**1. INTRODUCTION**

With the rapid development and wide application of 5G, IoT, Cloud Computing, and other technologies, network scale, and real-time traffic become more complex and massive, cyber-attacks have also become complex and diverse, bringing significant challenges to cyberspace security. As the second line of defense behind the firewall, the Network Intrusion Detection System(NIDS) needs to accurately identify malicious network attacks, provide real-time monitoring and dynamic protection measures, and formulate strategies.In real cyberspace, normal activities occupy the dominant position, so most traffic data are normal traffic; only a few are malicious cyber-attacks, resulting in a high imbalance of categories. In the highly imbalanced and redundant network 7550 This work is licensed under a Creative Commons Attribution 4.0 License. Cyber-attacks can hide in a large amount of normal traffic. Therefore, the machine learning algorithm cannot fully learn the distribution of a few categories, and it is easy to misclassify .

**1.1 RELEVANCE OF THE PROJECT**

By using this software one can easily get aware of the intrusion .Can get to know which type of intrusion is occured.

**1.2 PURPOSE**

There is no firewall that is foolproof, and no network is impenetrable. Attackers continuously develop new exploits and attack techniques designed to circumvent your defenses. Many attacks leverage other malware or social engineering to obtain use credentials that grant them access to your network and data. An intrusion detection system is crucial for network security because it enables you to detect and classify the intrusion.

**1.3 SCOPE OF THE PROJECT**

This software is very useful as new technologies are emerging. The number of intrusions is also increasing .This software helps to detect such intrusions and know which type of intrusion occurred. In future in addition to detection, prevention techniques can be implied in this system to prevent such intrusions.

**1.4 OBJECTIVE**

Intrusion Detection System is a software application to detect network intrusion using co-clustering algorithm.

**CHAPTER 2**

**2. LITERATURE REVIEW**

**1.An Intrusion Detection Model[D.E Denning],1987**

A model of real time intrusion detection expert system capable of detecting break-ins,penetration and other forms of computer abuse described.The model is based on the hypothesis that security violations can be detected by monitoring a system audit records for abnormal patterns of system usage.The model includes profiles for representing the behavior of subjects with respect to objects in terms of metrics and statistical models and rules for acquiring knowledge about this behavior from audit records and detecting anomalous behavior.

**2."‘Machine learning techniques for intrusion detection,’’[Mamani and M. Movahed] ,2013.**

An Intrusion Detection System (IDS) is a software that monitors a single or a network of computers for malicious activities (attacks) that are aimed at stealing orcensoring information or corrupting network protocols.Most techniques used in today's IDS are not able to deal with the dynamic and complex nature of cyber attacks on computer networks. Hence, efficient adaptive methods like various techniques of machine learning can result in higher detection rates, lower false alarm rates and reasonable computation and communication costs. In this paper, study several such schemes and compare their performance. In this paper, study several such schemes and compare their performance. Divide the schemes into methods based on classical artificial intelligence (AI) and methods based on computational intelligence (CI).

**3.‘‘Toward generating a new intrusion detection dataset and intrusion traffic characterization,’’ [Sharafaldin, A. H. Lashkari, and A. A. Ghorbani], 2018**

With exponential growth in the size of computer networks and developed applications, the significant in-creasing of the potential damage that can be caused by launching attacks is becoming obvious. Meanwhile,Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) are one of the most important defense tools against the sophisticated and ever-growing network attacks. Due to the lack of adequate dataset, anomaly-based approaches in intrusion detection systems are suffering from accurate deployment, analysis and evaluation. Based on our study over eleven available datasets since 1998, many such datasets are out of date and unreliable to use. Some of these datasets suffer from lack of traffic diversity and volumes, some of them do not cover the variety of attacks, while others anonymized packet information and payload which cannot reflect the current trends, or they lack feature set and metadata. This paper produces a reliable dataset that contains benign and seven common attack network flows, which meets real world cri-teria and is publicly available. Consequently, the paper evaluates the performance of a comprehensive set of network traffic features and machine learning algorithms to indicate the best set of features for detecting the certain attack

4.**‘‘I-SiamIDS: An improved Siam-IDS forbhandling class imbalance in network-based intrusion detection systems,’’[P. Bedi, N. Gupta, and V. Jindal, Sep. 2020.**

NIDSs identify malicious activities by analyzing network traffic. NIDSs are trained with the samples of benign and intrusive network traffic. Training samples belong to either majority or minority classes depending upon the number of available instances. Majority classes consist of abundant samples for the normal traffic as well as for recurrent intrusions. Whereas, minority classes include fewer samples for unknown events or infrequent intrusions. NIDSs trained on such imbalanced data tend to give biased predictions against minority attack classes, causing undetected or misclassified intrusionst. Data-level balancing approaches indirectly improve the performance of NIDSs, they do not address the underlying issue in NIDSs i.e. they are unable to identify attacks having limited training data only. This paper proposes an algorithm-level approach called I-SiamIDS, which is a two-layer ensemble for handling class imbalance problem. I-SiamIDS identifies both majority and minority classes at the algorithm-level without using any data-level balancing techniques. The first layer of I-SiamIDS uses an ensemble of b-XGBoost, Siamese-NN and DNN for hierarchical filtration of input samples to identify attacks. These attacks are then sent to the second layer of I-SiamIDS for classification into different attack classes using m-XGBoost.

**3. EXISTING SYSTEM**

Existing Systems were mostly based on deep learning. Data do not get updated automatically. Deep learning has limitations to learn preprocessed features and cannot take advantage of of its automatic feature extraction

**4. PROPOSED SYSTEM**

In this system when a sender sends a content to receiver the intrusion if occurred it is being detected and classified. The percentage of intrusion is graphically represented.In Feedback is being send to the sender from the receiver specifying the occurrence of intrusion Co-clustering algorithm is used in it. Machine learning is used that will keep improving in accuracy and efficiency.