A Survey on Cyber Security Meets Artificial Intelligence: AI– Driven Cyber Security

S. P. Samyuktha[1,*], P. Kavitha[1],V. A. Kshaya[1], P. Shalini[1], R. Ramya[1]

[1]Department of AI&DS, Panimalar Engineering College, Chennai, India

Emails : spsamyu516@gmail.com; bharathi3803@gmail.com; drkavitha.ads2021@gmail.com; shaluparthi789@gmail.com; ramesharithu@gmail.com

Abstract

The computerized version of human intelligence is Artificial Intelligence(AI). Artificial Intelligence systems combine large sets of data with intelligent and iterative processing algorithms in order to make predictions, based on patterns and features in the data that they analyse. With the booming technologies such as IOT and Cloud Computing, huge amounts of data are generated and collected that require cyber security protection today. There is a growing need for cyber security methods which are both robust and intelligent due to the ever-increasing complexity of cyber crimes. While data can be used to benefit business interests, it poses a number of challenges in terms of security and privacy protection. Artificial Intelligence (AI) based technologies, such as machine learning statistics, big data analysis, deep learning and so on, have been used to deal with cyber security threats. These technologies are used for intrusion detection systems, malicious software detection, and encrypted communications. In the rapidly growing field of AI driven security, scientists from multiple disciplines work together to combat cyber threats. AI models require unique cyber security defence and protection technologies. This survey provides various method, different datasets and methodologies that may be used for the proposed IA enabled cyber security technologies. This study aims to classify the AI-based cyber security solutions gathered and describe how they can help solve problems in the field of cyber security.

Keywords: Artificial intelligence; Cyber security; Machine learning; Detection system; AI based cyber security

1. Introduction

AI is a rapidly growing branch of computer science that seeks to develop theories, techniques, platforms, and applications that can stimulate, extend, and expand human intelligence. Artificial intelligence, considered one of the key technologies of the fourth industrial revolution, is one of the fastest-growing branches of the field. The use of artificial intelligence automates tasks that are predictive and make them easier or more efficient without requiring too much human interaction. AI can generate and analyses amount of data, such as from logs and network sensors, greatly reducing the workload security professional machine learning is the AI sub-discipline that focuses on the application of computer algorithms to discover patterns in data. The cyber security industry has greatly benefited from ML technologies.

AI solutions allow machines to collect historical data and identify past trends, facilitating future decision-making and planning. In this way, machines can distinguish between permissible and prohibited behaviours by using the clues available. Machine learning techniques can help identify and reduce the risk of system or network breaches using expert analysis.

DOI: https://doi.org/10.54216/JCHCI.020202

Received: October29, 2021 Accepted: March21, 2022

The classification techniques employed in this sub-discipline of artificial intelligence permit it to predict the likelihood of samples belonging to pre-defined classes, such as spam emails. In addition to clustering data into discrete groups, machine learning can also recognize security breaches by using certain key attributes. By doing so, we can easily identify items that don't conform with given clusters for further monitoring and testing.

A. AI-Driven Cyber Security

Expect system, computer vision, pattern detection, language translation, robotics, biometric system and internet of things are the application of artificial intelligence manmade inference is required for monitoring its activity because it can also use for demolition. Currently, artificial intelligence (AI) is the main focus of the cyber security in dustry.AI appears to be in vogue these days, but it refers to some techniques that can be very valuable for security.

It consists of ML algorithm that can detect and respond to threats as they occur. They can predict whether the inward data are actually male violent or safe. The use of artificial intelligence in cyber security increases speediness and scalability. This paper focus on "AI-driven cyber security" to make the cyber security figuring process computerized and smart than the conventional security systems in the zone.

Figure 1: AI in Cyber Security

B. Ml in Cyber Security

The ML algorithms help in resolving the problems of classification as well as sensing and mitigating cyber threats. In many areas, the machine learning techniques are used because of the ir unique characteristics like scalability, adaptability, etc....ML can be influenced by cyber security to improve the malware detection, alert organisation to security problem. In addition, machine learning increases the speed to tackle enormous volumes of attack. In cyber security attack, the AI and ML play a vital role in the detective works. Machine learning algorithms are used in application to detect and respond attacks.

Figure 2: AI in Cyber Security

DOI: https://doi.org/10.54216/JCHCI.020202

Received: October29, 2021 Accepted: March21, 2022

2. Related Works

To address the issue that needed intelligence from human perspective, a numerous methods were brought up in the field of artificial intelligence. An overview of [3][6] AI may not be able to present a full study of all applications of AI techniques. As an alternative, the methods and architectures have been grouped into several divisions: machine learning, neural networks, intelligent agents, data mining and constraint solving, expert systems, search. We get into these divisions and provide a solution to the applications of individual tactic in cyber security. The Role of Artificial Intelligence in Cyber Security Traditional methods for data security needs incredible humanoid efforts to recognize the threats, excerpt properties of threats and encrypt properties of threats into software to detect the intimidations.

Deep belief network- based attack defence [18] is used to directly recognise malware from the information flows in android applications Zhuelat (2017) projected a unique DL-based approach as "Deep flow" whose theme is enforced by DBN which support the deep flow and complex attack feature is analysed. it consists of 3 components: Flow Droid used for feature extraction, DBN metric capacity and also SUSI for feature coarse granularity. It provides deep learning solution for defending against cyber space attack.

Irbil H. Starker Mad Has and Furan Razz Norway proposed a signature-based technique intrusion detection system (SIDS)[7] regarding knowledge-based approach which is used to avoid and blocks the malicious activities after detection for the known attacks. It can be used on the beginning level. It is one of the most communal software recognition techniques. It detects the cyber-attack or malware by comparing certain signatures. Amazon Web Services are used by the Siemens AG, leader of Global electrification, automation and digitalization to provide high speed, self-controlled and elastic platform for CDC (cyber defence centre). ML can use security information and event management (SIEM) and security orchestration, automation, and response (SOAR) tools to improve data automation and intelligence gathering, detecting suspicious behaviour patterns, and automating the response depending on the input. Microsoft uses its own ATP (windows defender advanced threat protection) cyber security platform used for breach detection, automated investigation and preventive protection. It IS built-in; automatically employ multiple layers of ML algorithms and AI to detect threats.

With the use of neutral network [10], Menetal. (2017) proposed a novel model, named "malware classification based on static malware gene sequences (MCSMGS), "for malware classification for the intrusion detection. It was appealed that the organization accuracy was up to 98% with the projected scheme, and it was more efficient than the SVM model. RNN based attack detection which Cloud-based cyber physical intrusion detection was proposed by Lukasetal (2108) for the web of Vehicles employing a in-depth multilayer perceptron associated agree an RNN.

For the detection of malware, SVM (support vector machine) [4] is a supervised knowledge algorithm which is a core idea to separate the data by raising a suitable split plane. it it produces a lower false positive rate and higher accuracy proposed by Kokilaetal. SVM classifier is deployed to detect distributed denial of survive. They compared the performances between the SVM classifier and other techniques by some experiment on the DAPRA dataset. It shows 96.90% accuracy in spam base datasets. Decision tree algorithm [14] was proposed by J. Renetal to measure multiple types of buffer overflow of vulnerability. It is a projecting modelling method from the field of machine learning and statistics that construct as impel tree I like structure to model the fundamental pattern. It results in 87.51% accuracy.

DOI: https://doi.org/10.54216/JCHCI.020202
Received: October29, 2021 Accepted: March21, 2022

Table1:Summarization of Methodology and methods used in cyber security with artificial intelligence

AUTHOR	AI TECHNIQUE	PROPOSED METHODS	CYBER THREAT	MERITS
B.Christian,D.A.ElizondoandT.Watson[10]	Neutral network (Use of genetic algorithm for optimization problems)	ANN (ArtificialNeutral Network)	Network Intrusion	Ensures optimal security toopen channels(99%accuracy)
IqbalH.SarkerMd HasanFurharRaz Nowrozy[11] (26 March 2021)	Genetic algorithm	Genetic algorithm	Signature–based intrusion.	Avoids and block the known malicious activities after detection.
Jian–HuaLI[8] SyarifandGata(2017)	Pattern Recognition and Machine Learning Algorithm	K-means and Random Forest Algorithm, PSO(partial swap optimisation)	Dos,Probing,U2R,R2L.	Easy interpretation, low calculation
ShidawaBabaAtiku[12] (2020 Oct 10)	Approach towards data security	Amazon Web Services(AWS)	Phishing Attacks	Protect data from unauthorised access.
Zhuetal. (2017) Jian-huaLI (2018)[8]	Deep learning solution for defending. DL-based approach called “Deep Flow”.	Probabilistic neural network(PNN), DBN.	Cyber space attack	Unswervingly detect the malware from the data flow in android application
IqbalH.Sarker·Md HasanFurhad·RazaNowrozy[11] (22 March 2021)	Supervised learning algorithm.	The support vector machine(SVM)	Malicious network traffic	Improve accuracy of IDSs, produce low positive rate (FPR).

DOI: https://doi.org/10.54216/JCHCI.020202

Received: October29, 2021 Accepted: March21, 2022

Syarif Jamal Malik& Farrukh Aslam Khan. (2017)[13]	Hybrid approach	K-Nearest Neighbourhood (KNN) algorithm, PSO (practical swap optimisation)	Node pruning, Network intrusion	Easy interpretation, low calculation, better than other classifiers in terms of intrusion detection (2%moreaccuracy)
Carlasayaetal, Feng Tao, Muhammad Shoaib Akhtar and Zhang Jiayuan [7] (7 July 2021)	Intelligent support for a professional in human security.	Focus and implementation of an ICSA architecture	Cyber-attacks.	Effective analysis and progress automated and semi automatic behaviour to defence the vulnerabilities.
Binny Naik Ashir Mehta HiteshriYagnik2· MananShah3[14] (3Aug2021)	Artificial immune system	Deep CA, Signal categorization (99%accuracy)	IoT Network intrusion, DoS attacks	Improve efficiency and reduce the false-positive rates to limit the false alerts in the IoT network.
Shidawa Baba Atiku (10 Oct 2020)[12]	Intelligent agent(AI)	Artificial Digital police.	To evade Distributed Denial of Service (DDoS) attacks.	Provide execution of infrastructure to support mobility and communication of cyber agents.
SonuVelgekar, HarshKhandve,Ra jeshwariGundla (5 May 2021)[1]	Professional System	Adaptive Expert System (AES)	Detecting erudite cyber-attacks.	Increase the chances of detecting some complex anomalies and cyber outbreaks.

DOI: https://doi.org/10.54216/JCHCI.020202
Received: October29, 2021 Accepted: March21, 2022

3. Various datasets used:

A dataset is a collection of raw statistics and information generated by this research.

Table 2: Various datasets used for AI driven cyber security

Datasets	Description
DARPA dataset	Intrusion detection dataset that includes LLDOS1. 0 And LLDOS2.0.2 attack scenario data. data traffic and attack consisting in DARPA are placed together by MIT lin coin laboratory for estimating network intrusion recognition system
ISOT‟10dataset	An amalgamation of both malicious and non-malicious type of data traffic created by information security and object technology (ISOT) research at university of Victoria to gauge ML- based classification models ISOT dataset can be used.
CTU-13dataset	A labelled malware dataset including botnet „normal, and background traffic that was seized at CTU university, czech republic. CTU-13 can be used for data-driven malware examination using ML techniques and to evaluate the malware detection system.
MAWI dataset	A collection of Japanese network research institution used to spot and evaluate DDoS intrusion using ML algorithms.
Enron dataset	Using k-mean clustering you can build a model to detect fraudulent activities. k-mean mustering is an unsupervised machine learning algorithms. it separates the observation into k number of duster based on the similar pattern in the data.
Twitter base dataset	A spam detection support vector learning model.

In the above section we have discussed about the introduction, diverse new methods that can be used for AI driven cyber security and registered the purpose of those approaches. Each approach provides various purposes which are useful for defending cyber security outbreaks, various datasets used for AI and ML in cyber security are tabulated.

4. Conclusion

This paper has provided brief information about AI driven cyber security. AI gives an alarm to an individual before the attack of the private data and also protects the uses data using definite algorithms. The condition of AI and cyber security provides more and more applications. AI spots any spyware on a network immediately and mentors incident response. AI driven cyber security provides all the required investigations and threat identifications. The main goal of cyber security is to safe guard the data and it can be achieved with the help of AI. Since, AI is yet a developing field; it could become a good-fortune in the field of cyber-security. The concept of AI cyber security meets artificial intelligence which is explained in this paper can help there searchers as well as industry professionals of the ir forth coming study in the field of AI driven cyber security. As the cyber crime rate is increasing day by day, humans are notable to control it. Hence, AI in cyber security most ideal novel techniques is needed for the computational complexity of cyber crimes. This paper presents an outline and a review of application of AI in cyber security. Many methods of AI are implemented in cyber security such as security expert systems, search and some bio-inspired techniques. The integration of artificial intelligence with cyber security as proven to work more efficiently.

DOI: https://doi.org/10.54216/JCHCI.020202

Received: October29, 2021 Accepted: March21, 2022

References

[1] SomuVelgekar, HarshKhandve, RajeshwariGundla:"Survey of Artificial Intelligence Applications in Cyber security" , Volume10, Issue 5, May 2021.

[2] Dr.SunilBhutada, PreetiBhutada, "Applications of Artificial Intelligence in Cyber Security" (Volume5, Issue4, April 2018).

[3] JiagengChen, Chunhua Su and ZhengYan."AI-Driven Cyber Security Analytics and Privacy Protection", Hindawi Security and Communication Networks Volume 2019.

[4] YaoJun, Alisa Craig, Wasswa Shafik, and LuleSharif: "Artificial Intelligence Application in Cyber security and Cyber defense ",Hindawi Wireless Communications and Mobile Computing Volume 2021.

[5] IsaacWiafe, FelixNtiKoranteng, EmmanuelNyarkoObeng, NanaAssyne, AbigailWiafe, and StephenR.Gulliver: "Artificial Intelligence for Cyber security: A Systematic Mapping of Literature" , July 30, 2020.

[6] X.Chenetal. ,"Artificial intelligence-empowered path selection: A survey of ant colony optimization for static and mobile sensor networks, "IEEE Access, vol.8, pp.71497–71511, 2020, doi:10.1109/ACCESS.2020.2984329.

[7] FengTao, MuhammadShoaibAkhtar and ZhangJiayuan: "The future of Artificial Intelligence in Cyber security: A Comprehensive Survey"(07July2021)

[8] [8].Jian-huaLI: "Cyber security meets artificial intelligence: a survey", Dec.24, 2018.

[9] Harini MRajan, DharaniS "Artificial Intelligence in Cyber Security-An Investigation" Int. Res. J. Computer Science, Issue, vol.09, no.4, pp.28–30, 2017.

[10] B.Christain, D.A.Elizondo and T.Watson, ―Application of artificial neural networks and related techniques to intrusion detection‖,World Congress on Computation Intelligence, pp.949-954, 2010.

[11] I.H.Sarker, Y.B.Abushark, F.Alsolami, and A.I.Khan, "IntruD Tree: A machine learning based cyber security intrusion detection model,"Symmetry (Basel). vol. 12, no. 5, pp.1–15, 2020, doi:10.3390/SYM12050754.

[12] Shidawa BabaAtiku, AchiUnimkeAaron, GotengKuwunidiJob, FatimaShittu, and IsmailZahraddeenYakubu: "Survey on the Applications of Artificial Intelligence in Cyber Security", international journal of scientific & technology research volume 9, issue10, October 2020.

[13] Syarif A R, Gata W, 2017 .Intrusion detection system using hybrid binary PSO and K-nearest neighbourhood algorithm. 11th International Conference on Information & Communication Technology and System.

[14] BinnyNaik1·AshirMehta1·HiteshriYagnik2·MananShah3:"The impacts of artificial intelligence techniques in augmentation of cyber security: a comprehensive review", 3 August 2021

[15] P. Kavitha , R. Subha Shini , R. Priya, "An Implementation Of Statistical Feature Algorithms For The Detection Of Brain Tumor", Journal of Cognitive Human-Computer Interaction, 2021, DOI: https://doi.org/10.54216/JCHCI.010202.

[16] Sonia Jenifer Rayen, "Survey On Smart Cane For Visually Impaired Using IOT", Journal of Cognitive Human-Computer Interaction, 2021, DOI: https://doi.org/10.54216/JCHCI.010205.

[17] Ajith Krishna R , Ankit Kumar , Vijay K, " An Automated Optimize Utilization of Water and Crop Monitoring in Agriculture Using IoT", Journal of Cognitive Human-Computer Interaction, 2021, https://doi.org/10.54216/JCHCI.010105.

[18] Ashok Kumar M , Abirami A , Sindhu P , Ashok Kumar V D , Rani V, " Modern Medical Innovation on the Preferred Information about the Medicine using AI Technique", Journal of Cognitive Human-Computer Interaction, 2021, https://doi.org/10.54216/JCHCI.010102.

Received: October29, 2021 Accepted: March21, 2022