International Journal of Communication and Information Technology

E-ISSN: 2707-6628
P-ISSN: 2707-661X
www.computersciencejournals.com/ijcit
IJCIT 2023; 4(1): 46-53
Received: 06-01-2023
Accepted: 13-02-2023

Jatin Agrawal
AITCSE (AIML), Chandigarh University, Ajitgarh, Punjab, India

Samarjeet Singh Kalra
AITCSE (AIML), Chandigarh University, Ajitgarh, Punjab, India

Himanshu Gidwani
AITCSE (AIML), Chandigarh University, Ajitgarh, Punjab, India

Corresponding Author:
Jatin Agrawal
AITCSE (AIML), Chandigarh University, Ajitgarh, Punjab, India

AI in cyber security

Jatin Agrawal, Samarjeet Singh Kalra and Himanshu Gidwani

DOI: https://doi.org/10.33545/2707661X.2023.v4.i1a.59

Abstract
Artificial Intelligence (AI) is revolutionizing the field of cyber security, enabling organizations to better detect and respond to threats in real-time. AI-powered cyber security solutions leverage machine learning and other advanced techniques to analyze vast amounts of data and identify anomalies and patterns that might indicate an attack. This paper explores the various ways in which AI is being used in cyber security, including threat detection, incident response, security analytics, and more. It also discusses the benefits and challenges of using AI in cyber security and highlights some of the latest trends and developments in this rapidly evolving field.

Keywords: Artificial intelligence, cyber security, machine learning, threat detection, incident response, security analytics

Introduction

Cyber security is a major worry for businesses of all sizes and industries. As the number and complexity of cyber threats grow, security teams are finding it increasingly difficult to defend their networks and systems. Fortunately, Artificial Intelligence (AI) has emerged as an effective tool in combating cybercrime. AI-powered cyber security solutions use machine learning and other advanced approaches to detect and respond to threats in real time, allowing businesses to stay one step ahead of attackers. This paper will look at how AI is being used in cyber security, such as threat detection, incident response, security analytics, and more. We will also examine the advantages and disadvantages of employing AI in cyber security, as well as some of the most recent trends and breakthroughs in this fast expanding subject [1].

Threats in cybersecurity

Malware

Malware is software that is designed to damage a computer system, network, or device. Malware may take the shape of viruses, worms, Trojan horses and ransom ware. Once infected, malware may steal crucial data, damage files, or even take control of a device.

Phishing

Phishing is a social engineering method used by attackers to trick users into exposing personal information such as usernames, passwords, and credit card information. Phishing attacks may take numerous forms, including email scams, fake websites and malicious pop-ups [2].

DoS assaults: DoS attacks are designed to overwhelm a system with traffic, making it unreachable to legitimate users. DoS attacks may take many different forms, such as flooding a website with traffic or sending a vast amount of data to a network to cause it to collapse [4].
Insider risks are dangers presented by employees or contractors with access to sensitive data or systems.
Insider risks may manifest itself in a variety of ways, including intellectual property theft, sabotage and unauthorised access to sensitive data.

APTs (Advanced Persistent Threats): APTs are a kind of targeted and ongoing cyber assault. APTs may be used by nation-states, criminal gangs, or other skilled attackers to enter and maintain control of a network or system.

Ransom ware is a form of computer virus that encrypts data and demands payment in return for the decryption key. Ransom ware attacks may be harmful for both people and corporations, resulting in data loss and interruption of company operations [3].

Man-in-the-Middle (MitM) attacks include an attacker intercepting communications between two parties and modifying or stealing the data being sent. MitM attacks may steal login passwords, credit/debit card information, and other sensitive information.

Opportunities and Challenges

Opportunities

AI systems can analyse massive volumes of data in real time, allowing security teams to discover and respond to attacks more rapidly and effectively.

Improved accuracy

AI can assist enhance the accuracy of threat detection by analyzing data from many sources and discovering trends that people may miss.

Reduced false positives

AI-powered security solutions can minimise the amount of false positives, allowing security professionals to focus on the most critical threats.

Automated incident response

AI may assist in automating incident response, enabling security teams to react to attacks quickly and efficiently.

Improved efficiency

AI can help improve the efficiency of cyber security operations, reducing the workload for security teams and enabling them to focus on more complex tasks.

Challenges

AI algorithms rely on accurate data to perform well and acquiring this data can be difficult in cyber security, when data can be fragmented or missing.

Risk of false negatives

AI-powered security systems may overlook some risks, particularly those that are novel or have never been seen before.

Potential for malicious actors to control AI algorithms

Malicious actors may be able to influence AI algorithms to avoid detection, resulting in it being harder for security specialists to detect and respond to threats.

Skills gap

The use of AI in cyber security necessitates specialized skills and there may be a shortage of experts with the necessary competence [6].

Concerns using AI in cyber security

The use of artificial intelligence in cyber security involves ethical considerations, such as privacy, prejudice, and responsibility.

Artificial intelligence has the potential to improve cyber security through enhancing threat detection, lowering false positives, and automating incident response. However, there are significant hurdles to adopting AI in this industry, which organizations must carefully evaluate before installing AI-powered security solutions.

The use of artificial intelligence algorithms to detect and respond to cyber-attacks in real-time is known as AI-powered threat detection. This method enables organizations to analyse vast volumes of data from different sources in order to find trends and abnormalities that may indicate a cyber-assault [8].

Improved accuracy is one of the primary advantages of AI-powered threat detection. Traditional threat detection approaches may create a huge number of false positives, diverting security teams' attention away from the most serious threats. However, AI-powered systems may filter out unnecessary data and focus on the most critical dangers, minimising the chance of false positives and enhancing threat detection accuracy.

AI-powered threat detection can also increase the speed with which threats are detected and responded to. AI systems can swiftly discover new and emerging risks by continually analyzing data in real-time, allowing security teams to respond quickly. This can assist to mitigate the effects of cyber assaults and limit the harm they inflict.

However, there are several drawbacks to AI-powered threat detection. For example, in cyber security, where data may be fragmented or missing, these systems require high-quality data to perform properly. Obtaining this data might be problematic. Malicious actors may also be able to influence AI systems to avoid detection, making it more difficult for security teams to respond to attacks [5].

Overall, AI-powered threat identification is important tool in the fight. Organizations may better try to protect them from cyber assaults and minimize the harm caused by security events by enhancing the accuracy and speed of threat detection. However, the issues connected with AI-powered threat detection must be carefully considered, and these systems must be implemented and maintained efficiently.

Role of AI in cyber security

As the volume and complexity of cyber threats increase, so does the importance of AI in cyber security.

Here are a few examples of how AI is being utilized to improve cyber security:

Threat Detection

AI can detect and identify potential security threats such as viruses and spamming efforts. Algorithms using machine learning may be trained on enormous quantities of cyber security data to identify trends and anomalies that may suggest a cyber-attack [7].

Fraud Detection

Artificial intelligence may also be utilized in identifying fraudulent behavior, such as debit card scams and stealing an identity. Data trends may be analyzed by machine learning algorithms to identify suspicious conduct and flag it for further investigation.

Vulnerability management

AI may be used to assist uncover vulnerabilities in software and systems, allowing organizations to remedy them before they are exploited by cybercriminals.

Security Automation

Artificial intelligence (AI) may be used to automating routine security tasks such as threat evaluation and handling incidents. This frees up security specialists to concentrate on more complex tasks, such as developing and implementing security strategies.

Network Security

AI may be used to track network activity and detect potential security risks including unauthorized access attempts and unusual traffic patterns. In real time, machine learning algorithms can analyse network data and alert security experts to suspected security breaches.

AI has the potential to revolutionize cyber security by supporting enterprises in keeping ahead of the constantly evolving threat environment. Using the capabilities of NLP, ML, deep learning, computer vision, and other AI technologies, organizations may get beneficial insights into potential security vulnerabilities and avert them.

A. Why use AI in cyber security

AI may assist in more successfully detecting and preventing cyber assaults than conventional signature-based methods:-

Virus's detection

Traditional signature-based antivirus software may have difficulty detecting new and undiscovered viruses. AI-powered malware detection algorithms may discover and stop malware by analyzing patterns of behaviour using machine learning methods such as decision tree models, Support Vector Machines, and neural net.

Phishing prevention

Phishing attacks are a prevalent method for hackers to get sensitive information. AI can assist prevent phishing attempts by analyzing and identifying questionable emails and websites and then blocking them before they reach the end user.

Anomaly detection

AI may be applied to identify irregularities in network activity that may signal the existence of a cyber-threat. AI systems may identify even slight changes in behaviour that may be suggestive of an attack by analyzing massive volumes of data using methods such as clustering and deep learning.

Predictive analytics

AI is being used to analyze vast volumes of data and detect developments and trends that may be symptomatic of a cyber-attack using methods such as regression and time-series analysis. Organizations may utilise predictive analytics to detect and mitigate possible dangers before they cause harm.

Incident response

AI may be applied to computerize incident reaction operations, enabling security personnel to react to security issues swiftly and effectively.

Security teams may concentrate on more sophisticated duties, such as identifying the underlying cause of an attack, by automating basic operations like as threat analysis and incident triage. Security orchestration enabled by AI can also automate incident response operations such as threat hunting, alarm triage and remediation.

Limitations of traditional cyber security approaches

Traditional cyber security approaches have been widely adopted and have been effective to a certain extent, but they have several limitations. Some of the limitations are:

Inability to detect unknown threats

Traditional cyber security approaches rely on signatures or rules to detect known threats. This makes them ineffective in detecting unknown threats such as zero-day attacks, which exploit vulnerabilities that are not yet known to the security community.

High false-positive rates

Traditional cyber security approaches often generate false positives, which are alerts that suggest an attack is underway, but in reality, there is no attack. These false positives can distract security teams from actual threats and lead to alert fatigue.

Limited scalability

Traditional cyber security approaches are limited in their scalability due to the need for manual intervention. As the volume of data increase, these approaches become less effective, and it becomes tougher for teams to manually identify and respond to threats.

Inability to respond in real-time

Traditional cyber security approaches are often reactive, meaning that they are triggered after an attack has already occurred. This means that security teams are unable to respond in real-time, allowing the attack to cause significant damage before it can be mitigated.

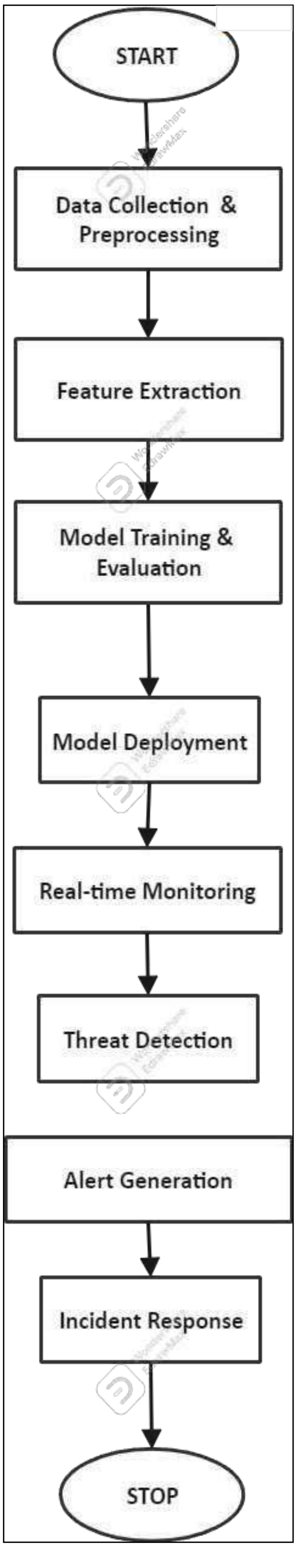
Limited ability to handle complexity

Cyber threats are becoming increasingly complex, and traditional cyber security approaches are struggling to keep up. They often lack the ability to analyze large volumes of data and they cannot detect subtle patterns of behavior that are indicative of an attack.

Traditional cyber security risk assessment methods are manual, time-consuming, and labor-intensive, making it challenging to identify and prioritize the most critical risks accurately. The conventional approach involves identifying assets, identifying threats, assessing vulnerabilities, and estimating the likelihood and impact of a successful attack.

AI-based cyber security risk assessment, uses ML algorithms and models to automate the process, reducing the time and effort required to identify and mitigate risks.

Basic Flowchart that illustrate the basic process of AI-powered threat detection in cyber security



*used edramax to draw flowchart

Fig 1: Basic Flowchart that illustrate the basic process of AI-powered threat detection in cyber security

Each step in the flowchart represents a specific process or action that occurs in the overall process of AI-powered threat detection in cyber security. Here's a brief explanation of each step:
Flowchart that illustrates the process of AI-powered threat detection in cyber security:
AI-powered threat detection in cyber security. Here's a brief explanation of each step:

Start: The process requires data collecting, which involves gathering cyber security data through many different places such as network activity records, system records, and security incidents.

Data collection: The acquired data is then cleaned and transformed into a usable format.

Pre-processing: This process includes reducing noise, dealing with missing data, and translating the information into a syntax that machine learning engines can understand.

Feature extraction: In this stage, important features from the already processed information are retrieved and utilized to train machine learning models.

Model training: Pre-processed and feature-extracted data is used to train machine learning models.

Model evaluation: The preciseness, recall, accuracy, and other performance features of the trained models are determined.

Model deployment: Once the models are trained and evaluated, they are deployed in a production environment for real-time monitoring.

Real-time monitoring: The deployed models monitor the network traffic and system logs in real-time, looking for patterns and anomalies that could indicate a cyber-security threat.

Threat detection: When a potential threat is detected, the models generate an alert.

Alert generation: The generated alert is then sent to the incident response team for further investigation.

Incident response: The incident response team investigates the alert and takes appropriate actions to mitigate the threat.

End: The process ends when the threat has been successfully mitigated, or when the models are updated and the process starts over again.

Offering what we have

Neural Net

Neural networks can be used in various ways to enhance cyber security. One such application is in the development of predictive models for threat detection. These models can be trained to identify patterns in large amounts of data that may indicate a potential cyber-attack, such as unusual network activity or the presence of malware.

Neural networks can also be used in irregularities identification, which involves identifying unique trends of behavior or activity that may indicate a potential threat. Anomaly detection algorithms can be trained using historical data to identify patterns that are consistent with a potential attack, and can then be used to detect and alert security teams to suspicious activity.

Furthermore, neural networks may be used to create malware detection systems, which are intended to identify and avoid unauthorized access to digital systems and networks. Neural networks may assist detect possible threats and trigger automatic actions to avert security breaches by analyzing network traffic and other data sources [9].

Finally, neural networks may be used to supplement current safeguards like firewalls and anti-virus software. Neural networks may assist to increase the efficacy of standard security measures and lower the danger of cyber-attacks by analyzing massive volumes of information and detecting possible threats more accurately and rapidly than traditional security measures.

Expert system

Expert systems are artificial intelligence-powered computer programs that are meant to emulate the capacity for choice of a human expert in a certain topic. Many areas of security operations, such as threat detection and response, may be automated using expert systems in cyber security.

In the development of systems to detect breaches, expert systems are used. These systems detect and prevent unlawful access to electronic networks and systems. Expert systems may be taught to recognize patterns of behavior that are consistent with a possible assault using previous data. When a possible danger is identified, the system may initiate automatic measures to protect against security breaches [14].

Another application of expert systems in cyber security is in the development of decision support systems for incident response. These systems can be used to guide security teams through the process of responding to a security incident, providing recommendations for actions based on the specific circumstances of the incident.

Expert systems can also be used in the development of risk management systems, which are designed to assess and mitigate potential risks to an organization's cyber security. By analyzing data from various sources, including network traffic, logs, and security alerts, expert systems can help to identify potential vulnerabilities and recommend actions to reduce the risk of a security breach [10].

Finally, expert systems can be used in the development of SIEM systems. These systems are designed to join and study data from multiple sources to identify potential security incidents. Expert systems can be used to automate many aspects of this process, including the correlation of data from different sources and the identification of potential threats.

Intelligent agent

Intelligent agents are AI-based systems that are capable of autonomous decision-making and action. In cyber security, intelligent agents can be used to automate many aspects of security operations, such as threat detection, response, and mitigation [11].

One application of intelligent agents in cyber security is in the development of autonomous security systems. These systems are designed to detect and respond to security threats without human intervention, using algorithms and decision-making processes that are based on machine learning and other AI technologies.

Intelligent agents may also be employed in the creation of decision support systems for security operations. These systems may analyse data from multiple sources, such as network traffic, logs, and security alerts, to detect possible dangers and offer mitigation measures [12]. The agents may then initiate automatic reactions to the danger, such as isolating impacted computers or blocking malicious traffic.

Intelligent agents are also used in the creation of security information and event management (SIEM) systems. These systems are intended to collect and analyse data from different sources in order to detect possible security issues. Many components of this process, including the correlation of data from many sources and the detection of possible dangers, may be automated using intelligent agents [13]. As AI and machine learning continue to grow, we should expect to see further advancements in the usage of intelligent agents and other AI technologies in cyber security.

Intelligent agents may also be employed in the construction of cyber threat intelligence systems. These systems may be used to monitor and analyse data from numerous sources, such as social media, news sources, and dark web forums, in order to detect possible cyber threats. Security teams may then get notifications and suggestions for action from the agents.

Search

Search algorithms are an useful component of AI-based systems in cyber security. They can be used to study vast amounts of information to identify threats or bugs, and to search for patterns or anomalies that may indicate an attack or breach.

One application of search algorithms in cyber security is in the development of malware detection systems. These systems can use search algorithms to identify known malware signatures or patterns in code, and to search for new or unknown malware that may be present in a system. The search algorithms can also be used to analyze network traffic and other data sources to identify potential malware infections [15].

Search algorithms can also be used in the development of intrusion detection systems. These systems can use search algorithms to identify patterns of behavior that are consistent with a potential attack, and to search for anomalies or deviations from normal network activity [16]. The algorithms can also be used to search for known attack signatures or patterns in network traffic.

Another application of search algorithms in cyber security is in the development of vulnerability assessment systems. These systems can use search algorithms to identify potential vulnerabilities in a system or network, and to search for known exploits or attack vectors that could be used to exploit those vulnerabilities [17].

Finally, search algorithms can be used in the development of cyber threat intelligence systems. These systems can use search algorithms to monitor and analyze data from various sources, including social media, news sources, and dark web forums, to identify potential cyber threats. The algorithms can search for specific keywords or phrases that may be associated with a particular type of attack or threat.

Future of AI and its impact

Artificial intelligence (AI) is rapidly transforming the field of cyber security, offering new tools and capabilities for identifying and mitigating threats. AI is quickly revolutionizing the world of cyber security, providing new tools and capabilities for detecting and managing threats. As artificial intelligence technology improves, we should expect to see ever more interesting applications in the field of cyber security. We'll look at the future of AI and how it could affect cyber security.

Advances in AI for Cyber security

Threat identification and response is one area where AI is already making substantial progress in cyber security. Machine learning algorithms are being used to analyse massive volumes of data in order to detect trends that may suggest harmful behaviour. This may help security teams react to possible attacks more swiftly and efficiently.

Furthermore, artificial intelligence is being utilized to enhance vulnerability assessment and patch administration. Security teams may concentrate their efforts on the most significant problems and limit the risk of exploitation by utilizing machine learning to discover and prioritize vulnerabilities.

Some potential areas where AI could make a significant impact

Enhanced Threat Detection and Response

As AI technology advances, we may anticipate more advanced algorithms for identifying and reacting to attacks. These algorithms will be capable of analyzing vast amounts of data and identifying possible dangers faster and more precisely than ever before.

AI-Powered Security Analytics

AI algorithms may assist in identifying trends and patterns in security data that human analysts may miss. This may assist security teams in detecting possible dangers and taking preventative actions to neutralize them.

Automated Incident Response

By automating incident response, security teams may react to threats more rapidly and effectively. This may assist to mitigate the effect of security events and lower the likelihood of data loss or other bad consequences.

AI may be used to improve identity and access management systems, increasing the accuracy of authentication and authorization procedures and lowering the danger of unauthorized access.

Proactive Threat Hunting

Using AI, security teams may proactively look for possible threats before they can do damage. This may aid in the detection and remediation of vulnerabilities before they are exploited.

Trends in AI applications for cyber security

In the battle against cybercrime, artificial intelligence (AI) has emerged as a potent weapon. As cyber security threats grow more complex, innovative tools to identify and prevent assaults are becoming more important. Machine learning-based threat detection is a prominent development in AI applications for cyber security. Machine learning algorithms are being used more and more to analyze enormous amounts of data and find trends that may suggest a possible cyber threat. These algorithms may use previous data to identify new forms of assaults and constantly improve their detection accuracy.

Another development in AI applications for cyber security is the use of natural language processing (NLP) to search for signals of cyber risks in text-based data such as emails, chat logs, and social media feeds. NLP may be used to extract useful information from unstructured data sources and find patterns that may suggest a possible attack. This technology may also be utilized to automate the investigation of security logs and warnings, saving security professionals valuable time.

Another cyber security development is AI-powered behavioral analytics. This system analyses user behaviour and identifies abnormalities that may suggest a possible cyber-attack using machine learning algorithms. For example, if an employee begins accessing sensitive data that they have never accessed before, this might indicate a data breach or an insider threat. AI-powered analytics may assist in detecting such abnormalities in real-time and alerting security professionals to take appropriate action.

Additionally, AI is being used to automate security operations, such as patching and updating software, as well as vulnerability scanning and penetration testing. Automation can help reduce the workload of security teams and ensure that vulnerabilities are identified and patched quickly.

AI is also being used to improve threat intelligence. With the vast amount of data available on the internet, it can be challenging for security teams to sift through all the noise and identify relevant threats. AI-powered threat intelligence may assist in identifying possible threats by automatically combining and analyzing data from multiple sources such as social media, forums, and dark web markets.

The trends discussed above, including machine learning-based threat detection, NLP, behavioral analytics, security automation, and AI-powered threat intelligence, are just some examples of how AI is being applied to cyber security. As the cyber security landscape continues to evolve, it is clear that AI will play an increasingly important role in protecting against cyber threats.

- AI-powered behavioral analytics can identify anomalies in user behavior that may indicate a potential cyber threat.
- Automation is being used to improve security operations, such as patching and vulnerability scanning.
- AI-powered threat intelligence can automatically aggregate and analyze data from various sources to identify potential threats.
- These trends in AI applications for cyber security enable faster and more accurate threat detection and response.
- AI is expected to play an increasingly important role in protecting against cyber threats as the cyber security landscape continues to evolve.
- AI is being used to enhance security for cloud-based applications and services.

Overall, the continued development of AI technologies promises to bring about significant advances in the field of cyber security. As AI becomes more sophisticated, it is likely to play an increasingly important role in detecting and responding to cyber threats, helping to keep individuals and organizations safe from harm.

Potential Risk and Concerns

While AI offers many benefits for cyber security, there are also potential risks and concerns to consider. For example, there is a risk that AI algorithms may be vulnerable to manipulation or attack, leading to false positives or false negatives in threat detection. In addition, there are concerns around the use of AI for automated incident response, as this could lead to unintended consequences or even further damage in some cases.

Conclusion

In the subject of cyber security, artificial intelligence (AI) has emerged as a potent tool. Organizations are increasingly turning to AI-based solutions to identify and react to cyber-attacks as the volume and complexity of these threats grows. AI has various potential advantages in cyber security, including faster attack detection and response times, more accurate risk assessments, and increased regulatory compliance. In this research paper, we will look at the importance of AI in cyber security and how it is being utilized to enhance security posture.

The capacity of AI to analyze massive volumes of data rapidly and correctly is one of its primary benefits in cyber security. AI can analyze enormous amounts of data using machine learning algorithms to discover trends and anomalies that may suggest a possible cyber-attack. This allows organizations to identify and react to threats more quickly than ever before, lowering the chance of a successful assault.

Another key industry where AI is having a huge influence is threat intelligence. Artificial intelligence-powered threat intelligence systems may collect and analyze data from a variety of sources, including social media, dark web forums, and other internet channels. This enables security teams to remain on top of new threats and react swiftly to new and developing attack vectors.

Artificial intelligence is also being utilized to enhance authentication and access management. AI can detect when a user's behaviour deviates from their regular patterns, signaling a possible security problem, by analyzing user behaviour patterns. This helps organizations to develop more effective access control measures while also lowering the risk of unauthorized access to critical data and systems.

However, the application of AI in cyber security is not without hurdles. One of the most difficult difficulties is the lack of high- quality data. AI algorithms need a big quantity of high-quality data to be successful. This data must also be carefully labelled so that the AI can find trends and anomalies. Another difficulty is the lack of qualified professionals capable of designing and efficiently implementing AI-based solutions.

References

1. Alkasassbeh M, Al-Naymat G, Hassanat AB, Almseidin M. Detecting Distributed Denial of Service Attacks using Data Mining Techniques. Int. J Adv. Comput. Sci. Appl.; c2016.
2. Manikumar DVVS, Maheswari BU. Blockchain based
3. DDoS mitigation using machine learning techniques in Proc. 2nd Int. Conf. Inventive Res. Comput. Appl. (ICIRCA); c2020. p. 794-800.
4. DdoS Evaluation Dataset (CICDDoS2019). https://www.unb.ca/cic/datasets/ddos2019.html
5. Doshi R, Apthorpe N, Feamster N. Machine Learning DDoS Detection for Consumer Internet of Things Devices. IEEE Security and Privacy Workshops (SPW); c2018.
6. Netscout Systems. Netscout Threat Intelligence Report; c2021. https://www.netscout.com/threatreport
7. Wani S, Imthiyas M, Almohamedh H, Alhamed KM, Almotairi S, Gulzar Y. Distributed denial of service (DDoS) mitigation using block chain-A comprehensive insight Symmetry. 2021;13(2):227.
8. Saini PS, Behal S, Bhatia S. Detection of DDoS Attacks using Machine Learning Algorithms. 7th International Conference on Computing for Sustainable Global Development (INDIA.Com); c2020. p. 16-21.
9. Rathore R. A Study on Application of Stochastic Queuing Models for Control of Congestion and Crowding. International Journal for Global Academic & Scientific Research. 2022;1(1):1-6. https://doi.org/10.55938/ijgasr.v1i1.6
10. Sharma V. A Study on Data Scaling Methods for

Machine Learning. International Journal for Global Academic & Scientific Research. 2022;1(1):23-33. https://doi.org/10.55938/ijgasr.v1i1.4

11. Rathore R. A Review on Study of application of queuing models in Hospital sector. International Journal for Global Academic & Scientific Research. 2022;1(2):1-6. https://doi.org/10.55938/ijgasr.v1i2.11
12. Kaushik P. Role and Application of Artificial Intelligence in Business Analytics: A Critical Evaluation. International Journal for Global Academic & Scientific Research. 2022;1(3):01-11. https://doi.org/10.55938/ijgasr.v1i3.15
13. Kaushik P. Deep Learning and Machine Learning to Diagnose Melanoma; International Journal of Research in Science and Technology. 2023 Jan-Mar;13(1):58-72. DOI: http://doi.org/10.37648/ijrst.v13i01.008
14. Kaushik P. Enhanced Cloud Car Parking System Using ML and Advanced Neural Network; International Journal of Research in Science and Technology. 2023 Jan-Mar;13(1):73-86. DOI: http://doi.org/10.37648/ijrst.v13i01.009
15. Kaushik P. Artificial Intelligence Accelerated Transformation in the Healthcare Industry. Amity Journal of Professional Practices, 2023, 3(01). https://doi.org/10.55054/ajpp.v3i01.630
16. Kaushik P. Congestion Articulation Control Using Machine Learning Technique. Amity Journal of Professional Practices, 2023, 3(01). https://doi.org/10.55054/ajpp.v3i01.631
17. Rathore R. A Study of Bed Occupancy Management in the Healthcare System using the M/M/C Queue and Probability. International Journal for Global Academic & Scientific Research. 2023;2(1):01-09. https://doi.org/10.55938/ijgasr.v2i1.36