**AI-Driven Innovations in Cyber Security: Strengthening Malware Detection and Prevention**

Ms. Samiksha Khule, Mr. Yogesh Kumar Sharma, Ms. Muskan Sihare, Ms. Rakhi Arora, Mr. Nitin Dixit

Institute of Technology and Management, Gwalior (M.P)

Samikshakhule.cse@itmgoi.in

**Abstract:**Due to the rise in malware activity that seriously threatens both privacy and security,The quick development of computer networks and users has made security a major problem. To maintain client safety and end\_user security in particular, protecting information from unwanted access is one of the most crucial concerns. Malware is a collection of potentially hazardous templates, proactive information, firmware, or spyware i.e. meant to damage the performance of computer programs, portable, and web-based applications. According to a study, unwary individuals are unable to distinguish between hazardous and benign malware. Computer networks and mobile apps should be designed to recognize dangerous activities in order to protect all parties. There are numerous methods for detecting malware activities that leverage cutting\_edge concepts like artificial\_intelligence, machine\_learning, and deep\_learning.In this work, we focus on methods for identifying and stopping activity related to malware that are based on artificial intelligence (AI). We provide a thorough analysis of the attributes, limitations, and solutions for enhancing the performance of the malware detection technologies available today. Give an in-depth evaluation of the deficiencies of the technology used today for malware detection and suggest improvements. According to our study, there will be major benefits to developing malware detection programs using forthcoming techniques. Understanding this integration will help researchers in their subsequent research on AI. based malware recognition and protection.

Keywords: Artificial\_Intelligence, Machine\_Learning, Deep\_Learning, Malware, Denial of Service(DoS), Supervised and Unsupervised learning

**Introduction:**

Artificial Intelligence (AI) has become a more popular tool for malware detection in recent years. In this sector, artificial intelligence (AI), a broad term that encompasses several Machine Learning (ML) and Deep Learning (DL) techniques, has gained increasing traction. Through the study of data patterns, machine learning algorithms help computers detect and classify malware, while deep learning models—which use intricate neural networks—offer even more advanced analytical and prediction abilities.

Combining these AI-driven approaches, which provide more precise and effective results than conventional methods, is transforming the way malware threats is recognized[1]. The field of artificial intelligence (AI), once known as "initial system intelligence," has origins almost as old as computer systems. In the initial phases of artificial intelligence, machines were predicted to be smarter than humans. But as time has gone on, these desires have frequently appeared to fade into the horizon. In the past, machines have accomplished amazing things. For example, they have mastered chess with extraordinary ability and answered complex problems with impressive efficiency[2]. The process of developing genuinely intelligent systems has been more difficult and time-consuming than first thought, notwithstanding these advancements. There have been several noteworthy turning points in the development of AI, such as advances in problem-solving and playing. Nevertheless, the search for devices that can truly mimic or surpass human cognitive capacities is still ongoing, illustrating both the field's persistent problems and its progress. With every advancement in AI technology, it is becoming more and more evident that, despite our progress, the goal of creating completely autonomous and extraordinarily intelligent machines is still a work in progress, with fresh obstacles and possibilities appearing at every opportunity[3].

**Role Of AI In Cyber Security**

AI has become a crucial component of contemporary cybersecurity, presenting potential as well as challenges[4]. The ability of artificial intelligence (AI) to quickly and effectively analyze massive amounts of data, spot abnormalities, and protect sensitive data and precious resources is what has fueled its adoption across industries and government sectors. AI improves the capacity to prevent security breaches by looking at patterns in behavior and spotting minor signs of possible dangers[5].

Artificial intelligence (AI) systems can be abused, notwithstanding their benefits. The constant conflict between security measures and attackers is caused by cybercriminals who are always changing their strategies to exploit weaknesses in AI defenses. Even though AI can process data at previously unheard-of speeds and offers strong, real-time protection, it continues to be a human-engineered technology that is vulnerable to new and sophisticated threats if it is not updated and improved on continually[6].

AI is becoming more and more important in enhancing security procedures and managing intricate datasets, as demonstrated by recent innovations like Google's Neural Structured Learning (NSL) and other cutting-edge machine learning models[7]. These developments show how AI may improve forecast accuracy and handle complex information flows. But the emergence of AI also emphasizes how cybersecurity procedures must constantly improve and adapt.

In conclusion, artificial intelligence (AI) presents new difficulties even as it plays a critical role in improving cybersecurity by providing quick and continuous threat identification. AI's potent capabilities and strategic, adaptive solutions are now essential for effective security in order to combat the ever-changing strategies used by hackers. To maintain strong defenses in an increasingly complex digital ecosystem, it is imperative to strike a balance between AI's advantages and alert, creative safety protocols[8].

**Intrution-Detection System**

An unauthorized attacker's attempt to interfere with or destroy network systems or sensor nodes frequently referred to as an intrusion. Intrusion Detection Systems (IDS) are used to monitor and defend networks and individual nodes versus malicious activity and unauthorized access in order to resist these threats[9].A security breach can be prevented by using an intrusion detection system (IDS). It works by keeping an eye on all network activity and traffic, evaluating the information to discern between beneficial and detrimental activities, and warning users of any dangers before serious harm is done. The IDS is an essential tool for protecting network integrity and averting disruption because it functions as a proactive surveillance system[10].

Three fundamental components usually comprise an IDS:

**Modules for monitoring:** These parts are in charge of keeping an eye on and documenting happenings on the local and nearby networks. To identify irregularities or unusual activity that can point to a security problem, they monitor resource usage, traffic patterns, and other network-related activities.

**Analysis and Detection Algorithms:** This essential part examines network behavior using sophisticated modeling approaches. The system determines if an action is legitimate or symptomatic of an intrusion by comparing the observed data with known patterns along with potential abnormalities. Accurately recognizing and categorizing risks depends on this analytical approach.

**Alert Mechanism:** When an incursion is detected, this part sends out notifications. The alert mechanism warns users or administrators of potential hazards when it detects suspicious activity. This early warning system makes it possible to safeguard the network and inhibit damage quickly.

Essentially, the main objective of the IDS is to analyze network packets and other data flows in order to detect threats that could be internal or external. Requiring it to distinguish between authorized users and possible intruders is essential to ensuring strong network security[11]. The intrusion detection system (IDS) improves overall network protection by combining extensive monitoring, advanced analysis, and timely warning. This is a crucial defense mechanism against many types of infiltration.

**Types Of IDS:**

Network security is greatly aided by intrusion detection systems (IDS), which use unique techniques to discover and neutralize security threats. The two most common IDS kinds are anomaly-based and signature-based, and each has positive and negative aspects of its own.



Figure 1: Types Of IDS

**Signature-Based intrusion detection systems:**

It use a static methodology, identifying recognized threats through predetermined rules and patterns. The way these systems work is by comparing system behavior or network traffic to a database of threat signatures. The activity has been identified by the IDS as possibly malicious when a match is discovered. Among the many advantages of this strategy are its ease of use and accuracy in identifying known hazards. It often generates fewer false positives due to its utilization of recognized patterns, which lowers the possibility that benign actions would be mistakenly categorized as assaults. On the other hand, the reach of Signature-Based IDS is restricted. It is ineffectual against new or unknown threats unless those patterns are manually added, as it can only identify assaults that have already been recorded in its signature database. Furthermore, it takes a lot of resources and storage space to maintain a large signature database, and regular updates have a responsibility to remain ahead of evolving threats[12].

**Anomaly-based intrusion detection systems:**

Event-Based IDS, another name for anomaly-based intrusion detection systems, employ a dynamic security strategy. These algorithms create a baseline of typical network behavior and keep an eye out for departures from this norm. Anomaly-Based intrusion detection systems use heuristic algorithms to identify anomalous activity that may point to a security breach. This approach is useful because it can detect deviations from predicted behavior that Signature-Based systems could overlook, thereby identifying novel and hitherto unidentified threats[13]. It also learns to handle new usual behavior patterns over time as it adapts. However, there are disadvantages to this strategy. Because natural fluctuations are flagged as anomalies, Anomaly-Based IDS may produce a higher proportion of false positives. It also requires complicated design because it can be difficult to define usual behavior and establish suitable thresholds. The ongoing learning and analysis of network traffic may also result in extra processing overhead, which would affect the performance of the system as a whole[14].

In conclusion, while Signature-Based IDS performs exceptionally well at accurately identifying known threats, it is not as good at identifying novel or unidentified assaults and necessitates continuous maintenance. However, false positives and complicated setup can be a problem for Anomaly-Based IDS. On the other side, by evaluating deviations from usual activity, it offers a valuable tool for spotting unique threats. Using both IDS types can provide a comprehensive and well-balanced approach to network security by utilizing their own strengths to defend against a wide range of cyberthreats.

**Research Areas Of IDS:**

Overcoming research obstacles in the field of intrusion detection is essential to creating efficient systems. IDSs have a number of intricate tasks to do, including as selecting the best detection algorithms, picking the proper data to gather, making sure the system is compatible with current tools, and verifying system performance. Any illegal activity that compromises the confidentiality, integrity, or availability of data is referred to as an intrusion and necessitates close monitoring. An IDS needs to seamlessly integrate with the target environment, be able to react to new threats, and to recognize known ones in order to be genuinely effective[15].

In order to develop IDSs that are useful and effective, addressing these research issues is crucial to enhancing information system security in the long run. By addressing these issues, we can improve IDS efficacy and strengthen defenses against various kinds of cyber threats[16].



Figure 2: Area of Research in IDS

窗体顶端

窗体底端

Here is a refined overview of the key areas in Intrusion Detection Systems (IDS):

**a) Foundations:** This fundamental area focuses on defining the types of intrusions and potential attackers that the IDS aims to defend against. It involves understanding the nature of threats and identifying system vulnerabilities[17].

**b) Data Collection:** This aspect addresses what data is necessary for effective intrusion detection. It covers the methods of data acquisition, the required logging systems, data processing locations, and critical data points to monitor[18].

**c) Detection Methods**: At the heart of IDS functionality, this area involves selecting and refining algorithms to differentiate between legitimate and malicious activities. It includes improving detection techniques and integrating new methods to enhance accuracy and effectiveness[15].

**d) Reporting and Response:** This section deals with notifying administrators or security personnel when suspicious activities are detected[16]. It focuses on creating effective alert mechanisms, developing user-friendly interfaces for manual intervention, and designing automated response solutions.

**e) IDS Environment and Architecture:** Given the complexity of modern computing environments, this area explores how to deploy IDS components effectively across varied systems. It also addresses challenges like monitoring in the presence of additional security measures, such as encrypted connections[19].

**f) IDS Security:** This area focuses on securing the IDS itself against threats. It ensures that IDS components are protected, data handling is secure, and that detection and response functions remain accurate and reliable.

**g) Testing and Evaluation:** This field involves assessing the performance of IDS systems. Challenges include creating suitable test data, defining relevant evaluation metrics, and identifying essential characteristics for different system models[17].

**h) Operational Aspects:** Practical considerations are crucial for end-users, including system maintenance, portability, and upgradability. Ensuring compatibility and interoperability between various IDS modules and systems is also important[20].

**i) Social Aspects:** The implementation of IDSs is influenced by legal and ethical issues. This area examines privacy concerns and the use of IDS performance for forensic purposes, which can impact the widespread adoption of these technologies[20].

**Malware Analysis Approaches:**

Malware analysis provides the foundation for creating practical detection techniques, which is the heart of effective malware detection. It is impossible to create efficient detection methods without first performing a thorough analysis of malware, since this analysis offers vital information on the traits and categories of dangerous files. Three different methods can be used to analyze malware: static, dynamic, and hybrid. Every method is essential for revealing various facets of malware behavior and for constructing a thorough detection system[21].

**Static analysis:** It is a method used to examine potentially malicious files without running them. It involves analyzing the file’s static attributes, such as its code structure, system calls, and control and data flow graphs. By inspecting these elements, static analysis seeks to uncover signatures or patterns that indicate the presence of malware. This approach is highly efficient and minimizes resource consumption, as it avoids executing the file, thereby preventing any potential impact on the system or environment.

However, its effectiveness is limited when dealing with obfuscated malware, which employs techniques to mask its true nature and evade detection. Additionally, static analysis falls short in revealing runtime behaviors, meaning it cannot detect malicious activities that occur only during execution. Despite these limitations, static analysis remains a crucial tool in the malware detection arsenal, often used in conjunction with other methods to enhance overall security[22].

**Dynamic analysis:** Dynamic analysis involves executing a potentially harmful file within a controlled environment, such as a sandbox, to monitor its behavior in real-time. This method provides valuable insights into how malware operates during execution, including its interactions with the system, network activities, and modifications to system files. One of its primary strengths is the ability to detect new or previously unknown malware by observing actual file behavior, which can reveal threats without prior signatures[22]. However, dynamic analysis is resource-intensive, requiring substantial computational power and time to run the file in a sandbox.

Additionally, it often results in a high rate of false positives, as benign activities may be misinterpreted as malicious due to their similarity to harmful behaviors. Despite these drawbacks, dynamic analysis is essential for identifying and understanding unknown threats that static methods might miss[23].

**Hybrid analysis:** Hybrid analysis integrates the strengths of both static and dynamic analysis to offer a more comprehensive malware detection approach. By using static analysis for initial inspection and dynamic analysis for real-time behavioral observation, hybrid methods enhance detection accuracy and reduce the incidence of false positives through cross-validation of findings. This integrated approach improves overall reliability by leveraging the strengths of both techniques.

However, it also presents challenges, such as the complexity of combining two distinct methods and the increased processing time required to conduct both analyses. Despite these challenges, hybrid analysis provides a robust solution by addressing the limitations inherent in each individual method, making it a valuable tool in the quest for effective malware detection[23].

**MalWare- Detection Techniques:**

Malware detection uses a variety of approaches, each geared to identify and combat threats in a unique way. The three main categories of malware detection techniques—behavior-based, heuristic-based, and signature-based—each employ distinct tactics and have pros and cons of their own.

**Signature-based Detection:**Signature-based detection, one of the earliest and most straightforward malware identification methods, relies on a database of known malware signatures—specific patterns like byte sequences, file hashes, domain names, or network activity patterns. This approach involves comparing these signatures against files or network traffic to flag malicious activity when a match is found[24]. Its primary advantages include high accuracy in detecting known threats and a low rate of false positives due to its reliance on precise matches. However, it faces significant limitations, such as its inability to detect new or unknown threats without corresponding signatures in the database, challenges with encrypted or obfuscated malware that may evade detection, and the need for frequent database updates, which can be resource-intensive.

**Behavioral-based Detection:** Behavior-based detection involves monitoring the runtime actions of files or applications in a controlled environment like a sandbox. By analyzing how a file interacts with the system—its actions, system calls, and network activity—this method aims to uncover suspicious or harmful behavior indicative of malware. The primary advantage is its ability to detect new or previously unknown threats by observing real-time behavior, offering insights into malware's operational impact. However, it has notable drawbacks, including high resource consumption due to the need for extensive computational power and time, as well as a higher false positive rate, where benign activities may be mistakenly flagged as malicious[25].

**Heuristic-based Detection:**Heuristic-based detection leverages rules derived from both static and dynamic analysis to identify malware, focusing on the behavior, structure, and other characteristics of files. These rules can be manually crafted by security experts or generated through machine learning techniques. The strength of heuristic-based detection lies in its ability to uncover previously unknown threats by recognizing suspicious patterns or behaviors that signature-based methods might miss. This adaptability allows it to evolve and respond to emerging malware trends[26].

However, it also presents challenges. Developing and managing heuristic rules can be complex, necessitating continuous refinement and expert oversight. Additionally, this method is prone to a higher rate of false positives, as legitimate activities may be mistakenly flagged as malicious if they closely resemble known attack patterns. Despite these limitations, heuristic-based detection enhances overall security by broadening the scope of threat detection beyond established signatures.

**AI Models:**

Numerous AI models are used for malware detection, and as time goes on, neural networks become deeper and deeper. Artificial intelligence models, which include techniques such as supervised, unsupervised, semi-supervised, and self-supervised learning, fall primarily into two categories: Shallow Learning and Deep Learning models[27]. The model selected will rely on the particular requirements and resources at hand. Deep learning models, like RNNs, are perfect for analyzing massive amounts of data, while shallow learning models work well in settings with little processing capability. In order to improve malware detection accuracy and interpretability, experts also investigate cutting edge AI approaches such as Transfer Learning and Explainable Artificial Intelligence (XAI)[28].



Figure 3: AI-Models

**Shallow-Learning Model:**Shallow learning models have been extensively utilized in AI-driven malware detection systems. These models, leveraging their simpler architectures, achieved commendable performance with smaller, labeled datasets, thus avoiding the complexities of deeper neural networks[29][30]. Their effectiveness stems from their ability to deliver strong detection and classification results without requiring extensive computational resources. Research in this domain typically involves deploying various shallow learning approaches and evaluating their comparative performance.

Commonly used models include Random Forest (RF), Logistic Regression, Decision Trees, and Support Vector Machines (SVM)[31]. Tools like the Waikato Environment for Knowledge Analysis (Weka) facilitate the implementation of these algorithms. While shallow learning models provide reliable malware detection, their capabilities are generally less sophisticated than those of deep learning models, which can capture more complex patterns and nuances in the data[32].

**Deep Learning Model:**In the pursuit of more accurate malware detection, researchers have increasingly turned to deeper AI models. Initially, simple Deep Neural Networks (DNN) were employed, serving as the foundation for more complex deep learning models[33][34]. Convolutional Neural Networks (CNN), known for their efficacy in image recognition tasks, have also been adapted for analyzing malware patterns. To address the challenge of continuous malicious activities, models such as Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) networks have been introduced, offering the capability to track and understand sequences of behavior over time. Recent advancements have seen the incorporation of Bidirectional Encoder Representations from Transformers (BERT) into malware detection frameworks.

 BERT, initially pre-trained on vast, unlabeled datasets, is then fine-tuned on smaller, labeled datasets to enhance its ability to classify malware and identify family types. This approach leverages both extensive pre-training and targeted learning to improve detection accuracy[35][36].

**Model Learning Method:**AI models can be trained using a variety of learning techniques, each tailored to different data scenarios and project goals. The primary methods include supervised, unsupervised, semi-supervised, and self-supervised learning.

*Supervised Learning* relies on labeled datasets where each input example is paired with a known output. This method is highly effective for tasks like classification and regression, where the model learns to predict outcomes based on the patterns established from the labeled training data. However, supervised learning can face challenges when the test data significantly diverges from the training set or when labeled data is scarce. The approach's success hinges on the availability of accurate and comprehensive labels.

*Unsupervised Learning* operates without labeled data, focusing instead on uncovering patterns, structures, or groupings within the input data. This technique is invaluable when dealing with complex datasets where labeling is impractical or when labeled data is limited. It excels in tasks such as clustering, where the goal is to identify natural groupings, and dimensionality reduction, which simplifies data while preserving essential features[37].

*Semi-Supervised Learning*merges elements of both supervised and unsupervised learning. It employs a small amount of labeled data combined with a larger set of unlabeled data. This approach capitalizes on the strengths of supervised learning to guide the process while using the unlabeled data to enhance model learning. It is particularly effective for classification and clustering tasks when only a few labeled examples are available.

*Self-Supervised Learning* is a more autonomous technique where models generate labels from the data itself, eliminating the need for external annotations. By training neural networks to predict parts of the data from other parts, self-supervised learning can discover and learn data representations without extensive labeling. This method is ideal for scenarios with large amounts of unlabeled data, offering a powerful solution for tasks requiring substantial datasets but limited labeling[38].

**Intrusion Prevention System (IPS)**

An Intrusion Prevention System (IPS) is a fundamental element in modern network security, delivering essential capabilities that safeguard against a wide array of cyber threats. Here’s why an IPS is indispensable:

**Protection Against Both Established and Emerging Threats:** An IPS excels in recognizing and blocking known threats through signature-based detection. Beyond this, it utilizes advanced detection methods such as anomaly detection and behavioral analysis to uncover and address new, previously unrecognized threats, ensuring comprehensive protection against both familiar and novel dangers.

**Immediate Threat Mitigation**: A key advantage of an IPS is its real-time operational capability. It continuously scrutinizes network traffic as it occurs, enabling prompt detection and interception of malicious activities. This rapid response capability is critical for preventing attacks from gaining a foothold and causing damage, thus maintaining network integrity.

**Regulatory Compliance:** Many sectors are governed by stringent regulations that mandate the use of security systems like an IPS to protect sensitive data. By implementing an IPS, organizations not only fulfill compliance requirements but also strengthen their defenses against data breaches, thereby safeguarding their reputation and avoiding legal ramifications.

**Economic Efficiency**: Investing in an IPS is often more cost-effective compared to the financial implications of a data breach. The costs associated with breach recovery, legal consequences, and reputational harm can far exceed the investment in an IPS, making it a prudent financial decision to prevent such incidents.

**Enhanced Network Insight:** An IPS provides critical visibility into network traffic and activities, offering detailed insights that help in identifying and managing potential security risks. This improved visibility supports better network management and proactive threat mitigation.

Intrusion Prevention Systems (IPS) are classified into four key types, each tailored to address different aspects of security:

**1.Network-Based Intrusion Prevention System (NIPS):** NIPS operates across the entire network, continuously monitoring and analyzing network traffic for signs of suspicious activity. By evaluating protocol behaviors and network communications, NIPS aims to detect and block potentially harmful traffic before it can impact network security.

**2.Wireless Intrusion Prevention System (WIPS):** WIPS specializes in safeguarding wireless networks. It scrutinizes wireless traffic and protocols to identify and counteract threats unique to wireless environments, such as unauthorized access or attacks targeting wireless communication channels.

**3.Network Behavior Analysis (NBA):** NBA systems focus on monitoring network traffic to detect unusual patterns or behaviors that could indicate security threats. This includes identifying anomalies such as distributed denial of service (DDoS) attacks, specific malware, and policy violations by analyzing deviations from standard traffic patterns.

**4.Host-Based Intrusion Prevention System (HIPS):** HIPS is designed to protect individual hosts by monitoring activities and events within that specific host. It examines internal processes and system activities to detect and prevent suspicious actions, offering targeted protection directly at the source.

These diverse types of IPS contribute to a layered security approach, each addressing different threats and vulnerabilities across network and host environments.

**Conclusion:**

The integration of artificial intelligence (AI) into malware detection has marked a significant advancement in cybersecurity, addressing many of the shortcomings of traditional detection methods. AI-driven approaches, particularly machine learning (ML) and deep learning (DL), have revolutionized the detection and prevention of malware by providing more nuanced and adaptive solutions.Shallow learning models, such as Random Forests and Support Vector Machines, offer effective detection with less computational overhead and are suitable for scenarios with limited data. However, the more complex deep learning models, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), excel at handling large datasets and identifying intricate patterns, which are crucial for detecting sophisticated malware. The incorporation of techniques like Transfer Learning and Explainable AI (XAI) further enhances these models by improving their accuracy and making their decision-making processes more transparent.Detection techniques have evolved from traditional signature-based methods, which rely on known patterns, to heuristic and behavior-based approaches that analyze patterns and behaviors to identify novel threats. Hybrid approaches, combining static and dynamic analysis, leverage the strengths of each method, providing a more comprehensive and robust detection system.Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) complement these techniques by monitoring network traffic and providing real-time threat mitigation. IDSs, with their anomaly-based and signature-based approaches, offer varying strengths and weaknesses, while IPSs enhance security by actively blocking malicious activities and ensuring compliance with regulatory standards.Despite these advancements, challenges such as adapting to new threats and minimizing false positives remain. Future research should focus on integrating emerging AI techniques to enhance model robustness, address these challenges, and maintain effective protection in the ever-evolving cybersecurity landscape.

**REFRENCES:**

1. Gaber, M. G., Ahmed, M., & Janicke, H. (2024). Malware detection with artificial intelligence: A systematic literature review. ACM Computing Surveys, 56(6), 1-33.
2. Das, R., & Sandhane, R. (2021, July). Artificial intelligence in cyber security. In Journal of Physics: Conference Series (Vol. 1964, No. 4, p. 042072). IOP Publishing.
3. Chmielewski, M., Wilkos, M., & Wilkos, K. (2010). Building a multiagent environment for military decision support tools with semantic services. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6070 LNAI(PART 1), 173–182. https://doi.org/10.1007/978-3-642-13480- 7\_19.
4. Das, R., & Sandhane, R. (2021, July). Artificial intelligence in cyber security. In Journal of Physics: Conference Series (Vol. 1964, No. 4, p. 042072). IOP Publishing.
5. Ghosh, A. K., Michael, C., & Schatz, M. (2000). A real-time intrusion detection system based on learning program behavior. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1907, 93–109. <https://doi.org/10.1007/3-540-39945-3_7.>
6. Hosseini, R., Qanadli, S. D., Barman, S., Mazinani, M., Ellis, T., & Dehmeshki, J. (2012). An automatic approach for learning and tuning gaussian interval type-2 fuzzy membership functions applied to lung CAD classification system. IEEE Transactions on Fuzzy Systems, 20(2), 224–234. <https://doi.org/10.1109/TFUZZ.2011.2172616.>
7. IOS Press. (n.d.). Retrieved 14 August 2020, from https://www.iospress.nl/book/algorithmsand-architectures-of-artificial-intelligence/.
8. Kotenko, I., & Ulanov, A. (2007). Multi-agent framework for simulation of adaptive cooperative defense against internet attacks. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 4476 LNAI, 212–228. <https://doi.org/10.1007/978-3-540-72839-9_18.>
9. Khule, S., & Sonker, (2020) A. Survey on Intrusion Detection System for various Attacks in IOT.
10. A. Anand, B. Patel, “An Overview on Intrusion Detection System and Types od Attacks It Can Detect Considering Different Protocol”, International journal of Advanced Re- search in Computer Science and Software Engineering, vol.2, no. 8, 2012
11. S. Khan, K.K.Loo, and Z.U.Din,” Framework for intrusion detection in IEEE 802.11 wireless mesh networks,” International Arab Journal of Information Technology,vol.7,no.4,pp.435-440,2010.
12. Neha Maharaj, Pooja Khanna,” A Comparative Analysis of Different Classification Techniques for Intrusion Detection System”, International Journal of Computer Application, 2014.
13. V.Jyothsna,V.V.Rama Prasad,” A Review of Anomaly based Intrusion Detection System”,International Journal of Computer Application,2011.
14. Jayesh Surana, 2 Jagrati Sharma, 3 Ishika Saraf, 4Nishima Puri,5Bhavna Navin,” A Survey On Intrusion Detection System,” International Journal of Engineering Development and Research (www.ijedr.org), 2017 IJEDR, Volume 5, Issue 2.
15. http://www.hcpro.com/HIM-24598-866/Tip-Consider-the-pros-and-cons-of-intrusiondetection-systems.html
16. Ajay Prakash Sahum” An Extensive Survey of Intrusion Detection Systems” International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 06 | June - 2017 www.irjet.net p-ISSN: 2395-0072
17. Hara, K., &Shiomoto, K. (2020). Intrusion Detection System using Semi-Supervised Learning with Adversarial Auto-encoder. NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium. doi:10.1109/noms47738.2020.9110343
18. Usman Asghar Sandhu,” A Survey of Intrusion Detection & Prevention Techniques,” 2011 International Conference on Information Communication and Management IPCSIT vol.16 (2011), PP.1-6.
19. Ou, C.-M. (2019). Host-based Intrusion Detection Systems Inspired by Machine Learning of Agent-Based Artificial Immune Systems. 2019 IEEE International Symposium on Innovations in Intelligent Systems and Applications (INISTA). doi:10.1109/inista.2019.8778269
20. Deng, B., Zhang, X., Gong, W., & Shang, D. (2019). An Overview of Extreme Learning Machine. 2019 4th International Conference on Control, Robotics, and Cybernetics (CRC). doi:10.1109/crc.2019.00046
21. Wolsey, A. (2022). The State-of-the-Art in AI-Based Malware Detection Techniques: A Review. arXiv preprint arXiv:2210.11239.
22. F. A. Aboaoja, A. Zainal, F. A. Ghaleb, B. A. S. Al-rimy, T. A. E. Eisa, and A. A. H. Elnour, “Malware Detection Issues, Challenges, and Future Directions: A Survey,” Applied Sciences, vol. 12, no. 17, p. 8482, 2022.
23. A. Corum, D. Jenkins, and J. Zheng, “Robust PDF malware detection with image visualization and processing techniques,” in 2019 2nd International Conference on Data Intelligence and Security (ICDIS), 2019, pp. 108–114
24. Beaudet, A., Sicard, F., Escudero, C., &Zamai, E. (2020). Process-Aware Model-based Intrusion Detection System on Filtering Approach: Further Investigations. 2020 IEEE. 53 The International Conference on the Industrial Technology (ICIT). doi:10.1109/icit45562.2020.9067195.
25. Brzezinski Meyer, M. L., &Labit, Y. (2020). Combining Machine Learning and Behavior Analysis Techniques for Network Security. 2020 International Conference on Information Networking (ICOIN). doi:10.1109/icoin48656.2020.9016500
26. Sharma, S., Zavarsky, P., &Butakov, S. (2020) Machine Learning based Intrusion Detection System for Web-Based Attacks. 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing (HPSC), and IEEE Intl Conference on Intelligent Data and Security (IDS). doi:10.1109/bigdatasecurity-hpsc-ids49724.2020.00048
27. Tensorflow, Transfer learning and fine-tuning, 2023, https://www. tensorflow.org/tutorials/images/transfer\_learning. (Accessed 15 May 2023).
28. What is explainable AI? 2024, https://www.ibm.com/topics/explaina ble-ai. (Accessed 5 February 2024).
29. What is random forest? 2023, https://www.ibm.com/topics/random-f orest. (Accessed 15 May 2023).
30. What is logistic regression? 2023, https://www.ibm.com/topics/logist ic-regression. (Accessed 15 May 2023).
31. Decision tree, 2023, https://www.geeksforgeeks.org/decision-tree/. (Accessed 15 May 2023).
32. Support vector machine — Introduction to machine learning algorithms, 2023, https://towardsdatascience.com/support-vector-mac hine-introduction-to-machine-learning-algorithms-934a444fca47. (Accessed 15 May 2023).
33. Deep neural network models, 2023, https://developers.google.com /machine-learning/recommendation/dnn/softmax. (Accessed 15 May 2023).
34. What is LSTM? 2023, https://www.mathworks.com/discovery/lstm.ht ml. (Accessed 15 May 2023).
35. J. Devlin, M.-W. Chang, K. Lee, K. Toutanova, Bert: Pre-training of deep bidirectional transformers for language understanding, 2018, arXiv preprint arXiv:1810.04805.
36. A. Rahali, M.A. Akhloufi, MalBERT: Using transformers for cybersecurity and malicious software detection, 2021, arXiv preprint arXi v:2103.03806
37. Supervised vs. Unsupervised learning: What’s the difference? 2024, https://www.ibm.com/blog/supervised-vs-unsupervised-learning/, (Accessed 5 February 2024).
38. Self-supervised learning vs semi-supervised learning: How they differ, 2024, https://analyticsindiamag.com/self-supervised-learning-vs-semisupervised-learning-how-they-differ/, (Accessed 5 February 2024).
39. Chakraborty, N. (2013). Intrusion detection system and intrusion prevention system: A comparative study. International Journal of Computing and Business Research (IJCBR), 4(2),1-8.
40. Wang, Z., & Li, X. (2013). Intrusion prevention system design. In Proceedings of the International Conference on Information Engineering and Applications (IEA) 2012: Volume 3 (pp. 375-382). Springer London.