Available online www.jsaer.com

Journal of Scientific and Engineering Research, 2021, 8(3):264-270

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Machine Learning and AI in Endpoint Security: Analyzing the use of AI and machine learning algorithms for anomaly detection and threat prediction in endpoint security

Sri Kanth Mandru

Mandrusrikanth9@gmail.com

Abstract: Endpoint security has sought to advance its relationship with AI and Machine Learning to improve the estimation and identification of threats and anomalies. The limitation of conventional security models is discussed in this paper. In the modern era of technology, security is changing and multifaceted, and the possibilities of AI-based security models are preferable. In concept separation to enhance the precision of irregularity detection and decrease the number of false positives and negatives, various techniques, such as classifiers, including clusters, ng, neural networks, and support vector machines, are frequently used. Some ways AI subverts endpoint protection are entities that are more aggressive about protection and act faster when faced with a threat. Based on the findings from this study, other notable observations emerge regarding the use of AI and ML in protecting endpoints from future threats.

Keywords: Machine Learning, Artificial Intelligence, Endpoint Security, Anomaly Detection, Threat Prediction

Introduction

Endpoint security, where computers, cellphones, and IoT, among others, cannot be probed or injected with malicious codes, has gained popularity over the years. Endpoints can only be included in an organization if its IT systems are to be protected against intrusions. It does not make sense to use traditional approaches based on the availability of specific malware patterns to combat threats in applications, including modern security threats and those that people have not faced before [1]. That is why threat prediction and anomaly detection have become the focus of attention in fighting cybercrime today.

Anomaly detection implies subscribing to what one might regard as a peculiar pattern or activity that could potentially be a security threat. Threat prediction, going a step further, involves using complex analysis to anticipate and neutralize threats. In the endpoint security context, these procedures have been transformed under the new integration of AI and ML.

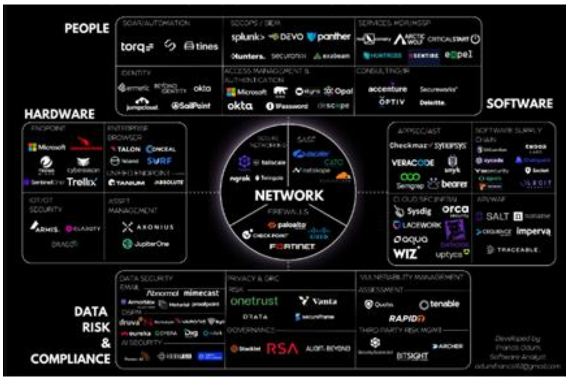

Figure 1: Cybersecurity Ecosystem [1]

A more flexible and effective protection method is the usage of artificial intelligence and machine learning algorithms; these tools work with massive amounts of data at once, and they adapt to the changes to increase their efficiency in identifying new threats. The general purpose of the given work is to emphasize the role of artificial intelligence and, more precisely, machine learning for endpoint security, as well as the patterns and trends to look for in search of signs of threat and potential deviations [2]. Specifically, the article will discuss current challenges, technologies, how these are used, user endpoint security challenges, and future uses of the given technologies. For this reason, this work aims to explain these two aspects of AI and ML and how they are transforming cybersecurity.

Problem Statement

New age threats continuously change, posing great difficulties in endpoint protection for all stakeholders. Using Canvas, the increase of endpoint devices such as smart mobile devices, laptops, and IoT makes them vulnerable targets to hackers. Increased incidences of new and complex threats are putting a lot of pressure on traditional security measures that deal with the use of signatures and rules for detection. As we saw, these methods do not look for patterns that are not known and, therefore, cannot effectively deal with zero-day, let alone APT threats. Because of this restriction, there are potentially much bigger openings that endpoints could exploit.

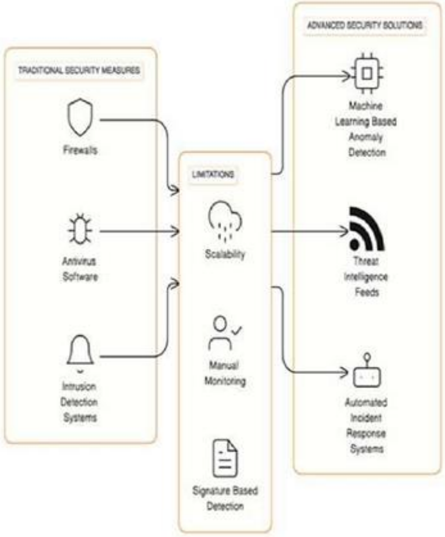
TRADITIONAL SECURITY MEASURES
Firewalls
Antivirus Software
Intrusion Detection Systems
LIMITATIONS
Scalability
Manual Monitoring
Signature Based Detection
ADVANCED SECURITY SOLUTIONS
Machine Learning Based Anomaly Detection
Threat Intelligence Feeds
Automated Incident Response Systems

Figure 2: Traditional vs non-traditional Security measures [3]

The critical facet of endpoint security is comprehending the odd patterns and foreseeing the threats that are likely to occur. However, conventional approaches in these domains may have higher False Negative or False Positive rates. Security analysts could become operationally weary by several false alarms from anomaly detection systems that use rule-based models [3]. On the other hand, they can be blind to small, fluctuating patterns of attacks, and therefore, negative actions go unnoticed, if not until they are disastrous. This is mainly because of the numerous endpoints that create massive traffic and where it becomes difficult to distinguish between normal and malicious 'flows.'' However, these complexity levels are folded with the dynamism and heterogeneity of endpoint settings. They are necessary since all the devices are set differently and used for different purposes. Handling a massive and complicated environment consisting of many endpoints using traditional interventions is nearly impossible due to these strategies' lack of adaptability and scalability. Therefore, there is a need to diversify the approaches that can potentially respond to the new emerging threats. Such issues could also have a remedy in the concept of machine learning and AI. These technologies can improve the case of finding anomalies and predicting threats by leveraging extensive data sets and sophisticated algorithms, which will further enhance the speed and effectiveness of threat identification.

Solution

The practice of endpoint security can be almost completely changed if the application of AI and ML strategies to address the present issues is considered. It is currently possible to get the exact prediction of future threats and considerable data training from such unprecedented technologies [4]. These innovative technologies make it possible for endpoint security to offer more than the superficial layers of protection. They can change over to other new layers once new threats come forward. To summarize, endpoint detection development and optimization heavily rely on some of the most significant algorithms. This one has to appreciate the neural networks' capability, more so deep learning networks of learning complex maps of the given data.

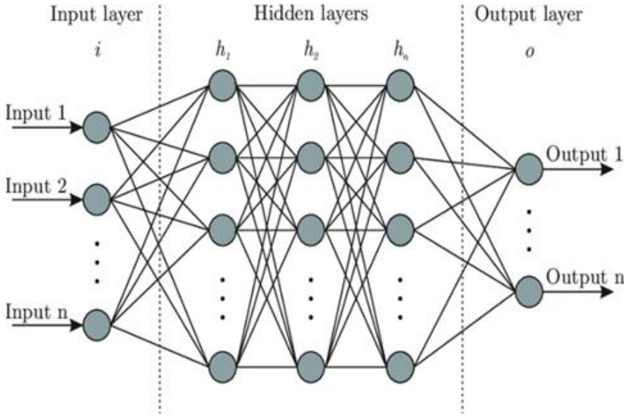

Figure 3: Anomaly detection using Neural Networks [4]

Using these models, the system can grasp the hierarchical representations and pinpoint deviations, which are not recognizable by most other systems that do not possess numerous stages of interpreters. Other threat behaviors better understood and discerned by neural networks are APTs and zero days.

The other essential methods in the AI arsenal include the support vector machines SVMs. Support vector machines work by determining the hyperplane that separates data and forms the top level of the region containing the best class [5]. SVM can decide if the activity in the network is regular or an attack regarding network security, traffic, user behavior, or application usage in the event of endpoint security. Hence, due to their capacity to process high-dimensionality and identify the presence of non-linear relations, they are best used for disentangling complex non-linear interactions.

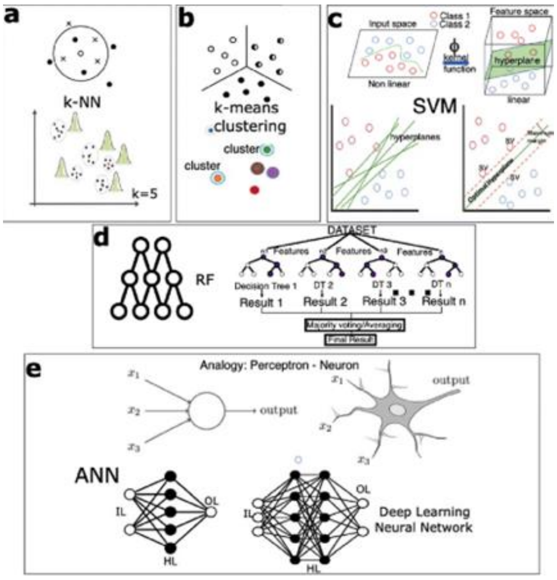

Figure 4: Machine Learning Algorithms [6]

Cluster algorithms include DBSCAN, whereby data and points are grouped according to similarity. These algorithms can be applied to cluster suspicious reports that indicate presently existing security threats. This is because the clustering techniques assist in identifying actual threats as the data is grouped in smaller clusters that minimize noise but enhance the congestion of significant trends [6]. The key to implementing endpoint security is data acquisition and grooming, where many endpoints, logs, traffic, and user activity must be gathered and normalized vastly. Next, the data can be preprocessed to cover the original data in the feature space for examination. That way, the models can prioritize threats since the training and validation datasets contain labeled threats and no room for false negatives or positives. Finally, as the danger is present at all times and can emerge at any time, the usability of the models is thus limited to consistent monitoring and subsequent tweaks. It can be stated that more significant improvements to endpoint protection may be achieved and that these could be made more potent, fungible, and even preemptive when the capabilities provided by AI/ML are harnessed.

Uses

Several security systems have been openly used, such as ML, as proof of connection to demonstrate the capability of the two technologies to improve threat prediction and animation. One example of such a tool is Falcon, which is the CrowdStrike platform that leverages machine learning for the live detection of events for billions of days. The real-time deployment of artificial intelligence algorithms in the Falcon helps minimize the time required to react and improves efficiency in identifying improved threats [7]. Analyzing users' interactions with the system could locate multiple attacks that are not discernible under other conventional models of attacks recognized in signature-based systems. CylancePROTECT, for instance, is a next-gen antivirus that utilizes AI to avoid malware occurrences and halt them beforehand.

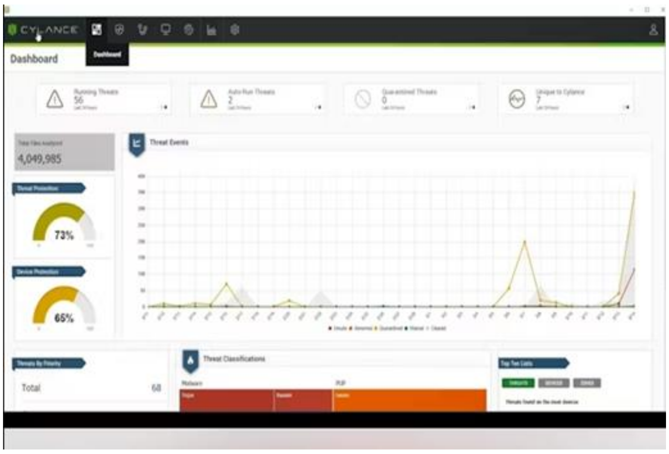

Figure 5: CylancePROTECT machine learning-based endpoint security [7]

CylancePROTECT uses multiple machine learning models, which were trained on many more files containing malware and clean files. Therefore, the system may reveal even new and previously unknown complete felons with several negative qualities. This is the maximum viable protection that stops attacks so that there is no high frequency of change to the signature and update [8]. Another AI product example is Darktrace and the enterprise Immune System, which employs unsupervised machine learning to build the initial blueprint of normal behavior for each endpoint network in an organization. Darktrace can discern shifts in activity that indicate a threat since it is not rigid, preventing it from adjusting to the various characteristics of each environment in which it is being trained. Far from being ineffective, this method has proved proactive in uncovering new malware attackers and insiders and stealthy attacks that traditional methods do not find. It is crucial because it points out how machine learning and artificial intelligence could help make endpoint security better in the practicality of it all [9]. The total result of such technologies is that it makes it possible for enterprises to use methods that may be used to prevent numerous forms of cyber attacks in advance by increasing the probabilities of correct threat predictions and detection of related anomalies, thus improving the general state of cybersecurity.

Impact

Implementing AI and machine learning in endpoint security has significantly boosted threat detection and response. In some of our significant areas of concern, the implemented solutions had a pull-through of increased performance indicators." For example, the CrowdStrike Falcon is a sophisticated security platform that works with Artificial Intelligence and is more precise in identifying threats than the conventional methods;

CylancePROTECT is another example of a sophisticated security solution that uses Artificial Intelligence for this reason [10]. These are very efficient systems that can recognize and eliminate any threat thanks to the capacity of real-time data processing.

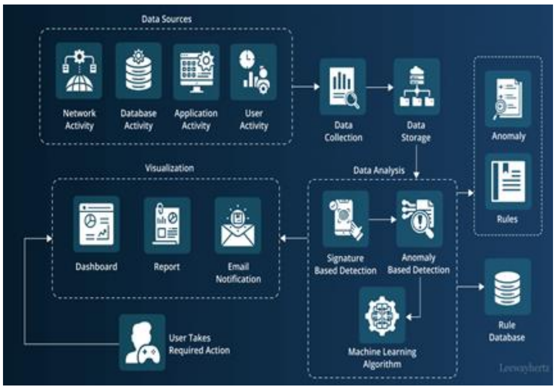

Figure 6: AI implementation in endpoint security [10]

One of the most likely noticeable changes in this respect is reducing false positives and negatives. More so, traditional security measures are associated with several false alarms, which are counterproductive because they cause alert fatigue to the security staff [12]. However, because of this characteristic that makes AI and machine learning able to learn from the sample data that depict normal behavior, it can become more accessible to distinguish between normal and abnormal behavior. As a result of the lowered potential rate of false positives, security professionals can concentrate on actual threats. However, the capabilities of artificial intelligence in learning lower the rate of false negatives because it detects minor signs that are disregarded easily. Many studies have demonstrated that this security application software based on artificial intelligence can identify threats 90% of the time, more than traditional systems [13]. Besides decreasing the work for security personnel, the lack of false positives improves business productivity. Also, threat identification is more effective using machine learning algorithms since it includes the preemptive coverage of openings before they are exploited.

Scope

The industry leaders and vendors suggested that they anticipate seeing more development and growth in the evolution of endpoint security through the assistance of artificial intelligence and machine learning in the coming years. Expanding the current solutions with several advancements, including Explainable AI, Federated learning, and Autonomous response systems, will be possible.

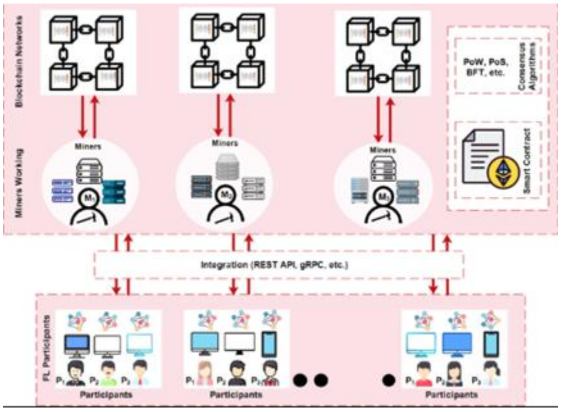

Figure 7: Federated learning in endpoint security [14]

It also differs from other models, such as the broadcasting model, which involves the exchange of data of all the participating devices; federated learning enhances the privacy and security aspects of the development of machine learning across multiple devices due to the learning capabilities of various endpoints [15]. Another crucial field comprises Explainable Artificial Intelligence (XAI), which aims at the possibility of explaining actions performed exclusively by artificial intelligence to the operators. Security practitioners will have more trust and rely more on the AI systems and, as such, be more capable of grasping the alarm given by the AI system. Another technique, lifelong learning, will be increasingly used in critical security applications when the AI models are explained.

Safety in a contemporary building adopting the aesthetics of an AI–styled building In particular, the systems of autonomous response entail that the security processes run simultaneously and autonomously. These systems can quarantine the infected endpoint, stop executing malicious processes, and start the cleanup procedure themselves. This, in turn, reduces the time used to contain attacks and the overall damage the attacks cause. Of these future consequences, one refers to the declared change in the area of cyber security as well as to the frameworks and measures from reactive to more proactive ones [16]. These solutions shall allow its continuous operation throughout the detected real-time danger because discretional rule-based systems came out of the picture instead of artificial intelligence and machine learning-based rule systems. As a result, another shift in cybersecurity rules will be required to cover the use cases of artificial intelligence technologies not only during their deployment but also in terms of the constant training of security staff on those emerging technologies.

Conclusion

Endpoint security has undergone a significant transformation with the integration of advanced solutions such as Artificial Intelligence (AI) and Machine Learning (ML). These technologies have revolutionized threat recognition and containment by their adaptive and proactive capabilities, evident from comprehensive analyses. They empower cybersecurity frameworks with enhanced reaction rates, swiftly identifying and responding to potential threats, thus minimizing the window of vulnerability. Moreover, AI and ML contribute to reducing both false positives and false negatives, crucial for optimizing operational efficiency and focusing resources effectively. The evolving landscape of cybersecurity demands these newer frameworks that continually adapt to emerging threats. AI-based endpoint detection, far from being just ongoing research, ensures sustainability in safeguarding against the escalating complexities of new and existing threats. These intelligent tools, equipped with self-learning capabilities, are poised to become increasingly indispensable in protecting valuable assets. As organizations strive to maintain adequate security measures, the relevance and effectiveness of AI and ML in endpoint security will continue to grow, ensuring robust defense against the ever-evolving cyber threat landscape.

References

[1]. M. Brundage et al., “The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation,” arXiv (Cornell University), Jan. 2018, doi: 10.48550/arxiv.1802.07228. Available: https://arxiv.org/abs/1802.07228

[2]. A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, “A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities,” IEEE Communications Surveys and Tutorials/IEEE Communications Surveys and Tutorials, vol. 21, no. 2, pp. 1851–1877, Jan. 2019, doi: 10.1109/comst.2019.2891891. Available: https://doi.org/10.1109/comst.2019.2891891

[3]. S. Nedelkoski, J. Cardoso, and O. Kao, “Anomaly Detection and Classification using Distributed Tracing and Deep Learning,” May 2019, doi: 10.1109/ccgrid.2019.00038. Available: https://doi.org/10.1109/ccgrid.2019.00038

[4]. L. Liu, O. De Vel, C. Chen, J. Zhang, and Y. Xiang, “Anomaly-Based Insider Threat Detection Using Deep Autoencoders,” Nov. 2018, doi: 10.1109/icdmw.2018.00014. Available: https://doi.org/10.1109/icdmw.2018.00014

[5]. S. Tedeschi, C. Emmanouilidis, J. Mehnen, and R. Roy, “A Design Approach to IoT Endpoint Security for Production Machinery Monitoring,” Sensors, vol. 19, no. 10, p. 2355, May 2019, doi: 10.3390/s19102355. Available: https://doi.org/10.3390/s19102355

[6]. A. Sallam, Q. Xiao, E. Bertino, and D. Fadolalkarim, “Anomaly Detection Techniques for Database Protection Against Insider Threats (Invited Paper),” Jul. 2016, doi: 10.1109/iri.2016.12. Available: https://doi.org/10.1109/iri.2016.12

[7]. S. Nedelkoski, J. Cardoso, and O. Kao, “Anomaly Detection from System Tracing Data Using Multimodal Deep Learning,” Jul. 2019, doi: 10.1109/cloud.2019.00038. Available: https://doi.org/10.1109/cloud.2019.00038

[8]. F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, “Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly,” IEEE Access, vol. 7, pp. 158126–158147, Jan. 2019, doi: 10.1109/access.2019.2948912. Available: https://doi.org/10.1109/access.2019.2948912

[9]. C. Feng, S. Wu, and N. Liu, “A user-centric machine learning framework for cyber security operations center,” Jul. 2017, doi: 10.1109/isi.2017.8004902. Available: https://doi.org/10.1109/isi.2017.8004902

[10]. U. Noor, Z. Anwar, A. W. Malik, S. Khan, and S. Saleem, “A machine learning framework for investigating data breaches based on semantic analysis of adversary’s attack patterns in threat intelligence repositories,” Future Generation Computer Systems, vol. 95, pp. 467–487, Jun. 2019, doi: 10.1016/j.future. Jan 2019.01.022. Available: https://doi.org/10.1016/j.future.2019.01.022

[11]. A. Zappone, M. Di Renzo, and M. Debbah, “Wireless Networks Design in the Era of Deep Learning: Model-Based, AI-Based, or Both?,” IEEE Transactions on Communications, vol. 67, no. 10, pp. 7331–7376, Oct. 2019, doi 10.1109/tcomm.2019.2924010. Available: https://doi.org/10.1109/tcomm.2019.2924010

[12]. R. Beausoleil et al., “Future Computing Systems (FCS) to Support ‘Understanding’ Capability,” Nov. 2019, doi 10.1109/icrc.2019.8914712. Available: https://doi.org/10.1109/icrc.2019.8914712

[13]. L. Cheng and T. Yu, “A new generation of AI: A review and perspective on machine learning technologies applied to smart energy and electric power systems,” International Journal of Energy Research, vol. 43, no. 6, pp. 1928–1973, Jan. 2019, doi: 10.1002/er.4333. Available: https://doi.org/10.1002/er.4333

[14]. E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and Md. S. H. Sunny, “Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review,” IEEE Access, vol. 7, pp. 13960–13988, Jan. 2019, doi: 10.1109/access.2019.2894819. Available: https://doi.org/10.1109/access.2019.2894819

[15]. A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke, and N. Kefalakis, “Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data : Towards End-to-End Security in IoT Systems,” Jun. 2019, doi: 10.1109/giots.2019.8766407. Available: https://doi.org/10.1109/giots.2019.8766407

[16]. S. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P. K. Singh, and W.-C. Hong, “Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward,” IEEE Access, vol. 8, pp. 474–488, Nov. 2019, doi: 10.1109/access.2019.2961372. Available: https://doi.org/10.1109/access.2019.2961372