International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.003 ISSN: 2581-4621

Harnessing Machine Learning for Advanced Attacker Behavior Analysis in Cybersecurity

Ganla Sneha[1]*, G Manogna[2], T C Swetha Priya[3]
[1] Student, Department of Information Technology, Stanley College of Engineering and Technology for Women, India
[2] Student, Department of Information Technology, Stanley College of Engineering and Technology for Women, India
[3]Assistant Professor, Department of Information Technology, Stanley College of Engineering and Technology for Women, India

Abstract
With the increasing complexity of cyber threats, many traditional security methods have become ineffective in keeping up with the ever-evolving tactics of cybercriminals. Since attackers constantly adapt and change their strategies, there is a clear need for proactive defense mechanisms. Machine Learning and Artificial Intelligence have become key forces in transforming cybersecurity, enabling real-time insights into attack behavior, predictive threat assessments, and automated response mechanisms. This paper explores how AI-based tools utilize supervised and unsupervised learning, anomaly detection, and deep learning techniques to enhance cybersecurity by identifying attack patterns, profiling threat actors, and mitigating risks. We also examine adversarial machine learning and data bias, discussing widely adopted approaches and the challenges they present. Additionally, we highlight future advancements in AI-driven security frameworks and their role in strengthening cyber defence strategies. By leveraging AI and ML for attacker behavior analysis, organizations can shift from reactive to predictive security, effectively minimizing their attack surface and reducing response time. Bridging the gap between AI innovations and practical cybersecurity applications will lead to a more resilient and adaptive threat intelligence system.
Keywords: *Machine Learning, Cybersecurity, Attacker Behavior Analysis, Threat Detection, Threat Intelligence.*

INTRODUCTION

Challenges of Cybersecurity

Cybersecurity is ever-changing and contends with the challenges of advancing technology and increasing sophistication of the threats posed by cyber criminals. APTs are one of the biggest, or rather the most crucial, threats in which attackers gain unauthorized access to your systems and stay tracked for long periods to extract sensitive data. This type of situation presents considerable risks to organizations dealing with critical information. Ransomware attacks have now developed to a level where criminals are not just encrypting data; they're also exfiltrating it and threatening to release that data unless demands are met, which adds yet another layer of pressure on victims. The widespread availability of usage of IoT devices has greatly increased the attack surface since many IoT devices are not equipped with solid security mechanisms, making it easy to find their way into exploitation and breaches into the enterprise network. As flexibility and scalability are functions of the big advantage offered by cloud computing, security often becomes an afterthought. The next thing one must consider in cloud computing is the security impacts that arise from misconfigurations, weak access controls, and unauthorized disclosure of data, thus highlighting the need for stringent security measures.[1]

Phishing and social engineering attacks persist as a problem, with cybercriminals using deceptive tactics to trick individuals into revealing confidential information or installing malicious software.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.003 ISSN: 2581-4621

Insider threat, whether intentional or accidental, represents another major risk to the security of information, as employees or contractors possessing sensitive data could inadvertently or intentionally induce a data breach. Supply chain attacks, another increasing threat study, allow attackers to exploit weaknesses in third-party vendors to target larger organizations, making the detection and prevention more challenging. Artificial Intelligence and Machine Learning get caught in the controversy, as cybercriminals aggravate this problem by using these technologies against cybercrime, which are then used in developing advanced cyber threats, automatically conducting attacks, and avoid defense mechanisms.

One of the major obstruction for the field of Cybersecurity is the scarcity of skilled manpower-the demand outweighs the supply of skilled professionals, thereby limiting the opportunities for organizations to defend against, detect, and mitigate threats proficiently. Also, compliance with data protection regulations adds complexity, as organizations have to meet multidimensional legal requirements while making certain their data integrity security is in place. Addressing these Cybersecurity challenges requires the intervention of a holistic Cybersecurity framework that entails implementing advanced security technology, building an awareness culture, conducting periodic risk assessment exercises, and creating effective incident response plans. To build resilience against cyber adversaries, it is critical to always keep current with emerging threats and adapt security strategies accordingly.

Role of Machine Learning in Cybersecurity

Machine learning plays a vital role in modern cybersecurity by enhancing both threat detection and response mechanisms. The cybersecurity framework consists of three fundamental stages: prevention, detection, and response. While it is nearly impossible to eliminate cyber threats entirely, and reacting to an attack often means damage has already occurred, advanced security systems, particularly those powered by machine learning, emphasize early detection to minimize risks.

One of the most significant applications of machine learning in Cybersecurity is malware detection. Since malware primarily targets specific devices, its detection involves analyzing data at the host level, such as through Host-based Intrusion Detection Systems (HIDS), with antivirus software being a common subset of these systems. Different malware variants are designed for specific operating systems, and historically, Windows OS has been the primary target due to its widespread use. However, as mobile devices become more prevalent, cybercriminals are increasingly focusing on platforms like Android OS, making malware detection on mobile devices equally important.[2]

Phishing remains a leading method used by attackers to infiltrate networks, making its early detection essential for modern Cybersecurity strategies. Machine learning significantly enhances phishing detection through two primary applications: identifying phishing websites and detecting phishing emails. In the case of websites, machine learning models analyze attributes such as the webpage's URL, HTML code, or even its visual similarity to legitimate sites. For emails, detection methods involve examining the text content, email headers, and attachments to identify potential phishing attempts. By leveraging machine learning for these tasks, Cybersecurity systems can efficiently identify and mitigate phishing threats, protecting users from falling prey to fraudulent schemes.

Focus

Many standards define cybersecurity differently and as a result, present blurred definitions. Various definitions from Cybersecurity-related technical committees of standards developing organizations can be analysed to arrive at a more common understanding. Cybersecurity is defined as protecting

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.003 ISSN: 2581-4621

the confidentiality, integrity and availability of digital assets in cyberspace from cyber threats. In this instance, cyberspace refers to interconnected computers, electronic devices, communication systems and services; wired and wireless networks; and the data that these networks carry.
Cyber attacks are seldom direct attacks; instead, measures that may hurt society as a whole. Cybersecurity's latest areas under the spotlight could include study in transportation systems, the Internet of Things (IoT), Cyber-Physical Systems (CPS) and healthcare. Cyber threats are changing, and with the introduction of new digital assets, organizations will have to adopt dynamic and adaptive cybersecurity strategies. This article looks at cybersecurity from an organizational viewpoint and provides some remedies for businesses facing security challenges in this highly digitized environment.

BACKGROUND AND RELATED WORK

Methods for Attacker Behavior Analysis
Computers are learned behavior of attackers very much important for identification and thus mitigation of cyber threats. Fusion of much improved Machine Learning as the Artificial Intelligence catchers-catchers with the ability in the way of seizing attack patterns as well as other so-called anomalies in the adoption of different cyber threateningly evolving strategies. In behavior of attacker detection, several methods, signature-based detection measure as one of the most widely used techniques.

a. Signature-Based Detection
The signature-based method is often used in most Intrusion Detection Systems (IDS) for identifying the malicious activities. The method basically looks at incoming events against the database of predefined signatures that characterize the attack patterns. The process of signature matching is one of the most computationally intensive tasks in an IDS where input event is compared to predefined rules that make an input event to be compared against only one ruling condition at a time. However good this method may be, it makes for very inefficient processing in terms of time and computational cost. Some of the innovative IDS solutions, in order to surf, would take recourse to optimized algorithm as well as advanced data structures to enhance the speed and accuracy of signature-matching.[3]
In signature detection, good identification is given for known threats with fewer false positive alerts as compared to anomaly detection methods. Signature detection systems are simple to implement and configure, and therefore find much favor with large production networks. Most commercial systems of intrusion detection and popularly adopted security frameworks utilize signature-based detection methodology. Even though these systems would work perfectly to detect known threats, they still suffer from several limitations. The signature-process limitations can be summed up below:
1. **Very Limited Detection –** It only works against known threats and cannot detect a specifically unknown attack, that is, zero-day attack, or a recently developed malware.
2. **Permanent Requirement for Updating –** A constant update is required to keep an updated database of attack signatures, which adds to the maintenance overhead.
3. **Easily Evaded by Attackers –** Cybercriminals can change their modes of attacks slightly so that such alterations would evade detection by systems operating on fixed signature detection.
4. **Huge Computational and Storage Need –** Signature-based detection requires heavy processing and storage, thus slowing down the performance of the system because of immediately increasing databases of attack signatures.
5. **Inability to Adapt New Threats –** Unlike machine-learning-based methods, signature-based detection has little ability to adapt to or recognize previously unseen attack patterns, which limits its long-term effectiveness.

b. Rule Based Detection
Rule-based detection is crucial in identifying previously known attack patterns. However, keeping up with this is improving with machine learning (ML) techniques in intrusion detection against

DOI:10.46647/ijetms.2025.v09si01.003 ISSN: 2581-4621

sophisticated cyber attacks. All of these improve the functions of both detection and increase the performance of Intrusion Detection Systems (IDS) for minimizing false positives and enhancing decision-making processes[4]. On overall purposes, (i) it should improve the accuracy of IDS while lessening the false alarms and (ii) using the predictions of the machine learning model to gain further insights of the network behaviour. However, these techniques are very good at detecting malicious activity in a network but usually generate too much alerts that might overwhelm administrators and thus possibly increase the false positive ratio. The combination tends to provide a balance in terms of effectiveness and practicality in defence against Distributed Denial-of-Service (DDoS) attacks and other threats posed by cyberspace by rule-based detection interfacing with the ML-driven analysis. Below are the limitations of rule-based detection:[5]

1. **High Manual Effort –** Cybersecurity expert definition, update, and management of rules requiring much resource.
2. **High False Positives** – Excessive general or broad rules lead to over alertness and fatigue much.
3. **Low Adaptability** – Cannot recognize customized or evolving mechanisms where attacks do not fall into predetermined patterns.
4. **Scalability Problems -** A large rule set for a large network increases the time taken to process and compute.
5. Complicated Configuration Fine tuning would be required consistently to achieve the right balance between strict detection and leniency.

Machine Learning techniques for attacker behavior analysis

Machine Learning is one of the things that have changed the face of Cybersecurity with the automation of threat detection, anomaly detection, and response mechanisms. Conventional security techniques are rule-based and signature-based and are rendered incapable of detecting zero-day attacks and advanced persistent threats. ML models, otherwise, look back at historical attack data to recognize real-time unusual behaviors and evolve against changing cyber threats. With the application of supervised and unsupervised learning, ML arms Intrusion Detection Systems for practical application to IDS, malware classifiers, fraud detection, and risk assessment, among others.[6]

a. Supervised Learning

The label data is extensively utilized for classification purposes in network traffic and detection in case of malicious eventstrings. Such algorithms include Decision Trees and Support Vector Machines (SVMs) help differentiate between normal and harmful traffic by segmenting data or determining optimal classification boundaries. These techniques are indeed critically important in intrusion detection systems, where the accurate classification of network activity is key.[7]

Advanced supervised learning models such as Deep Neural Networks (DNNs) can recognize complicated patterns into large and complex datasets, improving the detection of Cybersecurity threats. These models are measured in terms of accuracy, precision, recall, and F1-score. Well-prepared quality labelled data assist supervised learning models to meet their requirement, achieving breathtaking accuracies and precision in reducing false alarms in security applications. Simpler computational models, such as Decision Trees, easily train and predict with less time, which makes them ideal for real-time applications. On the contrary, a DNN needs a lot in its complexity and long training process, demanding much computation to execute the task.

b. Unsupervised Learning

In Cybersecurity, it is of great importance to use Unsupervised Techniques which avoids the use of labelled data but looks for unknown threats and anomalies. Examples of Unsupervised Techniques include k-means clustering and even Principal Component Analysis (PCA) for recognition of patterns and dimensional transformation. These are meant for intrusion detection especially on breaches and zero-day attacks. As much as unsupervised learning is quite proficient in the way it can bring out emerging threats, it usually raises false positives more often than supervised techniques. However, this makes it the most important technique where there is limited or no

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.003 ISSN: 2581-4621

labelled data or where there is a rapidly evolving threat landscape. [8]
From a computational standpoint, PCA efficiently reduces data complexity but may lose some critical information in highly intricate datasets. Clustering algorithms, while useful for grouping similar attack patterns, may struggle with high-dimensional data and require fine-tuning to prevent misclassification.

IMPLEMENTATION

De-Malwarization
Malware is used for invasion into a computers or mobile device systems and with the malicious actions causes degradation in the performance along with user's security, confidentiality and reliability. Malware can be in the form of program, script or any active content. Computer users require major mechanisms for security in their systems against the internet.[9]
The detection of an anomalous behavior of a component will lead to the further checks for the presence of malware. The engine makes use of pattern signatures of known malwares listed in a list called the Blacklist to verify if the detected anomalous behaviors match any of those included in the available behaviors. If they indeed match, then the typemalware will be classified according to the type of signature match it made, for instance, virus, trojans and so on.
After detection and classification of malware, the removal is done from the system while the computer restored to its previously stable state. In some cases, the malicious file is segregated from the rest of the files.

a. Signature based malware detection
In signature-based detection, the presence of at least one byte in malware input code will be checked against the accepted signatures of existing malware in a database, which is commonly called the Blacklist. The basic premise is that most malware can be identified via patterns or signatures, which is the most common method of malware detection. However, this technique has its own demerits.

b. Behavior based malware detection
Behavior-based malware detection method observes the behavior of a software program to arrive at a conclusion about whether the software is malicious. While the software behavior analysis performed on the executed code during the run in the system would check for abnormalities from the routine program flow would be called a behavior-based method. If anything abnormal is found, this behavior is matched against existing malicious behaviors and eliminated upon finding a match. The behaviors being monitored during the execution of the software are the system calls that are invoked onto the operating system. Since behavior-based detection relies on more than just a signature of pre-existing malware, but also takes into consideration how the software behaves, the limitations encountered in the signature-based approach are thereby circumvented.
A rule-based approach for attribute selection and intrusion detection in wireless sensor networks
Wireless sensor networks (WSNs) consist of dynamic multi-hop networks that are composed of a number of nodes. The nodes relay information in a multi-hop manner without needing any existing infrastructure. WSNs are characterized by great flexibility and the ability to be put in a wide range of applications, but with that flexibility comes great vulnerability, which adds to their security threats. However, the mechanisms for security for WSNs are very effective as measures of prevention since they are energy conscious. Thus, effective and efficient security mechanisms are required to secure and rely on WSNs.[12]
The rule-based decision manager adopts a forward chaining and backward chaining control flow. The Rule Manager implements some special techniques of rule firing and rule matching. The integrity and security of the entire framework must be maintained by the rule-based decision manager in conjunction with the administrator module. The rule-based decision manager stores rules in the rule base and manipulates them.
The rule base contains rules for security, rules for cluster information, and rules for fault tolerance.

DOI:10.46647/ijetms.2025.v09si01.003 ISSN: 2581-4621

All these rules are stored in the form of IF - THEN rules. The rules are also set up using the decision tree.

Behavior-Anomaly-Based System for Detecting Insider Attacks and Data Mining

Insider attack, also referred to as insider misuse, deals with that rather type of computer security threat. The nature of insider attacks can be categorized into three perpetrators: masqueraders, legitimate users, and clandestine users. Masqueraders are users who obtain the login credentials of legitimate users and improperly access the enterprise applications and data with these credentials. The legitimate users are persons who have authorized access to the enterprise computing resources but may misuse their access privileges to download considerable amounts of information or view information that does not pertain to the performance of their job functions[13]. Clandestine users, on the other hand, obtain administrative access privileges beyond or even unrelated to what they need for their job responsibilities. Clandestine users would normally already know the enterprise security systems and will find ways to bypass the same for accessing information. The proposed solution in this paper is intended for the detection of insider attacks by masqueraders and legitimate users. An alternative classification and detection approach may obtain its definition from an understanding of the computing infrastructure level at which the misuse can be identified, such as at the level of the network, system, or application. An intrusion detection system for real-time environment has been proposed, which depicts various detection approaches including descriptions of those used by our proposed solution and offers a common basis for intrusion detection system-development. Enterprises spend a significant part of their computer security budget in preventing attacks emanating from external hackers, who may be trying to gain unauthorized access to the enterprise or introduce malignant code such as worms and viruses into the enterprise. Identification and prevention of insider attacks prove to be difficult, more so than those of outsiders, since attacks are carried out through the internal firewall by trusted users who pass the usual authentication and authorization steps. To mitigate the impact on the users of such a forensic process, logs from security monitor applications, middleware programs, application servers, and other enterprise applications can be obtained for analysis after attacks occur.[14] This technique detects the insider attacks after the data has been accessed rather than as they are happening. This paper describes the nature of one insider attack involving employees of the enterprise engaging in access of resource behavior patterns which exceed normal for whatever their performing duties may involve. That is, while employees may have general authorization for accessing particular applications and data in the course of doing their jobs, they access excessive amounts of data or data not related to their assigned tasks.

So there is a proposed system for the early detection of insider attacks. This closed-loop system analyzes historical data to determine peer-group access behavior, initializes its real-time data-mining component with historical baseline data for that information, and meanwhile, monitors user-behavior statistics in real-time. Such real-time information could then update the historical analytical tool leading to the fine-tuning of behavior models, thus updating in turn the real-time monitoring component, and so on cyclically in a self-tuning fashion.

The system works by creating peer groups- that is groups of individuals with similar sets of characteristics. That is accounting for the knowledge and experience of the investigator with respect to the population and also deploying data mining techniques, which we shall examine shortly. As an illustration, a group of customer service representatives working in a corporate help desk constitutes a peer group. We figure that people who have roughly similar job functions will show similar access to enterprise applications and similar demand levels on systems for information. Set of personal and/or work-related information such as an employee's work history, physical locale, or performance rating may come into play in determining the classification of a certain user to a peer group. This can also be complemented with an understanding of the business processes in which any class of user participates.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.003 ISSN: 2581-4621

RESULTS AND DISCUSSION

The presented system runs in real time, capturing network packets and displaying such necessary attributes as source IP, destination IP, and protocol. When suspicious behavior- comprising port scans-is detected, an alert is dispatched. A number of packets are randomly selected and set out in a bar graph, where each thin bar represents a destination IP with a corresponding packet count. Fig 1 summarizes captured network traffic.

```
C:\Users\ganla\WSN_detector>python imple.py
🔍 Monitoring on interface: Intel(R) Wireless-AC 9560 (capturing 20 packets)...
📦 Packet: 192.168.0.117 → 239.255.255.250 | Protocol: udp
📦 Packet: 192.168.0.102 → 192.168.0.117 | Protocol: udp
📦 Packet: 192.168.0.102 → 192.168.0.117 | Protocol: udp
📦 Packet: 192.168.0.117 → 192.168.1.103 | Protocol: tcp
📦 Packet: 192.168.0.117 → 192.168.1.103 | Protocol: tcp
📦 Packet: 192.168.0.104 → 192.168.0.117 | Protocol: udp
📦 Packet: 192.168.0.117 → 192.168.0.104 | Protocol: tcp
📦 Packet: 192.168.0.104 → 192.168.0.117 | Protocol: tcp
📦 Packet: 192.168.0.117 → 192.168.0.104 | Protocol: tcp
📦 Packet: 192.168.0.117 → 192.168.0.104 | Protocol: tcp
📦 Packet: 192.168.0.104 → 192.168.0.117 | Protocol: tcp
📦 Packet: 192.168.0.104 → 192.168.0.117 | Protocol: tcp
📦 Packet: 192.168.0.117 → 192.168.0.104 | Protocol: tcp
📦 Packet: 192.168.0.107 → 192.168.0.117 | Protocol: udp
📦 Packet: 192.168.0.117 → 192.168.0.107 | Protocol: tcp
📦 Packet: 192.168.0.104 → 192.168.0.117 | Protocol: tcp
📦 Packet: 192.168.0.104 → 192.168.0.117 | Protocol: tcp
📦 Packet: 192.168.0.117 → 192.168.0.104 | Protocol: tcp
📦 Packet: 192.168.0.117 → 192.168.0.104 | Protocol: tcp
📦 Packet: 192.168.0.104 → 192.168.0.117 | Protocol: tcp
✅ Monitoring session complete.
```

***Fig. 1**: Captured network traffic summary*

Fig. 2 The network activity per destination IP is demonstrated based on packet count. The x-axis displays destination IP addresses, while the y-axis indicates the number of packets received, facilitating the analysis of network traffic. A successful compelete message verifies that the monitoring and visualization process was successfully completed.

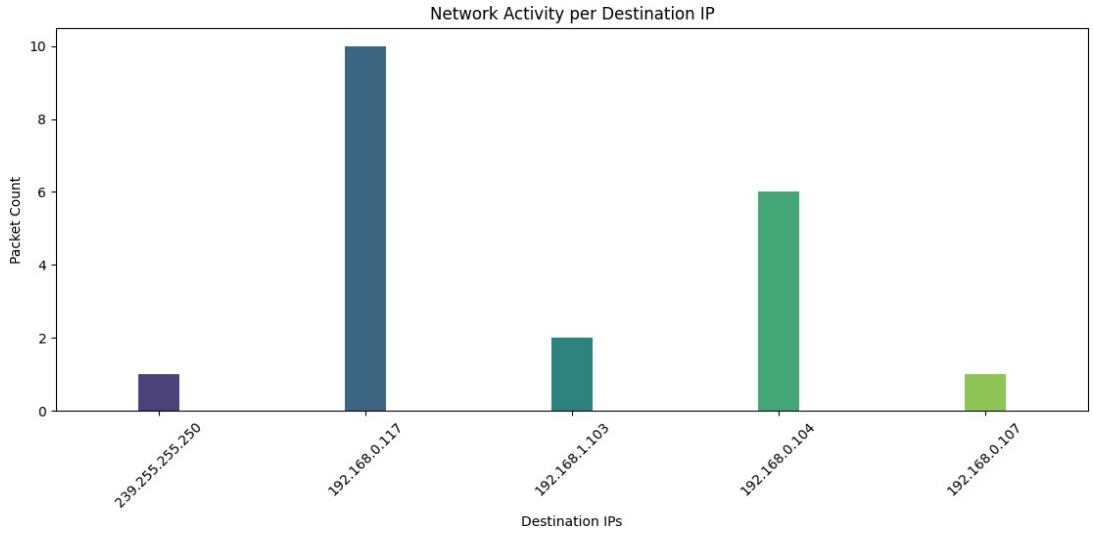

***Fig. 2**: Network activity per target IP based on packet counts.*

This chart of activity levels across an IP destination for a corresponding packet count shows us patterns in traffic flow and helps detect oddities in the network, which will be useful information for network monitoring in real time.

DOI:10.46647/ijetms.2025.v09si01.003 ISSN: 2581-4621

CONCLUSION

This investigation has tried to show how Machine Learning and Artificial Intelligence can be applied to improve attacker behavior analysis in the field of Cybersecurity. In their paper, they successively use the AI-based methodologies to prove the effectiveness of such techniques for threat detection, attacker profiling, and risk mitigation. The focus of the study was primarily on shifting the security postures from being reactive to a predictive stance, diminishing attack surfaces and thus creating a lesser need for response. Significant progress has indeed been made on some of those problems, but there are still issues, such as adversarial machine-learning bias or data bias, that remain outstanding. Future work would therefore focus on building evermore robust AI models, improving data integrity, and exploring adaptive security frameworks that can deal more effectively with new types of threats.

ACKNOWLEDGMENT

Basically, our guide, Mrs. T C Swetha Priya, has our sincere thanks for being there with us in guidance, support and valuable advice throughout this research. We would have profited from her insight in developing our awareness of AI-driven Cybersecurity. Many thanks to each of the co-authors for putting together their joint efforts in the conduction of this study, analysis of findings, and writing of this paper. Also, the collaboration was very much necessary for carrying out this research.

REFERENCES

[1].Tonge, A. M., Kasture, S. S., & Chaudhari, S. R. (2013). Cyber security: challenges for society-literature review. IOSR Journal of computer Engineering, 2(12), 67-75.
[2].Meng, X. (2024). Advanced AI and ML techniques in Cybersecurity : Supervised and unsupervised learning, and neural networks in threat detection and response. Applied and Computational Engineering, 82, 24-28.
[3]. Chakravarty, A. K., Raj, A., Paul, S., & Apoorva, S. (2019). A study of signature-based and behaviour-based malware detection approaches. Int. J. Adv. Res. Ideas Innov. Technol, 5(3), 1509-1511.
[4]. Anand, K., Ganapathy, S., Kulothungan, K., Yogesh, P., & Kannan, A. (2012). A rule based approach for attribute selection and intrusion detection in wireless sensor networks. Procedia Engineering, 38, 1658-1664.
[5]. Poria, S., Cambria, E., Ku, L. W., Gui, C., & Gelbukh, A. (2014, August). A rule-based approach to aspect extraction from product reviews. In Proceedings of the second workshop on natural language processing for social media (SocialNLP) (pp. 28-37)
[6]. G. Martín, A., Fernández-Isabel, A., Martín de Diego, I., & Beltrán, M. (2021). A survey for user behavior analysis based on machine learning techniques: current models and applications. Applied Intelligence, 51(8), 6029-6055.
[7]. Meng, X. (2024). Advanced AI and ML techniques in Cybersecurity : Supervised and unsupervised learning, and neural networks in threat detection and response. Applied and Computational Engineering, 82, 24-28.
[8]. Ghahramani, Z. (2003). Unsupervised learning. In Summer school on machine learning (pp. 72-112). Berlin, Heidelberg: Springer Berlin Heidelberg.
[9]. Nassiri, M., HaddadPajouh, H., Dehghantanha, A., Karimipour, H., Parizi, R. M., & Srivastava, G. (2020). Malware elimination impact on dynamic analysis: An experimental machine learning approach. Handbook of Big Data Privacy, 359-370.
[10]. Aslan, Ö. A., & Samet, R. (2020). A comprehensive review on malware detection approaches. IEEE access, 8, 6249-6271.
[11]. Fang, W., Love, P. E., Luo, H., & Ding, L. (2020). Computer vision for behaviour-based

DOI:10.46647/ijetms.2025.v09si01.003 ISSN: 2581-4621

safety in construction: A review and future directions. *Advanced Engineering Informatics*, *43*, 100980.
[12]. Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. Computer networks, 52(12), 2292-2330.
[13]. Velpula, V. B., & Gudipudi, D. (2009). Behavior-anomaly-based system for detecting insider attacks and data mining. International Journal of Recent Trends in Engineering, 1(2), 261.
[14]. Pattabiraman, K., Healey+2, W., Yuan, F., Kalbarczyk, Z., & Iyer, R. (2009). Insider attack detection by information-flow signature enforcement. Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, Tech. Rep.
[15]. Youssef, A., & Emam, A. (2011). Network intrusion detection using data mining and network behaviour analysis. *International journal of computer science & information technology*, *3*(6), 87.