IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SEARCH: COLLABRATIVE AND INTELLIGENT NIDS ARCHITECTURE FOR SND-BASED CLOUD IOT NETWORK

1. M.HARIKA, 2.K.AISHWARYA, 3.T.SWATHILAKSHMI, 4.V.ANANTHA KRISHNA

1. Student, 2.Student, 3.Student, 4.Professor

Department of computer science engineering,Sridevi women's engineering college, vattinagulapally, Gandipet, R.R Dist-500075

ABSTRACT

The network traffic in the cloud will lead to many attacks, this will lead to reduced security for the devices present on the cloud .The traditional architecture are insufficient to solve this security threats in cloud. The machine Learning techniques introduce numerous advantages that can effectively resolve cyber security matters for cloud-based IoT systems. , we propose collaborative and intelligent network-based intrusion detection system (NIDS) architecture, namely SeArch, for SDN-based cloud IoT networks. It composes a hierarchical layer of intelligent IDS nodes working in collaboration to detect anomalies and formulate policy into the SDN-based IoT gateway devices to stop malicious traffic as fast as possible.

Keywords: Software defined network, IDS(Intrusion detection system) nodes,

I.INTRODUCTION

The explosive rise of intelligent devices has increased the (IOT) network traffic in the cloud environment. The excessive amount of data in cloud increased the flow of data which led to traffic in cloud and created potential attack surfaces for cyber-attacks can effectively resolve cyber security matters for cloud-based IoT systems. We propose collaborative and intelligent network-based intrusion detection system (NIDS) architecture, namely SeArch, for SDN-based cloud IoT networks. It composes a hierarchical layer of intelligent IDS nodes working in collaboration to detect anomalies and formulate policy into the SDN-based IoT gateway devices to stop malicious traffic as fast as possible. "SeArch" architecture yield outstanding performance in anomaly detection and mitigation as well as bottleneck problem handling in the SDN-based cloud IoT networks

python, EDGE IDS,FOG IDS, Cloud servers, SVM, SOM, SAE Algorithms algorithms to detect attack signature in IoT networks as now-a-days everywhere small sensors are deployed to sense data and then send to centralized cloud server for further processing. These sensors can be deployed at road side to monitor traffic, military area, healthcare monitoring etc. This sensor will use 3 layers such as EDGE IDS, FOG IDS and Cloud server, these Sensors will send data to EDGE IDS by using optimize path and then EDGE ID will run SVM algorithm to check whether request contains normal or attack signature and then EDGE IDS will forward request to FOG IDS and then FOG IDS will run SOM (self-organizing map clustering) algorithm to check whether request contains normal or attack signature and in FOG IDS will send request to CLOUD server and then cloud server will run SAE (stacked auto encoder deep learning) algorithm to check request contains attack or normal signature.

II.OBJECTIVE

SeArch, for SDN-based cloud IoT networks. It composes a hierarchical layer of intelligent IDS nodes working in collaboration to detect anomalies and formulate policy into the SDN-based IoT gateway devices to stop malicious traffic as fast as possible. We first describe a new NIDS architecture with a comprehensive analysis in terms of the system resource and path selection optimizations. Next, the system process logic is extensively investigated in comparison with existing solutions. It composes a hierarchical layer of intelligent IDS (Intrusion detection system)nodes .We use the machine learning path selection optimizations. Next, the system process logic is extensively investigated through main consecutive procedures, including Initialization, Runtime Operation and Database Update. Afterwards, we conduct a detailed implementation of the proposed solution in an SDN-based environment and perform a variety of experiments. Finally, evaluation results of the SeArch architecture yield outstanding performance in anomaly detection and mitigation.

III.PROBLEM STATEMENT

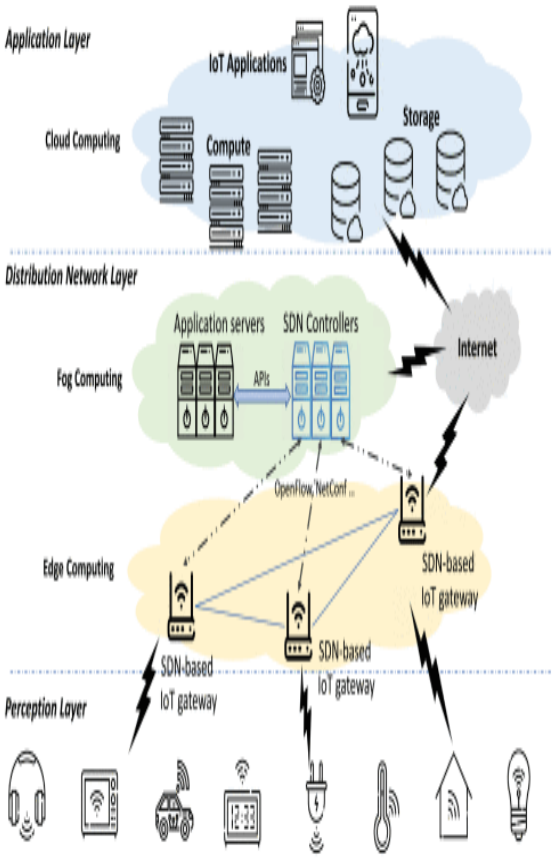
Excessive traffic in the cloud environment would lead many anomalies to the devices present on the cloud .The network traffic increases many security issues. The introduced security architecture consists of three main layers of IDS including Edge-IDS, Fog-IDS and Cloud- IDS. These Intrusion detection nodes will detect the attack signatures and will reduce security

IV.PROPOSED SYSTEM

SeArch, for SDN-based cloud IoT networks. It composes a hierarchical layer of intelligent IDS nodes working in collaboration to detect anomalies and formulate policy into the SDN-based IoT

V .MODULES

through main consecutive procedures, including Initialization, Runtime Operation and Database Update. Afterwards, we conduct a detailed implementation of the proposed solution in an SDN-based environment and perform a variety of experiments. Finally, evaluation results of the SeArch architecture yield outstanding performance in anomaly detection and mitigation.



We make use of following modules

1. Upload & Preprocess UNSEM_NB15 Dataset: Upload & Preprocess UNSW_NB15 Dataset Module is used to load dataset and in dataset we are displaying total number of normal and attack signature records.

2. Build SVM Algorithm: Build SVM Algorithm module to train SVM with above dataset And SVM is trained and we got its prediction accuracy as 100%.

3. Build SOM Algorithm: Build SOM Algorithm module to train SOM algorithm and SOM got 70% accuracy and in graph we can see it created 2 clusters.

4. Build SAE Algorithm: Build SAE Algorithm module to train SAE with above dataset And SAE is trained and we got its prediction accuracy as 72%.

5. Accuracy Comparison Graph: Accuracy Comparison Graph module is used to get graph. In above graph x-axis represents algorithm name and y-axis represents accuracy of those algorithms.

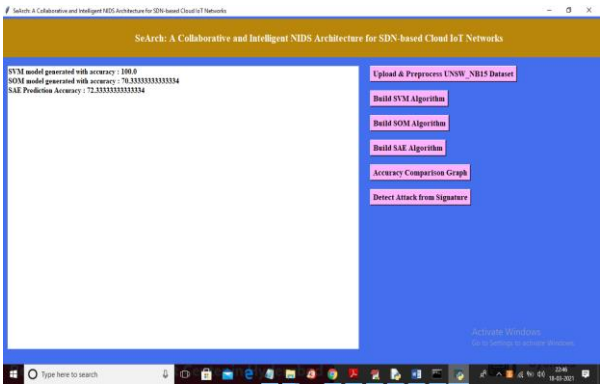
6. Detect Attack from Signature: Detect Attack from Signature Module and upload test new request signature. 'Contains Attack or Normal Signature'.

VI.ALGORITHM

SVM ALGORITHM: The Sensors will send and then EDGE ID will run SVM algorithm to check whether request contains normal or attack signature.

SOM ALGORITHM: EDGE IDS will forward request to FOG IDS and then FOG IDS will run SOM (self- organizing map clustering) algorithm to check whether request contains normal or attack signature.

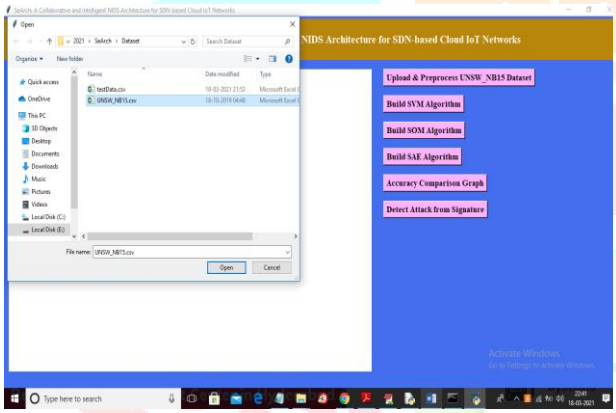
SAE ALGORITHM: FOG IDS will send request to CLOUD server and then cloud server will run SAE (stacked auto encoder deep learning) algorithm to check request contains attack or normal signature.

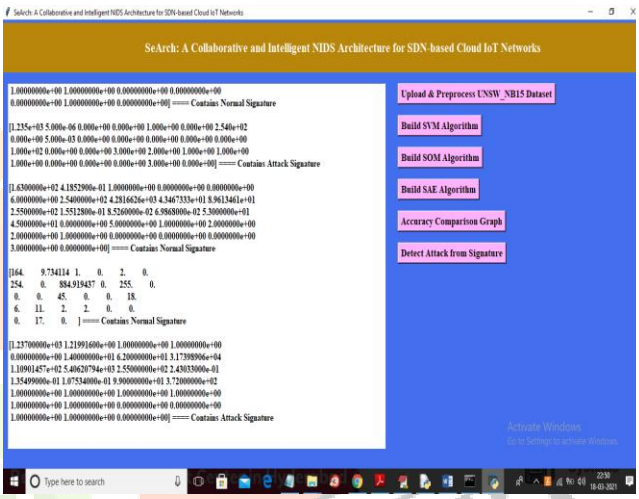


The accuracy of svm algorithm is 100%,the accuracy for som algorithm is 70% and the accuracy for sae algorithm is 72%.

VII.RESULTS AND DISCUSSION

To run project double click on 'run.bat' file to get below screen





We have test signature and after square bracket we got predicted result as 'Contains Attack or Normal Signature'

management. The more machine learning algorithms must be introduced in order to find the best accuracy method.

proposed to bring benefits to the resource

IX.CONCLUSION

This architecture leverages the use of machine learning/deep learning for intelligently detecting network-related threats from IoT devices. A novel system resource optimization and an optimal path selection scheme are proposed to bring benefits to the resource management and the overhead of

VIII.FUTURE ENHANCEMENTS

This architecture leverages the use of machine learning/deep learning for intelligently detecting network-related threats from IoT devices. A novel system resource optimization and an optimal path selection scheme are

17, pp. 2347– 2376, Fourthquarter 2015.

[2] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies,

communication of the proposed solution. In comparison with existing solutions, the SeArch solution achieves a remarkable anomaly detection performance, i.e., around 95.5% on average of detection rate, accuracy and precision, which is same to results obtained by the CFD and CFCD methods, while providing a right level of attack mitigation, i.e., only 7.0 ms on average in attack mitigation time, and tackling performance bottleneck problems as same as the DED scheme .

X .REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys Tutorials, vol.

security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, pp. 1125–1142, Oct 2017.

[3] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah, and P. Siano, "Iot-based smart cities: A survey," in 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), pp. 1–6, June 2016.