Traffic Anomaly Detection in SDN Using Deep Learning

Motivation:

- Rule-based firewalls are rigid and outdated
- SDN offers control, but opens new attack risks
- Deep Learning enables smart, real-time anomaly detection

Key Points:

- Simulate SDN using Mininet and Floodlight
- Collect flow-level traffic data using Floodlight Rest APIs
- Use DL models such as LSTM/Transformers to detect unusual traffic behaviour in real time

Simulation Topology & Floodlight Controller

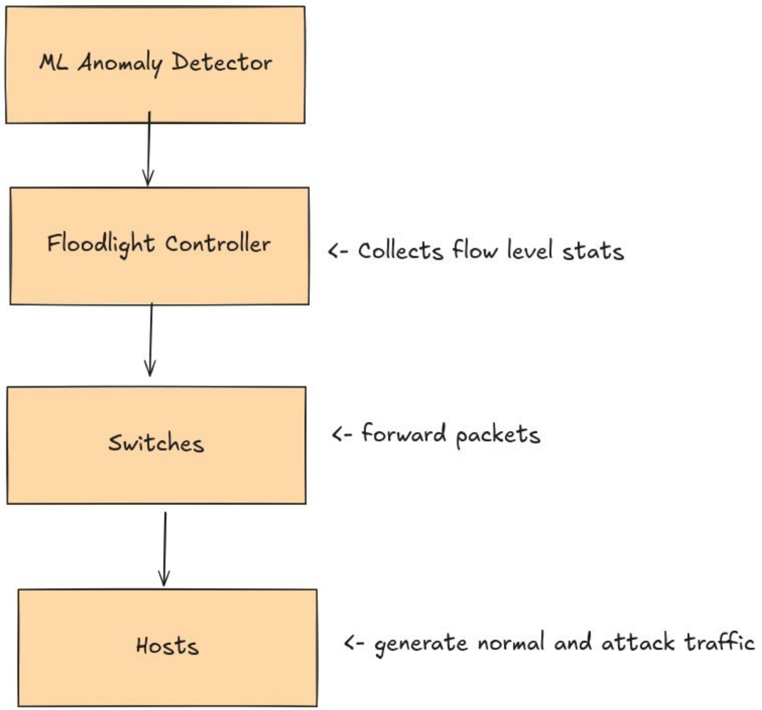
Network Setup:

- 6 Hosts (h1–h6)
- 3 Switches (s1–s3) in tree topology (depth=2, fanout=2)
- 1 Floodlight Controller running in Docker

Traffic:

- Normal: ping, iperf, curl
- Attacks: hping3, port scanning scripts

System Architecture



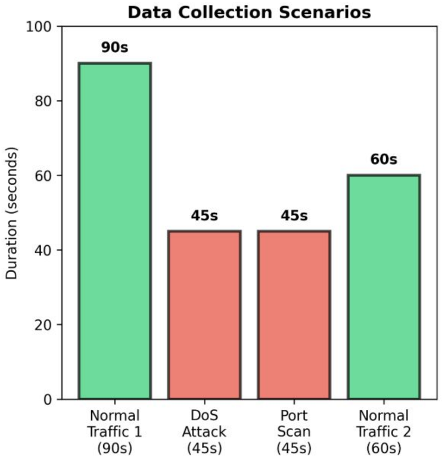
Data Collection

Network Topology:

- Mininet: 6 hosts, 3 OpenFlow switches
- Floodlight controller (OpenFlow 1.3)
- Tree topology

Dataset:

- Total flows: 1,340
- Normal: 806 (60%)
- Attack: 534 (40%)



Traffic Generation:

Normal Traffic:

- ICMP (ping)
- TCP (iperf)
- HTTP (wget)

Attack Traffic:

- DoS attacks (flooding)
- Port scanning

GET http://localhost:8080/wm/core/switch/all/flow/json

```
"flows": [
      {
        "match": {
          "in_port": 1,
          "eth_type": "0x0800",        // IPv4
          "ipv4_src": "10.0.0.1",
          "ipv4_dst": "10.0.0.2",
          "ip_proto": "6",             // TCP
          "tcp_src": 54321,
          "tcp_dst": 80
        },
        "actions": [
          {
            "type": "OUTPUT",
            "port": 2
          }
        ],
        "packet_count": 42,            // <- Key statistic
        "byte_count": 2688,            // <- Key statistic
        "duration_sec": 5,             // <- Key statistic
        "priority": 100,
        "idle_timeout": 60,
        "hard_timeout": 0,
        "cookie": "0x0"
      }
      // ... more flows
    ]
```

Features & Model

Raw Features:

- packet_count
- byte_count
- duration_sec

Derived Features:

- packet_rate (pkt/sec)
- byte_rate (bytes/sec)
- avg_packet_size

Training:

- 80/20 train/test split
- 30 epochs, Adam optimizer
- Cross-entropy loss

Model Architecture:

- LSTM (Long Short-Term Memory)
- Input: Sequences of 10 consecutive flows
- 2 layers, 64 hidden units each
- Output: Binary classification (normal/attack)

Results

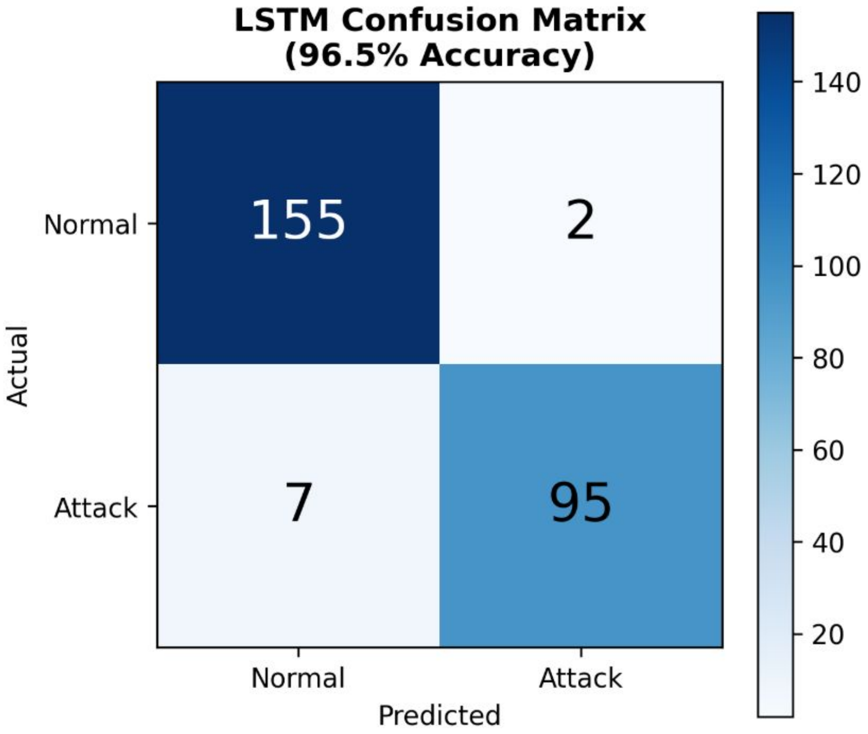
Model Performance:

Accuracy: 96.53%

Precision: 97.94%

Recall: 93.14%

F1-Score: 95.48%



Demo Script

```
======================================================================
Normal Traffic
Flow: 10.0.0.2 → 10.0.0.5 [s1]
----------------------------------------------------------------------
Packets:         2  |  Bytes:          108
Duration:     0.15s |  Pkt Rate:    13.07 pkt/s
----------------------------------------------------------------------
→ NORMAL (100%) - ALLOW
======================================================================

======================================================================
Normal Traffic
Flow: 10.0.0.2 → 10.0.0.5 [s1]
----------------------------------------------------------------------
Packets:         2  |  Bytes:          108
Duration:     0.15s |  Pkt Rate:    13.61 pkt/s
----------------------------------------------------------------------
→ NORMAL (100%) - ALLOW
======================================================================
```

```
======================================================================
ATTACK DETECTED!
Flow: 10.0.0.5 → 10.0.0.2 [s1]
----------------------------------------------------------------------
Packets:         2  |  Bytes:          108
Duration:     1.27s |  Pkt Rate:     1.57 pkt/s
----------------------------------------------------------------------
→ ATTACK (99%) - BLOCK
======================================================================

======================================================================
ATTACK DETECTED!
Flow: 10.0.0.5 → 10.0.0.2 [s1]
----------------------------------------------------------------------
Packets:         2  |  Bytes:          108
Duration:     1.27s |  Pkt Rate:     1.57 pkt/s
----------------------------------------------------------------------
→ ATTACK (99%) - BLOCK
======================================================================
```

```
===================================
  DEMO COMPLETE - FINAL RESULTS
===================================
  Total Flows:       27871
  Normal:            2117
  Attacks Detected:  25754
===================================

===================================
```

Limitations

Current Limitations:

1. Simulated Environment

2. Limited Attack Diversity

3. Dataset Size

   - 1,340 flows (proof-of-concept)

4. Flow Aggregation

   - OpenFlow aggregates packets into flows

Future Work

- Test on real network traces
- Add more attack types (DDoS, SQL injection, etc.)
- Larger, more diverse dataset
- Deploy on production SDN controller
- Real-time anomaly response (block malicious flows)

Conclusion

✓ Proposed flow-based anomaly detection for SDN

✓ Used LSTM to learn from OpenFlow statistics

✓ Achieved 96.5% accuracy without external IDS

✓ Demonstrated feasibility of ML/DL-based SDN security

Key Contributions:

- Real-time flow-based detection
- Proof-of-concept validation