Analysis of Security Parameters and Net Work Infrastructure on Cloud

Vipul Sharma, Rajat Kulkarni, Jitendra Data, Muskan Didwania
Department of Electronics and Communication,
SRM Institute of Science and Technology, Kattankulathur, Chennai,
Tamil Nadu, India - 603203

***Abstract*—This paper pertains to an analytical approach towards establishing standards for network performance on the cloud. Cloud being the most promising domain, is yet hindered by the lack of standardization. To resolve this issue we propose a methodology suitable for all essential protocols in contrasting network architectures. In addition to this, security breaches also sever the threat on cloud data and it's privacy. To bridge the two imperative aspects of a cloud service, we intend to deploy a Deep learning classification model on Google colab, acting as an interface between the cloud database and client-server. Essential parameters including throughput(X), average delay(ζ), loss function(l) and accuracy. We extend to present our results as the optimized cloud standards.**

1 INTRODUCTION

Cloud computing is the new phase of technology which has revolutionized the way computing is done rudimentarily. Cloud Computing is the on demand delivery of computational resources via the Internet. The computational resources generally provided are data storage and computation capability. Cloud Computing in general solves many of the obstacles to efficient computing such as requirement of a powerful hardware, computation of excess cycles, redundant cycles of software updates or incompetent handling of high loads. This new technology has also created certain new challenges and obstacles in terms of network infrastructure and security parameters which pose to be extremely hazardous in terms of security and privacy. The lack of standardization in the industry of cloud computing has also led to additional problems which has been the motivation for the work on this project.

Cloud computing is the new phase of technology which has revolutionised the way computing is done rudimentarily. Cloud Computing is the on-demand delivery of computational resources via the Internet. The computational resources generally provided are data storage and computation capability. Cloud Computing in general solves many of the obstacles to efficient computing such as requirement of a powerful hardware, computation of excess cycles, redundant cycles of software updates or incompetent handling of high loads. This new technology has also created certain new challenges and obstacles in terms of network infrastructure and security parameters which pose to be extremely hazardous in terms of security and privacy.

Cloud architecture refers to the various constituents in terms of databases, capabilities and applications which leverage the power of cloud resources to direct towards a specific complication which defines the relation between the components. Based on the occurring relationship between the components, the types of architecture are Software as Service (SaaS), Infrastructure as Service (IaaS), Platform as a Service (Paas). The cloud deployment model designates how the cloud services are made available to the users. The deployment models corresponding to cloud computation services are Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud. In the rush to improve the cloud services and their interfaces, a great deal of companies often ends up ignoring the most critical aspect of their service, that being the network infrastructure. For many companies it is imperative that they massively improve their network infrastructure as it is evident that with the expansion of cloud services the data traffic is only bound to increase in the networks which will make data access difficult be it from a remote location in the world or an institutions headquarters. Some of the principal aspects of a network are Bandwidth, Throughput, Latency. The mere action of improvement of infrastructure does not necessarily yield better network performance. Certain strategies could be implemented beforehand to further improve the network performance. Some of the optimization techniques include Caching, Compression, Traffic Management, Deduplication. There are various security mechanisms in the cloud which can be implemented to ensure the data privacy and security. Encryption is the most common method used for security mechanisms as various algorithms can be executed with them.

When encryption is applied on the plaintext data, the data is paired with a string of characters which is termed as an encryption key, a secret key that is established and shared among the relevant parties involved. Then the encryption key is used to decrypt the ciphertext back into its plaintext which was its original format. If any external third-party attempts to eavesdrop, it would be unsuccessful as it would not have the encryption key. The two most preferred forms of encryption are Symmetric Encryption, Asymmetric Encryption. Based on this the various algorithms which are implemented for cloud security are RSA Algorithm, DES Algorithm,·AES Algorithm, Blowfish Algorithm

2 METHODS

2.1 Process Flow

The process implemented is as, the pilot study was conducted to ensure the smooth on going of the project. The project was started with a prior study for project specification , Cost Estimation, Resources implemented and the timeline. The project specifications includes the analysis of the various protocols in two different topologies that have to be carried out in terms of the Throughput, Average Delay, Accuracy, Loss function, Complexity, and Security. We are really proud to mention that our project is really economic as we are using the easily available resources in our department labs. For the cloud simulations we are using Tensorflow library in Google colab which is a free of cost available open source platform for cloud processing purposes. For the security parameters also, we are using the Jupyter notebooks on Google colab. So our estimated cost is really low and it only includes the paperwork and other hardware.

2.2 Experimental Data Obtained

Primary data is the data being obtained from the first hand experiments on the cloud environment. For network performance we have taken the throughput, Average Delay and the comparative graphs. To obtain the performance on cloud we have checked the loss function and accuracy for the Deep Learning Model deployed on the cloud platform of Google colab. The inference obtained from the primary data and the conclusion drawn is secondary data.

2.3 Interpreted Comparative Study

For the project our secondary data is the comparative data we obtained by comparing the various results and analysing them. The result will be a comparative study of the parameters. Data analysis is an imperative part of our study which includes the measurement of data, recording of data into concise tabular formats.

Then for the purpose of comparative analysis, the obtained results are plotted into graphical representations. For the execution of all these tasks, we are implementing Google Sheets as the primary data analysis tool. The application was used to graphically represent the obtained results for a clearer understanding and better inference to derive a conclusion for the results. We have analysed the network performance and the security parameters separately. The network parameters were analysed on an available LAN server-client system. The security parameters were analysed by implementing various algorithms on cloud compilers and measuring the executing times with their complexity. As a common platform to bridge them both, we have used Google colab as a cloud platform for implementing a real time deep learning classification model with Tensorflow library and obtaining the loss function, accuracy and training time per sample.

3 SYSTEM DESIGN

The study had 2 different parts involving the network infrastructure and security parameters. Here’s a brief description of the system design of the network infrastructure.

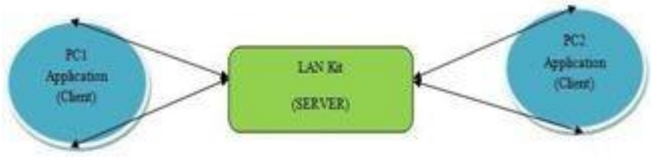

Fig.3.1. The Basic System Architecture

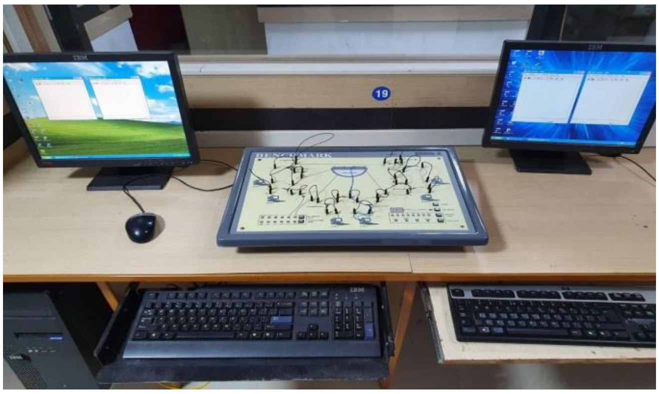

Fig.3.2. The Real Time Hardware System

The above image is a pictographic representation of the LAN Kit. The analysis of the network infrastructure was done using a LAN client-server kit. The client PC and the server/sender PC were connected to the LAN Kit with connecting wires.

These kits provide a menu driven interface and a C library which can give an access to the programming interface to the NIU. This kit has 6 nodes per NEU, meaning 3 parties can be connected but we have connected for concise and clear results. The parameters recorded in this setup are offered load, throughput and average delay.
Next, we evaluate the cloud system design which involves the use of Tensorflow library and the cloud platform, Google colab.

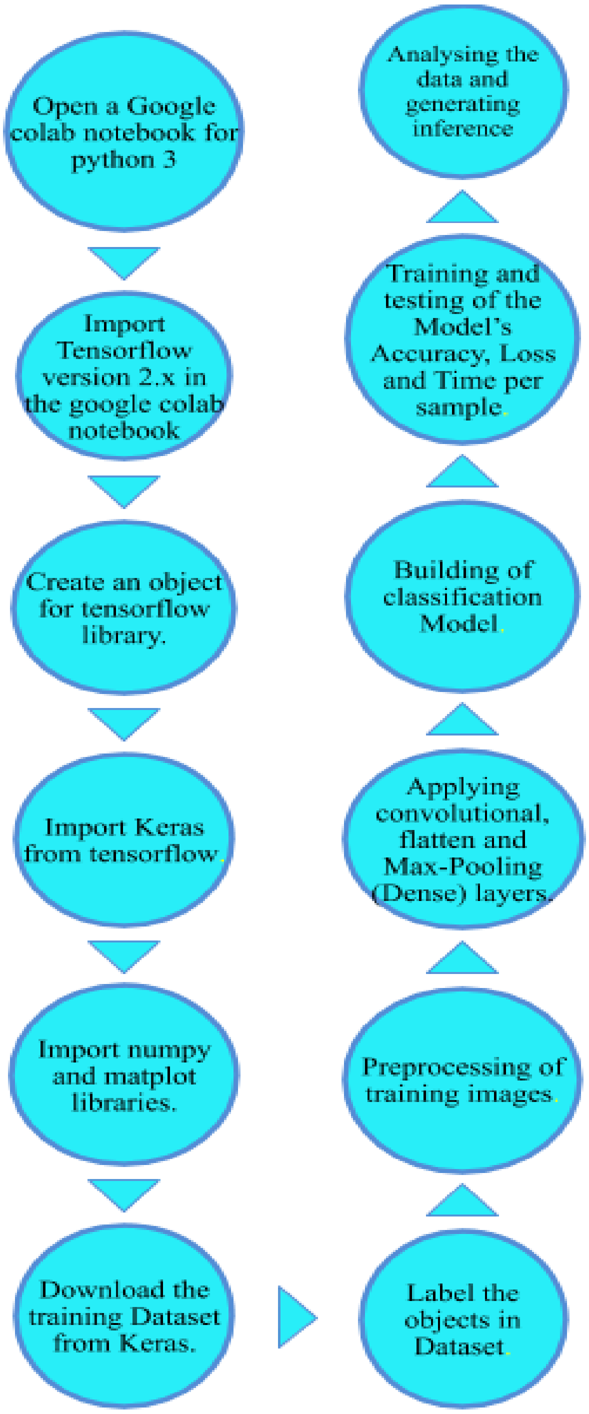
Open a Google colab notebook for python 3
Import Tensorflow version 2.x in the google colab notebook
Create an object for tensorflow library.
Import Keras from tensorflow.
Import numpy and matplot libraries.
Download the training Dataset from Keras.
Label the objects in Dataset.
Preprocessing of training images.
Applying convolutional, flatten and Max-Pooling (Dense) layers.
Building of classification Model.
Training and testing of the Model's Accuracy, Loss and Time per sample.
Analysing the data and generating inference

Fig.3.3. The Real Time Cloud Implementation Model

To begin, we first import the Tensorflow library in the Google Colab and create an object for the Tensorflow library. Then using Keras we download a training dataset where we import the matplot and other relevant libraries. After importing the Keras, we label the objects in the data set succeeding which the pre-processing of training images takes place. Then we apply convolutional flatten and max pooling layers to analyse the data and to generate an inference. Then we obtain the model's accuracy, loss and time per sample to build a classification model and obtain the relevant results. Here we implement the model with 10 - 1000 Epochs . Epoch in this algorithm is defined as the number of training instances per training attempt for a model with the same training data set. The concept of Epoch is applied here to demonstrate the optimization technique of Caching which refers to caching of frequently used images in a user's local disk. To analyse the security parameters, we proposed four different security encryption methods for the security of data.

4 RESULTS

The data from the system was recorded in a concise manner with a tabular representation as follows.

IPD	G1	G2	Sum G	Ack1	Ack2	Sum Tx	X	G*100
8000	13	13	26	11	9	20	0.02	0.0325
7000	14	14	28	11	11	22	0.022	40
6000	18	19	37	15	14	29	0.029	61.66666667
4000	30	30	60	24	25	49	0.049	150

Fig.4.1. The Data Obtained from Hardware System Implementation

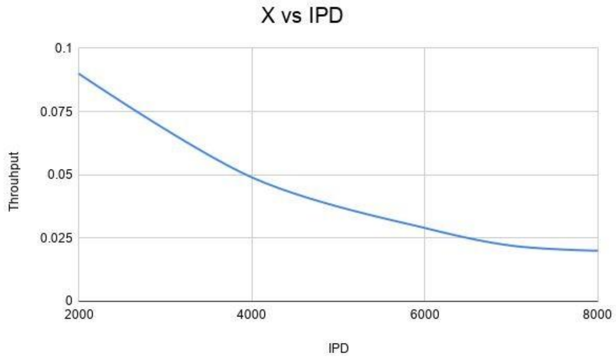

Fig.4.2. Comparative Study of Throughput and IPD

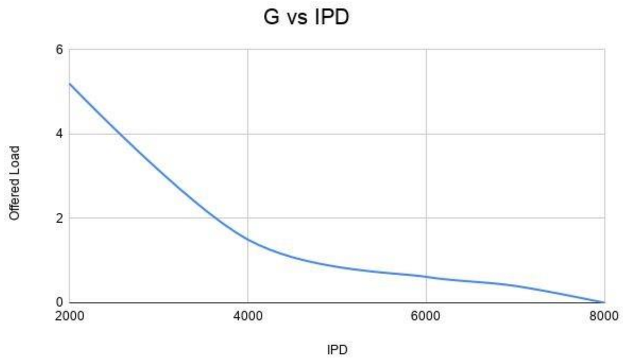

Fig.4.2. Comparative Study of Average Delay and IPD

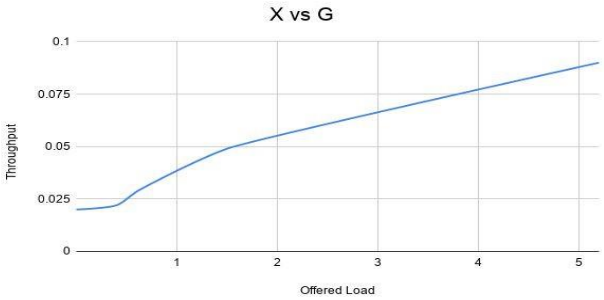

Fig.4.3. Comparative Study of Throughput and Average delay

The model was deployed and the following results were obtained.

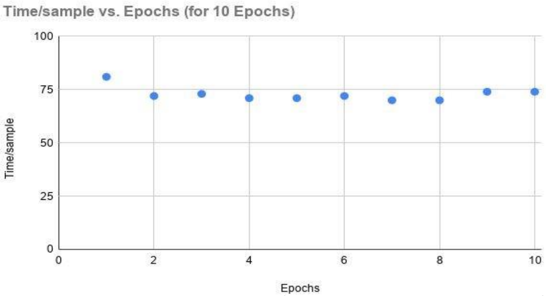

Fig.4.4. Comparative Study of Time/sample with Number of Epochs

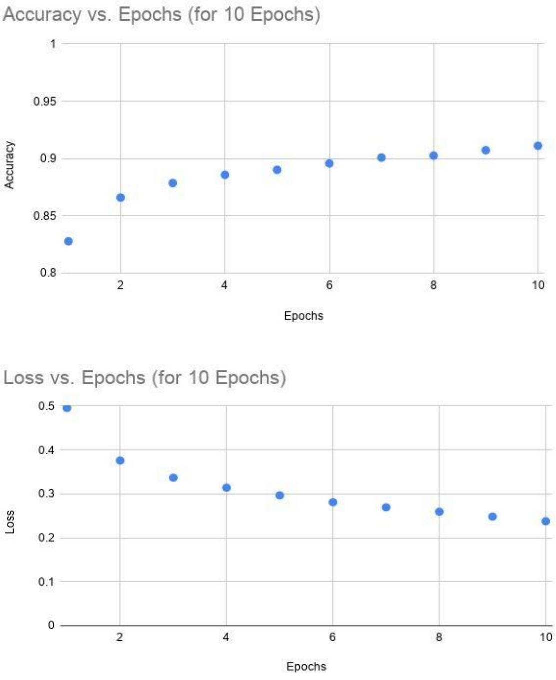

Fig.4.4. Obtaining of Accuracy and Loss Function with Number of Epochs

5 INFERRED DATA

For the network infrastructure analysis, the following inference was drawn-

Throughput v/s Offered load

- CSMA/CA: - It has a stiff slope & saturates after threshold . As Data rate increases - Stiffness ncreases in CSMA/CA.
- CSMA/CD: - Slope increases gradually & later decreases after threshold . As Data rate increases
  - Slope gradually tends towards stiffness.

Throughput v/s IPD

- CSMA/CA: As IPD increases Throughput decreases but changes are slower. As Data rate increases , no significant change in the graph.

- CSMA/CD: As IPD increases Throughput decreases but changes are faster in CSMA/CA compared to CSMA/CD. As Data rate increases, no significant change in the graph

IPD v/s Offered Load

- CSMA/CA: - As IPD increases offered load decreases & vice versa. As Data rate increases no significant change in the graph

- CSMA/CD: -As IPD increases offered load decreases & vice versa. Data rate increases rate of change of slope also increases

For the security when given the same binary input, most of the algorithms took over 4 seconds to execute. AES Algorithm took only 1.5 seconds to encrypt the data which was the fastest. AES Algorithm also requires the lowest memory to be run, making it the most viable option

6 CONCLUSION

The analytical study of the security parameters and network performance established standards pertaining to cloud. CSMA/CA was found to be the most suitable and optimized protocol for networking in cloud. In terms of security, AES algorithm performed in the most efficient manner in terms of execution time.

ACKNOWLEDGMENT

We would extend our gratitude towards our supervisor, Mr. S. Praveen Kumar, Assistant Professor, Department of Electronics and Communication Engineering, SRMIST, Chennai. Also we thank the ECE Department, SRMIST for helping us in getting all the resources.

REFERENCES

[1] R. Gargista Gustamas and Guruh Fajar Shidik - Analysis of Network Performance on Cloud Computing , IEEE 2017

[2] Cheikh Brahim Ould Mohamed El Mocta and Karim Konaté – Survey of Security Challenges in Cloud Computing, IEEE 2016

[3] S. Eman Mahmoodi R. N. Uma and KP Subbalakshmi – Optimal Joint Scheduling and Offloading for Cloud Computing – IEEE 2019

[4] G. Sousa, W. Rudametkin, and L. Duchien, ''Automated setup of multi cloud environments for microservices applications,'' in Proc. IEEE 9th Int. Conf. Cloud Comput. (CLOUD), Jun./Jul. 2016, pp. 327–334

[5] Z. Hao, E. Novak, S. Yi, and Q. Li, ''Challenges and software architecture for fog computing,'' IEEE Internet Comput., vol. 21, no. 2, pp. 44–53, Mar./Apr. 2017

[6] W. Cai, V. C. Leung, and L. Hu, "A cloudlet-assisted multiplayer cloud gaming system," Mobile Netw. Appl., vol. 19, no. 2, pp. 144–152, 2014.

[7] H. Hong, D. Chen, C. Huang, K. Chen, and C. Hsu, "Placing virtual machines to optimize cloud gaming experience," IEEE Trans. Cloud Comput., vol. 3, no. 1, pp. 42–53, Jan.-Mar. 2014.

[8] T. Verbelen, P. Simoens, F. De Turck, and B. Dhoedt, "Leveraging cloudlets for immersive collaborative applications," IEEE Pervasive Comput., vol. 12, no. 4, pp. 30–38, Oct.-Dec. 2013.

[9] I. 802, "Ieee standard for local and metropolitan area networks: Overview and architecture," IEEE Std 802–2014, p. 8, 2014.

[10] S. Das, M. Khatua, S. Misra, and M. Obaidat, "Quality-assured secured load sharing in mobile cloud networking environment," IEEE Trans. Cloud Comput., 2015, DOI: 10.1109/TCC.2015.2457416.

[11] M. Aazam and E.-N. Huh, "Dynamic resource provisioning through fog micro datacenter," in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops, Mar. 2015, pp. 105–110.

[12] E. Baccarelli, N. Cordeschi, A. Mei, M. Panella, M. Shojafar, and J. Stefa, "Energy-efficient dynamic traffic offloading and reconfiguration of networked data centers for big data stream mobile computing: review, challenges, and a case study," IEEE Netw., vol. 30, no. 2, pp. 54–61, Mar./Apr. 2016.

[13] Q. Peng, A. Walid, J.-S. Hwang, and S. H. Low, "Multipath TCP: Analysis, design, and implementation," IEEE/ACM Trans. Netw., vol. 24, no. 1, pp. 596–6

[14] D. Khusnia, "Pembuatan Video Klip Lagu Smartschool Pride And Happiness Sebagai Media Dokumentasi SMK Smart It Medan," vol. 2, no. 1, pp. 88–95, 2013. 09, Feb. 2016.

[15] V. Anagnostopoulos and E. Sardis, "Cloud Rendering a feasibility case study," pp. 684–687, 2014.

[16] M. R. Baharon and D. Llewellyn-jones, "Secure Rendering Process in Cloud Computing," pp. 82–87, 2013.

[17] GF Shidik and A Ashari," Efficiency energy consumption in cloud computing based on constant position selection policy in dynamic virtual machine consolidation," 2014.

[18] FA Gaetano, C. Massimo, D. Patrizio and D. Marco, "QoS Guarantees for Network Bandwidth in Private Clouds," 2016.