UNCOVERING BOTTLENECKS IN INTERNET OF THINGS (IoT): A HYBRID DEEP LEARNING APPROACH

Emani Soumya
Scholar,DepartmentofMCA
Vaageswari College of Engineering- Karimnagar

Dr.V.Bapuji
Professor & Head, Department of MCA
Vaageswari College of Engineering, Karimnagar

ABSTRACT- Using cloud-fog hybrid computation is the fundamental driver of the Internet of Things' rapid growth. However, it is vital to keep in mind that this expansion introduces major information security risks. Despite having a lower latency, the fog node should have a more lightweight intrusion detection mechanism. This research study provides a novel low-weight intrusion detection model that uses ConvNeXt-Sf to address the aforementioned difficulties. ConvNeXt, the current computer vision model, begins with a two-dimensional structure and then moves to a one-dimensional series. ConvNeXt is then built using the design ideas of the lightweight computer vision model ShuffieNet V2, resulting in a lighter total weight. In the data preparation model, the max-min normalization and label encoder work together to convert network data into a format that ConvNeXt can understand. The TON-IoT and BoT-IoT datasets are used to evaluate the proposed model. ConvNeXt-Sf is just 1.25 times larger than its predecessor, ConvNeXt. When compared to the ConvNeXt, the ConvNeXt-Sf cuts training and prediction times by 82.63 and 56.48 percent, respectively. Furthermore, its learning and recognition abilities are unaltered. When compared to established approaches, the proposed strategy lowers the False Acceptance Rate (FAR) by 4.49 percent while increasing accuracy by 6.18 percent. In terms of decreasing ConvNeXt's weight, ShuffieNet V2 exceeds other lightweight versions.

Index Terms: **Blockchain, Secure Data Sharing, Technology Acceptance Model, Technology Readiness Index.**

I. INTRODUCTION

When combined with hybrid cloud fog computing, the Internet of Things can help with a wide range of jobs that demand significant computing power and the ability to process large amounts of data.

As a result, it serves as a reliable and adaptive Computer system. The Internet of Things (IoT) is increasingly being used in a variety of areas, including transportation, healthcare, and industry.

It is critical in this age of the "Internet of Everything", in which devices are interconnected.

Cloud computing is helpful because it provides Internet of Things (IoT) applications with access to a variety of resources.

The Internet of Things' success can be due to its extensive network, metered service, rapid adaption, and self-service on demand. However, worries remain about the connectivity, speed, security, dependability, and efficiency of the internet link that connects cloud nodes and peripheral devices. Because of the frequency of these challenges, more people are becoming interested in fog computing. Figure 1 depicts the significance of the network connection between cloud nodes and end devices in fog computing.

The Internet of Things is created by combining cloud computing and vapor computing. Fog nodes allow resources to reach the network's edge. This allows IoT applications to access resources in a safe, reliable, and low-latency manner. Fog computing is the most effective way to develop secure and efficient Internet of Things services.

To improve network performance, continue to delegate resource-intensive processes to the cloud for execution. In a variety of fields, hybrid cloud-fog computing is enabling the Internet of Things (IoT). This area includes smart cities, health, farms, industries, and structures.

Breach-of-security vulnerabilities and the growing prevalence of network-based threats make IoT devices vulnerable to intrusion. Developing cutting-edge intrusion detection systems (IDS) for the Internet of Things (IoT) through the integration of cloud and fog architectures is an important area of cyber security research and development. Intrusion detection systems (IDS) have been used to secure networks since at least 1980.

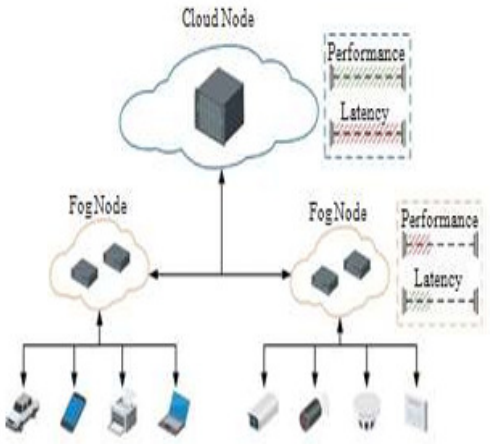

Figure 1: IoT with hybrid cloud-fog computing

Real-time examination of the intrusion detection system's (IDS) data alerts the network security team to potential threats.

The source of the information distinguishes between host-based and network-based intrusion detection systems. After configuration, a host-based intrusion detection system (HIDS) monitors the compromised host's activities during an intrusion. An intrusion detection system (IDS) is installed in important network areas to monitor and report on network data that may indicate a possible assault. An obvious example is the categorization of intrusion detection systems (IDS) into two types: signature-based and anomaly-detecting.

The breach detection system uses a signature-based technique to identify prospective assaults by comparing the data it receives to attack patterns stored in a database. While the system excels at identifying common assault types, it struggles to identify unique or unconventional attack techniques.

An anomaly-based intrusion detection system (IDS) recognizes patterns that could indicate malicious intent by comparing gathered data to standard data and identifying disparities.Despite a large number of false alarms, the system is still capable of recognizing and classifying new threats. Deep learning is a unique subset of machine learning. The deep learning model can gather the essential data without requiring huge, complex samples. Several cutting-edge deep learning models have been built in the fields of computer vision (CV) and natural language processing (NLP), achieving astonishing accomplishments. Scientists have extensively used computer vision (CV) and natural language processing (NLP) to detect Internet of Things (IoT) attacks.

To maintain the security of the Internet of Things (IoT), we advocate creating an Intrusion Detection System (IDS) built on the existing ConvNeXt framework and combining cloud and fog computing. The Intrusion Detection System (IDS) will be deployed on fog computers, which have limited computational capabilities. Our goal is to improve ConvNeXt's efficiency by integrating architectural approaches used in the construction of the efficient computer vision model ShuffieNet V2, while taking into account fog nodes' restricted processing capabilities.

The following information highlight the key contributions made in the paper. ConvNeXt is a cutting-edge application that performs vulnerability assessments on the Internet of Things using cloud and fog computing. Many computer vision (CV) professionals see ConvNeXt as a model for the approaching era. As a result, the primary deep learning models' utility has grown dramatically when applied to tasks like object recognition and image categorization.

In order to reduce ConvNeXt's effort, the model under consideration is the first to take advantage of ShuffieNet V2 design limits. Because of its small size and light weight, the ShuffieNet V2 is suitable for applications that require deep neural networks. Changing the components of this system allows the creation of numerous types of lightweight and fast deep neural networks.

The use of low-latency fog nodes may aid in the implementation of the suggested model in fog nodes with limited resources. When fog and cloud systems work together, the Internet of Things can be made safer.

II. REVIEW OF LITERATURE

X. Zhang, Y. Yuan, Z. Zhou, S. Li, L. Qi, and D. Puthal, "Intrusion detection and prevention in cloud, fog, and the Internet of Things," 2019. This article looks at cutting-edge approaches for detecting and preventing intrusions in the cloud, fog, and Internet of Things. The authors discuss the specific security concerns that these environments raise and propose a system that incorporates multiple approaches of detection and prevention.

The proposed solution aims to increase security by leveraging the distributed nature of fog computing and the pervasive connectivity of IoT devices.
"Using cloud computing to address challenges raised by the internet of things," Micrea, Micrea; Ghilic-Micu, B. (2017). This chapter investigates the potential uses of cloud computing to overcome the inherent issues presented by the Internet of Things (IoT). It provides a complete analysis of IoT requirements and cloud computing's ability to meet them. The authors' primary concerns are scalability, data management, and security, and they use case studies and real-world examples to demonstrate the benefits of merging cloud and IoT technology.

C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos (2018): "A comprehensive survey on fog computing: state-of-the-art and research challenges." This overview essay provides an in-depth look at the current state of fog computing and its potential applications. It examines fog computing's capabilities, benefits, and architecture in comparison to cloud computing. The authors identify the major research concerns, such as resource management, security, privacy, and interoperability, and provide practical solutions as well as recommendations for future research.

R. Pérez De Prado et al. released their paper "Smart Container Schedulers for Micro Services Provision in Cloud-Fog-IoT Networks: Challenges and Opportunities" in 2020. This study looks at how smart container schedulers are used to deploy microservices in cloud-fog-IoT networks. It highlights the challenges and opportunities associated with managing microservices in such scattered environments. The authors propose a method for scheduling smart containers in order to optimize resource utilization, improve performance, and ensure constant service delivery.

S. Prabavathy, K. Sundarakantham, and S. M. Shalinie published a paper in 2018 titled "Design of cognitive fog computing for intrusion detection in the Internet of Things". This paper offers an architecture for cognitive fog computing that aims to improve intrusion detection in Internet of Things environments. The recommended system employs real-time cognitive computing-based anomaly analysis and detection methods. By exceeding previous methods in terms of detection accuracy and reaction time, the authors demonstrate that their methodology is appropriate for resource-constrained and dynamic IoT applications.

J. P. Anderson (1980). "Computer security threat monitoring and surveillance." This key study lays the groundwork for modern intrusion detection systems by outlining the fundamental concepts of computer security threat monitoring and surveillance. Anderson introduces the concept of intrusion detection as a method for identifying and addressing security concerns in computer systems. The article discusses ways for detecting and mitigating different types of intrusions.

Heberlein, Dias, and Levitt devised a network security monitor in 1990. This article describes how to set up and install a network security monitor in order to detect

and remedy security problems in computer networks. The authors describe in detail the design and functioning of their monitoring system, emphasizing its ability to evaluate network traffic, detect suspicious activities, and alert administrators to potential threats.

W. Jo, S. Kim, C. Lee, and T. Shon. "Packet preprocessing in CNN-based network intrusion detection system," 2020. This study, which focuses on packet preprocessing techniques, investigates the application of convolutional neural networks (CNNs) in network intrusion detection systems. The authors' preprocessing strategy successfully controls network traffic data, resulting in improved CNN performance. Testing results reveal that the suggested strategy significantly improves the accuracy and speed of intrusion detection.

F. Hussain, S. G. Abbas, and M. Husnain published a paper in 2020 on the use of ResNet to detect IoT DoS and DDoS attacks. In this study, we employ ResNet, a deep residual network, to detect Denial of Service (DoS) and Distributed Denial of Service (DDoS) assaults in Internet of Things networks. The authors demonstrate how ResNet can successfully distinguish between benign and malicious traffic patterns, providing a robust defense against these types of attacks on IoT network security.

B. Zhong, Y. Zhou, and G. Chen's "Sequential model-based intrusion detection system for IoT servers using deep learning methods," released in 2021. This work proposes a sequential model intrusion detection system for Internet of Things servers based on deep learning. The authors use recurrent neural networks (RNNs) and long short-term memory (LSTM) to evaluate sequential data and detect anomalies. Because of its low false positive rate and high detection rate, the proposed method is suitable for real-time intrusion detection in Internet of Things systems.

III. PROPOSED METHOD

This paper proposes a novel approach for detecting malicious actions in an Internet of Things (IoT) environment using the ConvNeXt-Sf intrusion detection system. The suggested approach mixes cloud and fog computing to improve operational efficiency. Without classifying network data, it is impossible to uncover vulnerabilities in the Internet of Things (IoT) utilizing a hybrid cloud-fog computing strategy. The fog node's intrusion detection model may study network data in real time as it moves from cloud nodes, detecting and reporting any security violations or threats. Figure 2 depicts the intrusion detection method in two stages: data preparation and classification.

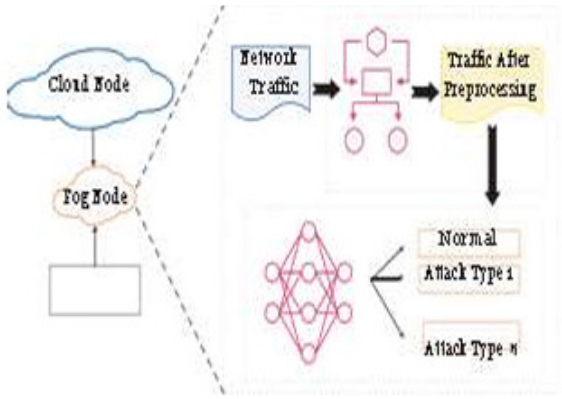

Fig 2: Intrusion detection of IoT with hybrid cloud-fog computing

(1). The first stage of data preprocessing entails changing raw network data into a recognizable shape for the classification model. This work explains the LE-MMN model.
It combines label encoder and max-min normalization techniques to prepare data. This approach quantifies and standardizes raw network flow data.

(2) After cleaning and organizing the data, the classification model may begin the task of categorizing network traffic. The multi classification model's data breakdown depicts a wide range of commonly used assault kinds. Implementing an intrusion detection model on a fog node should result in a compact system that correctly identifies intrusions. The ConvNeXt-Sf classification model was created by minimally altering a single dimension while conforming to the ShuffieNet V2. It was based on the ConvNeXt architecture.

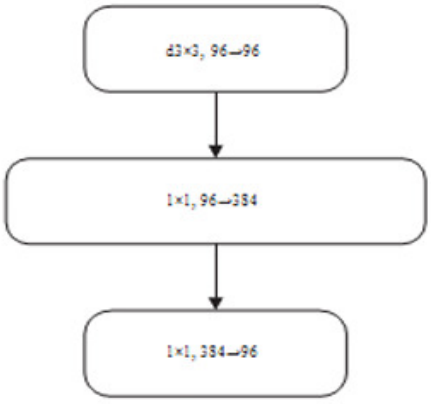

Figure 3: Inverted bottleneck structure in ConvNeXt.

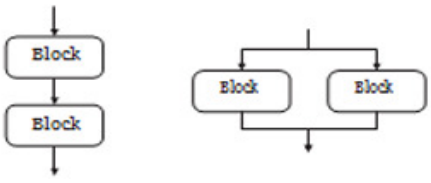

Figure 4 Fragmented Network

This study uses the TON-IoT and BoT IoT datasets to assess the proposed Internet of Things (IoT) paradigm using a hybrid cloud and fog computing architecture.

To demonstrate the growing prevalence of hybrid cloud-fog computing in the Internet of Things (IoT), the TON-IoT and BoT-IoT datasets were used. It is important to remember that the BoT-IoT and TON-IoT collections cover a wide range of IoT functions. This version includes a more comprehensive evaluation of the model's performance across a variety of Internet of Things (IoT) functions.

IV. RESULTS AND ANALYSIS

Figure: 4 Login Page

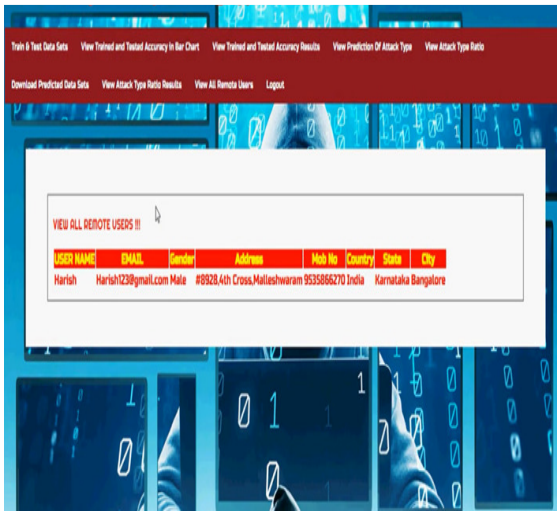

Figure: 5 View all remote users

Figure: 6 Prediction of attack detection types

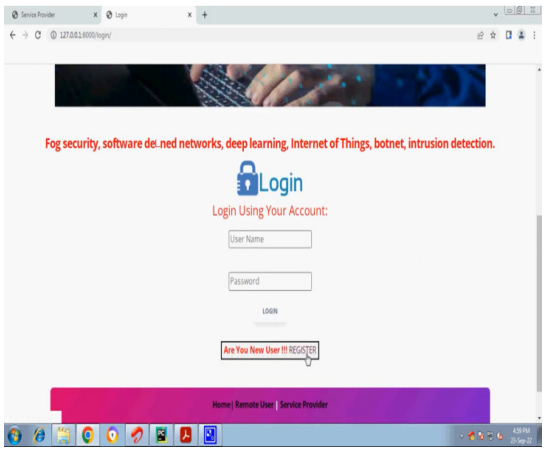

Figure: 7 login using your account

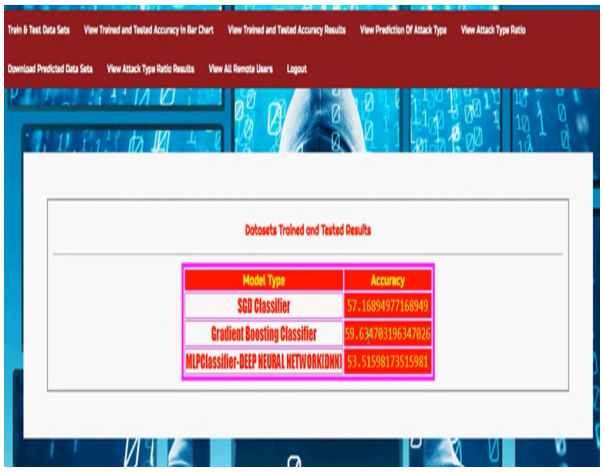

Figure: 8 Datasets trained and tested results

Figure: 9 Bar Chart Results

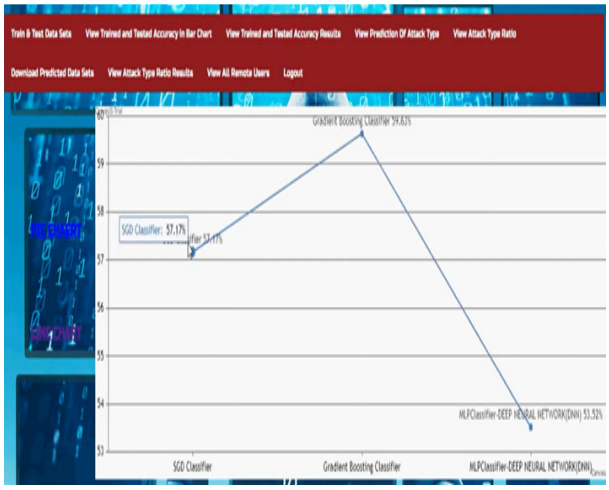

Figure: 10 Line Chart Analysis of Algorithms

Figure: 11 Pie Chart Analysis of Algorithms

V. CONCLUSION

This work investigates the problem of intrusion detection in the Internet of Things using ConvNeXt, a novel and efficient computer vision model. The study recommends altering intrusion detection systems (IDS) in fog nodes to make Internet of Things (IoT) devices marginally more safe. The ConvNeXt model was designed primarily to work with uni dimensional network data. The ConvNeXt-Sf classification model is constructed by combining the specifications of the lightweight computer vision model ShuffieNet V2 with the ConvNeXt architecture.

The combination of the ConvNeXt-Sf classification model and the LE-MMN data preprocessing model has the potential to produce a powerful model for identifying IoT attacks. Tests with the TON-IoT and BoT-IoT datasets show that ConvNeXt-Sf improves recognition accuracy while using less processing resources than ConvNeXt. In compared to ConvNeXt-Dense Net and ConvNeXt-Ghost Net, the suggested model outperforms them in terms of accuracy and false acceptance rate. Furthermore, it provides benefits such as faster training and prediction processes and less parameter needs. Using unsupervised or semi supervised learning approaches, additional effort will be put into enhancing the proposed strategy.

The majority of network data in an Internet of Things (IoT) or hybrid cloud data system does not include the names of individual users. Although time-consuming and resource-intensive, data labeling is an essential component of supervised learning. Implementing unsupervised or semi-supervised learning requires significantly less effort. Unsupervised learning has been extensively used in natural language processing (NLP), making it a viable option for IoT intrusion detection. This application makes it easier for specialists from different fields to collaborate and communicate.

REFERENCES

1. X. Zhang, Y. Yuan, Z. Zhou, S. Li, L. Qi, and D. Puthal, “Intrusion detection and prevention in cloud, fog, and internet of things,” Security and Communication Networks, vol. 2019, Article ID 4529757, 4 pages, 2019.
2. M. Micrea, M. Stoica, and B. Ghilic-Micu, “Using cloud computing to address challenges raised by the internet of things,” in Connected Environments for the Internet of Things, pp. 63 82, Springer, Switzerland, 2017.
3. C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, “A comprehensive survey on fog computing: state-of the-art and research challenges,” IEEE Communications Surveys and Tutorials, vol. 20, no. 1, pp. 416–464, 2018.

4. R. P´erez De Prado, S. Garc´ıa-Gala´n, J. E. Muñoz-Expo´sito, A. Marchewka, and N. Ruiz-Reyes, “Smart containers schedulers for microservices provision in cloud-fog-IoT networks. challenges and opportunities,” Sensors, vol. 20, no. 6, pp. 1714 1721, 2020.
5. S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, “Design of cognitive fog computing for intrusion detection in Internet of Things,” Journal of Communications and Net- works, vol. 20, no. 3, pp. 291–298, 2018.
6. J. P. Anderson, “Computer security threat monitoring and surveillance,” Technical Report, pp. 1–53, James P Anderson Company, kansas, KS, USA, 1980.
7. Levitt, L. T. Heberlein, G. V. Dias, and K. N. “A network security monitor,” in Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy, pp. 296–304, IEEE, Oakland, CA, USA, May 1989.
8. W. Jo, S. Kim, C. Lee, and T. Shon, “Packet preprocessing in CNN-based network intrusion detection system,” Electronics, vol. 9, no. 7, pp. 1151–1215, 2020.
9. Dr.V.Bapuji, Boddupalli Anvesh Kumar, “Efficient Privacy Preserving Communication Protocol For IOT Applications”,Brazilianjournal at Development, Volume10,Issue 1, Page 402-419,2024. .https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/download/66113/47175https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/download/66113/47175
10. F. Hussain, S. G. Abbas, and M. Husnain, “IoT DoS and DDoS attack detection using ResNet,” in Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC), pp. 1–6, IEEE, Bahawalpur, Pakistan, November 2020.
11. M. Zhong, Y. Zhou, and G. Chen, “Sequential model based intrusion detection system for IoTservers using deep learning methods,” Sensors, vol. 21, no. 4, pp. 1113–1121, 2021