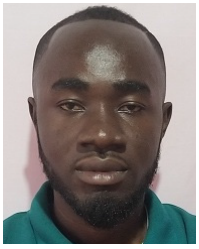
[48] Y. Li and W. Ma, "Applications of artificial neural networks in financial economics: A survey," in *Proc. Int. Symp. Comput. Intell. Des.*, Oct. 2010, pp. 211–214.

[49] J. Misra and I. Saha, "Artificial neural networks in hardware: A survey of two decades of progress," *Neurocomputing*, vol. 74, nos. 1–3, pp. 239–255, Dec. 2010.

[50] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, "Intrusion detection by machine learning: A review," *Expert Syst. Appl.*, vol. 36, no. 10, pp. 11994–12000, 2009.



ISAAC WIAFE received the bachelor's degree in mathematics from the Kwame Nkrumah University of Science and Technology, Kumasi, Ghana, and the M.Sc. degree in applied informatics and the Ph.D. degree in informatics from the University of Reading, U.K. He is currently the Head of the Intelligence Spaces and Machine Learning Laboratory, Department of Computer Science, University of Ghana, where he is leading advance research in AI applications for Human development. He is the inventor of the 3-Dimensional Relationship between Attitude and Behavior Model (3D-RAB): a robust model for gathering systems requirement for persuasive technology design. His research interest includes human–computer behavior change. His research interests include intelligent and persuasive spaces, information security behavior, and IT for behavior change and knowledge sharing in social networks.



FELIX NTI KORANTENG received the Bachelor of Science degree in computer science from the Kwame Nkrumah University of Science and Technology, Ghana, and the Master of Science degree in management information systems from the Ghana Institute of Management and Public Administration. He is currently a Researcher and a Lecturer Assistant with the University of Education, Winneba. His research interest includes persuasive technologies. He is particularly interested in persuasive systems that aim to entertain as well as educate. He is also concerned with issues of information and cyber security, human–computer interaction, social media sentiment analysis, and information and knowledge management. His current research interests include social networking sites and knowledge sharing in academic environments.

EMMANUEL NYARKO OBENG received the B.Sc. degree in computer science from the University of Ghana.

He was a Teaching Assistant with the Department of Computer Science, University of Ghana. He is currently an Associate with KPMG, Ghana. As a Consultant, his works focus on helping clients create and sustain value by establishing strategies to change, grow, adapt, shape and respond to disruptive forces, turning their technology vision into reality, optimizing their operations and streamlining support functions, converting their data into insight, transforming risk into a strategic advantage, embedding governance, risk and compliance throughout their organization, supply chain and business ecosystems and mitigating threats to their operations, and IT systems and business. He is also involved in the implementation of the control requirements of the following standards ISO 27001:2013 [Information Security Management System (ISMS)], ISO 27032:2012 (Cybersecurity Guidelines), ISO 27035:2016 (Information Security Incident Management), and ISO 22301:2019 [Business Continuity Management System (BCMS)], and an assessment of the SWIFT controls of the organization based on SWIFT Customer Security Program (CSP) framework for a leading financial institution in Ghana.

NANA ASSYNE received the bachelor's degree in business information technology from the Haaga-Helia University of Applied Sciences, Finland, and the Master of Science degree in information technology from the Lappeenranta University of Technology, Finland. He is currently pursuing the Ph.D. degree in computer science with the Faculty of Information Technology, University of Jyväskylä, Finland. He also holds a Professional Certificate in pedagogical studies in vocational teacher education with the Haaga-Helia University of Applied Sciences. He has over five years teaching experience in software engineering courses at the university level and supervising thesis, including supervising thesis at the Haaga-Helia University of Applied Sciences. Meanwhile, he is a Faculty Member of Ghana Institute Management and Public Administration (GIMPA), Ghana. Prior to working at GIMPA, he worked with the Haaga-Helia University of Applied Sciences, as a Student/Teacher Assistant, with nSense Oy, Finland, as a Software Developer, and with the Sekondi-Takoradi Metropolitan Assembly, Ghana, as the Head of the MIS Unit.

ABIGAIL WIAFE received the B.Sc. degree in computer science from Valley View University, Ghana, in 2007, and the M.Sc. degree in business technology consulting from the University of Reading, Reading, U.K., in 2012. She is currently pursuing the Ph.D. degree with the School of Computing, University of Eastern Finland, Finland. She is also a Lecturer with the Faculty of Computing and Information System (FoCIS), Ghana Technology University College. Her current research interests include affective music composition, genetic algorithms, machine learning, and music recommendation.

STEPHEN R. GULLIVER received the B.Eng. degree (Hons.) in microelectronics, the M.Sc. degree in distributed information systems, and the Ph.D. degree, in 1999, 2001, and 2004, respectively. He worked with the Human Factors Integration Defence Technology Centre (HFI DTC), before getting a job as a Lecturer at Brunel University, from 2005 to 2008. He joined the Henley Business School, University of Reading, in 2008, as a Lecturer and in 2014 was promoted to the role of an Associate Professor. Since 2005, his teaching and research (in the U.K. and abroad) has linked to the area of pervasive informatics. His research interests include multimedia and information assimilation, e-learning and education systems, usability and human factors, technology acceptance, persuasion systems, health systems, and systems conflict and failure.