Journal of trends in Computer Science and Smart technology (TCSST) (2020)
Vol.02/ No. 01
Pages: 46-55
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2020.1.005

Anomalies Detection in Fog Computing Architectures Using Deep Learning

Dr. Subarna Shakya
Professor, Department of Electronics and Computer Engineering,
Central Campus, Institute of Engineering, Pulchowk,
Tribhuvan University,
Pulchowk, Lalitpur Nepal.
Email: drss@ioe.edu.np.

Dr. S. Smys
Professor,
Department of Computer Science Engineering
RVS technical Campus
Coimbatore, India
Email:smys375@gmail.com

Abstract: A novel platform of dispersed streaming is developed by the fog paradigm for the applications associated with the internet of things. The sensed information's of the IOT plat form is collected from the edge device closer to the user from the lower plane and moved to the fog in the middle of the cloud and edge and then further pushed to the cloud at the top most plane. The information's gathered at the lower plane often holds unanticipated values that are of no use in the application. These unanticipated or the unexpected data's are termed as anomalies. These unexpected data's could emerge either due to the improper edge device functioning which is usually the mobile devices, sensors or the actuators or the coincidences or purposeful attacks or due to environmental changes. The anomalies are supposed to be removed to retain the efficiency of the network and the application. The deep learning frame work developed in the paper involves the hardware techniques to detect the anomalies in the fog paradigm. The experimental analysis showed that the deep learning models are highly grander compared to the rest of the basic detection structures on the terms of the accuracy in detecting, false-alarm and elasticity.

Keywords: Deep Learning, Fog Computing, Anomalies Detection, Accuracy in Detecting, False-Alarm and Elasticity

1. Introduction

A novel platform of dispersed streaming is developed by the fog paradigm for the applications associated with the internet of things. The architecture of Fog is composed of several planes arranged in hierarchical manner and supports the processing of data that was collected from the lower plane at the user edge. They are very much preferred by the Iot platform nowadays as the processing the remote cloud is much time consuming and costly. So the delay sensitive tasks prefer the Fog computing.

There are enormous number of applications such as the smart parking, smart heath, smart traffic control, supply chain, logistics, and power distribution that are enabled by the internet of things, all these application empowered by IOT perform two things in common they are the “monitoring”- observing the periodic status of the sensors and “actuating” – responding to the data’s that were perceived during “monitoring”. Some data’s observed are essential while some of the data collected are unanticipated. The se unanticipated data may occur either due to the changes incurred in the atmosphere or purposefully done or even might be due to improper functioning or coincidence. These were termed as anomalies. The occurrence of the anomalies are expected to happen even due to the incapability’s of the sensors used in the edge.

There are several IoT applications which are prone to delay. It is necessary to identify abnormalities early in order to safeguard the integrity of the executions, “in addition to rectifying anomalous sources and responding to the environmental changes. Anomaly detection can be effectively achieved in the cloud.” Nevertheless, with a very large number of sensors, perhaps billions in some applications, and thus the massive amount of data they produce, it will take very high bandwidth to send the input data to the cloud for anomaly detection. Edge systems are not going to have the capability. However, many equipment’s don't have cloud access 24/7. Anomalies are supposed to be identified, in the fog or edge layer to minimize the delay in anomalies identification.

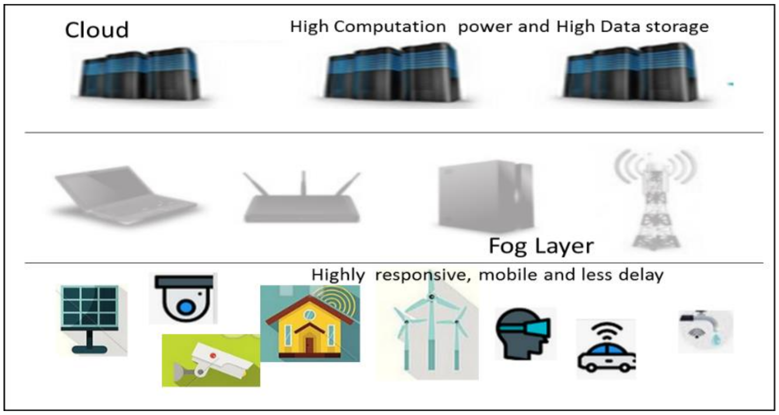

Cloud
High Computation power and High Data storage
Fog Layer
Highly responsive, mobile and less delay

Figure.1. Fog Structure Modified From [1]

The basic structure of the fog network is shown in the figure.1 above. The fog placed in middle of the user edge and the cloud computing is known as the expansion of cloud with the competencies to compute the data at proximity to the user. It solves the issues related to the conveyance, delay and the network utilization. It is involves the “IoT + data and the business engineered insights obtained from the data transmitted among these smart objects”. “The fog nodes are highly scalable and more responsive for hosting and security services than the cloud”. It also provides a layered frame work similar to cloud and extends assistance to wide range of applications. “The fog computing saves the network resources and the response time, as transmitting any data to cloud or any other central point would cause the enormous huge scarce bandwidth, inevitably paving way to high response time that could affect the operation of certain real time applications”

The deep learning frame work developed in the paper involves the hardware techniques to detect the anomalies in the fog paradigm. The experimental analysis showed that the deep learning models are highly grander compared to the rest of the basic detection structures on the terms of the accuracy in detecting, false-alarm and elasticity is arranged with the part two disclosing the literature survey on the Fog architecture and the deep learning strategies. , part three explaining the proposed deep learning strategy for anomalies detection, part four explaining the “evaluation performance of the system in comparison with other algorithms that are shallow on the basis of accuracy, detection rate and elasticity” and fifth part with the conclusion.

2. Literature Survey

Diro, et al [1] proposes the"Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing."   , Virushabadoss, S et al [2] presents the “Analysis of behavior profiling algorithm to detect usage anomalies in fog computing." Lyu et al [3] has put forth the "Fog-empowered anomaly detection in IoT using hyperellipsoidal clustering." Jyothirmai, P et al [4] presents the "Secure interoperable architecture construction for overlay networks."

Praveena, A., et al [5] present the. "Anonymization in social networks: a survey on the issues of data privacy in social network sites." Raj, Jennifer S., et al [6]discusses the “Novel Classification via Clustering Method for Anomaly Based Network Intrusion Detection System” and the “Performance Improvement in MANETs: A Cross Layer Approach via TCP”, Kumar, T. Senthil et al [7] proffers the "Efficient resource allocation and QOS enhancements of IoT with FOG network."

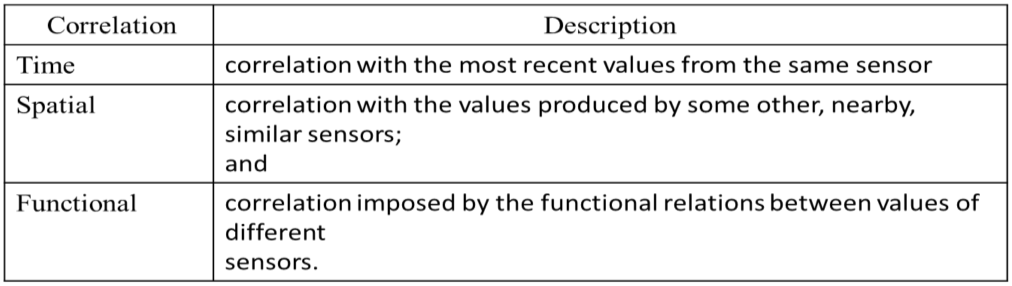
Karthiban, K., et al [8] discloses the "Privacy preserving approaches in cloud computing." Anguraj,et al [9] puts forth the “Trust-based intrusion detection and clustering approach for wireless body area networks.” S. Smys et al [10] in his paper describes the. "Efficient cryptographic approach for data security in wireless sensor networks using MES VU."

Praveena, A., et al [11] put forth the "Prevention of inference attacks for private information in social networking sites." And further Smys, S. et al [12] in his paper puts forward a “DDOS Attack Detection in Telecommunication Network Using Machine Learning” Bestak, et al [13] presents the "Big Data Analytics For Smart Cloud-Fog Based Applications."

The author Sivaganesan, D et al [14] has "Designed and Developed Ai-Enabled Edge Computing for Intelligent-Iot Applications." Bashar et al [15] has elaborated the "Survey on Evolving Deep Learning Neural Network Architectures." Ananthi, J. Vijitha et al [16] proffers the “Peer to Peer Overlay Approach for Topology Maintenance in Wireless Networks."

3. **Methodology**

As the unanticipated data received from the lower plane devices of the fog network are termed to be the abnormalities/ glitches/ anomalies, the variance from the expected values is detected as the glitches, comparing the data perceived to the with the data’s that is actually expected gives the real glitch that is present in the sensed data. “The categories of correlations”, that are essential in comparing the abnormalities with the expected-data is listed below in the table.1.



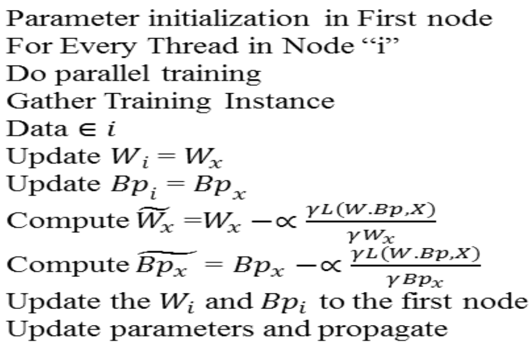
Correlation	Description
Time	correlation with the most recent values from the same sensor
Spatial	correlation with the values produced by some other, nearby, similar sensors; and
Functional	correlation imposed by the functional relations between values of different sensors.

Table.1 Different Types of Correlation

The glitches disturbing the performance could be either in the form of single data observed currently, or cluster of data's or even data gathered from the same type of sensors or from variety of other components. The data expected are learned through a deep learning model in the proposed work and it is used to identify the abnormalities in the network.

3.1. Deep learning Architecture for Anomaly Identification

The proposed model employs the stacked auto encoder which by its self-learning capacity identifies the normal data expected and the unanticipated data based on the training provided to it. The identified particulars are "mapped to the labeled test data as the anticipated or the unanticipated data's the "trained features are fed as the input to the classification algorithms such as the softmax regression" The identification of the abnormalities in the fog employing the deep-learning demands prefect managing of data dispersion, parameter involved and the necessary updates required. The constant engagement of the "stochastic gradient descent" to the fog network is unfeasible as the side by side computation would be demanded to handle the network that operates in the distributed nature and the enormous amount of data flowing form the IOT devices. So a "host centric training approach" with the capability of being expanded and processed through the "back prorogation" was used for identifying the abnormality, with a consistent learning rate " $\propto$ " . If the weights for the initial training and the parameters of bias were set as W_i and that are conveyed from the initial node. With data "i" being gathered from the devices of the lower plane in the fog network, the observed data are used in the parallel training the model and updating the particulars periodically by dispersing across the nodes threadsN_{th}. The algorithm below in figure.3



```
Parameter initialization  in First node
For Every Thread in Node "i"
Do parallel training
Gather Training Instance
Data $\in i$
Update $W_i = W_x$
Update $Bp_i = Bp_x$
Compute $\widetilde{W_x} = W_x - \propto \frac{\gamma L(W.Bp,X)}{\gamma W_x}$
Compute $\widetilde{Bp_x} = Bp_x - \propto \frac{\gamma L(W.Bp,X)}{\gamma Bp_x}$
Update the $W_i$ and $Bp_i$ to the first node
Update parameters and propagate
```

Figure.2 Training Algorithm

ISSN: 2582-4104

According to the algorithm in figure.2 the deep-learning is employed to the first node and the then sent to the following nodes in the FOG network. The data used for training as well as the parameter optimization are performed locally for each nodes. The optimizers and the gradients in the deep learning at every node engages in updating the parameters and accumulating updates and sending back to the first node. The updates of every threads of the local nodes are sent to the first node. The significance of the structure is multi fold, the local nodes following the first node identifies the abnormalities locally in their particular position and the first node holds responsibility of parameter update utilizing the gradient descent.

The Following Steps Describe the Identification Process

1. Computation begins at level 1
2. Checks abnormality using the trained deep learning model.
3. If dangerous unanticipated data's are found in input the further data processing is stopped.
4. If dangerous unanticipated data's (DUAD) found in the output the further forwarding of the data is stopped.
5. Every DUAD identified is updated to the following nodes and the sent back for training as unanticipated data.
6. If no DUAD is found in any stage of processing this is also updated to the following nodes and sent back for training as normal anticipated data.

So if no abnormalities are detected in any of the stage of processing the computation is carried out without any interruptions and the updates are done accordingly.

4. Assessment of Performance

The deep learning abnormality detection process was validated with the data set gathered from the Fog network that handles the normal activities absorption of industries in a SITCO, the number of data set for training and the testing are listed in the table.2

Data	Training	Testing
Normal	65,342	10,000
Abnormal	55,645	14,000
Total	120,987	24,000

Table.2 Dataset Utilized

The proposed model was evaluated on the basis of the performance metrics such as the detection rate, accuracy and the false alarms along with the scalability to adapt to the change in the data flow. The proposed frame work engaged 151 first layer neurons, 125 second layer neurons and 50 third layer neurons with the final softmax layer for classification. “The frame work used 30 epochs and trained with the dropouts to elude the overheating problem.” The evaluation results of the proposed frame work was compared with the Softmax without initial training on terms of the Accuracy in detecting, scalability, false alarms and the rate of detection. These metrics were estimated based on the, “true positives, false negatives, false positives and true negatives”

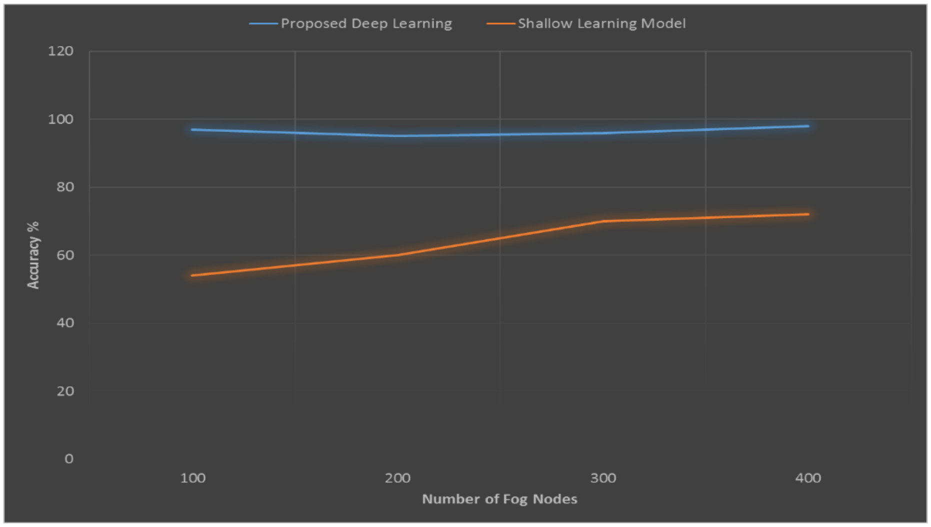


Figure.3 Accuracy

The accuracy results observed for the proposed and the other learning models are presented in the figure.3 it was found that the deep learning showed up with the better accuracy percentage compared to the softmax without pre-training.

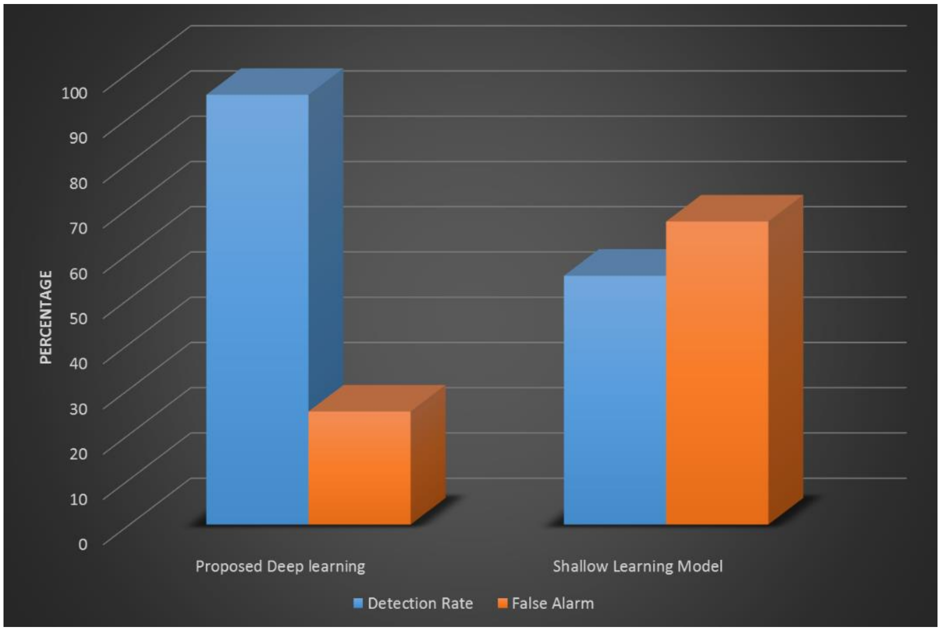


Figure.4 Detection rate and the False alarms

The figure.4 shows the percentage of the detection rate and the false alarms observed for the proposed and the other learning models, it was found that the deep learning showed up with the better percentage detection and false alarms compared to the softmax without pre-training. The above three results proves the scalability of the proposed structure is much better compared to the other learning models.

5. Conclusion

In order to identify the abnormalities in the data gathered in the Fog network the paper proposes the deep learning model as it is capable of self-learning, processing at a high speed and providing accurate results compared to the traditional machine learning models. The proposed model utilizes the host centric training and the back prorogation and the softmax regression classifier at the final stage to identify the abnormalities. The results obtained through the evaluation of the proposed model based on the performance metrics such as the accuracy, detection rate and the false alarm, shows the proficiency and the scalability of the proposed model compared to the shallow learning models current used.

References

[1] Diro, Abebe Abeshu, Naveen Chilamkurti, and Neeraj Kumar. "Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing." *Mobile Networks and Applications* 22, no. 5 (2017): 848-858.

[2] Virushabadoss, S., and C. Bhuvaneswari. "Analysis of behavior profiling algorithm to detect usage anomalies in fog computing." In *One Day National Conference On Internet Of Things-The Current Trend In Connected World*. 2018.

[3] Lyu, Lingjuan, Jiong Jin, Sutharshan Rajasegarar, Xuanli He, and Marimuthu Palaniswami. "Fog-empowered anomaly detection in IoT using hyperellipsoidal clustering." *IEEE Internet of Things Journal* 4, no. 5 (2017): 1174-1184.

[4] Jyothirmai, P., and Jennifer S. Raj. "Secure interoperable architecture construction for overlay networks." In *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, pp. 1-6. IEEE, 2015.

[5] Praveena, A., and S. Smys. "Anonymization in social networks: a survey on the issues of data privacy in social network sites." *Journal of International Journal Of Engineering And Computer Science* 5, no. 3 (2016): 15912-15918.

[6] Raj, Jennifer S., S. Smys, G. Josemin Bala, B. Praba, R. Sujath, V. Hilda Christy Gnanam, M. Abdul Rahiman et al. "Editorial Board v-vi A Novel Classification via Clustering Method for

[7] Anomaly Based Network Intrusion Detection System 1-6 Mrutyunjaya Panda and Manas Ranjan Patra Performance Improvement in MANETs: A Cross Layer Approach via TCP 7-11."

[8] Kumar, T. Senthil. "Efficient resource allocation and QOS enhancements of IoT with FOG network." *J ISMAC* 1 (2019): 101-110.

[9] Karthiban, K., and S. Smys. "Privacy preserving approaches in cloud computing." In *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, pp. 462-467. IEEE, 2018.

[10] Anguraj, Dinesh Kumar, and S. Smys. "Trust-based intrusion detection and clustering approach for wireless body area networks." *Wireless Personal Communications* 104, no. 1 (2019): 1-20.

[11] Praveena, A., and S. Smys. "Efficient cryptographic approach for data security in wireless sensor networks using MES VU." In *2016 10th international conference on intelligent systems and control (ISCO)*, pp. 1-6. IEEE, 2016.

[12] Praveena, A., and S. Smys. "Prevention of inference attacks for private information in social networking sites." In *2017 International Conference on Inventive Systems and Control (ICISC)*, pp. 1-7. IEEE, 2017.

[13] . Smys, S. "DDOS ATTACK DETECTION IN TELECOMMUNICATION NETWORK USING MACHINE LEARNING." *Journal of Ubiquitous Computing and Communication Technologies (UCCT)* 1, no. 01 (2019): 33-44.

[14] Bestak, Robert, and S. Smys. "BIG DATA ANALYTICS FOR SMART CLOUD-FOG BASED APPLICATIONS." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 02 (2019): 74-83.

[15] Sivaganesan, D. "DESIGN AND DEVELOPMENT AI-ENABLED EDGE COMPUTING FOR INTELLIGENT-IOT APPLICATIONS." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 02 (2019): 84-94.

[16] Bashar, Abul. "SURVEY ON EVOLVING DEEP LEARNING NEURAL NETWORK ARCHITECTURES." *Journal of Artificial Intelligence* 1, no. 02 (2019): 73-82.

[17] Ananthi, J. Vijitha, and Jennifer S. Raj. "A Peer to Peer Overlay Approach for Topology Maintenance in Wireless Networks."