Solid State Technology
Volume: 63 Issue: 6
Publication Year: 2020

Network Security for SDN-based Cloud IoT Using Deep Learning

A.Banushri[1*], Dr.R.A.Karthika[2]
Department of Computer Science & Engineering,
Vels Institute of Science,Technology and Advanced Studies(VISTAS), Chennai.

Abstract -The unpredictable rise of intellectual devices have significantly increased the traffic of Internet of Things (IoT) in cloud environment and produced prospective attack level. Conventional Security Structures are insufficient and ineffective to concentrate on security threats in cloud-based IoT networks. Machine Learning practices and SDN (Software Defined Networking) bring in an abundant advantage that could successfully resolve cyber security problems for cloud-based IoT systems. This paper defines an intrusion detection scheme with Deep Learning technology for SDN cloud IoT networks. This arrangement encompasses an intellectual IDS nodes present in the cloud and SDN Controller to identify the anomalies and devise the guidelines into the SDN IoT gateway devices to impede malicious traffic as speedy as possible. The system progression logic is generally investigated with the help of successive procedures such as Runtime process, Initialization and Database Update. Then the proposed system is implemented in an SDN-based environment to execute a range of try-outs. Ultimately, the assessment outcomes of the architecture give path for excellent performance in anomaly revealing, alleviation and also bottleneck problems seen in the SDN cloud IoT networks in association with existing solutions.

Keywords: Software Defined Networking, Deep Learning, Distributed Cloud Computing, Internet of Things, Intrusion Detection System.

1 Introduction

In today's human existence, the IoT (Internet of Things) brings a huge capacity for intellectual connectivity of assorted devices and apps. By offering sensing and acting capacity and consciousness, smarter devices could afford a vibrant life for humans. IoT applications have been expanded quickly due to a wide range of fresh technologies. The industrial revolution has integrated the physical components more promptly together. To facilitate, the M2M (Machine to Machine) and IoT are integrating workflows and data rapidly which forms the basis for increasing speeds of global economy. The notion of cloud computing has the capability to provide computational capability for the end users in low cost. The combination of these technologies would create a platform that would redefine the global economy very rapidly.IoT has progressively transformed the way by which regular tasks are completed [4]. For example, take smart home, where the devices at the home could be controlled remotely through their mobile phones, with the help of internet. IoT has also used as a utensil in business environments across several industries.

With the amount of big data that is being generated by IoT, a lot of pressure is put on the internet infrastructure. This has done administrations and businesses look for a decision that would condense this load. Cloud computing facilitates organizations to ingest a compute resource, like a virtual machine (VM) as a replacement for constructing a computing set-up on premise.Today, the cloud computing has pierced conventional IT and its infrastructure. Many tech bigwigs such as Google, Amazon, and Oracle are constructing machine learning tools with the service of cloud technology to provide a wide range of resolutions to businesses worldwide.IoT and Cloud computing work towards

improving the efficiency of everyday responsibilities and both have a corresponding relationship. By assisting developers to store and access data remotely, the cloud permits developers to implement the projects without any deferment. By stowage of data in the cloud, a large amount of data could be accessed by IoT companies [9].

A new category is evolving for security within next-generation backgrounds called software-defined security. The SDN could contribute network engineers to dynamically change the performance of a network on a node-by-node basis which is not normally obtainable in a traditional network. An SDN relates virtualization to modernize the supervision of network resources and provides a resolution for the increased capacity without expressively increasing expenses [1]. Network functions virtualization deals with a different manner to establish and to undertake SDN network protection by decoupling the network function such as intrusion detection and firewalling from the exclusive hardware appliances. It is anticipated to dispense the networking mechanisms needed to provision a fully virtualized infrastructure. As societies make use of SDN, there is a risk of exposing new types of attacks and threats in their network. A leading anxiety with SDN security makes emphases on the SDN controller. The controller gives cleverness for the entire network. The SDN controller is the main part for because the active assaults on the controller could completely disrupt network operations [1]. To battle those attacks, an association could configure role-based authentication which assures that the right people get access to the data and the applications. SDN-based protection apps would promptly gain traction to fight against cybercrime. SDN could commence to gather network facts, which might provision progressed algorithm design to detect attacks.

The innovative assertions may take advantage of SDN agents for the progress of policy enforcement and traffic abnormality detection and alleviation. Those apps are furnished to block mischievous intruders before they could enter the acute regions. As network controls have evolved from hardware to software and the effect is that the several devices are fused into the controller, that make things easier for the network engineer to regulate the complete network [9].A substantial issue concerning SDN security is that all part of the network infrastructure virtualization raises the attack footprint [2]. The utmost substantial aim for the invaders is the SDN controller because; it is indispensible circumstance for inferences and also for the failure. Attackers might crash to procure control of the network by breaching into a controller or play-acting to be one. If a substantial controller is permissible, an interloper could procure whole control of the network. This might be considered as an astonishing situation, but it could be promising as SDN custom develops [8]. The DoS attacks could take advantage of potential scaling limits of SDN infrastructure by tracing definite automatic processes that might use a substantial amount of CPU cycles. As the control and data planes are separate in the SDN network, it is unpredictable to attacks. An interruption in the communication path between these two planes possibly results in a chief hole that the attackers could negotiate. It is substantial to use high-accessibility controller architecture to preclude distributed denial-of-service (DDoS) attacks [1]. Section II provides the details of SDN-based cloud IoT network threats. Section III presents the proposed architecture and Section IV deals with results and discussion. Finally, section V gives conclusion and suggests some future developments.

2 Sdn-Based Cloud Iot Network Threats

Cloud background for IoT networks not only provides connectivity between IoT applications and devices but also distributed resources and stowage. Consequently, some realistic security disclosures have been demoralised recently by the attackers. The network attacks which are indicated in this

paper are (1) Distributed Denial-of-Service attack (DDoS) (2) Worm Hole attack and (3) Sniffing attack.

2.1 DDoS Attack

This attack involves computer networks from all over the universe. Distributing the attack amplifies it and makes it more problematic for the affected party to safeguard itself. The attackers use botnets, i.e, numerous computers, would act under the control of a mischievous group or individual. Botnets are produced by the fixative of malware without user's awareness. The ultimate risky cyber threat is DDoS attack in cloud IoT environment .Overflowing of network links and the IoT equipments with a massive traffic could rapidly dissipate network and computational resources causing unreachability of the IoT communication system. Worthy features of SDN offer new opportunities to overthrow attacks in cloud computing surroundings. Among the security inevitabilities of cloud computing, accessibility is vital since the key task of cloud computing is to afford on-demand facilities at different stages. DDoS attacks are an action to create a machine or network resource unreachable to its intended users [2].Although the competences of SDN makes it possible to discover and to counter DDoS attacks in cloud surroundings. The partition of the data plane and control plane in SDN presents different attack planes.SDN itself, a goal for definite attacks, and prospective DDoS exposures occur through SDN platforms. The trespasser can make use of benefits of SDN to introduce DDoS attacks beside all the three layers of SDN [5].

2.2 Wormhole Attack

Wormhole attack could alter the network even without the awareness of cryptographic procedures implemented.For this reason it is very challenging to detect the attack. It might be thrown by one, or more number of nodes. If there survives two ended wormhole, the packets might be directed over wormhole link from source to destination node. When the packets are acknowledged by destination node, it replicates them to the other end. A wormhole attack that take advantage of collaboration/ collusion between two malicious nodes to speedily send the information, with the aim of destruction of the routing protocols which depend on speed of wireless transmission [7]. The control messages are transferred from a node to a destination node, to make certain the optimum route on the network.With the support of the protocols the anticipations are made to find the fastest / shortest routes that are obviously identified by viewing the messages arrived at the destination first. Successively, once the beacon message has attained the endpoint, the route is anticipated to be found. Any other beacon messages that arrive later are expected to signify as suboptimal routes and it is discarded [6].

Assume that there are two attackers A & B, and two nodes in the network that are connected like the following:

Sender- - - AttackerA ——— AttackerB - - - Receiver

Then the Attacker A node could take a beacon and send it along the network to AttackerB, which then delivers it to the destination node faster than any other normal route relying on all other wireless hops. Thus this route including the two attack nodes will be recognized as the shortest and utmost ideal path. Potentially any one can use this capability to develop the shortest path across the network. The Attackers could drop the traffic, could sniff/alter traffic, or could accomplish advanced attacks on top. This attack could be rectified with the help of SDN network.

2.3. Sniffing Attack

Sniffing attack, in which a device or a program takes imperative statistics from the traffic of network. The rudimentary objective of sniffer is to find out delicate evidence of the user, which compromises the secrecy. Server Side Sniffing take advantage of protocol like http and the Sniffer outbreaks the server statistics. In Browser Sniffing, the websites are used to regulate the web and produces several wicked activities like cascading style sheets, misinterpretation of HTML, etc. The static network in conventional method provide suitability for sniffer attack. The static configurations and route information makes the attacker to analyse and get the network data.SDN could bring new technique to comprehend dynamic pattern. SDN splits the forwarding plane and the control plane and relates centralized logic control. The dominant control and the management of network ability makes the SDN to realize the dynamic network further flexible.

The SDN has programmable nature which is used to control the flow table directly for the forwarding devices and avoids routing inflation and service intermissions. The global view of the entire network could be controlled by centralized SDN and so it could realize the changes of multiple network. We can style the SDN to make variation in the communication information and the routing paths of both ends. This might make difficult for the attackers to separate the data of a particular user among many user data. Difficulty in analysing and to getting the data will be increased for the attacker to execute the target sniffing.

3 Proposed System Architecture

The existing system is Support Vector Machine (SVM), which is used for regression challenges and also for classifications [3]. The proposed system is Deep learning, which is more powerful than SVM. Linear Regression algorithm based on Deep learning technique is used to detect the invaders. The proposed architecture consists of three layers namely Network, Application and Perception layer. The Application layer consists of IoT applications and storage. Network layer comprises application servers, SDN IoT gateways, SDN Controllers. Perception layer comprises IoT objects. The proposed Architecture consists of Intrusion detection system in the cloud itself, to detect the intruders and it is named as Cloud-IDS. In the network layer, the IDS is present at the Controller to detect and mitigate the attackers and it is named as Controller-IDS. The Controller-IDS and cloud-IDS works under the concept of Deep learning (DL) system to predict the intruders. The simplification power of DL-based techniques is better than traditional ML-based methods and the DL based system could even discover zero-day malware. Any considerable aberrations from the baselines can be elicited as an anomaly that raises warnings, which is enquired by the safety analysts. Nowadays, deep learning-based schemes are used to identify several categories of anomalies. Linear Regression algorithm based on Deep learning technique is used to detect the invaders. The Linear Regression is used to predict a continuous, mathematical value depends on the given data input and this algorithm is a Supervised Learning algorithm**.** Each data sample is a point, from the geometrical perspective. Linear Regression tries to discover the parameters of linear function and the distance between the line and all the points is as small as possible**.** Gradient Descent Algorithm is used for parameters update. Regression study evaluates the relationship between an independent variable and the dependent variable. The foremost uses of regression analysis is to define the strength of predictions, forecasting the consequences and trend forecasting.

In order to minimize the security issues, the proposed intellectual IDS architecture for SDN based cloud IoT networks is shown in Fig.1. The security architecture contains IDS such as Cloud IDS and

Controller IDS. The IDSs present in the same computing level could be in the distributed arrangement. In particular, Controller-IDS are installed as an SDN app above the SDN controllers, and Cloud IDS is an IoT security application running on the cloud with enough storage resources and computation. Similarly, Fog-IDS and Cloud-IDS set up their passages to send and receive data. The main intention behind this arrangement is to lessen the information exchange latency and to evade outage complications. The higher layers must primarily perform information/data exchange and the edge devices must concentrate on handling IoT traffic. In concise, the main responsibilities of Fog-IDS are to aggregate and extort received data to develop a set of preferred characteristics, and then feed this description into deep learning-based engine for anomaly revealing. Consequently, it makes guidelines and relates to the committed SDN-based IoT gateway if feasible. Otherwise, it directs to a Cloud-ID for further sophisticated analyses concerning unrecognized traffic designs. The Fog-IDS could load balance with its Fog-IDS neighbours in case of an outage condition caused by a huge amount of data progressed from the Edge nodes. A Cloud-IDs is referred as cloud-based revealing engine at the cloud computing layer running as IoT applications with unlimited resource supply, which could be fashioned in a distributed style. The essential engine of Cloud-IDS could activate deep learning-based detection algorithms. Hence the result of the finding is alleged as the most mindful of the traffic design which is directed from Fog-IDS. Cloud IDS sends suitable strategies to Fog-IDS for instantaneously preventing wicked traffic flows which is produced from IoT networks. The IDS engines in this security mechanism are instigated simply as virtual machines with the flexibility of SDN/NFV technologies.

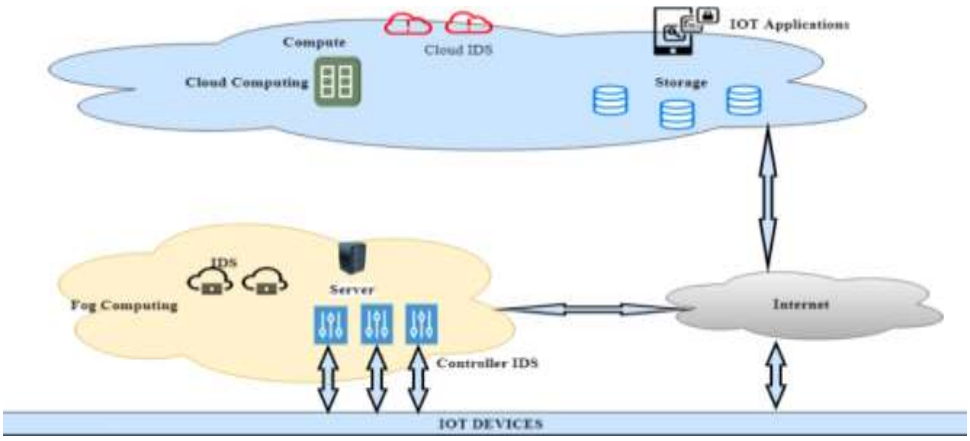

Fig. 1. IDS architecture for SDN based cloud IoT Networks

Let N be the set of nodes, which distribute traffic based on usage of resource of each IDS node.

VRi be the Virtual resource provided by physical servers of IDS node i.

VRi ∈ {vMemory, vCPU} and VRi <=Rmax(i),where Rmax(i) is the capacity at node i.

Let Bw (ji) be the bandwidth transferred from node j to i.

The total bandwidth between the two nodes i and j must be Bw (ji) + Bw (ij).And this bandwidth should not be larger than the capacity of full duplex link.

Let D be an IDS node, where D ∈ N

Let DRi (Bi) be the usage of resource R, processing bandwidth Bi (Mbps) of IDS node i,

Where $Bi \leq Bmax(i)$ and $DRi\ (Bi) \leq Rmax(i)$, $\forall VRi \in \{vCPU,vMemory\},i \in N$

In order to avoid overload and to make load balancing decision, this formulation is used to calculate maximum traffic incoming on an IDS node.

Let S_{IDS} and C_{IDS} be the set of IDS nodes at SDN level and cloud level. Where $S_{IDS,\ CIDS} \in N$.

Bw(i) be the total bandwidth incoming at IDS node i for certain time.

Then calculate Bw(i),$D_i^{vCPU}(Bw(i))$ and $D_i^{vMemory}(Bw(i))$.

If $(D_i^{vCPU}(Bw(i)) \leq vCPU_i^{max})$ and $(D_i^{vMemory}(Bw(i)) \leq vMemory_i^{max})$ then continue,

Otherwise Forward ΔBw(i) to each SDN-IDS or Cloud-IDS .

Then extract features from the left over data amount and feed the inputs to the SDN-IDS.If the consequence is normal, carry on the process. If the consequence is malicious, request for the policies. Accelerate it to the associated cloud-IDS and send the report to the Cloud admin.

3 Results and Discussion

Maxinet is used as a distributed SDN emulator with 3 physical machines. In each machine, OpenvSwitches are set up for running SDN-based IoT gateways with some edge nodes and some container based nodes are distributed. For SDN controller, ONOS is chosen. For cloud set up, 2 physical machines are used, which is connected to SDN network with the help of L2 switches. Diverse attacks such as DDoS attack, Wormhole attack and Sniffing attack are launched to the proposed system. IDS nodes are skilled for abnormality detection based on to their consistent IoT traffic patterns. The Controller-IDS node gathers traffic info from the SDN based IoT gateway devices and makes its discovery. If there is an overload, then the SDN-IDS node makes a balancing of load with Cloud-IDS node for further progressive analyses. Attack alleviation enactment depends on average detection time of new attack, fallen malicious packets, Policies accompanied to increase the quality of traffic flow in SDN-based IoT gateways. Fig. 2. displays the No. of plunged packets at the time of attack, which is compared between linear regression and SVM. Fig. 3. displays the No. of Packet-In, which is focussed to the SDN network during attack. In both the cases, linear regression is more efficient than SVM.

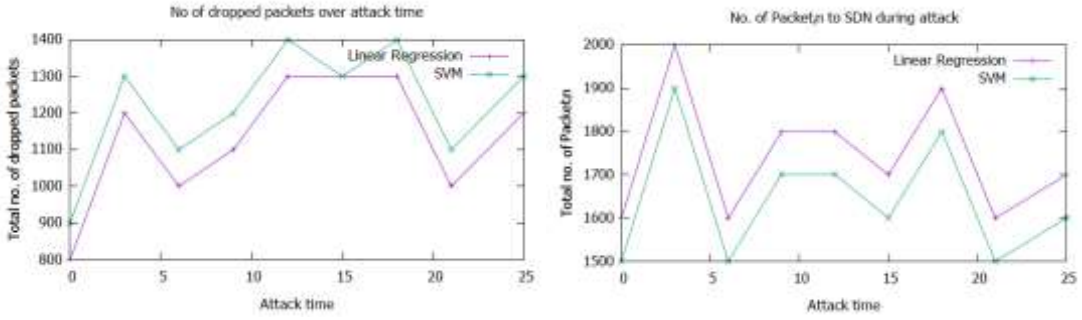

Fig. 2. No. of dropped packets over attack time **Fig. 3.** No. of Packet_In (message) to SDN during attack

5 Conclusion

In this paper, security architecture is proposed for SDN-based cloud IoT networks. In this arrangement, the cloud IDS and the SDN IDS are introduced for an operational teamwork among nodes. This system encourages the usage of deep learning technique for perceptively identifying network-related threats for IoT devices. A comparative study is made using linear regression and SVM algorithms. The performance of the proposed linear regression is based on the average detection rate and accuracy. From the study, it is obvious that the linear regression is more efficient than SVM. For future development, other deep learning algorithms could be implemented and more data sets could be used with different traffic patterns.

References

1. Qiao Yan, F. Richard Yu, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges", IEEE, 2015
2. Normaziah A. Aziz, Teddy Mantoro, M. Aiman Khairudin, A. Faiz b A. Murshid, "Software Defined Networking (SDN) and its Security Issues", 4th International Conference on Computing, Engineering, and Design (ICCED), IEEE, 2018
3. TRI GIA NGUYEN, TRUNG V. PHAN, "SeArch: A Collaborative and Intelligent NIDS Architecture for SDN-based Cloud IoT Networks", IEEE, 2019
4. Weiqi Dai, Pengfei Wan, Weizhong Qiang, "TNGuard: Securing IoT Oriented Tenant Networks based on SDN", IEEE, 2018
5. SHI DON , KHUSHNOOD ABBAS, AND RAJ JAIN, "A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments", IEEE, 2019
6. Roshani Verma, PROF. Roopesh Sharma, "New Approach through Detection and Prevention of Wormhole Attack in MANET", International Conference on Electronics, Communication and Aerospace Technology ICECA 2017
7. Mousam A. Patel, Manish M. Patel, "Wormhole Attack Detection in Wireless Sensor Network", IEEE, 2018
8. Samir Kumar Tarai , Samar Shailendra, "Optimal and Secure Controller Placement in SDN based Smart City Network", IEEE, 2019
9. Ivan Farris, Tarik Taleb, Yacine Khettab, and JaeSeung Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems", IEEE, 2018
10. Anubhi Kulshrestha, Sanjay Kumar Dubey , "A Literature Review on Sniffing Attacks in Computer Network", International Journal of Advanced Engineering Research and Science (IJAERS), 2014