Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021: 9711 – 9715

Research Article

A Machine Learning centric NIDS Architecture for SDN-based Cloud IoT Networks

Varkala Kishore[a], Dr. D. Srinivasa Rao[b]
[a] Member, IAENG
[b] Member, IEEE

Abstract

The exponential development in smart gadgets with all-round connection has hugely reduced the flow inside the cloud Internet of Things (IoT) and generated possible cyber-attack surfaces. Traditional security techniques to handle security risks in cloud-based IoT networks are insufficient and ineffective. Software Defined Networking (SDN), Network Function Virtualization (NFV), and Machine Learning Technologies provide several advantages to tackle cyber security problems for fog IoT devices. This article proposes collaboration and smart network-based design for IoT networks, called NIDS, for access control based on SDNs. It consists of a hierarchic level of smart IDS nodes that work together to identify abnormalities and create policies in SDN-based integrated application devices to block malicious traffic at the quickest opportunity. First we outline a novel NIDS architecture with an extensive small network and track decision evaluation. Next, the logic of the control system is explored comprehensively by the major sequential procedures comprising initialization, realtime operations and database updates. Then we build the developed model in complete in an SDN-based ecosystem and undertake a number of tests. Finally, the NIDS architecture assessment findings offer great results in anomalous identification and reduction and the treatment of problem bottleneck mostly in SDN-based cloud Iot systems compared with existing alternatives.

Keywords: *Security Iot, Defined Internet software, virtualized of networking devices, machine learning, authenticator, shared clouds computer*

Introduction

The development of Internet of Things has brought enormous capabilities in many areas of human life for omnipresent intelligent connectivity and applications [1],[2]. Smarter equipment can provide human beings an intelligent and active life by facilitating sensing and action, contextual awareness [3],[4]. Recently the variety of new technologies, such as sensors, wireless communications and Cloud Computing Technology (SDN) and Network Function Virtualization (NFV) has expanded dramatically owing to IoT appliances [5]. As an excellent instance, Cisco Systems [6] anticipates worldwide mobile data traffic and growth trends from 2017 to 2022, with 12.3 billion mobile devices connected by 2022, and global mobile data traffic reaching 77 exabytes by 2022 per month. The huge quantity of data being absorbed into the Internet with intelligent gadgets, driverless cars, wearable devices,

environmental sensors and nearly everything we can think. Therefore, the opportunities offered by IoTs are endless and their capabilities and potential will be tangible soon when a large number of IoT devices are connected daily with the Internet. IoT network systems, on the other hand, provide current promising hacker surfaces for malevolent attackers can cause enormous economic and reputable devastation for system owners [7] [8], unless there are proper protective measures. The network softwarisation, including SDN and NFV, is a great success for Telco sectors, with numerous advantages in terms of dynamism, flexibility and management. As for network security, both of these essential supporters of cloud - based services are gaining pace with the introduction of dynamic and adaptable cloud protection mechanisms [9]. Although a number of studies have also been presented on the basis of SDN/NFV technology to deal better with IoT safety threats[10]. Current solutions, however, still face some important challenges such as bottleneck difficulties and lack of collaboration while offering cloud-based IoT network security services or processes. In addition, because of the enormous amount of IoT devices, each network operator is always challenged in creating an effective cyber attack defence mechanism in IoT networks [7]. Therefore, in that paper, we are proposing a unique, collaborative and smart intrusion detection system (NIDS) architecture in the SDN-based cloud IoT networks, called SeArch, to protect successfully against network-related cyber assaults. This security architecture comprises a hierarchy of NIDS nodes, including Edge-IDS, Fog-IDS and Cloud-IDS. These IDSs relied on machine learning/deep learning algorithms for their detective activities and can be deployed in a distributed architecture with those situated in the same computer layer. Especially, Edge IDS is a lightweight security application, which is built into the edge computing SDN IoT gateways, FogIDS is running on the SDN controller as an SDN application in the fog computing layer, Cloud-IDS is a cloud-based IoT security application with sufficient computing power and storage resources. This design offers an efficient collaborative method amongst IDS nodes for network-related IoT traffic detection by building up communication channels between data synchronisation and load balancing nodes. The following can be found among our important contributions: Firstly, we examine current security methods and give motivation to utilise machine learning and profound learning technology for cyber assaults in cloud-based IoT networks. Then we illustrate the problem of resource usage on the edge of our previous experiment. Secondly, we offer a new Security infrastructure, SeArch, which represents a collaborating and smart NIDS infrastructure in the SDN-based cloud IoT networks and introduces an efficient cooperation between nodes to arrange three levels of IDS Nodes, namely Edge-IDS, Fog-IDS and Cloud-IDS. We also carry out a complete system analysis and take into account the management of resources and the overall communication of the solution offered. Then we develop a new system optimization system and optimum path selection technique. Finally, we conduct extensive experiments on a cloud-based IoT emulation network using SDN. A mainly refers of SeArch with current systems demonstrates substantial improvements in anomaly detection, abatement and bottleneck performance management.

Methodology

In this research, the author uses machine learning techniques to detect attack signatures in Iot devices since tiny sensors are now every day used to sense data and send them to the

centralised cloud server for processing. The sensors can be used on the roadside for traffic control, military, health monitoring, etc. This sensor uses three distinct devices, including EDGE IDS, FOG IDS and the cloud server. The sensors are sent to EDGE IDS by the path optimization, the EDGE ID is executed by an SVM algorithm to see if the request contains a normal signature or an attack signature. The EDGE IDS is then sent to FOG IDS and then FOG IDS runs SOM algorithm to check if the query did contain a common or an attack signature. Here all three devices work together to identify attacks on IOT networks. The author of the proposal has offered three algorithms.

Runtime operations at EDGE IDS: This collects traffic from sensors that send traffic by choosing the way to optimise, and then extracts traffic characteristics and then uses the SVM algorithm to assess the normal or malicious signatures. Send a request to FOG ID whether the signature is normal.

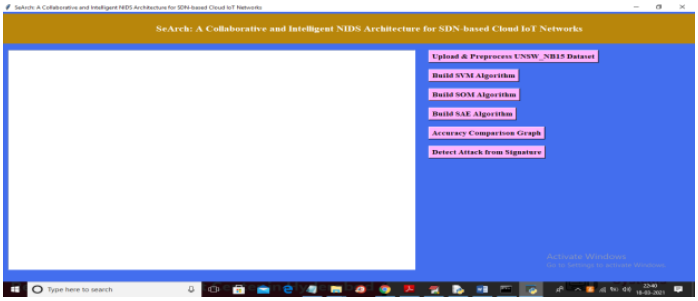
Runtime operations at FOG IDS: This collects traffic from EDGE ID, then EDGE ID transmits traffic, optimising the route, removing traffic characteristics and then applying SOM algorithms to assess the normal signature or attack signature. Send a request to the CLOUD ID if the signature is normal.

Runtime operations at CLOUD IDS: This collects traffic from FOG ID, sends it via route optimization, extracts traffic functions and then uses the SAE method to check for normal signatures or attack signatures. If the signature is normal, the request is processed by cloud. Here cloud updates the machine learning model database.

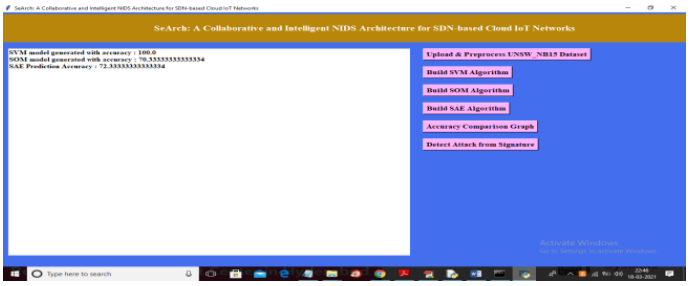
There is no sensor or any edges or fog or data center server in this case, so we construct a machine learning model and then submit the test identity to the built-in model to see if requests are normal or have an attack.

Results And Dıscussıon

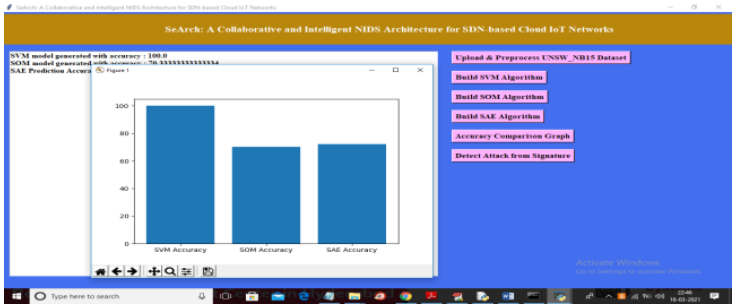
In this article the author uses UnSW NB15 and shows the signature of the IOT request from this dataset.



We are uploading Dataset & UNSW NB15 In the data set, we present the entire amount of normal and malicious signature recordings, then the application uses 1500 dataset records, trains the ML app using 1,200 records and tests the ML screening approach utilizing 300 records.



We run SVM, SOM and SAM techniques using above-trained data sets, and we have SVM with 100% efficiency and SOM with 70 percent accuracy, and SAE with SAE is trained and 72 percent with accuracy. The results below show the precision comparison graph.



In the aforementioned graph x-axis, the name of the method and y-axis is accurate and the SVM graph above shows high accuracy.

Conclusıon

In this study we offer an architecture for the collaborative and intelligent NDS system in SDN cloud IoT networks called SeArch, which introduces an effective collaborative arrangement of three levels of IDS nodes (Edge-IDS, Fog-IDS and CloudIDS). This design utilises machine learning to intelligently detect risks associated with the network from IoT devices. A new optimization of system resources and an ideal path selection method are suggested in order to provide benefits for the management of resources and the overall communication of the real method. The NIDS solution achieves remarkable anomalous detection performance, i.e. about 95.5% on average detection rate, accuracy and accuracy that corresponds to results obtained using the methods CFD and CFCD while ensuring an adequate mitigation level, i.e. only about 7.0 ms on average for the mitigation period, and for tackling bottleneck performance In addition, the architecture of the SeArch system only has a little overhead. In the future we aim to examine different machine learning/deep learning algorithms and cyber assaults with a wider range of data sets and other sorts of traffic in the architecture described.

References

[1] A. AlFuqaha, M.Guizani, M. Mohammadi, M. Aledhari, and M.Ayyash, IEEE Communications Surveys Tutorials, vol.17, pp.2347–2376, Fourthquarter 2015, "The internet of things: enabling technologies, protocols and applications."

[2] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "Internet study of: architecture, technology enabling, security and confidentiality, and applications," Things Journal IEEE Internet, vol. 4, pp. 1125–1142, Oct 2017.

[3] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah, P. Siano, IEEE 16th International Conference on the Environment and Electrical Engineering, IEEE, pp. 1–6, June 2016.

[4] "The Internet of Things Review of Smart Home Applications" [4] M.Alaa, A.Zaidan, B.Zaidan, M.Talal, and M.Kiah, Network Journal and Computer Applications, Vol. 97, pp. 48 – 65, 2017.

[5] Y. Li and M. Chen, 'Network Virtualization Defined Software Function: A Study': IEEE Access, vol. 3, pp. 2542–2553, 2015.

[6] "Cisco Visual Network Index: Global Mobile Data Traffic Forecast Update, WHITE 2017-2022, accessible at https://www.cisco.com/n/us/solutions/serviceprovider/vni/white-paper-c11-738429.html."

[7] H. Aldowah, S. Ul Rehman and I. Umar, 'Internet security for things: questions, problems and solutions,' in recent trends in data science and soft computing (F. Saeed, F. Mohammad, N. Gazem, and A. Busalim, eds).

[8] Kolias, Kambourakis, Stavrou, and Voas, Computer, Vol. 50, No. 7, pp. 80–84, 2017. [8] Ddo in the iot: Mirai and other botnets.

[9] V. Varadharajan and U. Tupakula, "Safety as a Cloud Environment Services Model," IEEE Network and Service Management Transaction, Vol. 11, pp. 60–75, March 2014.

[10] I. Farris, T. Taleb, Y. Khettab, and S. Song, IEEE Communications Survesys Tutorials, pp. 1-1, 2018 "Studying Emerging Sdn and Nfv Security Mechanisms for Ultrasound Systems."