International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 172-175, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE28
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

Analysis of Network Traffic Using Deep Learning

[1]V. Lakshmi Chaitanya, [2]K. Vyshnavi, [3]U. Deepika, [4]S. Sana Sameeren, [5]S. Misba Sania, [6]U. Jayanthi, [7]T. Shobha Rani

[1]Assistant Professor, Department of Computer Science & Engineering, Santhiram Engineering College, India
[2,3,4,5,6,7]Student, Department of Computer Science &Engineering, Santhiram Engineering College, India
E-mail: [1]chaitanya.cse@srecnandyal.edu.in

***Abstract* - Data protection, faster internet, and the detection of anomalous activity all depend on network traffic analysis. Large volumes of data cannot be processed using traditional ways as more gadgets connect to the internet.This study analyzes network traffic effectively using deep learning and big data. Deep learning models such as CNNS (Folding Networks) and RNN (Recursive Neural Networks) can help identify threats to identify traffic classification and abnormal patterns. Big data technologies such as Apache Spark and Hadoop process large amounts of data at lightning speeds. Together, these technologies can improve security, avoid cyberattacks, and accelerate and stabilize your network. This study explains how AI-based solutions can revolutionize network security. Issues, improvements and future developments in this area will also be resolved. The goal is to develop a more intelligent and secure network that protects data and improves internet performance.**

Keywords: Big Data, Deep Learning, Network Traffic, Apache Hadoop.

I. INTRODUCTION

In recent years, information technology has been implemented in each life area (health, agriculture, transportation, etc.), and several devices such as smartphones, computers, sensors, and other devices send data through the network, but the communication of cheese always includes safe and hidden attacks and built in. However, in order to detect invasions, the present security system and mechanism rely on specific regulations and programs. They cannot develop independently to recognize the appearance new threat. This project suggests some methods to detect the new threat. Furthermore, detection is made more difficult by the fact that the data was carried over a network and was incredibly big and variable. Due of the continuously growing amount of data produced globally, including weather, GPS signals, sound, and video Using information or social networks to regulate or save proved challenging. Because of the ever increasing volume of data generated worldwide, including sound, video, GPS signals, and weather. It was difficult to control or save using information or social networks. Common data management tools have led to new nomenclature. It was developed using the term "big data," which indicates a new method of storing information.

This significant occurrence is connected to deep learning. Information and secret knowledge can be extracted from this data. To solve the above problem, we propose a new approach to analyzing network traffic in this article. It was established to store large amounts of data using large data techniques to disclose new hidden attacks and intrusions and analyze this data according to deep learning methods.

II. RELATED WORK

This article covered the concepts of realtime network traffic analysis and anomaly recognition. The authors outlined the need for new tools to analyze large amounts of internet traffic to identify attacks. This process involves three phases: First, traffic is split into many segments to protect its structure using hashing techniques. Second, all data segments are subject to attack detection. And finally, the results will be made available to the network manager in the form of reports.

This study illustrates a new approach to using the Hadoop framework to monitor and analyze large amounts of network data. The authors point out that traditional transport analysis techniques can be easily used when manipulating large amounts of data. To record data, we recommend that the Hadoop Distributed File System (HDFS) is data using the Map Reduce program, a storage component of Hadoop, and presenting results via an interface and a multilayer transport analysis system. The effectiveness of the system was tested with the help of mobile communication traffic networks, and the results showed promising

The proposed solution is notable, but it lacks adaptation methods for detecting new hidden threats and does not address attack perception. A study referenced as introduced innovative techniques for monitoring security and analyzing network traffic. This architecture comprises two main components: one for storing network traffic data and another for analyzing the data using correlated algorithms to identify intrusions. While the system provides effective options for analyzing critical traffic data, the scalability of the correlation algorithm poses a limitation for identifying new threats.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 172-175, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE28
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

Modern techniques for assessing network data and intrusion recognition have been addressed in detail in another research study. This technology improves memory and analytical capabilities by using distributed models in cloud computing environments. However, the authors did not examine this concept through experiments, focusing primarily on recognizing known attacks instead of discovering new attacks.

The publication introduced a more current method for examining network data and detecting intrusions; it is predicated on a distributed concept in cloud computing. Intended to increase storage and analysis capabilities. The notion is confined to identifying existing attacks rather than novel, unidentified intrusions, and the authors did not demonstrate its efficacy through experimentation. The authors of the research discussed an alternative idea for tracking internet traffic using the Big Data management system Spark, and they acknowledged that the outdated traffic analysis methods have significantly

III. BACKGROUND

A. Big Data

Recently, quantitative explosions and various data have been causing problems with outdated data management tools. This forced researchers to find new ways to manage them. The new concept is that it is big data and is defined by the characteristics (5v). The three main issues are data volume, diversity, bicycles and bicycles. The two secondary ones are: The authenticity related to the reliability and reliability of the collected information defines values from the use of big data

B. Deep Learning

New approaches, particularly deep learning, were created in response to the difficulties of big data, with the aim of placing insightful information from this vast amount of data. Deep learning uses a number of learning algorithms in deep learning to recognize objects, perform predictive reviews, and extract information. Stacked auto coder (SAE), deep face network (DBN), foigation network (CNN), and repeating neuronal network (RNN) are the most popular algorithms within the recently popular deep learning framework. These basic models are usually the basis of other existing algorithms. The inlet layer, hidden layer and output layer are usually the three layers that make up the architecture of deep learning techniques.

IV. PROPOSED SYSTEM

A. Components

1. Traffic collection machine

The machine is fitted with an operating system that is intended to capture network traffic. TCPDUMP dynamically manages, captures and saves traffic packets passing through routers for future analysis.

2. Router

This part of the network equipment facilitates data transfer between the Internet and the local network.

3. Big data management system

Considering the substantial amount of data exchanged between machines on the Internet, it is necessary to provide the creation of a system management system and later analyze it on the local network and the Internet. Under the extensive options using open source, we decided to have Hadoop and Spark. This system consists of two common components for data storage, with the other systems being used for analysis and processing of processed data. Spark was compared to Hadoop, a machine learning application, and was chosen as a solution for managing large data at great speeds, and compared with the integrated Mllib library to simplify the implementation of analytical algorithms.

B. Treatment

1. Traffic Survey: This initial phase involves collecting network traffic using the TCPDUMP tool, and collecting all data related to incoming and outgoing network traffic. Recorded traffic is stored on the same computer that TCPDUMP works, allowing for subsequent shops to the big data management system.

2. Traffic Memory: In this step, data collected by traffic monitoring Therefore, we strive to plan the integration of this newly collected data traffic into a big data management system. After completing the load process, traffic data from the collector is deleted and storage capacity is optimized.

3. Transportation analysis: In this phase, it is important that the traffic data perform training on the dataset before implementing deep learning algorithms to assess existing attacks. After training, these algorithms are applied to stored traffic data to determine and identify potential new attacks and intrusion attempts.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 172-175, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE28
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

V. CONCLUSION

To identify the problem, this study suggested a new solution to analyze significant amounts of network traffic. The main idea is to collect storage using large data methods and analyze using deep learning algorithms. In the future, we plan to integrate approaches such as security devices and evaluate how well it works in real time.

REFERENCES

[1] R. Fontugne, J. Mazel, K. Fukuda, "Hashdoop: A MapReduce Framework for Network Anomaly Detection", in 2014 IEEE INFOCOM Workshops: 2014 IEEE INFOCOM Workshop on Security and Privacy in Big Data, Japan, pp. 494-499, 2014.

[2] Mohd R. G., Durgaprasad G., "Hadoop, MapReduce and HDFS: A Developers Perspective", in International Conference on Intelligent Computing, Communication & Convergence ((ICCC-2014), India, pp.45-50, 2015.

[3] Jun L., Feng L., Nirwan A., "Monitoring and Analyzing Big Traffic Data of a Large-Scale Cellular Network with Hadoop", IEEE Network, Japan, vol. 28, Iss. 4, pp. 32-39, 2014.

[4] Mahammad, Farooq Sunar, et al. "Key distribution scheme for preventing key reinstallation attack in wireless networks." AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024.

[5] Suman, Jami Venkata, et al. "Leveraging natural language processing in conversational AI agents to improve healthcare security." Conversational Artificial Intelligence (2024): 699-711.

[6] Sunar, Mahammad Farooq, and V. Madhu Viswanatham. "A fast approach to encrypt and decrypt of video streams for secure channel transmission." World Review of Science, Technology and Sustainable Development 14.1 (2018): 11-28.

[7] Mahammad, Farooq Sunar, Karthik Balasubramanian, and T. Sudhakar Babu. "A comprehensive research on video imaging techniques." All Open Access, Bronze (2019).

[8] Mahammad, Farooq Sunar, and V. Madhu Viswanatham. "Performance analysis of data compression algorithms for heterogeneous architecture through parallel approach." The Journal of Supercomputing 76.4 (2020): 2275-2288.

[9] Devi, M. Sharmila, et al. "Extracting and Analyzing Features in Natural Language Processing for Deep Learning with English Language." Journal of Research Publication and Reviews 4.4 (2023): 497-502.

[10] Devi, M. Sharmila, et al. "Machine Learning Based Classification and Clustering Analysis of Efficiency of Exercise Against Covid-19 Infection." Journal of Algebraic Statistics 13.3 (2022): 112-117.

[11] Mandalapu, Sharmila Devi, et al. "Rainfall prediction using machine learning." AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024.

[12] Chaitanya, V. Lakshmi, et al. "Identification of traffic sign boards and voice assistance system for driving." AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024.

[13] Chaitanya, V. Lakshmi. "Machine Learning Based Predictive Model for Data Fusion Based Intruder Alert System." journal of algebraic statistics 13.2 (2022): 2477-2483.

[14] Chaitanya, V. Lakshmi, and G. Vijaya Bhaskar. "Apriori vs Genetic algorithms for Identifying Frequent Item Sets." International journal of Innovative Research &Development 3.6 (2014): 249-254.

[15] Parumanchala Bhaskar, et al. "Incorporating Deep Learning Techniques to Estimate the Damage of Cars During the Accidents" AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024.

[16] Parumanchala Bhaskar, et al "Cloud Computing Network in Remote Sensing-Based Climate Detection Using Machine Learning Algorithms" remote sensing in earth systems sciences (springer).

[17] Parumanchala Bhaskar, et al. "Machine Learning Based Predictive Model for Closed Loop Air Filtering System." Journal of Algebraic Statistics 13.3 (2022): 416-423.

[18] Paradesi Subba Rao,"Detecting malicious Twitter bots using machine learning" AIP Conf. Proc. 3028, 020073 (2024),https://doi.org/10.1063/5.0212693.

[19] Paradesi Subba Rao, "Morphed Image Detection using Structural Similarity Index Measure"M6 Volume 48 Issue 4 (December 2024), https://powertechjournal.com

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 172-175, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE28
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

Citation of this Article:

V. Lakshmi Chaitanya, K. Vyshnavi, U. Deepika, S. Sana Sameeren, S. Misba Sania, U. Jayanthi, & T. Shobha Rani. (2025). Analysis of Network Traffic Using Deep Learning. In proceeding of International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25), published by *IRJIET*, Volume 9, Special Issue of INSPIRE'25, pp 172-175. Article DOI https://doi.org/10.47001/IRJIET/2025.INSPIRE28

****

