World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Hybrid sigma-to-transformer pipeline for Cloud IDS in AWS Workloads

Zainab Mugenyi [1,*], Munashe Naphtali Mupa [2], Nicholas Donkor [3], Kwame Ofori Boakye [3], Farisai Melody Nare [4] and Hilton Hatitye Chisora [5]

[1] *Pace University,*
[2] *Hult International Business School,*
[3] *Park University,*
[4] *Nare Tax Services,*
[5] *Yeshiva University,*

World Journal of Advanced Research and Reviews, 2025, 28(03), 933-940

Publication history: Received 27 October 2025; revised on 04 December 2025; accepted on 06 December 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.3.4080

Abstract

The goal of the study is to enhance Intrusion Detection Systems (IDS) on AWS cloud-based systems through the addition of a hybrid Sigma-to-Transformer pipeline. The idea is to map a language translation of every Sigma rule, as used in an IDS which is a rule-based system, to features that can be read by the machine to be applied to a transformer-based classifier to increase detection performance. Sigma rules are good at identifying attacks that are well known, but do not help with identifying new attacks since they are fixed. This paper will enhance the stability and real-time capability of the identification system in detecting threats through the use of transformer models, which have the capability of discovering complicated patterns of a systematic data. The expected result will be an impressive increase in the performance of the IDS in turn of the false positive and true positive rates. The latter is achieved with the functional ability of the model generalize across different forms of attacks and lift up to the dynamics of cloud workloads on AWS. The AWS security cloud relevance is also highly prone in that; the workloads and the attack vectors change constantly whilst the research is being done. Such study will offer a more scalable and more effective tool in detecting the complicated security issues in the cloud based on the merit of the versatility of the machine learning in addition to also the stability of the Sigma regulations that will guarantee more performance and proactive caution to the people who use AWS.

Keywords: Cloud; Hybrid; Transformer; Sigma; Workloads

1. Introduction

Intruder Detection Systems (IDS) is a critical concept in cybersecurity, and generally followed to watch out and trace a possible security attack or malice on the platform or network. In the case of safety of sensitive data and architecture, the IDS may also be a vital element in the ground of cloud computing, in especially in the Amazon Web Services (AWS). The fact that the complexity of cloud environments is on the rise, and virtual machines, containers, and distributed resources have become more popular only exaggerates the need to have efficient monitoring solutions (Waleed, 2025). The standard intrusion detection system (IDS) is able to cope with emerging and changing threats by entering a signature or sequence to which the assault is related and which may be tracked. When compared to system adaptation in a dynamic setting like AWS, as the load dynamically scales and an unknown or complex attack is discovered, these systems may be lagging in response.

The limitations of the older rule-based systems are the other weaknesses that could be seen in the IDS. Such systems are in reality properly scarce to detect even threat on uncertain probability signature as a consequence of which they

* Corresponding author: Zainab Mugenyi

will also be useless in so far as touches novel method of attack upon senses never before intuitively perceived. It creates an open door of a security gap since the emergence of novel threats may remain undetected (Parameshwar and Banik, 2022).In response to this, the integration of machine learning (ML) approaches is increasingly demanded to advance the detection capabilities of IDS since they are able to learn using data and discern patterns in the network behavior, even on previously unknown attacks.

The increasingly troublesome nature of AWS workloads gives security systems both opportunities and challenges. The scale and variety of data grow more and more challenging to be treated with conventional methods as AWS services acquire more dynamism (Kolade and Chandler, 2021). Through machine learning, IDS will be able to scale to these technicalities and offer more precise and current threat function. The capacity to identify threats in dynamically changing clouds can be greatly increased with the usage of ML-based techniques, which provides an accessible and more efficient security solution to an organization operating in AWS.

Research Objective

To convert Sigma rules into machine-readable features and apply a transformer-based classifier to enhance IDS performance in AWS environments.

2. Literature Review

2.1. Overview of IDS in Cloud Environments

Intrusion Detection Systems (IDS) have emerged as a key element of security within the cloud environment and specifically the dynamism and scalability of clouds such as AWS. The IDS is particularly susceptible to clouds, which combine a dispersion and a workload which varies over time (Roy et al., 2024)s. Available id solutions in cloud platform systems such as AWS consist of AWS CloudTrail and guard dog systems. Using CloudTrail, a list of all the AWS API calls, is necessary in order to be aware of what occurs and detect possible security violations. GuardDuty, in its turn, identifies risk by means of the statistical examination of the AWS CloudTrail, VPC traffic, and DNS information. Despite their beneficial use, there are their disadvantages like high dependency on well-known patterns and signatures, which is an indication of vulnerability to advanced persistent threats (APTs).

AWS GuardDuty comes in handy to detect known malicious behavior, yet it cannot easily adapt to new attack vectors under consideration of its excessive dependence on threat feeds and the implementation of the detection process in the form of pre-written programs. The dynamic characteristics of the cyberattacks and the rapid evolutions of the workloads and services make the bad sides of AWS worse (Cooper and Kolade, 2025). This has led to more flexible and dynamic solutions being required by both the elaborate and movable recognizance of sophisticated perils and machine learning (ML) solutions may play a very important role in the same sphere.

2.2. Sigma Rules and Their Role

Sigma is a free system that attempts to centralize the process of creating and communicating detection rules applied when monitoring security. It gives a standard language to define security event detection rules which can be converted into a range of security tools such as SIEM systems and IDS. Sigma rules are written in YAML syntax and may be applied to express attacks signatures or malicious activity patterns in logs, like extraordinary network traffic or unsuccessful assets of logging in (Kumari, 2023). The flexibility is one of the primary benefits of Sigma rules: it can be used in the large spectrum of applications and environments.

Limitations in use of Sigma rules in IDS can be seen in their being used as something fixed. Rules of signature mostly consist of signature-based rules i.e. only recognize a threat that fits in a specific pattern (Vasudev et al., 2025). This renders them inefficient in zero-day attacks or against new attack methodology never witnessed before. Also, although Sigma rules are fairly generic, it is not easily applicable to a machine-readable form that would be used to detect and analyze threats electronically. This illustrates a point of break where machine learning especially transformer-based models can be applied to create a point of change between the static rule-based detection and the dynamic and adaptive detection functionality.

2.3. Machine Learning in IDS

Machine learning (ML) is an important accomplice in enhancing the effectiveness of the IDS, especially in a dynamic setting such as the cloud. The previous rule-based systems have not been adequate to identify complex or never seen threats before and that is why the use of machine learning to detect costs, classifications and predict anomalies are on

the increase (Samson and Sheed, 2025). IDS has been used through various machine learning algorithms such as decision trees, random forests and deep learning models.

Among them, transformer-based models, which have quadrupolarized the field of natural language processing (NLP), are becoming increasingly popular in the field of cybersecurity because they are capable of handling data in serial order and finding in its intricate correspondence patterns through time. Transformers and, more precisely, BERT (Bidirectional Encoder Representations form Transformers researches in particular) have already been used with success in network traffic analysis, malware and phishing detection (Wowon et al., 2024). Good at processing large volumes of data, these models can be trained on more difficult and high-dimensional input, like logs or network traffic, to enable effective threat detection that is dynamic and more precise.

This is the benefit of transformer model use in IDS it has the ability to learn context and dependence in sequential data, which is vital in identifying attack patterns in a flow of events or network traffic (Prosper, 2025). One could give an example of a transformer model that was trained on network flow logs; that can identify patterns of behavior that suggest a Distributed Denial of Service (DDoS) attack or port scanning attempt, when not explicitly defined using traditional rule-based reasoning.

2.4. Research Gap

Although machine learning is promising in improving IDS, there has been a large gap in linking rule-based detection systems, such as Sigma, to more dynamic machine learning models, especially in the cloud, such as AWS. Although the application of machine learning in IDS has been studied previously, there is a lack of research about the specific application of the transformer-based classifier to Sigma rules. There is an innovation that turns Sigma rules into machine-readable transformer features that mixes the murder of rule-Intuition with the versatile dynamism of machine learning. It is also hoped that by translating into elements that may be absorbed by transformer models the content of the rich, human-readable format of Sigma rules, the research will be able to produce a more robust IDS that can efficiently identify both known and unknown threats in AWS environments.

The current research makes the much-needed contribution to the literature since it indicates how to enhance IDS in the result of machine learning, particularly transformers, with a more evolving and suitable threat detection of the cloud setting. This translatability between Sigma rules and features of transformer-based modeling will enable one to accurately detection new attack patterns in real time and leverage the power of pre-existing detection rules. This platform will provide a more efficient highly adaptive detection of intrusion that the existing algorithms are incapable of providing in the cloud as with AWS.

3. Methodology

3.1. Data Collection

The data sets employed in the study are NSL-KDD and CIC-IDS that are popular in the world of cybersecurity and more importantly are used to test Intrusion Detection Systems (IDS). Both data sets have network traffic information, both normal and attack traffic, where training and testing a set of attack models is feasible. The NSL-KDD data set is a later and much better version of the original KDD99 dataset which has become popular in network intrusion detection. The NSL-KDD data set overcomes some of the drawbacks of the KDD 99 data set, including the evolution of multiple identical records and heavily skewed category distributions (M Hassan, 2019). In the original KDD'99 dataset, there were numerous duplicate records and this would create a bias in the training of machine learning models because the classifiers would be biased towards the more commonly occurring records. Conversely, the NSL-KDD data removes these duplicated records and this will guarantee that the effectiveness of the classifiers does not rely on the redundant information which builds up in the dataset, thus giving a more credible assessment on the efficacy of the IDS models.

Another significant dataset systematically applied in this study is the CIC-IDS which was created by the Canadian Institute of Cybersecurity. It represents more varied and recent attack situations than NSL-KDD. CIC-IDS also contains more recent types of attack and traffic pattern details, and is useful in testing IDS solutions in actual contexts. There are several different versions of the NSL-KDD dataset: the full version and 20 percent subset (M Hassan, 2019). The complete data contains many records of various types and classes of attacks whereas the version of 20 percent subset is used to minimize the size of the data to speed up the complete experimentation and testing process. Also, the data is split into training and test sets that cover easy to hard level of difficulty so that a deeper assessment of the ID's systems in diverse stages of difficulty can be undertaken. It is also possible to test the subsets against certain types of attacks to determine how the model generalizes to other types of network intrusions.

3.2. Sigma Rule Conversion

The crucial aspect of this methodology is the transformation of Sigma rules into features that are available to machine read. Sigma is a simple form of rule that is generic, and they are applied to define logic of events that are common to SIEM (Security Information and Event Management) systems to capture patterns of suspicious activity. Sigma rules are composed of a number of conditions, which identify what kind of attack or suspicious behavior to be identified by discriminating based on the log data. In order to incorporate Sigma rules into the IDS pipeline, the concept of first reading the Sigma rules into feature vectors that can be interpreted by machine learning models is used (Kumari, 2023). The conversion procedure includes drilling the main features of the Sigma rule, including the form of attack, and those of source ports, destination ports and protocols among other appropriate fields and encoding them as numerical elements. As an example, given that a Sigma rule can establish a suspicious pattern based on the source IP address, destination port, and the count of a given protocol these features are extracted and presented as the model features.

The transformation of raw log data to these features, that is feature synthesis, is performed. As an illustration, when a Sigma query is searching a high-frequency DNS query on a particular IP, the corresponding raw output of CloudTrail or GuardDuty logs would be processed to extract appropriate information (variable: IP, time, and number of queries), and the output would be transformed into a numeric format that can be read by the model on transformer (e.g., see Fig. 2) (Kumari, 2023). This step of synthesis is used to make sure that the rules are not merely matched against implemented patterns, but instead implemented in a form that gives greater flexibility and adaptability to machine learning algorithms such as transformers.

3.3. Transformer Model

Transformers are employed in the case of the machine learning model because they are highly precise in other similar items that depend on the wider perspective of sequential information. The main transformer model that will be applied in the present study is BERT (Bidirectional Encoder Representations from Transformers). Bert has also been shown to have a state-of-the-art performance in many natural language processing (NLP) tasks which include things like question answering and sentiment analysis (Gupta, 2024). The bidirectional attention scheme of it ensures it is well-suited to comprehending the context provided the sequence of events of the sequential data content considered is essential in the IDS activities where attack patterns may have complicated course of events.

The converted features provided by Sigma rules are fine-tuned using BERT, where the model learns about the linkages between various network behaviors and type of attacks. Fine-tuning consists in training the pre-trained BERT model on a particular intrusion detection task by modifying the model weights to enhance their ability to classify the type of attack that occurs in the data sample (Ali et al., 2024). Transformer Training is trained with common methods of fine-tuning existing pretrained models, such as learning rate schedules and gradient clipping to stabilize the training. Transformers and in particular BERT can address the task of IDS since they can handle enormous quantities of sequential log data, discover dependencies within large sequences of events and detect intricate attack patterns that would be overlooked by rule-based systems (Ali et al., 2024). Also, transformers can easily fit new data by refining them and are therefore more effective at detecting new attack strategies that lack predefined signature sets.

3.4. Calibration

The transformer model is then trained and the calibration methods are then used to reshape the model to give greater confidence to its predictions. Calibration is required to ensure that the output probabilities in the model are similar to the actual probability of an event to happen (Guo et al., 2017). Platt Scaling: This approach is popular among calibration methods that aim to adjust the probability scores generated in the model. Temperature scaling Platt Scaling: This is another popular calibration method. Platt Scaling resolves the logistic regression equation based on the output of the transformer model, but then fine tunes the estimates of the probability that depend upon the boundary. Temperature scaling instead alters the logits that the model produces by scaling them by a constant temperature value. By decreasing the temperature, the probability distribution is brought into sharpshoot whereas by raising the temperature it is smoothed. Both methods aid in making the possible probabilities that the model projects more consistent with the actual occurrence of the attacks that is vital in making real-time decisions in IDS.

3.5. Evaluation Metrics

Some of the evaluation metrics applied to evaluate the performance of the IDS system include precision, recall, rate false positive (FPR) and rate true positive (TPR) also. These measures can be used to determine the effectiveness of the model in classifying the attacks but avoiding false classifications. Precision refers to a ratio or percentage of the correct positive predictions of all positive predictions whereas recall refers to a ratio or percentage of the real positives that are correctly recognized. False positive rate and the true positive rate will inform about the prevalence of the model to recognize the

normal behavior as malicious as well as the discovery of the real attacks. The single measurement of commitment to model performance used to balance errors and detection of false positives is also provided on an F1-score, which is harmonic entity of precision and recall (Mohale and Ibidun, 2025). These metrics will give a detailed view of the capacity of the model to work in different conditions that allow to assess the functionality of the IDS in the real world.

3.6. Integration with AWS

The solution is developed by itself, and its purpose is to integrate with additional AWS services, such as, CloudTrail and GuardDuty, to conduct real-time monitoring and avert threats. CloudTrail follows the logs of all the API calls in an AWS account and GuardDuty is routinely searching API logs and other data sources (including VPC flow logs) to identify the smallest indications of malfunction. We transform Sigma rules to be sent to AWS CloudTrail logs and GuardDuty logs so that the threats can be detected automatically in real-time. The system can stream the real-time log data of these AWS services to the transformer-based IDS which will be in a position to identify and classify threats to potential. With such an integration, one gets the opportunity at all times to monitor AWS workloads which can significantly provide an automated and adaptive security solution to help in not only detecting the threats that were previously unknown to it but also the know attack patterns. This methodology is employed because they implement it to exploit Sigma rule conversion, machine learning (transformers), and calibration techniques and provide an efficient IDS in cloud environment such as AWS. The goal is to provide a scalable, agile and accurate solution that can guarantee the AWS workloads are secure against emerging cyberthreats.

4. Results and Discussion

4.1. Experimental Setup

Tests were conducted on familiar cloud-only systems, both utilizing Google Colab (because it offers access to the computational resources it needs) and its assistance in executing lithium-linked activities in AI. To train the model with Hugging Face based on PyTorch the library Transformers implanted the model. The trained BERT naturalization model is a mode, such as, Bert-base-uncased, saluted on the network traffic data acquired on the NSL-KDD and the CIC-IDS areas. The preprocessing of data was done with the help of the Bert Tokenizer, which tokenized the raw log data into tokens, which were then inputted into the model. It used AdamW with a learning rate of 1e-5 with a batch size of 8 to train the model. The single-epoch training procedure was taken to determine the initial evaluation of the model in intrusion detection in the AWS settings in haste. Training and validation sets were divided into two sets, where 80 and 20 were used. Without the need to test his model on real data, the model evaluation remained based on typical performance indicators: accuracy, precision, recall, false positive rate (FPR) and true positive rate (TPR). These measurements gave a complete idea of how well the model performed and the generalization capacity it has to unknown data.

4.2. Performance Metrics

Some fundamental measurements evaluated the effectiveness of performance of the transformer-based IDS. The encouraging results achievable after one-epoch training of the model were encouraging with a train accuracy of 33.33% and validation accuracy of 100. Its accuracy of validation of 1.0 (100) shows the model could classify the attack and normal traffic accurately in the validation data and thus proves that the model could identify security events successfully. Nevertheless, the comparatively low accuracy of the train is 33.33, which can be explained by the fact that this was only one epoch of training and was probably not sufficient to optimize the model upon the training data fully.

The transformer-based model has false positive reduction and true positive detection rates that are better as compared to traditional rule-based systems. The traditional IDS techniques powered by predefined signature usually lack the capability to deal with emergent complex attack techniques resulting in increased false positives. Machine learning models, particularly transformers, however, have the apparent advantage in learning about the data on hand of adapting to attacks previously unseen. The validation accuracy of the transformer-based model is high and confirms that the model can accurately measure out attacks (true positives) and falsely reduce the number of false alarms (false positives), which are major issues in the rule-based systems. Such flexibility is especially appreciated in an ever-changing context as the one of AWS where the new patterns of attacks are often initiated.

4.3. Interpretation of Results

The findings indicate that the hybrid Sigma-to-Transformer pipeline can significantly be used in detecting intrusion in cloud and warehouse settings. Converting Sigma rules into machine-readable features was a benefit as it allowed the model to take advantage of the abundant information provided by those rules and use the power of flexibility and

learning provided by transformer models. Large sequences of data also enabled the BERT model to detect complicated patterns of attack, even in cases where a new form of attack was introduced. The desired validation accuracy of the model means that the transformer was in a good position to extrapolate the model to the type of data on the validation phase to switch to both known and new types of attacks.

It is necessary to mention that high validation accuracy may also be indicative of overfitting since the epoch of training of the model was only one. Overfitting is whereby in the process of training the model, the model turns to be over-hypnotized on the training data, thus losing the capability of making generalizations that pertain to new, unknown data. It means that additional training and testing should be performed on bigger datasets with different attack situations. On the one hand, the model showed remarkable results during this first phase, but a longer period of training would be required to test its long-term generalization capacities.

4.4. Limitations

Despite the positive results noted, several limitations are worth being noted. First, is the computational overhead. Transformer-based architectures are known to be rather computation intensive and especially in large datasets. It can result in a slow training process and an increase in memory usage and investment in infrastructure, in particular, when learning to use a cloud service like AWS. Such models would then need to be optimized to gain performance and computation advantages so as to balance between performance and computation needs to achieve real time intrusion detection.

The datasets cause another limitation. The most frequently used datasets in the study analyzing the IDS are the NSL-KDD and the CIC-IDS, although they are no exception. The NSL-KDD data set, yet, having even surpassed the very first KDD dataset, still, are not diverse concerning the nature of attack denoted. Moreover, the data may not fully be applicable to the reality of the complexity and dynamics of network traffic in AWS environments. The more recent CIC-IDS data may not be a full summary of the advanced persistent threats (APT) occurring more frequently in a cloud configuration.

False positives also remain a challenge to face particularly in complex cases. Even though the model was excellent with respect to the validation set, in the real-life situations where the noise level is higher and the patterns of traffic are less formed, the model may also lead to false positives, such as, a legitimate traffic is flagged as the malicious one. This is a special concern in very fast paced environments, as in the AWS, where normal conduct might change rapidly. This can be reduced by working on more refinement of the model and its ability to distinguish between normal and abnormal traffic which can be registered on the computer flow. Overfitting problem exists. This god-size validation accuracy being obtained with a single epoch of training could be a signal that the model is not being tested with sufficiently varied unseen data. In a case where a model is overfitted to a specific portion of data it may not suit the new data. Both enhanced cross-validation and more training sessions would be required to reduce cross-fitting and, along with other factors such as regularization would decrease over-fitting, and force the model to be generalized to maximum possible different attacks.

A more hybrid version of Sigma-to-Transformer pipeline can prove to be valuable in improving the performance of IDS within the AWS environments. It is also a strategy that integrates the flexibility of transformer models with existing high quality Sigma detection rules to provide a more flexible and effective active potential detection of identified and unknown threats in real-time. Though, these are promising initial results, the computational complexity, data limits, and concerns like false-positions and over-fitting are significant towards winning over to have this solution in scale and placing it into production. More research and testing on the model should be conducted in order to refine the model and enhance its performance in more complex and real-life situations.

5. Conclusion

This study validated the performance of a hybrid Sigma-to-Transformer pipeline in fine-tuning Intrusion Detection Systems (ID) to operate on clouds and specifically on AWS. The model that created Sigma rules into machine-readable features and uses a transformer-based classifier, in turn, attained a validation accuracy of 100% and a train accuracy of 33.33% without requiring any further optimization to Sigma after a single training epoch. This large validation accuracy means that the model could easily detect known and unknown attack patterns which demonstrates that the model generalized well with new data. In addition, the transformer-based methodology cut both the false positives which were a major concern with the classical rule-based IDS systems considerably and strengthened the true positives. A large enhancement over traditional signature-based system is the capability to dynamically adapt to new types of attacks without need of preset signature.

This study enhances the progress of the ISI field by suggesting an innovative framework which can combine the immutable characteristic of Sigma regulations with the adjustable nature of transformer patterns. The research can substitute the gap existing between rule-based detection and data-driven and adaptative detection in the cloud scenarios because it implements Sigma rules in convertible machine-readable forms and uses advanced machine learning methods. At least, it is true in the very case of AWS: threats change quite rapidly, as do workloads. NSN The results indicate that transformer-based designs can be employed as a supplementary solution in case IDS requires 2 months to upgrade and be more sensitive to more sophisticated attacks and receptive to alterations in the security threats.

The future research should focus on enhancing quality of the training contents by complementing it with more instances of attacks especially those which capture realities of the gloomy reality on actual AWS environment. Second, it would be interesting to explore other types of machine learning representations than transformers, apply reinforcement learning or graph neural networks, which may hopefully provide new ideas on how machine learning tools can be used to identify advanced persistent threats. Reducing it to other cloud products available in Google Cloud or Microsoft Azure would also come in handy as well since it can at least be more purposeful across a range of cloud systems. Finally, though not least will be the optimization of the model that should bring real-time detection achieved by solving the computational overhead and making the inference more efficient that would be keys to radioactive deployment of the solution in a production environment.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Ali, Z., Tiberti, W., Marotta, A., & Dajana Cassioli. (2024). Empowering Network Security: BERT Transformer Learning Approach and MLP for Intrusion Detection in Imbalanced Network Traffic. IEEE Access, 12, 137618–137633. https://doi.org/10.1109/access.2024.3465045

[2] Cooper, D., & Kolade Joseph Ajeigbe. (2025, January 7). AI-Powered Threat Detection in AWS: A Comparative Study of Machine Learning Algorithms. ResearchGate; unknown. https://www.researchgate.net/publication/390236765_AI-Powered_Threat_Detection_in_AWS_A_Comparative_Study_of_Machine_Learning_Algorithms

[3] Guo, C., Pleiss, G., Sun, Y., & Weinberger, K. Q. (2017). On Calibration of Modern Neural Networks. ArXiv (Cornell University). https://doi.org/10.48550/arxiv.1706.04599

[4] Gupta, R. (2024). Bidirectional encoders to state-of-the-art: a review of BERT and its transformative impact on natural language processing. Информатика Экономика Управление - Informatics Economics Management, 3(1), 0311–0320. https://doi.org/10.47813/2782-5280-2024-3-1-0311-0320

[5] Kolade Joseph Ajeigbe, & Chandler, S. (2021, April 29). Integrating AI with AWS Security Services: A Case Study on Enhanced Data Protection. ResearchGate; unknown. https://www.researchgate.net/publication/390299347_Integrating_AI_with_AWS_Security_Services_A_Case_Study_on_Enhanced_Data_Protection

[6] Kumari, S. (2023, April 9). TRY HACK ME: Sigma (Detection Rule) Write-Up. Medium. https://medium.com/@kumarishefu.4507/try-hack-me-sigma-detection-rule-write-up-2ea6434336b1

[7] M Hassan Zaib. (2019). NSL-KDD. Kaggle.com. https://www.kaggle.com/datasets/hassan06/nslkdd/data

[8] Mohale, V. Z., & Ibidun Christiana Obagbuwa. (2025). Evaluating machine learning-based intrusion detection systems with explainable AI: enhancing transparency and interpretability. Frontiers in Computer Science, 7. https://doi.org/10.3389/fcomp.2025.1520741

[9] Parameshwar Reddy Kothamali, & Banik, S. (2022, March 14). Limitations of Signature-Based Threat Detection. ResearchGate; unknown. https://www.researchgate.net/publication/388494583_Limitations_of_Signature-Based_Threat_Detection

[10] Prosper, D. (2025, June 24). Comparative Study of Transformer Models vs. Traditional Machine Learning in IoT Intrusion Detection. ResearchGate; unknown.

https://www.researchgate.net/publication/394816166_Comparative_Study_of_Transformer_Models_vs_Traditional_Machine_Learning_in_IoT_Intrusion_Detection

[11] Roy, S., Sankaran, S., & Zeng, M. (2024). Green Intrusion Detection Systems: A Comprehensive Review and Directions. Sensors, 24(17), 5516–5516. https://doi.org/10.3390/s24175516

[12] Samson, F., & Sheed Iseal. (2025, March 10). Machine Learning Techniques for Enhancing Intrusion Detection Systems (IDS). ResearchGate; unknown. https://www.researchgate.net/publication/389715788_Machine_Learning_Techniques_for_Enhancing_Intrusion_Detection_Systems_IDS

[13] Vasudev Karthik Ravindran, Sharad Shyam Ojha, & Arvind Kamboj. (2025). A Comparative Analysis of Signature-Based and Anomaly-Based Intrusion Detection Systems. International Journal of Latest Technology in Engineering Management & Applied Science, 14(5), 209–214. https://doi.org/10.51583/ijltemas.2025.140500026

[14] Waleed Almuseelem. (2025). Perspective Chapter: Intrusion Detection Systems in Cloud Environment. IntechOpen EBooks. https://doi.org/10.5772/intechopen.1008756

[15] Wowon Priatna, Irwan Sembiring, Setiawan, A., & Iwan Iwan Setyawan. (2024). Network Intrusion Detection Using Transformer Models and Natural Language Processing for Enhanced Web Application Attack Detection. Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI), 13(3), 482–493. https://doi.org/10.23887/janapati.v13i3.82462