Turkish Journal of Computer and Mathematics Education *Vol.13 No.03 (2022), 274-281*

Research Article

Securing Private Cloud Using Deep Neural Network. Review Case

Ohoud Alshabib [a] ,and Dr. Ayman Mohamed Mostafa[b]

[a] Student, Jouf University, Department of Cybersecurity, College of ComputerScience and Information ,Al Jouf,KSA

[b]Assistant Professor of ComputerScience, College of ComputerScience and Information ,Al Jouf,KSA

Abstract: Due to the commonness of public cloud, few research publications discuss the applicability of the proposed Deep Learning solutions to private cloud systems. Companies can now explore a wide variety of resources and applications, which were not possible a few short years ago. One of the most sought-after and sought-out resource is private cloud. Private cloud is a term that has come to represent the use of network computing for an exclusive, private use. Also, has opened up newer avenues for Distributed Denial of Service (DDoS) attacks. In this paper, we discussed how to access the security and protection of the private cloud from a type of DDoS attack using one of the deep learning algorithms, LSTM approach. Through this solution, we propose to protect the private cloud in the work environment of Google.

Keywords: Security Private Cloud Computing, Distributed Denial of Service, Deep learning algorithm.

1. Introduction

The existence of the concept of cloud computing in the world of the Internet has helped reduce the costs of all the consequences of the infrastructure, so all organizations have the ability to control all cloud resources through the network and therefore the infrastructure will be distributed in nature, which makes it central and then exploit attacks as Distributed Denial of Service this point to attack or intrusion (**K.B. Virupakshar et al.2020**).

The distributed denial of service attack is one of the most famous attacks on the cloud computing. Therefore, this work will focus in this paper on studying the protection of private cloud infrastructure and services using the Deep Neural Network Approach.

The private cloud infrastructure includes several advantages, including efficiency in both backup and recovery, storage space and cost, lighter movement and scalability, including the diversity and multiplicity of devices and many advantages (**K.B. Virupakshar et al.2020**).

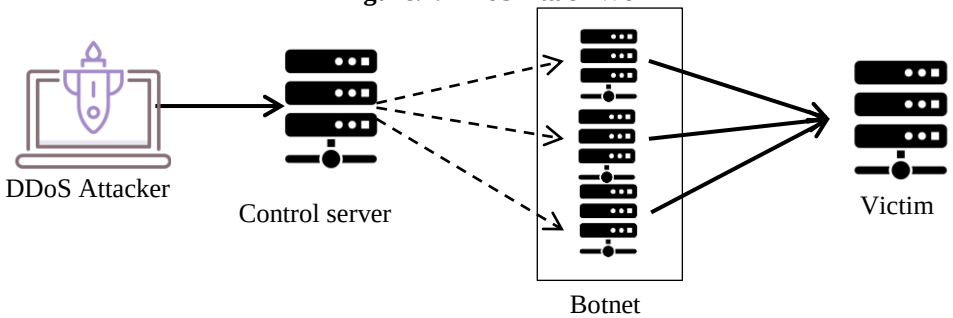
The idea of the private cloud computing came to change the idea of some traditional organizations to this innovation. This type is considered a basic building block for every private institution or even benefiting from the service for a group of people.

One of the basics of configuring this type of cloud is storage and management as well as managing applications, network and servers. It is usually managed internally, but it can be managed externally through a Managed Service Provider (MSP) (**R.M.Pir et.al.2020**).

Consequently, detection of such attacks in the cloud requires that extraordinary attention be paid. Moreover, the firewall alone cannot adequate to counter DDoS attacks, so the chairman requires an extra interruption detection system supplementing the firewall in arrange to distinguish DDoS attacks (**Sh.Gumaste et.al.2020**).

As appeared in **Figure.1**, the attacker employments a command and control centre and the botnet to perform a DDoS attack on the casualty machine. The foe machine indicates the assault sort and the victim's IP address to the command and control server. At that point, the command and control server sends this data to the botnet arrange. Numerous machines comprising the botnet network send a stream of attack demands to the casualty machine, by throwing an off-base input or by sending a colossal number of requests at the same time. Indeed after the casualty server reacts to this ask, the botnet machines toss the same request once more and once more. In this way, assets of the victim server will be depleted, the server crashes and its execution debases (**Sh.Gumaste et.al.2020**).

Figure.1. DDoS Attack Work



In this paper, the solution depends on the use of the deep neural network approach to detect the distributed denial of Service attack in private cloud computing .Deep Learning algorithms are utilized to classify traffic parcels and to anticipate interruptions. Choice of the Appropriate Deep learning algorithm for each dataset is a critical issue. So one must select the correct algorithm (**Sh.Gumaste et.al.2020**).

This paper is organized as follows: The second section reviews previous literature that contributed to security of private cloud. While in the third section, we will discuss the Security in private cloud computing. After that in the fourth section, we identify the research methodology. The fifth section, we discuss the solutions in details. The seventh section we build a security private cloud, and finally, the conclusion comes with the references.

2. Literature review

Researchers (**B.Khadka et.al.2015**) , recognize the characteristics of a DDoS attack and give an Interruption Discovery Framework (IDS) tool based on Grunt to distinguish DDoS. The framework is Proposed which can caution the organize director regarding. Any assault for any conceivable assets and the nature of the attack. Moreover, it suspends the assailant for a few time to allow the arrange admin to actualize a fallback arrange. The Proposed instrument makes a difference minimize the effect of DDoS by detecting the assault at an early arrange and by modifying with different parameters, which encourage to effortlessly analyzing the issue.

Researchers (**N.D G et.al.2016**), examine the cloud design and its plan. Also talks about the significance of recognizing DDoS attacks at the network layer. This paper proposes machine and deep learning calculations to be specific Choice tree, Naïve Bayes, DNN, and KNN to distinguish DDoS attacks in SDN. At this point, these algorithms are assessed utilizing parameters such as detection rate and productivity.

Researchers (**S.R.M.Zeebaree, and y.sufyan.2020**),(**A. N. Asadi et.al.2019**) recognize that cloud computing has become a very important and even very important role, and in their research they focused on the problem of security and what vulnerabilities and attacks can cause within it. Their Study aimed at an overview of everything related to the house, including its advantages, disadvantages, and different types.

Researcher (**A.Caballero.2017**), provide few strategies that can increase the transfer speed, upgraded, organizing, and capabilities of computing. The cloud computing permits the clients with high speed of looking with long execution. On the other hand, it gives boundless assets, which mean the high-performance computing (HPC), too analyzing massive data by running multi-machines at the same time. Some companies can analyze tremendous information with a fast scalable enhancement arrangement on cloud computing.

Researcher (**AnalyticsVidhya.2021**) examine Proposed an expository show and numerical evaluation for the execution and control of cloud infrastructure by utilizing the stochastic compensate nets (SRNs). The reason of making such a framework is to Analyze the influence of organize traffics and temperature on the execution and strength of cloud computing frameworks, which was dismissed in the larger part of approaches that have been displayed previously. In the purposed plan, there are two categories for incoming tasks: hot and cold, showing different vitality consumption patterns, which seem fall flat since of the activity and bandwidth constraints. By actualizing the purposed framework, when cold and hot errands are relegated to virtual machines and taking into Consideration the organize activity, there is the capacity to compare and assess different asset assignment techniques in terms of performance and control.

3. Methodology

Considered that deep learning is part of machine learning, but it has advantages that make it superior, including automatic learning through computer algorithms, also depends on artificial neural networks, which are designed to resemble human thinking, and they are characterized by lack of complexity (**Machine Learning Mastery.2021**). The Artificial Neural Network (ANN) that creates up Deep Learning is classified as a type of network and each layer in it speaks to complex operations, which made numerous companies surge to utilize it to execute modern business models (**J.Delua and IBM.2021**).

The security measurements on cloud computing can contain different layers for detecting threats and attacks (**Y.Taguri et.al.2021**). In the first layer or input layer, the input data includes DDoS attacks will be known to us. For example, DDoS attack in private cloud for and small or big organization, university. In the second layer that is called the hidden layer, the intrusion detection systems (IDS) and intrusion response systems (IRS) are applied to detect anomalous behavior on cloud services. The last layer that is called the output layer will explore the resulting values that will be categorized and detect DDoS attacks.

With deep learning, many operations will be applied between the input and output layers in the hidden layer. The famous deep learning algorithms in briefly as follows(**Machine Learning Mastery.2021**):

- Artificial Neural Network (ANN).

- Convolutional Neural Network (CNN).
- Recurrent Neural Networks (RNNs).
- Long Short-Term Memory Networks (LSTMs).
- Stacked Auto-Encoders.
- Deep Boltzmann Machine (DBM).
- Deep Belief Networks (DBN).

There are two types of deep learning methodologies, supervised and unsupervised deep learning. These types are explained as follows:

1. Supervised learning: In this approach (**J.Delua and IBM.2021**), the method of work depends on a set of classified data, and these data are subject to supervision to predict the results with high accuracy. By using the input and output elements, the accuracy of this model can be known over time. Supervised learning is divided into two parts:

- The Classification: is used to set the data obtained. For example, separating spam in a separate folder from the inbox in the email. Therefore, these words do not appear while browsing the program and the inconvenience that results.
- The Regression: is used to understand the relationship between the dependent and independent variables to give accurate numerical ratios such as forecasting the percentage of sales for a business.

2. Unsupervised learning: In this approach(**J.Delua and IBM.2021**), the method of work depends on discovering invisible patterns of data without supervision without human intervention. The unsupervised learning is divided into three parts:

- Clustering part: the role of his work comes in order to know how to collect data that is in an indefinite state based on similarities and differences.
- Association part: which is in order to know all the relationships between all variables. For example, if you purchase a product, it will suggest or recommend to you “others have bought this product too.”
- Dimensionality part: that is used for reduction in a simplified form. Examples of this type are the algorithms that work to clarify an image or remove the blurring part so that the image appears with high accuracy.

4. Discussion

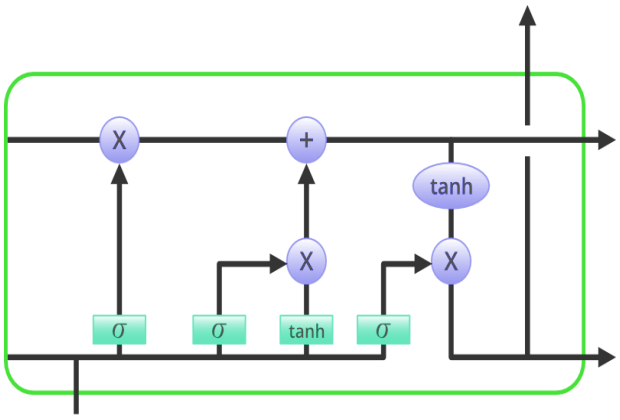
Deep learning works in a way that the computer works in reaching results through prior training on the available examples and this thing has been enabled deep learning by reaching and producing impossible results. As for the rest of the learning tools, they work as pivot machines behind many applications, and many more. The framework of a deep learning computer is automatic, and it is trained to classify and isolate tasks from each other, whether they are text, sound or images, in addition to that, deep learning guarantees you accuracy and wonderful performance that surpasses human work.

The development of cloud computing is noticeable and the issues of privacy for providing safety for the cloud infrastructure should be applied from many types of attacks.

Distributed Denial of Service (DDoS) have received great attention for many specialists, and therefore we will use one of the deep learning algorithms to protect the private cloud computing, namely Long Short-Term Memory Networks (LSTMs).

This algorithm is designed to address many problems and provides us with the advantage of retaining information for a long Time compared to other algorithms. Moreover, as we can see in **Figure. 2**, it use of cells that allow storing information, for example, the private cloud computing for a longer period outside the regular flow and in this is a security to protect data or information from a Distributed Denial of Service attack.

Figure. 2. LSTMs Algorithm. Google figure

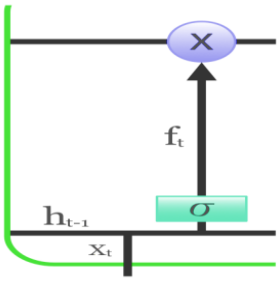


The LSTM contains different gates: the forget gate, the input gate, and the output gate (**aakarsha_chugh.2019**). These gates are explained as follows:

- The Forget gate has the property of removing information that does not have meaning or information in which a kind of DDoS attack in order to complete the performance of its task, and this step is very necessary as a first step to improve the performance of the private cloud (**Y.Taguri et.al.2021**). The forget gate will have two entries:
  - The first **(x_t)** to be entered at a certain time for the cell.
  - The **(h_{t-1})** it is the output of the previous cell.

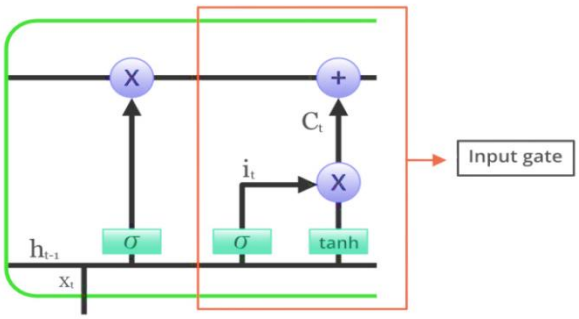
These two parameters are multiplied by matrices called weight matrices in addition to biases then the output will be passed through the activation function whose results are binary i.e. either zero or one and if the cell output is zero, the data will be forgotten. If the output is the one then the data will be saved for future use as shown in **Figure. 3**.

Figure.3. Forget Gate of LSTMs. Google figure



- The Input gate is used to add information related to private cloud, for example, to the concerned cells. After that, the information that is free from the ddistributed denial of services (DDoS) will be entered into the input portal. Input information will be organized by the sigmoid function method and it will be filtered out that information that must be remembered according to the forgetting gate by the method of the main parameters **(x_t)** and **(h_{t-1})** as shown in **Figure. 4**.

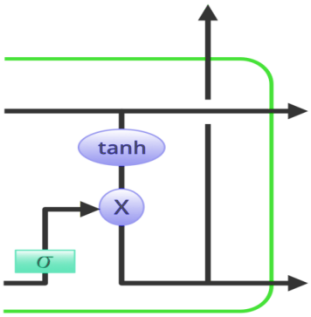
Figure. 4. Input gate of LSTMs. Google figure



- The output gate is used to extract information. The extracted information will be identified and classified. For example, information about DDoS attack or other matters related to this type. As for the information that is not necessary, it will keep it and will never remove it, so that it is not subject to the presence of a particular attacker.
  A cell vector will be made through a function application **(tanh)** that will be organized by the method of the sigmoid function. The information that must be remembered will be filtered according to the forgetting portal by the method of the main parameters **(x_t)** and **(h_{t-1})**.

The last step will be to multiply the values that came from the vector and by the method of the function **(tanh)** and then take it out intact from any attack and enter it safely into the next cell as shown in **Figure. 5**.

Figure.5. Output Gate of LSTMs. Google figure



In this paper, we will cover three methods to build a more secure private cloud:

- **Ensure performance of virtual security:**

One of the reasons why most data breaches remain undetected for quite some time is the large volume of traffic in private cloud data centers. This means that the devices must work consistently in both physical and virtual factors, and not only start with devices that are safe, high-intelligence and faster. Regardless of where they are deployed, seamless communication is a top priority for security platforms to ensure consistent policy application in addition to securing complex, cloud-based traffic and configuration necessities.

- **Automate cloud security:**

Because data is constantly changing, it is not possible for human IT managers to keep up. Reactions to changes in the network and security holes are developed for the possibility of predicting and exploiting them by security solutions. Alternatively, it is necessary to integrate the core-computing infrastructure with the security solution directly so that when dynamic changes occur in the network and security topologies at the same time.

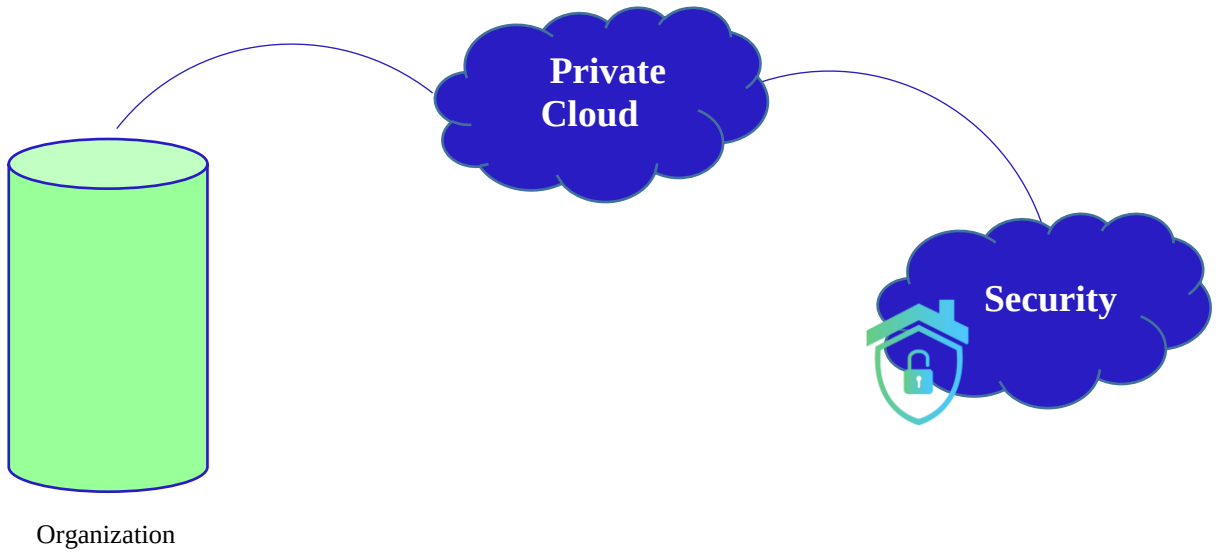
- **Integrate security for the dynamic cloud:**

It is important for organizations to implement a comprehensive and integrated security architecture to ensure a holistic view of the single part and a control system for the Entire cloud environment.

Moreover, the cloud service owner must also work on defense points to ensure the security and integrity of their organization's cloud to reduce the success points for intrusion like DDoS and access to these services. In addition, consideration must be given to encrypting the information that must be stored on the cloud in order to ensure the security of the data at a high level.

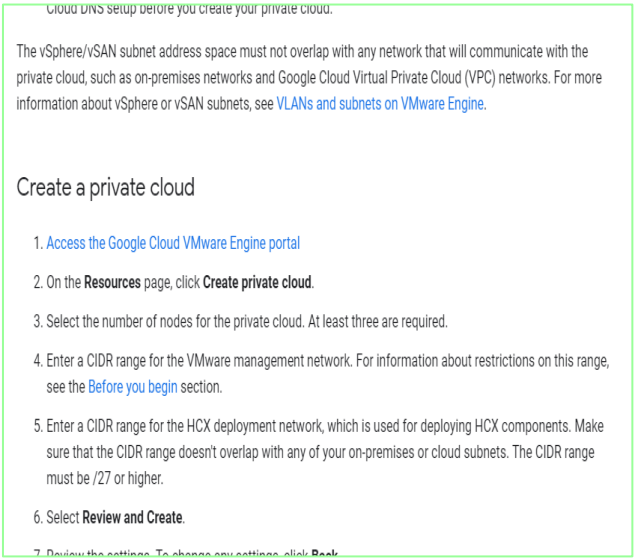
As shown in **Figure. 6**, the necessity to backup data in case the data is lost accidentally is highly important. In addition to using virtual private networks (VPNs), virtual local area network (VLAN), as well as Intrusion Prevention Systems (IPS) and intrusion detection systems (IDS) are also applied.

Figure. 6. Secure Private Cloud Scenario.



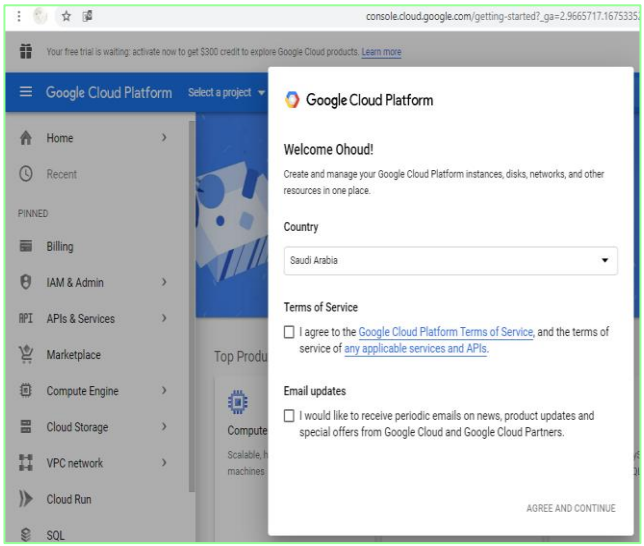
Therefore, the main steps in this paper is to create a private cloud using the Google environment as shown in **Figure. 7**.

Figure. 7. Step 1: Create Private Cloud



In the next step, we will be asked to log in by relying on Google platform as shown in **Figure. 8**. We will choose the region, agree to the terms, and continue to build the cloud after pressing the agree and continue button.

Figure. 8. Step 2: Build Private Cloud



Then we will move on to creating our private cloud as shown in **Figure. 9, 10, and 11**.

Figure. 9. Step 3: Go to the Private Cloud

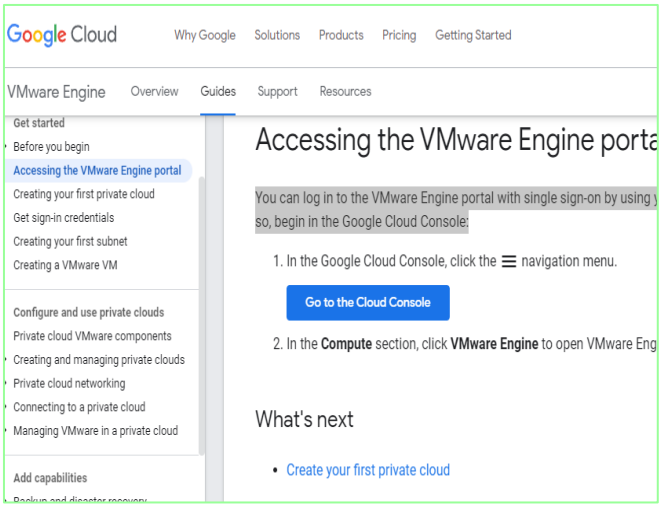


Figure. 10.VMware Engine API in Google Environment

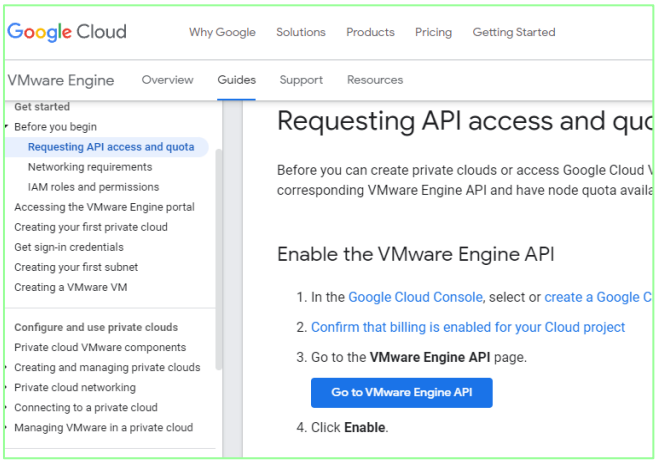
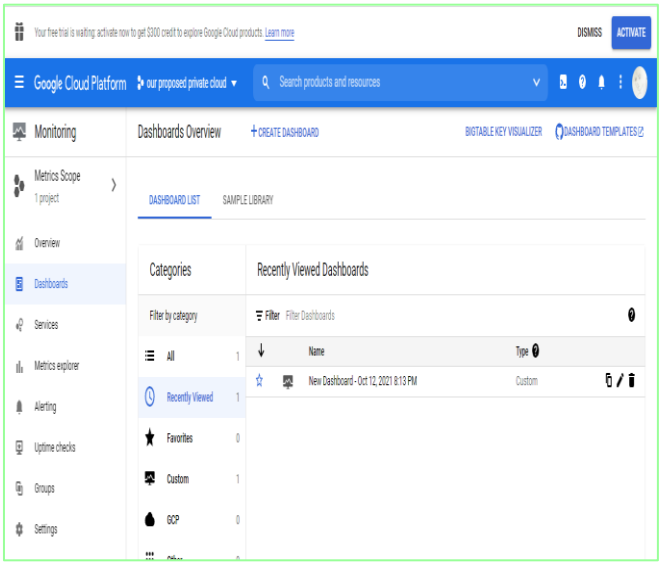


Figure. 11. Proposed Private Cloud



After creating the private cloud in this paper using the Google environment, there may be risks in building it on large public servers, but we can say side by side in using a deep learning LSTM algorithm to addressing a distributed denial of service attack, this may help reduce the damage or risks involved.

5. Conclusion

In this paper has been discussed at the beginning about the concept of cloud computing, and it helped greatly in reducing the costs of the infrastructure, so we see that most organizations or companies have control over all resources through the network, and therefore they can be exploited for a type of attack, which is DDoS. This study focused on this type of DDoS attack because it is one of the most popular types of attack, and we focused on how to protect the infrastructure, including cloud services for the private cloud, using deep learning.

We have discussed security in the private cloud and how deep learning LSTM algorithm works. Finally discussed how to protect with this type of deep learning and how to build a private cloud insecurely for the algorithm-chosen approach to protecting against distributed denial-of-service attacks.

6. Acknowledgement

The authors would like to thank the Deanship of Graduate Studies at Jouf University for funding and supporting this research through the initiative of DGS, Graduate Students Research Support (GSR) at Jouf University, Saudi Arabia.

References

K.B. Virupakshar, M.Asundi , K.Channal, P.Shettar, S.Patil, and N.D. G.(2020) “Distributed Denial of Service (DDoS) Attacks Detection System for OpenStack-based Private Cloud ” International Conference on Computational Intelligence and Data Science (ICCIDS) , (167), 2297-2307.

R.M.Pir , R.M.S.Pir , and I.U.Ahmed .(2020) " A Survey on Build Private Cloud Computing implementation tools" , Journal of Emerging Technologies and Innovative Research (JETIR) , (1) ,194-201.

Sh.Gumaste, N.D. G., S.Shinde, and A.K .(2020) " Detection of DDoS Attacks in OpenStack-based Private Cloud Using Apache Spark ", journal of telecommunication and information technology , 1-10.

B.Khadka, Ch.Withana, A.Alsadoon, and A.Elchouemi.(2015) "Distributed Denial of Service attack on Cloud Detection and Prevention. School of Computing and Mathematics" , Charles Sturt University International Conference, 1-5.

N.D G, M.M.Mulla, L.Barki, A.Shidling, and Ni.Meti.(2016) " Detection of Distributed Denial of Service Attacks in Software Defined Networks" , Intl. Conference on Advances in Computing, Communications and Informatics ,1-3.

S.R.M.Zeebaree, and y.sufyan .(2020) "State of Art Survey for Significant Relations between Cloud Computing and Distributed Computing" , International Journal of Science and Business ,53-61.

A. N. Asadi, M. A. Azgomi, and R. Entezari-Maleki.(2019) “Unified power and performance analysis of cloud computing infrastructure using stochastic reward nets,” Comput. Commun., (138), 67–80.

A.Caballero .(2017) " Information Security Essentials for Information Technology Managers " , Computer and Information Security Handbook (Third Edition).

AnalyticsVidhya .(2021) " Introduction to Supervised Deep Learning Algorithms " , URL : https://www.analyticsvidhya.com/blog/2021/05/introduction-to-supervised-deep-learning-algorithms/.

Machine Learning Mastery .(2021) " Deep Learning Algorithms" , URL : https://machinelearningmastery.com/a-tour-of-machine-learning-algorithms/ .

J.Delua , IBM .(2021) " Supervised vs. Unsupervised Learning: What’s the Difference? " , URL : https://www.ibm.com/cloud/blog/supervised-vs-unsupervised-learning .

Y.Taguri , S. Erlichmen ,and R.Lussato.(2016) " Deep learning long short-term memory (LSTM) networks: what you should remember" , Missinglink.ai , URLhttps://missinglink.ai/guides/neural-network-concepts/deep-learning-long-short-term-memory-lstm-networks-remember/.

aakarsha_chugh ..(2019) "Deep learning | introduction to long short term memory" ,Geeksforgeeks , URL: https://www.geeksforgeeks.org/deep-learning-introduction-to-long-short-term-memory/.