REVIEW OF RESEARCH
ISSN: 2249-894X
IMPACT FACTOR : 5.7631(UIF)
VOLUME - 14 | ISSUE - 6 | MARCH - 2025

THE ROLE OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

Dr. Kiran Vinayakrao Magar
Assistant Professor Lal Bahadur Shastri Senior College Partur,
Dr.Babasaheb Ambedkar Marathwada University,
Chhatrapati Sambhgaji Nagar.

ABSTRACT :

Artificial intelligence (AI) is a powerful technology that helps cyber security teams automate repetitive tasks, accelerate threat detection and response, and improve the accuracy of their actions to strengthen the security posture against various security issues and cyber attacks. This article presents a systematic literature review and a detailed analysis of AI use cases for cyber security provisioning. The review resulted in 2395 studies, of which 236 were identified as primary. This article classifies the identified AI use cases based on a NIST cyber security framework using a thematic analysis approach. This classification framework will provide readers with a comprehensive overview of the potential of AI to improve cyber security in different contexts. The review also identifies future research opportunities in emerging cyber security application areas, advanced AI methods, data representation, and the development of new infrastructures for the successful adoption of AI-based cyber security in today's era of digital transformation and polycrisis.

KEYWORDS : *Artificial intelligence (AI) , cyber security , AI methods.*

1. INTRODUCTION

The term cyber security refers to a set of technologies, processes and practices to protect and defend networks, devices, software and data from attack, damage or unauthorized access [1]. Cyber security is becoming complex because of the exponential growth of interconnected devices, systems and networks. This is exacerbated by advances in the digital economy and infrastructure, leading to a significant growth of cyberattacks with serious consequences. In addition, researchers report the continued evolution of nation-state-affiliated and criminal adversaries, as well as the increasing sophistication of cyber attacks, which are finding new and invasive ways to target even the savviest of targets [2]. This evolution is driving an increase in the number, scale and impact of cyber attacks, and necessitating the implementation of intelligence-driven cyber security to provide a dynamic defence against evolving cyber attacks and to manage big data. Advisory organizations, such as the National Institute of Standards and Technologies (NIST), are also encouraging the use of more proactive and adaptive approaches by shifting towards real-time assessments, continuous monitoring and data-driven analysis to identify, protect against, detect, respond to, and catalogue cyber attacks to prevent future security incidents [3].

AI is an intriguing tool that can provide analytics and intelligence to protect against ever-evolving cyber attacks by swiftly analyzing millions of events and tracking a wide variety of cyber threats to anticipate and act in advance of the problem. For this reason, AI is increasingly being integrated into the cyber security fabric and used in a variety of use cases to automate security tasks or support the work of human security teams. The flourishing field of cyber security and the growing enthusiasm of researchers from both AI and cyber security have resulted in numerous studies to solve problems related to the identification, protection, detection, response and recovery from cyber attacks.

Several reviews on cyber security and AI applications were published in recent years [4], [5], [6], [7]. However, to the best of our knowledge, there is no comprehensive review that covers state-of-the-art research to explain cybersecurity activities covered by AI techniques and the details of how they are applied. Therefore, our objective was to provide a systematic review, a comprehensive view of AI use cases in cyber security, and a discussion of the research challenges related to the adaptation and use of AI for cyber security to serve as a reference for future researchers and practitioners.

2. BACKGROUND

This section is dedicated to analyzing the background information concerning the key concepts of this review, including the operational definition of cyber security using the NIST cyber security framework [3] and the AI taxonomy proposed by AI Watch [8] to clarify the concept of different applications of AI for cyber security.

2.1. CYBER SECURITY

Cyber security puts policies, procedures and technical mechanisms in place to protect, detect, correct and defend against damage, unauthorized use or modification, or exploitation of information and communication systems and the information they contain. The rapid pace of technological change and innovation, along with the rapidly evolving nature of cyber threats, further complicates the situation. In response to this unprecedented challenge, AI-based cyber security tools have emerged to help security teams efficiently mitigate risks and improve security. Given the heterogeneity of AI and cyber security, a uniformly accepted and consolidated taxonomy is needed to examine the literature on applying AI for cyber security. This structured taxonomy will help researchers and practitioners come to a common understanding of the technical procedures and services that need to be improved using AI for the implementation of effective cyber security.

For this purpose, a well-known cyber security framework proposed by NIST was used to understand the solution categories needed to protect, detect, react and defend against cyber attacks [3]. The NIST cyber security framework's core describes the practices to improve the cyber security of any organization. The framework's core has four elements: Functions, Categories, Subcategories and Informative references. The first two levels of the NIST framework, which consist of 5 cyber security functions and 23 solution categories, were used to classify the identified AI use cases. The functions provide a comprehensive view of the lifecycle for managing cyber security over time. The solution categories listed under each function offer a good starting point to identify the AI use cases to improve the cyber security. The main purpose of selecting these two levels is to provide a clear and intuitive categorization to classify the existing AI for cyber security literature into the appropriate solution category. The proposed taxonomy introduces a third level consistent with the first two levels by specifying AI-based use cases corresponding to each level of the cyber security framework, as shown in Fig. 1. A detailed description of the proposed taxonomy with a state-of-the-art review of AI for cybersecurity is provided in Section 5.

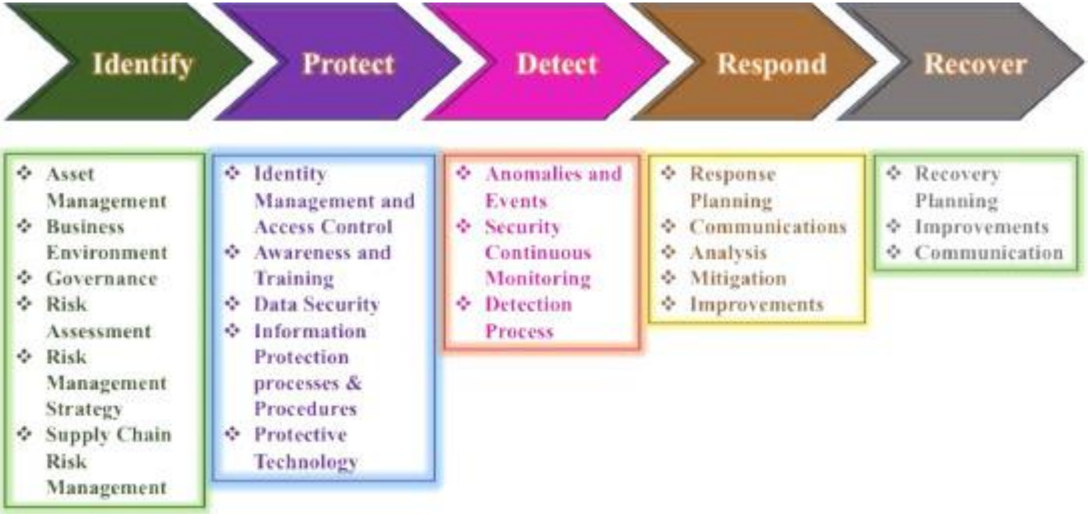


Fig. 1. NIST cybersecurity framework.

This taxonomy forms the basis for our SLR, by providing a description of the related subfields to cover the main aspects and fundamental keywords in the definition of cyber security solution categories. A detailed description of the keyword selection can be found in Section 3.

2.2. Artificial intelligence

Several definitions of AI systems can be found that relate to (a) the fields in which they are used and (b) the stages of an AI system's lifecycle, such as research, design, development, deployment and use. Since the focus of this paper is on AI applications for cyber security, a prevailing, but simplified, definition of AI is adopted: "systems that exhibit intelligent behaviour by analyzing their environment and with some degree of autonomy take actions to achieve specific goals" [9]. In practical terms, AI refers to a number of different technologies and applications that are used in a variety of ways. AI use cases in cyber security describe which environmental situations are desirable and undesirable, and assign actions to sequences.

For this SLR, the AI taxonomy proposed by Samoili et al. [8], which defines the core and transversal AI domains and subdomains, is used. The core AI domains, i.e., reasoning, planning, learning, communications and perception, were found to be useful as they encompass the main scientific areas of AI. Reasoning deals with knowledge representation and different ways of reasoning, while planning also covers searching and optimisation. Learning includes machine learning; communication is related to natural language processing; and perception is about computer vision and audio processing [8]. The approaches and technologies that make up these AI domains include, but are not limited to, fuzzy logic, case-based reasoning, genetic algorithm, Bayesian optimization, evolutionary algorithm, planning graph, artificial neural network, deep learning, support vector machine, natural language processing, text mining, sentiment analysis, image processing, sensor networks, object recognition and speech processing.

AI is a large, multidisciplinary research area, with a large body of literature addressing its applications and consequences from a variety of perspectives, e.g., technical, operational, practical and philosophical. This study focuses on the literature's thread that discusses the implications of the aforementioned methods and AI applications in cyber security scenarios. It analyses in detail how AI methods can be used for the identification, protection, detection, response and recovery in the domain of cyber security.

3. RESEARCH METHODOLOGY

The SLR aims to identify, evaluate and interpret all the available research in the area of interest to identify potential research gaps and highlight the frontiers of knowledge. It provides a high-quality, transparent and replicable review to summarize the large number of research studies. This study follows an SLR methodology for the following reasons: (i) AI for cyber security is a diverse field with a large quantity of literature; (ii) this study aims to answer specific research questions; (iii) the rigour and replicability it provides leads to an unbiased scientific study. The procedure for the SLR is described in detail below.

3.1. Selection of bibliometric database

Scopus and Web of Science (WoS) are the two most popular bibliometric databases. The Scopus database was chosen for this study because its coverage is almost 60% larger than that of the WoS [10]. In addition, Scopus offers better data management due to its wider coverage, advanced search filters and data analysis grids.

3.2. Search strategy

Between November 2021 and February 2022, a comprehensive search for terms related to AI and cyber security was conducted for the purpose of a thorough literature review of the impact of AI on cyber security. The search was performed using the well-specified search terms for the AI and cyber security fields, as shown in Table 2. The keywords of the AI and cyber security fields were combined using the logical AND operator. The logical OR operator within the different keywords was used to find studies that are related to any of the terms in each field. Specifically, the AI keywords correspond to the AI taxonomy proposed by AI Watch [8], and the cyber security keywords were taken from the NIST cyber security framework [3].

AI Keywords	Cyber Security Keywords
(("reasoning" OR "optimization" OR "machine learning" OR "artificial intelligence" OR "Natural language processing" OR "text mining" OR "classification" OR "feature extraction" OR "data mining" OR "sentiment analysis" OR "computer vision" OR "recognition" OR "genetic" OR "filtering" OR "GAN" OR "deep learning" OR "reinforcement learning" OR "data driven" OR "topic modelling")	("cyber security") AND (("asset management" OR "inventory" OR "configuration" OR "security control validation" OR "assessment" OR "asset" OR "security control testing" OR "security posture" OR "business impact" OR "governance" OR "risk management" OR "team" OR "risk indicators" OR "risk assessment" OR "automated vulnerability" OR "vulnerability" OR "fuzzing" OR "penetration" OR "vulnerability severity" OR "vulnerability management" OR "threat hunting" OR "automated penetration" OR "attack graph" OR ("risk" AND "investment") OR "risk quantification" OR ("risk" AND "supply chain") OR "role mining" OR "role maintenance" OR "Multi-Factor authentication" OR "authentication" OR “identity” OR ("contextual" AND "authentication") OR "access control" OR "unauthorized access" OR “VPN” OR ("attribute based access") OR "Role based access" OR "segregation" OR "isolation" OR "isolate" OR "network segmentation" OR "data loss" OR "data leakage" OR "SQL injection attack" OR "APT" OR "email" OR "malicious domain" OR ("integrity" AND

AI Keywords	Cyber Security Keywords
	"files") OR ("integrity" AND ("monitoring" OR "auditing")) OR ("automated" AND "configuration") OR "fake news" OR "backup" OR (("backup") AND (“data” OR “code”)) OR "plan" OR (("business continuity" OR "disaster Recovery" OR "incident response") AND ("automated")) OR "risk scoring" OR "risk prioritization" OR "vulnerability exploitation" OR (("Risk") AND ("remediation")) OR (("log" OR "audit") AND ("analysis")) OR "SIEM" OR "VPN" OR "firewall" OR "IPS" OR "antivirus" OR "antimalware" OR "immune system" OR ((("anomaly") OR ("event") OR ("intrusion") OR ("fraud")) AND ("detection") OR (("event correlation") OR ("security intelligence") OR ("event analysis") OR ("correlation") OR ("SIEM") OR ("SOC") OR ("monitoring") OR ("behavior Based") OR ("social network") OR ("threat intelligence")) OR ("dark web") OR ("chatter noise") OR ("translate") OR ("topic modelling") OR ("sentiment analysis") OR ("cyber trap") OR ("threat intelligence”) OR ("darknet") OR ("deepnet") OR ("social network") OR ("sentiment") OR ("honeypot")) OR (("incident") AND (("detection") OR ("response") OR ("playbook") OR ("case based") OR ("case") OR ("identification") OR ("assessment") OR ("classification") OR ("categorisation") OR ("categorising"))) OR (("cybersecurity") AND ("triage")) OR (("forensic") AND (("intelligent") OR ("incident")) OR "isolation" OR "remediation" OR "risk quantification" OR "recommender system" OR (("incident") AND (("analysis") OR ("report") OR ("document") OR ("information"))) OR (("recovery") AND (("planning") OR ("dynamic")) OR ("safe")) OR "recovery")

3.3. Inclusion and exclusion criteria

Following the search stage, the studies identified were screened to eliminate irrelevant work. To find the pertinent papers that address the research questions, the studies gathered in the earlier stage were subject to inclusion and exclusion criteria. A significant, yet manageable, selection of studies must be ensured at this point. The search conducted was not limited to a specific period and also considered early publications to avoid overlooking any important studies. The inclusion criteria were as follows:

-The article is written in English.
-The article is a full research paper (i.e., not a presentation or supplement to a poster).
-The article should make it apparent that AI is its primary emphasis or include AI as a large part of the methodology. For example, publications that explicitly include machine learning as a core component of their methodology/research.
-One or more of the research questions posed in this research are directly answered by the article.
-For studies that have appeared in multiple journals or conferences, the most recent version is considered.
-The following publications were excluded from further review:
-The studies that are not written in English;
-The studies that provide a review or survey of AI in different cyber security domains;
-The articles that represent the same work by authors in different conferences or journals were also filtered to remove duplicates;
-The articles that provide a comparative analysis of different AI models or existing techniques for cyber security tasks;
-The articles that improve the security of AI techniques to make them attack resistant;
-The papers providing only recommendations, guidelines or principles for cyber security (non-scientific);
-Editorials, books, chapters and summaries of workshops and symposiums;
-The studies that do not provide sufficient information;
-The studies that have fewer than 5 pages;
-The studies where a full text could not be found.

3.4. Selection of primary studies

Fig. 2 shows in detail the selection process for the study. After the initial step of identifying and applying a search term, the inclusion and exclusion criteria were applied to refine the 2395 studies retrieved from the Scopus database. Based on the removal of non-English papers, posters, reviews, surveys, non-scientific publications, editorials, books, chapters, summaries of workshops and symposia, duplicates, guideline documents, and comparative studies, 366 articles were removed, leaving 2029. These 2029 studies were analyzed based on the title and abstract. The title and abstract provided a clear indication of whether the study was outside the focus of the review and could therefore be excluded. If the title or abstract did not clearly indicate the application domain or contribution of the study, it was included in the review for subsequent steps where full text of the article was examined. Based on the title and abstract analysis, the 2029 studies were further narrowed down to 638. After a thorough examination of the full articles, 402 additional studies were eliminated. As a result, a total of 236 primary studies served as the basis for this SLR. The next sections present the findings and analysis of these 236 primary studies.

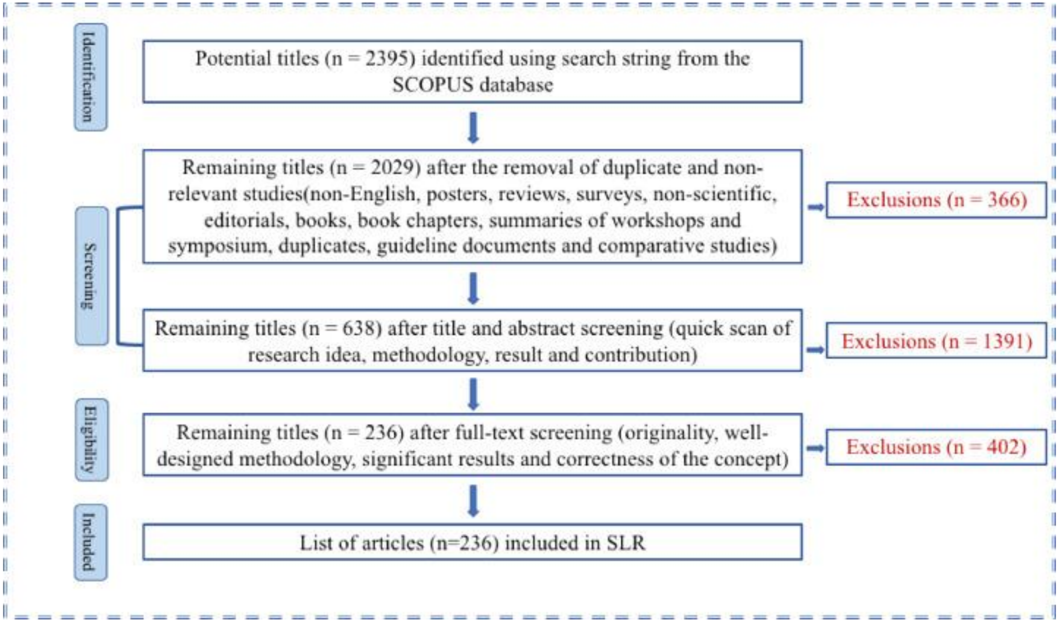

Identification
Potential titles (n = 2395) identified using search string from the SCOPUS database
Screening
Remaining titles (n = 2029) after the removal of duplicate and non-relevant studies(non-English, posters, reviews, surveys, non-scientific, editorials, books, book chapters, summaries of workshops and symposium, duplicates, guideline documents and comparative studies)
Exclusions (n = 366)
Remaining titles (n = 638) after title and abstract screening (quick scan of research idea, methodology, result and contribution)
Exclusions (n = 1391)
Eligibility
Remaining titles (n = 236) after full-text screening (originality, well-designed methodology, significant results and correctness of the concept)
Exclusions (n = 402)
Included
List of articles (n=236) included in SLR

Fig. 2. Selection process and study count at each stage of the SLR protocol.

4. DATA EXTRACTION

After the selection of the primary studies, data extraction began to feed the state-of-the-art and descriptive analysis phase. The main goal of data extraction is to break down each study into its constituent parts and describe the overall relationships and connections. The data extraction parameters (explained in Table 3) collect the qualitative and contextual data from the primary studies selected for the SLR. The qualitative data are collected to write a short summary of each primary study to present the contribution along with the demographic information. The contextual data include details about the cyber security function, solution category, use cases, and core AI domain, to have a clear understanding of the existing literature. These qualitative and contextual data are further examined to identify the relationships between the different studies.

Table 3. Data extracted from each primary study.

Data Type	Data Item	Description
Qualitative Data	Title	Title of the primary study
	Author	Author of the study
	Year Published	Publication year of study
	Article Type	Publication type, i.e., conference, journal
	Source	Journal/Conference name that published the study
	Geographical Region	Geographic region of the authors of the primary study
	Summary	A summary of the paper, with major contribution.
Contextual Data	Cyber security Function	Type of cyber security activity in primary study. NIST taxonomy defines cyber security activities as 5 functions: Identify, Protect, Detect, Respond, Recover.
	Solution	Identification of the main solution category in which primary

Data Type	Data Item	Description
	Category	study falls. The NIST taxonomy provides a subdivision of each cyber security function into groups of cyber security solution categories, e.g., the detection function is divided into 3 categories: anomalies and events, security continuous monitoring and detection processes.
	Specific Use Case	Specific cyber security use case of primary study for AI application to match the function and solution category.
	Core AI Domain	Core AI domain of the AI technique used by the primary study as defined by the AI Watch [7].

5. STATE OF THE ART

To identify the studies that evaluate the application of AI for cyber security, a taxonomy is proposed to classify the studies that address the first two research questions (RQ1 and RQ2). The first two levels of the taxonomy are adopted from the NIST cyber security framework. The first level organizes the cyber security literature into five core functions: identify, protect, detect, respond and recover. These five cyber security functions cover the use of AI tasks from the prevention of the security attack to the more complex mechanism of actively looking for new threats and counterattack. The functions cope with different aspects of the cyber security attack lifecycle for an effective defence. The second level of taxonomy uses the NIST framework's categories to expand the core functions into different cyber security solutions with closely tied programmatic needs and particular activities. The last level of the taxonomy presents the AI use cases associated with the upper level of taxonomy and link the SLR with each identified use case. Fig. 3 summarizes the proposed taxonomy and presents the logical progression of cyber security functions along with a detailed description of the different categories of cyber security solutions implemented using the AI technologies.

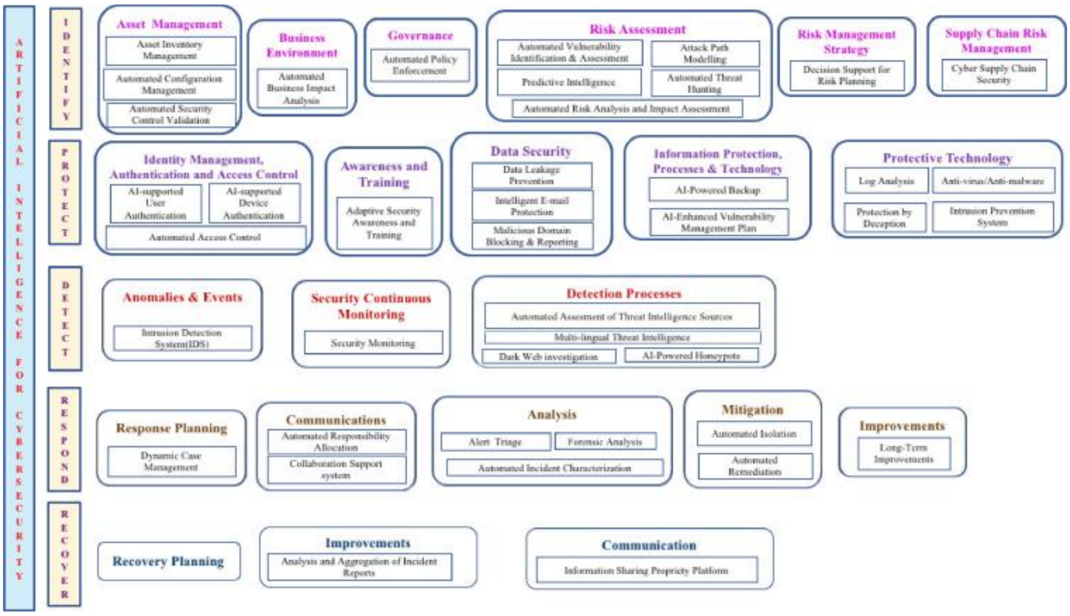

ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY
IDENTIFY
Asset Management
Asset Inventory Management
Automated Configuration Management
Automated Security Control Validation
Business Environment
Automated Business Impact Analysis
Governance
Automated Policy Enforcement
Risk Assessment
Automated Vulnerability Identification & Assessment
Attack Path Modelling
Predictive Intelligence
Automated Threat Hunting
Automated Risk Analysis and Impact Assessment
Risk Management Strategy
Decision Support for Risk Planning
Supply Chain Risk Management
Cyber Supply Chain Security
PROTECT
Identity Management, Authentication and Access Control
AI-supported User Authentication
AI-supported Device Authentication
Automated Access Control
Awareness and Training
Adaptive Security Awareness and Training
Data Security
Data Leakage Prevention
Intelligent E-mail Protection
Malicious Domain Blocking & Reporting
Information Protection, Processes & Technology
AI-Powered Backup
AI-Enhanced Vulnerability Management Plan
Protective Technology
Log Analysis
Anti-virus/Anti-malware
Protection by Deception
Intrusion Prevention System
DETECT
Anomalies & Events
Intrusion Detection System(IDS)
Security Continuous Monitoring
Security Monitoring
Detection Processes
Automated Assesment of Threat Intelligence Sources
Multi-lingual Threat Intelligence
Dark Web investigation
AI-Powered Honeypots
RESPOND
Response Planning
Dynamic Case Management
Communications
Automated Responsibility Allocation
Collaboration Support system
Analysis
Alert Triage
Forensic Analysis
Automated Incident Characterization
Mitigation
Automated Isolation
Automated Remediation
Improvements
Long-Term Improvements
RECOVER
Recovery Planning
Improvements
Analysis and Aggregation of Incident Reports
Communication
Information Sharing Propriety Platform

Fig. 3. Proposed taxonomy of AI techniques in the cybersecurity domain.

5.1. Identify

The **identify** function provides the foundation for the other cybersecurity functions by pinpointing the critical functions and risks associated with systems, people, assets and data. This helps develop an understanding of the current state of the cyber security, identify gaps, and develop an appropriate risk management strategy to achieve the desired security based on the organization's own needs, risks and budget. Table 4 summarizes the main contribution of each primary study in the identify function.

5.2. Protect

The **protect** function helps plan and implement appropriate controls to limit or contain the impact of a potential cyber security event. This includes a number of technical and procedural controls to proactively protect against internal and external cyber threats. AI can improve the resilience of the system by authenticating users, devices and other assets, monitoring the user behaviour, automated access control, adaptive training, data leakage prevention & integrity monitoring, automated information protection and processes and provision of protective solutions to proactively secure the system

5.3. Detect

The **detect** function enables the timely discovery of the cyber security events by developing and implementing appropriate activities to identify their occurrence. This function is crucial for the security as prompt detection will minimize the disruption. It includes activities for the timely detection of intrusions and anomalies along with the impact assessment, implementation of security continuous monitoring to verify the effectiveness of protective measures, and appropriate maintenance of detection processes to ensure the awareness of cyber events. AI can improve the detection speed by monitoring the internal and external information sources and swiftly correlating this information to detect the unusual activities to minimize the repercussions. Table 6 presents a summary of the main contribution of each research study to the detect function, along with the details of the solution category, AI use cases and the AI domain used.

5.4. Respond

The **respond** function creates a roadmap for managing and limiting the impact of a potential cyber security event. This function is critical as it represents the first line of Defence in incident handling and develops risk mitigation approaches for the future. This function includes planning ahead to develop effective processes to address the problem, analyze the incidents to determine their cause, scope and impact, incident containment, and the coordination of communication during and after an attack. By using AI techniques for response activities, incidents can be resolved more quickly and with less time and effort for security analysts.

6. DESCRIPTIVE ANALYSIS

After the state-of-the-art analysis, the statistical distribution of the primary studies is shown in terms of the taxonomy, the AI technique used, the publication type, the publication year, and the geographical distribution of the research advances to answer RQ3.

6.1. Distribution by article type

Of the 236 articles selected for the SLR, 101 articles (43%) are sourced from conference proceedings and 135 (57%) from peer-reviewed journals, as shown in Fig. 5.

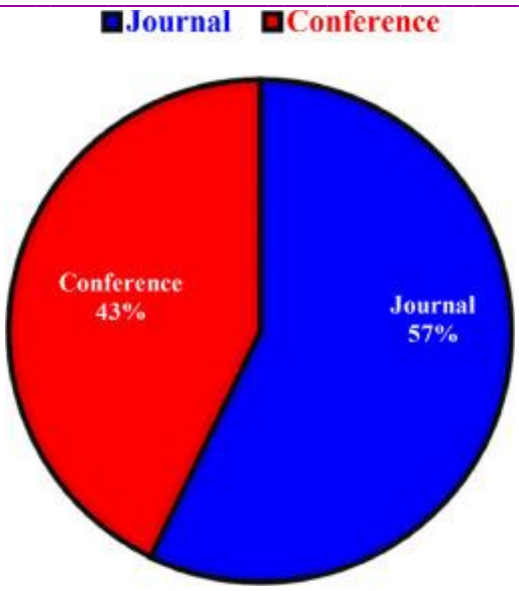


Fig. 5. Article distribution by type of publication.

6.2. Distribution by publication year

The time span of this review was 2010 to February 2022. As Fig. 6 illustrates, AI for cyber security was a relatively under researched topic till 2016, with only a handful of studies published in peer-reviewed journals and at conferences. Only in the last four years (2018 to 2021) has there been an increase in interest in AI as a cyber security research topic. Fig. 6 also shows the implications of Covid-19 in terms of a smaller number of conference publications in 2021 compared to previous years. In contrast, the number of journal publications in 2021 increased by nearly 2.6 times compared to the previous year.

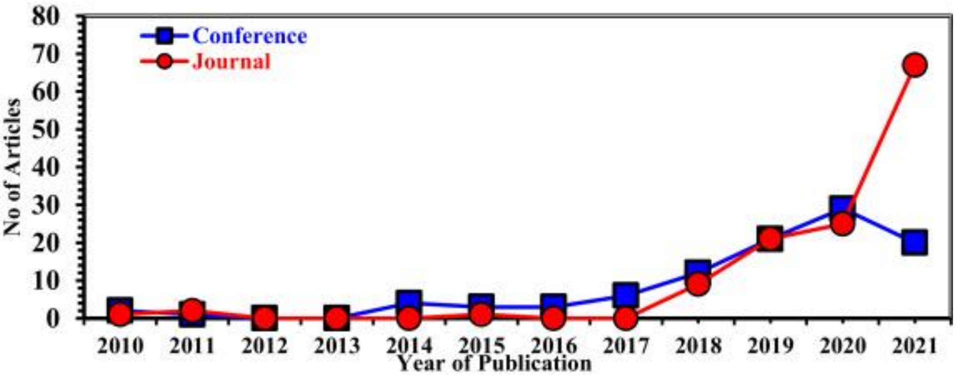
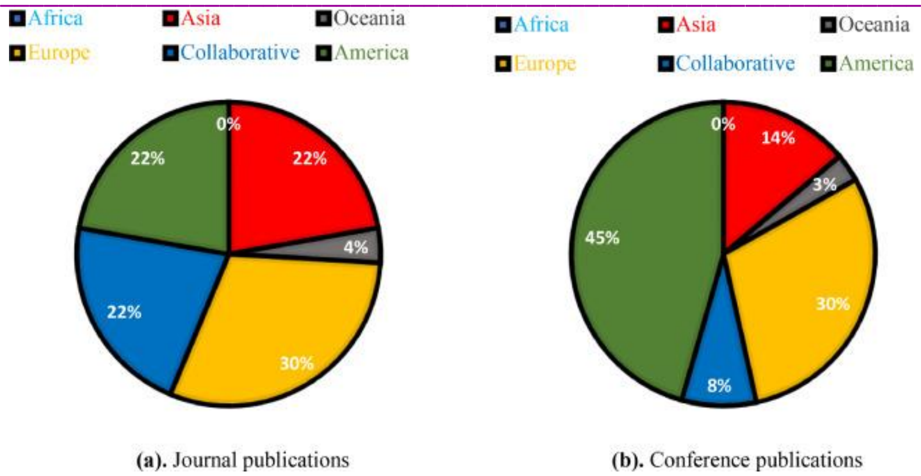


Fig. 6. Annual distribution of articles.

6.3. Distribution by geographical region

The geographical distribution of the authors of the referenced articles is presented here according to the five continents: Asia, America, Europe, Africa, and Oceania. The joint articles by authors from different continents are presented as a collaborative region. For the selected journal publications (see Fig. 7(a)), 30% of the researchers are located in Europe, followed by 22% researchers in Asia, and 22% in America. Oceania has relatively few research papers on the topic, only 4%. Africa has zero journal publications in the selected pool. The remaining 22% of articles are collaborative efforts by researchers from different continents.



(a). Journal publications (b). Conference publications

Fig. 7. Geographical distribution of primary studies related to AI for cyber security.

7. RESEARCH GAPS

To answer the research question of this paper, the literature relevant to our research questions was scrutinized to highlight potential research gaps and identify opportunities for future AI for cyber security research. A key element in conducting AI for cyber security research is identifying emerging application areas, appropriate resources (e.g., data sources and management, computational infrastructure, etc.), and advanced AI techniques for the successful adoption of AI for cyber security. This section provides useful directions for future research in four main areas: (i) emerging areas of cyber security applications, (ii) data representation, (iii) advanced AI methods for cyber security, and (iv) research and development of new infrastructure.

8. LIMITATIONS

The presented SLR provides valuable information on the intersection between cyber security and AI techniques, along with the identification of research gaps to feed future research. Nevertheless, our study misses the articles that are published in scientific databases other than Scopus or used different keywords. Also, recent publications (after February 2022) are not included in the studied literature due to time spent on analysing the selected primary studies to obtain reliable results.

9. CONCLUSIONS

This SLR study examines the current state-of-the-art research on AI applications for cyber security. This was achieved by identifying 236 primary studies out of 2395 related articles from the Scopus database over a 13-year period (2010 to February 2022). The presented study discusses the different AI techniques applied in the cyber security domain and which cyber security activities have taken advantage of the AI technology. The selected literature is analyzed in terms of (i) the presented taxonomy of AI in cyber security, (ii) the frequency of publication by year, (iii) the frequency of publication by geographical region, (iv) the cyber security contribution type, and (v) the type of AI technique used.

This SLR examined the "how" and "what" of the existing research on AI applied to cyber security with an in-depth exploration of specific use cases and the theoretical basis of the research. This study contributes to the body of knowledge by analyzing the evolution of AI applications in the cyber security domain and identifying research gaps. The evolution of AI in cyber security was studied with respect to different functions, solution categories, specific use cases, and the type of AI technique used. The results of the analysis revealed that the number of publications is increasing, but more attention must be paid to the acquisition and representation of historical data related to different cyber security functions to implement practical AI-based cyber security solutions. The main contribution of this study is the classification of the primary studies to integrate the state of literature in this area and to comprehend the significance of AI for cyber security. In addition, the article has proposed future research directions to address emerging issues for the successful adoption of AI for cyber security.

REFERENCES

1. Bhardwaj, M.D. Alshehri, K. Kaushik, H.J. Alyamani, M. Kumar Secure framework against cyber-attacks on cyber-physical robotic systems J. Electron. Imaging, 31 (6) (2022) Google Scholar P. Chithaluru, A.T. Fadi, M. Kumar, T. Stephan Computational intelligence inspired adaptive opportunistic clustering approach for industrial IoT networks IEEE Internet Things J (2023), 10.1109/JIOT.2022.3231605 View at publisher Google Scholar
2. M. Barrett Technical Report National Institute of Standards and Technology, Gaithersburg, MD, USA (2018) Google Scholar
3. I. Wiafe, F.N. Koranteng, E.N. Obeng, N. Assyne, A. Wiafe, S.R. Gulliver Artificial intelligence for cybersecurity: a systematic mapping of literature IEEE Access, 8 (2020), pp. 146598-146612 CrossrefView in ScopusGoogle Scholar
4. Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, K.K.R. Choo Artificial intelligence in cyber security: research advances, challenges, and opportunities Artif. Intell. Rev., 55 (2022), pp. 1029-1053 CrossrefView in ScopusGoogle Scholar
5. J. Martínez Torres, C. Iglesias Comesaña, P.J. García-Nieto Machine learning techniques applied to cybersecurity Int. J. Mach. Learn. Cybern., 10 (10) (2019), pp. 2823-2836 CrossrefView in ScopusGoogle Scholar
6. T.C. Truong, I. Zelinka, J. Plucar, M. Čandík, V. Šulc Artificial intelligence and cybersecurity: past, presence, and future Artificial intelligence and evolutionary computations in engineering systems (2020), pp. 351-363 CrossrefView in ScopusGoogle Scholar
7. S. Samoili, M.L. Cobo, E. Gomez, G. De Prato, F. Martinez-Plumed, B. Delipetrev, A.I. Watch Technical report Joint Research Center (Seville site) (2020) Google Scholar
8. High-Level Expert Group on Artificial Intelligence. (HLEG AI), A definition of AI: main capabilities and disciplines, (2019). Retrieved from Brussels https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341. Google Scholar
9. D. Zhao, A. Strotmann, Analysis and visualization of citation networks, Synthesis lectures on information concepts, retrieval, and services, 7 1 (2015) 1–207. Google Scholar
10. V.G. Promyslov, K.V. Semenkov, A.S. Shumov A clustering method of asset cybersecurity classification IFAC-PapersOnLine, 52 (13) (2019), pp. 928-933 View PDFView articleView in ScopusGoogle Scholar
11. K. Millar, A. Cheng, H.G. Chew, C.C. Lim Operating system classification: a minimalist approach 2020 International Conference on Machine Learning and Cybernetics (ICMLC) (2020), pp. 143-150
12. CrossrefView in ScopusGoogle Scholar A. Aksoy, M.H. Gunes Automated iot device identification using network traffic IEEE International Conference on Communications (ICC) (2019), pp. 1-7 View at publisherCrossrefGoogle Scholar
13. A. Sivanathan, H.H. Gharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath, V. Sivaraman Classifying IoT devices in smart environments using network traffic characteristics IEEE Trans. Mobile Comput., 18 (8) (2018), pp. 1745-1759 Google Scholar