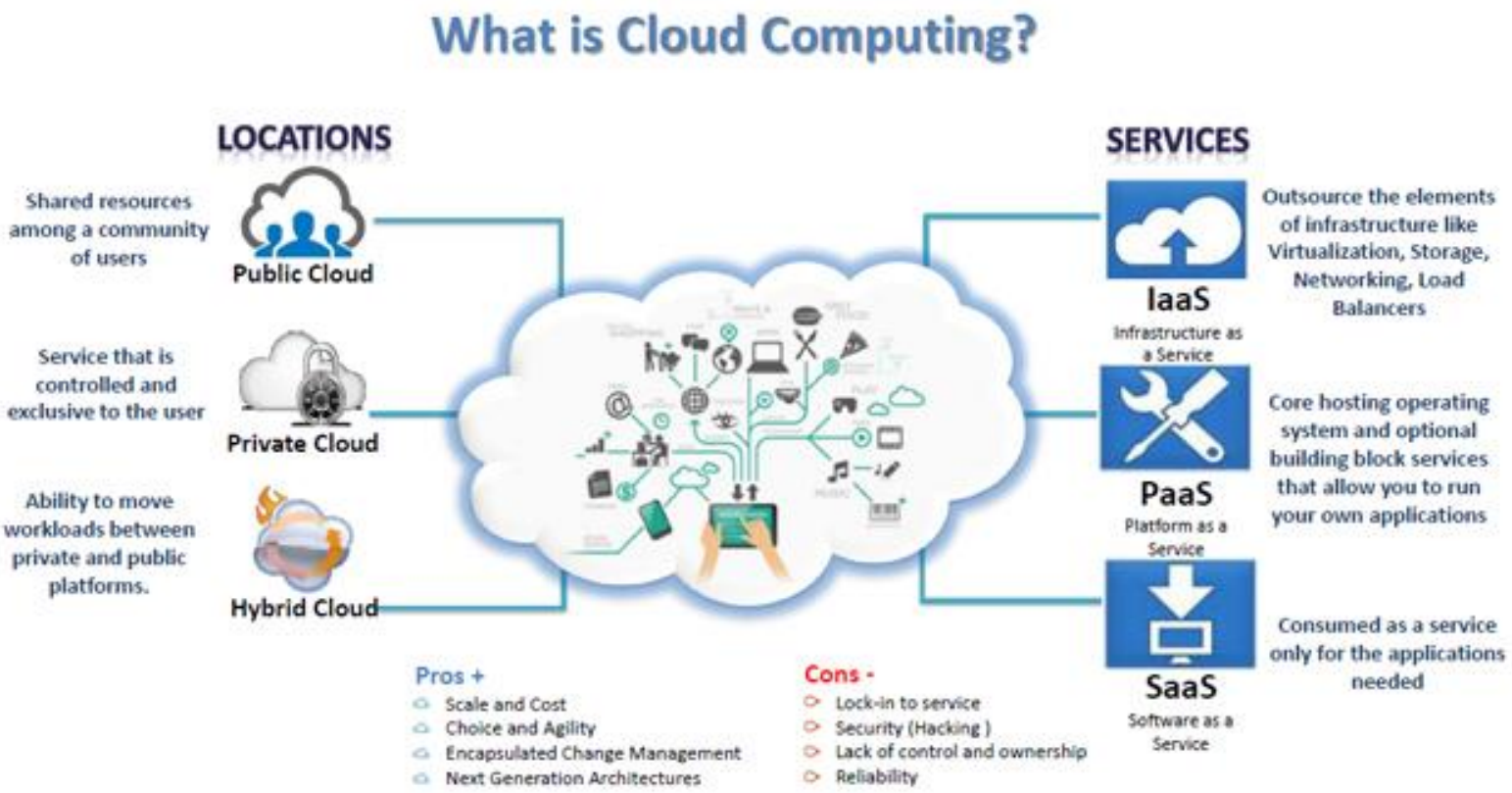
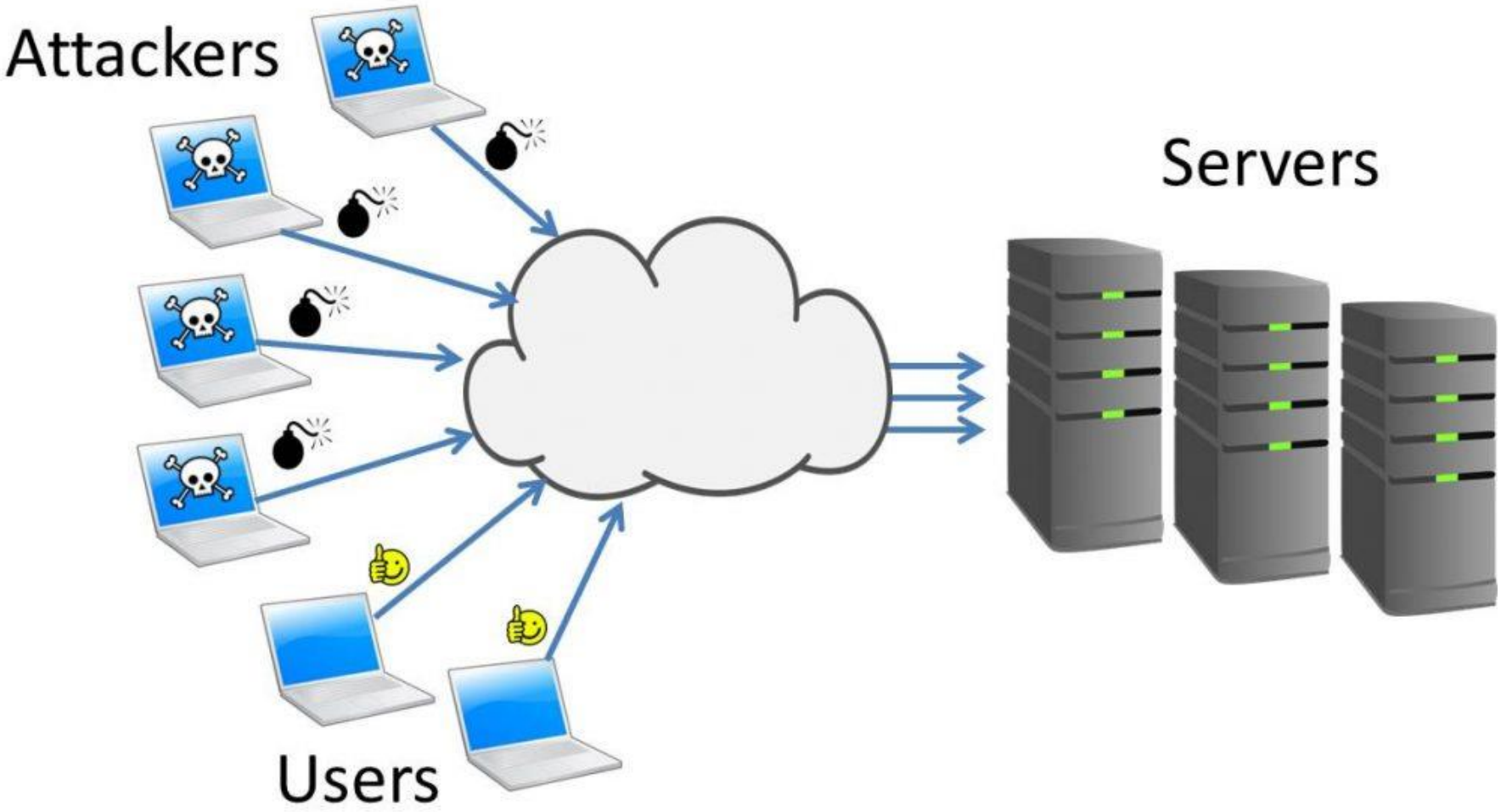
Two-phase Deep learning-based EDoS Detection

Authors: Chien Nguyen Nhu
Park Minho

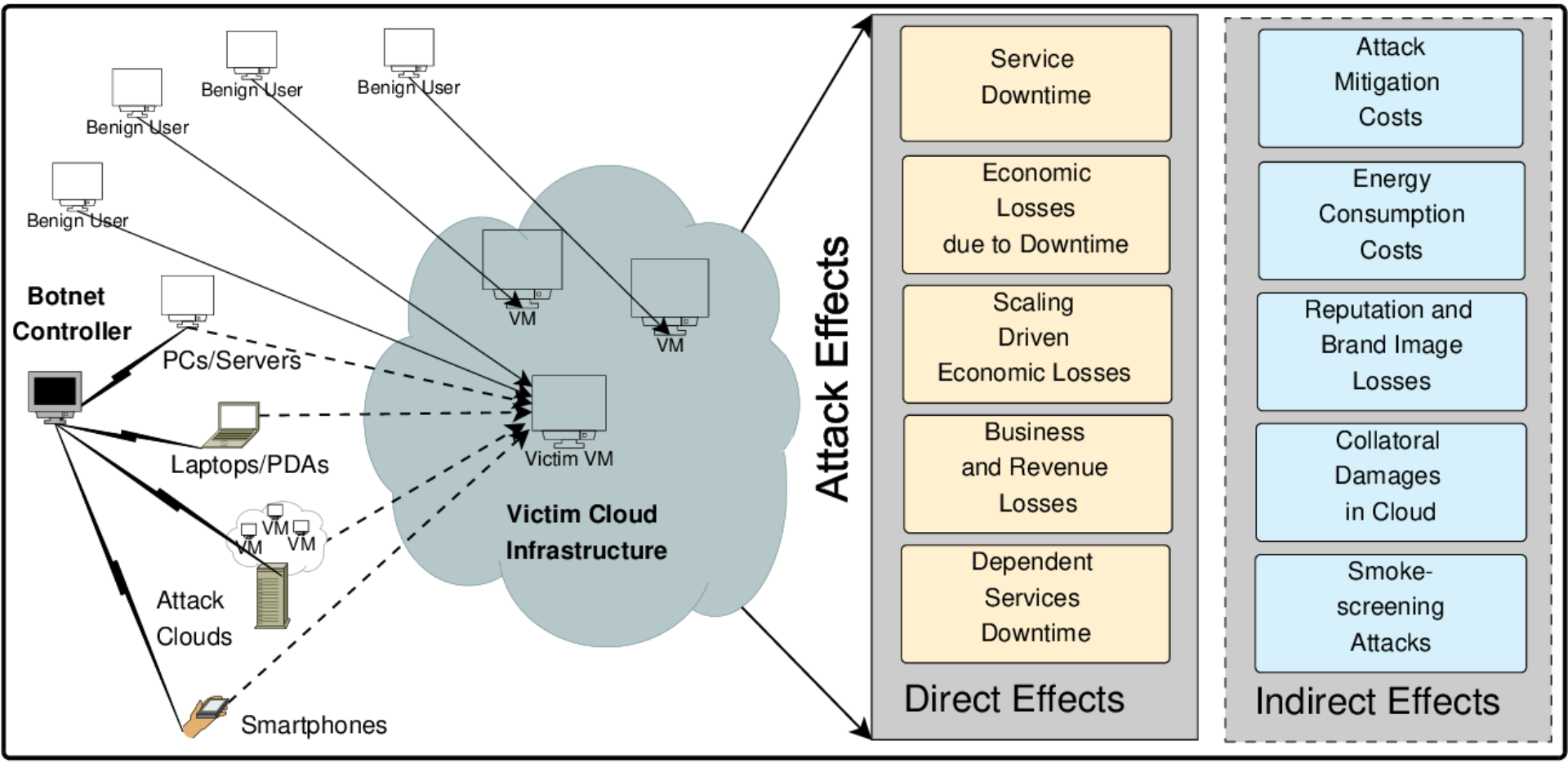
DDoS attack in Cloud Computing



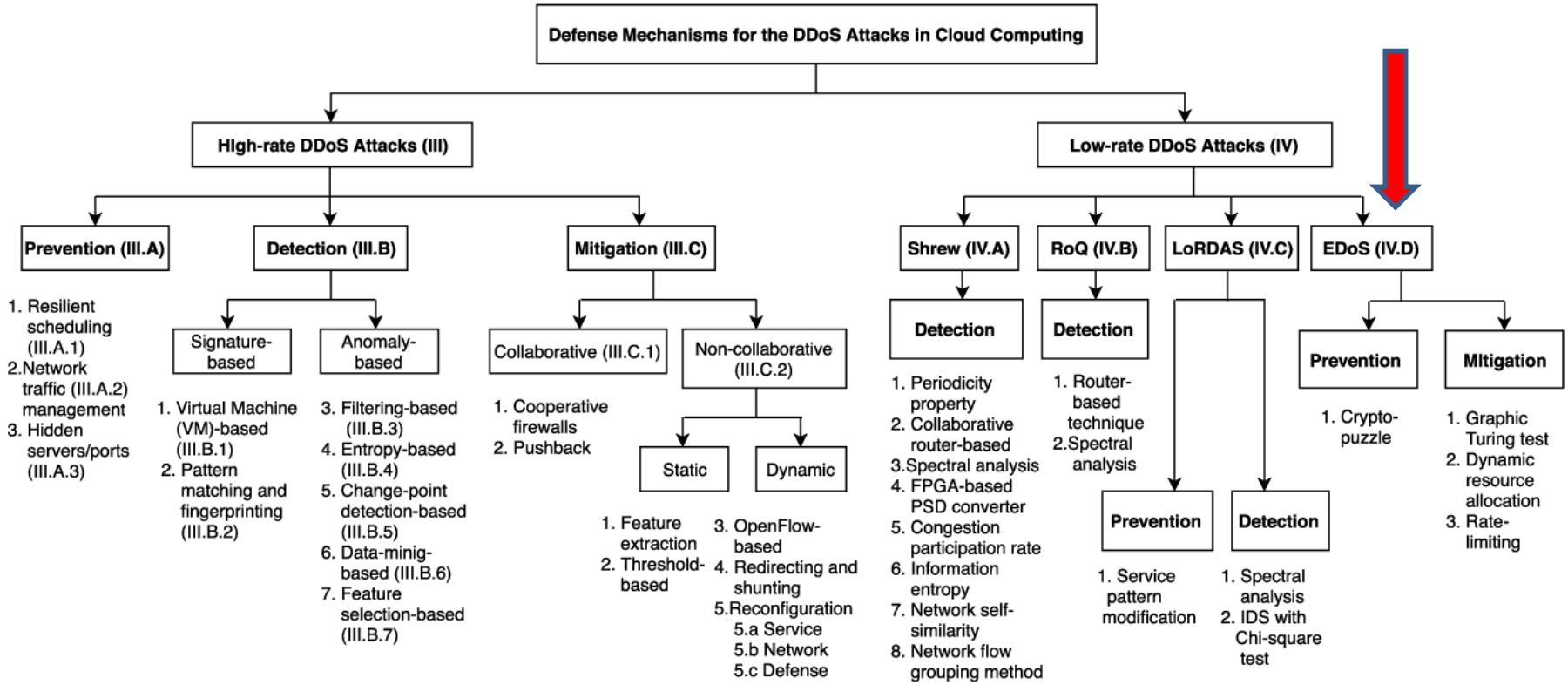
DDoS attack in Cloud Computing



DDoS attack in Cloud Computing



EDoS attack detection



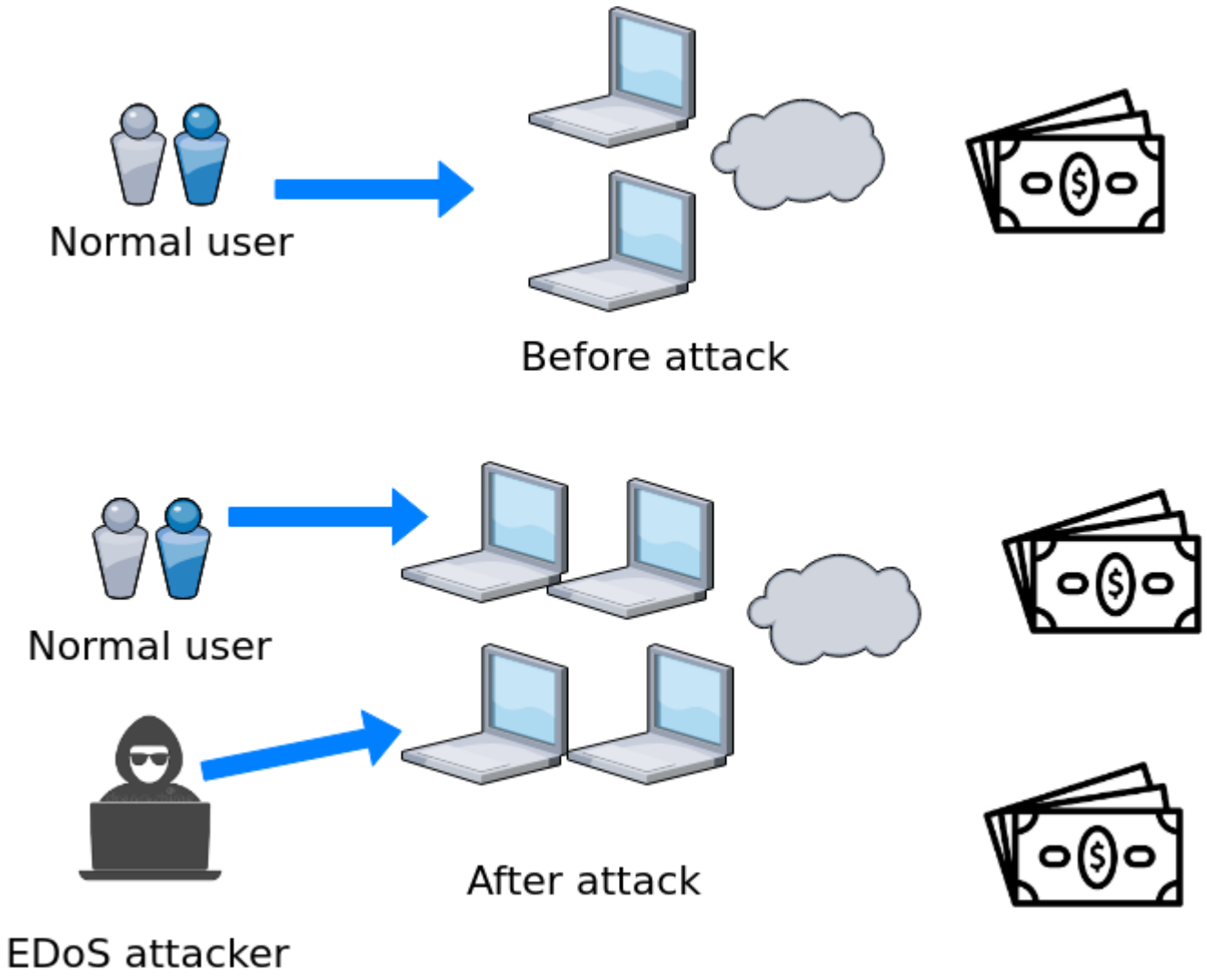
EDoS attack

Although EDoS is another variant of low-rate DDoS attack, it has some diff erent points with DDoS attack.

- A high-rate DDoS attack wants to shut down a service offered by a clou d server. Thus, the attackers irrationally launch an attack over a short am ount of time with their maximum resources to disrupt the server as soon as posibe.
- An EDoS attack exploits the auto-scaling feature and pay-as-you-go feature of cloud computing. It launches an attack to make the server have to require more new virtual machines or resources from cloud providers. The cloud consumer has to pay more for new resources and lead to bankruptcy if the attack is maintained for a long time. Thus, the EDoS attacker will gradually push illegitimate traffic over a longer period of time and with a slower rate attack.

=> EDoS attack's behavior is quite similar as normal requests.

EDoS attack


Normal user
Before attack
Normal user
EDoS attacker
After attack

Related works

-Almost the existing researches which focused on mitigation are based on graphical turing test, crypto-puzzle or predefined threshold to distinguish normal and abnormal traffic.

However, these solutions leads to high false-negative and false-positive Rates and increase end-to-end latency of the system.

Abbasi *et.al* " ***Machine Learning-Based EDoS attack Detection Technique Using Execution Trace Analysis***""proposes a machine learning-based metho d (SVM) to detect EDoS attack. They also propose a new set of metrics to cl assify 3 kinds of EDoS attack and normal traffic.

Our limitation: their system only detects there is an attack happening in Traffic and warns the system server to react not suppling resources for the s erver instead of detect which exact flow is abnormal flows

Related works

The EDoS attack rate looks similar to the legitimate network traffic from the victim-end in each time period. To detect this kind of slow rate attacks efficiently, it is required to trace or collect the historical information of the attack source. Thus, LSTM or GRU-two variants of RNN are proposed in 2 researches in EDoS detection([1]"***Dynamic Economic-Denial-of-Sustainability (EDoS) Detection in SDN-based Cloud***," [2]"***R-EDoS: Robust Economic Denial of Sustain- ability Detection in an SDN-Based Cloud Through Stochastic Recurrent Neural Network***"). These algorithms can handle sequential relationship data problems very effectively. Mechanisms on two paper achieve high accuracy and are evaluated via a lot of metrics such as accuracy, detection time, cost and complexity.

However, using LSTM and GRU leads to the problem of high resources consumption. The sequence length of input data required for two algorithms is long (250 and 100). It makes the detection time become longer and the resources of the defense system being high.

Problem statement

As shown in the above review, no existing proposals have the right approach which can both achieve high accuracy, use less resources and detect on each flow of network traffic in EDoS attacks tackling.

The idea

Recognizing that using LSTM or other variants of RNN for EDoS attack detection in each flow of network traffic can achieves high accuracy and low-false alarm rate than other approaches, we want to take this advantage but eliminating the disadvantage of this algorithm which is requires a long sequential input data (make the entire system consumes more resources and the calculation time increases).

=>we propose a two-phase deep learning based EDoS detection scheme using the LSTM algorithm to detect and mitigate each abnormal flow; how- e ver, the sequence length of the LSTM model is reduced significantly.

System Description

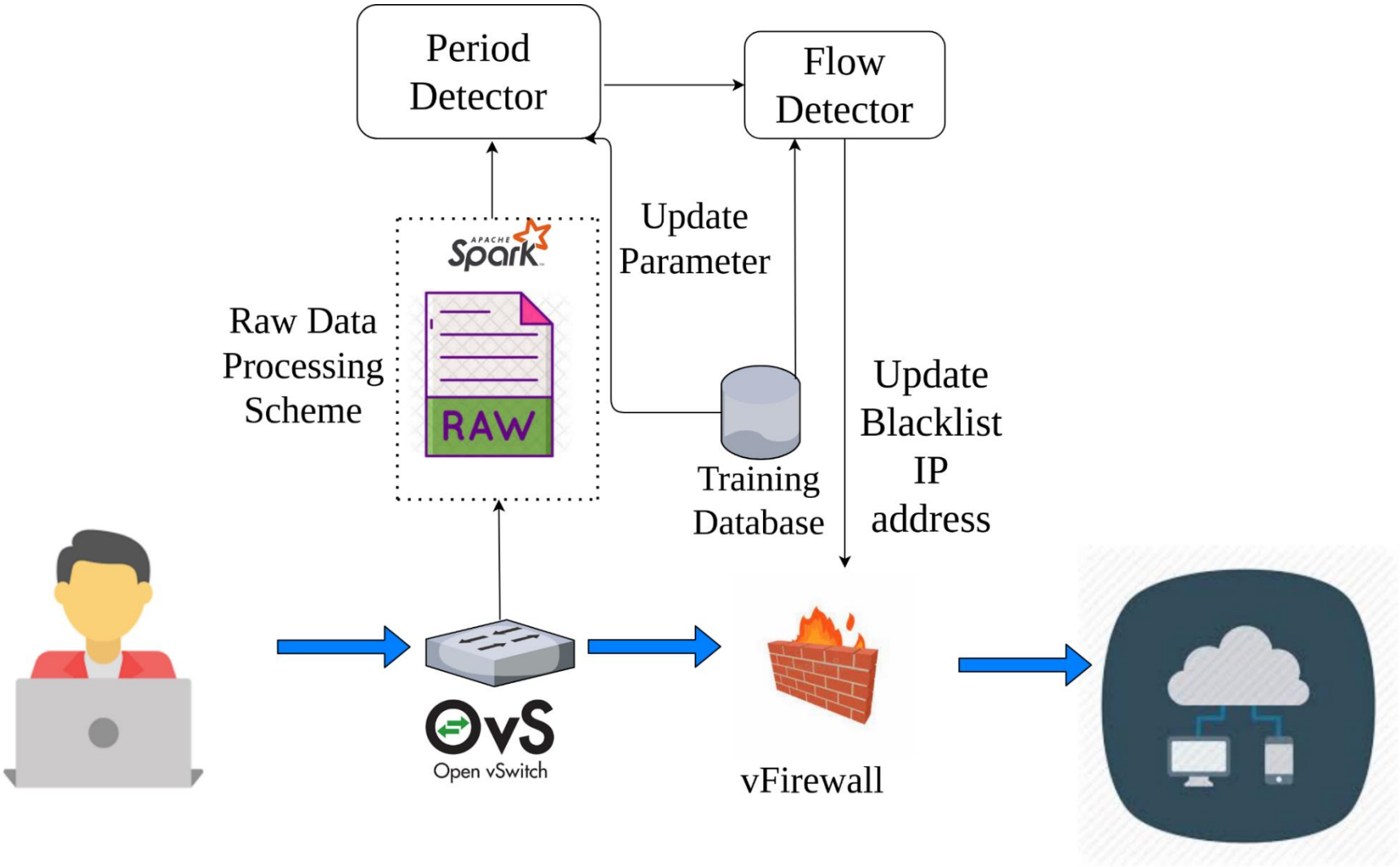


Figure 1: Conceptual architecture of the proposed model

System Description

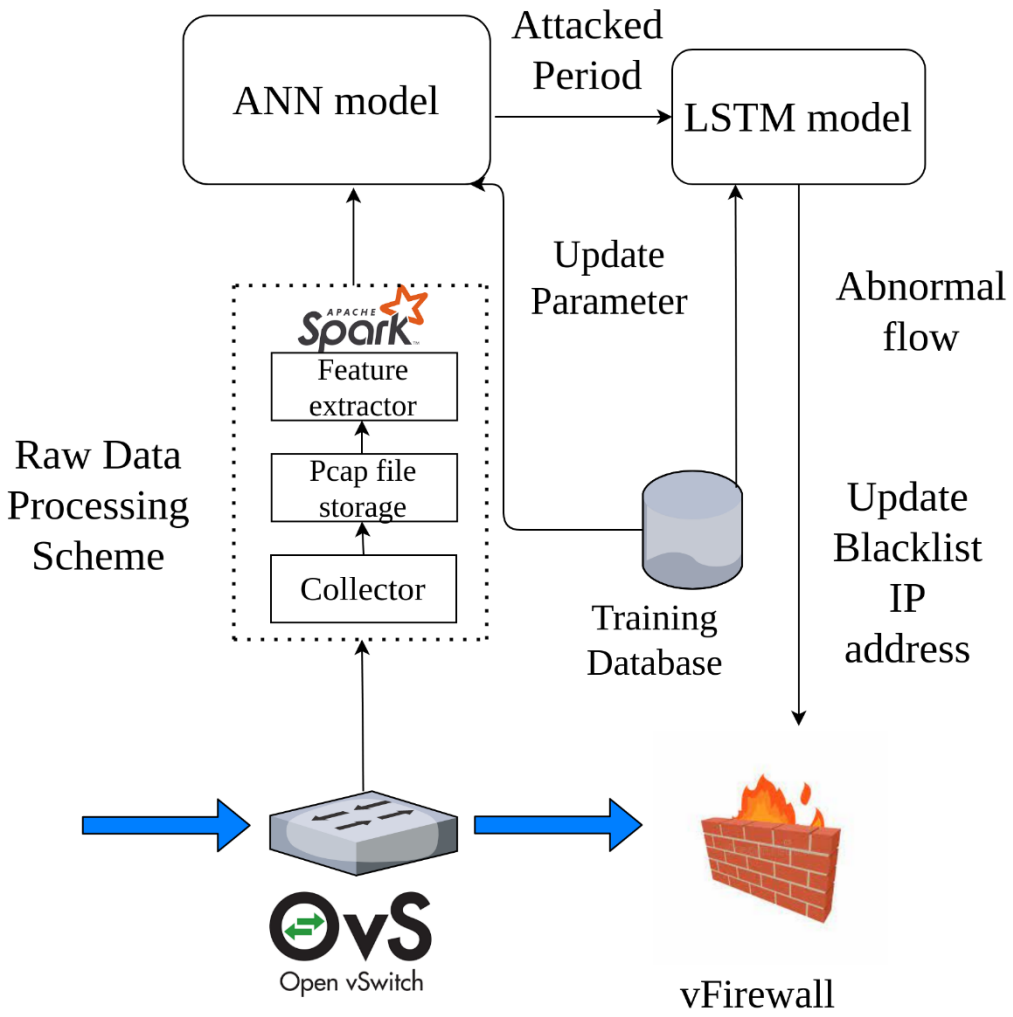


Figure 2: Detail architecture of the proposed model

System Description

- In the first phase, an artificial neural network (ANN) algorithm observes the network traffic in a time interval to check if there is an attack in that time p eriod

- The second phase detection using the LSTM algorithm is triggered to detect an attack flow if any attacks are detected in the first phase. The secon d detector exactly decides which is an abnormal flow, which is called the flow detector.
- Using the period detector before the flow detector, we can know when an a ttack happend and which data is the most critical part of the input data for the LSTM model. By doing so, we can reduce the sequence length of the LSTM input data

System Description

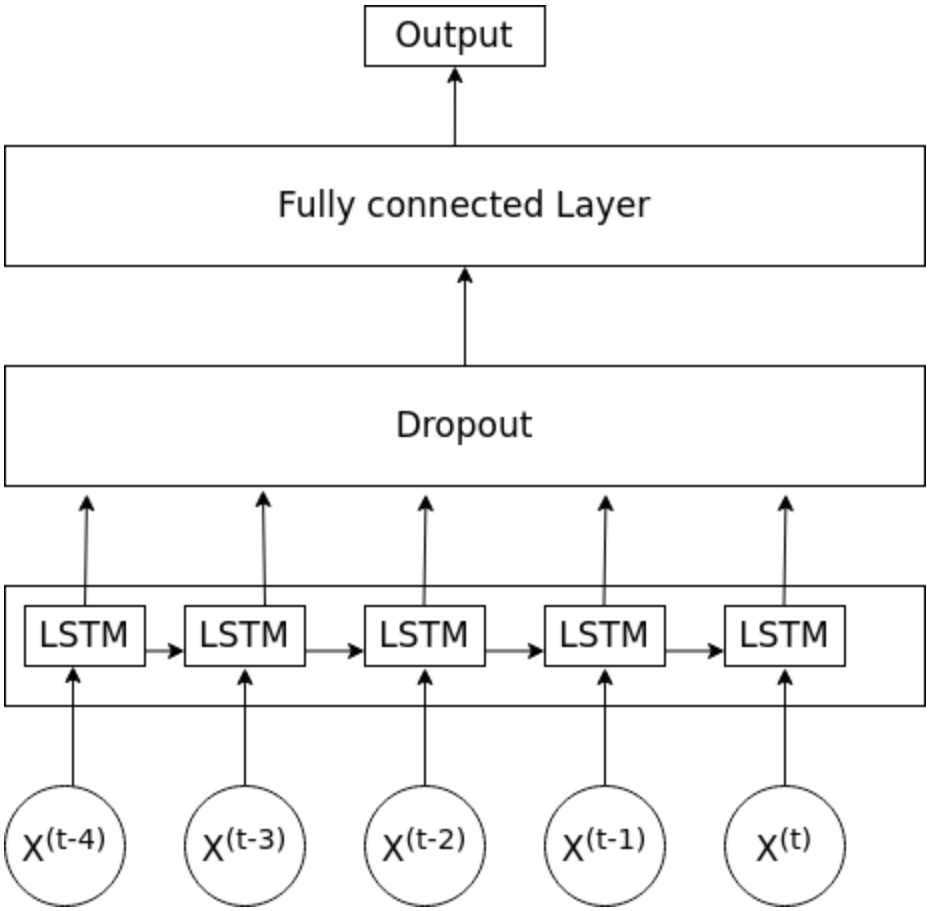


Figure 3: The architecture of LSTM model

Evaluation

- Based on other related works, we implement a testbed to evaluate our proposed model and compare to other methods. We will use a same simulation tool to simulate an EDoS attack model.
- We will compare our proposed method with two other references: A machine learning-based model using SVM and same metrics as us to detect EDoS attack and a LSTM-based model.
- We want to illustrate that our proposed model can achieve much higher accuracy, lower-false alarm rate than other solution or at least same as other LSTM-based method and consumes lower resources than the other LSTM-based method. Thus our system will response more quickly compared to other methods

[1] ***Machine Learning-Based EDoS attack Detection Technique Using Execution Trace Analysis.***
[2] ***R-EDoS: Robust Economic Denial of Sustain- ability Detection in an SDN-Based Cloud Through Stochastic Recurrent Neural Network***

Evaluation

Base on other reated works, we evaluate our proposed solution through Quality of Service (QoS) and Resource Consumption

1. QoS:

We use 3 metrics include:

- Accuracy=$\frac{TP+TN}{TP+TN+FP+FN}$
- Detection rate=$\frac{TP}{TP+FN}$
- False Alarm rate=$\frac{FP}{FP+TN}$

We use two more metric to compare with two other related works in term of detection time and response time. Because our model need a shorter length o f sequence input data=> calculation time is faster=> detection time is faster => response time of the entire system is faster.

- Detection time
- Response time

2. Resource consumption

We evaluate how resources is used (CPU Usage, Memory usage) by our LSTM. Comparing to another LSTM-based model , our LSTM uses less CPU usage and Memory usage

Evaluation

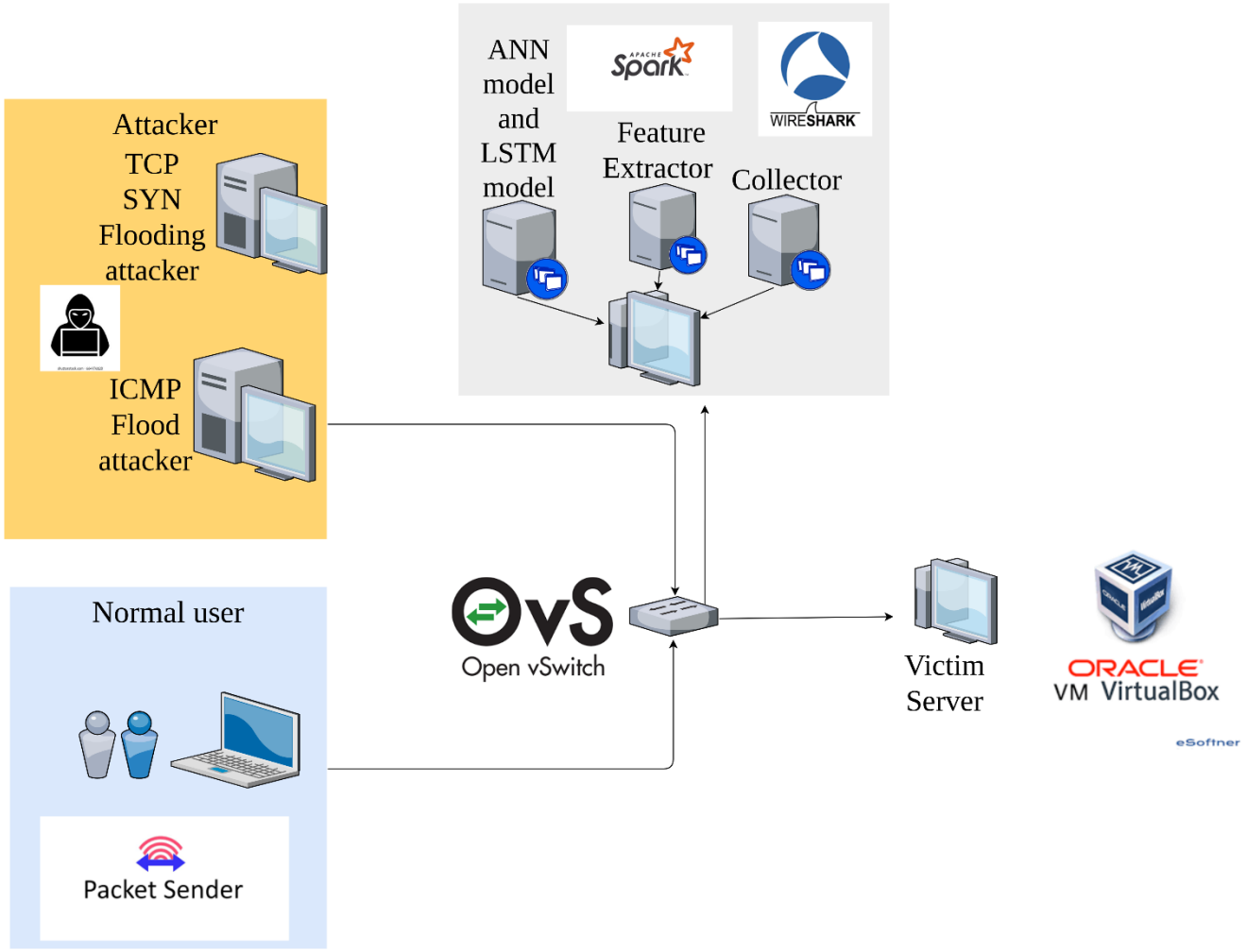


Figure 4: The Experimental Topology

Results

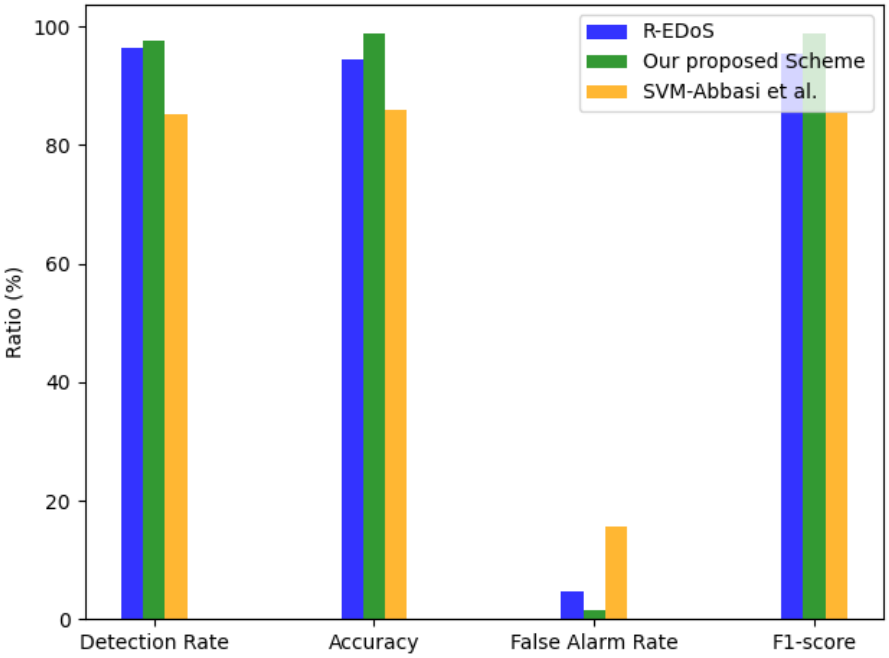


Figure 6: Detection performance comparison of the flow detector

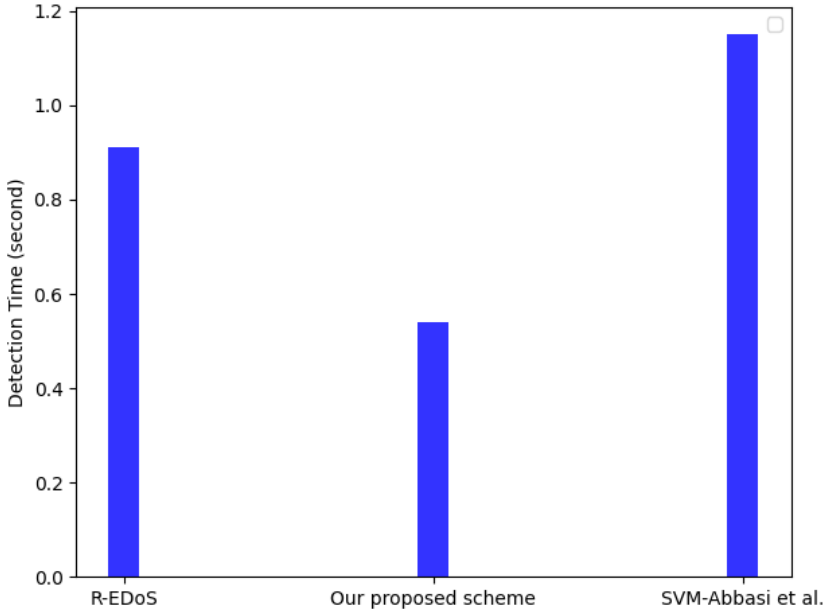
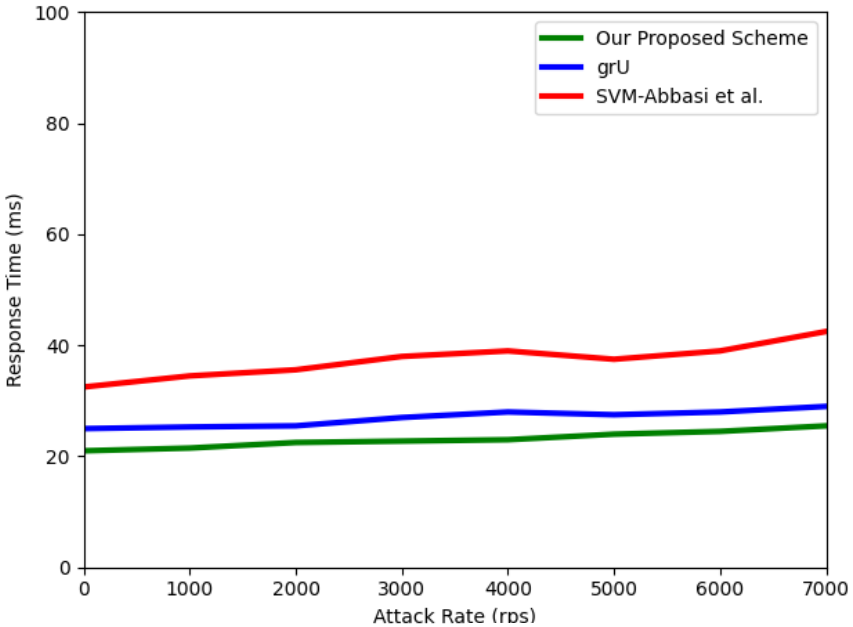
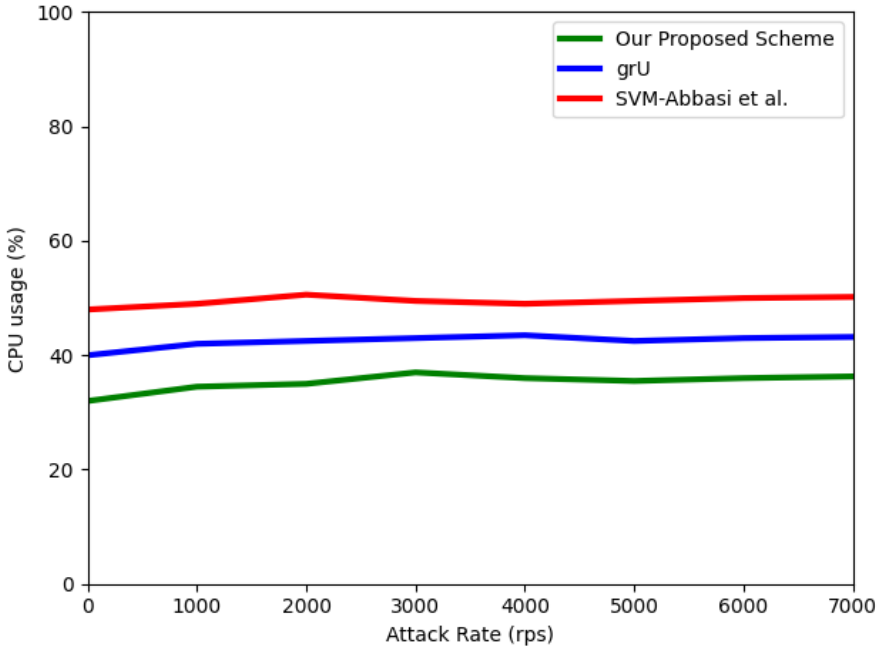
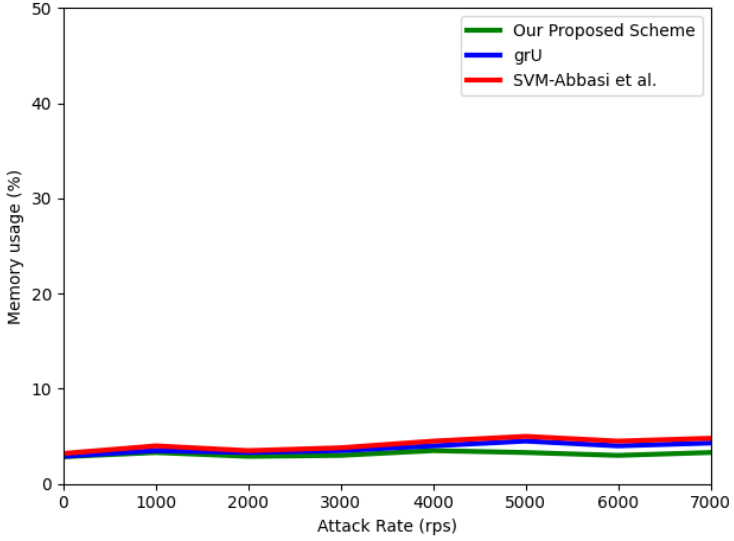


Figure 7: Detection Time among 3 solutions

Results


Our Proposed Scheme
grU
SVM-Abbasi et al.
Response Time (ms)
Attack Rate (rps)
0
20
40
60
80
100
0
1000
2000
3000
4000
5000
6000
7000


Our Proposed Scheme
grU
SVM-Abbasi et al.
CPU usage (%)
Attack Rate (rps)
0
20
40
60
80
100
0
1000
2000
3000
4000
5000
6000
7000


Our Proposed Scheme
grU
SVM-Abbasi et al.
Memory usage (%)
Attack Rate (rps)
0
10
20
30
40
50
0
1000
2000
3000
4000
5000
6000
7000

Thank You