Deep Leanring of ABAC in Cloud

Maitrey Govind Ranade
(18CS30026)

Divyanshu Kumar
(18CS30016)

Gawai Laukik
(19CS10032)

What is Access Control

- Access control is the practice of regulating who can access certain resources, data, or services in a computing environment.
- It is a fundamental aspect of cybersecurity and is used to protect against unauthorized access, theft, modification, or destruction of sensitive information
- Types of Access Control
  - Discretionary Access Control (DAC
  - Mandatory Access Control (MAC)
  - Role-Based Access Control (RBAC)
  - Attribute-Based Access Control (ABAC)

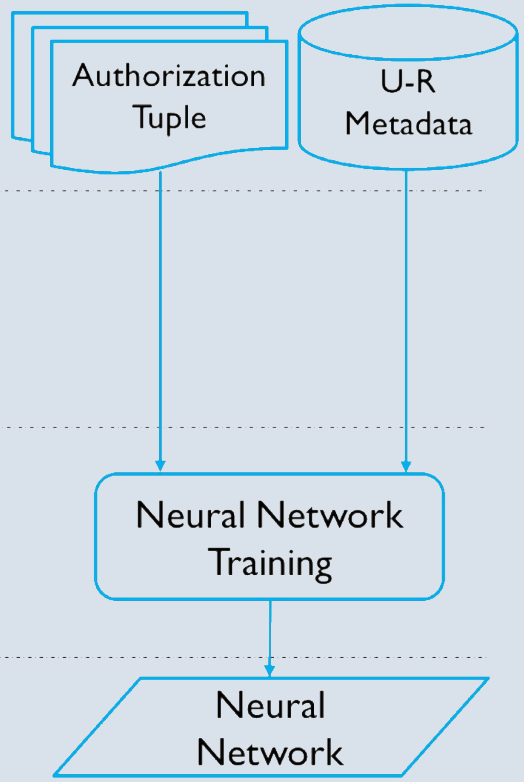
Related Approaches to Access Control

- Classical policy mining approaches
- Machine learning based policy mining approaches
- ML approaches to make control decision instead of mining

- Implemented framework:
  - DLBACα: Deep learning based decision making approach

The DLBACα Framework

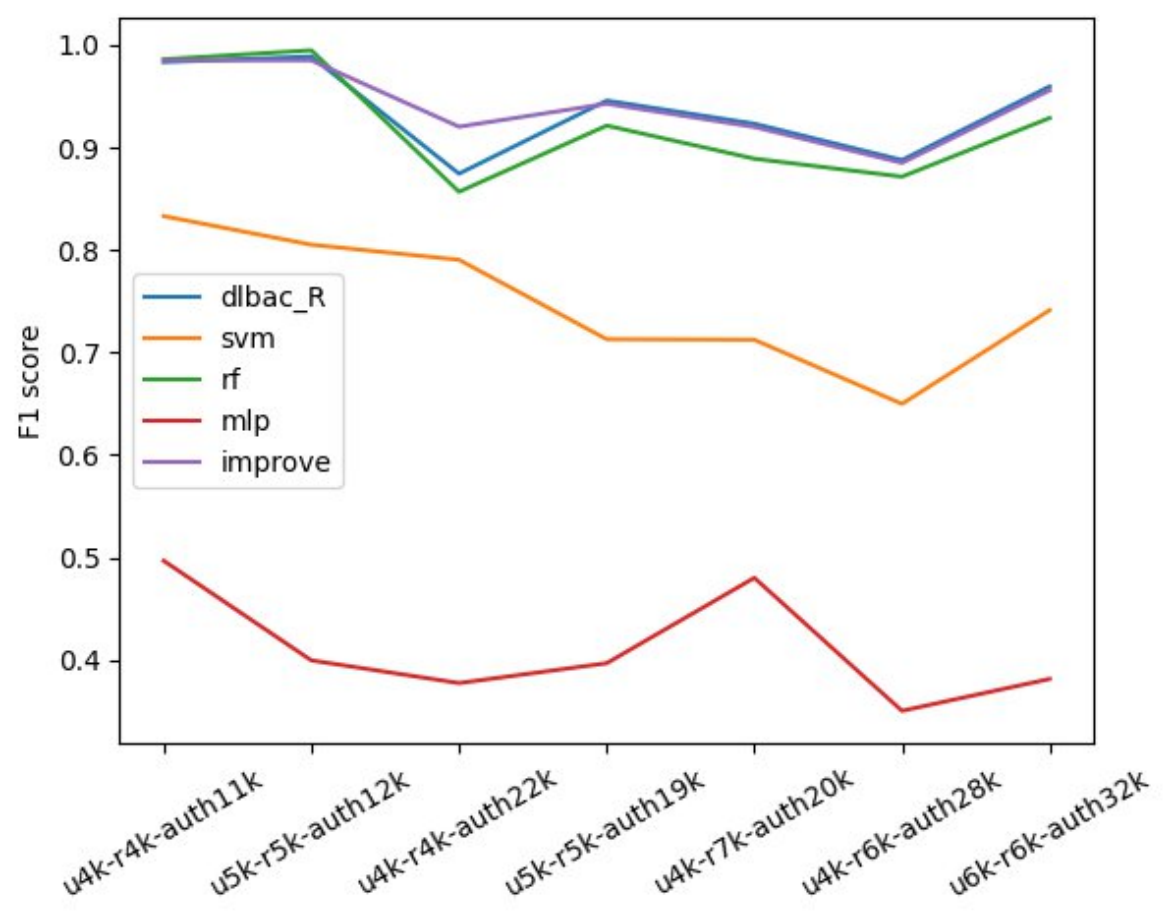
- A framework to let user access resources
- Each resource and user is associated with their own metadata
- It constructs a Residual Deep neural network
  - Takes in user and resource metadata
  - Outputs an authorization tuple
    - A boolean vector with dimensions = Types of operations
    - 0 meaning access denied to the type of operation
    - 1 meaning access granted

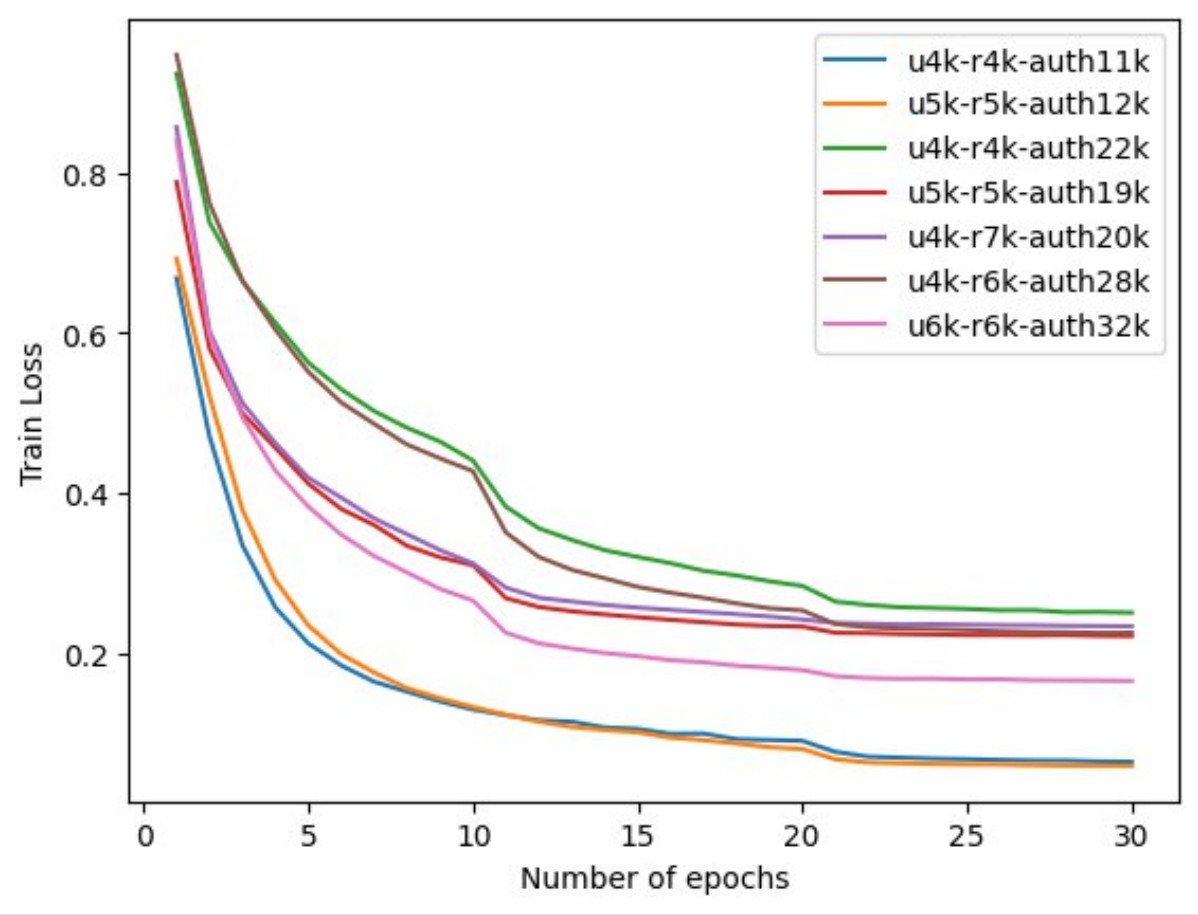


Proposed Improvement

- The original framework calcualates the number of epochs as:
  - IF d > 9 = e1 ELSE epochs = e2
  - For given dataset e1 = 30, e2 = 60
  - The depth function is proposed as d = n*6 + 2, where n is depth parameter based on metadata length
- However in any dataset we do not observe any improvement on loss going beyond for about 20 epochs, hence propose to not take this decision. This leads to a faster training process which is crucial as the model may be needed to update in a real-life situation.
- To improve learning of complex datasets like “u5k-r5k-auth12k” We double the number of convolution filters.
- Through our experimentation, we found that the the if we set num_filters to the length of the feature vector, the model performed the best.

Observations





Deployment in cloud

- As suggested, to deploy the framework in an actual cloud based scenario, we modify the “decision engine” for the framework DLBACα
- This helps user access their files through the web
- Th framework is easily deployed inside a docker container and lets user query and access files with the trained network as the access control barrier.

THANK YOU