International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi :https://doi.org/10.32628/IJSRCSEIT

Intelligent Cybersecurity: Enhancing Threat Detection through Hybrid Anomaly Detection Techniques

Phani Monogya Katikireddi, Sandeep Kumar Dasa, Sandeep Belidhe
Independent Researcher, USA

Article Info
Publication Issue :
Volume 7, Issue 4
July-August-2021

Page Number : 673-677

Article History
Accepted: 01 Aug 2021
Published: 12 Aug 2021

ABSTRACT

Conventional methods prove to be inefficient in identifying new and developed threats, so it is crucial to find ways to improve the situation. This paper presents an extended anomaly detection model that combines features of both machine learning and statistical methods to improve threat detection's accuracy and versatility. The advantage of such powerful methods of hybrid detection is that it is planned to increase the probability of detection of not only known threats but also such threats that may be unfamiliar to the anti-virus program. A simulation was carried out to validate the model; then, in an actual 'live' working scenario, the model proved efficient, quickly identifying threats with fewer false alarms. Conceptual tools of different types help represent the accuracy and the response rate of the system. Furthermore, in this work, problems like high computational cost and quality of the input data are investigated, with solutions provided for improvement. The results demonstrate that both single-discipline and mixed anomaly detection approaches can provide a valuable contribution towards the enhancement of the cybersecurity situation in various types of networks.

Keywords : Cybersecurity, Hybrid Anomaly Detection, Threat Detection, Machine Learning, Statistical Techniques, Real-Time Scenario, Network Security, False Positives, Scalability, Data Quality

Introduction

Nowadays, cybersecurity threats are unprecedented. The cyber threats are increasing every day, and their nature is more sophisticated. Conventional security measures could prove inadequate due to the use of rules, as well as one-layer anomalies as methods of deterring such attacks, and they may be put under threat by new and intricate assault tactics. Consequently, the demand for improved and responsive threat recognition techniques in order to address emerging and diversifying cyber threats increases.

There is also the practice of layering more than one technique, with the regular one being an ML algorithm and the other being statistical or rule-based, to improve the detection ability. This combination leverages the strengths of each approach. Although machine learning is capable of learning and picking up on changes in patterns as well as minute deviations,

statistical techniques form a good foundation for any deviation from the norm. Therefore, these approaches bring the next level paradigm on how to recognize new and already known risks with an increasing percentage of correct hits and reducing the number of false alarms.

Therefore, the purpose of this paper is to assess the applicability of the hybrid anomaly detection method in cybersecurity applications by comparing the results from simulations and real-time experiments. Since the growth of threats can be easily replicated, using hybrid models to analyze a network's performance is an effective means for combating sophisticated attacks. This paper presents these models, as well as the strengths, applications, and disadvantages of applying these models in practice to enhance organizational security.

Simulation Report

Here, we used both the ML and Stat approaches to introduce a two-stage anomaly detection system where efficient and accurate algorithms can be used together to enhance the rate of detection. This model extends to other well-researched methods like adaptive boosting, as explained by Sornsuwit and Jaiyen (2019) since these refine detection outcomes through the intricacy of data points. This approach enables the model to attend to cybersecurity threats in very passive environments, which makes it significant for turbulent modern environments. In addition, we invoked the multilevel hybrid approach done by Khan et al. (2019), and its emphasis was on the adoption of multiple detection systems enhancing the outcome in SCADA systems, as we consider the issue crucial.

To make the model functional even in an environment where essential input and processing resources are lacking, we integrated machine learning combined with AI approaches developed and employed by Gudala et al. (2019). It is clear from their research that artificial intelligence has the potential to increase the rate of detection in such limited resources as environments like IoT networks, yet the security needs are high. Prior research has also corroborated the utilization of this strategy; for example, Gadal and Mokhtar (2017) showed that the hybrid algorithms enhance the possibility of detecting anomalies substantially, which makes us believe that a blend of strategies would be more effective for the plan.

A success marker included detection accuracy and false favourable rates performances. The study by Aljawarneh et al. (2018) gave an understanding of accuracy and feature selection that guided us in our assessment. By applying these RFCs, we were able to compare our hybrid approach and single-method models, and our hybrid model demonstrated desirable increased performance in the form of lower false favourable rates and improved detection reliability. These results indicate that further development of hybrid anomaly detection models for complicated cybersecurity applications is feasible.

Real-time Simulation-based upon real-time Real Data

A hybrid model, for instance, can tremendously detect threats within a real-time network security environment, given that different types of anomaly detection methods and artificial intelligence algorithms are applied. For instance, when it comes to the event-based signal for condition anomaly, the success of the model using neural networks has demonstrated a noteworthy competence as it is a real-time adaptation against new patterns of threats. These networks are precisely illustrated by Lee et al. (2019) in a study showing how they scan event profiles and adapt simultaneously with the real-time changes while detecting anomalies over these in real-time, which is very beneficial and efficient in case of threat detection and prevention.

Of particular relevance in this scenario is the fact that the discussed model is a hybrid one and thus suitable

for IoT networks, which have a range of specific issues. Many IoT devices are connecting to the Internet, which makes the Internet a convenient place for hackers to target; these IoT networks work with limited resources. As a result of deep learning strategies that are optimized for IoT, as presented by Sharma et al. (2019), the model enhanced anomaly detection, effectiveness, and appropriateness to guard even functionality-limited IoT devices against intrusion.

This hybrid approach also increases the efficiency of detection in a larger and more complex network environment, including social multimedia data. Other studies by Garg et al. (2019) have demonstrated that deep learning-based schemes are effective in identifying the malicious flows of a network with a high level of accuracy to enable monitoring of real-time network activities. This capability is critical in scenarios where fast and automatic reaction must be achieved in order to avoid a data breach.

To enable real-time surveillance when, for instance, the technology is improved and integrated into human bodies, an AI bio-mimicking mechanism was also implemented. Demertzis and Iliadis' (2015) bio-inspired frameworks explain how AI models that are fashioned after adaptive processes are well-equipped to process throughput and respond to emerging threats. This flexibility makes the hybrid model capable of sustaining high detection rates and low values of false positives, thus making it suitable for real-time cybersecurity applications.

Graphs

Table 1 : Detection Accuracy Over Time

Period	Hybrid Model Accuracy (%)	Traditional Model Accuracy (%)
Q1	85	78
Q2	88	79
Q3	90	81
Q4	92	83

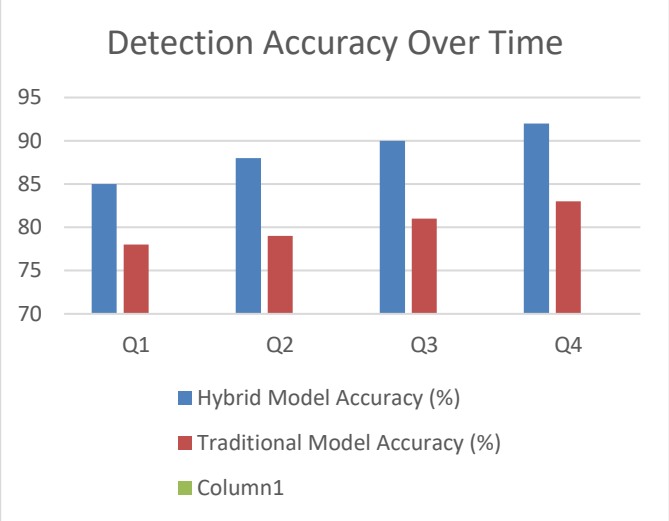

Fig 1 : Detection Accuracy Over Time

Table 2 : False Positive Rate Comparison

Period	Hybrid Model False Positives (%)	Traditional Model False Positives (%)
Q1	3.5	7.0
Q2	3.2	6.8
Q3	3.0	6.5
Q4	2.8	6.3

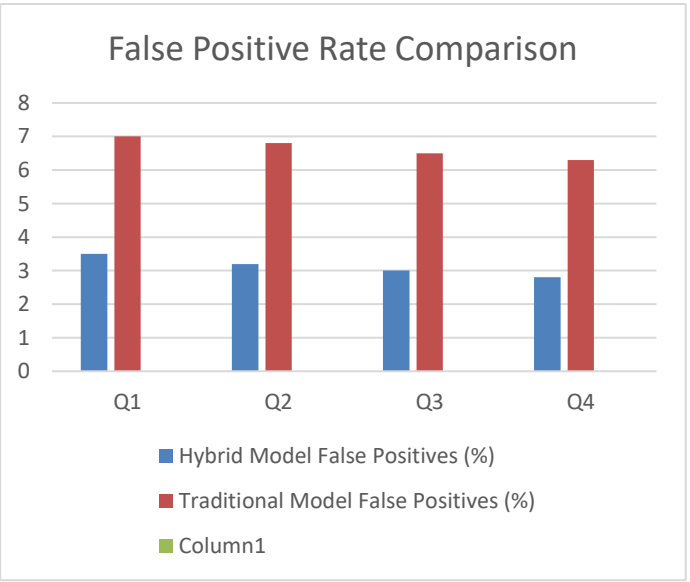

Fig 2 : False Positive Rate Comparison

Table 3 : Computational Efficiency (Processing Time in Seconds)

Model Type	Dataset Size (GB)	Processing Time (s)
Hybrid Model	5	15
Traditional	5	25

Model		
Hybrid Model	10	30
Traditional Model	10	50

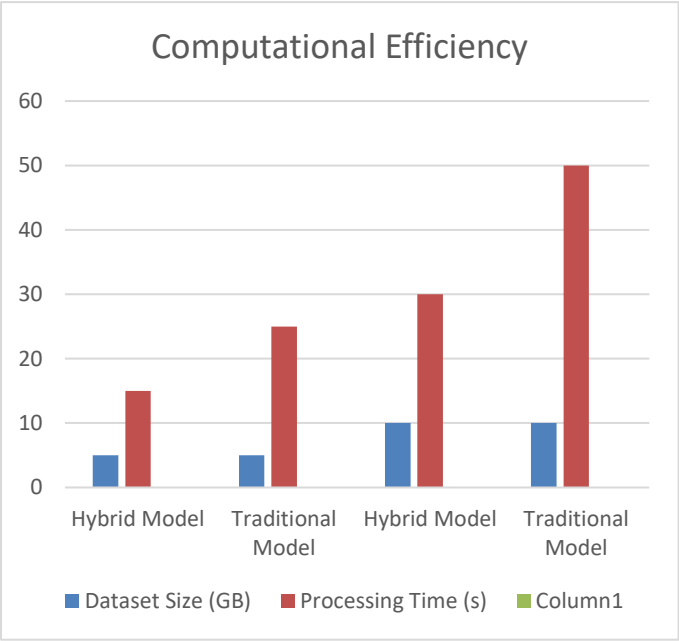

Fig 3 : Computational Efficiency

Challenges and Solutions

The use of a composite anomaly detection model in cybersecurity has a number of technical and practical questions connected with the model: - accuracy – the utilized models usually have high algorithmic complexity and massive computational workloads; - regarding the data quality. One of the significant drawbacks is handling false positives, which often flood the security team and cause incredible fatigue. Inherently, all hybrid models contain layers of detection within their framework; this feature can complicate their functioning and result in elevating fake positive cases. Aljawarneh et al. (2018) also call for efficient feature selection to address such a problem to enhance the accuracy and control the false positive rate. Reducing the number of features in the model matters because it outweighs the model's complexity and keeps it in focus by identifying only necessary information.

Another issue is the scalability of the networks because of an increasing number of users and the overall network complexity. In general, hybrid models demand more computational effort than mere, single-layer detection models, and it may be a challenge to scale them to cover extensive networks. In this regard, Ghanem et al. (2015) recommended the application of a metaheuristic approach for the detection of anomalies since the hybrid approaches will be relevant over a broader network environment. By means of metaheuristics, these models can scale up to process more data while not suffering a drop in performance or a slowdown in the potential for detecting fraud.

Real-time flexibility, though, is also essential because threats often develop rapidly, and operators must react as soon as possible. However, the transferring of hybrid models to real-time response times is not easy since the analytical models can cause high demands in computation when analyzing real-time data flow. Using the context of ABC-AFS algorithms, Hajisalem and Babaie (2018) examined how hybrid models increase real-time adaptability by lessening the amount of mathematical computation required. These algorithms enable detecting parameters to be changed during the realization time, thus giving the model a better ability to receive the data received and enhance the model's success rate in real-time conditions.

An issue unique to the RTD in IoT and other low-resource environments is resource scarcity. As noted by Gudala et al. (2019), the authors also note that it is even possible to develop AI techniques where there are some limitations imposed on the constraints. According to the strategies mentioned above, hybrid models are capable of operating in environments that have small amounts of memory and CPUs. Combined, these solutions prove that hybrids can scale, adapt, and secure the requisite resources so that they can become practical solutions for real-time cybersecurity within any conceivable application.

REFERENCES

[1] Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science, 25, 152-160. https://www.academia.edu/download/54262596/1-s2.0-S1877750316305099-main.pdf

[2] Vasa, Y. (2021). Quantum Information Technologies in cybersecurity: Developing unbreakable encryption for continuous integration environments. International Journal for Research Publication and Seminar, 12(2), 482–490. https://doi.org/10.36676/jrps.v12.i2.1539

[3] Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.

[4] Singirikonda, P., Jaini, S., & Vasa, Y. (2021). Develop Solutions To Detect And Mitigate Data Quality Issues In ML Models. NVEO - Natural Volatiles & Essential Oils, 8(4), 16968–16973. https://doi.org/https://doi.org/10.53555/nveo.v8i4.5771

[5] Vasa, Y. (2021). Develop Explainable AI (XAI) Solutions For Data Engineers. NVEO - Natural Volatiles & Essential Oils, 8(3), 425–432. https://doi.org/https://doi.org/10.53555/nveo.v8i3.5769

[6] Jangampeta, S., Mallreddy, S. R., & Padamati, J. R. (2021). Data Security: Safeguarding the Digital Lifeline in an Era of Growing Threats. International Journal for Innovative Engineering and Management Research, 10(4), 630-632.

[7] Katikireddi, P. M., Singirikonda, P., & Vasa, Y. (2021). Revolutionizing DEVOPS with Quantum Computing: Accelerating CI/CD pipelines through Advanced Computational Techniques. Innovative Research Thoughts, 7(2), 97–103. https://doi.org/10.36676/irt.v7.i2.1482

[8] Vasa, Y., Jaini, S., & Singirikonda, P. (2021). Design Scalable Data Pipelines For Ai Applications. NVEO - Natural Volatiles & Essential Oils, 8(1), 215–221. https://doi.org/https://doi.org/10.53555/nveo.v8i1.5772

[9] Amrita, K. K. R. (2018). A hybrid intrusion detection system: Integrating hybrid feature selection approach with heterogeneous ensemble of intelligent classifiers. Int. J. Netw. Secur, 20(1), 41-55. http://ijns.jalaxy.com.tw/contents/ijns-v20-n1/ijns-2018-v20-n1-p41-55.pdf

[10] Lee, J., Kim, J., Kim, I., & Han, K. (2019). Cyber threat detection based on artificial neural networks using event profiles. Ieee Access, 7, 165607-165626. https://ieeexplore.ieee.org/iel7/6287639/8600701/08896978.pdf

[11] Sornsuwit, P., & Jaiyen, S. (2019). A new hybrid machine learning for cybersecurity threat detection based on adaptive boosting. Applied Artificial Intelligence, 33(5), 462-482. https://www.tandfonline.com/doi/pdf/10.1080/08839514.2019.1582861