

Vancouver

## **INCS 775: Data Center Security**

# **Assignment #2** (Group) - Applying ML to Detect DoS Attacks in Data Center Network

**Posted**: *June 14*, 2024 **Due**: *June 28*, 2024

Instructor: Dr. Zhida Li

Summer 2024 INCS, 775-VA3 (1391)

Email: zli74@nyit.edu

In this assignment, we will learn four types of intrusions and use the machine learning (ml) model(s) to detect DoS with **coding (Python) in** the ".ipynb" file. **DoS** attack and **Regular** data will be detected based on our developed ml model(s).

### Tasks:

#### 1. Download the shared folder from Google Drive (for NYIT login):

https://drive.google.com/drive/folders/1L1LU\_dQ5hajJd9JvQzkXDFkU8vrsy7yE?usp=sharing

Folder name:

ML in DCN

Unzip the folder.

#### **Folder content:**

- Python code (Jupyter file): INCS775\_Lab2\_MLinDCN.ipynb
- NSL-KDD training data (42 columns): KDDTrain+ 20Percent 775.csv
- NSL-KDD testing data (42 columns): KDDTest+ 775.csv
- Webpage (NSL-KDD) offline: nsl-kdd\_index.html
- Paper for NSL-KDD: A detailed analysis of the KDD CUP 99 data set.pdf

Content of the CSV files:

Row 1: header (feature names)

Columns 1-41: features

Column 42: labels for Regular = 0, DOS = 1, R2L = 2, U2R = 3, Probe = 4.

#### 2. Learn and understand your NSL-KDD data:

Cyber attacks are becoming more sophisticated and, hence, more difficult to detect. Using efficient and effective machine learning techniques to detect network anomalies and intrusions is an important aspect of cyber security.

Machine learning algorithms have been evaluated for robustness, high accuracy, and training time when classifying various datasets collected from communication networks. Reliable testing and validation of anomaly and intrusion detection algorithms depend on the quality of datasets such as traffic collected from deployed networks or experimental testbeds. The most widely used benchmark datasets in the literature are Knowledge Discovery in Databases (KDD) Cup 1999 (KDD'99) and NSL-KDD. KDD'99 intrusion dataset is based on the Defense Advanced Research Projects Agency (DARPA) 1998 dataset.

The NSL-KDD dataset is an improved version of the KDD'99 intrusion dataset. Data were captured from an evaluation testbed and included large numbers of virtual hosts and user automata. The KDD'99 dataset was used in various IDSs. NSL-KDD is a randomly selected subset of KDD'99 after redundant data were removed and is a widely used benchmark for evaluating anomaly detection techniques. NSL-KDD dataset captures TCP, UDP, and Internet Control Message Protocol (ICMP) traffic collected using the tcpdump utility. It contains four types of intrusion attacks: DoS, R2L, U2R, and Probe described in Table 1.

Each network connection is represented by 41 features: 38 numerical and 3 categorical ("protocol\_type", "service", and "flag") features. Categorical features will be converted to numerical in our experiment.

Table 1: NSL-KDD: Four types of intrusion attacks are listed: DoS, R2L, U2R, and Probe.

Type	Intrusion attacks	
DoS	back, land, neptune, pod, smurf, teardrop, mailbomb,	
	processtable, udpstorm, apache2, worm	
U2R	buffer-overflow, loadmodule, perl, rootkit, sqlattack, xterm, ps	
R2L	fpt-write, guess-passwd, imap, multihop, phf, spy, warezmaster,	
	xlock, xsnoop, snmpguess, snmpgetattack, httptunnel, sendmail,	
	named	
Probe	ipsweep, nmap, portsweep, satan, mscan, saint	

The features with continuous and discrete types are described in Table 2. We consider binary classification, only considering Regular, DoS. The labels in the CSV files are Regular, DoS, R2L, U2R, and Probe, labeled as 0, 1, 2, 3, and 4, respectively. We process the KDDTrain+\_20Percent\_775 dataset for training and KDDTest+\_775 dataset for testing.

Before beginning the experiment, extract the data points (rows) that are labeled only as Regular (0) and DoS (1). Count the number of data points for Regular (0) and DoS(1). (These tasks are shown in the file INCS775\_Lab2\_MLinDCN.ipynb)

Table 2: NSL-KDD features: Definitions, types, and descriptions. Each network connection is represented by 41 features: 38 numerical and 3 categorical ("protocol\_type", "service", and "flag")

## features.

discrete discrete type of the protocol (TCP, UDP)  service discrete type of the protocol (TCP, UDP)  service discrete type of the protocol (TCP, UDP)  service on the destination, (HTTP, telnet)  flag discrete continuous continuous no. of data bytes from source to destination no. of data bytes from source to destination to source of otherwise on the same host/port; of otherwise no. of "wrong" fragments no. of wrong" fragments no. of "wrong" fragments no. of wrong "fragments no. of "wrong" fragments no. of "wrong" fra	Feature	Definition	Type	Description
discrete discrete network service on the destination, (HTTP, telhet)  flag discrete continuous continuous no. of data bytes from source to destination no. of fuse the same host from/to the same host as the current connection in the past 2 s no. of "noof" roof" ragments no. of "roof" ragments no. of stall packets no. of filed login at tempts a life on the same host no. of connections to the same host no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the	_	duration	continuous	length (seconds) of the connection
4 flag discrete continuous no. of data bytes from source to destination no. of data bytes from source to destination no. of data bytes from destination to source discrete 1 if connection is from/to the same host/port; 0 otherwise no. of "wrong" fragments no. of "hot" indicators no. of failed login attempts 12 logged in discrete 1 if successfully logged in; 0 otherwise no. of "compromised" continuous no. of alied login attempts 13 num_compromised discrete 1 if successfully logged in; 0 otherwise no. of "compromised" conditions no. of shell prompts no. of "sompromised" conditions no. of "compromised" conditions no. of "sompromised" conditions no. of "compromised" conditions no. of "sompromised" conditions no. of shell prompts no. of shell prompts no. of otherwise no. of outbound commands in an ftp session outbound command		protocol_type	discrete	type of the protocol (TCP, UDP)
4 flag 5 src_bytes 6 dst_bytes 7 land 6 myrong_fragment 9 urgent 10 hot 11 num_failed_logins 12 logged_in 13 num_compromised 14 root_shell 15 su_attempted 16 num_root 17 num_falle_creations 18 num_shells 20 num_outbound_cmds 21 is_host_login 22 is_guest_login 23 count 24 srv_count 25-26 serror_rate 27-28 rerror_rate 29 same_srv_rate 27-28 rerror_rate 27-28 rerror_rate 27-28 rerror_rate 30 diff_srv_rate 31 dst_host_srv_serror_rate 32 dst_host_serror_rate 33 dst_host_srv_serror_rate 36 dst_host_srv_serror_rate 36 dst_host_srv_serror_rate 40-41 dst_host_srv_serror_rate 40-51 discrete continuous continuous continuous and dst_host_srv_serror_rate 40-41 dst_host_srv_serror_rate 40-41 dst_host_srv_serror_rate 40-41 dst_host_srv_serror_rate 40-41 dst_host_srv_serror_rate 40-51 discrete continuous	3	service	discrete	network service on the destination,
5 src_bytes continuous 6 dst_bytes continuous 7 land discrete 1 if connection is from/to the same host/port; 0 otherwise 10 hot continuous 11 num_failed_logins continuous 12 logged_in discrete 1 if successfully logged in; 0 otherwise 13 num_compromised continuous 14 root_shell discrete 1 if successfully logged in; 0 otherwise 15 su_attempted discrete 1 if successfully logged in; 0 otherwise 16 num_root continuous 17 num_falle_creations continuous 18 num_shells continuous 19 num_access_files continuous 20 num_outbound_crnds continuous 21 is_host_login discrete 1 if the login is a "guest"login; 0 otherwise 22 is_guest_login discrete 1 if the login is a "guest"login; 0 otherwise 23 count continuous continuous as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the p				(HTTP, telnet)
6 dst_bytes 7 land discrete 8 wrong_fragment continuous 9 urgent continuous 10 hot continuous 11 num_failed_logins continuous 12 logged_in discrete 13 num_compromised continuous 14 root_shell discrete 15 su_attempted discrete 16 num_root continuous 17 num_file_creations continuous 18 num_access files continuous 19 num_access files continuous 20 num_outbound_cmds 21 is_host_login discrete 23 count continuous 24 srv_count continuous 25-26 serror_rate and srv_serror_rate 27-28 rerror_rate and srv_serror_rate 27-28 rerror_rate and srv_serror_rate 27-28 rerror_rate and srv_serror_rate 30 diff_srv_rate 31 dst_host_srv_count 32 dst_host_same_srv_rate 35 dst_host_same_srv_rate 36 dst_host_same_srv_rate 37 dst_host_srv_diff_host_rate 38-39 dst_host_srv_serror_rate 40-41 dst	4	flag	discrete	normal or error status of the connection
Second	5	$src\_bytes$	continuous	no. of data bytes from source to destination
8 wrong_fragment continuous no. of "wrong" fragments no. of "wrong inclinate phont in the pack 2 send in the pac	6	$dst\_bytes$	continuous	no. of data bytes from destination to source
9 urgent continuous no. of urgent packets no. of "hot" indicators no. of file login attempts 11 num_failed_logins continuous no. of filed login attempts 12 logged_in discrete 1 if successfully logged in; 0 otherwise no. of "compromised" conditions 14 root_shell discrete 1 if "su root" command attempted; 0 otherwise 15 su_attempted discrete 1 if "su root" command attempted; 0 otherwise 16 num_root continuous no. of shell is obtained; 0 otherwise 17 num_file_creations continuous no. of shell prompts no. of shell prompts no. of operations on access control files continuous no. of outbound commands in an ftp session 1 if the login belongs to the "hot" list; 0 otherwise no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service and srv_serror_rate 29 same_srv_rate continuous and srv_serror_rate and srv_serror_rate 29 same_srv_rate continuous no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service no. of connections to different hosts no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of conne	7	land	discrete	
10 hot num_failed_logins continuous no. of "hot" indicators no. of failed login attempts 12 logged_in discrete 1 if successfully logged in; 0 otherwise no. of failed login attempts 14 root_shell discrete 1 if successfully logged in; 0 otherwise no. of "compromised" conditions 1 if root_shell is obtained; 0 otherwise 1 if "su root" normand attempted; 0 otherwise no. of "root" accesses number of file creation operations no. of shell prompts no. of shell prompts no. of otherwise no. of outbound commands in an ftp session 1 if the login belongs to the "hot" list; 0 otherwise no. of connections to the same service and srv_serror_rate 2 same_srv_rate 2 same_srv_rate 2 dst_host_srv_count 2 continuous 2 dst_host_srv_rate 3 dst_host_same_srv_rate 3 dst_host_srv_rate 3 dst_host_same_srv_rate 3 dst_host	8	wrong_fragment	continuous	no. of "wrong" fragments
11 num_failed_logins 12 logged_in 13 num_compromised 14 root_shell 15 su_attempted 16 num_root 17 num_file_creations 18 num_access_files 19 num_access_files 20 num_outbound_cmds 21 is_host_login 22 is_guest_login 23 count 24 srv_count 25-26 serror_rate 27-28 rerror_rate 29 same_srv_rate 29 same_srv_rate 21 sy_diff_host_rate 29 same_srv_rate 30 diff_srv_rate 31 sv_diff_host_rate 32 dst_host_soun_srv_rate 33 dst_host_srv_count 34 dst_host_srv_cuilf_host_rate 35 dst_host_same_srv_port_rate 36 dst_host_same_srv_perror_rate 37 dst_host_srv_eerror_rate 38-39 ddt_host_srv_error_rate 40-41 dst_host_rerror_rate 40-41	9	urgent	continuous	no. of urgent packets
12 logged_in num_compromised continuous no. of "compromised" conditions 14 root_shell discrete 1 if root_shell is obtained; 0 otherwise 1 if root_shell is obtained; 0 otherwise 1 if "out_root" command attempted; 0 otherwise 2 otherwise 2 otherwise 2 num_file_creations 2 continuous 2 num_file_creations 2 continuous 2 num_outbound_cmds 2 continuous 2 num_outbound_cmds 2 is_host_login 2 is_guest_login 2 is_guest_login 3 count 4 continuous 2 is_guest_login 4 continuous 2 is_guest_login 4 continuous 2 is_guest_login 5 count 6 continuous 2 is_guest_login 6 count 6 continuous 7 continuous 8 continuous 8 count 8 count 8 count 9 continuous 9 continuous 9 continuous 9 continuous 9 continuous 1 if the login belongs to the "hot" list; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login belongs to the "hot" list; 0 otherwise 1 if the login belongs to the "hot" list; 0 otherwise 1 if the login belongs to the "hot" list; 0 otherwise 1 if the login belongs to the "hot" list; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login belongs to the "hot" list; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 is the current co	10	hot	continuous	no. of "hot" indicators
num_compromised discrete 1 if root shell is obtained; 0 otherwise 1 if root sh	11	$num\_failed\_logins$	continuous	no. of failed login attempts
14 root_shell discrete discrete 1 if root shell is obtained; 0 otherwise 1 if "su root" command attempted; 0 otherwise 1 otherwise 2 is_guest_login discrete 2 is_guest_login discrete 2 is_guest_login discrete 2 if the login belongs to the "hot" list; 0 otherwise 2 otherwise 1 if the login is a "guest"login; 0 otherwise 2 otherwise 1 if the login is a "guest"login; 0 otherwise 2 otherwise 2 otherwise 1 if the login is a "guest"login; 0 otherwise 2	12	logged_in	discrete	1 if successfully logged in; 0 otherwise
15 su_attempted discrete 0 otherwise 16 num_root continuous no. of "root" accesses 17 num_file_creations continuous no. of shell prompts 18 num_shells continuous no. of shell prompts 19 num_access_files continuous no. of operations on access control files 20 num_outbound_cmds continuous no. of outbound commands in an ftp session 21 is_host_login discrete 1 if the login belongs to the "hot" list; 0 otherwise 22 is_guest_login discrete 1 if the login is a "guest"login; 0 otherwise 23 count continuous no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service no. of connections to the same service no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service no. of connections to the same service no. of connections to different hosts no. of connections to different hosts no. of connections to different hosts no. of connections to the same source port no. of connections to the same source port no. of connections that have "SYN" errors no. of conn	13	$num\_compromised$	continuous	no. of "compromised" conditions
16 num_root continuous number of file creation operations on of shell prompts no. of operations on access control files no. of outbound commands in an ftp session 1 if the login belongs to the "hot" list; of otherwise no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors no. of connections to the same service no. of connections to different services no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to different services no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same se	14	$root\_shell$	discrete	1 if root shell is obtained; 0 otherwise
16 num_root continuous no. of "root" accesses number of file creation operations no. of shell prompts no. of operations no. of shell prompts no. of operations no. of shell prompts no. of operations no. of opera	15	$su\_attempted$	discrete	1 if "su root" command attempted;
num_file_creations  num_shells  num_access_files  num_outbound_cmds  is_host_login  continuous  continuous  discrete  is_guest_login  continuous  continuous  continuous  discrete  is_guest_login  continuous  continuous  continuous  discrete  is_guest_login  continuous  continuous  continuous  continuous  discrete  if the login belongs to the "hot" list;  0 otherwise  1 if the login is a "guest"login; 0 otherwise  no. of connections to the same host  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same services  no. of connections to the same services  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  no. of connections to				0 otherwise
num_shells continuous no. of shell prompts num_access_files continuous no. of operations on access control files num_outbound_cmds continuous no. of outbound commands in an ftp session discrete 1 if the login belongs to the "hot" list; 0 otherwise 22 is_guest_login discrete 1 if the login is a "guest"login; 0 otherwise no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to different services no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to different services no. of connections to different hosts no. of connections to the same source port no. of connections to the same source port no. of connections that have "SYN" errors no. of connections that have "S	16	num_root	continuous	no. of "root" accesses
num_access_files  num_outbound_cmds  continuous  no. of operations on access control files  no. of outbound commands in an ftp session  1 if the login belongs to the "hot" list;  0 otherwise  22 is_guest_login  discrete  1 if the login is a "guest"login; 0 otherwise  23 count  continuous  no. of connections to the same host  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections that have "SYN" errors  and srv_serror_rate  27-28 rerror_rate and srv_rerror_rate  29 same_srv_rate  continuous  30 diff_srv_rate  31 srv_diff_host_rate  continuous  32 dst_host_count  continuous  33 dst_host_srv_count  continuous  continuous  continuous  no. of connections to different hosts  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to different hosts  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  no. of co	17	$num\_file\_creations$	continuous	number of file creation operations
num_outbound_cmds  is_host_login  discrete  1 if the login belongs to the "hot" list;  0 otherwise  22 is_guest_login  discrete  1 if the login belongs to the "hot" list;  0 otherwise  23 count  continuous  no. of connections to the same host  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections that have "SYN" errors  and srv_serror_rate  27-28 rerror_rate and srv_rerror_rate  29 same_srv_rate  continuous  30 diff_srv_rate  31 srv_diff_host_rate  32 dst_host_count  continuous  33 dst_host_same_srv_rate  34 dst_host_same_srv_rate  35 dst_host_diff_srv_rate  36 dst_host_same_src_port_rate  37 dst_host_srv_diff_host_rate  38-39 dst_host_srv_gerror_rate  40-41 dst_host_srv_serror_rate  continuous  no. of connections to the same source port  no. of connections to the same source port  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection to different hosts  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connections to the same service  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the pa	18	num_shells	continuous	no. of shell prompts
is_host_login  discrete  lif the login belongs to the "hot" list;  o otherwise  lif the login is a "guest"login; 0 otherwise  lif the login is a "guest"login; 0 otherwise  no. of connections to the same host  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections that have "SYN" errors  and srv_serror_rate  continuous  no. of connections that have "REJ" errors  no. of connections to the same service  no. of connections to different services  no. of connections to different hosts  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  as the current connection in the past 2 s  no. of connections to the same service  no. of con	19	num_access_files	continuous	no. of operations on access control files
is_guest_login discrete continuous no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors no. of connections that have "REJ" errors no. of connections to the same service no. of connections to the same service no. of connections to the same service no. of connections to different services no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection to the same service no. of connections to the same service no. of connections to the same service no. of connections to the same source port no. of connections to different hosts no. of connections to different hosts no. of connections to different hosts no. of connections to the same source port no. of connections to different hosts no. of connections to the same source port no. of connections to the same source no. of	20	$num\_outbound\_cmds$	continuous	no. of outbound commands in an ftp session
22 is_guest_login discrete continuous no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors and srv_serror_rate  27-28 rerror_rate and srv_rerror_rate continuous no. of connections that have "REJ" errors no. of connections to the same service no. of connections to different services no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection to the same service as the current connection to the same service as the current connections to different services no. of connections to different services no. of connections to the same source port no. of connections to the same source port no. of connections to the same source port no. of connections to the same service no. of connect	21	is_host_login	discrete	1 if the login belongs to the "hot" list;
count continuous no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors no. of connections that have "REJ" errors no. of connections to the same service no. of connections to the same service no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same source port no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections t				0 otherwise
as the current connection in the past 2 s  24 srv_count continuous  15 serror_rate  25-26 serror_rate  27-28 rerror_rate and srv_rerror_rate  27-28 rerror_rate and srv_rerror_rate  29 same_srv_rate  30 diff_srv_rate  31 srv_diff_host_rate  32 dst_host_count  33 dst_host_srv_count  34 dst_host_srv_count  35 dst_host_same_srv_rate  36 dst_host_same_src_port_rate  37 dst_host_same_src_port_rate  38-39 dst_host_srv_diff_host_rate  39 continuous  30 dst_host_srv_rate  30 diff_srv_rate  31 srv_diff_srv_rate  32 dst_host_srv_count  33 dst_host_srv_count  34 dst_host_same_srv_rate  35 dst_host_same_src_port_rate  36 dst_host_same_src_port_rate  37 dst_host_srv_diff_host_rate  38-39 dst_host_srv_diff_host_rate  38-39 dst_host_srv_serror_rate  40-41 dst_host_srv_serror_rate  40-41 dst_host_srrerror_rate  40-41 dst_host_srrerror_rate  40-41 dst_host_srrerror_rate  40-41 dst_host_srrerror_rate  40-41 continuous  40-41 continuous	$^{22}$	is_guest_login	discrete	1 if the login is a "guest" login; 0 otherwise
24 srv_count continuous no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors and srv_serror_rate continuous no. of connections that have "SYN" errors and srv_serror_rate continuous no. of connections that have "REJ" errors no. of connections to the same service no. of connections to the same service no. of connections to different services no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service no. of connections to different hosts no. of connections to the same source port dst_host_srv_diff_host_rate continuous no. of connections to different hosts no. of connections that have "SYN" errors no. of connections that have "REJ" errors	23	count	continuous	no. of connections to the same host
as the current connection in the past 2 s no. of connections that have "SYN" errors and srv_serror_rate  27-28 rerror_rate and srv_rerror_rate 29 same_srv_rate continuous 30 diff_srv_rate continuous 31 srv_diff_host_rate continuous 32 dst_host_count continuous 33 dst_host_srv_count 34 dst_host_same_srv_rate 35 dst_host_diff_srv_rate 36 dst_host_same_src_port_rate 37 dst_host_srv_diff_host_rate 38-39 dst_host_srv_serror_rate 39 continuous 40-41 dst_host_rerror_rate 40-41 dst_host_rerror_rate 40-41 dst_host_reror_rate 40-41 dst_host_r				as the current connection in the past 2 s
25-26 serror_rate continuous no. of connections that have "SYN" errors and srv_serror_rate  27-28 rerror_rate and srv_rerror_rate continuous no. of connections that have "REJ" errors  29 same_srv_rate continuous no. of connections to the same service  30 diff_srv_rate continuous no. of connections to different services  31 srv_diff_host_rate continuous no. of connections to different hosts  32 dst_host_count continuous no. of connections to different hosts  33 dst_host_srv_count continuous no. of connections to the same service as the current connection in the past 2 s  34 dst_host_same_srv_rate continuous no. of connections to the same service as the current connection in the past 2 s  35 dst_host_diff_srv_rate continuous no. of connections to the same service no. of connections to the same service continuous no. of connections to the same service no. of connections to different services no. of connections to the same source port no. of connections to the same source port continuous no. of connections to the same source port no. of connections to different hosts  38-39 dst_host_srv_diff_host_rate continuous no. of connections to different hosts  38-39 dst_host_srv_serror_rate continuous no. of connections to the same source port no. of connections to the same source port no. of connections to the same source port continuous no. of connections that have "SYN" errors no. of connections that have "REJ" errors	$^{24}$	$srv\_count$	continuous	
and srv_serror_rate  27-28 rerror_rate and srv_rerror_rate continuous no. of connections that have "REJ" errors  29 same_srv_rate continuous no. of connections to the same service  30 diff_srv_rate continuous no. of connections to different services  31 srv_diff_host_rate continuous no. of connections to different hosts  32 dst_host_count continuous no. of connections to the same service  33 dst_host_srv_count continuous no. of connections to the same service  34 dst_host_same_srv_rate continuous no. of connections to the same service  35 dst_host_diff_srv_rate continuous no. of connections to the same service  36 dst_host_same_src_port_rate continuous no. of connections to different services  37 dst_host_srv_diff_host_rate continuous no. of connections to the same source port  38-39 dst_host_srv_diff_host_rate continuous no. of connections to different hosts  38-39 dst_host_srv_serror_rate continuous no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "REJ" errors				
27-28 rerror_rate and srv_rerror_rate continuous no. of connections that have "REJ" errors continuous no. of connections to the same service no. of connections to different services no. of connections to different services no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to different services no. of connections to different services no. of connections to the same source port continuous no. of connections to the same source port no. of connections to different hosts no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "REJ" errors	25-26	serror_rate	continuous	no. of connections that have "SYN" errors
29 same_srv_rate continuous no. of connections to the same service 30 diff_srv_rate continuous no. of connections to different services 31 srv_diff_host_rate continuous no. of connections to different hosts 32 dst_host_count continuous no. of connections to the same service 33 dst_host_srv_count continuous no. of connections to the same service 34 dst_host_same_srv_rate continuous no. of connections to the same service 35 dst_host_diff_srv_rate continuous no. of connections to the same service 36 dst_host_same_src_port_rate continuous no. of connections to different services 37 dst_host_srv_diff_host_rate continuous no. of connections to the same source port continuous no. of connections to different hosts 38-39 dst_host_serror_rate continuous no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "REJ" errors		and srv_serror_rate		
30 diff_srv_rate continuous no. of connections to different services 31 srv_diff_host_rate continuous no. of connections to different hosts 32 dst_host_count continuous no. of connections to the same service as the current connection in the past 2 s 33 dst_host_srv_count continuous no. of connections to the same service as the current connection in the past 2 s 34 dst_host_same_srv_rate continuous no. of connections to the same service 35 dst_host_diff_srv_rate continuous no. of connections to different services 36 dst_host_same_src_port_rate continuous no. of connections to the same source port continuous no. of connections to different hosts 38-39 dst_host_srv_diff_host_rate continuous no. of connections to different hosts 38-39 dst_host_srv_serror_rate continuous no. of connections that have "SYN" errors no. of connections that have "SYN" errors and dst_host_srv_serror_rate continuous no. of connections that have "REJ" errors	27-28		continuous	
31 srv_diff_host_rate continuous no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to different services no. of connections to different services no. of connections to the same source port continuous no. of connections to different hosts no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "REJ" errors	29		continuous	no. of connections to the same service
dst_host_count continuous no. of connections to the same service as the current connection in the past 2 s  dst_host_srv_count continuous no. of connections to the same service as the current connection in the past 2 s  dst_host_same_srv_rate continuous no. of connections to the same service as the current connection in the past 2 s  dst_host_same_srv_rate continuous no. of connections to the same service no. of connections to different services  dst_host_same_src_port_rate continuous no. of connections to the same source port continuous no. of connections to different hosts  dst_host_srv_diff_host_rate continuous no. of connections that have "SYN" errors and dst_host_srv_serror_rate no. of connections that have "SYN" errors  dst_host_rerror_rate continuous no. of connections that have "REJ" errors	30		continuous	no. of connections to different services
as the current connection in the past 2 s  33 dst_host_srv_count  34 dst_host_same_srv_rate 35 dst_host_diff_srv_rate 36 dst_host_same_src_port_rate 37 dst_host_srv_diff_host_rate 38-39 dst_host_serror_rate 38-39 dst_host_srv_serror_rate 38-39 dst_host_srv_serror_rate 39-40-41 dst_host_rerror_rate 40-41 dst_host_rerror_rate 40-41 dst_host_rerror_rate  38 the current connection in the past 2 s  no. of connections to the same service no. of connections to different services no. of connections to different hosts continuous no. of connections to different hosts no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "REJ" errors	31	$srv\_diff\_host\_rate$	continuous	no. of connections to different hosts
dst_host_srv_count  continuous  no. of connections to the same service as the current connection in the past 2 s  dst_host_same_srv_rate  continuous  no. of connections to the same service as the current connection in the past 2 s  no. of connections to the same service  no. of connections to the same service  continuous  no. of connections to the same service  no. of connections to different services  continuous  no. of connections to the same service  continuous  no. of connections to different services  no. of connections to the same source port  continuous  no. of connections to different hosts  continuous  no. of connections to the same service  continuous  no. of connections to the same service  no. of connections to the same service  continuous  no. of connections that have "SYN" errors  no. of connections that have "SYN" errors  no. of connections that have "REJ" errors	32	$dst\_host\_count$	continuous	no. of connections to the same service
as the current connection in the past 2 s  34				as the current connection in the past 2 s
dst_host_same_srv_rate continuous no. of connections to the same service dst_host_diff_srv_rate continuous no. of connections to different services dst_host_same_src_port_rate continuous no. of connections to different services continuous no. of connections to the same source port continuous no. of connections to different hosts dst_host_srv_diff_host_rate continuous no. of connections to different hosts continuous no. of connections to the same service no. of connections to the same service continuous no. of connections to the same service no. of connections to the same service no. of connections to the same service continuous no. of connections to the same service no. of connections to the same service continuous no. of connections to different hosts no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "REJ" errors	33	$dst\_host\_srv\_count$	continuous	no. of connections to the same service
dst_host_diff_srv_rate continuous no. of connections to different services  dst_host_same_src_port_rate continuous no. of connections to different services  continuous  no. of connections to different services  no. of connections to different services  no. of connections that have "SYN" errors				•
36 dst_host_same_src_port_rate continuous no. of connections to the same source port 37 dst_host_srv_diff_host_rate continuous no. of connections to different hosts 38-39 dst_host_serror_rate continuous no. of connections that have "SYN" errors and dst_host_srv_serror_rate no. of connections that have "SYN" errors 40-41 dst_host_rerror_rate continuous no. of connections that have "REJ" errors				
37 dst_host_srv_diff_host_rate continuous no. of connections to different hosts 38-39 dst_host_serror_rate continuous no. of connections that have "SYN" errors and dst_host_srv_serror_rate no. of connections that have "SYN" errors 40-41 dst_host_rerror_rate continuous no. of connections that have "REJ" errors			continuous	
38-39 dst_host_serror_rate continuous no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "SYN" errors dst_host_rerror_rate continuous no. of connections that have "REJ" errors				_
and dst_host_srv_serror_rate no. of connections that have "SYN" errors dst_host_rerror_rate continuous no. of connections that have "REJ" errors				
40-41 dst_host_rerror_rate continuous no. of connections that have "REJ" errors	38-39		continuous	
and dst_host_srv_rerror_rate	40-41		continuous	no. of connections that have "REJ" errors
		and dst_host_srv_rerror_rate		

#### References:

[1] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl.*, Ottawa, ON, Canada, July 2009, pp. 1–6.

[2] J. McHugh, "Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln laboratory," *ACM Trans. Inform. Syst. Secur.*, vol. 3, no. 4, pp. 262–294, Nov. 2000.

#### 3. Go back to Google Drive:

#### **Create your own copy of the folder:**

ML\_in\_DCN \_teamNumber

\* Note: This is very important so that you do not alter the original code.

While in your own folder on Google Drive, upload your data, run (double click) on: *INCS775 Lab2 MLinDCN.ipvnb* 

#### Note:

We assume that you do not already have the Colab web application. To use Colab, select "Open with", search for Application named Colaboratory, and install it. Finally, connect to the Application.

For advanced users only:

----

If you wish to run the exercise locally, you need to install Jupyter's development environment.

Instructions are posted at:

https://jupyter-notebook.readthedocs.io/en/stable/

To install Jupyter, you will also need the "pip" package management system (installer) for Python:

python get-pip.py

Instruction is available at:

https://jupyter.org/install

----

## 4. You are now ready to follow the steps:

INCS775\_Lab2\_ MLinDCN.ipynb

Scientific Computing and Machine learning libraries may be used:

- https://numpy.org/: numpy (built-in)
- https://scikit-learn.org/stable/index.html: sklearn
- https://pandas.pydata.org/: pandas
- https://pytorch.org/: torch
- https://www.tensorflow.org/: tensorflow

## **Grading Scheme** (total 10 points)

- 1. Code implementation: (even if not completed) (7 points)
- 2. Results can be regenerated based on the submission: (1 point)
- 3. Steps/explanations/comments: (2 points)

## **Please Submit:**

- Code (.ipynb), and please keep the output in the .ipynb file. Include code, steps/explanations/comments in the .ipynb file.
- Submit the file for your project submission to the Canvas site.
   Additionally, the link to the Colab can also be provided in the comments for better grading.
- Note:

More credit will be given to completed assignments than to ambitious unfinished work. In the case of teamwork, we will make every attempt to evaluate the individual performance of each team member.