

**TOPIC NAME : Network Intrusion Detection using Machine Learning Technique**

**Real time network based intrusion detection using decision tree**

WHAT NSL-KDD FEATURES CONTAIN 41 Features

@relation 'KDDTest'

@attribute 'duration' real [not found]

@attribute 'protocol\_type' {'tcp','udp', 'icmp'} [found]

@attribute 'service' {'aol', 'auth', 'bgp', 'courier', 'csnet\_ns', 'ctf', 'daytime', 'discard', 'domain', 'domain\_u', 'echo', 'eco\_i', 'ecr\_i', 'efs', 'exec', 'finger', 'ftp', 'ftp\_data', 'gopher', 'harvest', 'hostnames', 'http', 'http\_2784', 'http\_443', 'http\_8001', 'imap4', 'IRC', 'iso\_tsap', 'klogin', 'kshell', 'ldap', 'link', 'login', 'mtp', 'name', 'netbios\_dgm', 'netbios\_ns', 'netbios\_ssn', 'netstat', 'nnsp', 'nntp', 'ntp\_u', 'other', 'pm\_dump', 'pop\_2', 'pop\_3', 'printer', 'private', 'red\_i', 'remote\_job', 'rje', 'shell', 'smtp', 'sql\_net', 'ssh', 'sunrpc', 'supdup', 'systat', 'telnet', 'tftp\_u', 'tim\_i', 'time', 'urh\_i', 'urp\_i', 'uucp', 'uucp\_path', 'vmnet', 'whois', 'X11', 'Z39\_50'} [not found]

@attribute 'flag' { 'OTH', 'REJ', 'RSTO', 'RSTOS0', 'RSTR', 'S0', 'S1', 'S2', 'S3', 'SF', 'SH' } [not found]

@attribute 'src\_bytes' real [not found]

@attribute 'dst\_bytes' real [not found]

@attribute 'land' {'0', '1'}

@attribute 'wrong\_fragment' real [not found]

@attribute 'urgent' real

@attribute 'hot' real [not found]

@attribute 'num\_failed\_logins' real [not found]

@attribute 'logged\_in' {'0', '1'} [not found]

@attribute 'num\_compromised' real [not found]

@attribute 'root\_shell' real [not found]

@attribute 'su\_attempted' real [not found]

@attribute 'num\_root' real [not found]

@attribute 'num\_file\_creations' real [not found]

@attribute 'num\_shells' real [not found]

@attribute 'num\_access\_files' real [not found]

@attribute 'num\_outbound\_cmds' real [not found]

@attribute 'is\_host\_login' {'0', '1'} [not found]

@attribute 'is\_guest\_login' {'0', '1'} [not found]

@attribute 'count' real

@attribute 'srv\_count' real

@attribute 'serror\_rate' real [not found]

@attribute 'srv\_serror\_rate' real [not found]

@attribute 'rerror\_rate' real [not found]

@attribute 'srv\_rerror\_rate' real [not found]

@attribute 'same\_srv\_rate' real [not found]

@attribute 'diff\_srv\_rate' real [not found]

@attribute 'srv\_diff\_host\_rate' real [not found]

@attribute 'dst\_host\_count' real

@attribute 'dst\_host\_srv\_count' real

@attribute 'dst\_host\_same\_srv\_rate' real [not found]

@attribute 'dst\_host\_diff\_srv\_rate' real [not found]

@attribute 'dst\_host\_same\_src\_port\_rate' real [not found]

@attribute 'dst\_host\_srv\_diff\_host\_rate' real [not found]

@attribute 'dst\_host\_serror\_rate' real [not found]

@attribute 'dst\_host\_srv\_serror\_rate' real [not found]

@attribute 'dst\_host\_rerror\_rate' real [not found]

@attribute 'dst\_host\_srv\_rerror\_rate' real [not found]

@attribute 'class' {'normal', 'anomaly'}

**7 COMMON FEATURES**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**protocol**

**land**

**urgent**

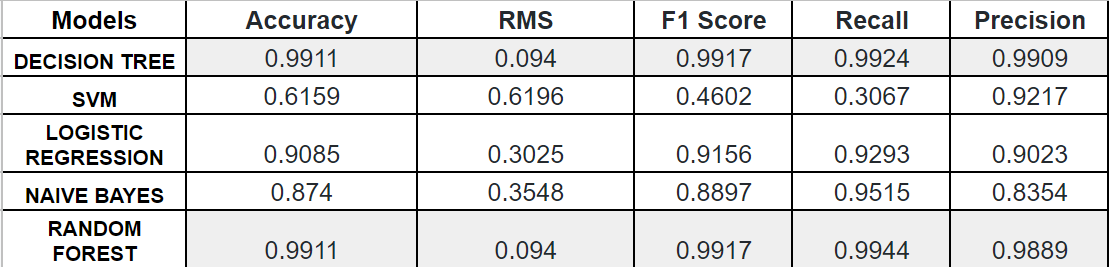
**count**

**srv count**

**dst\_host\_count**

**Dst\_host\_srv\_count**

**RESULT OBTAINED BY TRAINING THE 7 FEATURES**

****

DOUBTS:

**Count-** Number of connection to the same destination host as the current connection in the past two second.

**Srv\_Count-** Number of connection to the same service(port number) as the current connection in the past two second.

**Dst\_host\_count**- number of connection having the same destination Ip address.

**Dst\_host\_srv\_count**- number of connection having the same port number.

THE DATA WE HAVE FROM SINGLE PACKET:

Layer ETH:

Destination: 1c:4d:70:68:cb:58

Address: 1c:4d:70:68:cb:58

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

Source: 00:1e:a6:3a:b6:78

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Address: 00:1e:a6:3a:b6:78

Layer IP:

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 52

Identification: 0x0000 (0)

Flags: 0x40, Don't fragment

0... .... = Reserved bit: Not set

.1.. .... = Don't fragment: Set

..0. .... = More fragments: Not set

Fragment Offset: 0

Time to Live: 62

Protocol: TCP (6)

Header Checksum: 0x2bb1 [validation disabled]

Header checksum status: Unverified

Source Address: 142.250.192.10

Destination Address: 192.168.1.102

Layer TCP:

Source Port: 443

Destination Port: 26654

Stream index: 0

TCP Segment Len: 0

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 2698175263

Next Sequence Number: 1 (relative sequence number)

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 4080155540

1000 .... = Header Length: 32 bytes (8)

Flags: 0x010 (ACK)

000. .... .... = Reserved: Not set

...0 .... .... = Nonce: Not set

.... 0... .... = Congestion Window Reduced (CWR): Not set

.... .0.. .... = ECN-Echo: Not set

.... ..0. .... = Urgent: Not set

.... ...1 .... = Acknowledgment: Set

.... .... 0... = Push: Not set

.... .... .0.. = Reset: Not set

.... .... ..0. = Syn: Not set

.... .... ...0 = Fin: Not set

TCP Flags: ·······A····

Window: 276

Calculated window size: 276

Window size scaling factor: -1 (unknown)

Checksum: 0x0fdc [unverified]

Checksum Status: Unverified

Urgent Pointer: 0

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

TCP Option - No-Operation (NOP)

Kind: No-Operation (1)

TCP Option - Timestamps: TSval 305562517, TSecr 8692183

Length: 10

Timestamp value: 305562517

Timestamp echo reply: 8692183

Timestamps

Time since first frame in this TCP stream: 0.000000000 seconds

Time since previous frame in this TCP stream: 0.000000000 seconds

TCP Option - No-Operation (NOP)

Kind: No-Operation (1)

Kind: Time Stamp Option (8)