International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 3380–3388

Securing Artificial Intelligence Applications using Protector Hiding

Garima Jain

Noida Institute of Engineering and Technology
garimajain@niet.co.in

Abstract

Artificial Intelligence (AI) has a vast extent of advancement, and re-searchers are continuously working on the development scope of AI instruments. AI is associated with the existing research and has the area of the incoming research topics. As the name AI suggests, some intelligence, insight appeared by the machines to work as people and work on accomplishing the objectives they are being furnished. Another utilization of AI could be to provide safeguards against the present day's cyber threats. AI explains some intelligence theoreti-cally, but inside the implementation, it too contains a lot of code that must be secure from intruders. AI has a lot of potential for making the world a better, wiser place, but it also poses many secu-rity dangers. Attackers can alter the inference results in ways that lead to misjudgment due to a lack of security awareness during the early development of AI systems. Security concerns can be disas-trous in vital domains such as healthcare, transportation, and sur-veillance. Successful attacks on AI systems can lead to property damage or put people's lives at risk. We must protect the technolo-gies used to implement the AI code. Several types of research have been done, like a default defense system, etc., but that system is still not so secure. The authors of this paper propose a term called "Pro-tector Hiding" as an alternative for securing Artificial Intelligence.

Keywords: Cyber Security, Artificial intelligence, Protector hiding, Robotics, Deep Neural Network, IoT, UAV.

1. Introduction

AI is at present being alluded to as what's to come. It is because this future is vast and has a ton of extensions to improve day by day lives of individuals. Artificial intelligence is the knowledge that is the need of great importance [1]. The calculations that existed are beginning to evaporate. It's because of the continuous improvement in innovation. The headways in applications do not have the option to run up on those current calculations or work wastefully. Artificial reasoning can be a distinct advantage for such issues. They are instructing the machine itself to make answers for the problems related to applications [2]. The intelligence itself needs calculations to work and having the option to help this point of view. Thus, rather than working independently on estimates for special applications, individuals have been working to make the machines solid by furnishing them with the knowledge, permitting them to become like that of a human cerebrum.

In theoretical analyses and actual AI deployments, there are security issues associated with AI. For example, attackers can modify files to get through AI-based detection techniques or add noise to home automation and voice recognition commands to launch malicious software. Attackers can also interfere with terminal data or indulge in adversarial discussions with a chat robot to induce a predicted mistake in the core AI system [3-6]. It's important to incorporate small tags on road signs or automobiles that lead robotic vehicles to make incorrect judgments. Since intelligence is consistently defenseless against being ruined by the avarice of others or self, and it represents a significant risk to the world. History expresses that numerous astute have prompted a few

ISSN: 2233-7857 IJFGCN

fiascos. Thus, Artificial Intelligence would itself be able to be a hotspot for issues. These weaknesses may bring about hurting others. It can result from working oppositely than it is intended to be. It can bring about information burglaries, protection attacks, executing them if there should be robots. The vulnerabilities may occur because of the self-defilement of the insight, or it very well may be controlled by the Black Hats. It is imperative to bring down these weaknesses to make sure about our future in solid insight.

Big data, computational power, and deep learning algorithms have opened a new era of development fueled by AI. Humans have yet to produce intelligent computers with sentient intelligence, even though AI aims to "examine the essence of intelligence." As a result, AI is still in its early stages, primarily in three areas: First, there is still in AI research and application [7]. Despite advances in the field of dedicated AI, dedicated intelligence tends to be weak AI, deficient in autonomy, and hence unable to accomplish conceptual abstraction, inference decision-making, or problem-solving fully. Artificial general intelligence (AGI), sometimes known as "strong AI" or "humanlike machine intelligence," is a self-aware AI capable of reaching human levels of brightness and adapting to external environmental difficulties [8]. The human brain, for example, is a general-purpose intelligent machine that can learn by analogy and master via extensive study. It can look, observe, evaluate, explain, analyze, plan, organize and build for diverse issues.

AI found as the potential future the authors are anticipating for some time. Improvement in AI has just brought forth a lot of practical applications. These applications are improving and making our lives simpler step by step [9-11]. Simulated intelligence is advancing now, and the authors have no thought what statures it can reach. Artificial intelligence being a potential resource in itself, may, in general, be a risk whenever abused. It should be improved the artificial intelligence's security systems, too, with time since the Blackcaps are likewise advancing presently. They are searching for better approaches to penetrate AI to get to its applications and degenerate them. Present guarded measures are very acceptable at holding AI's trustworthiness. Be that as it may, they may get obsolete very soon, and improving them with form updates probably won't sufficiently be. Endless supply of the applications is should a test that is by and large ceaselessly influencing the development. It is ideal for working upon another style of conservative measures to secure AI just as its applications [12].

2. Background

As, AI is a new technology, its governance goes both ways. The strict oversight of artificial intelligence is not recommended, particularly at the current application level. On the other hand, it is critical to investigate the impact of AI on human civilization in numerous domains and begin gradually putting in place regulatory frameworks. As a result, we can build the best AI application practices and look forward to a better future with artificial intelligence.

The author of [13] analyzed a cross-section of security risks and defensive approaches at various phases of machine learning from a data-driven perspective; however, their evaluation did not address existing attacks on reinforcement learning. They also present a systematic methodology for demonstrating attack tactics against AI applications and assessing numerous cyber defenses to prevent AI applications from such attacks [15]. They also stress the need to comprehend hostile aims and capabilities, particularly in light of recent attacks on industry applications, to create adaptive defenses to safeguard AI systems [16]. Finally, we go over the significant difficulties and future studies paths in AI security and privacy.

We hold debates about artificial intelligence privacy, security, and ethnicity issues, as well as potential hazards and threats [17]. Countermeasures in research,

ISSN: 2233-7857 IJFGCN

legislation, and supervision are offered, as well as our expectations for the growth of artificial intelligence [18]. This paper focuses on a critical discussion about how to best leverage Artificial Intelligence's potential in the context of cybersecurity [19]. Artificial intelligence techniques are increasingly being applied in cybersecurity, particularly detecting and preventing cybercrime [20]. This research aims to show signs of progress in using artificial intelligence (AI) techniques in cybersecurity, particularly in cybercrime, and to open up possibilities for future research. De Silva et al. (2019) investigated the possible threats posed by CPSs and AI-based workplace automation and brought together the most recent breakthroughs in industrial computing and artificial intelligence [21]. The concept of a medical CPS introduces as a study case for the technological fields of machine intelligence in health care [22]. A complete list of the most frequently utilized computation techniques and algorithms had collected. The Idea of a healthcare CPS has come to light as a case study for the technological fields of machine intelligence in health care [23].

3. AI Applications

The uses of AI are numbering up step by step. The current applications came into existence to get together the present requirements and for endurance. AI techniques such as image identification, voice recognition, and speech recognition have grown widespread due to massive data accumulation, dramatic gains in computer power, and ongoing innovation in ML methodologies [24]. Artificial intelligence is being a vital factor in the headway of uses and concocting new advancements. Novel thoughts introduce each day, and many are being proposed and started. Below are a few examples of such applications: -

2.1 Robotics

Artificial intelligence is helping in building practical robots. Robots have shown their existence for quite a while, and they have progressed a great deal. The impetus in this progression would be AI since AI empowers the robots to act more human-like while performing errands. Different robots have come into existence in fields, such as Medical, to assist specialists with troublesome medical procedures.

2.2 Deep Neural Network

A machine's acknowledgment capacities are getting exact nowadays. It has likewise been conceivable on account of the AI. Computer-based intelligence has built up the DNN's so much that the machines have the option to perceive an item, living being precisely. It has demonstrated to perceive protests in a way that is better than an unaided eye in specific situations. Deep learning is a branch of machine learning that uses deep artificial neural networks to learn [25]. Because a feature engineer must find meaningful qualities from the input data, the machine learning techniques covered thus far in this section are known as Deep Learning. There are numerous variations of sensing measures. One such technique is the Random pixel determination and afterward producing the picture around it.

2.3 Medical

As of late, there have been numerous instances of disappointments at medical procedures. These disappointments have called attention to the requirement for improved careful frameworks. Artificial intelligence has given a choice to lessen these disappointments. It has brought about training machines to go about as assistance to specialists. It can aid medical workers in making diagnoses, improving patient compliance, and reducing the risk of neurologic disease and hospital admissions. In rural locations and many underdeveloped countries, such a

ISSN: 2233-7857 IJFGCN

technology can help doctors make decisions on behalf of specialists, which are rare resources [26]. Simulated Intelligence Applications, popularly known as robots, are used ideally to play out a portion of troublesome tasks. They make their presence in the field. Additionally, it has just begun demonstrating positive outcomes.

2.4 IoT

AI in IoT empowers clients to control their applications no sweat, giving them a straightforward interface to connect on. Computer-based intelligence has assigned all the applications to speak with one another and comprehend the human orders all the more unmistakably to play out their undertakings with a precision satisfying their clients [27]. Simulated intelligence has additionally received information digging for better working with IoT applications.

2.5 UAV

Automated Vehicles have given the world to investigate regions that are unavailable or risky to humanity. UAV's have been used for quite a while, whether from the military side or by researchers to study. The new UAV defines scrambling by Artificial Intelligence to get to the new areas without breaking a sweat and working effectively. Artificial intelligence can work the UAV's likewise to those as people, possibly more proficiently.

2.6 Training Programs

Artificial intelligence has made it conceivable to furnish us with increased reality and assist people with planning conditions and difficulties without really entering them. It reproduces the ideal circumstance with the gathered information and helps us encounter the case previously, so the authors prepare to confront it appropriately.

2.7 Cognitive approach

At last, Artificial Intelligence has started to copy the human upgrades to a stunning extent. It hasn't had the option to imitate human advancements totally, yet what has been as of now came to have given a decent chance in contrast to critical thinking. It is done by recording the human improvements and attempting to combine it with the AI by changing the registered information into calculations thus. These calculations have brought about honing the knowledge and permit the AI to perform effectively in numerous situations.

4. Cyber Security using AI

Author The authors regularly seem to be Artificial Intelligence being supposed to be what's to come. In any case, the inquiry is the reason to be view as what's to come. The basic answer would result from its vast space to develop itself and improve the world's innovation [28]. The authors have just observed a portion of the utilization of the AI above. Those applications are themselves the verification of the viability of AI. AI has offered life to numerous applications. It wouldn't be a mix-up to consider that AI can be actualized with all the fixings since it genuinely can be executed with all the fixings.

In addition, it is imperative to keep this future splendid and keep it from trans-forming into murkiness. These applications are available to weaknesses that can be abused by the Black Hats to control the working of its applications or to use them for voracity. Simulated intelligence needs to have a solid safeguard frame-work only not to ensure the applications being constrained by it however to se-cure its insight also from undermining and prompting debacles.

ISSN: 2233-7857 IJFGCN

Cyber Security has been genuinely improving with the usage of AI in its cy-cles. Artificial intelligence learns the assaulting component acquired by the Black Hats. In the wake of learning the instrument, it races to distinguish the weaknesses utilized by the programmers to abuse the frameworks. On the off chance that the failings are distinguished, they shut them before using. The AI searches for the comparable assaulting designs utilized previously on the off chance that weaknesses are not distinguished if the insight recognizes such an example, the countermeasures to dispose of the attack.

AI has the option to diminish Fraud, Scams, Phishing, Data Thefts for an immense scope. It has been talked about in different researches to improve spaces of network protection. One such study is actualized, which tries to perceive the vindictive conduct with the assistance of neural organizations and afterward execute the countermeasures. In general, these pernicious conducts are more likely to happen in frameworks working on Windows because of the enormous region of weaknesses. AI's other idea for improving security previously discussed in past meetings is recognizing Low-rate circulated for swearing administration utilizing TCP association boundaries at the application layer. Fig 1 depicts one such malicious behavior system: -

Fig 1. Malware System Behavior Architecture

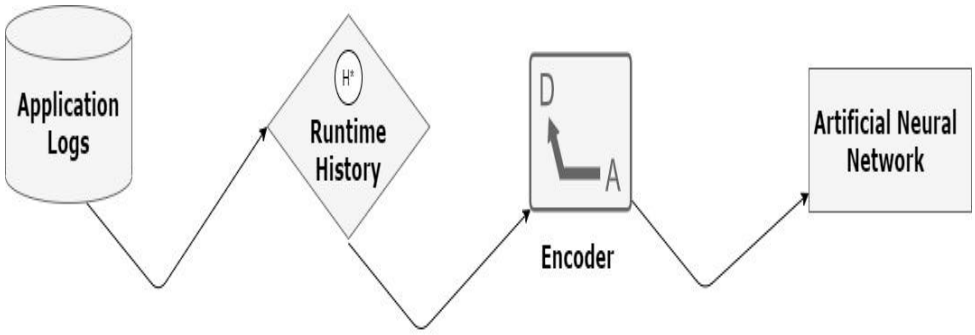

Figure 1. Malware System Behavior Architecture

LDDoS attacks are prone to be covert and hard to distinguish. The current methods used to identify LDDoS haven't been powerful [29]. Along these lines, it is well defined to determine the LDDoS assaults by considering the attributes of TCP to be the key differentiator. The proposition's test was noteworthy.

4.1. Issue with the Application Security

The programmers may use DDoS or other techniques related to hacking to make it look as if the objective is being attacked by penetrating the AI-first. However, this is a ploy to keep the AI's computations busy sending countermeasures for itself rather than keeping a watch on applications that introduce to support the system.

ISSN: 2233-7857 IJFGCN

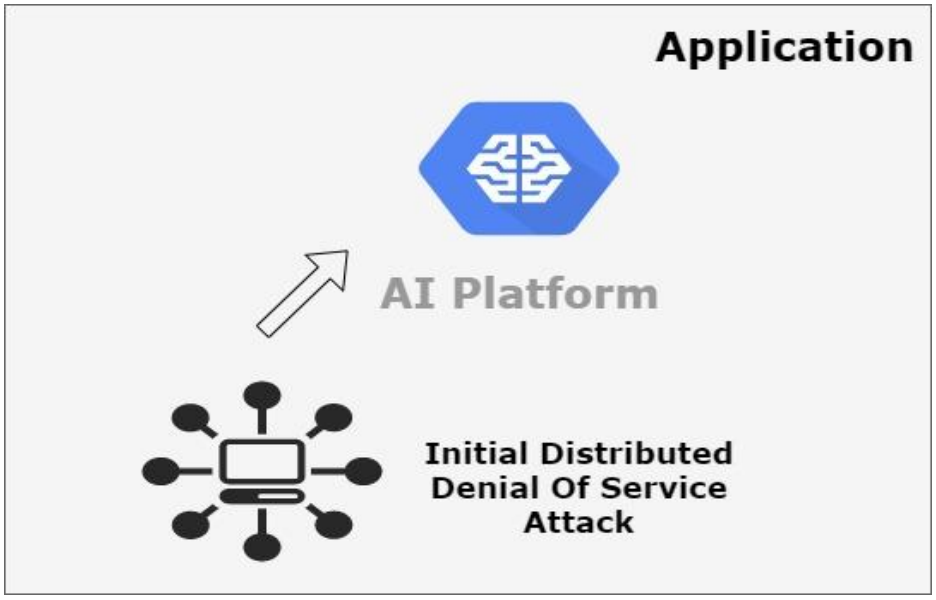

Figure 2. Misleading AI and generating vulnerability

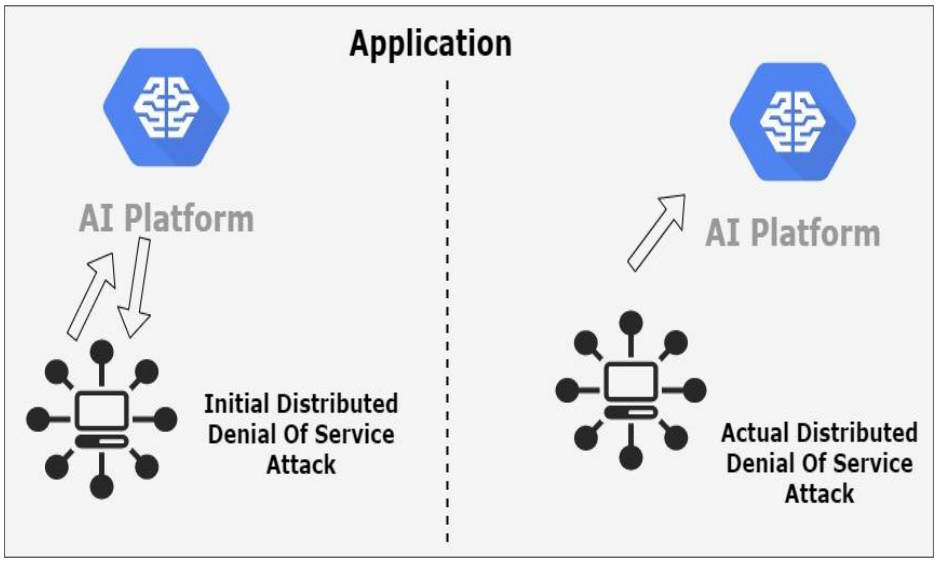

Figure 3. Misleading AI and generating vulnerability

5. The Proposed Solution

The authors might want to propose a thought as an option for such issues. The authors have named the accompanying proposition as "Protector Hiding" A choice to determine such problems could be building up another AI next to each other with a center AI for the application. In this manner, the authors can limit the center AI's multifaceted nature to give security to itself. The center AI's target is protecting from assaults just to its application. Presently, this way, the center AI is helpless against defilement just as control. Here's the point at which the new AI comes helpful.

The other AI's sole reason is to give security to center AI too to itself. This AI will go about as the watchman whose performance task is to ensure itself and other people. This gatekeeper AI makes a connection to the center AI through covering to provide its source stays untraceable. Thus, regardless of whether the Blackcaps

ISSN: 2233-7857 IJFGCN

needs to penetrate the center AI, they will initially have to invade the gatekeeper AI, which would be extremely troublesome as covering would monitor its source, henceforth continually misleading the programmers to discover its weaknesses.

The issue that surfaces with this proposition are that the two AIs contact an organization so that the veiling can happen constantly. To conquer this issue, the authors as a whole would have to come up and cooperate to discover its answer. By joining the entirety of our insight, we won't have the option to reinforce this thought yet. In addition, they may have the chance to concoct much better and solid alternatives to see this issue just like the others.

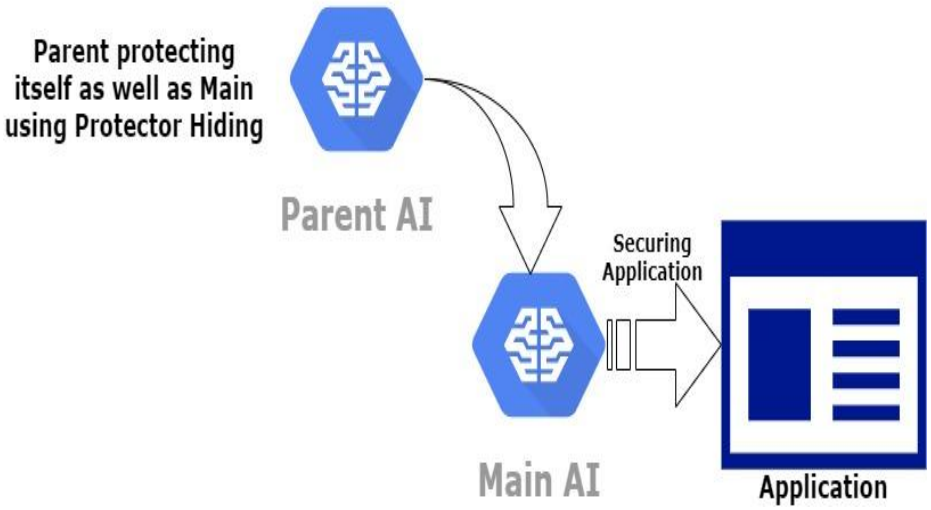

Figure 4. Proposed Idea

6. Conclusion

AI's blossoming itself carries risks to its honesty, as the programmers regularly will, in general, enter into things improving human existence. It's a significant worry to keep up its uprightness and secure it, to dodge any perils. Its applications are huge in numbers, and a lot more are coming step by step to help better our lives. Computer-based intelligence is likewise answerable for giving security in numerous fields nowadays, ensuring our information, personality, and work. A little control in the calculations could prompt debasement of AI, which is perilous and may bring about extraordinary occasions. Henceforth, it requires a need to work upon its prudent measures to stabilize and keep up its uprightness.

There's a need to concoct new methods and instruments to make sure about AI and our information. Gatekeeper Masking is so far an idea that may be a steadily achievable goal for the time. The view can't be executed immediately and should be used to touch more before pushing forward with it.

7. Future work

Our plans include the usage of Protector Hiding appropriately. As of now, it’s just an idea that requires a lot of changes before being brought right into it. In the future, we will not simply work after advancing Protector Hiding yet also invest energy in social affairs more data about the openings in safety efforts to create something steadier.

ISSN: 2233-7857 IJFGCN

References

1. D. Lily Chan, B. and Wang, T. G. (2013). “A Simple Explanation of Neural Network in Artificial Intelligence”, IEEE. Trans on Comtrol System, vol. 247, pp. 1529–5651.
2. Yuriy V. Lonchakov, Boris I. Kryuchkov, Andrey A. Kuritsyn, Valeriy A. Sivolap, Petr A. Saburov and Igor G. Sokhin, "New approaches to cosmonaut training of the program of scientific - applied research and experiments aboard the ISS Russian segment", IAC Paper IAC-15, pp. 1995-6258.
3. Dr. Mohammed Abdul Kashem, Mohammad Naderuzzaman: On An Enhanced Pairwise Search Approach for Generating Optimum Number of Test Data and Reduce Execution Time. Computer Engineering and Intelligent Systems http://www.iiste.org ISSN 2222–1719 (Paper) ISSN 2222–2863 (Online) Vol. 4, No.1, 2013.
4. Corder Gregory W., DaleI. Foreman Nonparametric Statistics: A Step-by Step Approach (2nd eds), John Wiley & Sons (2014).
5. Yang Liu, and Pinpin Tang, The prospect for the application of the surgical navigation system based on artificial intelligence and augmented reality, 17 January 2019, https://ieeexplore.ieee.org/document/8613675.
6. Sagar B.S, Niranjan S, Nitin Kashyap, and Sachin D.N, Providing Cyber Security using Artificial Intelligence – A survey, 29 August 2019, https://ieeexplore.ieee.org/document/8819719.
7. Harini M Rajan, "Artificial Intelligence in Cyber Security-An Investigation", Int. Res. J. Comput. Sci. Issue, vol. 09, no. 4, pp. 28-30, 2017.
8. Alberto Perez Veiga, "Application of Artificial Intelligence (AI) to Network Security", ITEC 625 – Information Systems Infrastructure, 2018.
9. Enn Tyugu, "Artificial Intelligence in Cyber Defense", 3rd International Conference on Cyber Conflict.
10. Anna L. Buczk and Erhen Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection", IEEE Commun. Surv. Tutorials, vol. 18, no. 2, pp. 1153-1176, 2016.
11. Michael Siracusano, Stavros Shiaeles, and Bogdan Ghita, Detection of LDDoS Attacks Based on TCP Connection Parameters, 7 February 2019, https://ieeexplore.ieee.org/document/8635701.
12. E. Adi, Z. Baig and P. Hingston, "Stealthy Denial of Service (DoS) attack modelling and detection for HTTP/2 services", Journal of Network and Computer Applications, vol. 91, pp. 1-13, August 2017.
13. H. Alshamrani and B. Ghita, "IP prefix hijack detection using BGP connectivity monitoring", 2016 IEEE 17th International Conference on High Performance Switching and Routing (HPSR) Yokohama, pp. 35-41, 2016.
14. RONALD C. ARKIN, Ethical Robots in Warfare, 16 March 2019, https://ieeexplore.ieee.org/document/4799405.
15. Hu Shuijing, The Influence of Artificial Intelligence Development on Patent Legislation, 22 August 2019, https://ieeexplore.ieee.org/document/8806576
16. Oseni, Ayodeji, Nour Moustafa, Helge Janicke, Peng Liu, Zahir Tari, and Athanasios Vasilakos. "Security and Privacy for Artificial Intelligence: Opportunities and Challenges." arXiv preprint arXiv:2102.04661 (2021).\
17. Radu, R. (2021). Steering the governance of artificial intelligence: national strategies in perspective. Policy and society.
18. Noor, Arshil, Tabrez Nafis, Samar Wazir, and Mohammad Sarfraz. "Impact Of Artificial Intelligence In Robust & Secure Cybersecurity Systems: A Review." Available at SSRN 3834207 (2021).
19. Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things, 1(1), 1-14.
20. Romancheva, N. I. "Duality of artificial intelligence technologies in assessing cyber security risk." In IOP Conference Series: Materials Science and Engineering, vol. 1069, no. 1, p. 012004. IOP Publishing, 2021.

ISSN: 2233-7857 IJFGCN

21. Cotton, A. (2021). Identification of Manual Cybersecurity Tasks for Artificial Intelligence Automation Conversion: A Qualitative Study (Doctoral dissertation, Colorado Technical University).
22. Racovita, Monica. "Industry Briefing Cybersecurity for the Internet of Things and Artificial Intelligence in the AgriTech Sector."
23. Akinsola, Jide Ebenezer Taiwo, Samuel Akinseinde, Olamide Kalesanwo, Moruf Adeagbo, Kayode Oladapo, Ayomikun Awoseyi, and Funmilayo Kasali. "Application of Artificial Intelligence in User Interfaces Design for Cyber Security Threat Modeling." In Intelligent User Interfaces. IntechOpen, 2021.
24. Leenen, L., & Meyer, T. (2021). Artificial intelligence and big data analytics in support of cyber defense. In Research Anthology on Artificial Intelligence Applications in Security (pp. 1738-1753). IGI Global.
25. Alhayani, Bilal, Husam Jasim Mohammed, Ibrahim Zeghaiton Chaloob, and Jehan Saleh Ahmed. "Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry." Materials Today: Proceedings (2021).
26. Bistron, M. and Piotrowski, Z., 2021. Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens. Electronics, 10(7), p.871.
27. Fischer, Sophie- Charlotte, and Andreas Wenger. "Artificial Intelligence, Forward- Looking Governance and the Future of Security." Swiss Political Science Review 27, no. 1 (2021): 170-179.
28. Mohanty, Sachi Nandan, Sirisha Potluri, V. Bhanu Prakash, B. Srinath, and B. Manjunath. "Cloud Security Concepts, Threats and Solutions: Artificial Intelligence Based Approach." In Cloud Security, pp. 1-20. De Gruyter, 2021.
29. Jain, H., Vikram, A., Kashyap, A., & Jain, A. (2020, July). Weapon detection using artificial intelligence and deep learning for security applications. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 193-198). IEEE.
30. Lv, Zhihan, Dongliang Chen, Ranran Lou, and Ammar Alazab. "Artificial intelligence for securing industrial-based cyber–physical systems." Future generation computer systems 117 (2021): 291-298.

Authors

Garima Jain was born on November 3, 1992. She has received her M.Tech. degree from Galgotias College of Engineering, in 2017. Presently she is working in Noida Institute of Engineering and Technology, Greater Noida. She has 4 years of academic's experience. She has also worked with industry. She has good understanding of emerging technologies like R Language, Python, Blockchain, SQLite. She is also a NAAC coordinator. She also attended more than 40 Faculty Development Programme from recognized organizations like IIT Bombay, IIT Roorkee, DTU Delhi on Machine Learning, python, IoT and many more. She has also attended more than 50 workshops, seminar, and webinars from reputed association like IEEE, Elsevier, and NIT's. She has also published various Book chapters, Research Papers in National & International Conference and Journals including Scopus and other reputed journals. She is also awarded with a Best paper Presentation Award in year 2017. She has also got a merit certificate for Ideal innovation idea presentation at National Level. She also participated equality in gender awareness program in university and activity participated along with student in outreach extension activity.

ISSN: 2233-7857 IJFGCN