DDOS assault detection and mitigation with the usage of statistical and machine learning methods in SDN

1 . ABSTRACT

The future of networking is software-defined networks, which separate the records plane and control plane of community gadgets to permit centralized network manage. SDN allows us to configure the community for higher ease of use and performance at the same time as also imparting superior community control and security. but, SDN is vulnerable to attacks. DDOS attacks are the most intense and dangerous attacks in a network due to the fact they could flood the community with great numbers of packets and exploit network assets to prevent service to new requests. DDOS attacks are acknowledged to expand in a cloud surroundings. To successfully detect and mitigate DDOS attacks in SDN, the solution supplied combines statistics and system mastering methodologies. The device mastering method deployed has obtained an accuracy of 98.26 percentage and a detection fee of a hundred percent in detecting and mitigating DDOS attacks in a software-described community utilizing Ryu controller and mininet community simulator with OpenFlow SDN protocol.

KEYWORDS
DDoS, IoT, SDN,Snort,Sampling , Detection , Mitigation, Mininet, Machine learning .

2 . OBJECTIVE

Cloud computing is growing in recognition, and lots of organizations and establishments are migrating their offerings to the cloud in the hopes of improving performance and security. human beings now have an inextricable dependence at the internet, which incorporates their non-public statistics, and they are always involved approximately security. To keep the facts secure and at ease from safety network threats, safety features should be implemented. DDOS attacks are community attacks that restriction get entry to to the server and deny cloud clients offerings. To avoid this, severa studies and tasks had been undertaken, one in every of that is using software program defined networks to reap this purpose.

3. PROBLEM STATEMENT

During the beginning phases of computing research, the following research question was presented: -

“Is it possible to improve the detection and mitigation of distributed denial of service (DDOS) assaults in a cloud network environment using software defined networking?”

4. INTRODUCTION

Due to the important benefits it can supply above traditional networks, the cloud computing generation has experienced rapid expansion in domains which includes enterprise and academia inside the closing several years. inside the realm of networking and cloud networks, software-described networking (SDN) has seen enormous increase in popularity. SDN is a networking technology that will increase community overall performance and management by using taking into consideration centralised community control and the programming of network gadgets.

A allotted denial-of-service (DDoS) assault is a malicious attempt to disrupt a centered server's, provider's, or community's normal traffic by means of flooding the goal or its surrounding infrastructure with internet traffic.

Software program described networking separates the statistics and manage planes of a community tool, allowing an SDN controller to configure the control plane. SDN structure is made of three layers: infrastructure, which houses networking devices which includes switches and hosts, manage, which homes the controller, and application, which houses networking packages. SDN is used to display and operate the network from a unmarried place, making it less complicated to trade and configure network devices. It enhances scalability, overall performance, and controllability at the same time as additionally supplying flexibility and cloud management. Cloud computing networks use software program described community-primarily based cloud environments to improve security and control even as additionally providing networking as a service (NAAS)

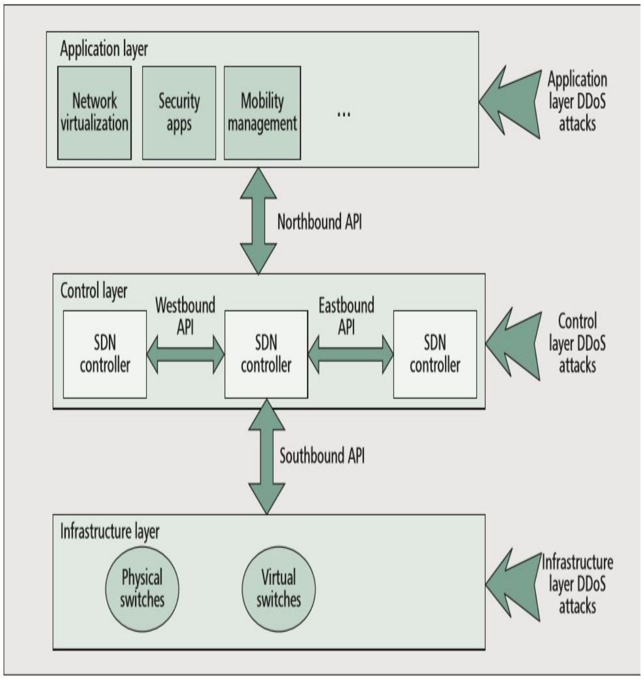


FIG Representing SDN structure with vulnerabilities of DDOS assaults

The image above depicts the several layers of the SDN which are prone to DDOS attacks. because SDN decouples the network layers, there is a hazard of protection concerns at various levels of the SDN architecture. For the cloud community, distributed denial of service (DDOS) attacks are accepted, unsafe, and dangerous. DOS assaults occur when an attacker attempts to dam a network with site visitors packets, forcing the community to reject any in addition offerings for any inbound requests, as well as the usage of all network sources.

When a single attacker assaults the community, a Dos attack happens, at the same time as a DDOS assault happens when more than one attackers or botnets ship traffic packets/requests at the equal time.consistent with a studies article published by Akamai on community safety, DDOS attacks have elevated by using as much as a hundred twenty five percentage over the years. SDN, then again, has the ability to offer improved protection and centralised manipulate with the intention to discover and mitigate community DDOS attacks.

Those safety challenges in software defined networks need to be addressed, and plenty research and improvement has gone into developing new procedures and techniques to save you attacks. For more than a decade, DDOS attacks in cloud networks had been an open studies trouble, with increasingly more new strategies to save you them from occurring. I supplied a way to resolve this issue and become aware of and mitigate DDOS attacks using software defined networks in my studies project.

5 RELATED WORK

Software program-defined in recent times, networking is frequently referred to as the "future of Networking." The decoupling of the control plane from the facts aircraft of networking devices is the cause for this generation's brief growth and first rate achievement. The manipulate plane permits centralised control of the entire network and switches, getting rid of the want to manually setup every networking tool. The records aircraft, which is made from switching devices, permits community visitors to be forwarded based totally on rules set by using programs running on top of the programmable controller. This significant advancement within the area of networking has aided in the acceleration of carrier transport and the provisioning of both physical and digital community gadgets from a central place.

The literature assessment is organised into 3 sections: SDN site visitors analysis, SDN site visitors evaluation, and SDN visitors evaluation.

Anomaly identification and mitigation for DDOS assaults using SDN and machine mastering technologies. those sections provide an in depth evaluation of the research and techniques used to prevent DDOS assaults the usage of SDN.

5.1 SDN Traffic Analysis

The methodologies and work provided and carried out via researchers in analysing incoming traffic in a software program defined community are described on this section. those techniques can be used to become aware of DDOS assaults and examine visitors:

i) Analysing the network records
ii) SNMP evaluation of facts

Records evaluation on the network This method involves detecting malicious community visitors as a way to decide the opportunity of a DDOS attack. each community visitors has its personal set of characteristics, which have to be retrieved by means of specifying sure assault visitors characteristics. To identify site visitors from attack traffic, the behaviour and characteristics of normal traffic need to also be collected. Many studies have provided numerous methodologies and capabilities extraction parameters. The authors supplied a concurrent algorithmic technique that modifies the waft monitoring abilities on community switches to hastily become aware of potential victims, malicious visitors, and suspicious attackers.The writers have examined the proposed approach, and the graphs and effects within the article returned up the assertions said with the aid of the writer. but, the record provides inadequate data regarding the tools and simulation methodologies utilised to produce the results, which had been attained with incredible accuracy with the aid of capturing uneven float.

SDN technology is being used to do exploratory examine into enhancing IoT security. For the IoT region, the authors created a disbursed comfy architecture based totally on SDN. further, the authors checked out a preliminary dialogue on how to save you DDoS assaults on IoT gadgets. They used SDN-based totally sampling methodologies to find out anomalies, with the primary purpose of collecting switch facts to improve safety accuracy. furthermore, the authors developed a hybrid security countermeasure device to shield SDN-based IoT controllers from hyperlink spoofing assaults.

Wang et al. (2019) provide four characteristic extraction procedures, such as accumulating visitors information and counting the byte charge, symmetric and uneven go with the flow adjustments, and counting small quantities of incoming packets in the community. The proposed algorithm is carried out using a ryu controller and simulated with a mininet; the outcomes show that the controller reaction time is diminished beneath DDOS attack.

He et al. used a comparable strategy, however with exceptional characteristic extraction parameters and a density peak clustering set of rules (2017). the ambiguity detection manner begins with the collection of visitors features, observed through the identification of robust and weak correlation elements with malicious site visitors traits, and in the end the utility of the density height clustering algorithm to the correlated facts for DDOS attack detection in the network. For assessment, the authors used Python 2.7.nine with the MINE bundle and various open source Python machine mastering libraries to develop the algorithms. The authors declare that their approach outperforms existing machine mastering procedures, but it does no longer remember real-time records from network visitors.

The visitors information is collected and stored the use of the simple network management Protocol's (MIB) management information Base. Integrating an intrusion detection machine (IDS) with MIB records lets in for the detection of DDOS attempts. Nhu-Ngoc Dao et al. advise a practical way to combat DDOS assaults in SDN (2020). This approach detects a community flooding assault through counting the variety of incoming packets, the counter of IPs within the community, and common user connections. those characteristics are compared to threshold values to stumble on the attack.The authors have tested and simulated this approach the use of mininet, however the controller details are lacking, and this approach may be easily defeated with the aid of numerous IP assets and not on time assaults. The experiment can not be replicated since the paper lacks enough specifics.

Jin et al. (2021) recommended a defence device in opposition to DDOS faked visitors by using a hop-depend filtering approach, wherein each IP packet should journey a exact quantity of hops to reach its vacation spot. The authors declare that the hop remember filtering technique can pick out 90% of the faked IP packets by way of monitoring the hops remember and TTL-Time to stay fee in the IP header. The assessments were carried out the usage of the Linux kernel to generate TCP and ICMP visitors. The results are nicely-represented through graphs, but the experimental setup is far extra difficult and time-consuming to finish.

6. GAPS IN EXISTING WORK

To decrease the total burden of a single controller in SDN, design a allotted DDoS detection and mitigation device using the generalised records idea metric.

Characterization of flash events from similar-searching excessive-rate DDoS assaults can also be a tough discipline of investigation.

even as existing research has made widespread development in device mastering-based totally detection solutions for DoS/DDoS, extra contributions can be made the usage of graph, KNN, and clustering algorithms.

One potential research place is constructing and enhancing optimization-based algorithms for detecting DoS/DDoS towards SDN and in SDN-primarily based answers to minimise false positives and maximise proper positives.

Use the performance of deep mastering models to discover DDOS attacks and topological poisoning attacks. the usage of Deep studying algorithms to differentiate benign from malicious conversation is computationally expensive, but the results are promising.

Because the controller is a single point of failure and for this reason a vulnerable goal for attackers, DoS/DDoS attacks will in all likelihood stay a major fear in future SDN structures.

While in comparison to other modern-day classifiers, the proposed version for community assault detection has a lower mistakes rate, higher accuracy, and detection charges.

Have a look at the impact of additional deep neural strategies on the overall and Discriminator (e.g., Gated-Recurrent Unit, Stacked auto-Encoder).

improve our algorithm with the aid of concurrently optimising multiple objectives. We also plan to merge our method with other state-of-the-art algorithms.

The technique appropriately detects community anomalies and broken switches (98.80%).

By means of incorporating correlations between traits, the HESS approach's actual-time performance can be improved.

The efficiency of the cautioned technique in mitigating DDoS attacks on dispersed settings will be proven using flat and hierarchical SDN structures with numerous controllers.

Completely at SDN-enabled area switches with real-time traffic streams to conduct shrewd periodic polling based totally sampling, that could help to reduce the crucial overhead.

7. DESIGN SPECIFICATION

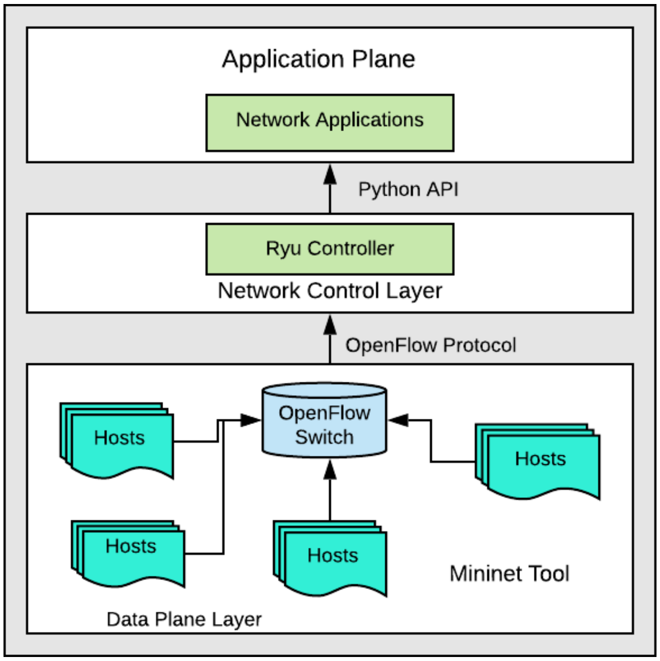


Fig representing SDN Framework.

The data plane of the provided SDN framework has many nodes/hosts built sincerely using mininet, all of which might be linked to the openflow switch, which defines the SDN protocols and connects with the manipulate plane of the framework. The statistics aircraft and switches are managed by means of the manage plane, which also defines guidelines and video display units network site visitors drift. The Ryu controller is utilised because the controller, which gives programming skills and permits us to handle network routing sports. The manage aircraft is written in Python considering that ryu is a Python-primarily based controller that communicates with the utility layer via a Python-primarily based API, which in our case is community traffic apps.

7.1 NETWORK DESIGN

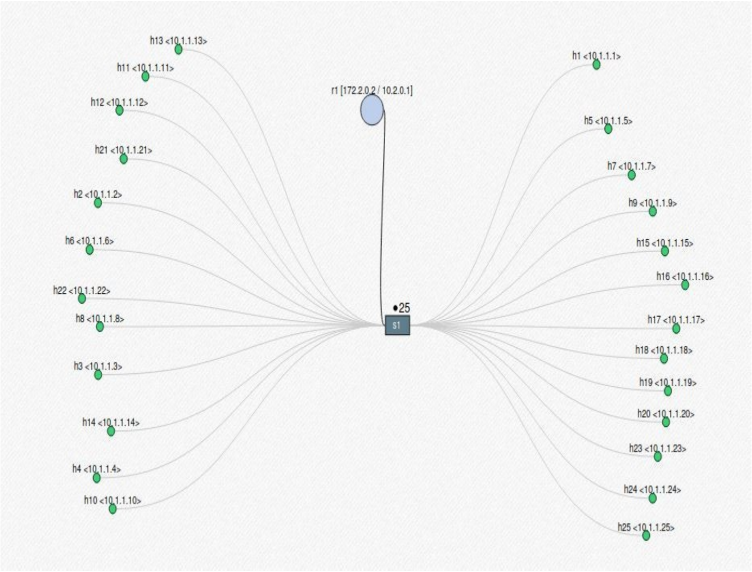


Fig representing Mininet community layout

Mininet community simulator changed into used to construct the network topology, which includes 25 hosts/nodes, one openflow switch, and one ryu controller. The switch is hooked up to the controller, and the switch is attached to all of the hosts. The ryu controller is in fee of all of those hosts and switches, and any port that is attacked can be stopped immediately.

8. IMPLEMENTATION

To discover and mitigate DDOS assaults in a software described community, the cautioned answer employs both data and system mastering methodologies. To hit upon an assault in a community, the applied technique necessitates training the SVM ML set of rules.

The statistics collection module need to collect facts from both everyday and assault site visitors and save it in a CSV document for usage by means of the system mastering set of rules. ordinary traffic data have to be collected first, accompanied by means of assault traffic facts; for stepped forward accuracy, ordinary site visitors information have to be amassed once more following assault traffic statistics.

After the statistics is gathered and the controller is positioned to detection mode, the SVM set of rules anticipates ordinary visitors and detects DDOS attack traffic straight away, blocking the port from which the visitors is coming in. The controller is configured to a 120-second hardtime after the port has been blocked, following which it unblocks it.

However, if the assault continues, the port is detected and blocked for another a hundred and twenty seconds. Following the blocking, normal community visitors go with the flow from other ports is permitted. So long as the assault lasts, this technique will continue.

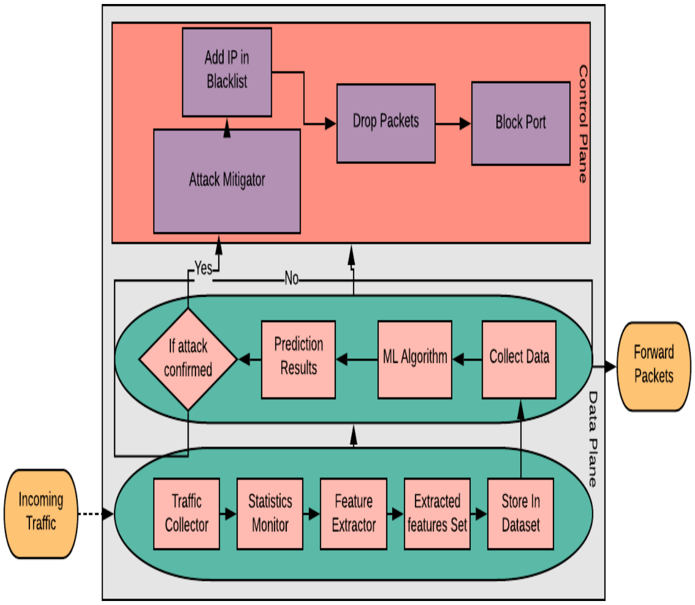


Fig representing Flowchart of the Presented Method.

Exclusive protocols and controllers are utilized in software program described networks, every of that is designed to act in a specific way and give efficiency and flexibility in a selected location. In a software program described community, the given solution is constructed using the maximum popular and outperforming technology for detecting and mitigating DDOS attacks. For this challenge, openVswitch is utilised since the Openflow Protocol is the most not unusual and wellknown protocol for software program described networks.

The reasoning and processes are programmed in Python for the reason that furnished method is a aggregate of statistical and device learning methodologies. Statistical methods include traits like supply IP speed, float entires speed, and flowpair access ratio, which can be all entered into the controller.

Ryu Controller is a programmable controller based totally on Python this is used to specify the regulations and logic for the switches to follow within the technique.

Mininet is a community simulator that builds a digital network structure with a controller, switches, and hosts. For this mission, a single openVswitch with 10 and 25 hosts is generated for severa tests.

Hping3 is a community packet generator that creates TCP/IP visitors. it is in most cases used to assess community security. Usingthis programme, everyday and assault site visitors scripts are constructed to generate site visitors routinely.

Iperf is a community site visitors generator and community overall performance tester that is used to manually generate traffic on this mission. All of these equipment are installed on Ubuntu 20.04.1 LTS, that is going for walks on VMware pc.

9. EVALUATION

This section details the SDN exams, which covered sending everyday and attack site visitors to the community from numerous ports, in addition to the overall detection and mitigation technique, in addition to the accuracy and detection rate of the applied method. The datasets have been first built with six hundred+ samples of everyday site visitors statistics and three hundred+ samples of attack site visitors statistics for the SVM algorithm to teach and analyse which will forecast the assault. The experiments are run for 300 seconds with a 2 2d site visitors series c program languageperiod, with SVM predicting traffic each 2 seconds.

9.1 CASE STUDY 1

Everyday site visitors is brought from all ports on this experiment, even as an assault is despatched from port/host 1 at the network, with incoming traffic being accumulated every 3 seconds. Mininet is used to design the network topology, which includes one openflow transfer and ten hosts.

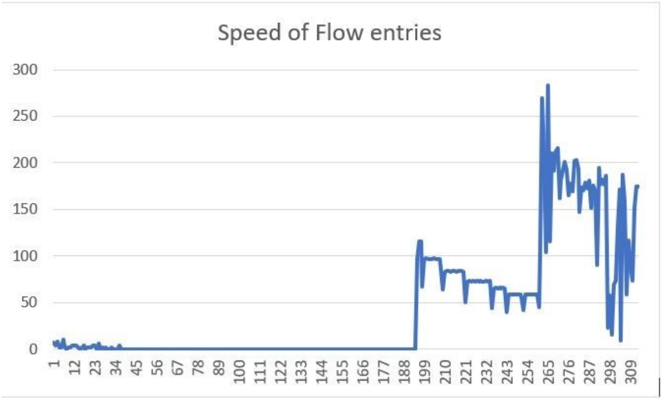


Fig representing SFE

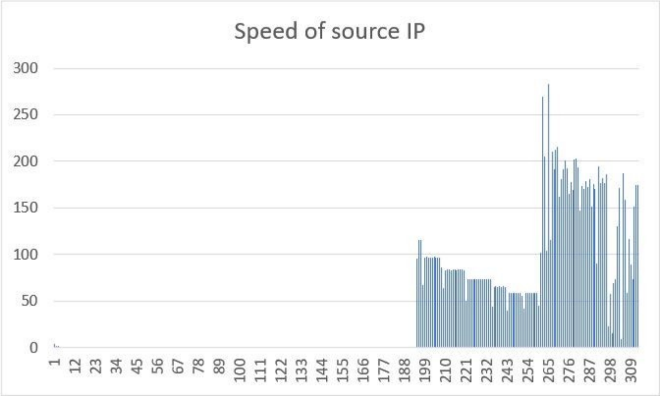
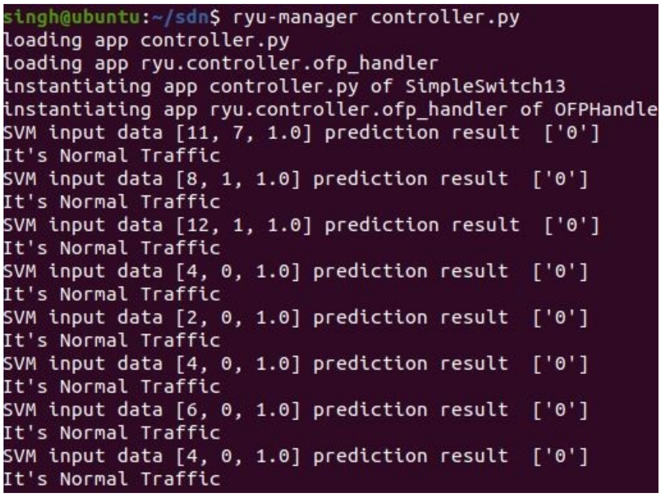


Fig representing SSP

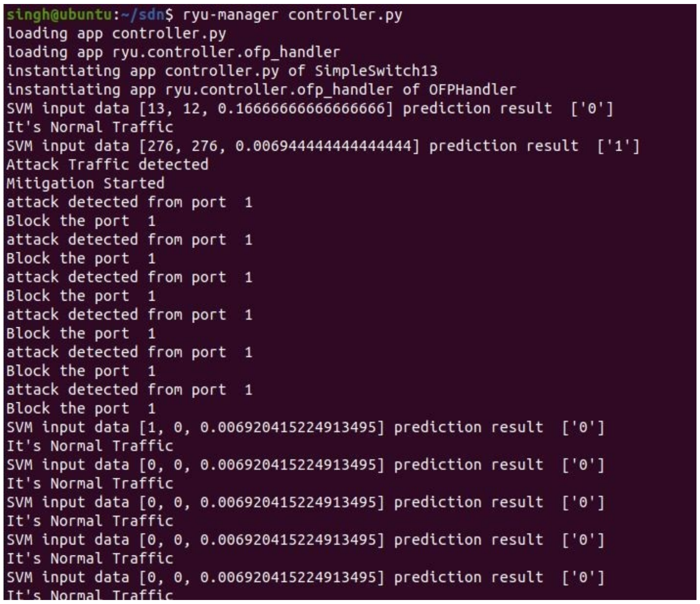
The information counts are at the X axis, whilst the rate counts of the waft entries and supply IP are on the Y axis in graphs A and B. when attack site visitors is injected into the network, the velocity of flow entries and IP origins rises, at the same time as the immediately line represents everyday community site visitors waft.



```
singh@ubuntu:~/sdn$ ryu-manager controller.py
loading app controller.py
loading app ryu.controller.ofp_handler
instantiating app controller.py of SimpleSwitch13
instantiating app ryu.controller.ofp_handler of OFPHandle
SVM input data [11, 7, 1.0] prediction result  ['0']
It's Normal Traffic
SVM input data [8, 1, 1.0] prediction result  ['0']
It's Normal Traffic
SVM input data [12, 1, 1.0] prediction result  ['0']
It's Normal Traffic
SVM input data [4, 0, 1.0] prediction result  ['0']
It's Normal Traffic
SVM input data [2, 0, 1.0] prediction result  ['0']
It's Normal Traffic
SVM input data [4, 0, 1.0] prediction result  ['0']
It's Normal Traffic
SVM input data [6, 0, 1.0] prediction result  ['0']
It's Normal Traffic
SVM input data [4, 0, 1.0] prediction result  ['0']
It's Normal Traffic
```

Fig representing Normal Traffic Prediction

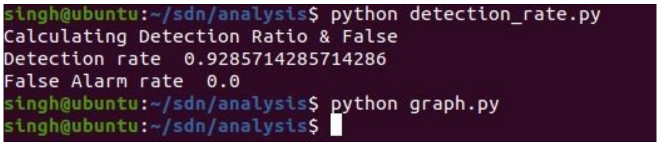
The SVM device mastering system predicts that the visitors may be regular.



```
singh@ubuntu:~/sdn$ ryu-manager controller.py
loading app controller.py
loading app ryu.controller.ofp_handler
instantiating app controller.py of SimpleSwitch13
instantiating app ryu.controller.ofp_handler of OFPHandler
SVM input data [13, 12, 0.16666666666666666] prediction result  ['0']
It's Normal Traffic
SVM input data [276, 276, 0.006944444444444444] prediction result  ['1']
Attack Traffic detected
Mitigation Started
attack detected from port  1
Block the port  1
attack detected from port  1
Block the port  1
attack detected from port  1
Block the port  1
attack detected from port  1
Block the port  1
attack detected from port  1
Block the port  1
attack detected from port  1
Block the port  1
SVM input data [1, 0, 0.006920415224913495] prediction result  ['0']
It's Normal Traffic
SVM input data [0, 0, 0.006920415224913495] prediction result  ['0']
It's Normal Traffic
SVM input data [0, 0, 0.006920415224913495] prediction result  ['0']
It's Normal Traffic
SVM input data [0, 0, 0.006920415224913495] prediction result  ['0']
It's Normal Traffic
SVM input data [0, 0, 0.006920415224913495] prediction result  ['0']
It's Normal Traffic
```

Fig Representingg Attack Traffic Prediction

The SVM machine gaining knowledge of algorithm predicts the web site traffic as DDOS attack traffic, triggering the mitigation manner and blocking off the port 1 from which the assault web site visitors originates.



```
singh@ubuntu:~/sdn/analysis$ python detection_rate.py
Calculating Detection Ratio & False
Detection rate  0.9285714285714286
False Alarm rate  0.0
singh@ubuntu:~/sdn/analysis$ python graph.py
singh@ubuntu:~/sdn/analysis$ 
```

Fig representing Detection Rate

The given technique detected ninety two.eight percent of DDOS assault hobby inside the community with 0 fake alarms, indicating that no normal visitors turned into mistaken for attack traffic.

9.2 CASE STUDY 2

Everyday traffic is added from all ports in this experiment, even as an attack is despatched from port/host eight on the community, with incoming visitors being amassed every 2 seconds. Mininet is used to design the community topology, which consists of one openflow switch and 25 hosts.

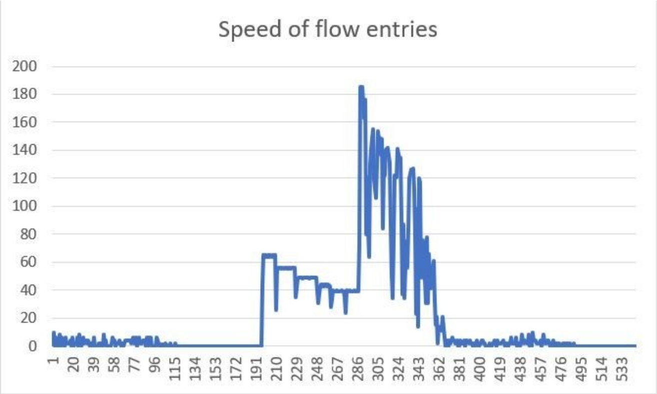


Fig Representing SFE

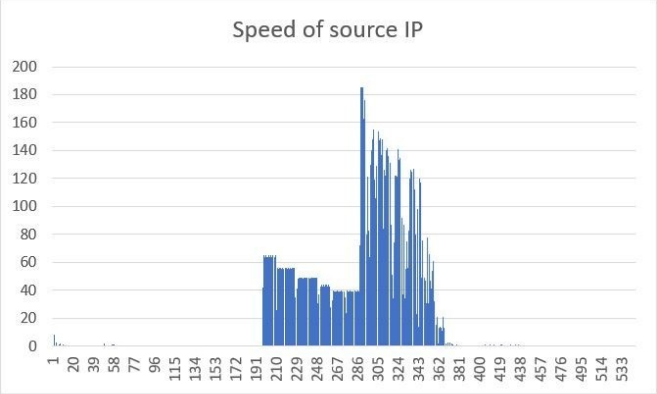
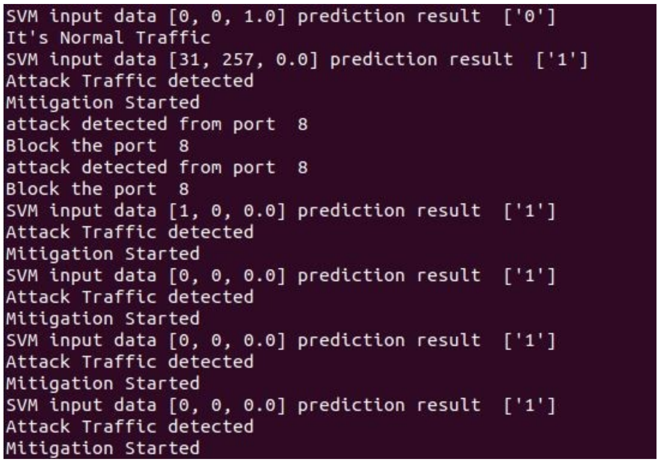


Fig Representing SSP

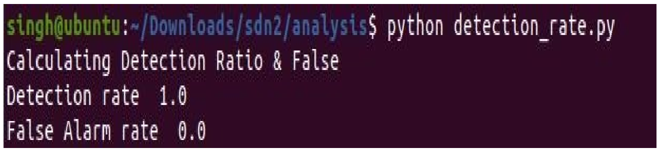
The X axis in graphs A and B represents information counts, whilst the Y axis represents flow access and source IP pace counts. while assault site visitors is introduced into the community, the velocity of glide entries and the rate of supply IP will increase, while the straight line represents ordinary site visitors drift inside the community. The graph A depicts the flow pair ratio.



```
SVM input data [0, 0, 1.0] prediction result  ['0']
It's Normal Traffic
SVM input data [31, 257, 0.0] prediction result  ['1']
Attack Traffic detected
Mitigation Started
attack detected from port  8
Block the port  8
attack detected from port  8
Block the port  8
SVM input data [1, 0, 0.0] prediction result  ['1']
Attack Traffic detected
Mitigation Started
SVM input data [0, 0, 0.0] prediction result  ['1']
Attack Traffic detected
Mitigation Started
SVM input data [0, 0, 0.0] prediction result  ['1']
Attack Traffic detected
Mitigation Started
SVM input data [0, 0, 0.0] prediction result  ['1']
Attack Traffic detected
Mitigation Started
```

<u>Fig Representing Attack Trafic Prediction</u>

The SVM system mastering set of rules predicts the site visitors as DDOS assault traffic, triggering the mitigation technique and blocking off the port eight from which the assault traffic originates.



```
singh@ubuntu:~/Downloads/sdn2/analysis$ python detection_rate.py
Calculating Detection Ratio & False
Detection rate  1.0
False Alarm rate  0.0
```

<u>Fig Representing Detecion Rate</u>

The given answer produced a a hundred% detection rate of DDOS attack site visitors inside the community with 0% false alarm, which means no regular site visitors was labeled as attack traffic.

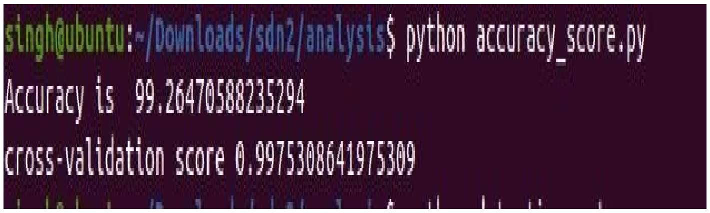
9.3 DISCUSSION

Two separate assault eventualities were used to test the implemented technique. In test 1, attack visitors is despatched from port 1 to simplest 10 hosts inside the community, and the effects display that the SVM ML algorithm accomplished accuracy of 98.71 percentage and a pass validation rating of 99.57 percentage with the training records, and the assault traffic detection charge was close to one hundred percent and not using a fake alarms, indicating that no regular site visitors was considered malicious.

In experiment 2, the attack visitors is despatched from port 8 with just 25 hosts within the community, and the effects reveal that the SVM ML algorithm executed accuracy of 99.26 percent and a cross validation score of ninety nine.seventy five percent the use of the schooling information, with a detection charge of 100 percent and no false alarms. those findings monitor that the given approaches are extraordinarily accurate in detecting malicious site visitors within the community, with zero false alarms, implying that no legitimate site visitors is denied get entry to to the community.

However, if an IP deal with this is taken into consideration normal in skilled statistics and is in a trusted IP list is used to assault the community, this method will now not discover it, and the attacker could be capable of skip safety and advantage access to the community. whilst the probabilities of this occurring are very low, a complete network visitors analyser should be designed to prevent this from happening.

10. ALGORITHM ACCURACY



```
singh@ubuntu:~/Downloads/sdn2/analysis$ python accuracy_score.py
Accuracy is  99.26470588235294
cross-validation score 0.9975308641975309
```

<u>Fig representing Accuracy Score</u>

The accuracy score of the supplied approach is 99.26 percent, at the same time as the move validation score with training and check statistics is 99.75 percent.

11. CONCLUSION AND FUTURE WORK

In assessment to conventional networks, software defined networks permit us to programme network layout and operations. The important reason of this studies turned into to use SDN to perceive and mitigate DDOS assaults in a cloud placing. To detect and are expecting DDOS attacks inside the community, the carried out method uses a aggregate of statistical capabilities such as supply IP, velocity of glide entries, flowcount, and ratio of flow-pair, as well as the SVM gadget studying set of rules. Experimented effects display that the proposed approach can provide accuracy of ninety nine.26% and malicious visitors detection charge of one hundred%, with zero false visitors predictions.

however, security is in no way complete and might continually be compromised. as an example, an attack from a trusted IP source may be leveraged to transmit malicious traffic into the network, which the SVM can not predict.

The applied method might be designed within the future to consist of severa switches and controllers in the community, as well as a radical community packet analyser. presently, four functions are hired in statistical analysis; however, features can be extracted and mixed with gadget gaining knowledge of algorithms to enhance and improve the accuracy of malicious site visitors prediction.

12. REFERENCES

Singh, Jagdeep, and Sunny Behal. "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions." *Computer Science Review* 37 (2020): 100279.

Alhijawi, Bushra, Sufyan Almajali, Hany Elgala, Haythem Bany Salameh, and Moussa Ayyash. "A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets." *Computers & Electrical Engineering* 99 (2022): 107706.

Ahuja, Nisha, Gaurav Singal, Debajyoti Mukhopadhyay, and Neeraj Kumar. "Automated DDOS attack detection in software defined networking." *Journal of Network and Computer Applications* 187 (2021): 103108.

Valdovinos, Ismael Amezcua, Jesus Arturo Perez-Diaz, Kim-Kwang Raymond Choo, and Juan Felipe Botero. "Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions." *Journal of Network and Computer Applications* 187 (2021): 103093.

Sambangi, Swathi, Lakshmeeswari Gondi, and Shadi Aljawarneh. "A Feature Similarity Machine Learning Model for DDoS Attack Detection in Modern Network Environments for Industry 4.0." *Computers and Electrical Engineering* 100 (2022): 107955.

Novaes, Matheus P., Luiz F. Carvalho, Jaime Lloret, and Mario Lemes Proença Jr. "Adversarial Deep Learning approach detection and defense against DDoS attacks in SDN environments." *Future Generation Computer Systems* 125 (2021): 156-167.

Iranmanesh, Amir, and Hamid Reza Naji. "A protocol for cluster confirmations of SDN controllers against DDoS attacks." *Computers & Electrical Engineering* 93 (2021): 107265.

Fouladi, Ramin Fadaei, Orhan Ermiş, and Emin Anarim. "A DDoS attack detection and defense scheme using time-series analysis for SDN." *Journal of Information Security and Applications* 54 (2020): 102587.

Long, Zhang, and Wang Jinsong. "A Hybrid Method of Entropy and SSAE-SVM Based DDoS Detection and Mitigation Mechanism in SDN." *Computers & Security* (2022): 102604.

El Kamel, Ali, Hamdi Eltaief, and Habib Youssef. "On-the-fly (D) DoS attack mitigation in SDN using Deep Neural Network-based rate limiting." *Computer Communications* 182 (2022): 153-169.

Ujjan, Raja Majid Ali, Zeeshan Pervez, Keshav Dahal, Ali Kashif Bashir, Rao Mumtaz, and Jonathan González. "Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN." *Future Generation Computer Systems* 111 (2020): 763-779.