AI-DRIVEN APPROACH FOR ACCESS CONTROL LIST MANAGEMENT

AUTHORS: SHAHATA NADER, HIROKAZU HASEGAWA, HIROKI TAKAKURA
EMAILS: nader@nii.ac.jp, hasegawa@nii.ac.jp, takakura@nii.ac.jp

NATIONAL INSTITUTE OF INFORMATICS
CENTRE FOR STRATEGIC CYBER RESILIENCE RESEARCH AND DEVELOPMENT
TOKYO - JAPAN

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

IARIA

Presenter Resume

Name: Nader Shahata

Career title: Project Researcher at National Institute of Informatics (NII).

Research Interests: Internet Security, Artificial Intelligence and Cloud Computing

Outline

- Introduction
- Background
- Objectives and Goals
- Proposed Idea
- Architecture Overflow
- Architecture Proposal
- Conclusion

Introduction

- **Securing our activities online has become a crucial component of our daily life**
- **Access Control models are essential components in the field of information security**
- **When our systems are infected, malicious activities removal can be challenging**

Background

- **ACL systems have some weaknesses**

  - Managing an ACL system can be very challenging.

  - ACL maintenance calls for constant work and modification.

  - The ACL needs to be manually updated if the environment changes.

- **The network analyst needs to maintain a high number of access control entries which could affect the performance of the network.**

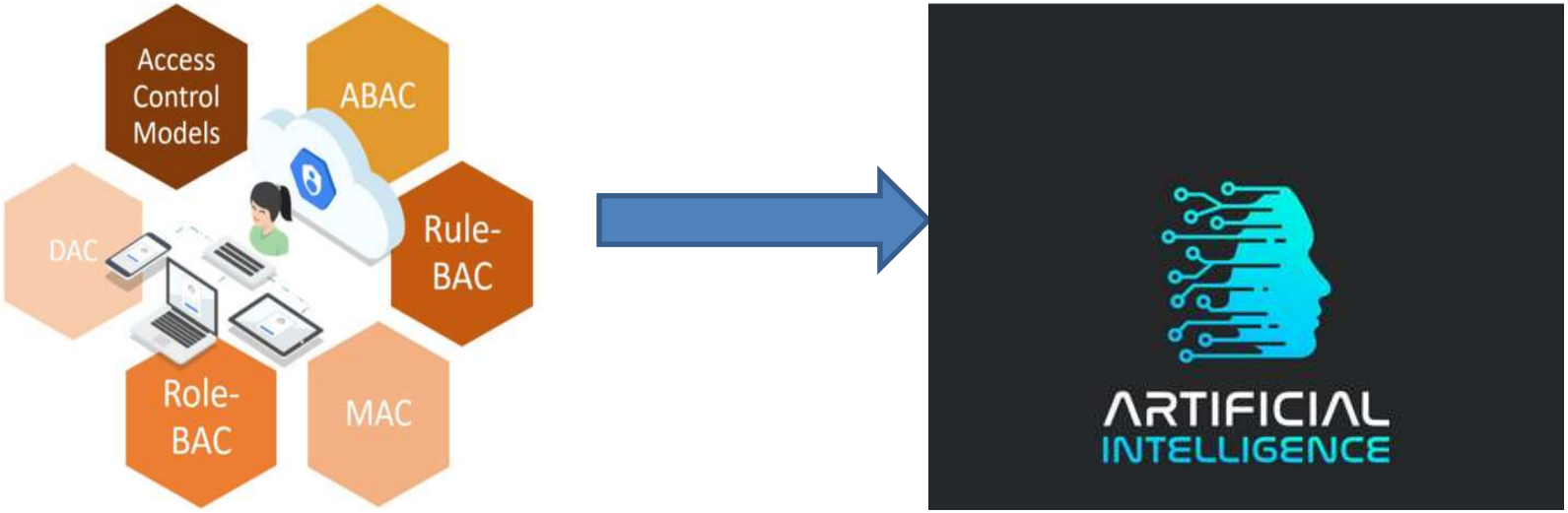
  - Managing alerts from an Intrusion Detection System (IDS) can be a challenging task for a network analyst.

  - The volume of these alerts can overwhelm analysts, which may cause inaccurate response taking.

Objective and Goals

- **To propose an architecture that can help in increasing the organization's network security.**
- **To find an alternative way in dealing with updating ACL rather than depending on the current manual approach.**
- **To apply AI for generating countermeasures based on ACL rules.**
- **Helping network analysts when receiving alerts coming from anomaly detection methods (IDS).**

Proposed Idea



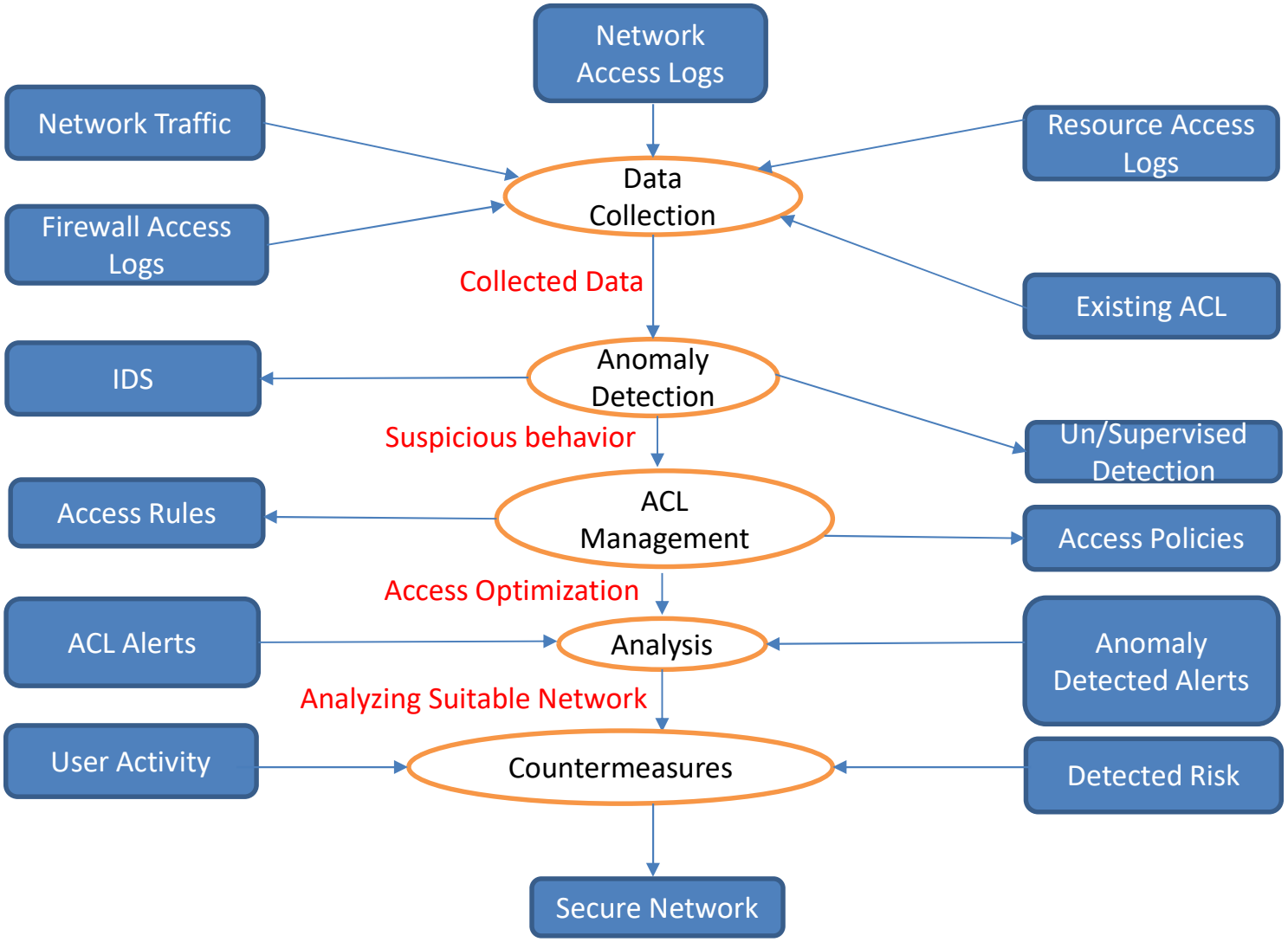
AI Access Control Advantages

- **Detecting New Threats**
- **Battling Bots**
- **Breach Risk Prediction**

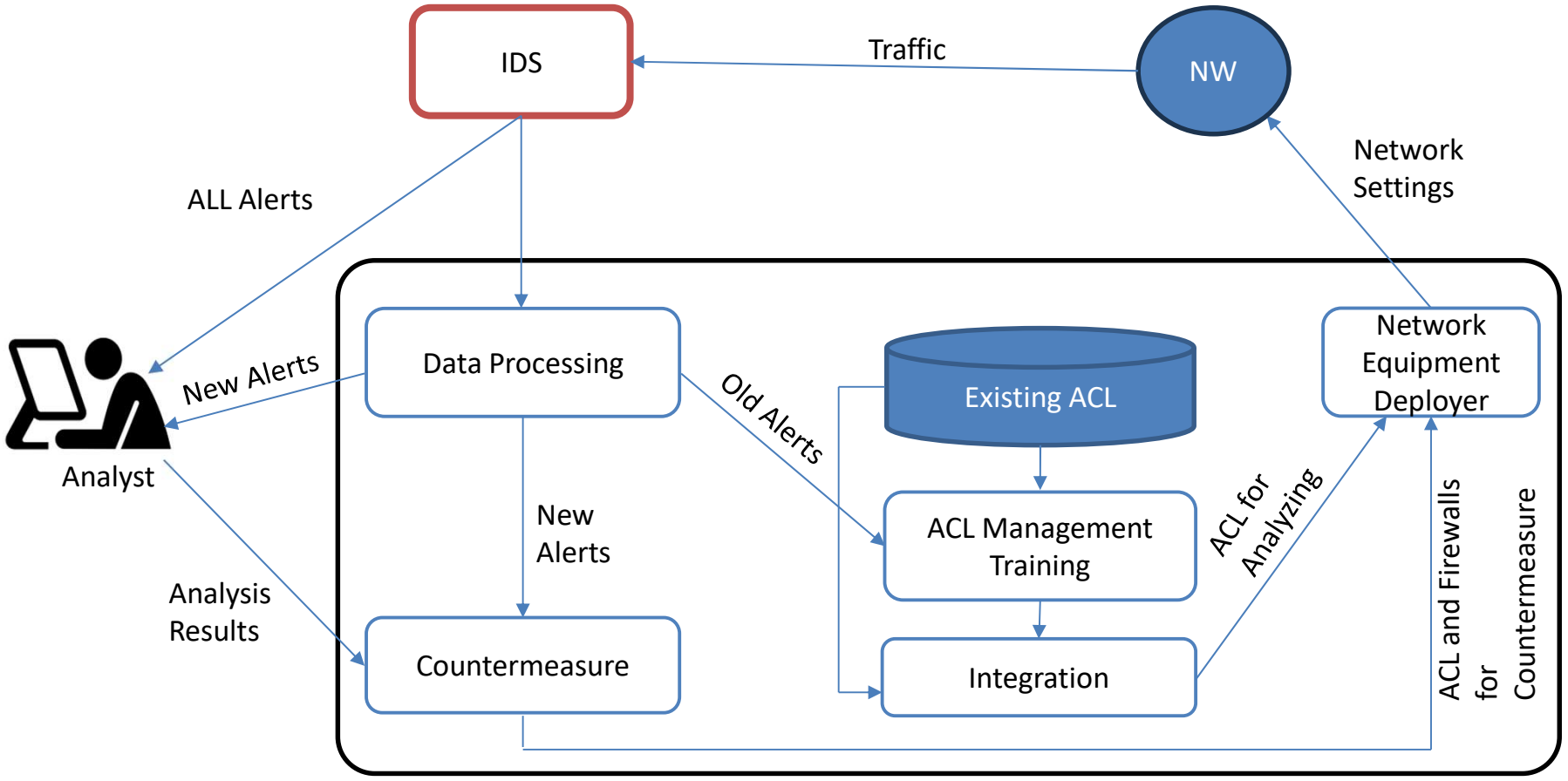
AI Methods

- **There are several AI methods such as: Machine learning, natural language processing and deep learning.**
- **Machine learning will be our preference among them.**
- **Machine learning models can learn and adapt to new patterns and anomalies without the need for manual rule updates**
- **It can help in system's continuous improvement**

Architecture Overflow



Architecture Proposal



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

How ACL will be Analyzed

- **Source**: (user, IP address) asking for access.
- **Permission**: What actions will be taken (allowing or denying)
- **Resource**: Which resource (e.g. server) the user applies to.
- **Conditions**: Any conditions that must be met for the rule to be applied.

Assumptions

- ✓ The data will be available.
- ✓ The AI-ACL based model has to be continuously trained.
- ✓ A precise definition of anomalies is necessary
- ✓ Access control policies must be predefined and available.
- ✓ Constant learning and adaptation.

Challenges

- **The threat landscape is also continually changing, with new attack vectors appearing frequently.**
- **False positives and false negatives are possible.**
- **The Use of VPN**

Conclusion

- **Managing ACLs for analyzing suspicious traffic and for generating relevant countermeasures.**
- **Creating wise access control decisions by adopting an AI-based ACL .**
- **Predicting possible risks that may occur before an incident may happen.**
- **Helping Network Analysts in identifying alerts efficiently.**

Reference List

[1] N..Muhammad, U.Shams, Badar.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. j. Kang, "Semi-supervised Anomaly Detection with Reinforcement Learning", Computers and Communications (ITC-CSCC), Phuket, Thailand, 2022, pp. 933-936, July 2022.

[3] Chandola, V., Banerjee, A., and Kumar, V., "Anomaly detection: A survey". ACM Computing Surveys, vol.41(3), pp.1-58, July 2009.

[4] Chalapathy, R., and Chawla, S., "Deep learning for anomaly detection: A survey". arXiv:1901.03407, January 2019.

[5] Choi.K, Yi,J, Park,C, Yoon.S, "Deep Learning for Anomaly Detection in Time-Series Data: Review, Analysis, and Guidelines". IEEE, vol.9, pp. 120043 – 120065, August 2021.

[6] Hodge.V,and Austin.J, " A Survey of Outlier Detection Methodologies". Artificial Intelligence Review 22, Springer, pp.85-126, October 2004.

[7] Buczak.A and Guven.E, "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] Himeur.Y, Ghanem.K, Alsalemi. A, Bensaali.F, and Amira.A, "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] Zhao.S, Chandrashekar.M, Lee.Y, and Medhi.D, "Real-Time Network Anomaly Detection System Using Machine Learning".IEEE, pp. 267-270, July 2015.

[10] DeMedeiros.K, Hendawi.A, Alvarez.M, "A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks".Sensors vol.23(3), January 2023.

[11] X. Liu, B. Holden and D. Wu, "Automated Synthesis of Access Control Lists," International *Conference on Software Security and Assurance (ICSSA)*, Altoona, PA, USA, pp. 104-109, July 2017.

[12] S. Zaman, K. Alhazmi, M. A. Aseeri, M. R. Ahmed, M. R. Ahmed, R. T. Khan, M. S. Kaiser, 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. Kaleem,"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.

Thank You