*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9s*
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

# An Intrusion Detection System (Ids) Schemes for Cybersecurity in Software Defined Networks

**Dr. Rohith Vallabhaneni,**

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA. rohit.vallabhaneni.2222@gmail.com

**Dr. Srinivas A Vaddadi,**

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA. Vsad93@gmail.com

**Dr. Abhilash Maroju,**

Ph.D. Research Graduate, Department of Information Technology, University of the Cumberlands , USA. doctorabhilashmaroju@gmail.com

**Sravanthi Dontu,**

PhD Research Student, Department of Information Technology, University of the Cumberlands, USA. sravanthi.dontu13@gmail.com

## ABSTRACT

The process of analysing and improving network traffic is of tremendous relevance to network management and multimedia data mining techniques. Security in Software Defined Networks (SDNs), which rely on a programmable controller in the middle, has recently emerged as the most challenging aspect of SDNs. Network traffic monitoring is critical for detecting and exposing intrusion anomalies in an SDN context. Thus, this study offers a thorough assessment of the NSL-KDD dataset using five separate clustering algorithms: K-means, Farthest First, Canopy, Density-based method, and Exception-maximization (EM). The software used to conduct the comparisons is the Waikato Environment for Knowledge Analysis (WEKA). In addition, the article introduces a knowledge discovery in databases (KDD)–based deep learning (DL) model for intrusion detection that is SDN-based. Initially, the dataset that is being used is clustered into four main attack types and one normal category. We will next go over the steps necessary to build a deep learning intrusion detection system that is based on SDN. The results provide an objective assessment of the several attack types present in the KDD dataset. Just like other methods, the results demonstrate that the proposed deep learning strategy provides better intrusion detection performance. As an illustration, the tested dataset demonstrates a detection accuracy of 94.21% when using the suggested approach.

## 1. INTRODUCTION

Internet and communication technology (ICT) have come a long way since the 1990s, elevating it to the position of preeminent global network system. Approximately half of the global population uses the internet, with 95% of that number residing in North America and 85% in Europe, according to the research. Due to the expansion of the internet of things (IoT), the number of devices connected to the internet has been rising at a steady rate over the past several years. According to Cisco, there will be around 27.1 billion network devices globally by the end of 2021 [1]. Innovations in cellular networks, big data, and cloud computing are directly responsible for the explosion of connected devices and IoT use cases. Smart buildings, online healthcare services, home automation systems, autonomous vehicles, and surveillance systems are just a few examples of how the Internet of Things (IoT) is making our lives easier. Hackers' ability to exploit this exceptional architecture to corrupt various network systems and data assets is a reflection of both technological innovation and this rapid growth.

### 1.1. SDN framework

The control, infrastructure, and application layers make up a typical SDN architecture. Among the many services made available by the application layer—the top and most fundamental layer—are task scheduling, traffic control, and system safety. This application plane must inform the control plane of its needs and the information it plans to transmit about the network through the Northbound Interface (NBI).

A centralised conceptual controller is a part of SDN's control plane; it provides an idealised view of the system to SDN applications and transforms application layer requirements into SDN data paths. These controllers allow for the management and control of assets in the data layer and also include control logic. In contrast, the data layer—also known as the forwarding plane or switches—of SDN has a number of network components. All system-wide network activity is broadcast by conventional devices, which also reveal the communication channel. Transmitting packets according to rules given by the controller is the job of the more basic modules known as switches in a software-defined network. Programmatically handling all forwarding is the responsibility of the data plane and SDN control plane, which together form the southbound interface of the SDN [2]. The separation of the control plane and data plane makes it easy for network administrators to modify security policies. This lets them build adaptable networks that can handle software-based rather than hardware-based control of business needs [3].

### 1.2. SDN and open flow

The control and information management modules of a typical network device are where most of the action takes place. However, in software-defined networking (SDN), the two planes are physically separated. In order to establish the network's architecture, this controller is linked to several networking devices [4-8]. With the flow stat command, the system administrator can also remove harmful flow entries and change the communication's trajectory.

## 2. LITERATURE REVIEW

The wide variety of SDN implementations poses a significant threat to SDN security. Consequently, a reliable NIDS is necessary for the network. The term "intrusion detection system" (IDS) can refer to either software or hardware that constantly scans a network for any suspicious activity. When it detects suspicious activity, it notifies the operator. Moreover, it records instances of exploited packets on the network. The intrusion detection system's SDN block diagram is displayed in Figure 1[9].

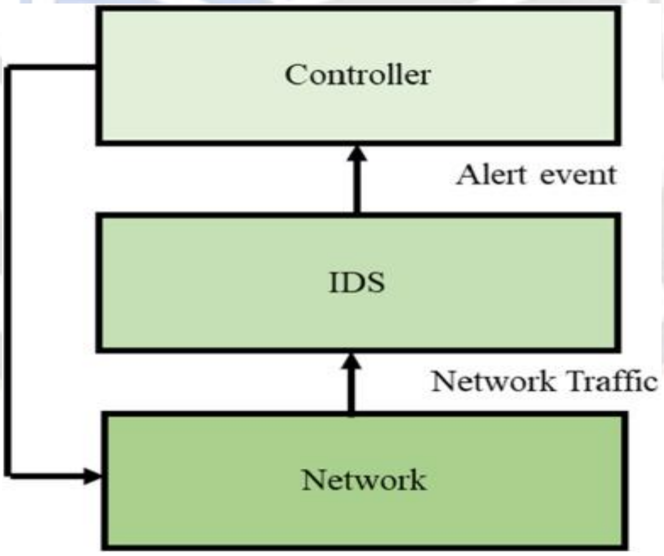


Fig. 1. Block diagram of IDS in SDN.

Due to the fact that many researchers have been focusing on the problem of network intrusion and assault detection. This paper's authors, Jose, Ancy Sherin, and others [10], created and implemented a system to identify and mitigate flooding DDoS attacks through SDN network activity. Various variants of these assaults include flooding with TCP SYN requests, HTTP requests, UDP, and ICMP. The proposed system used a litany of classification algorithms to determine whether incoming communication was benign or malicious [11].

***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

We employed an ANOVA (Analysis of Variance) F-Test statistical technique in conjunction with a features extraction tool to identify the generated characteristics for classification. Evaluation metrics for the three features selected from the feature selection unit were used to test all of the classifiers. After that, everything was put together. A novel software-enabled intrusion detection system (IDS) design that accounts for SDN was proposed by Ibrahim, Omar Jamal, and colleagues [12] to make use of SDN's capabilities. The authors combined the capabilities of ML algorithms with those of the IDS to protect the network from threats and obtain high classification accuracy [13].

In [14], a comprehensive approach to protecting SDNs against malicious activities was proposed. This method takes advantage of everything that SDNs are intrinsically good at while simultaneously using data mining techniques to identify and classify SDN data layer errors. In addition, the mechanics and framework of the system were covered, with an emphasis on flow rule classification and definition. A software-defined networking (SDN) testbed that mimicked real-world SDN flows was used to evaluate the idea. In addition, the study demonstrated that the system has potential for effective application in SDNs, reducing risks associated with various forms of hostile intrusion. A comparison of various systems' abilities to identify and categorise malicious traffic showed that hybrid data mining techniques performed the best.

The suggested approach in [15-16] integrated the best features of intrusion detection systems that were based on flow and packets to achieve the best possible detection accuracy and network speed. The present flow-based intrusion detection system uses support vector machines (SVMs) trained on the DARPA database for anomaly identification. Intruders can be located and stopped at this initial line of defence.

## 3. PROPOSED INTRUSION DATA-BASED CLUSTERING AND DETECTION SCENARIOS

This section provides an in-depth analysis of the planned effort to cluster traffic data and detect intrusions in SDNs. Figure 2 depicts the full hybrid system that was proposed for gathering and categorising intrusion data via SDN.

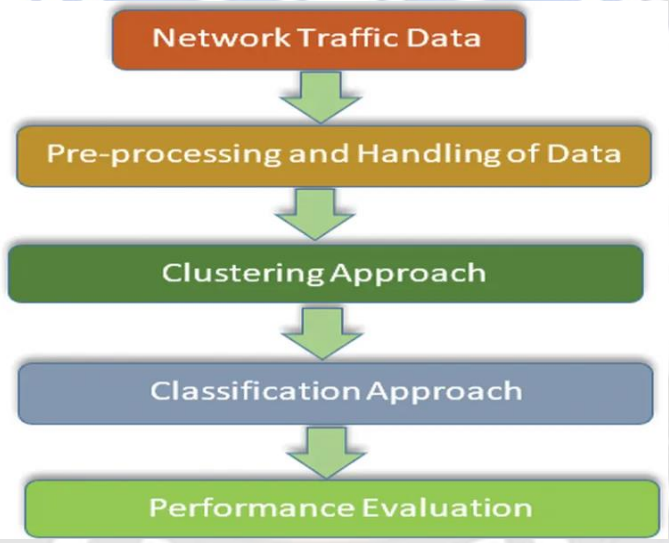


**Figure 2:** An intrusion detection hybrid system that combines clustering and classification was proposed for SDN.

### 3.1 Traffic Data-Based Clustering Algorithms

Data is clustered when it is divided into groups according to shared or unique characteristics. One major benefit of clustering is that it can identify suspicious intrusions even when no background information is known. In this essay, we will examine and analyse five different clustering algorithms: K-means, Farthest First, Canopy, Exception-maximization (EM), and density-based approach. Here we present the comparison clustering techniques that were used.

1) **K-means clustering algorithm.** The K-means clustering algorithm is a cluster analysis approach that we use to create K disjoint clusters based on the feature values of the items that need to be categorised.
2) **Farthest first clustering algorithm.** Similar to the K-means algorithm, it selects cluster centres and assigns objects to them using a maximum distance metric. As a starting point, we can look at the values that are most dispersed around the mean. Cluster assignment is an alternate clustering approach that yields a link with a high

***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

Session Count at the beginning of the cluster, for example, more at cluster 0 than cluster 1, and so on.

3) **Canopy clustering algorithm.** This approach is unsupervised and uses pre-clustering. You can use it before running the Hierarchical clustering or K-means algorithms as a pre-processing step. This clustering approach is quick, easy, and accurate; it arranges clustered objects such that each one is the only point in a space with many dimensions of features. The fast approximation distance measure and two thresholds, T1 > T2, are used for processing in the canopy scheme.

4) **Exception-maximization (EM) clustering algorithm.** The K-means scheme is thought of as an extension of it. It uses a weight that represents the membership likelihood to group the object into a cluster. Accordingly, groups do not have any hard and fast rules. The EM scheme outperforms the K-means scheme in terms of accuracy.

5) **Density-based clustering algorithm.** It is an algorithm for clustering data. It takes a set of points in a given place and clusters them according to how densely they are populated, labelling as outliers any points that are isolated in low-density areas where their neighbours are too far away.

### 3.2 SDN-Based IDS Using Deep Learning Model

In this section, we present the suggested SDN-based IDS that utilises deep learning. With the proposed method, malicious attacks can be more accurately identified as intrusion actions. Figure 3 displays the proposed IDS deep learning model based on SDN. The NSL-KDD dataset is utilised to evaluate the suggested SDN-based IDS using a DL technique. The experiments were conducted on a machine that has an Intel Core i5 GHz CPU, 12 GB of RAM, and 500 GB HD. The software used for the experiments was Spyder on Anaconda navigator, which is a Python programming language.

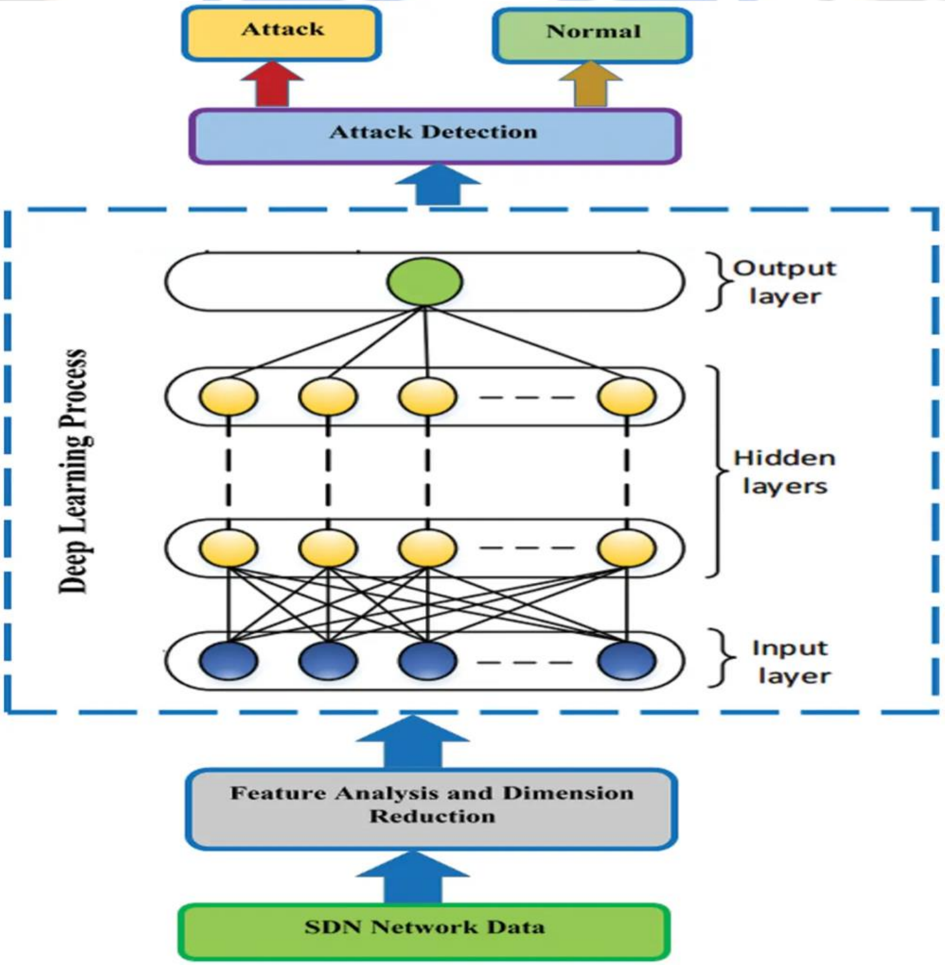


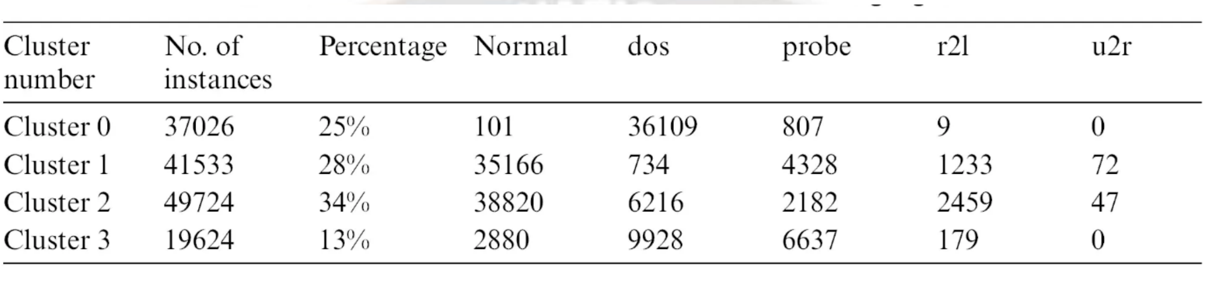
**Figure 3:** A model for intrusion detection using SDN-based deep learning

***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

The algorithms used in this work are evaluated using the NSL-KDD dataset. This dataset was introduced to fix a number of problems with the KDD-cup 1999 dataset. Historically, IDS model effectiveness was evaluated using the test and train datasets, which made up the initial KDD'99 dataset. Basic features, content-dependent features, and traffic-based features are all integrated. The NSL-KDD dataset is a way to add additional information to the KDD dataset. This research uses it to assess the quality of the strategies proposed for feature selection subgroups.

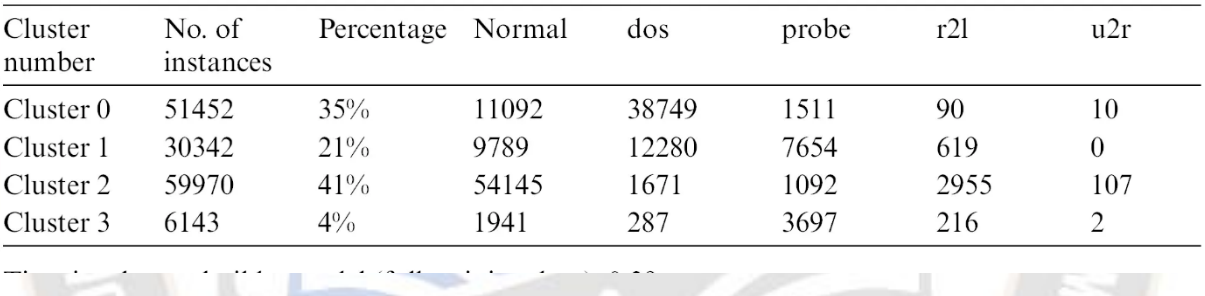
## 4. RESULTS AND DISCUSSIONS

**Table 1: Simulation resuls of K-Means clustering algorihthm**



| Cluster number | No. of instances | Percentage | Normal | dos | probe | r2l | u2r |
|---|---|---|---|---|---|---|---|
| Cluster 0 | 37026 | 25% | 101 | 36109 | 807 | 9 | 0 |
| Cluster 1 | 41533 | 28% | 35166 | 734 | 4328 | 1233 | 72 |
| Cluster 2 | 49724 | 34% | 38820 | 6216 | 2182 | 2459 | 47 |
| Cluster 3 | 19624 | 13% | 2880 | 9928 | 6637 | 179 | 0 |

**Table 2: Simulation results of farthest first clustering algorithm**



| Cluster number | No. of instances | Percentage | Normal | dos | probe | r2l | u2r |
|---|---|---|---|---|---|---|---|
| Cluster 0 | 51452 | 35% | 11092 | 38749 | 1511 | 90 | 10 |
| Cluster 1 | 30342 | 21% | 9789 | 12280 | 7654 | 619 | 0 |
| Cluster 2 | 59970 | 41% | 54145 | 1671 | 1092 | 2955 | 107 |
| Cluster 3 | 6143 | 4% | 1941 | 287 | 3697 | 216 | 2 |

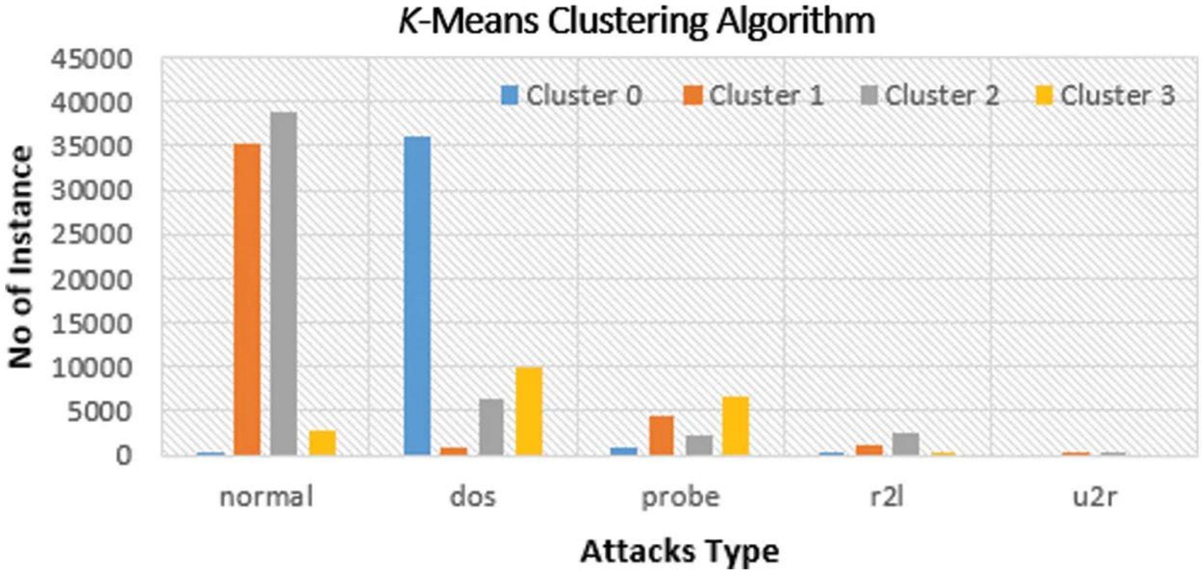


**Figure 4:** Clustering instances according to the K-means algorithm

***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

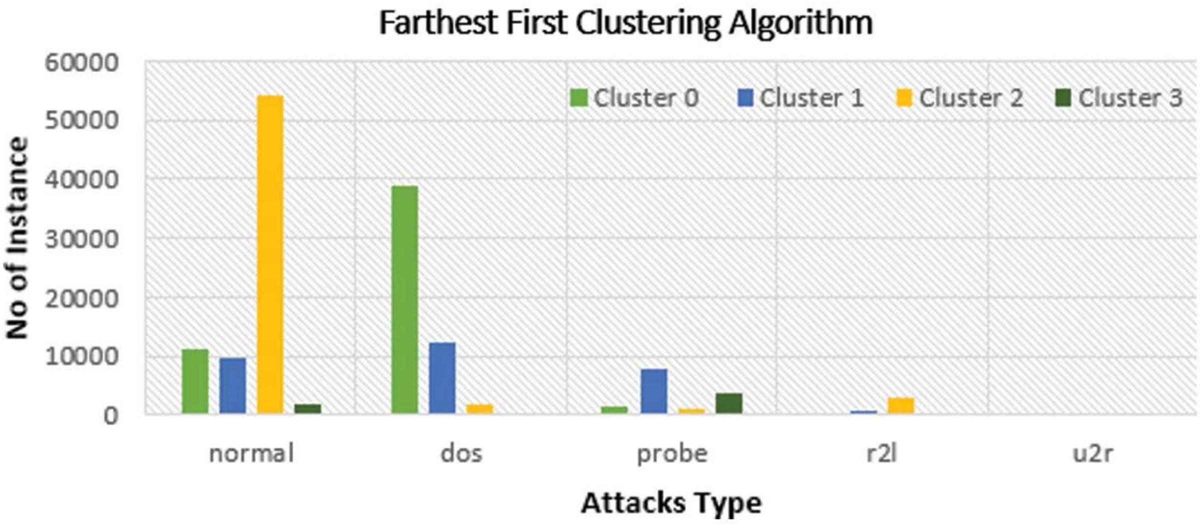


**Figure 5:** A method for clustering instances based on their distance from the origin.

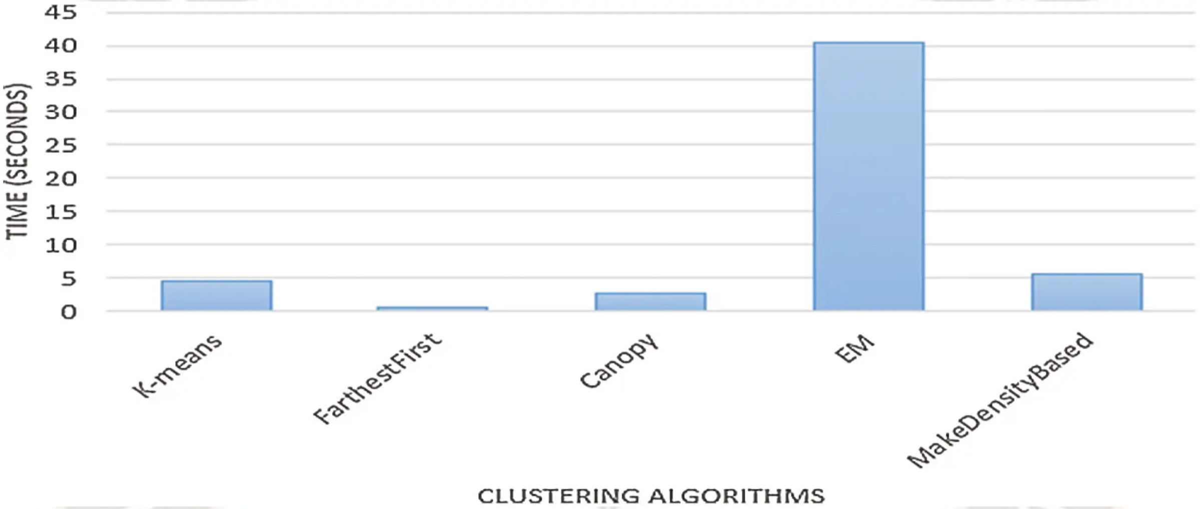


**Figure 6:** Evaluation of clustering methods' performance in relation to runtime

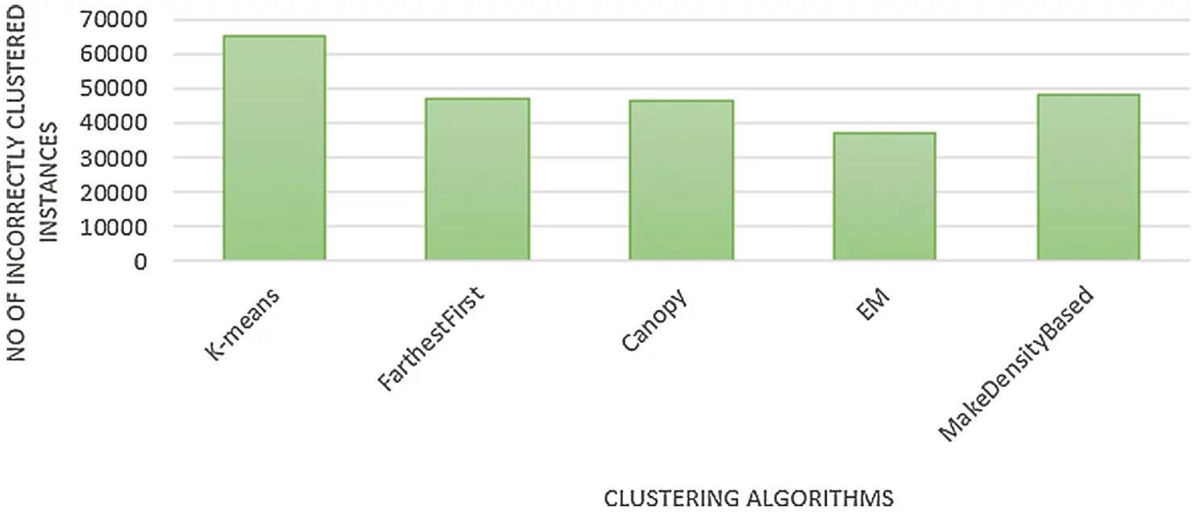


**Figure 7:** Analysing the five clustering strategies in relation to the amount of instances that were erroneously clustered

In Figure 5, we can observe the outcomes of the Farthest First algorithm's clustering of instances. Figure 6 compares the five algorithms in terms of how long it takes to run each one. Figure 7 displays a comparison of five different clustering algorithms, ordered by the amount of instances that were improperly grouped.

## CONCLUSION AND FUTURE WORK

Identifying and preventing intrusions by unknown or unseen threats is a pressing issue in the development of secure SND systems that rely on intrusion detection systems. Thus, this research presents a study of the NSL-KDD dataset based on clustering, employing the following algorithms: EM, K-means, Canopy, and Farest First are also methods for density-based clustering. In addition, it paves the way for the development of an intrusion detection system by introducing a deep learning system that can successfully detect unknown malicious and illegitimate behaviours. The simulation results show that the Farthest First strategy had a better example distribution compared to the other four clustering techniques. When it comes to detecting intrusion events, the deep learning model outperforms conventional methods. An impressive 94.21% detection accuracy was attained by the suggested DL approach, for instance. To identify updated forms of assaults on SDN networks, we want to use sophisticated AI algorithms in our future projects. On top of that, we will create and plan the actual deployment of an IoT-based SDN network for cybersecurity applications.

## REFERENCES

1. Pedro Manso, José Moura, Carlos SerrãoSDN-based intrusion detection system for early detection and mitigation of DDoS attacksInformation (2019), p. 106 10.3
2. Yogita Hande, Akkalashmi Muddana, Santosh DaradeSo ftware-defined network-based intrusion detection systemInnovations in Electronics and Communication Engineering, Springer, Singapore (2018), pp. 535-543
3. S. Smys, A. Basar, H. WangHybrid intrusion detection system for internet of Things (IoT)J. ISMAC, 2 (4) (2020), pp. 190-199
4. A.K. Sarica, P. Angin Explainable security in SDN-based IoT networks Sensors, 20 (24) (2020), p. 7326, 10.3390/s20247326 Published 2020 Dec 20 View article Google Scholar
5. Bei Gong, Jingxuan Zhu, Yubo Wang Construction of trusted routing based on trust computation Wireless Communications and Mobile Computing 2021 (2021) Google Scholar
6. Guiping Zheng, Bei Gong, Yu Zhang Dynamic network security mechanism based on trust management in wireless sensor networks Wireless Commun. Mobile Comput. (2021), p. 2021 Google Scholar
7. Esubalew M. Zeleke, Henock M. Melaku, Fikreselam G. Mengistu Efficient intrusion detection system for SDN orchestrated internet of things J. Comput. Netw. Commun., 2021 (2021), 10.1155/2021/5593214
8. Mavra Mehmood, et al. A hybrid approach for network intrusion detection CmcComput. Mater. Continua, 70 (1) (2022), pp. 91-107
9. Ancy Sherin Jose, Latha R. Nair, Paul VargheseTowards detecting flooding DDOS attacks over software defined networks using machine learning techniquesRev. Geintec-GestaoInovacao E Tecnol., 11 (4) (2021), pp. 3837-3865
10. Jonathon S. Goodgion Active Response Using Host-Based Intrusion Detection System and Software-Defined Networking (2017)
11. Omar Jamal Ibrahim, Wesam S. BhayaIntrusion detection system for cloud based software-defined networksJournal of Physics: Conference Series, vol. 1804, IOP Publishing (2021)1
12. Mahmoud Said ElSayed, et al. A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique J. Netw. Comput. Appl., 191 (2021), Article 103160
13. M. Amanowicz, D. Jankowski Detection and classification of malicious flows in software-defined networks using data mining techniques Sensors, 21 (9) (2021), p. 2972, 10.3390/s21092972 Published 2021 Apr 23
14. Q. Schueller, K. Basu, M. Younas, M. Patel, F. Ball A hierarchical intrusion detection system using support vector machine for SDN network in cloud data center 2018 28th International Telecommunication Networks and Applications Conference (ITNAC) (2018), pp. 1-6, 10.1109/ATNAC.2018.8615255
15. Ramya Manikyam, J. Todd McDonald, William R. Mahoney, Todd R. Andel, and Samuel H. Russ. 2016.Comparing the effectiveness of commercial obfuscators against MATE attacks. In Proceedings of the 6th Workshop on Software Security, Protection, and Reverse Engineering (SSPREW'16)
16. R. Manikyam. 2019.Program protection using software based hardware abstraction.Ph.D.Dissertation.University of South Alabama