

DEVELOPMENT OF SECURE AND ENERGY EFFICIENT REMOTE HEALTH MONITORING SYSTEM AND IMPROVED NETWORK PERFORMANCE

Unnati Sharma

School of Computer Science
and Engineering Sharda University Greater Noida, Uttar Pradesh
2021384800.unnati@dr.sharda.ac.in

Prof. (Dr.) Sibaram Khara

Sharda University Greater Noida Ghaziabad
sibaram.khara@sharda.ac.in

Dr. Nihar Ranjan Roy

School of Engineering and Technology Vivekananda Institute of Professional Studies,
Ranikhet, Pitampura, New Delhi, nihar.roy@vips.edu

ABSTRACT:

A novel approach to cyber protection with intelligent defence capabilities is the health prevention concept. It has the ability to promptly respond to incursion activity in addition to detecting it. This study integrates health prevention technology with semi-supervised clustering and deep learning theory. The current direction in neural network development is represented by deep learning, which is based on deep structures. For achieving health prevention with a low recognition error rate, semi-supervised learning makes use of a bulk amount of unlabeled (cyber traffic data) and a less amount of labelled (cyber traffic data). Because of its low mistake rate, discriminative deep belief network (LSTM)-based cyber defence technology has becoming a latest research topic in the field of health prevention. Suggested a Remote health monitoring. In order to address the issue of the health prevention model's high classification error rates, this study suggests a technique for large-scale semi-supervised deep learning based on local and non-local regularization that uses LSTM. The proposed LSTM model ensure the lowest error rate, by making relationship with the results of the Hopfield, support vector machine (SVM), generative adversarial network (GAN) and a deep belief network random forest (DBN-RFS) classifiers in terms of health prevention. Therefore, the suggested approach improves the functionality of the health prevention system.

Keywords- *Prevention, discriminative “deep belief networks”, “intrusion prevention”, “local and non-local regularization”, ‘semi-supervised deep learning’*

I. INTRODUCTION

The performance of the overall defense system is directly impacted by algorithms. One of the latest emerging research topics is intelligent detection

completely based on machine learning. It is difficult for supervised clustering-based intrusion detection algorithm used in standard machine learning to detect securities. Furthermore, in Real-world cyber scenarios, it is challenging to predict the intrusion method, On the other hand unsupervised learning-based methods are capable of detecting unknown securities. But they struggle to accurately classify them properly. Since

supervised and unsupervised learning approaches are not able to produce the best classification results, semi-supervised learning methods have been taken into consideration. Many comparative studies and performance evaluations have demonstrated the ability of these approaches to extract a greater number of discriminant features and provide valuable benefits to activities related to health prevention.

The rest of the paper is organized as follows:Section II present the Review Related work ,Section III discusses the Operations and thereafter Section IV discusses Implementation part and Section V provides the Performance analysis and Section VI Result generation finally Section VII conclusion .

II. REVIEW RELATED WORK

Prior research indicates that changes in modulation scheme that may confuse the intruder, particularly deep neural networks (DNNS). In the literature, adversarial security measures are primarily examined in the context of image classification. Here, they present a security Risk by revealing the classifiers Susceptibility to minute changes in the inputs, which are undetectable to humans but can result in wrong decisions. Conversely, we apply the same approach here to secure communication links from intruders that using DNNS strategies for interception.

1. N. Martins et.al, (2023) Adversarial machine learning applied to intrusion and malware scenarios:[1] A systematic review, presented “Distributed denial of service (DDoS) offer a significant threat to the availability of conventional or cloud computing resources. Many DDOS, Securities have been launched against different organizations, over the past 10 years which directly affecting vendors and users, while many researches have attempted to address the security threat offer by DDOS by combining classification algorithms with distributed computing However, their valuable solutions have been static in terms of classification algorithm used.in fact ,modern DDOS securities have become so dynamic and sophisticated that they can pass detection system, making it harder for solutions to detect .In this research paper, they presented dynamic DDOS Security detection system composed of 3 main component 1)classification algorithm 2)a distributed system 3)a fuzzy logic system.[1]

2. G. Karatas et.al, (2023) “Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset” [2]. Presented the range of data parallelism that is now accessible for neural network training has expanded significantly due to recent hardware developments. Increasing the batch size in the standard mini -batch neural network training technique is one of the easiest ways to harness next- generation hardware. In this paper the main work is to define the effects of increasing the batch size on training time experimentally, by calculating the no. of steps required to achieve a target out of sample error. they examine the variations in this relationship with respect to the training algorithm, model and data set, and we discover a very wide range of variations between workloads Along the way, which demonstrate inconsistencies seen in the literature regarding how batch size influences model quality. Which shows differences in meta parameter tuning and compute budgets at different batch sizes. They don’t find any proof that out of sample performance

suffers with greater batch sizes. Lastly, they talked about how findings will affect future efforts to train neural networks, considerably more quickly made experimental data available to the public as a database containing 71,638,836 loss measures collected throughout the training process for 168,160 different models in 35 workloads. Usually, hosts or end-user devices connected by the network architecture make up data communication networks. Hosts share this infrastructure, which uses communication lines and switching components like switches and routers to transfer data between them. Typically, switches and routers are "closed" systems with constrained and vendor-specific control interfaces. As a result, once implemented and put into use, the current network infrastructure finds it very difficult to change; in other words, implementing updated versions of current protocols (like IPv6), as well as entirely new protocols and services, is nearly impossible in today's networks. As a network of networks, the Internet is not an exception. As previously stated, the tight connection between the data- and control planes—i.e., choices regarding data traveling over the network are determined on-board each network element—is partly responsible for the so-called Internet "ossification." Deploying new network apps or features in this kind of setting is definitely not straightforward because they have to be integrated into the infrastructure directly. Because there isn't a single control interface for all of the network devices, even simple operations like configuration or policy enforcement could take some time and effort as an alternative, solutions have been developed and implemented to get past the network ossification effect, such as employing "middleboxes" (firewalls, intrusion detection systems, network address translators, etc.) over or atop the underlying network architecture. One such instance is Content Delivery Networks (CDNs). [2]

3. T. Su, H. Sun et al, (2023) "Deep learning methods on network intrusion detection using NSL-KDD dataset" [3] presented The Internet's multitudinous network traffic and its rapid expansion have presented DDoS Security detection with new and formidable obstacles. Increasing the True Negative Rate (TNR), accuracy, and precision while ensuring the detection system's durability, stability, and universality. In this research, we create a heuristic detection technique based on Singular Value Decomposition (SVD) to construct our detection system and propose a hybrid heterogeneous multi-classifier hybrid learning based DDoS Security detection method. The outcomes of our experiments demonstrate the superior TNR, accuracy and precision of our detection technique. As a result, our system performs well as a detective for DDoS security. By means of comparative analyses between Random Forest, -NN, and Bagging, which comprise the component classifiers, when the three algorithms are employed independently by SVD and by un-SVD, it is demonstrated that our model outperforms the most advanced Security detection techniques in terms of detection stability, overall detection performance, and system generalization ability. The detection of network security behavior is facing new and serious issues due to the Internet's multitype network traffic and its accelerated expansion. Certain conventional detection methods and approaches, particularly those related to DDoS security, have not been able to meet the demands of precise and effective detection for the variety and complexity of security traffic in the high-speed network environment.[3]

4. H. Jiang et al, 2023" Network intrusion detection based on PSO-xgboost model" [4], In

this study, they offer HADEC, a framework for Hadoop-based Live DDoS Detection that uses MapReduce and HDFS to analyze flooding security in an effective manner. Using MapReduce, they developed a counter-based DDoS detection system for the four main flooding security protocols (TCP-SYN, HTTP GET, UDP, and ICMP) in MapReduce. subsequently set up a testbed to assess the HADEC framework's performance in real-time DDoS detection. The experiment demonstrated that HADEC can process and detect DDoS securities in a reasonable amount of time. Create a representative collection of tests to evaluate how well the majority of common virtualization techniques function against common TCP-based distributed denial of service (DDoS) attacks Additionally, they contrast them with the identical DDoS attacking the same services on nonvirtualized servers. Experiments include cutting edge implementations of a wide range of virtualization systems and look at a sizable set of benchmarks. Using them, an effort is made to respond to the next two important questions. One of the earliest forms of virtualization to gain widespread acceptance was paravirtualization, which is still in use today. PVM relies on specific kernels and drivers that are aware that they are being virtualized, rather than specific hardware, to achieve virtualization. When a guest machine running on a PVM host sends a request for hardware access or privileged system calls, the hypervisor receives it and determines what to do with it. There is a slight loss of operating system choice when special kernels and drivers are used. A user of a virtualization solution based on PVM in particular has to have an operating system that can be altered to function with the hypervisor. For users of proprietary operating systems like Microsoft Windows, this poses a challenge, even though it does not pose a major issue for open-source

operating systems like Linux. There are some benefits to paravirtualization, such as lower overhead when virtualizing privileged operating system calls because special hardware is not required to intercept them. One of the easiest and most prevalent security flaws on the Internet is the TCP SYN flood. This security exploits the quantity of resources that a server must allot in order to carry out a three-way handshake. In an attempt to prevent a victim from responding to valid queries, a securityer tries to overwhelm them with so many connection requests. The Securityer uses TCP SYN packets to establish many connections to the victim's system in order to carry out this security.[4]

5. A. Nagaraja et al 2023 "Similarity based feature transformation for network anomaly detection" [5], presented a DDoS Security detection method based on deep learning (Deep Defense). Strong representation and inference can be obtained by automatically extracting high-level characteristics from low-level ones using a deep learning approach. In order to identify trends in network traffic sequences and track network security activity, they create a recurrent deep neural network. The experimental findings show that our model performs better than traditional machine learning methods. When compared to a traditional machine learning approach, they lower the error rate from 7.517% to 2.103% using a larger data set. [5]

III. OPERATIONS

At first the system model will be designed to all the parameters which is based on remote patient monitoring system using energy-efficient IoT sensors is proposed to meet security

demands. The optimization of network clustering and cluster head selection is performed based on trust, inter- and intra-cluster distance, and energy level by the proposed SS-ROW algorithm.

The System architecture consist following module

1. Data Collection
2. Data preprocessing
3. Splitting dataset into train and test data
4. Classification
5. Prediction
6. Result generation

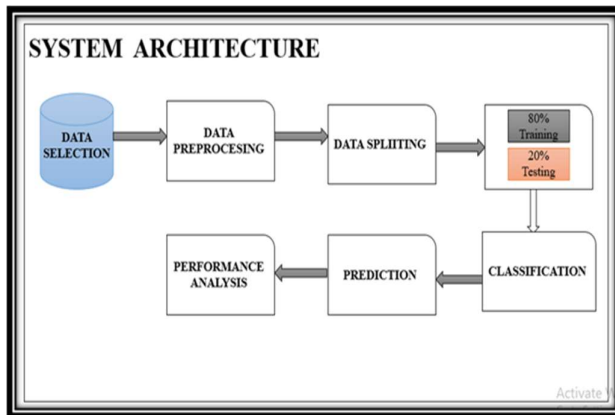
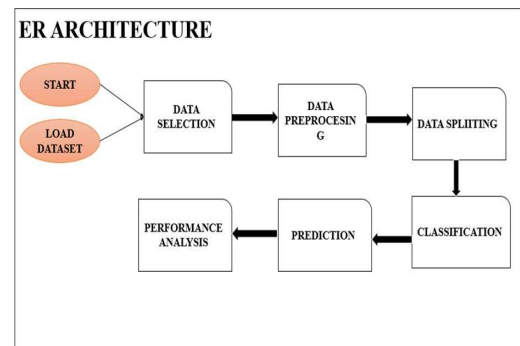


FIG 1: System Architecture



The system architecture for the health prevention concept integrates several advanced technologies to enhance cyber protection and intrusion prevention. At its core, the architecture employs a discriminative deep belief network (DBN) utilizing Long Short-Term Memory (LSTM) networks, which effectively processes both labeled and unlabeled cyber traffic data through a semi-supervised learning approach. This architecture incorporates local and non-local regularization techniques, allowing for improved classification accuracy while minimizing error rates. The system is designed to promptly detect and respond to intrusion activities, leveraging deep learning algorithms to analyze patterns in cyber traffic. By combining these elements, the architecture aims to create a robust health prevention system capable of adapting to evolving cyber threats while maintaining high operational efficiency.

IV. IMPLEMENTATION

It employs SS- GWO Algorithm and a leach K mean clustering algorithm for cluster formation

FIG.2:ER Architecture

User: Represents individuals interacting with the system (esystem administrators, cyber analysts).

Attributes: UserID

Cyber Traffic Data: Represents the data collected for analysis.

Attributes: DataID, Timestamp, SourceIP, DestinationIP, Protocol, Label (labeled/unlabeled).

Model: Represents the machine learning models used (e.g., LSTM).

Attributes: ModelID, ModelType, TrainingDate, Accuracy. Intrusion: Represents detected intrusions.

Attributes: IntrusionID, DetectionTime, Severity, Response Action.

Feedback: Represents feedback on the system's performance.

Attributes: FeedbackID, UserID, Date, Comments, Rating.

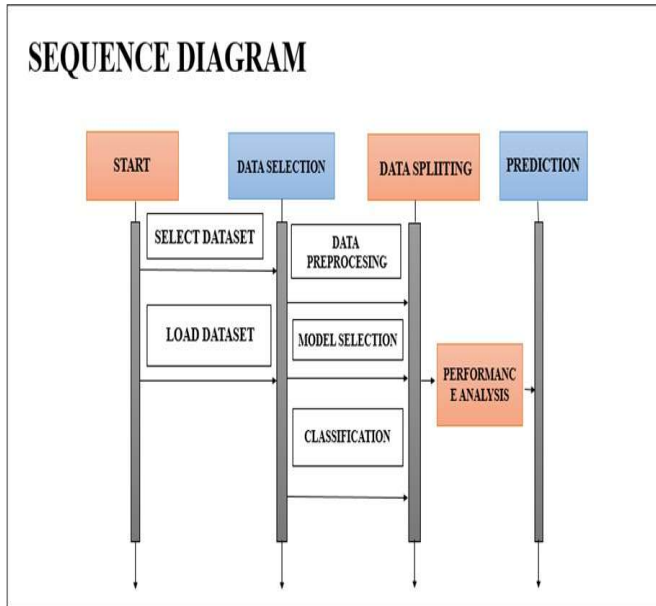


FIG 3: Sequence Diagram

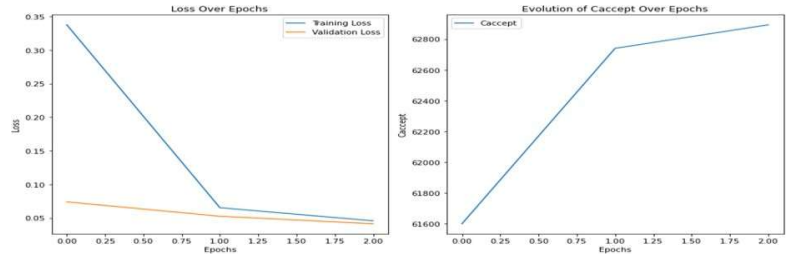
A sequence diagram visually represents the interactions between various components in the health prevention system over time, illustrating how processes flow and communicate. In this diagram, entities such as the User, Cyber Traffic Data, Model, and Intrusion Detection System are depicted as vertical lines, while horizontal arrows indicate messages exchanged between them. For example, the User initiates the process by inputting Cyber Traffic Data, which is then analyzed by the Model. The Model subsequently detects any intrusions and sends alerts back to the User. Additionally, the User may provide feedback on the detection results, completing the interaction loop. This diagram effectively captures the dynamic behavior of the system, showcasing the order of operations and how different components collaborate to ensure effective cyber protection.

V. PERFORMANCE ANALYSIS

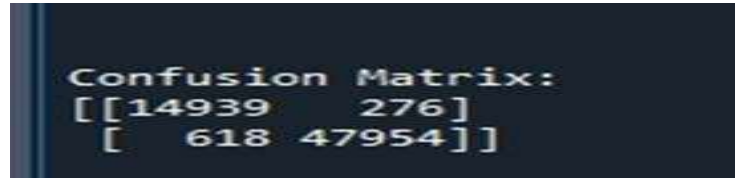
The Final Result will get generated based on the overall classification and prediction.

The performance of this proposed approach is evaluated using some measures like,

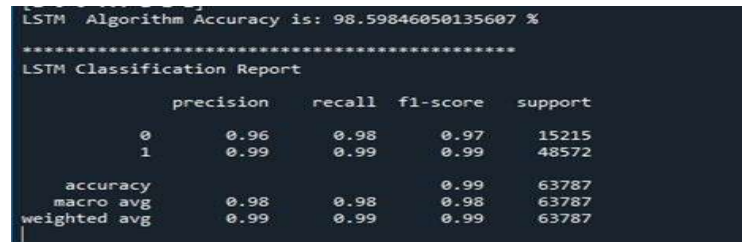
- Accuracy-98.59846050135607 %
- Precision-0.96
- Recall-0.96
- ROC -0.99



- **Confusion Metrics**



- **Classification Report**



Key Features:

LSTM combines the strengths of both generative and discriminative approaches, allowing for effective feature learning and robust classification.

Multiple hidden layers make up the conventional LSTM architecture, with the higher layers learning more specialized, task-oriented characteristics and the lower layers learning general, low-level features.

A DBN-style unsupervised pre-training of the hidden layers and supervised fine-tuning of the entire network using labeled data are both required for the training of an LSTM.

Advantages:

To extract intricate, hierarchical characteristics from the data, the LSTM can make use of deep neural networks' representational capabilities. Comparing discriminative training to generative models can result in better classification results, particularly when working with high-dimensional, large-scale data. When labeled data is hard to come by or prohibitively expensive, having the capacity to use both labeled and unlabeled data (through semi-supervised learning) might be advantageous. **Prediction**

- LSTM can be deployed in various network architectures, including traditional networks, software-defined networks (SDN), and edge computing environments.
- The algorithm can be integrated with existing network monitoring and security solutions to enhance the overall DDoS Security detection and mitigation capabilities.

- Predictive models can also be used to detect anomalies in network traffic or behavior, which can be indicative of potential security threats, such as DDoS securities or network intrusions.
- By establishing baseline patterns of normal network activity, predictive models can flag deviations from the expected behavior, enabling early detection and response to potential threats.

VI. RESULT GENERATION

The overall classification and forecast will be used to create the Final Result. The effectiveness of this suggested method is assessed using a number of metrics, including:

Accuracy

The ability of the classifier is referred to as accuracy. It accurately predicts the class label, and predictor accuracy measures how effectively a particular predictor can estimate the expected attribute value for a fresh set of data.

$$AC = (TP + TN)/(TP + TN + FP + FN)$$

Precision

The number of true positives divided by the total number of true positives plus false positives is the definition of precision.

$$Precision = TP/(TP + FP)$$

Recall

The number of right answers divided by the total number of results that ought to have been returned is known as recall. Recall in binary classification is referred to as sensitivity. It can be thought of as the likelihood that the query will return a pertinent document.

ROC

The relationship/trade-off between clinical sensitivity and specificity for each potential cut-off for a test or set of tests is commonly represented graphically via ROC curves. Additionally, the benefit of using the test or tests in question is suggested by the area under the ROC curve.

Confusion matrix

A confusion matrix is a table that is frequently used to explain how well a classification model (also known as a "classifier") performs when applied to a set of test data for which the true values are known. Although the confusion matrix itself is rather easy to understand, there can be some difficulty with the associated terminology

Testing of Product

Before the start of live operations, system testing is the stage of implementation that aims to ensure that the system operates accurately and effectively. The process of running a software with the goal of identifying errors is called testing. A test case that has a high likelihood of identifying an error is good. If a test addresses an error that hasn't been found yet, it's successful. The system's success depends on testing. System testing logically assumes that the objective will be accomplished if every component of the system is functioning properly. A range of tests are conducted on the candidate system, including Volume Street, online response, recovery, security, and usability tests. Before the system is prepared for user The following methods can

be used to test any engineered product. When a product's intended function is known, tests may be carried out to confirm that every feature works as intended. When a product's internal operation is understood, tests can be carried out to make sure that "all gears mesh," or that all internal components have received enough exercise and the product operates internally in accordance with specifications.

VII. CONCLUSION

Large-scale semi-supervised deep learning using local non-local regularization is facilitated by LSTM. Semi-supervised feature selection assesses the relevance of features using both labelled and unlabelled cyber traffic data. Deep learning has been specifically used in health prevention to lower

the mistake rate in health prevention and identify implicit security behavior based on intrusion data. When labelled data are sparse, LSTM can significantly improve its learning capacity for health prevention by employing a huge volume of unlabeled data. It was discovered that semi-supervised deep learning using LSTM, employing the exponent loss function with both local and non-local regularization, was more discriminative and outperformed in health-prevention tasks.

Future Enhancement

- Advancements in threat detection and response automation.
- Improving the accuracy and speed of intrusion prevention systems.
- Developing more robust and adaptive access controls.
- Enhancing data encryption and secure data management.
- Leveraging machine learning and AI for proactive defence.
- Strengthening human-centric Prevention through better training and awareness.
- Integrating emerging technologies like blockchain, quantum computing and edge computing to improve cyber resilience.

Reference

1. N. Martins, J. M. Cruz, T. Cruz and P. Henriques Abreu, "Adversarial Machine Learning Applied to Intrusion and Malware Scenarios: A Systematic Review," in *IEEE Access*, vol. 8, pp. 35403-35419, 2020, doi: 10.1109/ACCESS.2020.2974752.
2. G. Karatas, O. Demir and O. K. Sahingoz, "Increasing the Performance of Machine Learning-Based IDSs on an Imbalanced and Up-to-Date Dataset," in *IEEE Access*, vol. 8, pp. 32150-32162, 2020, doi: 10.1109/ACCESS.2020.2973219.
3. Su, T., Sun, H., Zhu, J., Wang, S. and Li, Y., 2020. BAT: Deep learning methods on network intrusion detection using NSL-KDD dataset. *IEEE Access*, 8, pp.29575-29585.
4. Jiang, Hui, Zheng He, Gang Ye, and Huyin Zhang. "Network intrusion detection based on PSO-XGBoost model." *IEEE Access* 8 (2020): 58392-58401.
5. Nagaraja, A., Boregowda, U., Khatatneh, K., Vangipuram, R., Nuvvusetty, R. and Kiran, V.S., 2020. Similarity based feature transformation for network anomaly detection. *IEEE Access*, 8, pp.39184-39196.
6. Architecture Working Group. View on 5G Architecture. Tech. rep. Available on-line at <https://5g-ppp.eu/wpcontent/uploads/2014/02/5G-PPP-5G-Architecture-WP-July2016.pdf>. 5G PPP, 2016.

7. F. Callegati et al. “SDN for dynamic NFV deployment”. In: *IEEE Communications Magazine* 54.10 (2016), pp. 89–95. DOI: 10.1109/MCOM.2016.7588275.
8. Davide Borsatti et al. “Mission Critical Communications Support With 5G and Network Slicing”. In: *IEEE Transactions on Network and Service Management* 20.1 (2023), pp. 595–607. DOI: 10.1109/TNSM.2022.3208657.
9. Naga Katta et al. “Clove: Congestion-aware load balancing at the virtual edge”. In: *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*. 2017, pp. 323–335.
10. Hui Han et al. “Applications of sketches in network traffic measurement: A survey”. In: *Information Fusion* 82 (2022), pp. 58–85.
11. Tooska Dargahi et al. “A survey on the security of stateful SDN data planes”. In: *IEEE Communications Surveys & Tutorials* 19.3 (2017), pp. 1701–1725.
12. Ran Ben-Basat et al. “Heavy hitters in streams and sliding windows”. In: *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. IEEE. 2016, pp. 1–9.
13. Ran Ben-Basat et al. “Efficient measurement on programmable switches using probabilistic recirculation”. In: *2018 IEEE 26th International Conference on Network Protocols (ICNP)*. IEEE. 2018, pp. 313–323.
14. Lu Tang, Qun Huang, and Patrick PC Lee. “A fast and compact invertible sketch for network-wide heavy flow detection”. In: *IEEE/ACM Transactions on Networking* 28.5 (2023), pp. 2350–2363.
15. Tushar Swamy et al. “Taurus: a data plane architecture for per-packet ML”. In: *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*. 2022, pp. 1099–1114.
16. Coralie Busse-Grawitz et al. “pforest: In-network inference with random forests”. In: *arXiv preprint arXiv:1909.05680* (2019).
17. Bruno Coelho and Alberto Schaeffer-Filho. “BACKORDERS: using random forests to detect DDoS securities in programmable data planes”. In: *Proceedings of the 5th International Workshop on P4 in Europe*. 2022, pp. 1–7.