Webology, Volume 18, Number 4, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I4/150

Usability of Artificial Intelligence in Cyber Security

Noor Mohd[1], Rajat Bahuguna[1], Deepak Upadhyay[2]

[1]Department of Computer Science & Engineering Graphic Era Deemed to be University,
Dehradun, Uttarakhand, India
[2]Department of Computer Science & Engineering, Graphic Era Hill University, Dehradun,
Uttarakhand India, 248002

ABSTRACT

The Internet of Things is getting increasingly intelligent and sophisticated. The use of smart devices is rapidly expanding. Artificial intelligence and machine learning are being integrated into IoT applications, resulting in competitive benefits such as increased operational productivity. Large businesses have been purchasing smaller start-ups that have been working at the intersection of artificial intelligence and the Internet of Things over the past decade. In addition, leading IoT service providers are increasingly offering advanced AI features including machine-based learning analytics. We evaluated various papers relevant to the application of artificial intelligence in cyber-security in this report.

Keywords: Cyber security, IDS, IoT, AI, ML

INTRODUCTION

The Internet of Things (IoT) has rapidly evolved since its introduction in 2008 [1] and is now a widespread fixture in many homes and businesses as well as a crucial aspect of daily life. The definition of the Internet of Things (IoT) is difficult because it has evolved since its inception. It is best described as a network of computers, automated and basic machines, and unique identities (UIDs) that may share information without requiring human connection [2]. This often involves a person interacting with a central hub point device or application, which in turn transmits information and instructions to at least one outside IoT device [3]. In the extremely odd event that it's necessary, peripheral devices can perform actions and transmit data back to the hub device or application, which a person can see. The Internet of Things (IoT) concept has improved the world's openness, accessibility, flexibility, mystery, and interoperability in terms of device networks [4]. IoTs, on the other hand, are defenceless against attacks due to a combination of numerous attack surfaces and their novelty, resulting in a lack of safety principles and safeguards [5]. Depending on the system component they are targeting and what they hope to obtain, attackers can employ a wide range of assaults on IoTs. As a result, there has been substantial research on cybersecurity in relation to IoT. This integrates AI techniques for protecting IoT devices from intruders, typically by spotting strange movement that could suggest an attack [6]. Cybercriminals, however, always have the upper hand when it comes to IoT because they only need to uncover one weakness whereas cybersecurity experts must safeguard a number of goals. Therefore, cybercriminals are increasingly using AI to get around complex computations that spot unusual behavior and make it go undetected [7]. As IoT innovation has increased, AI has attracted a lot of interest. This increase has led to the usage of simulated intelligence innovations like as decision trees, straight relapse, AI, SVM, and neural networks in IoT cybersecurity applications to identify threats and potential attacks. IDS discussed this in [23, 24].

literature survey

In this particular section we have done some recent literature survey based on role of AI in IoT cybersecurity. Authors in [8] thinks about IoT innovations as far as uprightness, obscurity, secrecy, protection, access control, verification, approval, strength, and self-association, just as gives a nitty gritty investigation of the security concerns related with IoT applications and reasonable countermeasures. The authors use the CICIDS2017 datasets, which have a high exactness of 97.16 percent, to provide Deep learning models for DDoS assaults detection in IoT (Internet of Things) network defense [9]. The authors of [10] test ANN in a gateway device to check whether they can recognize inconsistencies in information came from edge gadgets. The discoveries show that the proposed strategy can build IoT framework security. In [11], the authors present an Artificial Intelligence -based control procedure for identifying and assessing digital attacks in modern IoT frameworks, just as making up for them. The authors in [12], construct various antagonistic procedures and protection components against them and test their strategy utilizing datasets like as MNIST, CIFAR-10, and SVHN to offer a hearty omnipresent identification for IoT Environments. Because IoT devices are increasingly being incorporated into digital actual frameworks, the authors of [13] analyses the new development of AI dynamic in these frameworks and predict that this advancement is almost self-governing. They also predict that the value of AI dynamic due to its speed and effectiveness in handling a lot of information will more than likely make this development inevitable. Authors in [14] examines imaginative procedures to chance examination dependent on AI and AI, with an emphasis on IoT networks in mechanical settings. At last, [15] addresses strategies for gathering and examining online protection dangers to IoT gadgets to normalize such techniques so that danger in IoT frameworks might be perceived and relieved all the more viably. In this report I have covered an assortment of points identified with network protection, the IoT, and AI, just as how they all identify with each other. It's anything but a thorough survey of cyberattacks against IoT devices and prescribes AI-based strategies to ensure against these attacks.

different methods to attack iot devices

There are various flaws in IoT devices security, hackers now a days have got variety of methods to hack IoT devices using various attack surfaces. IoT devices uses Hardware and software both which itself makes it vulnerable attackers can attack IoT devices either using hardware or through software of IoT device. Few methods have been discussed below for attacking IoT devices

Physical Attacks

Physical attacks are a low-tech type of attack where the objective gadget's equipment is used to the attacker's benefit here and there. Physical attacks can take an assortment of structures. Attacks that disrupt the organisation to which the devices are connected through blackouts; real harm in which the devices or their components are damaged to prevent authorised use; Article sticking, in which sign sticking is used to prevent appropriate use, and malicious code infusion, in which a hacker embeds a USB containing an infection into the target device. In this paper, persistent denial of service (PDoS) attacks are discussed. For instance, if an IoT gadget is connected to a high voltage power source, its force supply may become overwhelmed and require replacement [16].

Initial Reconnaissance

Prior to endeavoring a cyberattack on an IoT gadget, IoT attackers would habitually look at it for shortcomings. This is much of the time achieved by buying an imitation of the IoT contraption they need from the market. From that point forward, they figure out the gadget to develop a testing attack to figure out what yields could be gained and which attack choices are accessible. Opening up the gadget and considering the inside equipment like the glimmer memory to find out about the product, and meddling with the microcontroller to discover touchy data or trigger unforeseen conduct are two instances of this [17]. To prevent detection, equipment-based security is necessary for IoT devices. Because the application processor contains sensors, actuators, force, and correspondence, it must be situated in a secure environment [17]. Equipment-based security, in which the gadget can verify its authenticity to the worker to which it is connected, can also be used to cultivate device verification.

Man in middle

The Man-in-the-Middle (MITM) attack is perhaps the most well-known IoT attacks. A MITM attack, with regards to PCs, captures correspondence between two hubs and permits the attacker to go about as an intermediary. MITM attacks might be utilized on an assortment of associations, including a PC and a switch, two mobile phones, and, frequently, a worker and a customer. On account of the Internet of Things, the attacker for the most part executes MITM attacks between the IoT gadget and the application with which it-imparts. Particularly vulnerable to MITM attacks are IoT devices since they require standard executions to defend against them. The two types of MITM attacks that occur the most frequently are cloud surveying and direct association. The smart home device often communicates with the cloud during cloud surveying, primarily to check for firmware updates. Attackers can reroute network data via the Address Resolution Protocol (ARP) or DNS settings, or they can intercept HTTPS traffic by using self-signed certificates or tools like the (Secure Sockets Layer) SSL strip [18].

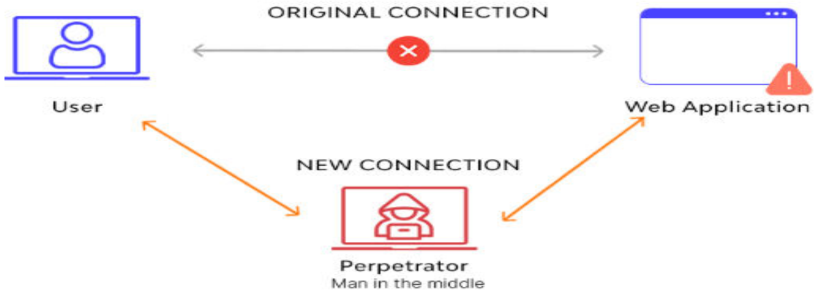

Figure 1. Representation of MITM attack

Botnets

A well-known hazard posed by IoT devices is the large-scale assemblage of equipment used to build botnets and conduct DDoS attacks. This is achieved by mixing attacks from different sources into a DDoS onslaught. The term "denial of service" (DoS) assault refers to a planned attempt to thwart authorised use of a service. DDoS assaults try to overwhelm the infrastructure supporting the objective aid and stop the normal information flow. To launch DDoS assaults on the target, the hacker searches for unprotected or insecure equipment. Attacking vulnerable machines and introducing infectious code are aspects of misuse and disease. The hacker searches for vulnerable computers, finds out which ones are online, and then schedules when to attack those computers [22]. IoT devices are arguably the most well-known ways to obtain compromised PCs and carry out DDoS assaults because to their widespread accessibility and frequently inadequate security and maintenance.

Denial of service attacks (DDoS)

DoS attacks are much of the time completed by IoT gadgets, yet they are additionally powerless against them. Lasting refusal of administration (PDoS) attacks, which leave a gadget or framework completely unusable, are especially defenseless against IoT gadgets. Overburdening the battery or force frameworks, or, all the more usually, firmware attacks, can be utilized to achieve this. In a firmware attack, the attacker abuses defects in a gadget's major programming (regularly its working framework) to supplant it with a harmed or flawed rendition, making it unusable [16]. At the point when a gadget gets phlashed, the proprietor must choose the option to streak it with a new duplicate of the working framework and any substance that may have been introduced. When done lawfully, this technique is known as blazing, and when done illicitly, it is known as "phlashing." Phlashing can make harmed programming exhaust the equipment, making recuperation incomprehensible except if the telephone is totally supplanted [16]. Attacks against the gadget's force supply, but less notable, might be significantly more ruinous. A USB gadget which contains virus put away on it that, when embedded into a PC, attacks the gadget's capacity to the point that the gadget's equipment is totally harmed and should be supplanted is an illustration of this kind of attack [16]. For instance, BrickerBot is a type of PDoS malware. PDoS malware known as BrickerBot uses the force structure of a USB device to fully destroy the electronics of the target device and compel a replacement. The devastation caused by this attack often involves replacing or installing all of the equipment. Later, IoT engineers should make sure that their solutions have robust defenses against these dangers. Customers wouldn't mistakenly buy unsafe devices if IoT security guidelines were widely disseminated.

Artificial intelligence in cyber security

Many cybersecurity professionals are looking at artificial intelligence as a means to dynamically protect systems against threats (AI). The most common application of artificial intelligence (AI) in cybersecurity is intrusion detection, which entails analysing traffic patterns and searching for activity that could be an indication of an attack.

Using ML

Supervised learning and unsupervised learning are the two subcategories of machine learning. People physically distinguish between obtaining information that is dangerous or true, and they then feed that knowledge into the algorithm to build a model with "classes" of information that it compares to when evaluating the traffic it is currently observing. Unsupervised learning avoids the use of pre-processing information and manual naming for classifying almost identical pieces of information based on their clarity within each class and their specificity between classes [19]. The Bayesian theorem, which attempts to classify information dependent on the Bayesian theorem, where atypical practices are totally accepted to come from unmistakable events as opposed to a solitary attack, is one normal AI method for network safety. Nave Bayes is a supervised learning calculation that examinations each activity to assess the probability that it is atypical whenever it has been prepared and made its classes [19].

K- Nearest Neighbor

Simply expressed, the k-nearest neighbor (k-NN) approach measures the Euclidean distance between previously ordered bits of information and new pieces to determine which class the new piece should be placed in [19]. Information tests are then used to establish the classes [19]. The k-NN technique is appealing for interruption identification frameworks because it can quickly learn from new traffic examples to identify previously undetected attacks, including zero-day attacks. Network protection analysts are additionally taking a gander at how k-NN may be utilized to recognize cyberattacks continuously [19]. The methodology has been utilized to identify attacks, for example, counterfeit information infusion and works viably when information can be addressed by a model that takes into consideration the estimation of distance to other information, like a Gaussian appropriation or a vector.

ANN

Artificial neural networks (ANNs) are a recent development in technology that model how brain neurons interact and process information when working together. A neuron in an artificial neural network is a mathematical condition that collects data and produces an objective worth. This objective worth is then sent to the succeeding neuron based on its value. The neurons can learn and change their loads by comparing the difference between the normal and prior yield values as the ANN technique intensifies until the yield value is sufficiently within the confines of the objective worth. The calculation then displays a numerical condition that generates a value that can be used to organize the data [19]. When new types of traffic and attacks become commonplace, other numerical models may become out-of-date, however ANNs may update their numerical models when given fresh data [19]. The fact that ANNs evaluate new data more carefully than static numerical models suggests that they are also better at identifying existing obscure and zero-day threats. As a result, ANNs make excellent frameworks for interruption recognition and have proven effective against DoS attacks [19]. Utilizing AI in cybersecurity is a more modest yet quick extending subject right now. It's also expensive and resource-intensive, thus it might not be possible to send AI to protect a small framework. However, businesses with large networks may win from these partnerships, particularly if they are considering or have already implemented IoT devices for their company. With AI cybersecurity, the massive systems found in a smart city would benefit, and the AI would have the opportunity to provide extraordinarily short response times, which are crucial in systems like traffic signals. Later, cybersecurity powered by computer intelligence might be applied to simpler structures like self-driving cars or luxurious homes.

attack on iot device using ai techniques

Cybercriminals have started utilizing destructive AI to help attacks, regularly to keep away from interruption location calculations on account of IoT, or focusing on valuable AI in such a way that the AI neutralizes its own framework.

Vulnerability detection automation

Vulnerability in a framework can be found through AI. While this innovation can assist with peopling looking to protect a framework by cleverly looking for weaknesses that should be fixed, attackers can likewise utilize it to discover and misuse blemishes in their objective framework. As innovation turns out to be all the more broadly utilized, especially those with helpless security necessities, like IoT gadgets, the measure of weaknesses that attackers may misuse, including zero-day weaknesses, has expanded also. Attackers oftentimes use artificial insight (AI) to uncover weaknesses and adventure them far quicker than engineers can fix them. Designers can utilize these identification apparatuses also, yet it ought to be noticed that with regards to getting a framework or gadget, engineers are in a tough spot; they should discover and address each and every expected vulnerability, while attackers just need to discover one, making programmed discovery an important instrument for attackers.

Input attacks

An input attack occurs when an attacker modifies the contribution of a framework for artificial intelligence in a way that causes the artificial intelligence to malfunction or produce false results. Information attacks are carried out by changing the contribution in accordance with an attack design, which can range from adding tape to a real stop sign to confuse autonomous vehicles to adding tiny amounts of commotion to a picture that is invisible to the human eye but can confuse artificial intelligence [20]. Unbelievably, a data assault just needs to change the information that the attacker wants to consider the impact of. It doesn't even need to affect the AI's real calculations or security. The attacker may not have to use innovation in the example of tape on a stop sign. More mind boggling attacks, then again, are totally hidden from the exposed sight, where the attacker adjusts a little space of the picture in a precise way to trick the calculation. Information attacks are oftentimes characterized dependent on where they fall on two tomahawks: detectable quality and configuration.

Fuzzing

Fuzzing is a trying methodology that makes the objective programming crash by creating irregular sources of info (i.e., numbers, burns, metadata, pairs, and particularly "known-to-beperilous" qualities like zero, negative or amazingly enormous numbers, SQL questions, uncommon characters) [21]. There are two kinds of fuzzing: idiotic fuzzing and astute fuzzing. Moronic fuzzing simply creates issues by changing info factors aimlessly; this is fast since changing information factors is clear, however it isn't especially effective at distinguishing abandons since code inclusion is restricted [21]. Keen fuzzing, then again, makes input esteems that are proper for the objective programming relying upon the arrangement and blunder age of the product. This product investigation is useful to brilliant fuzzing on the grounds that it educates the fuzzing calculation about likely issues; by and by, building a powerful savvy fuzzing strategy requires master information and tweaking [21].

Data Poisoning

Data poisoning and input attacks are practically the same, however the objective of data poisoning is to change contributions over a long sufficient timeframe that the AI that investigations information moves and is intrinsically imperfect; accordingly, information harming is generally completed while the AI is as yet being prepared before it is conveyed [20]. As a rule, AI figures out how to fizzle on specific information sources picked by the attacker; for instance, if a military utilizes AI to distinguish airplane, the contradicting military may harm the AI to keep it from perceiving particular sorts of airplane, for example, drones [20]. AIs that are persistently learning and assessing information to make and change expectations, like prescient support frameworks, can be harmed by information harming. To harm an AI, attackers can use one of two different ways.

Dataset Poisoning

The most immediate type of data harming is perhaps injuring an AI's dataset. Since AI derive all of their knowledge from the training datasets that they are given, any errors in those datasets would essentially debase the AI's data. When the goal dataset contains inaccurate or incorrectly labelled information, dataset damaging occurs [20]. Given that AI learns by identifying patterns in datasets, damaged datasets may disturb patterns or give new false instances, which may cause AI to incorrectly identify or recognize inputs [20]. Since numerous information bases are gigantic, finding harmed information inside them can be testing. Utilizing traffic designs for instance, an attacker may change dataset marks so the AI no longer perceives stop signs, or add information and names with the goal that the AI orders a red light as a green light.

Algorithm Poisoning

Algorithm poisoning attacks exploit expected defects in the AI's learning calculation. This sort of attack is very normal in unified realizing, which is a method of preparing AI while keeping a person's information security. Rather than social occasion possibly touchy information from clients and joining it into a solitary dataset, combined learning trains minuscule models straightforwardly on their gadgets and afterward incorporates them to assemble the last model. Clients' information is never sent outside of their gadgets, making it more protected; in any case, if an attacker is one of the clients whose information the calculation is using, they are allowed to alter their own information to harm the model [20]. When combined with different calculations, the harmed calculation can possibly harm the last model. Thusly, they may harm the model or even introduce an indirect access. Google's Gboard is an illustration of unified realizing, which utilizes it to find out about word designs to prepare prescient consoles [22]. In spite of Google's extensive information verifying cycles, clients could hypothetically enter outlandish expressions to delude the prescient content or, all the more forebodingly, embed code into the calculation to offer themselves a secondary passage on the off chance that they adopted a less mindful strategy. Along these lines, some state of the art IoT gadgets are beginning to utilize unified figuring out how to gain from each other.

conclusion

IoT frameworks are vulnerable to a tonne of attacks, and as IoT usage grows, more and more threats are being found. This is because different attack surfaces are provided by IoT frameworks. Securing frameworks requires the adoption of the most potent defense against these dangers. As threats increase in number and frequency, researchers are turning to artificial intelligence (AI) to gradually and carefully secure these frameworks. Of course, attackers find ways to counter AI, and they could even use AI to their advantage while attacking a system. This article examines strategies that are routinely employed to breach or interfere with IoT and analyses how these assaults are successfully executed. The application of different AI computations to cybersecurity is then covered. In general, these models aren't used in many commercial applications right now, they're still in the experimental development stage, or they're challenging to utilize, which makes them distinctive. In the meanwhile, the models offered are promising, and in a few years they might serve as frameworks for unavoidable assault locations. Techniques for blocking AI and utilizing AI in attacks are also discussed in relation to IoT frameworks. These attacks will grow more lethal as IoT frameworks develop, especially as large networks like smart cities look into new uses for them. This is owing to the fact that large networks have a lot of attack surfaces, making them more difficult to secure, as well as the fact that security and everyday life are centered around AI, which should essentially be impenetrable. By focusing on these topics, this study aims to provide experts and cybersecurity specialists with a useful tool for evaluating IoT in terms of cybersecurity and AI to safeguard IoT frameworks. Additionally, it makes an effort to highlight the outcomes of fresh innovation as well as the effects each of these orders will have on the others. It is important to consider all of the potential effects of a mechanical advancement both before and after it is disclosed because cyber attackers are constantly looking for ways to use new technologies for their potential benefit, whether that involves diverting the technology from its intended purpose or using the technology as a tool to spread other attacks. This study, for instance, shows how the Internet of Things and artificial intelligence have been abused or had their weaknesses exploited. In order to identify these faults in the future to stop cyber-attacks, this information will help investigators control existing risks and promote mindfulness.

References

1. D. Evans, “The Internet of Things: how the next evolution of the internet is changing everything”, Cisco Internet Business Solutions Group, Cisco, 2011, [Online], Available: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pd
2. S. Alexander Gillis, “What is IoT (Internet of Things) and how does it work? IoT Agenda, TechTarget” [Online] Available: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT
3. D. Linthicum , “App nirvana: when the internet of things meets the API economy.” [Online] Available: https://techbeacon.com/app-dev-testing/app-nirvana-when-internetthings-meets-api-economy
4. Lu Y, Xu LD, “Internet of Things (IoT) cybersecurity research: a review of current research topics”, IEEE Internet Things, vol. 6 no. 2, pp. 2103–15, 2016.
5. C. Vorakulpipat , E. Rattanalerdnusorn , P. Thaenkaew , HaiHD , “Recent challenges, trends, and concerns related to IoT security, an evolutionary study”, In: 2018 20th international conference on advanced communication technology (ICACT), Chuncheon, Korea (South), 2018, pp. 405 - 410.
6. A. Lakhani , “The role of artificial intelligence in IoT and OT security”, [Online] Available: https://www.csoonline.com/article/3317836/the-role-of-artificial-intelligence-iniot-and-ot-security.html
7. A. Pendse , “Transforming cybersecurity with AI and ML”, [Online] Available: https://ciso.economictimes.indiatimes.com/news/transforming-cybersecurity-with-ai-andml/67899197
8. F. Meneghello , M. Calore , D. Zucchetto , M. Polese , A. Zanella, “IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices”, IEEE Internet Things Journal, 2019, vol. 6 no.5, pp. 8182 - 8201.

9. M. Roopak , G. Yun Tian , J. Chambers , “Models deep learning, for cyber security in IoT networks” , In: IEEE 9th annual computing and communication workshop and conference (CCWC), Las Vegas, NV, USA, 2019, pp. 0452–7.
10. Cañedo J, Skjellum A, “Using machine learning to secure IoT systems”, In 14th annual conference on privacy, security and trust (PST), Auckland, 2016, pp. 219–22,
11. F. Farivar , M.S. Haghighi, A. Jolfaei , M. Alazab , “Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT” IEEE Transaction on Industrial Informatics, 2019, vol.16 no. 4, pp. 2716–2725.
12. S. Wang , Z. Qiao , “Robust pervasive detection for adversarial samples of artificial intelligence in IoT environments”, IEEE Access 2019, vol.7, pp. 88693-88704.
13. P. Radanliev , D. De Roure , M. Van Kleek , O. Santos , U. Ani , “Artificial intelligence in cyber physical systems”, AI & society Journal of Knowledge, Culture and Communication, Springer, 2020, p. 1–14.
14. P. Radanliev , D. De Roure , K. Page , J.R. Nurse , R. Mantilla Montalvo, O. Santos , L.T. Maddox, P. Burnap , “Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains”. Cybersecurity, Springer Open, 2020, vol. 3, pp. 1–21.
15. P. Radanliev , D.C De Roure , J.R. Nurse , R.M Montalvo, S. Cannady , O. Santos , P. Burnap , C. Maple , “Future developments in standardisation of cyber risk in the Internet of Things (IoT)”, SN Applied Science. 2020, vol.2 no.2, pp.169.
16. S. Woo , “The right security for IoT: physical attacks and how to counter them”, In Minj VP, editor. Profit From IoT, [Online] Available: https://www.iot.electronicsforu .com/headlines/the-right-security-for-iot-physical-attacks-and-how-to-counter-them/
17. C. Herberger, “DDoS fire & forget: PDoS, a permanent denial of service”, Radware Blog, Radware Ltd, [Online] Available: https://blog.radware.com/security/2015/10/ddos-fireforget-pdos-a-permanent-denial-of-service
18. Cekerevac Z, Dvorak Z, Prigoda L, Čekerevac P, “Internet of things and the man-in-themiddle attacks–security and economic risks” Mest J, 2017, vol. 5, pp. 15–25
19. M. De Donno , N. Dragoni , A. Giaretta , A. Spognardi , “ Analysis of DDoS-capable IoT malwares”, In federated conference on computer science and information systems (FedCSIS), Prague, 2017, pp. 807-816.
20. S. Zeadally , E. Adi , Z. Baig , I.A. Khan, “Harnessing artificial intelligence capabilities to improve cybersecurity”, IEEE Access, 2020, vol. 8, pp. 23817–23837.
21. J. Jurn , T. Kim , H. Kim , “An automated vulnerability detection and remediation method for software security”, Sustainability, 2018, vol. 10, no. 5 pp. 1652.
22. M. Comiter , “Attacking artificial intelligence”, Belfer Center for Science and International Affairs, [Online] Available: https://www.belfercenter.org/publication/AttackingAI
23. Mohd, N., Singh, A., & Bhadauria, H. S. (2021). Intrusion Detection System Based on Hybrid Hierarchical Classifiers. *Wireless Personal Communications*, *121*(1), 659-686.
24. Mohd, N., Singh, A., & Bhadauria, H. S. (2020). A novel SVM based IDS for distributed denial of sleep strike in wireless sensor networks. *Wireless Personal Communications*, *111*(3), 1999-2022.