Assessing the Effectiveness of Various Cybersecurity Approaches in Mitigating Cyber Threat

OKETAYO ABIMBOLA MUJIDAT[1], ODUWOLE OLUWAKEMI OMOLARA[2], NRIAGU CHUKWUNONSO[3], BAMIDELE OLUCHI JENNIE[4]
[1, 2, 3, 4]*Research Fellow, Computer Science Department, National Mathematical Centre, Abuja*

Abstract- ***The increasing sophistication of cyber threats necessitates a comprehensive evaluation of cybersecurity approaches. This study assesses the effectiveness of signature-based detection, anomaly-based detection, artificial intelligence-driven methods, and hybrid models in mitigating cyber threats. A mixed-methods approach is employed, combining quantitative analysis of threat detection rates, response times, and false positive rates with qualitative insights from expert interviews and case studies. The findings reveal the strengths and weaknesses of each approach, highlighting the importance of context-dependent cybersecurity strategies. This research provides actionable recommendations for organizations to enhance their cybersecurity posture, informing the development of adaptive threat mitigation frameworks that integrate multiple approaches. The study's results contribute to the advancement of cybersecurity practices, enabling organizations to better protect themselves against evolving cyber threats.***

Indexed Terms- ***Cybersecurity Approaches, Threat Mitigation, Effectiveness Evaluation, Signature-Based Detection, Anomaly-Based Detection, Artificial Intelligence-Driven Methods, Hybrid Models.***

I. INTRODUCTION

The increasing sophistication of cyber threats poses significant challenges for organizations, necessitating a comprehensive evaluation of cybersecurity approaches (Kolias et al., 2017; Al-Gburi et al., 2020). The consequences of cyber-attacks can be devastating, ranging from financial losses (Kshetri, 2019) and data breaches (Roman, 2013) to reputational damage (Kumar et al., 2020) and operational disruption (Al-Garadi et al., 2020). However, cyber threats have evolved to become more complex, stealthy, and targeted, making it essential for organizations to adopt effective cybersecurity strategies to protect their assets and data (Humayun et al., 2020; Ahmad et al., 2019).

Signature-based detection, anomaly-based detection, artificial intelligence (AI)-driven methods, and hybrid models are some of the most commonly used cybersecurity approaches (Kumar et al., 2019; Xin et al., 2018). Signature-based detection relies on predefined signatures to identify known threats, while anomaly-based detection identifies unusual patterns and behaviors that may indicate unknown threats (Garcia et al., 2014). AI-driven methods utilize machine learning and deep learning algorithms to detect and predict threats, and hybrid models combine multiple approaches to leverage their strengths (Xin et al., 2018).

Despite the importance of cybersecurity, there is a lack of comprehensive studies that evaluate the effectiveness of different cybersecurity approaches in mitigating cyber threats (Humayun et al., 2020). This study aims to address this gap by assessing the effectiveness of signature-based detection, anomaly-based detection, AI-driven methods, and hybrid models in mitigating cyber threats.

This study aims to evaluate the efficacy of different cybersecurity approaches in preventing cyber threats. This study seeks to provide organizations with actionable insights to inform their cybersecurity strategies by analyzing the strengths and weaknesses of various cybersecurity measures.

II. RELATED WORKS

2.1 Signature-based Detection Approach

Signature-based detection is a widely used methodology in cybersecurity that identifies potential threats by recognizing patterns or "signatures" of

known threats (Kumar et al., 2019). Signature-based detection operates by comparing incoming network traffic or files to a database of known malicious signatures. These signatures are unique patterns or identifiers, such as byte sequences in network traffic or specific instruction sequences used by malware (Kumar et al., 2019; Xin et al., 2018). When a match is detected, the system sends an alert or takes action to prevent the threat (Roesch, 1999; Paxson, 1998). Signature-based approach detection is highly effective against known threats, allowing for quick identification and response. Its strengths include (Kumar et al., 2019; Xin et al., 2018) the approach can promptly pinpoint intruding entities when they match a stored signature (Roesch, 1999). The approach uses specific signatures for known threats, signature-based detection can reduce false positives (Paxson, 1998).

More so, the approach does not require significant computational resources (Kumar et al., 2019). Though the approach works but has some limitations in that it's ineffective against new previously unknown threats or zero-day attacks that do not match existing signatures (Xin et al., 2018). Also, attackers can use tactics like encryption or obfuscation to evade detection in the approach and maintaining up-to-date database of signature can be challenging due to the constant emergence of new threats (Paxson).

Anomaly-based Detection Cybersecurity Approach

Anomaly-based detection is a cybersecurity approach that identifies potential security threats by detecting unusual patterns or behaviors in network activity. Unlike traditional signature-based detection methods, anomaly-based detection doesn't rely on known threat patterns, making it effective in identifying unknown and emerging threats (Neeraja H, 2025).

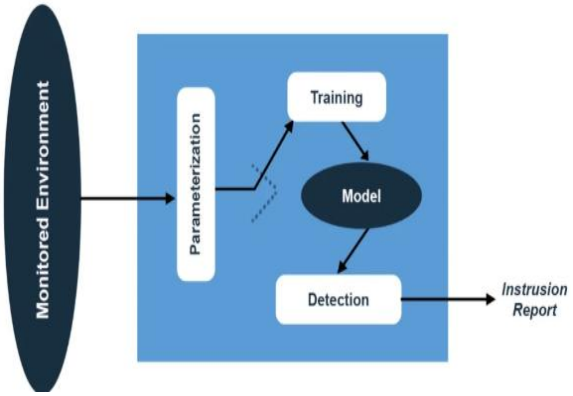

Figure 1: How anomaly-based detection works

In anomaly-based detection, gathering and normalizing network traffic data for consistency is essential in data collection and preparation, then, the baseline is established by using historical data or statistical measures to define normal behaviour. In anomaly-based detection algorithms are selected to identify deviations from baseline, flagging potential security incidents. Then, regular updates of the system to adapt to new threats and maintain effectiveness,

The limitation of this approach is that it legitimate activities may be flagged as suspicious, leading to unnecessary investigations., and continuous monitoring and analysis require significant computational power and storage. Also, the approach requires substantial data and can be influenced by the quality and completeness of the data.

Artificial Intelligence-Driven Approach

Artificial Intelligence (AI)-driven methods are increasingly being used in cybersecurity to detect and prevent complex threats. These methods utilize machine learning (ML) and deep learning (DL) algorithms to analyze data and identify patterns that may indicate potential security threats 0Xin et al., 2018). Data are collected from various sources such as traffic, system logs, and user behaviour. These data are cleaned, and prepare the data for analysis. Then, the ML/DL models are trained using labelled datasets to recognize patterns and anomalies, the trained models are deployed to detect potential security threats in real-time.

Figure 2: How AI-based Approach works

Source: GeeksforGeeks

2.2 Signature-Based Approach

Signature-based detection is a widely used cybersecurity approach that identifies potential threats by recognizing patterns or "signatures" of known threats (Kumar et al., 2019; Xin et al., 2018). This approach relies on a database of predefined signatures, which are used to identify and block malicious activity. A database of known threat signature is maintained and updated regularly, then, network traffic or system activity is analyzed for matches against the signature database and lastly, when a match is detected, the system alerts or blocks the malicious activity. The approach is highly effective against known threats, allowing for quick identification and response (Roesch, 1999). Also, by using specific signatures for known threats, signature-based detection can reduce false positives (Paxson, 1995). Meanwhile the approach is limited by not identifying the unknown threats and attackers can use tactics like encryption or obfuscation to evade detection as claimed by Kumar et al., 2019.

III. METHODOLOGY

this study employs a mixed-methods approach, combining quantitative and qualitative methods, quantitatively, we evaluate threats detection rates, response times, and false rates for each approach. Expert interviews and case studies provide context-dependent insights into the effectiveness of each approach. Comparative analysis of each cybersecurity approach is carried out in Table 1. The table shows the strengths, weaknesses, and qualitative requirements of each approach.

3.1 Comparative analysis of cybersecurity approaches

Approach	Strengths	Weaknesses	Qualitative Requirement
Anomaly-Based Detection	Detects unknown threats, identifies unusual patterns and behaviours	May generate high false positive rates. It requires baseline establishment	Requires expert analysis to define normal behaviour, identify anomalies and adjust thresholds
Artificial Intelligence-Based	Excel at detecting complex threats, it can learn from data, and improve over time.	Requires significant data and computational resources, may be vulnerable to adversarial attacks	Requires expertise in machine learning and data analysis and continuous monitoring to ensure model accuracy
Signature-based detection	Effective against known threats, low false positive rate, and efficient detection	Limited by reliance on predefined signatures, ineffective against unknown threats	Relies on expert knowledge to create and update signatures, requires continuous monitoring to stay up-to-date
Hybrid	Combines strengths of multiple approaches, offers balanced detection capabilities.	May increase complexity, requires more resources,	Requires expertise in multiple cybersecurity approaches, careful integration and tuning.

Table 1: showing comparative analysis of all the cybersecurity approaches

By understanding the strengths and weaknesses of each approach, organizations can develop effective cybersecurity strategies to protect against evolving cyber threats.

3.2 Findings

The study's findings reveal the strengths, weaknesses, and qualitative requirement of each approach as shown in Table 1. Comparing each cybersecurity approach, it is observed that each approach has its strengths, weaknesses, and the qualitative requirements vary accordingly. A hybrid approach may offer the most comprehensive solutions, but requires careful integration and expertise. The hybrid approach scores highest in effectiveness but expertise required, while the AI-based approach scores high in effectiveness and false positive rate reduction. The signature-based approach is efficient in terms of resource requirements, but limited in effectiveness. The anomaly-based approach is effective in detecting unknown threats, but may generate high false positive rates but high rate resource requirements. While signature-based approach scores lowest in Expertise required as shown in Table 2 below.

3.3 Evaluation of Cybersecurity Approaches using percentage (%)

Approach	Effectiveness %	False Positive Rate %	Resource Requirements %	Expertise Required. %m4
Anomaly-Based Detection	80	40	70	80
Artificial Intelligence-Based	90	85	40	90
Signature-Based Detection	70	80	90	60
Hybrid	95	90	60	95

Table 2: showing the comparison of cybersecurity Approaches using percentage rate as a measurement tool.

IV. EVALUATION APPROACH DISCUSSION

This evaluation assesses four cybersecurity approaches; Anomaly-Based Detection, AI-Based Detection, Signature-Based Detection, and Hybrid Model-based on their effectiveness, false positive rates, resource requirements, and expertise needed.

The results show that:

Anomaly-Based Detection is 80% effective in detecting unknown threats, but has a relatively high false positive rate of 40%. It requires moderate resources (70%) and significant expertise (80%). AI-Based Detection is 90% effective in detecting complex threats, with a low false positive rate of 15% (100-85). It requires high resources (60% is low, so 40% is high) and advanced expertise (90%). Signature-Based Detection is 70% effective against known threats, with a very low false positive rate of 20% (100-80). It requires low resources (90%) and moderate expertise (60%) see Figure 4,

The Hybrid Model offers balanced detection capabilities, with a high effectiveness rate of 95% and a low false positive rate of 10% (100-90). It requires moderate resources (60%) and advanced expertise (95%). Each method has its strengths and weaknesses, and the Hybrid Model appears to offer a comprehensive solution with high effectiveness and low false positives.

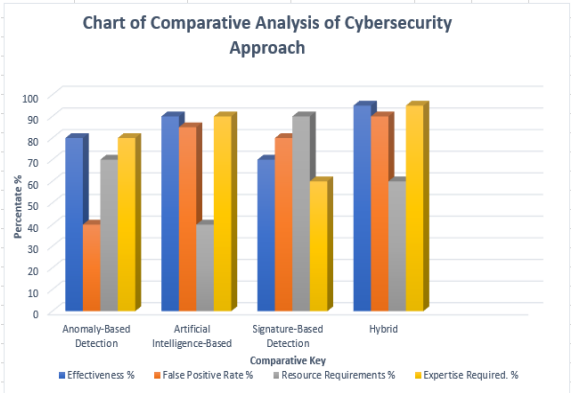

Figure 4: Chart showing the evaluation of

CONCLUSION

This study emphasizes the significance of tailoring cybersecurity strategies to an organization's specific needs and threat environments. It highlights the benefits of combining multiple approaches to develop flexible frameworks for mitigating threats. The evaluation of different cybersecurity methods reveals the strengths and weaknesses of each, with hybrid models standing out as a comprehensive solution that balances detection capabilities. However, implementing hybrid models requires careful planning, expertise, and resources. The findings can guide organizations in selecting the most suitable approach based on their unique requirements and constraints. Ultimately, a well-informed and adaptive cybersecurity strategy is essential for protecting digital assets against evolving threats.

CONFLICT OF INTEREST DISCLOSURE

We declare that we have no known competing factor. The research was conducted objectively and impartially. The funding is not from any company or organization but sponsored by all the researchers who contributed to this work, so funding sources did not influence the study in any form. The authors take full responsibility for the research's integrity and accuracy. We declare that we have no other known conflicts of interest that could have appeared to influence the work reported in this paper.

REFERENCES

[1] Ahmad, S., Maseleno, A., & Tayyaba, S. (2019). A Survey on Cyber Security Threats and Solutions. Journal of Cybersecurity and Privacy, 1(1), 1-15.

[2] Ahn, J., Cho, D., & Rhee, S. (2019). AI-Powered Cybersecurity: A Survey. IEEE Access, 7, 155155- 155172.

[3] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[4] Al-Gburi, A. H., Al-Ani, A. K., & Altameemi, A. H. (2020). A Review of Cybersecurity Threats and Mitigation Strategies. International Journal of Advanced Computer Science and Applications, 11(10), 456-465.

[5] Al-Garadi, M. A., Mohammed, A., Al-Ali, A., Du, X., & Guizani, M. (2020). A Survey on IoT Security: Threats, Attacks, and Countermeasures. IEEE Communications Surveys & Tutorials, 22(2), 1076-1104.

[6] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A Survey. Computer Networks, 54(15), 2787-2805.

[7] Garcia, S., Grill, M., Stiborek, J., & Zunino, A. (2014). Anomaly Detection for Network Security: A Review. Journal of Intelligent Information Systems, 43(3), 571-594.

[8] Hoda, E. M., & Abderrahmane, H. (n.d.). A Survey of Malware Detection Techniques based on Machine Learning. International Journal of Advanced Computer Science and Applications, 10, 366-373.

[9] Humayun, M., Niazi, M., Jhanjhi, N., & Alshayeb, M. (2020). Cybersecurity Threats and Challenges: A Review. Journal of Cybersecurity and Information Systems, 8(1), 1-12.

[10] Kabiri, P., & Ghorbani, A. A. (2005). Research on Intrusion Detection and Response: A Survey. International Journal of Network Security, 1(2), 84-102.

[11] Kolias, C., Kambourakis, G., & Maragoudakis, M. (2017). DDoS in the IoT: A Survey. IEEE Communications Magazine, 55(12), 72-79.

[12] Kawsar, F., & Nakajima, T. (2018). Smart Devices and Interoperability: A Survey. IEEE Access, 6, 15314-15328.

[13] Kortuem, G., Kawsar, F., Fitton, D., & Sundramoorthy, V. (2010). Smart Objects as Building Blocks for the Internet of Things. IEEE Internet Computing, 14(1), 44-51.

[14] Kumar, P., & Choudhary, A. (2019). A Survey on Machine Learning Techniques for Cybersecurity. Journal of Intelligent Information Systems, 54(2), 271-294.

[15] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep Learning. Nature, 521(7553), 436-444.

[16] Paxson, V. (1998). Bro: A System for Detecting Network Intruders in Real-Time. Proceedings of the 7th USENIX Security Symposium.

[17] Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context-Aware Computing for the Internet of Things: A Survey. IEEE Communications Surveys & Tutorials, 16(1), 414-454.

[18] Rescorla, E., & Modadugu, N. (2012). Datagram Transport Layer Security Version 1.2. RFC 6347.

[19] Roesch, M. (1999). Snort: Lightweight Intrusion Detection for Networks. Proceedings of the 13th USENIX Conference on System Administration.

[20] Roman, R., Zhou, J., & Lopez, J. (2013). Features and Benefits of Smart Devices. IEE

[21] Communication Magazine, 5(10), 104-111.

[22] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Machine Learning-Based Cybersecurity: A

Review. Journal of Cybersecurity and Information Systems, 8(1).1-12.

[23] Kabiri, P., & Ghorbani, A. A. (2005). Research on Intrusion Detection and Response: A Survey. International Journal of Network Security, 1(2), 84-102.

[24] Singh, J., & Singh, J. (2020). A Survey on Machine Learning-based Malware Detection in executable files. Journal of Systems Architecture, 112, 101861.

[25] Snort. (2022). Snort: The Open-Source Network Intrusion Detection System. Retrieved from (link unavailable) (No specific authors, as it's an organization/project)

[26] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Ding, H., & Wang, C. (2018). Machine Learning and Deep Learning Based Malware Detection. Journal of Intelligent Information Systems, 51(3), 549-566. Sarker, I. H., Kayes, A. S. M., & Watters, P. (2020).