# IDENTIFYING BOTTLENECKS IN THE INTERNET OF THINGS USING HYBRID DEEP LEARNING APPROACH

**[#1]YELUKA PRIYANKA, Dept of *MCA*,**

**[#2]P.SATHISH , Assistant Professor,**

**[#3]Dr.V.BAPUJI, Associate Professor& HOD,**

**Department of Master of Computer Application,**

**VAAGESWARI COLLEGE OF ENGINEERING, KARIMANGAR, TELANAGANA.**

**Abstract—** While cloud-fog hybrid computing is accelerating the growth of the Internet of Things, it offers major information security risks. The intrusion detection system on the fog node has a reduced latency but should be lighter. In response to the aforementioned issues, this work proposes a ConvNeXt-Sf-based lightweight intrusion detection model. First, the existing computer vision model ConvNeXt's two-dimensional structure is reduced to a one-dimensional sequence. The design requirements of the lightweight computer vision model ShuffieNet V2 are then used to develop ConvNeXt in order to make it lighter. Finally, the data preprocessing model incorporates the max-min normalization and label encoder to convert network traffic into a format compatible with ConvNeXt learning. The proposed model is tested using the TON-IoT and BoT-IoT datasets. ConvNeXt-Sf's parameters are just 1.25% of those of ConvNeXt. When compared to the ConvNeXt, the ConvNeXt-Sf reduces training and prediction times by 82.63% and 56.48%, respectively, without sacrificing learning or detection capacity. When compared to established approaches, the proposed methodology improves accuracy by 6.18% while decreasing FAR by 4.49%. The ShuffieNet V2 outperforms other lightweight variants in terms of making ConvNeXt lightweight.

**Index Terms—**blockchain, secure data sharing, Technology Acceptance Model, Technology Readiness Index.

## I. INTRODUCTION

Many tasks that necessitate extensive data processing and computing capacity can benefit from the IoT when combined with hybrid cloud-fog computing. As a result, it is a powerful and scalable computing architecture [1]. The manufacturing, medical, and transportation sectors are just a few examples of growing adoption of the Internet of Things (IoT). It is now indispensable in the age of interconnected "Internet of Everything" gadgets. Cloud computing's abundance of resources is a boon to Internet of Things (IoT) applications. Self-service on demand, a vast network, metered service, and rapid adaptability are all elements that contribute to the success of the Internet of Things [2]. On the other hand, there are a few problems with the Internet connection between cloud nodes and edge devices [3, 4] that can affect performance, security, latency, and stability. As a result of these issues, interest in fog computing is growing. As can be seen in Figure 1, the network connection between cloud nodes and end devices is an integral part of fog computing. This fusion produces the Internet of Things (IoT) by way of a cloud-fog computing hybrid architecture. Because of fog nodes, resources can be brought to the network's periphery. Because of this, IoT programs can more easily get resources in a safe, dependable, and low-latency fashion. If you want reliable and secure IoT services, fog computing is the way to go [4]. Continue uploading resource-intensive jobs to the cloud to be completed so as to improve network performance. Smart cars, smart buildings, smart utilities, smart cities, smart health, smart farms, and smart industries are just a few examples of how hybrid cloud-fog computing is being leveraged to make the Internet of Things (IoT) a reality [5].

Because of security holes and the improvement of network-based attacks, Internet of Things (IoT) gadgets are vulnerable to cyberattacks [6]. As a

result, developing next-generation intrusion detection systems (IDS) for IoT using a hybrid cloud-fog architecture is a critical area of research and development in the field of cyber security. Intrusion detection systems (IDS) have been used to safeguard networks since at least 1980 [7, 8].

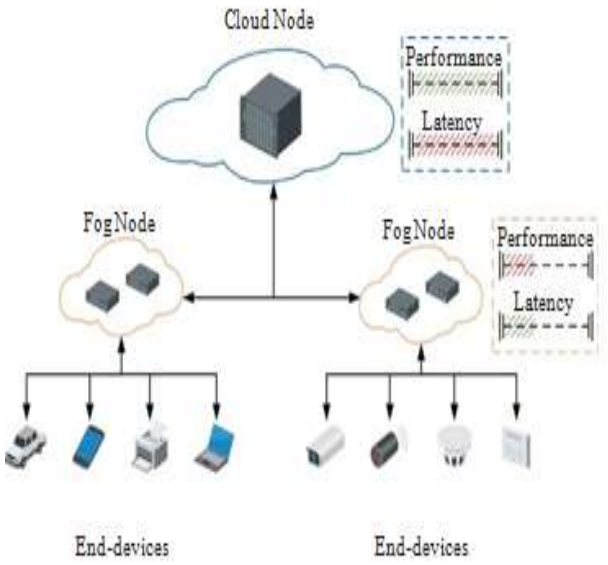


Figure 1: IoT with hybrid cloud-fog computing

The network's security team can be alerted to potential intrusions in real time thanks to the intrusion detection system's (IDS) ability to analyze collected data in real time.

Based on the origin of its information, intrusion detection systems (IDS) can be classified as either host-based or network-based. A host-based intrusion detection system (HIDS) monitors the host's behavior during an assault after it has been installed on the host. The purpose of a network-based intrusion detection system (IDS) is to monitor and identify hostile behaviors in network traffic, and it is typically installed on critical network nodes. Based on their methods for detecting intrusions, Intrusion Detection Systems (IDS) can be roughly divided into two categories: those that look for signatures and those that check for anomalies. The signature-based detection mechanism employed by the breach detection system compares the data it has collected to details in an attack database to identify potential attacks. While the algorithm excels at locating common types of attacks, it struggles when presented with novel or unseen ones. The collected data is compared to baseline data in order to identify outliers that may indicate malicious activity using an anomaly-based intrusion detection system (IDS). The system has a high rate of false warnings (FAR), yet it successfully detects and identifies novel dangers.

Deep learning is a subset of machine learning. Large-scale, high-dimensional datasets are not required for the deep learning model to extract relevant information. Numerous cutting-edge deep learning models have been developed, and they've had a lot of success in computer vision (CV) and natural language processing (NLP). Computer vision (CV) and natural language processing (NLP) have been heavily utilized by researchers in their pursuit of IoT intrusion detection.

We believe that a hybrid cloud-fog computing approach with an Intrusion Detection System (IDS) based on the existing ConvNeXt paradigm is the best solution to safeguard the security of the Internet of Things (IoT). This IDS will be installed on fog servers with restricted processing capabilities. Due to the restricted computing power of fog nodes, we want to boost ConvNeXt's performance by adopting some of the same architectural principles used in the creation of the lightweight computer vision model ShuffieNet V2. The paper's significant contributions are demonstrated via the following:

With ConvNeXt, hybrid cloud-fog computing is employed for the first time to detect vulnerabilities in the Internet of Things. ConvNeXt is widely regarded as a state-of-the-art model in the field of computer vision (CV). Main deep learning models' effectiveness in tasks like target detection and image categorization have been significantly boosted as a result.

The model under consideration is the first to make use of the ShuffieNet V2 design constraints to reduce the computational burden on ConvNeXt. The ShuffieNet V2 is a lightweight CV model, making it suitable for apps that require deep neural networks. Its concepts for design can be adapted to the creation of various efficient lightweight deep neural networks.

Implementing the proposed model in resource-constrained fog nodes may be facilitated by using low-latency fog nodes. This can improve IoT security through a combination of cloud and fog computing.

## II. RELATED WORK

In terms of learning, deep learning models excel at handling complex data. As a result, they have been widely adopted for usage in CV, NLP, and other areas, where they have proven to be highly effective. As a result, many professionals in the field of network security employ deep learning models to enhance the performance of Intrusion Detection Systems (IDS).

Changing the format of network data is one solution for dealing with the problem that CVs and NLP objects have a different format than network traffic. A feature from the NSL-KDD dataset was converted into a pixel form for use in the study by Jo et al. (2019). This modification reduced a single record to a flat image. Keeping these considerations in mind, the study team devised three methods for transforming the NSL-KDD dataset into 28-by-28-pixel images. The images were then classified using Convolutional Neural Networks (CNNs). Convolutional neural networks (CNNs) have been shown to be capable of simultaneously processing data from several different protocols. When compared to deep learning models such as autoencoders and recurrent neural networks, they have this distinguishing feature. In their study, Hussain et al. Then, 63 pictures were made using information from both everyday traffic and violent incidents. Each image was constructed from a total of 60,000 individual samples. The reduced resolution of 224x224x3 pixels allowed the ResNet18 model to be fed the image. Denial of service (DoS) and distributed DoS (DDoS) attacks on IoT devices can be detected with this paradigm. Word2Vec is a technique developed in the field of Natural Language Processing (NLP) that was applied by Zhong et al. (2011) to convert network traffic data into word vectors. The word vectors were then organized using sequence models like test-CNN and gate recurrent unit (GRU). To characterize the features of frames broadcast by a specific IP address over a specific time period, Kozik et al. [12] inserted 37 values they had found into a probabilistic data structure. The encoder portion of the transformer model was combined with a feed-forward neural network to create a classifier for intrusion identification. The above procedure is effective at identifying transient malicious network activity. It is not anticipated that this technique will improve the model's performance. However, if the data structure is altered, the information transmitted via network flow may shift, which may affect the model's ability to acquire knowledge. Also, during the data preparation phase, when there is a lot of traffic on the network, fog node devices with restricted capabilities cannot disregard the additional resources this strategy requires.

Altering the model's structure to support network activity is another option. Hassan et al. (2013) developed a convolutional neural network (CNN) and a weighted long short-term memory (WDLSTM) model for application in an intrusion detection system (IDS). The enormous network traffic dataset was simplified by employing a one-dimensional convolutional neural network (CNN) with deep architectures and a weight-sharing approach. Using a probabilistic dropout process in neurons in conjunction with Long-Term Short-Term Memory (LSTM) proved to be an effective method for preventing overfitting. In their research, Derhab et al. [14] utilized a temporal convolutional neural network (TCNN) to develop an IDS for the IoT. This strategy employs a single-layer convolutional neural network and the technique of cause convolution. Experiments with BoT-IoT datasets indicated that the TCNN outperformed the CNN in terms of detection accuracy, but both models required roughly the same amount of time to train. Although this approach does not necessitate the deployment of additional assets, it is critical to ensure that modifying the model's structure does not negatively impact performance and that it remains within acceptable bounds.

The models used to control network traffic can be implemented immediately. In 2015, Almiani et al. developed a fog-based intrusion detection system (IDS). A recurrent neural network (RNN) with multiple layers was employed, and it was trained using a modified version of the back-propagation technique. A two-tiered Recurrent Neural Network (RNN) was set up sequentially to handle difficult-to-detect attacks like Denial of Service

(DoS). Using the long-short term memory mechanism, Xu et al. (16) successfully transplanted new neurons into the anterior cingulate. The created IoT IDS utilizes Long Short-Term Memory (LSTM) to store time series features and an Autoencoder (AE) to learn these features in order to detect intrusions. Since the current scenario lacks the drawbacks of the previous two choices, it is preferable. When it comes to computer vision (CV), the myth that models from other domains may be simply integrated to breach detection must be dispelled. This is mostly due to the fact that CV models do not interpret their input as consisting of a single variable.

In order for the Internet of Things (IoT) to take use of hybrid cloud-fog computing, Kumar and his colleagues (2017) deployed the proposed TP2SF on cloud nodes and fog nodes. At initially, it was the fog nodes' job to finalize financial deals. Transactions that the fog node is unable to process are routed to the cloud node. A trustworthiness module, a privacy module with two tiers, and an intrusion detection module made comprised the TP2SF. The module for spotting irregularities employed an algorithm called XGBoost. Kumar et al. (2018) developed the Sp2f framework, which features a two-tier privacy engine and a deep learning-based anomaly detection engine. In the two-level secrecy engine, the Sp2f was deployed to fog nodes, but blockchain data was solely stored in the cloud. This method of task distribution aids fog nodes in making do with limited means. The secondary privacy engine submitted its data to the anomaly detection engine, which examined the information for possible indicators of infiltration using a stacked LSTM model. Both the fog layer and the cloud layer's security measures are examined in the two articles that came before this one. The same intrusion detection system (IDS) is used by all nodes across both tiers. Although the cloud layer and the fog layer both have useful effects, they are distinct in many respects. Good performance in all areas may be challenging for a single Intrusion Detection System (IDS).

Therefore, it is preferable to devise a method of constructing an Intrusion Detection System (IDS) that accommodates the unique qualities of each layer. The likelihood of security risks to another layer is reduced when the IDS of the lower layer is effective.

## III. PROPOSED METHOD

This research paper presents a novel intrusion detection model that makes use of ConvNeXt-Sf to identify malicious activity in an IoT setting. The proposed model incorporates cloud and fog computing for improved performance. IoT breach detection using hybrid cloud-fog computing relies on properly categorizing network data. When network data travels from cloud nodes to the fog node, the fog node's intrusion detection model can analyze it for threats. As can be seen in Figure 2, there are two distinct phases to the intrusion detection model: data pretreatment and sorting.

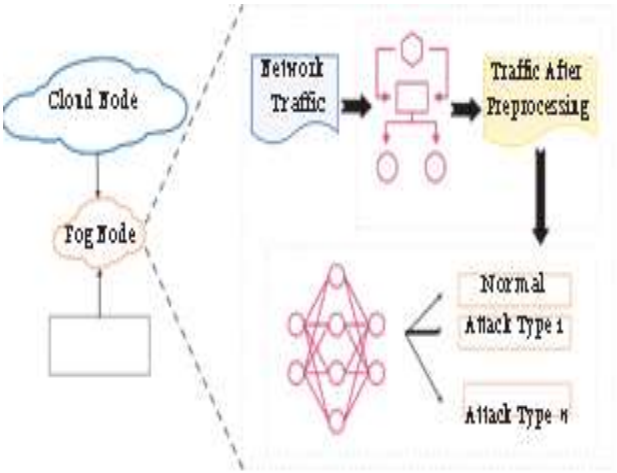


Fig 2: Intrusion detection of IoT with hybrid cloud-fog COMPUTING

(1) The data preprocessing model is responsible for transforming the raw network data into a form usable by the classification model in the first stage of data preprocessing. In this research, we combine the label encoder and max-min normalization techniques to create the LE-MMN model for preparing data. The raw data on network flow is measured and standardized using this methodology.

(2) When the data has been cleaned and organized, the classification model can begin classifying network traffic. Many common forms of assault are represented in the multi-classification model's breakdown of the data. The intrusion detection model implemented on a fog node ought to be lightweight while still being able

to locate intrusions. The ConvNeXt-Sf classification model was developed by slightly modifying the original ConvNeXt architecture on a single dimension in accordance with ShuffieNet V2's recommended practices for such modifications.

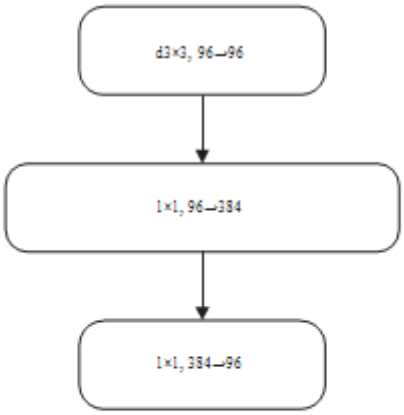


Figure 3: Inverted bottleneck structure in ConvNeXt.

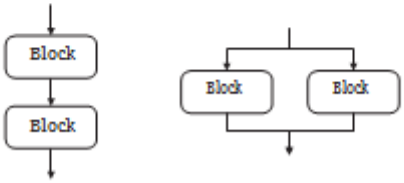


Figure 4: Fragmented network.

In this research, we deploy a hybrid cloud-fog computing setup to evaluate the proposed Internet of Things (IoT) model on the TON-IoT and BoT-IoT datasets. Hybrid cloud-fog computing is a growing trend in the Internet of Things (IoT) industry, and the TON-IoT and BoT-IoT datasets were chosen to reflect this. The fact that both the TON-IoT dataset and the BoT-IoT dataset encompass a comprehensive set of IoT operations is something else to keep in mind. This extension allows for a more thorough assessment of the model's performance across a variety of Internet of Things (IoT)-related tasks.

## IV. CONCLUSION

In this research, the issue of intrusion detection in the IoT is addressed by employing ConvNeXt, a novel high-performance computer vision model. The research also proposes tweaking the intrusion detection systems (IDS) in fog nodes for marginal gains in protection of Internet of Things (IoT) gadgets. The ConvNeXt model was developed to process network data by dealing with one-dimensional data. Incorporating the needs of the ShuffieNet V2 lightweight computer vision model into ConvNeXt yields the ConvNeXt-Sf classification model. By fusing the LE-MMN data preprocessing model and the ConvNeXt-Sf classification model, a robust IoT intrusion detection model may be created. Experiments conducted on the TON-IoT and BoT-IoT datasets demonstrate that ConvNeXt-Sf is more computationally efficient than ConvNeXt while simultaneously improving detection accuracy. In comparison to ConvNeXt-DenseNet and ConvNeXt-GhostNet, the proposed model achieves higher accuracy and lower FAR. It also has advantages, such as a reduced need for parameters and faster training and prediction.

There will be additional work to improve the proposed approach by incorporating unsupervised or semisupervised learning. In a hybrid cloud-fog computing or Internet of Things (IoT) implementation, the vast bulk of the network data does not have labels. It takes a lot of time and energy to use supervised learning for data tagging. The use of unsupervised or semi-supervised learning drastically reduces overhead. The widespread application of unsupervised learning in NLP has also paved the way for its usage in IoT intrusion detection. This app has the potential to facilitate communication and collaboration amongst specialists from many disciplines.

**REFERENCES**

[1] X. Zhang, Y. Yuan, Z. Zhou, S. Li, L. Qi, and D. Puthal, “Intrusion detection and prevention in cloud, fog, and in- ternet 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] H. Sabireen and V. Neelanarayanan, “A review on fog computing: architecture, fog with IoT, algorithms and re- search challenges,” ICT Express, vol. 7, no. 2, pp. 162–176, 2021.

[5] 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.

[6] 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.

[7] J. P. Anderson, “Computer security threat monitoring and surveillance,” Technical Report, pp. 1–53, James P Anderson Company, kansas, KS, USA, 1980.

[8] L. T. Heberlein, G. V. Dias, and K. N. Levitt, “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.

[9] 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.

[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.

[12] R. Kozik, M. Pawlicki, and M. Chora´s, “A new method of hybrid time window embedding with transformer-based traffic data classification in IoT-networked environment,” Pattern Analysis and Applications, vol. 24, no. 4, pp. 1441– 1449, 2021.

[13] M. M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, “A hybrid deep learning model for efficient in- trusion detection in big data environment,” Information Sciences, vol. 513, pp. 386–396, 2020.

[14] A. Derhab, A. Aldweesh, A. Z. Emam, and F. A. Khan, “Intrusion detection system for internet of things based on temporal convolution neural network and efficient feature engineering,” Wireless Communications and Mobile Com- puting, vol. 2020, Article ID 6689134, 16 pages, 2020.