AI-Driven Analysis for Network Attacks: Enhancing IDS Alerts and ACL Integration

Nader Shahata
Center for Strategic Cyber Resilience Research and Development
National Institute of Informatics
Tokyo, Japan
e-mail: nader@nii.ac.jp

Hirokazu Hasegawa
Center for Strategic Cyber Resilience Research and Development
National Institute of Informatics
Tokyo, Japan
e-mail: hasegawa@nii.ac.jp

Masahiko Kato
Department of health data science
Juntendo University
Tokyo, Japan
e-mail: m.kato.ug@juntendo.ac.jp

Hiroki Takakura
Center for Strategic Cyber Resilience Research and Development
National Institute of Informatics
Tokyo, Japan
e-mail: takakura@nii.ac.jp

***Abstract*—Due to the widespread deployment of digital systems, and the increasing complexity of cyber threats, it has become crucial to us to secure our resources in computer connected systems. Access Control Lists (ACLs) are fundamental frameworks that govern the authorization and authentication processes that occur in our network. Essentially, ACLs are a set of rules that define users who have permissions to access particular resources. Furthermore, ACLs indicate whether a user's access will be permitted and what specific actions they will be able to perform. Access control lists play a vital role in the security and confidentiality of sensitive information and resources. However, the emergence of artificial intelligence has the ability to transform the process of access control lists which may result in securing our network. When the system manages the network traffic with the generated ACL, it will enable the network analysts to track certain threats first without having to monitor all network traffic. This method will allow for more efficient threat detection and analysis ending up with saving time and resources. In this paper, we will discuss the usefulness of artificial intelligence and its role in generating access control lists and the consequences of using such technology in securing our network.**

Keywords-Access Control List; Cyber Security; Network; Intrusion Detection; Artificial Intelligence.

I. INTRODUCTION

This work is a follow-up to our prior work "AI-based Approach for Access Control List Management", published in the proceedings of SECURWARE2023 [1]. Access control models are crucial components in the field of information security, ensuring that only authorized individuals or entities can gain entry to protected resources [2]. Over the years, advancements have been shifted towards access control systems. One such transformation is the integration of AI and access control models. AI, with its ability to mimic human intelligence and to make informed decisions based on a massive amount of data, can transform the way access control is managed, which will lead to securing our networks in return. When implemented, AI-powered access control lists can provide numerous benefits over the traditional current systems, which include dynamic access management, behavioral analysis, and adaptive learning. These models can have the ability to strengthen machine learning algorithms [8] to analyze and understand network traffic patterns, behaviors and contextual information to make real-time based access decisions. The move from manual ACLs rules to dynamic ones can lead to more accurate and adaptive access control managements. For instance, manual ACLs require human assistance in terms of rules, which are vulnerable to errors and mistakes.

On the other hand, shifting to AI techniques will help in strengthening the security measures and reducing the risks of potential unauthorized access. By learning from historical data, AIs can detect irregular patterns that identify unusual behavior that network analyst would miss. By analyzing historical data and learning from previous patterns, AI models can establish a baseline of normal behavior for users and systems [8]. Any change in the deviation from this baseline can trigger alerts and generate preventive needed actions, helping in mitigating risks and preventing security breaches; ensuring our systems to be safe by minimizing the potential risks of network attacks. This defensive approach to access control is very crucial in today's ever-evolving threat landscape, where traditional manual rule-based systems often fail in detecting sophisticated attacks; ensuring that future arising threats are recognized and dealt with correctly.

Furthermore, AI can significantly improve user experience in access control systems. The reason is with traditional models, users often face cumbersome processes, such as repeatedly entering passwords or providing multiple credentials for different systems.

The purpose of our paper is to propose an architecture that can help increase the organization’s network security by

applying AI to generate countermeasures based on ACL rules. To do so, we will discuss how feasible is AI in generating ACLs when dealing with IDS alerts. We will examine the role that IDS plays in determining potential threats, and how AI can use those alerts provided by IDS to make dynamic and corresponding ACL related rules. We will provide a feasibility on how effective the concept of AI-based ACL systems on enhancing the efficacy of network security operations through automated, context-aware access control mechanisms by the end of this paper.

The remaining of this paper is organized as follows: Section II presents the background, which discusses the current problems that this paper is aiming to solve. In Section III, we presented the Related Works where it shows the previous researches that were conducted on the field. we presented our vision on solving the drawbacks that were discussed in the background Section through an overflow figure in Section IV. The integration and merging of AI with Anomaly detection and ACL will be presented in Section V followed by our architecture proposal in Section VI along with a detailed description of its components. The feasibility of AI in managing ACLs will be shown in Section VII. Section VIII will discuss the assumptions, whereas the challenges and considerations are explained in Section IX. In Section X discusses the importance of AI in generating ACLs. The discussion part in Section XI describes how effective our proposed system can be if it is applied when detecting anomalies and generating ACLs. We end our paper with a conclusion and future work in Section XII.

II. BACKGROUND

By controlling user access and privileges, access control models can have a significant part in guaranteeing the security and integrity of digital systems. There is considerable interest in examining the potential enhancement of access control systems in light of the significant advancements in AI. This background section seeks to give an overview of AI's use in the access control paradigm, as well as its advantages, challenges, and potential future applications. The goal is to obtain understanding of the evolving status of AI-powered technology and its influence on cybersecurity by studying existing literature and industry practices [9].

The existing ACL mechanism has a number of disadvantages that are frequently encountered [14]. For instance, managing an ACL system can be very challenging. The more users, resources, and permissions there are, the harder it is to accurately manage and update ACLs. When the number of users and available resources considerably rises, ACL systems can experience scalability problems. The network administrator in this case will need to maintain a high number of access control entries, which could affect the performance of the network [14]. ACL maintenance calls for constant work and modification. The ACL needs to be manually updated if the environment changes, such as when a new user joins a workplace or when resources are added or deleted. This maintenance work can get tedious, especially in complex systems.

In traditional ACL-based systems, ACLs are inefficient because they only support explicitly declared access controls. For example, if a user has access or permissions that are unique because they belong to both the IT department and the management department, that level of access should be explicitly stated rather than inferred on belonging to both. The requirement to explicitly declare these access controls also has an impact on scalability. As the number of users, groups, and resources increases, so does the length of the ACL and the time it takes to determine how much access is granted to a particular user. Also, ACLs lack visibility because user permissions and access levels can be scattered across many independent lists. Auditing, modifying, or revoking access require testing every ACL in the organization's environment to apply the new permissions [15]. Therefore, we need a system that can deal with the previously mentioned current problems as the cyber-attacks are on the rise of being more sophisticated. The promising machine learning algorithms that are used by AI-based ACL can create wise access control decisions. It can help in dynamically determining access privileges, which involves examining a number of variables such as users' behaviors, and previous historical data [16]. This strategy can improve security by spotting and identifying anomalies.

Reducing the number of generated alerts, improving the capability to handle complex IDS alerts, and reducing the time to respond are still challenging issues for a network analyst working on an Intrusion Detection System (IDS). The reason is most modern IDS systems can generate a large number of alerts, especially in large and complex networks. The volume of these alerts can quickly overwhelm analysts, making it difficult to prioritize genuine threats that require immediate response. Our proposed system will be focusing on managing ACLs for analyzing suspicious traffic and for generating relevant countermeasures. This strategy can improve security by spotting anomalies and abnormal behaviors. Managing ACLs plays a crucial role in doing such tasks. By configuring ACLs properly, suspicious traffic can be filtered out, preventing potentially malicious packets from reaching critical network resources. Therefore, ACLs can help in identifying common attacks that have the ability to compromise the network. By analyzing ACLs on a regular basis in order to mitigate suspicious traffic, the organization's network security posture can continue to improve. ACL management is an integral part of network security because it provides the best way to prevent suspicious traffic from breaching the system. Analyzing ACLs improves the network security posture by allowing network analysts to readjust access control rules, ultimately making the network infrastructure stronger and more resistant to intruders.

Our proposed system will be relying on machine learning algorithms [7] to assist our AI-based ACL to create wise access control decisions. This strategy can improve security by spotting anomalies. AI-based ACLs will be capable of using related data to determine access decisions and generate countermeasures based on the activities of the users and possible risks that may occur when an incident may happen. By considering these generated countermeasures, the proposed system can have the ability to accurately determine the risk involved with each access request and modify access rights as necessary. The reason behind this accuracy is due to the fact that AI-based ACLs can continuously learn from access patterns and modify their decision-making models as necessary.

III. RELATED WORK

As the explosion of the digital network space has simultaneously created new forms and types of cybersecurity threats, developing sophisticated IDS systems is considered a good idea: a system that can identify attacks in real time and counteract them accordingly. Current IDS approaches rely on signature based-detection that are good at identifying known attackers but don't scale to new attack patterns. This is why machine learning and artificial intelligence have been drawn into recent studies because they are able to identify anomalous behavior and enhance IDS's responsiveness in open networks. Among the most prominent new advances in improving the IDS performance is deep learning techniques. Thus, the deep neural network-based IDS model from Zhang et al. (2019) [22] proposes several deep learning-based IDS schemes and evaluate them accordingly. These schemes include: Auto-encoder based schemes, Restricted Boltzmann machine-based schemes, Deep belief network-based schemes, Recurrent Neural network-based schemes, Deep Neural Network-based Schemes and Hybrid IDS schemes. examines several parameters and applied them into auto-encoder based IDS schemes. Their approach was relying on classifying the deep IDS Schemes based on deep learning approach associated within each. They then reviewed how each scheme will apply deep learning methods for the purpose of recognizing various intrusion types.

Similarly, Ali (2024) studied traditional IDS-based ML methods by leveraging the power of Large Language Models (LLMs) and introduces a module named HUNTGPT. Their approach proves that LLMs have the ability to play a role in the next-generation cyber security application [18].

Moreover, Zhang et al. (2019) [12] presented a research one approach called "Automated Synthesis of Access Control". Their developed a system in this paper called EASYACL uses natural language processing to provide users with the ability to create ACL rules without needing to learn complex command syntax. This represents a departure from the existed approaches, as it has the ability to interact with the system in a more intuitive and user-friendly. The extension of their work in was on conversational AI and natural language interfaces itself lies in the use of Eliza, a prototype of AI implemented natural language descriptions into ACL commands. EASYACL is an ACL-specific application and provides multi-platform outputs for devices like Cisco and Juniper.

IV. SYSTEM OVERVIEW

We propose a dynamic AI based Access Control system for solving the problems, which are explained in Section II. Our system involves the integration of AI and generating ACL for improving the network structure in dealing with suspicious traffic analysis [6]. This can lead to generate an efficient countermeasure against future similar attacks. Figure 1 shows an overview of our proposed system, it consists of five phases, which work in a sequential step-by-step order. We will describe details of each phase below.

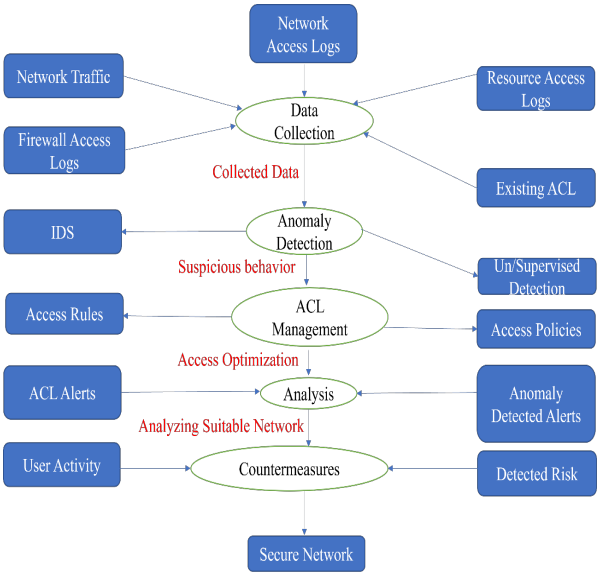

Figure 1. Proposed System Overview

A. Data Collection

This is the first phase, in which the collection of several attributes of data is required [10]. To be specific, we will be focusing on five attributes. These attributes have an edge over other candidates due to their particular concentration on certain aspects of network security. Organizations can improve their capability to identify, address, and avoid security issues by gathering and analyzing data from these sources.

These attributes include network traffic that contains all network traffic data that is observed in the organization's network, e.g., source IP-address and destination IP-address, protocol, source port, destination port. The second attribute is the firewall access logs, which are obtained and stored in

the firewall, e.g., rule numbers, protocols that have been used and the action that is taken by the firewall. The third attribute is the network access logs, (which includes the permissions of allowing or denying users from accessing the network, e.g., the user's name, connection type and connection duration). Then, we have the fourth attribute which is the resource access logs (that determine which resource are allowed or denied for specific users to access with its timestamp, e.g., accessing a financial report by a specific user in 3:00 PM). The final attribute is the applied network ACL that already existed in the system, e.g., source IP-address, destination IP-address, protocol, source port, destination port, and the action that has been taken for that rule. These attributes vary depending on the product and configuration, but are basically above formats. These attributes are all required for the next anomaly detection phase [4].

B. Anomaly Detection

In this phase, the collected data in phase one will be the input to several anomaly detection methods [5]. Currently, a lot of anomaly detection methods exist. With such existing methods, we can detect anomaly behavior from the collected data in phase one. As a typical example, we will consider IDS in detecting anomaly traffic from the network traffic data. Moreover, the applied network ACL and access logs can be used in detecting suspicious activities that are out of the authorized scope access of the network. We chose IDS in our case because it can be adapted to fit the several security configurations and the needs of organizations as well as its effectiveness when combining it with machine learning methods [8]. They can adjust to various network and system designs because of their flexibility. By inputting these data to AI, it can help in deciding whether the unauthorized activity is due to a user's fault or if it is a suspicious access attempt.

C. ACL Management

In the first and second phases, we used the existing techniques. The third phase is where AI will be applied by controlling ACL configurations to keep track of suspicious activities. Generally, this phase is the core of our architecture and is responsible for managing access rules and access policies. It will also be used to examine historical access logs and permissions data to identify patterns and their relationships. It is important to mention that the patterns and security criteria that are found here will introduce optimization algorithms or reinforcement learning approaches to enhance the ACL policy for later effective countermeasures. This will help in adjusting the ACL rules to make the network more efficient and secure.

D. Analysis

In this phase, the network analyst will evaluate the alert outcomes from the detected anomalies (in the second phase) and from the alerts that are generated from the ACL management (the third phase) to obtain a comprehensive understanding of the system security posture [6]. This posture analysis will be the input for the final countermeasures phase.

E. Countermeasures

After the network analyst evaluation, the countermeasure phase with the help of AI will prioritize the alerts and examine the likelihood and potential consequences based on the analysis result. AI will recommend the suitable countermeasures by adjusting ACLs accordingly based on those outcomes. This will help in providing more focus on the targeted resources by adjusting those resources towards the most critical security issues, instead of considering each potential threat as equally important.

V. The AI Merging of Anomaly detection and Generating Access Control Lists

AI helps in access control list (ACL) merging with anomaly identification. ACLs are used to restrict access to resources and systems based on predefined rules, whereas anomaly detection focuses on spotting patterns or behaviors that dramatically depart from the norm [3]. By employing machine learning algorithms [8] to analyze massive volumes of data and spot strange patterns and behaviors, AI can enhance anomaly detection [7].

AI also can play a major role in real-time monitoring IDS alerts. When anomalies (such as unusual traffic patterns, malware or exploited traffic caused be network attacks) are detected, AI has the ability to analyze and examine such patterns and creates specific Access Control Lists (ACLs) to prevent or restrict access according to these incidents.

ACLs, on the other hand, will get evolved and updated very conveniently by the help of AI by learning the network behavior and historic past attack patterns. This will also help in keeping the network security measures in sync against zero-day attacks as well [27].

An AI model may learn what is considered typical behavior and recognize variations that may reveal potential security issues or anomalies by being trained on previous data samples. Identifying unauthorized access attempts and odd system activities will be easier for the network analyst for examining the network's security position. AI can assist in automating the management and enforcement of access restrictions in the context of access control lists. AI algorithms are able to decide what permissions are appropriate for certain users or groups of users by examining user behavior and previous access patterns [6]. This will also simplify the management of ACLs [12], particularly in complicated systems with lots of users and resources. Access control lists and anomaly detection can be used to offer a more complete security solution. AI system's detection of anomalous behavior may result in updates to access control lists (ACLs) to restrict access or notifications for further enquiry. By dynamically modifying permissions based on in-the-moment abnormalities, this integration makes it possible to take a preventative approach to

security, lowering the likelihood of unauthorized access and malicious activities.

Overall, AI can enhance security posture, automate procedures, and increase the effectiveness of permission management in complicated systems by combining anomaly detection and access control lists.

VI. PROPOSED ARCHITECTURE

Before presenting our proposed system in this section, it is important to mention the idea of iteration. Our system is based on the alerts and the generated ACL rules that will be the fundamental concept behind our architecture to work properly. Moreover, it will validate the accuracy and effectiveness when they will be examined by a network analyst. This iterative process helps refine the architecture's performance and will enhance the overall system's output. The proposal of our architecture is as follows.

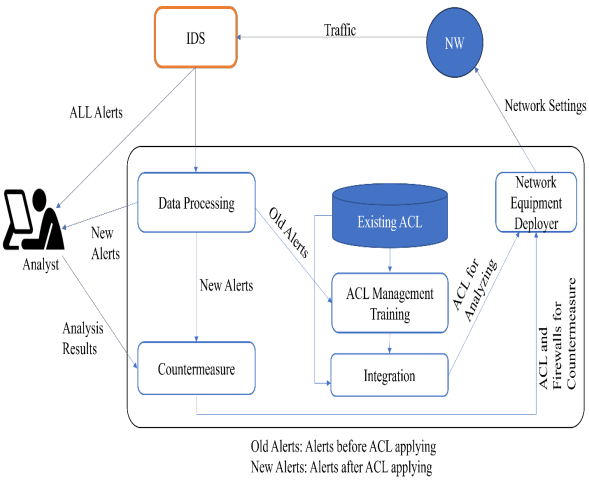

Figure 2. Proposed System

When matching the discussed overflow in Figure 1 with the system proposed in Figure 2, we will notice that the architecture is emphasizing on generating an AI-based ACL rules (phase 3) depending on the alerts from the Intrusion Detection System IDS (phase 2). The analysist (phase 4) will be responsible for monitoring the results of the IDS (phase 2) and regulating the countermeasures (phase 5) when examining the system. Our architecture's components are presented in Figure 2.

A. Data Processing

In this step, the preparation of data will be managed to distinguish the data to two types of alerts: old and new alerts. The old alert refers to the alerts that are initially coming from the IDS; while the new alert refers to the alerts that is coming from IDS after applying AI to the managed ACL. In other words, the system will receive concerning alerts previously due to the fact of being IDS always analyzing the traffic and sending alerts accordingly. Therefore, the input data is a combination of both types of alerts (old and new).

B. Existing ACL

We mean by this a dataset of existing ACLs. These data sets will contain examples of input queries and descriptions along with their corresponding ACL rules. It is worth mentioning that these datasets should cover a wide range of scenarios to train the module effectively.

C. ACL Management Training

In here, the AI model will be adjusted to our processed dataset. The adjustment involves training our module on the ACL rules to make it more knowledgeable and better at generating relevant ACLs. Some machine learning approaches are needed to train the model at this stage.

D. Integration

This step is the result of the combination between the existing ACL and the ACL management training unit. The integration will be beneficial for well training the system to new rules and as a result adapting to newly upcoming permissions. This will also help in optimizing the system's countermeasures.

E. Network Equipment Deployer

The countermeasures (phase 5) that were generated by the alerts of the IDS will be shared with the results of the newly integrated AI-ACL rules. The deployment process will help in generating flexible ACL rules that will be able to deal up with changes that may occur to the network.

F. IDS

Intrusion Detection Systems will include analyzing patterns and behaviors within our system to identify abnormalities from the norm. It will generate alerts when detecting unusual or suspicious actions. These alerts are usually based on pattern recognition techniques but as within our system it will be enhanced with the machine learning approach [7]. In our system, the IDS will be generating alerts when it finds activities that fall outside the predefined threshold.

G. Countermeasure

This phase plays a key role in our case. They help in dealing with alerts that the network analyst handles in order to stop or reduce threats impact on the network. These actions include stopping malicious IP-address, changing firewall settings and letting network analysts know the possible threats to deal with them effectively.

VII. FEASIBILITY OF AI IN MANAGING ACL

We implemented another system to verify the feasibility of AI in generating effective ACLs based on processing IDS alerts and we named it Snort IDS Alert Analyzer. The Snort IDS alert Analyzer provided in Figure 3 demonstrates the significance of reliability of GPT (Generative Pre-trained

Transformer) in achieving promising results [18] when dealing with the components of the proposed system architecture that was discussed earlier. By ensuring that alerts are consistently generated, perceived, processed, analyzed and acted upon, the snort IDS alert analyzer contributes into the operations of the proposed system architecture in: IDS alerts handling, receiving, forwarding, reading, processing and ACL management. The consistency between snort IDS alert analyzer and the proposed system is initially seen in the output visualization in Figure 4. We used streamlit a python framework web application [17] and combined it with one of AI models to automate and enhance the performance of analyzing and responding to IDS alerts. This section examines the feasibility of using AI in the Snort's IDS Alerts and how effective it is in analyzing and generating ACLs. The test was conducted using GPT-2 model in its XL (Extra Large) variant, because large language models are often ideal for natural language processing tasks [18]. The other reason of deploying GPT-2 XL is because it has a larger model size and was proven for effectively handling longer text generation tasks. Although newer models have been developed with other advantages such as vastly larger parameter sizes, our initial testing shows that adopting GPT-2 XL is reliable and can assist in our specific use case [21]. Additionally, our code uses, the transformers library with the GPT-2 XL model, along with its tokenizer and language model aiming to perform a text generation output from snort's IDS alert input.

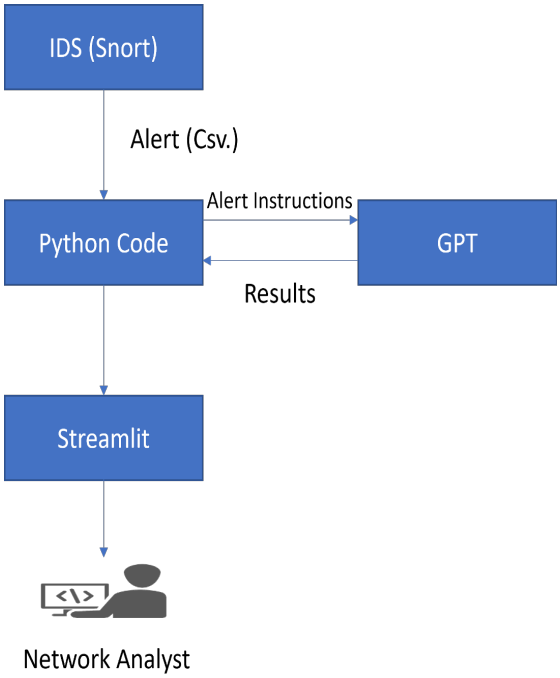

Figure 3. Snort IDS Alert Analyzer Design

Figure 3 demonstrates an organized task management of Snort IDS alerts. The workflow from alert reading to result displaying is closely controlled and firmly managed according to the modular task approach, promising a smooth handling of the task deployment [20]. The tasks are broken down into smaller tasks. Our approach enables the tasks to be divided into four instruction parts and then the python code incorporates these steps into a Streamlit app giving network analysts the chance to see and engage with the analysis and responses through an easy-to-use interface. These instructions are:

- Read Alerts: Getting snort IDS alerts from csv. file.
- Analyze Alerts: Identifying the severity level (high or low) for each alert and which ACL action rule will be associated with that alert.
- Generate Blocking Reasons: Providing a reason for blocking an IDS alert if GPT founded it suspicious.
- Generate Details: Displaying the alerts, the taken action and the blocking reasons.

The snort IDS alert analyzer mechanism relies on reading IDS alerts generated by Snort from a csv. file, and then analyses the severity and generates an ACL action response accordingly. If an alert that has some features such as indications of attack is considered critical, the system automatically blocks that IP address that is associated to the alert. AI will then recognize and analyze how severe the coming alert is and will generate a corresponded ACL rule.

- If the alert has a high severity with a deny ACL rule; AI will take an automated action by blocking the IP-address that is associated with that alert.
- If the alert has a low severity with an allow ACL rule; AI will let that connection pass without further action taken. The passed alerts will be manually reviewed by human analyst later if there is a need for further investigation.

Figure 4 shows the output when dealing with a Cross-site Scripting (XSS) alert and how does AI react to this alert. The reasons we believe this part of the implementation is feasible are primarily to its modular design and to the use of models beside streamlit [17]. GPT-2 is used on the explanation generation module for clear and contextually fluent reasons for the purpose of analyzing and taking security actions. It is clear that using AI (GPT-2 in this case) to automate the generation of ACLs from Snort IDS alerts is very promising.

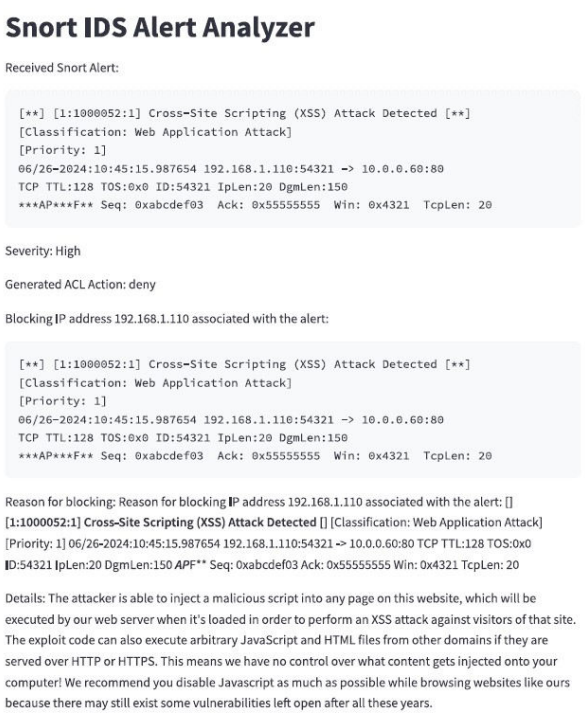

Figure 4. AI output example for ACL Management

The AI ability to deal up with complex sets of data, identify emergent patterns, and dynamically respond to changing threats can dramatically enhance network security operations, both in terms of speed and effectiveness. More tests are essential to evaluate the system in order to make it robust and versatile. Therefore, real network data should be used to test our system. The tested data should contain several IDS alert types and in various scenarios. By doing so, we can analyze the alerts behavior in different and more dynamic network environments. To check that, we can test it with as many alerts as we can, in order to optimize the processing techniques and the model's performance to work with a huge number of alerts at once (i.e., high-throughput scenarios). With all the tests we've run so far, we can also improve the interface, as well as add new features such as customized rules to handle what to do with each alert and other filtering options. Moreover, additional research should be conducted to boost performance, reliability and scalability, and to enable successful integration with the proposed system. This approach improves the efficiency of security operations, and infuses machine-learning insights into decisions to further enhance network defenses against the growing sophistication of cyber-attacks [19].

There are several assumptions to take into consideration when implementing our system. It is expected that our system will continuously fine-tune their behavior to match changing patterns and trends. In order to securely facilitate efficient anomaly detection and access control lists are primed to update based on new instances, and access-control policies are allowed to be finetuned over time.

Snort IDS alert analyzer uses the GPT-2 XL model and tokenizer from the Hugging Face Transformers library [21], and is designed to be run in a Streamlit environment (a library for developing interactive web-based interfaces) [17], which is a suitable environment to deal with a large number of alerts, where the alerts need to be processed in a more complex and a mission-critical style.

Furthermore, The IP-address format used in our system is IPv4, when the alert format changes by using IPv6 incorrect results will be generated as we have not tested this format in our case.

VIII. ASSUMPTIONS

Several assumptions have to be taken into consideration for a successful design, implementation, and analysis of the proposed system.

When implementing the system, we assume that computational resources will be available to be deployed for real-time alerts analyzing as well as to processing power. The system's performance results will be inaccurate if the available hardware is not properly maintained. We are emphasizing here about the need for continuous monitoring and probably upgrading the system's hardware so it will operate optimally when dealing with under heavy alerts load.

Another important assumption is regarding the accuracy and quality of the data that are fed into the system. The data here should be pre-processed and set according to the standards in the system. Inaccurate or distorted IDS format will lead to errors during the alert detection process, which will cause a manual interference to handle these errors effectively. We are stressing here on the importance of a well-defined information to ensure that the input data that enters the system is clean, structured, and free from noise that would impact the anomaly detection and access control management phases.

We assume that the AI model used in the proposed system will continuously learn and improve over time. The AI is therefore expected to treat the new alerts processed, as well as new countermeasures to be applied, as additional sources of education, reformulating its rules and ACLs dynamically in response to an evolving security threat landscape. This assumption is largely critical, as the network environment is always changing, new attack vectors come into the picture, and the system is to respond and readjust features in order to remain effective against emerging threats.

IX. CHALLENGES AND CONSIDERATIONS

The data we use in the Snort IDS Alert Analyzer shown in Figure 4 have a significant impact on how effective AI can be when implemented on the proposed system. In our case

we initially dealt with, GPT model [21], snort IDS alerts and ACLs as essential components to our system. However, to enhance the efficiency in our system; additional components are required. The dataset we used are considered to be sufficient but it should be extended and improved to get a better system performance. The needed data are in terms of continual, unbiased and contextually relevant anomaly detection and response creation [13]. Integration of these dataset will enable a much more refined and accurate analysis, which will lead to a greater resilience and reliability of the system as a whole.

False positives and false negatives are also possible [4]. Systems for detecting anomalies can produce false positives (which considered an indication of a network threat, when actually there is no threat exists), and false negatives (which it is an indication of no network threat, when actually there is a threat exists).

This puts greater demands on the complexity of the training datasets and, in turn, the sophistication of adversarial scenarios. This makes model development more difficult, and potentially expensive in terms of the computational resources required and the domain expertise needed to devise appropriate scenarios. To make the AI components such as GPT-2 more resilient to adversarial attacks, what is really important is to include adversary training to provide counter-examples during the training phase of the model; input validation ensures that the inputs are clean, e.g., they are in the expected format.

As most traffic communications are becoming encrypted to ensure user privacy and security, attackers have also started using encryption to mask their malicious activities, making it hard for security systems to detect and for network analysts to mitigate. Encrypted traffic does not follow the traditional analysis methods in inspecting the actual content of data packets as they appear obfuscated [33]. Analyzing encrypted traffic by the proposed system requires using additional mechanisms for identifying metadata and traffic patterns.

These difficulties and factors are highlighting the complexity in implementing access control lists, anomaly detection, and AI into one system architecture. Carefully addressing these issues will assist in creating a strong and reliable security framework.

X. Improving Access Control Lists with AI

As stated in our proposal, we can utilize AI to examine patterns and behavior to spot anomalies in network access requests. AI models used in the network systems can identify suspicious or suspicious access attempts and send notifications and take preventive measures by learning the typical behavior of users [8]. AI can be used to dynamically modify access control policies depending on current information and circumstances. AI algorithms are able to intelligently decide whether to give or refuse access in a more precise and context-aware manner by considering specific user behavior, device attributes, network information, and other related aspects.

ACL rules can be improved over time by AI algorithms that continuously learn from access patterns and security events. This adaptive learning strategy [8] can help in the evolution of ACLs to block unauthorized access more successfully while lowering false positives. AI algorithms can analyze large volumes of data related to user behavior, network traffic, and system logs to identify patterns, anomalies, and potential security risks [9]. This analysis helps in understanding the access requirements and potential threats [6], forming the basis for ACL generation.

Based on historical data and specified risk models, AI algorithms can evaluate the risk related to granting or rejecting particular rights. By taking into account elements like the user's role and potential vulnerabilities, AI models can provide access control policies that reduce security risks.

Network traffic, user behavior, and security events will be continuously monitored by AI, which may see changes and emerging patterns that can call for ACL adjustments [12]. By constantly modifying ACLs based on current findings, our proposed system can contribute to the maintenance of an efficient and up-to-date access control architecture.

AI classifies various kinds of network traffic and user behaviors using machine learning algorithms [11]. AI models can create ACL rules that permit or limit access based on particular categories or traits by comprehending these classifications.

XI. Discussion

Network traffic is monitored using Snort IDS in our system; AI can be used to increase the effectiveness in analyzing Snort IDS with GPT to give a realistic response and related explanation to these alerts [18]. By implementing our system, a network analyst not only can identify the abnormality but can also get information in a more meaningful and explanatory way, thus allowing for a better decision-making response.

GPT model is beneficial with the ACL-management in adding dynamicity to the access control process. The use of an AI-based component provides more intelligence to ACL management, where access can be requested and granted based on the context gathered from an AI-generated response to the alerts. This can help in IP flagging, analyzing, and mitigating suspicious IP-address through using ACL rules in a more context-aware and automated way. This is considered to be beyond the capabilities of conventional static rule-based ACL filtering approaches. The dynamic nature of network attacks means we will probably want to further train our AI models and update our IDS signatures as new patterns emerge.

Botnets have the ability to mimic authentic users [23] and can be detected using AI but it is not going to be an easy task to deal with. Due to the distributed nature of botnets and their complicated evasion tactics, it can be hard for AI

to detect the normal network traffic from abnormal ones. However, when using advanced techniques such as botnet fingerprinting in conjunction with proper machine learning models [24]; AI systems can better recognize these types of attacks. Moreover, integrating threat intelligence will also be important for a higher detection rate [25].

As security is deployed in our architecture (in the form of Intrusion Detection Systems, Access Control Lists and countermeasures), the architecture described above in Figure 2 can enhance zero trust networks [30]. Zero trust networks need to be authenticated and verified constantly to ensure the access requests are legitime [26]. In this context; the AI-generated ACLs will dynamically adjust access control policies in real time, based on the latest threats and network activity. This means the network is always protected based on up-to-date insights. Continuously analyzing old and new alerts allows the system to put in place the newly generated ACLs aligned with zero-trust principles. Even internal actors must be verified in a zero-trust network. This will ensure the integrity of people and resources that can bypass security controls through the automatic generation and deployment of ACLs based on old and current alerts.

Our system needs enhancements to distinguish between legitimate and malicious behaviors to minimize the effect of attackers who try to resemble the patterns of legitimate users. When such attackers imitate legitimate user actions, their behaviors can still be exposed and detected through deep alert analysis [28][29]. Behavior analysis can also play a significant role here as it shows an effective way to differentiate between legitimate users and malicious actors [31]. The proposed system by the help of AI, has to continuously learn about the typical behavior of authorized users, and needs to point out any suspicious deviations by using applicable machine learning approaches [32]. Moreover, the system must adopt machine learning models to analyze metadata and identify suspicious traffic with much better efficiency [34]. This will lead to group the investigated traffic to a manageable set for detailed examination performed by network analysts.

Integrating machine learning into this system brings promising benefits with the rise in traffic encryption [35]. Machine learning enhances the functions of IDS, as the system learns to adapt continuously to new patterns and threats. AI and countermeasure processes will now be dynamic and automated in nature, as machine learning optimizes ACL generation, deploys countermeasures, as well as to network performance. This will enhance the network analyst's role with ML-driven insights, making the approach to network security proactive and dynamic.

XII. CONCLUSION AND FUTURE WORK

In this paper, an architecture to manage ACLs to detect the suspicious traffic and to thus to secure our network was presented. It will help security analysts to make wise decisions based on the results that AI capabilities bring by identifying patterns and predicting potential threats proactively. This work introduces the pros and cons of managing ACL using AI in security systems. In our future work, we will look into adapting ACLs based on anomalies and policies. Adaptations will provide 'digital immunity' to quickly perform the required containment and mitigation actions upon the detection of a threat. Adaptations can also help improve the resilience of network defenses against evolving threats. We would also be making the system more reliable by continuing to adjust AI models and examine the integration of other cybersecurity concepts. System modifications will change the behavior pattern of a system. In this case, AI must adapt to recognize the new changes in order to avoid misclassifying legitimate changes as suspicious or even mistakenly considered to be attacks. Therefore, network administrators need to guarantee the performance of the system after such updates are conducted. This will include; the type of the update, the type of IDS alerts and the applied corresponded ACL. Fine-tuning the required parts of the system will take hours to days and the retraining process with new data will take weeks. Therefore, real-time monitoring, periodic retraining and considered adjustments can ensure the system will employ the processes needed for ACL to be Generated accurately. One of the open aspects in this research is the possibility of attackers exploiting the system by inducing false positives on the IDS, which could lead to DoS attacks. Although this concern has been identified, no thorough evaluation of the system's resilience to such attacks has been conducted. As future work, we will analyze this vulnerability by finding ways in which the system could be secured against such malicious users, with a view to ensuring that false positives do not impact on either the availability or the reliability of the network. We hope that such an extensible and effective system will help network analysts quickly respond and resolve more and more alerts when faced with new and evolving threats. Our goal is to support critical infrastructures and the integrity of data in complex threat environments. It exhibits great advantages as it enables adaptive threat detection and response and can be a solution to security threats that are constantly evolving. Accordingly, addressing these challenges poses numerous opportunities to achieve better protection of our network from security threats.

ACKNOWLEDGMENT

This work was partially supported by JSPS KAKENHI Grant Number JP19K20268, JP24K14959.

REFERENCES

[1] N.Shahata, H.Hasegawa, and H.Takakura, "AI-driven Approach for Access Control List Management," Proc. of The Seventeenth International Conference on Emerging Security Information, Systems and Technologies, 2023, pp. 52 – 58.

[2] N. Muhammad, U. Shams, B. Mohammad, "Network intrusion prevention by configuring ACLs on the routers, based on snort IDS alerts," *IEEE Communications Surveys & Tutorials,* vol. 22, no.2, pp. 1392-1431, Oct. 2010.
[3] C. Lee, J. Kim and S. Kang, "Semi-supervised Anomaly Detection with Reinforcement Learning," *Computers and Communications (ITC-CSCC),* Phuket, 2022, pp. 933-936, Jul. 2022.
[4] C. Varun, B. Arindam, and K. Vipin, "Anomaly detection: A survey," *ACM Computing Surveys,* vol.41, no.3, pp. 1-58, Jul. 2009.
[5] C. Raghavendra, and C. Sanjay, "Deep learning for anomaly detection: A survey*". arXiv:1901.03407*, Jan. 2019.
[6] C. Kukjin, Y. Jihun, P. Changhwa, and Y. Sungroh, "Deep Learning for Anomaly Detection in Time-Series Data: Review, Analysis, and Guidelines," *IEEE Access*, vol. 9, pp. 120043 – 120065, Aug. 2021.
[7] H. Victoria, and A. Jim, "A Survey of Outlier Detection Methodologies," *Artificial Intelligence Review*, vol. 22, Springer, pp. 85-126, Oct. 2004.
[8] B. Anna, and G. Erhan, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153 – 1176, Oct. 2015.
[9] H. Yassine, G. Khalida, A. Abdullah, B. Faycal, and A. Abbes, "Artificial intelligence-based anomaly detection of energy consumption in buildings: A review, current trends and new perspectives," *Applied Energy*, vol. 287, pp. 1-26, Apr. 2021.
[10] Z. Shuai, C. Mayanka, L. Yugyung, and M. Deep, "Real-Time Network Anomaly Detection System Using Machine Learning,"*IEEE*, pp. 267-270, Jul. 2015.
[11] D. Kyle, H. Abdeltawab, and A. Marco, "A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks," Sensors*,* vol. 23, no. 3, Jan. 2023.
[12] L. Xiao, H. Brett, and W. Dinghao, "Automated Synthesis of Access Control Lists*,"* Proc. International *Conference on Software Security and Assurance (ICSSA)*, Altoona, pp. 104-109, Jul. 2017.
[13] Z. Shakila, A. Khaled, A. Mohammed A, A. Muhammad Raisuddin, K. Risala. Tasin., K. M. Shamim, M. Mahmud, "Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey," IEEE *Access*, vol. 9, pp. 94668-94690, Jun. 2021.
[14] Twingate, "Access Control Lists (ACLs): How They Work & Best Practices". [Online]. Available from: https:twingate.com/blog/access-control-list/ 2023.07.25
[15] Dandelife, "Understanding the Pros and Cons of Access Control Lists". [Online]. Available from: https://dandelife.com/understanding-the-pros-and-cons-of-access-control-lists/ 2023.07.26
[16] I. Muhammad, W. Lei, M. Gabriel-Miro, A. Aamir, S. Nadir, M. K. Razzaq, "PrePass-Flow: A Machine Learning based technique to minimize ACL policy violation due to links failure in hybrid SDN," *Computer Networks*, vol. 184,107706, Jan. 2021.
[17] Streamlit, [Online]. Available from https://streamlit.io/ 2024.03.20
[18] Ali.T, "Next-Generation Intrusion Detection Systems with LLMS: Real-time Anomaly Detection, Explainable AI, and Adaptive Data Generation," pp. 1-65.
[19] R. Trifonov, O. Nakov and V. Mladenov, "Artificial Intelligence in Cyber Threats Intelligence," *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, Mon Tresor, 2018, pp. 1-4.
[20] P. K. Mannam, "Optimizing Software Release Management with GPT-Enabled Log Anomaly Detection," *2023 26th International Conference on Computer and Information Technology (ICCIT)*, Cox's Bazar, 2023, pp. 1-6.
[21] Huggingface [Online]. Available from https://huggingface.co/ 2024.03.25
[22] J. Lansky et al., "Deep Learning-Based Intrusion Detection Systems: A Systematic Review," *IEEE Access*, vol. 9, pp. 101574-101599, 2021.
[23] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "Design and analysis of a social botnet," *Computer Networks*,Vol. 57, no. 2, pp. 556-578, 2013.
[24] R. Vijayakanthan, K. M. Waguespack, I. Ahmed and A. Ali-Gombe, "Fortifying IoT Devices: AI-Driven Intrusion Detection via Memory-Encoded Audio Signals," *2023 IEEE Secure Development Conference (SecDev)*, Atlanta, GA, USA, 2023, pp. 106-117.
[25] R. Trifonov, O. Nakov and V. Mladenov, "Artificial Intelligence in Cyber Threats Intelligence," *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, Mon Tresor, Mauritius, 2018, pp. 1-4.
[26] P. Assunção, "A zero trust approach to network security," Proc. the Digital Privacy and Security Conference, vol. 2019. Porto Portugal, 2019, pp. 65-72.
[27] L. Yee Por *et al*., "A Systematic Literature Review on AI-Based Methods and Challenges in Detecting Zero-Day Attacks," *IEEE Access*, vol. 12, pp. 144150-144163.
[28] S. McElwee, J. Heaton, J. Fraley and J. Cannady, "Deep learning for prioritizing and responding to intrusion detection alerts," *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, 2017, pp. 1-5.
[29] A. Imeri and O. Rysavy, "Deep learning for predictive alerting and cyber-attack mitigation," *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC),* Las Vegas, 2023, pp. 0476-0481.
[30] D. Eidle, S. Y. Ni, C. DeCusatis and A. Sager, "Autonomic security for zero trust networks," *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, New York, 2017, pp. 288-293.
[31] W. Zhenqi and W. Xinyu, "NetFlow Based Intrusion Detection System," *2008 International Conference on MultiMedia and Information Technology*, Three Gorges, China, 2008, pp. 825-828.
[32] S. Saad et al., "Detecting P2P botnets through network behavior analysis and machine learning," *2011 Ninth Annual International Conference on Privacy, Security and Trust, Montreal*, 2011, pp. 174-180.
[33] Natureprotfolio. *Vigilance still critical in highly encrypted networks.* [Online]. Available from: https://www.nature.com/articles/d42473-023-00326-y/ 2024.11.22
[34] S. Hiruta, I. Hosomi, H. Hasegawa, and H. Takakura, "Security Operation Support by Estimating Cyber Attacks Without Traffic Decryption," *Proc. 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, Torino, 2023, pp. 1127-1132.
[35] M. Shen et al., "Machine Learning-Powered Encrypted Network Traffic Analysis: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 25, pp. 791-824, 2023.