A COMBINED APPROACH NIDS ARCHITECTURE FOR SDN BASED CLOUD AND IOT NETWORKS

M.Kavitha, Associate Professor, Sridevi Women's Engineering College, Hyderabad
N.Ruchitha, B.Tech, Dept of Information Technology, Sridevi Women's Engineering College, Hyderabad
T.Nikhitha, B.Tech, Dept of Information Technology, Sridevi Women's Engineering College, Hyderabad
D.Gayatri, B.Tech, Dept of Information Technology, Sridevi Women's Engineering College, Hyderabad

ABSTRACT: The explosive rise of intelligent devices with ubiquitous connectivity has dramatically increased Internet of Things (IoT) traffic in cloud environment and created potential attack surfaces for cyber-attacks. Traditional security approaches are insufficient and inefficient to address security threats in cloud-based IoT networks. In this vein, Software Defined Networking (SDN), Network Function Virtualization (NFV) and Machine Learning techniques introduce numerous advantages that can effectively resolve cybersecurity matters for cloud-based IoT systems. In this paper, we propose a 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. 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 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 as well as bottleneck problem handling in the SDN-based cloud IoT networks in comparison with existing solutions.

Keywords: Internet of Things Security, Software Defined Networking, Network Function Virtualization, Machine Learning, Intrusion Detection System, Distributed Cloud Computing.

1. INTRODUCTION

The advancement of Internet of Things (IoT) has been bringing enormous capabilities for ubiquitously intelligent connectivity and applications in many domains of human life [1], [2]. Smarter devices can provide a smart and active life for human by enabling sensing and actuation abilities, contextual awareness [3], [4]. Recently, the IoT appliances have been exponentially increased due to a wide range of new technologies [1] such as sensors, wireless communications and cloud computing technologies, e.g., Software-Defined Networking (SDN), Network Function Virtualization (NFV) [5]. A good illustration, Cisco Systems [6] forecasts the global mobile data traffic projections and growth trends for a period of time from 2017 to2022, in which there will be 12.3 billion mobile-connected devices by 2022, and the global mobile data traffic will reach77exa bytes every month by 2022. The tremendous amount of data would be absorbed into the Internet consisting of smart-home devices, autonomous vehicles, wearable devices, environmental sensors and almost anything we can imagine.

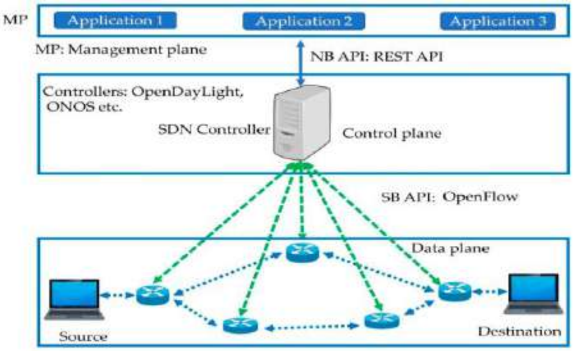


Fig.1 SDN architecture

Consequently, the opportunities from the development of IoTs are endless, and its capabilities and potential will be tangible very soon as a vast number of IoT devices are getting connected to the Internet Day by day. On the other hand, IoT network systems present new potential cyber-attack surfaces for malicious attackers leading to tremendous economic and reputation destruction for system operators/providers [7], [8], if there are no correctly protection solutions. Fortunately, the network softwarization including SDN and NFV cloud technologies are representing a major break-through in Telco industries, by providing several benefits regarding dynamics, flexibility and manageability. Concerning network security, these two key enablers of cloud computing technologies are obtaining a great momentum by introducing dynamic and flexible security protection mechanisms to cloud environment [9]. Although, a variety of studies based on SDN/NFV technologies have been proposed to better cope with IoT security threats [10].

2. LITERATURE REVIEW

Internet of things: A survey on enabling technologies, protocols, and applications

This paper provides an overview of the Internet of Things (IoT) with emphasis on enabling technologies, protocols, and application issues. The IoT is enabled by the latest developments in RFID, smart sensors, communication technologies, and Internet protocols. The basic premise is to have smart sensors collaborate directly without human involvement to deliver a new class of applications. The current revolution in Internet, mobile, and machine-to-machine (M2M) technologies can be seen as the first phase of the IoT. In the coming years, the IoT is expected to bridge diverse technologies to enable new applications by connecting physical objects together in support of intelligent decision making. This paper starts by providing a horizontal overview of the IoT. Then, we give an overview of some technical details that pertain to the IoT enabling technologies, protocols, and applications. Compared to other survey papers in the field, our objective is to provide a more thorough summary of the most relevant protocols and application issues to enable researchers and application developers to get up to speed quickly on how the different protocols fit together to deliver desired functionalities without having to go through RFCs and the standards specifications. We also provide an overview of some of the key IoT challenges presented in the recent literature and provide a summary of related research work. Moreover, we explore the relation between the IoT and other emerging technologies including big data analytics and cloud and fog computing. We also present the need for better horizontal integration among IoT services. Finally, we present detailed service use-cases to illustrate how the different protocols presented in the paper fit together to deliver desired IoT services.

A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications

Fog/edge computing has been proposed to be integrated with Internet of Things (IoT) to enable computing services devices deployed at network edge, aiming to improve the user's experience and resilience of the services in case of failures. With the advantage of distributed architecture and close to end-users, fog/edge computing can provide faster response and greater quality of service for IoT applications. Thus, fog/edge computing-based IoT becomes future infrastructure on IoT development. To develop fog/edge computing-based IoT infrastructure, the architecture, enabling techniques, and issues related to IoT should be investigated first, and then the integration of fog/edge computing and IoT should be explored. To this end, this paper conducts a comprehensive overview of IoT with respect to system architecture, enabling technologies, security and privacy issues, and present the integration of fog/edge computing and IoT, and applications. Particularly, this paper first explores the relationship between cyber-physical systems and IoT, both of which play important roles in realizing an intelligent cyber-physical world. Then, existing architectures, enabling technologies, and security and privacy issues in IoT are presented to enhance the understanding of the state-of-the-art IoT development. To investigate the fog/edge computing-based IoT, this paper also investigates the relationship between IoT and fog/edge computing, and discuss issues in fog/edge computing-based IoT. Finally, several applications, including the smart grid, smart transportation, and smart cities, are presented to demonstrate how fog/edge computing-based IoT to be implemented in real-world applications.

A survey on IOT-based smart cities

Due to the growing developments in advanced metering and digital technologies, smart cities have been equipped with different electronic devices on the basis of Internet of Things (IoT), therefore becoming smarter than before. The aim of this article is that of providing a comprehensive review on the concepts of smart cities and on their motivations and applications. Moreover, this survey describes the IoT technologies for smart cities and the main components and features of a smart city. Furthermore, practical experiences over the world and the main challenges are explained.

A survey on a review of smart home applications based on internet of things

The new and disruptive technology of smart home applications (hereafter referred to as apps) based on Internet of Things (IoT) is largely limited and scattered. To provide valuable insights into technological environments and support researchers, we must understand the available options and gaps in this line of research. Thus, in this study, a review is conducted to map the research landscape into a coherent taxonomy. We conduct a focused search for every article related to (1) smart homes, (2) apps, and (3) IoT in three major databases, namely, Web of Science, ScienceDirect, and IEEE Explore. These databases contain literature focusing on smart home apps using IoT. The final dataset resulting from the classification scheme includes 229 articles divided into four classes. The first class comprises review and survey articles related to smart home IoT applications. The second class includes papers on IoT applications and their use in smart home technology. The third class contains proposals of frameworks to develop and operate applications. The final class includes studies with actual attempts to develop smart home IoT applications. We then identify the basic characteristics of this emerging field in the following aspects: motivation of using IoT in smart home applications, open challenges hindering utilization, and recommendations to improve the acceptance and use of smart home applications in literature.

A survey on Software defined network function virtualization

Diverse proprietary network appliances increase both the capital and operational expense of service providers, meanwhile causing problems of network ossification. Network function virtualization (NFV) is proposed to address these issues by implementing network functions as pure software on commodity and general hardware. NFV allows flexible provisioning, deployment, and centralized management of virtual network functions. Integrated with SDN, the software-defined NFV architecture further offers agile traffic steering and joint optimization of network functions and resources. This architecture benefits a wide range of applications (e.g., service chaining) and is becoming the dominant form of NFV. In this survey, we present a thorough investigation of the development of NFV under the software-defined NFV architecture, with an emphasis on service chaining as its application. We first introduce the software-defined NFV architecture as the state of the art of NFV and present relationships between NFV and SDN. Then, we provide a historic view of the involvement from middlebox to NFV. Finally, we introduce significant challenges and relevant solutions of NFV, and discuss its future research directions by different application domains.

Security in internet of things: Issues, challenges and solutions

In the recent past, Internet of Things (IoT) has been a focus of research. With the great potential of IoT, there comes many types of issues and challenges. Security is one of the main issues for IoT technologies, applications, and platforms. In order to cover this key aspect of IoT, this paper reviews the research progress of IoT, and found that several security issues and challenges need to be considered and briefly outlines them. Efficient and functional security for IoT is required to ensure data anonymity, confidentiality, integrity, authentication, access control, and ability to identify, as well as heterogeneity, scalability, and availability must be taken into the consideration. Considering these facts, by reviewing some of the latest researches in the IoT domain, new IoT solutions from technical, academic, and industry sides are provided and discussed. Based on the findings of this study, desirable IoT solutions need to be designed and deployed, which can guarantee: anonymity, confidentiality, and integrity in heterogeneous environments.

Ddos in the iot: Mirai and other botnets

The Miraa botnet and its variants and imitators are a wake-up call to the industry to better secure Internet of Things devices or risk exposing the Internet infrastructure to increasingly disruptive distributed denial-of-service attacks.

Security as a service model for cloud environment

Cloud computing is becoming increasingly important for provision of services and storage of data in the Internet. However, there are several significant challenges in securing cloud infrastructures from different types of attacks. The focus of this paper is on the security services that a cloud provider can offer as part of its infrastructure to its customers (tenants) to counteract these attacks. Our main contribution is a security architecture that provides a flexible security as a service model that a cloud provider can offer to its tenants and customers of its tenants. Our security as a service model while offering a baseline security to the provider to protect its own cloud infrastructure also provides flexibility to tenants to have additional security functionalities that suit their security requirements. The paper describes the design of the security architecture and discusses how different types of attacks are counteracted by the proposed architecture. We have implemented the security architecture and the paper discusses analysis and performance evaluation results.

A survey on emerging SDN and NFV security mechanisms for IOT systems

The explosive rise of Internet of Things (IoT) systems has notably increased the potential attack surfaces for cybercriminals. Accounting for the features and constraints of IoT devices, traditional security countermeasures can be inefficient in dynamic IoT environments. In this vein, the advantages introduced by software defined networking (SDN) and network function virtualization (NFV) have the potential to reshape the landscape of cybersecurity for IoT systems. To this aim, we provide a comprehensive analysis of security features introduced by NFV and SDN, describing the manifold strategies able to monitor, protect, and react to IoT security threats. We also present lessons learned in the adoption of SDN/NFV-based protection approaches in IoT environments, comparing them with conventional security countermeasures. Finally, we deeply discuss the open challenges related to emerging SDN- and NFV-based security mechanisms, aiming to provide promising directives to conduct future research in this fervent area.

3. IMPLEMENTATION

In existing system, Traditional security approaches are insufficient and inefficient to address security threats in cloud-based IoT networks. In this vein, Software Defined Networking (SDN), Network Function Virtualization (NFV) and Machine Learning techniques introduce numerous advantages that can effectively resolve cybersecurity matters for cloud-based IoT systems.

Disadvantages:

➢ In bottleneck problem handling in the SDN-based cloud IoT networks in comparison with existing solutions.

➢ However, current solutions still face with some critical problems such as bottleneck issues and lacking of collaboration while providing security services or mechanisms for cloud-based IoT networks.

Here, we propose a 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. 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 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.

Advantages:

➢ Here, intelligent network-based intrusion detection system (NIDS) architecture, namely search, for SDN-based cloud IoT networks.

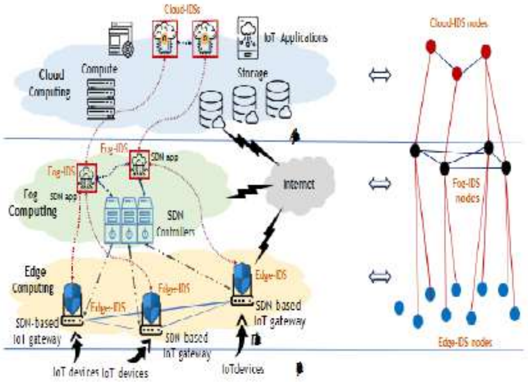


Fig.2: System architecture

However, current solutions still face with some critical problems such as bottleneck issues and lacking of collaboration while providing security services or mechanisms for cloud-based IoT networks. In addition, due to the huge quantity of IoT devices, it is always challenging for every network operator to create an effective defense mechanism against cyber-attacks in IoT networks. Therefore, in this article, we propose a novel collaborative and intelligent network-based intrusion detection system (NIDS) architecture to effectively defense against network-related cyber-attacks in SDN-based cloud IoT networks, entitled search. This security architecture consists of a hierarchical distribution of NIDS nodes, including Edge-IDS, Fog-IDS and Cloud-IDS, respectively. In which, these IDSs are based on machine learning/deep learning algorithms for their detection operations, and those located in the same computing layer can be in a distributed design. In particular, Edge-IDS is a lightweight security application integrated into an SDN-based IoT gateway in the edge computing level, Fog-IDS located in the fog computing layer runs as an SDN application on top of SDN controller, and Cloud-IDS is an IoT security application running on the cloud computing level with enough computation power and storage resources. This architecture introduces an effective collaboration way among IDS nodes in network-related anomaly IoT traffic detection by setting up communication channels among nodes for data synchronization and load balancing.

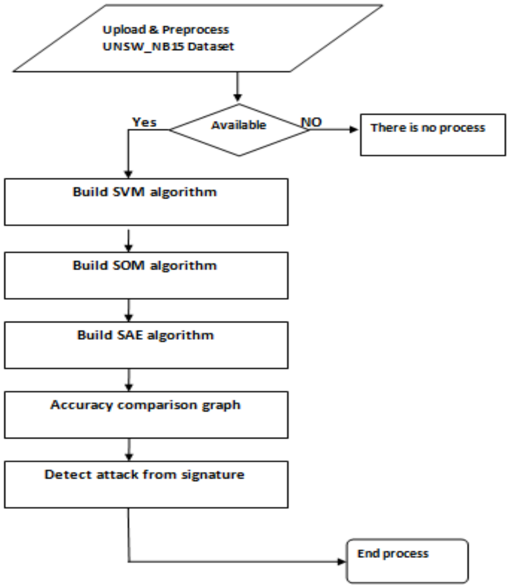


Fig.3: Dataflow diagram

4. ALGORITHMS

In this paper author is using machine learning 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 different devices such as EDGE IDS, FOG IDS and Cloud server. 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 then 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.

Here all 3 devices will collaborate each other to detect attack in IOT networks. In propose work author has given 3 algorithms

1) Runtime operations at EDGE IDS: This will collect traffic from sensors and sensor will send traffic by selecting optimize path and then extract features from traffic and then apply SVM algorithm to check normal or attack signature. If signature normal then request send to FOG ID

2) Runtime operations at FOG IDS: This will collect traffic from EDGE ID and EDGE ID will send traffic by selecting optimize path and then extract features from traffic and then apply SOM algorithm to check normal or attack signature. If signature normal then request send to CLOUD ID

3) Runtime operations at CLOUD IDS: This will collect traffic from FOG ID and FOD ID will send traffic by selecting optimize path and then extract features from traffic and then apply SAE algorithm to check normal or attack signature. If signature normal then request will be process by cloud. Here cloud will update database of machine learning model.

Here we don't have any sensor or any other edge or fog or cloud server so we are building machine learning algorithms model and then sending test signature on built model to detect whether request is normal or contains attack.

To implement this project, we are using UNSW_NB15 dataset and below screen shots showing IOT request signature from this dataset.

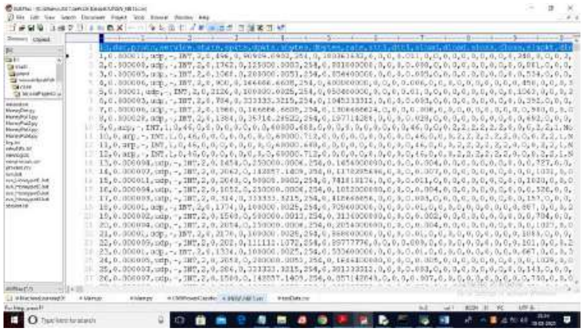


Fig.4: dataset-1

In above screen first row contains column name and other rows contains column values and in below screen in last column we can see attack or normal class label.

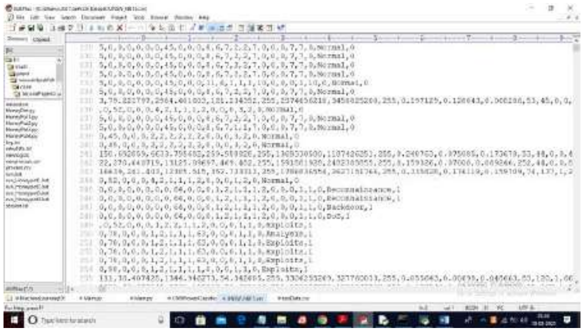
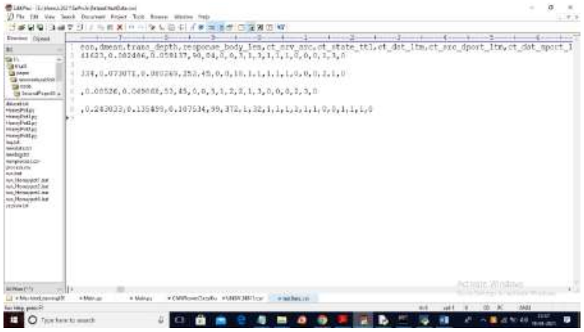


Fig.5: dataset-2

In above screen with each associate record signature we have class label as normal or attack name and we will use above dataset to build machine learning models. After building model we will use below test dataset to predict whether signature contains or normal or attack symbol.



```
eon,dmean,trans_depth,response_body_len,ct_srv_src,ct_state_ttl,ct_dst_ltm,ct_src_dport_ltm,ct_dst_sport_l
41623,0.082486,0.058137,90,84,0,0,3,1,3,1,1,1,0,0,0,2,3,0

334,0.073071,0.080249,252,45,0,0,18,1,1,1,1,1,0,0,0,2,1,0

,0.00526,0.049068,53,45,0,0,3,1,2,2,1,3,0,0,0,2,3,0

,0.243033,0.135499,0.107534,99,372,1,32,1,1,1,2,1,1,0,0,1,1,1,0
```

Fig.6: dataset-3

In the above test dataset, we can see in last column we don't have normal or attack name and when we apply above data on machine learning model then it will predict whether record is normal or attack. As we don't have sensors or edge id or cloud server to send request so we are manually uploading above test data and then making ML model to predict it class label.

ALGORITHM:

Support Vector Machine (SVM):

Machine learning involves predicting and classifying data and to do so we employ various machine learning algorithms according to the dataset. SVM or Support Vector Machine is a linear model for classification and regression problems. It can solve linear and non-linear problems and work well for many practical problems. The idea of SVM is simple: The algorithm creates a line or a hyper plane which separates the data into classes. In machine learning, the radial basis function kernel, or RBF kernel, is a popular kernel function used in various kernelized learning algorithms. In particular, it is commonly used in support vector machine classification. As a simple example, for a classification task with only two features (like the image above), you can think of a hyper plane as a line that linearly separates and classifies a set of data. Intuitively, the further from the hyper plane our data points lie, the more confident we are that they have been correctly classified. We therefore want our data points to be as far away from the hyper plane as possible, while still being on the correct side of it. So, when new testing data is added, whatever side of the hyperplane it lands will decide the class that we assign to it.

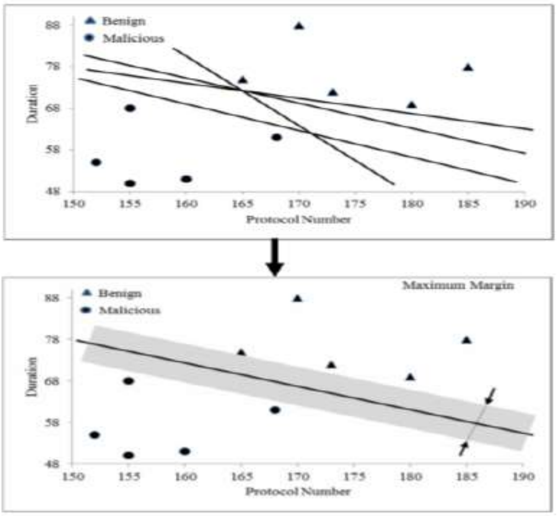


Fig.7: SVM model

5. EXPERIMENTAL RESULTS

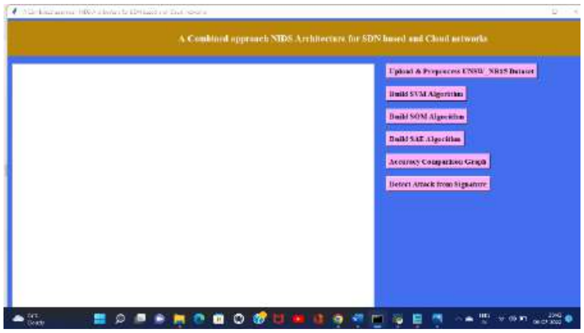

A Combined approach NIDS Architecture for SDN based and Cloud networks
Upload & Preprocess UNSW_NB15 Dataset
Build SVM Algorithm
Build SOM Algorithm
Build SAE Algorithm
Accuracy Comparison Graph
Detect Attack from Signature

Fig.8: Output screen

In above screen click on ‘Upload & Preprocess UNSW_NB15 Dataset’ button to load dataset

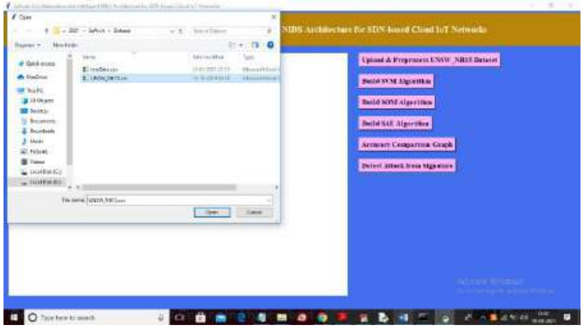
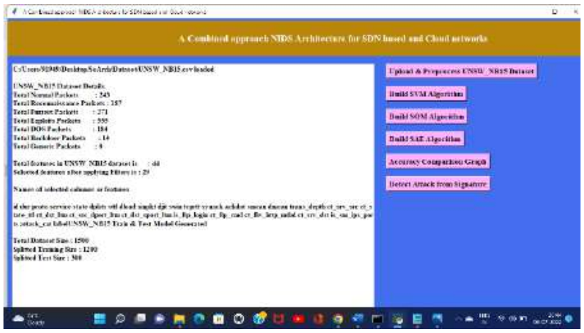

Open
File name: UNSW_NB15.csv
Open
Cancel
NIDS Architecture for SDN based Cloud IoT Networks
Upload & Preprocess UNSW_NB15 Dataset
Build SVM Algorithm
Build SOM Algorithm
Build SAE Algorithm
Accuracy Comparison Graph
Detect Attack from Signature

Fig.9: output screen

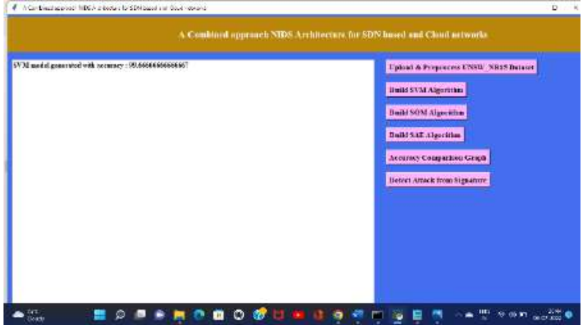
In above screen selecting and uploading ‘UNSW_NB15.csv’ file and then click on ‘Open’ button to load dataset and to get below screen.


A Combined approach NIDS Architecture for SDN based and Cloud networks
Upload & Preprocess UNSW_NB15 Dataset
Build SVM Algorithm
Build SOM Algorithm
Build SAE Algorithm
Accuracy Comparison Graph
Detect Attack from Signature

```
C:/Users/91948/Desktop/SeArch/Dataset/UNSW_NB15.csv loaded

UNSW_NB15 Dataset Details
Total Normal Packets         : 343
Total Reconnaissance Packets : 157
Total Fuzzers Packets        : 271
Total Exploits Packets       : 555
Total DOS Packets            : 184
Total Backdoor Packets       : 14
Total Generic Packets        : 8

Total features in UNSW_NB15 dataset is    : 44
Selected features after applying filters is : 29

Names of selected columns or features

id dur proto service state dpkts sttl dload sinpkt djit swin tcprtt synack ackdat smean dmean trans_depth ct_srv_src ct_s
tate_ttl ct_dst_ltm ct_src_dport_ltm ct_dst_sport_ltm is_ftp_login ct_ftp_cmd ct_flw_http_mthd ct_srv_dst is_sm_ips_po
rts attack_cat labelUNSW_NB15 Train & Test Model Generated

Total Dataset Size : 1500
Splitted Training Size : 1200
Splitted Test Size : 300
```

Fig.10: Output screen

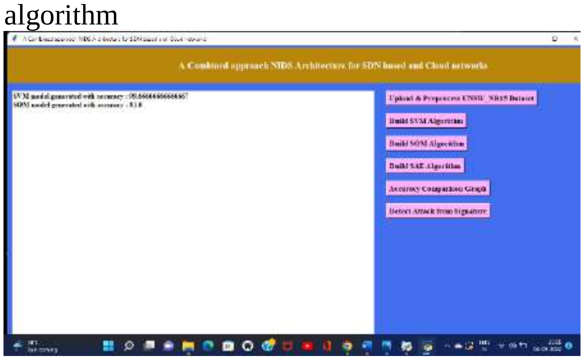
In above screen dataset loaded and in dataset we are displaying total number of normal and attack signature records and then application displaying 44 features or columns found in dataset and we are remove irrelevant features to reduce its size to 28 and then displaying column names of selected 29 features and then application using total 1500 records from dataset and to train ML application using 1200 records and to test ML model application using 300 records and now both train and test data is ready and now click on ‘Build SVM Algorithm’ button to train SVM with above dataset


A Combined approach NIDS Architecture for SDN based and Cloud networks
Upload & Preprocess UNSW_NB15 Dataset
Build SVM Algorithm
Build SOM Algorithm
Build SAE Algorithm
Accuracy Comparison Graph
Detect Attack from Signature

```
SVM model generated with accuracy : 99.66666666666667
```

Fig.11: Output screen

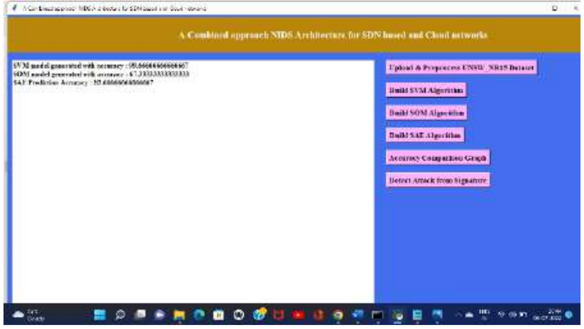
In above screen SVM is trained and we got its prediction accuracy as 100% and now click on ‘Build SOM Algorithm’ button to train SOM algorithm


A Combined approach NIDS Architecture for SDN based and Cloud networks
Upload & Preprocess UNSW_NB15 Dataset
Build SVM Algorithm
Build SOM Algorithm
Build SAE Algorithm
Accuracy Comparison Graph
Detect Attack from Signature

```
SVM model generated with accuracy : 99.66666666666667
SOM model generated with accuracy : [illegible]
```

Fig.12: Output screen

In above screen SOM got 70% accuracy and in graph we can see it created 2 clusters and some records put inside 0 cluster and some in cluster 1 and now click on ‘Build SAE Algorithm’ button to SAE model for cloud


A Combined approach NIDS Architecture for SDN based and Cloud networks
Upload & Preprocess UNSW_NB15 Dataset
Build SVM Algorithm
Build SOM Algorithm
Build SAE Algorithm
Accuracy Comparison Graph
Detect Attack from Signature

```
SVM model generated with accuracy : 99.66666666666667
SOM model generated with accuracy : 67.33333333333333
SAE Prediction Accuracy : 83.66666666666667
```

Fig.13: Output screen

In above screen SAE is trained and its accuracy is 72% and now click on ‘Accuracy Comparison Graph’ button to get below graph

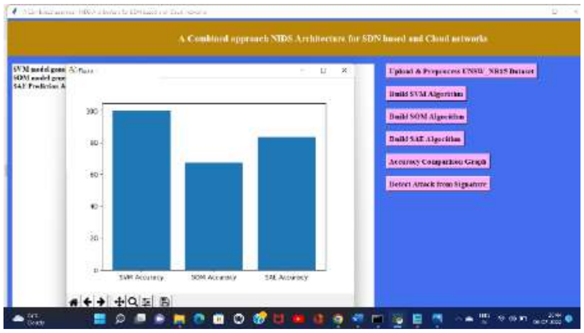
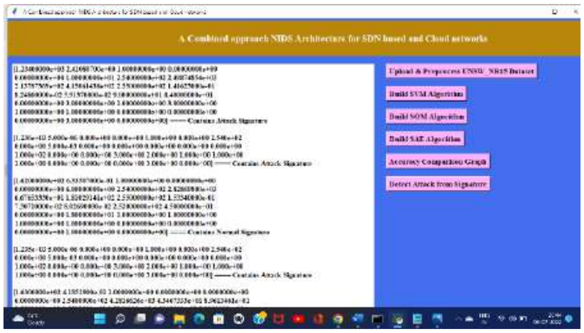

A Combined approach NIDS Architecture for SDN based and Cloud networks
Figure 1
100
80
60
40
20
0
SVM Accuracy
SOM Accuracy
SAE Accuracy
Upload & Preprocess UNSW_NB15 Dataset
Build SVM Algorithm
Build SOM Algorithm
Build SAE Algorithm
Accuracy Comparison Graph
Detect Attack from Signature

Fig.14: Output screen

In above graph x-axis represents algorithm name and y-axis represents accuracy of those algorithms and in above graph SVM got high accuracy and now click on ‘Detect Attack from Signature’ button and upload test new request signature.


A Combined approach NIDS Architecture for SDN based and Cloud networks
Upload & Preprocess UNSW_NB15 Dataset
Build SVM Algorithm
Build SOM Algorithm
Build SAE Algorithm
Accuracy Comparison Graph
Detect Attack from Signature

```
[1.23400000e+03 2.41080700e+00 1.00000000e+00 0.00000000e+00
[illegible]
[illegible] ——— Contains Attack Signature

[1.236e+03 [illegible]
[illegible] ——— Contains Attack Signature

[1.41000000e+03 [illegible]
[illegible] ——— Contains Normal Signature

[1.235e+03 [illegible]
[illegible] ——— Contains Attack Signature

[1.43000000e+03 [illegible]
[illegible]
```

Fig.15: Output screen

In above screen in square bracket, we have test signature and after square bracket we got predicted result as ‘Contains Attack or Normal Signature’.

5. CONCLUSION

In this paper, we propose a new security architecture, search, representing a collaborative and intelligent NIDS system in SDN-based cloud IoT networks, in which an arrangement of three layers of IDS nodes (Edge-IDS, Fog-IDS and Cloud-IDS) is introduced with an effective collaboration among nodes. 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 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 7.0ms on average in attack mitigation time, and tackling performance bottleneck problems as same as the DED scheme does. Additionally, the search architecture presents only a minor overhead of the system collaboration, i.e., from 8.5% to 15.0%. As our future development, we plan to investigate other machine learning/deep learning algorithms and cyber-attacks with a more massive amount of data sets and various/heterogeneous traffic types in the proposed architecture.

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. 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, 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.

[4] M. Alaa, A. Zaidan, B. Zaidan, M. Talal, and M. Kiah, “A review of smart home applications based on internet of things,” Journal of Network and Computer Applications, vol. 97, pp. 48 – 65, 2017.

[5] Y. Li and M. Chen, “Software-defined network function virtualization: A survey,” IEEE Access, vol. 3, pp. 2542–2553, 2015.

[6] C. sytems, “Cisco visual networking index: Global mobile data traffic forecast update, 2017-2022 white paper, available at https://www.cisco.com/c/en/us/solutions/collateral/serviceprovider/visual-networking-index-vni/white-paper-c11-738429.html.”

[7] H. Aldowah, S. Ul Rehman, and I. Umar, “Security in internet of things: Issues, challenges and solutions,” in Recent Trends in Data Science and Soft Computing (F. Saeed, N. Gazem, F. Mohammed, and A. Busalim, eds.), (Cham), pp. 396–405, Springer International Publishing, 2019.

[8] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “Ddos in the iot: Mirai and other botnets,” Computer, vol. 50, no. 7, pp. 80–84, 2017.

[9] V. Varadharajan and U. Tupakula, “Security as a service model for cloud environment,” IEEE Transactions on Network and Service Management, vol. 11, pp. 60–75, March 2014.

[10] I. Farris, T. Taleb, Y. Khettab, and J. S. Song, “A survey on emerging sdn and nfv security mechanisms for iot systems,” IEEE Communications Surveys Tutorials, pp. 1–1, 2018.

[11] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, “A multi-level ddos mitigation framework for the industrial internet of things,” IEEE Communications Magazine, vol. 56, pp. 30–36, Feb 2018.

[12] Q. Shafi, A. Basit, S. Qaisar, A. Koay, and I. Welch, “Fog-assisted sdn controlled framework for enduring anomaly detection in an iot network,” IEEE Access, vol. 6, pp. 73713–73723, 2018.

[13] J. Li, Z. Zhao, R. Li, H. Zhang, and T. Zhang, “Ai-based two-stage intrusion detection for software defined iot networks,” IEEE Internet of Things Journal, pp. 1–1, 2019.

[14] A. Santos da Silva, J. A. Wickboldt, L. Z. Granville, and A. SchaefferFilho, “Atlantic: A framework for anomaly traffic detection, classification, and mitigation in SDN,” in NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, pp. 27–35, April 2016.