AI-driven Approach for Access Control List Management

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

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

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

Abstract—**With the increasing dependence on digital systems and the pervasive nature of cyber threats, ensuring secure access to information and resources has grown to be a crucial component of our activities online. Access control lists serve as foundational frameworks that govern the authorization and authentication processes within computer systems. This paper examines how access control lists canbe employed effectively in the field of cybersecurity and digs into its important role in protecting sensitive data, mitigating risks, and safeguarding against unauthorized access. Access control lists play a vital role in ensuring the security and confidentiality of sensitive information and resources. Traditionally, access control has relied on predefined rules and policies to determine who has the eligibility in accessing which data. However, the rise of Artificial Intelligence (AI) has introduced new possibilities and challenges in the field of access control. This paper explores the impact of AI on access control lists, examining the benefits and potential concerns associated with the integration of AI technologies. In order to secure the organization's network, we propose an AI-driven ACL management system which generates ACL automatically. By managing the network traffic with the generated ACL, the system supports network analysts to prioritize certain threats that require immediate response. By discussing the effectiveness of the system, we explore the possibility of AI-driven ACL management.**

Keywords-Access Control; Cyber Security; Network; Artificial Intelligence.

I. INTRODUCTION

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 [1]. Over the years, advancements in technology 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 make informed decisions based on a vast amount of data, can revolutionize the way of how access control can be managed which can lead to securing our networks. When applied, AI-powered access control models can offer numerous benefits over traditional rule-based systems. These models can have the ability to strengthen machine learning algorithms [7] to analyze and understand network traffic patterns, behaviors and contextual information to make real-time based access decisions. The shift from static rules to dynamic decision-making can lead to more accurate and adaptive access control mechanisms, strengthening security measures and reducing the risk of unauthorized access. One of the key advantages of AI in access control models is its ability to detect anomalies and identifying potential security threats. By analyzing historical data and learning from past patterns, AI algorithms can establish a baseline of normal behavior for users and systems [7]. Any deviation from this baseline can trigger alerts or generate preventive actions, helping in mitigating risks and preventing security breaches. This proactive approach to access control is particularly crucial in today's ever-evolving threat landscape, where traditional rule-based systems often fall in detecting sophisticated attacks.

Furthermore, AI can significantly improve the user's experience in access control systems. With traditional models, users often face heavy 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 in increasing the organization's network security when applying AI to generate countermeasures based on ACL rules.

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 our vision on solving the drawbacks that were discussed in the background section through an overflow figure. Section IV illustrates the benefits of AI when it is integrated with detecting anomalies and generating ACLs. Our architecture proposal is presented in section V along with a detailed description of its components. The architecture's assumptions, challenges and limitations are explained in Section VI and Section VII respectively. In Section VIII discusses the importance of AI in generating ACLs. The discussion part in section IX describes how effective our proposed system can be if it is applied when detecting anomalies and

ISBN: 978-1-68558-092-6

generating ACLs. We end our paper with a conclusion in section X.

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 a considerable interest in examining the potential enhancement of access control systems in the light of 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 an understanding of the evolving status of AI-powered technology and its influence on cybersecurity by studying the existing literature and industry practices [8].

The basis for controlling users' interactions with digital systems and safeguarding sensitive data is access control models. Role-based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are common access control methods. The current Access Control List (ACL) system has some weaknesses even though it works well in many situations.

The existing ACL mechanism has a number of disadvantages that are frequently encountered [13]. 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 [13]. 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 [14]. 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 [15]. This strategy can improve security by spotting and identifying anomalies.

Managing alerts from an Intrusion Detection System (IDS) can be a challenging task for a network analyst. These difficulties include the volume of generated alerts, the complexity of the alerts and the need for quick and accurate responses. 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. Regular analysis of ACLs and their effectiveness in dealing with suspicious traffic can lead to a continuous improvement in the organization's network security posture. Managing ACLs is an essential part of network security because of its efficiency in detecting and preventing suspicious traffic. By analyzing ACLs and adjusting access control rules, network analysts can improve the security of their network infrastructure and protect it from potential threats.

Our proposed system will be relying on machine learning algorithms [6] 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. System Overflow

We propose a dynamic AI based Access Control system for solving the problems which are explained in Section 2.

Our system involves the integration of AI and generating ACL for improving the network structure in dealing with suspicious traffic analysis [5]. This can lead to generate an efficient countermeasure against future similar attacks. Figure 1 shows an overview of our proposed architecture, it consists of five phases which work in a sequential step-by-step order. We will describe details of each phase below.

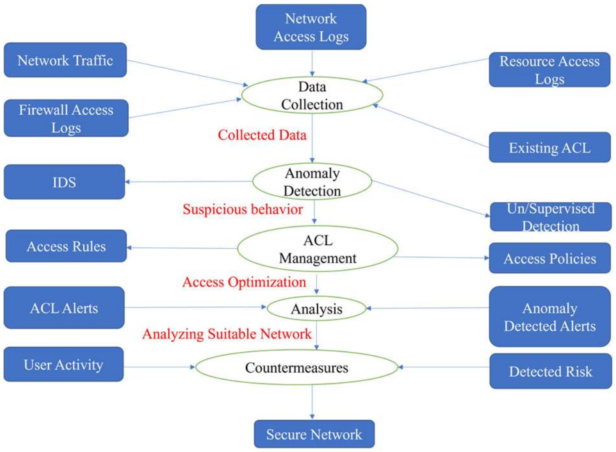


Figure.1 Proposed System Overflow

A. Data Collection

This is the first phase, in which the collection of several attributes of data is required [9]. 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 (which is all the 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 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 [3].

B. Anomaly Detection

In this phase, the collected data in phase one will be the input to several anomaly detection methods [4]. 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 into several security configurations and to the needs of organizations as well as its effectiveness when combining it with machine learning methods [7]. 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 [5]. This posture analysis will be the input for the final countermeasures phase.

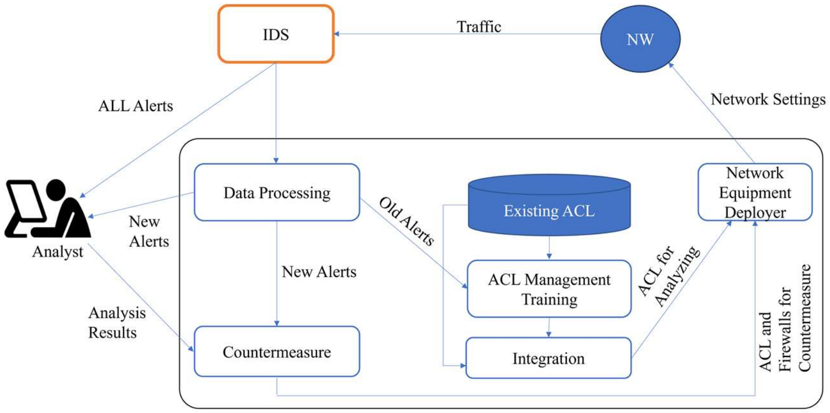
E. Countermeasures

After the analyst's evaluation, the countermeasure phase with the help of AI will estimate the seriousness and potential consequences of the detected alerts based on the analysis result.

IV. 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 [2]. By employing machine learning algorithms [7] to analyze massive volumes of data and spot strange patterns and behaviors, AI can enhance anomaly detection [6].

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 [5]. This will also simplify the management of ACLs [11], 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.



Old Alerts: Alerts before ACL applying
New Alerts: Alerts after ACL applying

Figure 2. Proposed System

V. 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.

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 form 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 system 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 [6]. In our system, the IDS will be generating alerts when it finds activities that fall outside the predefined threshold.

G. Countermeasure

The role of countermeasures in our case is to respond to the alerts that the network analyst handles to prevent or mitigate the identified threats. These responses may include blocking malicious IP addresses, modifying firewall rules and notifying the network analyst about potential threats.

VI. Assumptions

There are several assumptions to take into consideration when implementing such a system. It is expected that plenty of data will be available to train the AI model for both access control lists and the detected anomalies. To create precise models and comprehend typical patterns and behaviors, we will need enough data samples to begin with.

Our system in which the AI model will be deployed is presumed to be represented by the data used to train the AI model. This presumption guarantees that the model can accurately identify anomalies and decide what the best access control measures are based on actual circumstances. A precise definition of anomalies is necessary [3]. The system must have a clear understanding of what defines an anomaly. This definition could change depending on the system's situation. Therefore, it is crucial to have clear standards for spotting unusual patterns or behaviors.

Access control policies must be in place before AI can be integrated into access control lists. These regulations specify who has access to what resources and how. Rules governing access levels (network administrators), responsibilities (managing alerts), permissions (allowing), and restrictions (denying) are examples of prerequisites that are needed. In real-time applications, AI systems should be scalable to handle any data volumes as well as to the amount of access control requests. We mean by this that traditional anomaly detection methods may struggle with complicated data to handle effectively. To find abnormalities and decide on access restrictions without noticeably affecting performance of the system, our system has to be able to process and analyze data effectively.

AI systems are expected to be able to continuously learn from and modify their behavior to match changing patterns and trends. To enable efficient anomaly detection and access control, The system should be able to update models based on new data and to modify access control policies accordingly.

VII. Challneges and Considerations

The quality and accessibility of the data used for the training purposes have a significant impact on how effective our AI systems will be. To identify deviations from typical patterns and impose the proper access rules, anomaly detection and access control systems need thorough and precise data.

The threat landscape is also rapidly changing, with new attack vectors appearing frequently. In order for models to continuously learn and update for countering new threats, our AI system design must be flexible. It is crucial to routinely update anomaly detection and access control systems based on newly fresh updated information to retain efficacy [12].

False positives and false negatives are also possible [3]. Systems for detecting anomalies can produce false positives (which misinterpret typical behavior as abnormal) and false negatives (which fail to detect actual anomalies). It is crucial to strike a balance between these two types of errors in order to prevent unneeded disruptions and potential security breaches. Adjusting the thresholds and the AI model are both necessary to minimize any likelihood of errors.

Techniques for adversary strength, such as adversary training and input validation, should be taken into consideration to make the AI system more resistant to such attacks [10]. 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.

VIII. Improving Access Control Lists with AI

As was stated in our proposal, we can utilize AI to examine patterns and behavior to spot anomalies in network access requests. AI systems can identify suspicious or suspicious access attempts and send notifications and take preventive measures by learning the typical behavior of users [7]. 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 [7] 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 [8]. This analysis helps in understanding the access requirements and potential threats [5], 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 systems 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 [11]. By constantly modifying ACLs based on current findings, AI systems 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. AI systems can create ACL rules that permit or limit access based on particular categories or traits by comprehending these classifications.

IX. Discussion

Anomaly detection systems and access control lists (ACLs) are fundamental components for protecting computer networks from unauthorized access and potential threats. An IDS is designed to monitor network traffic and generate alerts when suspicious or malicious activity is detected. AI-based ACLs, on the other hand, use AI techniques to automatically manage and enforce access control policies. Combining AI algorithms for IDS (Intrusion Detection System) alerts with ACL (Access Control List) alerts provides a more complete and intelligent approach to threat detection and response will improve the organization’s network security.

Anomaly detection systems are designed to monitor network traffic and detect potential security breaches and malicious activity [2]. It will be used in generating alerts when suspect behavior or patterns are detected. ACLs, on the other hand, are used to regulate access to network resources by creating rules that permit or deny traffic based on predetermined criteria. By combining the AI algorithms of IDS alerts and ACL Alerts, the organizations can harness the power of machine learning and sophisticated analytics to evaluate, classify, and take appropriate actions of incoming alerts.

X. Conclusion and future work

By leveraging the capabilities of AI in conjunction with anomaly detection and access control lists, organizations can achieve proactive threat detection, adaptive access control policies, and efficient countermeasure generation. This paper presented an architecture for managing ACLs for analyzing suspicious traffic and for generating relevant countermeasures. We believe that this will help in creating wise access control decisions by adopting an AI-based ACL. This will help in predicting possible risks that may occur before an incident happen. This research highlights the potential benefits and challenges associated with integrating AI into security systems, along with implementation strategies and performance evaluation metrics. It emphasizes the importance of continually updating and refining AI models to stay ahead of emerging security threats, ultimately strengthening the overall security posture of various domains. Moreover, this will help network analysts in identifying alerts efficiently. In our future work, we will be focusing on managing how ACL can be adapted based on anomalies and policies to create a more secure environment.

Acknowledgment

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

References

[1] 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, October 2010.

[2] C. Lee, J. Kim and S. Kang, "Semi-supervised Anomaly Detection with Reinforcement Learning", Computers and Communications (ITC-CSCC), Phuket, Thailand, 2022, pp. 933-936, July 2022.

[3] C. Varun, B. Arindam, and K. Vipin, “Anomaly detection: A survey”. ACM Computing Surveys, vol.41(3), pp.1-58, July 2009.

[4] C. Raghavendra, and C. Sanjay, “Deep learning for anomaly detection: A survey”. arXiv:1901.03407, January 2019.

[5] C. Kukjin, Y. Jihun, P. Changhwa, and Y. Sungroh, “Deep Learning for Anomaly Detection in Time-Series Data: Review, Analysis, and Guidelines”.IEEE, vol.9, pp. 120043 – 120065, August 2021.

[6] H. Victoria, and A. Jim, “A Survey of Outlier Detection Methodologies”. Artificial Intelligence Review 22, Springer, pp.85-126, October 2004.

[7] 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 (2), pp. 1153 – 1176, October 2015.

[8] 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, ScienceDirect Applied Energy, vol 287, pp.1-26, April 2021.

[9] Z. Shuai, C. Mayanka, L. Yugyung, and M. Deep, “Real-Time Network Anomaly Detection System Using Machine Learning”.IEEE, pp. 267-270, July 2015.

[10] D. Kyle, H. Abdeltawab, and A. Marco, “A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks”.Sensors vol.23(3), January 2023.

[11] L. Xiao, H. Brett, and W. Dinghao, "Automated Synthesis of Access Control Lists,” International *Conference on Software Security and Assurance (ICSSA)*, Altoona, PA, USA, pp. 104-109, July 2017.

[12] 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," in IEEE Access, vol. 9, pp. 94668-94690, June 2021.

[13] Twingate, Access Control Lists (ACLs): How They Work & Best Practices. [online]. Available from: https:twingate.com/blog/access-control-list/ 2023/07/25

[14] 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

[15] 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, January 2021.