IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305432 |

Intrusion Detection System in Cloud Computing using Machine Learning Technique

Mrs. Swetha T[1], Manasa Sindhu P[2], Meghana B[3], Monika K[4], Nikitha S A[5]

Assistant Professor, Department of Computer Science and Engineering, S J C Institute of Technology, Chickaballapur, Karnataka, India[1]

U.G. Student Department of Computer Science and Engineering, S J C Institute of Technology, Chickaballapur, Karnataka, India[2,3,4,5]

ABSTRACT Research on intrusion detection systems for cloud using artificial neural networks (ANN) with machine learning procedures. Interruption location is an versatile engineering that can identify malevolent movement in cloud computing. Cloud computing may be a maritime innovation outlined to encourage get to to organize and computing assets to enhance and empower frameworks. The essential good thing about the cloud is that it gives an environment that can adaptably scale to meet changing needs, is repeatable, and can be right away scaled down as required. You wish to ensure your cloud environment from malevolent assaults. This preparing tallied malevolent action inside a cloud computing environment. Preparing was conducted employing a preprocessed dataset of an gatecrasher alert framework. The comes about appear that the proposed engineering is exceedingly viable in recognizing different assaults, with moo untrue positive and wrong positive rates. This approach can naturally identify assaults, sparing time and assets. The proposed framework employments manufactured neural systems, which are administered and unsupervised machine learning calculations, to distinguish known and obscure assaults, individually.

KEYWORDS: Artificial Neural Network, Intrusion detection system, Machine learning, anomaly detection, cloud computing, feature engineering.

I. INTRODUCTION

Nowadays, the cloud suffers from many security issues such as availability, data confidentiality, integrity, and control privileges. Additionally, the Internet is used to facilitate access to services provided by the cloud. This is a major source of threats that can infect cloud systems and resources. Improving cloud security then becomes a key challenge for cloud providers. Therefore, different approaches such as firewall tools, data encryption algorithms, authentication protocols, and cloud technologies enable convenient, on-demand access to shared networks, storage, and resources, giving you more choices regarding service models. These models are platform mode Software as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS). Used in private, public, or hybrid cloud deployment models. It is based on information technology and infrastructure for providing various resources such as hardware equipment, operating systems, storage services, networks, entire software applications, and infrastructure at low cost. Benefit from greater Cost efficiency, scalability, faster development, and minimal administrative effort. Due to its elasticity and measured service characteristics according to the American Standards Institute, the cloud provides high- performance services. Comparison with a single intruder alarm system, a coordinated intrusion detection system improves detection accuracy. This is because knowledge of attack patterns and impact is limited. The solution to this type of threat is to develop effective intrusion detection systems. He has his two types of approaches to attack detection in IDS. This approach allows you to achieve higher accuracy. Additional features have been developed to better protect cloud environments from various attacks. However, traditional systems are not suitable for securing cloud services against different boundaries. Therefore, numerous intrusion detection approaches have been proposed and applied to detect and prevent unwanted activities in real time. Detection methods are generally categorized as exploit detection methods that use known attacks to detect intrusions andanomalies. When new computer systems are introduced, scientists and researchers are concerned about their protection. Ensuring the security of information processing in information systems is critical to the success of knowledge acquisition systems.

II. LITERATURE SURVEY

In this section, previously performed studies on intrusion detection using machine learning techniques are done. Many researchers are interested in using machine learning to find unusual patterns in network traffic in cloud

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305432 |

computing. They've come up with different methods to detect these anomalies effectively. One common approach is using sliding window techniques along with deep learning and machine learning algorithms. These methods help in spotting abnormal traffic and potential attacks. Researchers keep developing new algorithms to keep up with technology changes.

These algorithms use machine learning and deep learning to detect intrusions and classify various types of attacks. The studies have found success in detecting abnormal patterns in network traffic, especially in the IoT environment. They've introduced techniques like Long Short-Term Memory and automated encoders, which help extract accurate information. These methods highlight the potential of using deep learning and machine learning for spotting anomalies in cloud computing. Therefore, more research in necessary to handle high-dimensional data effectively and detect network anomalies in real-time. The present state of the art proposes many solutions for the avoidance year 2021.
One study introduces a new method for cloud providers to detect attacks in IoT environments using hierarchical adversarial attack generation and graphneural networks.

This method helps identify vulnerable nodes and prioritize traffic patterns with high attack potential. Another study addresses the challenge of detecting anomalies in industrial cyber- physical systems with limited data and security concerns. In 2020, an architectural model was introduced for assessing the risk of information systems and network data using the CICIDS2017 dataset and machine learning algorithms. This model evaluated techniques like k- nearest neighbor, gradient boosting tree, and decision tree. It aimed to predict intrusions effectively in IoT environments. While these methods produced better and more accurate outcomes, they required significant resources to establish hidden layers and units. Increasing input and rules in cloud resulting in overfitting issues that affect the efficiency of the neural network.

III. PROPOSED METHODOLOGY

In this area, we depicted the strategies utilized for the interruption location. Different machine learning strategies are utilized expound the arrangement. The modules included within the proposed demonstrate are data collection, data pre- processing, clustering layer and classification.

Data Collection:
The lack of an idealized dataset makes data collection in the field of interruption discovery potentially difficult. Some of the analysts utilize self-generated dataset to overcome these issues.

Data Pre-processing:
It is the method of expulsion of unwanted, erroneous or unimportant data from the chosen dataset.

Data Purification:
Within the chosen dataset there will be a small number. To evaluate those lost, erroneous and insignificant data, data Purification process is utilized.

Standardization:
It includes changing crude data into reliable arrange which is appropriate for investigation.

Feature reduction:
Include diminishment diminishes the features of the dataset, in result which makes a difference within the data representation.

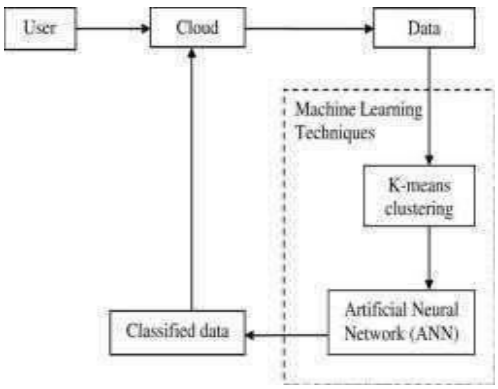

Fig 1: Architecture of the proposed system

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305432 |

IV. ALGORITHMS

Clustering Layer:

1. K-means clustering method : This algorithm gathers data in an unsupervised manner by instances in the dataset where testing and preparation are done.
2. This clustering algorithm generates the number of clusters according on the predefined esteem. In this case, the clusters resulting in overfitting issues that affect the are shaped by the calculation according to the centroid esteem.
3. Reducing the distance between data occurrences and the groups they belong to is clustering algorithms primary goal. This process is repeatedly carried out until the computation identifies the superior clusters. 'K' number of clusters are obtained at the method's conclusion; however, k may be a predefined value. The K-means algorithm's strategy is given as follows after takes after and the K-means algorithm's process is described as below. The K-means method is shown in step by step procedure in the below process of the algorithm.

Artificial Neural Networks (ANNs):

ANN is a another type of administered machine learning computation that draws its inspiration from the way the human brain's apprehensive framework functions. ANNs comprise of interconnected nodes, called neurons or counterfeit neurons, organized into layers. AN input layer, one or more hidden layers, and a yield layer are consistently incorporated into the layers. This machine learning calculation makes a difference to classify the highlights in the dataset and produces a indicated yield whether it may be a known or obscure assault.

V. RESULTS

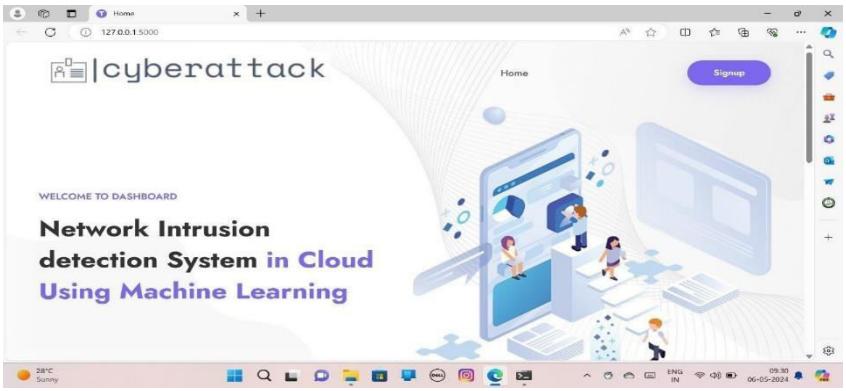

Figure 1: homepage to welcome the users to the dashboard indicating the page might be part of a larger application interface.

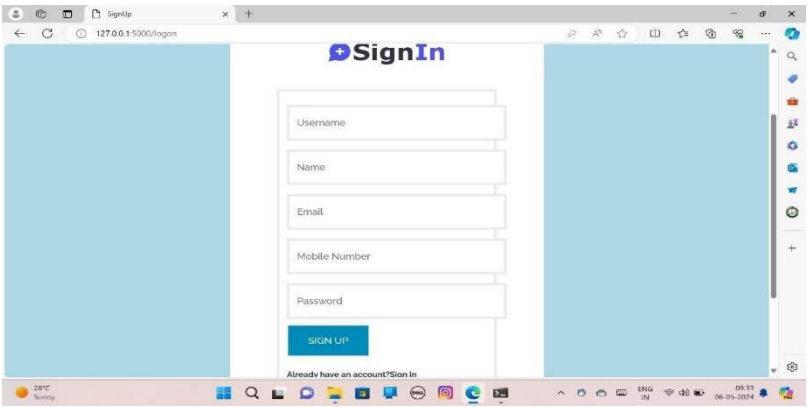

Figure 2: This page allows the new users to login to the network intrusion detection system by entering their credentials like Username, Name, Email, Mobile Number, Password.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305432 |

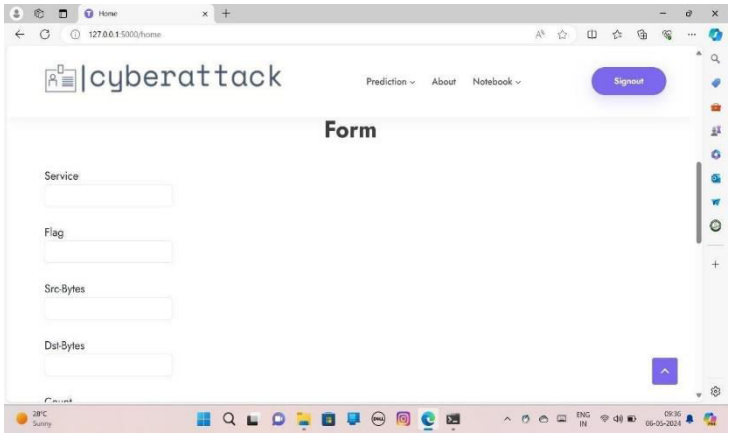

Figure 3: This page indicates the fields where the values to be detected are entered. The Prediction field may be used to display the NIDS's prediction about whether the network traffic is normal or malicious. The count field may be used to display the number of times that a particular type of network traffic has been seen.

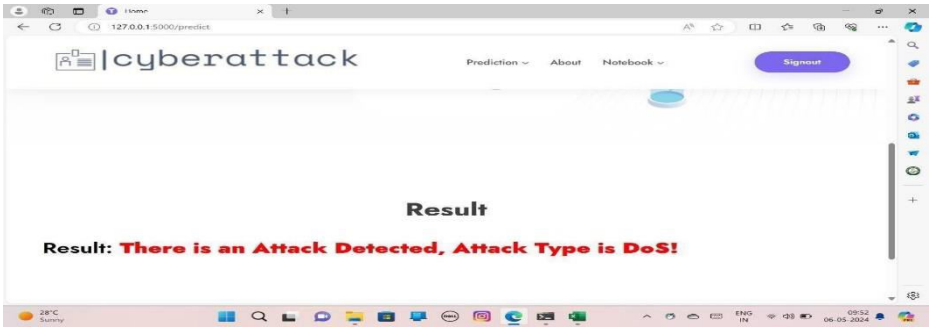

Figure 4: This page tells that the values entered for the prediction of attack are normal and there is no attack detected.

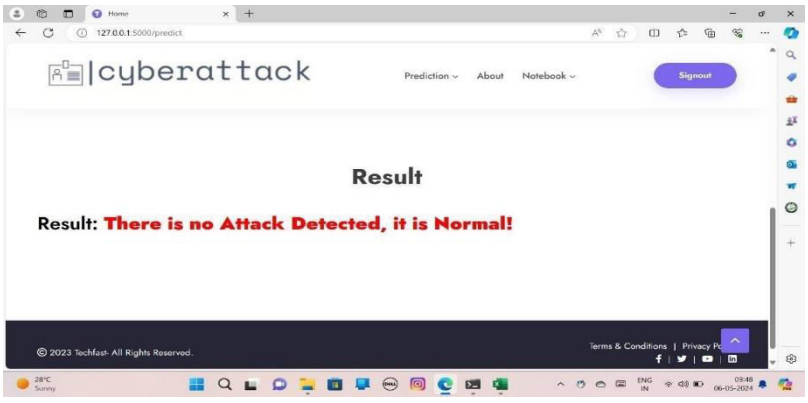

Figure 5: This page tells that the values entered are not normal and there is detection of attack. Network Intrusion Detection Systems (NIDS) are designed to continuously monitor a network for suspicious activity and raise an alarm when something potentially malicious is identified.

VI. CONCLUSION

With the widespread use of cloud computing by people and businesses, security in the cloud is of the utmost concern. Thus, the potential of machine learning models to classify incoming network packets as normal or abnormal was exploited to identify intrusions and preserve user data, and this was done at an acceptable resource cost that distinguishes machine learning models from deep learning models. The suggested intrusion detection system aims to develop a model that would leverage increased intrusion detection's accuracy by combining the strengths of each

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305432 |

employed feature selection algorithm (information gain, chi-square, and particle swarm optimization) to find an optimal feature subset that not only enhances the performance of the model but also offers useful features that are strongly associated with the target variable.

REFERENCES

1. R. R. Kumar, A. Tomar, M. Shameem, and M. N. Alam, ‘‘OPTCLOUD: An optimal cloud service selection framework using QoS correlation lens,’’ Comput. Intell. Neurosci., vol. 2022,
2. pp. 1–16, May 2022, doi: 10.1155/2022/2019485.
3. R. R. Kumar, M. Shameem, R. Khanam, and C. Kumar, ‘‘A hybrid evaluation framework for QoS based service selection and ranking in cloud environment,’’ in Proc. 15th IEEE India Council Int. Conf., Oct. 2018, pp. 1–6, doi: 10.1109/INDICON45594.2018.8987192.
4. M. Bakro, S. K. Bisoy, A. K. Patel, and M. A. Naal, ‘‘Performance analysis of cloud computing encryption algorithms,’’ in Advances in Intelligent Computing and Communication, in Lecture Notes in Networks and Systems, vol. 202. Singapore: Springer, 2021, pp. 357–367, doi: 10.1007/978-981-16-0695-3_35.
5. (2020). Malware Statistics & Trends Report | AV-TEST. Accessed: Jan. 21, 2023. [Online].
6. Digital Technology Market Research Services | Juniper Research. Accessed: Jan. 21, 2023.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details