Data Security Model Enhancement in Cloud Environment

Abhilash Pulipati[1]
[1]Department of Electronics & Communication Engineering
[1]Jawaharlal Nehru Technological University

Abstract—With the rapid developments across the information technology usage of cloud infrastructure has increased a lot. There are lots of services offered by cloud where data storages occupies the primary stand when compared to rest of the services. Data security across the cloud is the main aspect to be considered while storing the data of any organization across a remote location. There are many parameters to be considered while providing security to cloud integrity, confidentiality and availability. There was ample research done in this context where there are many security models available for all the three aspects discussed. The main aim of the proposed system is to make the cloud data server available by blocking unwanted traffic with a firewall. OPNET simulation is done to evaluate the performance of the cloud data storage and the corresponding security issues. From the overall analysis of the results it is clear that blocking the unwanted web traffic over the cloud storage security has improved a lot in terms of traffic and packet managements.

Key words: Data storage, Cloud computing, Cloud data security, web traffic, firewall.

I. INTRODUCTION

The basic principle of cloud computing belongs to distributed computing where lots of data centers and web services. There are many cloud computing service providers and the major include Microsoft, Yahoo, Google and Amazon and all these service providers provide data storage with ample security. There are many architectures of cloud computing but the most sophisticated architecture of cloud was proposed by Amazon during the year 2002. The concept of data storage over servers has taken the cloud computing technology to a new phase and got popular and huge response from lots of companies. There are many techniques to store the data over cloud server and the main aspects considered here include client's confidentiality, availability and integrity of the data stored across a remote server. Confidentiality plays an important role in storing and keeping the clients data private where the privacy place a key role as the data is stored across a remote cloud server. Confidentiality of the client's data is maintained by traditional techniques like legal protection, encryption and access control. Integrity refers to the level of confidence against the data that need to be supported across the cloud and the way data is protected from unauthorized usage. When the case with availability is considered it refers to the anticipation against usage of the cloud data by the users. Users should have access to the data at any point time after passing through the authentication process. In general data is stored across the cloud either at single location or as multiple replicas based on the priority of data. A typical cloud storage environment is as shown below fig. 1.

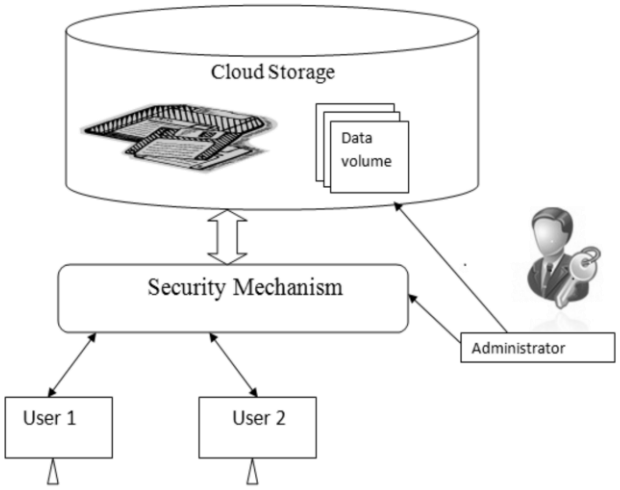


Fig. 1: cloud storage architecture

There was lot of research done in terms of cloud data storage security in terms of confidentiality and integrity. Availability is equally important as whenever the users want to either access or upload data to the cloud and there were some research gaps in this context. Availability of data plays an important role as this aspect is affected with lot of factors like network and server traffic over the cloud. In general performance of the cloud is affected with lot of issues like nature of the applications being maintained over the cloud and the corresponding traffic. In general most of the applications maintained across cloud are web based and huge web traffic is generated over the network and this might affect the overall database operations against its availability to the users. The main focus of this research is to evaluate the availability of the cloud data and propose a possible solution that make data access much faster with ample security and information protection. Proposed solution can be achieved with a simulation procedure where an internet based cloud can be simulated where different applications can be set for better traffic and safety management. The actual procedure followed to simulate an internet based cloud is explained in the below section.

II. PROPOSED SOLUTION

As discussed in the previous sections, the main aim of this study is to evaluate the security of the data storage across clouds against availability issues. OPNET IT guru is used as the simulation tool to create an internet based cloud and this tool provides options to create number of scenarios where the results can be compared and performance is evaluated. In this simulation three scenarios are created where the first scenario has no security constraints. In this scenario have no firewalls across the simulation and normal working conditions are simulated.

Two applications are simulated across the cloud like the database application and web application. Required application and profile configurations are created at the node level and thus now the cloud supports and generates the database traffic and web traffic. In this scenario data traffic is dominated by the cloud traffic and the availability of database resources is very less. Two subnets are used where they act as service providers of clouds, an internet based IP cloud is used and two Ethernet routers are used to create the required simulated network. DB query and DB response time are used as the performance metrics for database, where HTTP page response is considered for the web applications. Almost 150 workstations are used and they act as the end users of the database and web application. In the second scenario a router is replaced with firewall router and this now has better security constraints for the database application. Packet latency is set to 0.05 seconds thus a perfect packet filtering aspects are issued in this scenario Third scenario also has firewall routers and few configurations are made to block the web traffic. Thus web traffic has some constraints over this scenario and unauthorized web traffic is blocked and now the database access has less traffic to the users. Simulation is run for 1 hour and the results are compared for the three scenarios. Overall simulation setup created with OPNET in the first scenario is as shown below

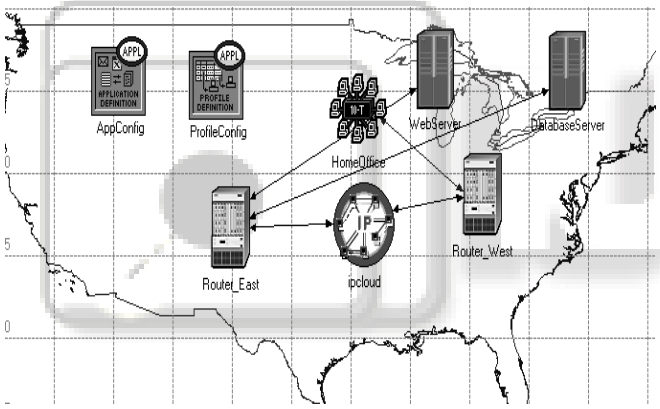
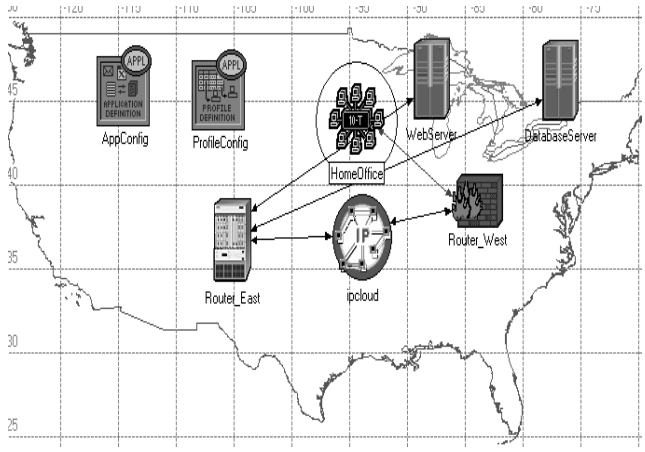


Fig. 2: Internet cloud simulation setup for first scenario

Below screen shows the simulation setup for second and third scenarios



Fig, 3: Simulation setup for second and third scenarios

Below figure shows the changes made to the third scenario where the web traffic is blocked

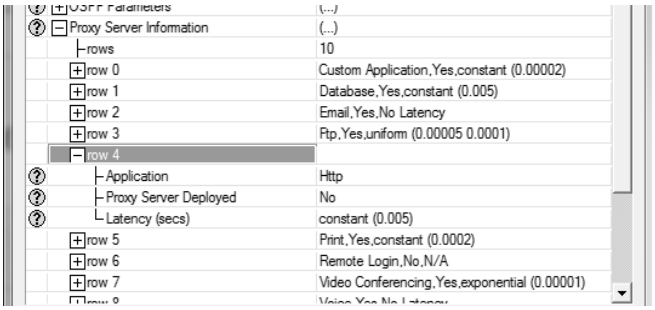


Fig. 4: Configurations made to block the unauthorized web traffic

III. RESULTS

A. DB query response time

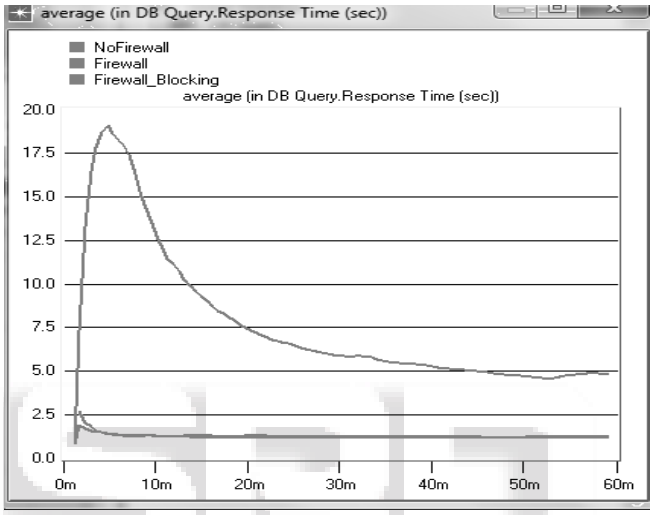


Fig. 5: Graph of DB Query Response Time

From the graph of figure 5 it is clear that database query response time is more with the firewall scenario and thus the availability of data is more in this context

B. Database server point to point utilization

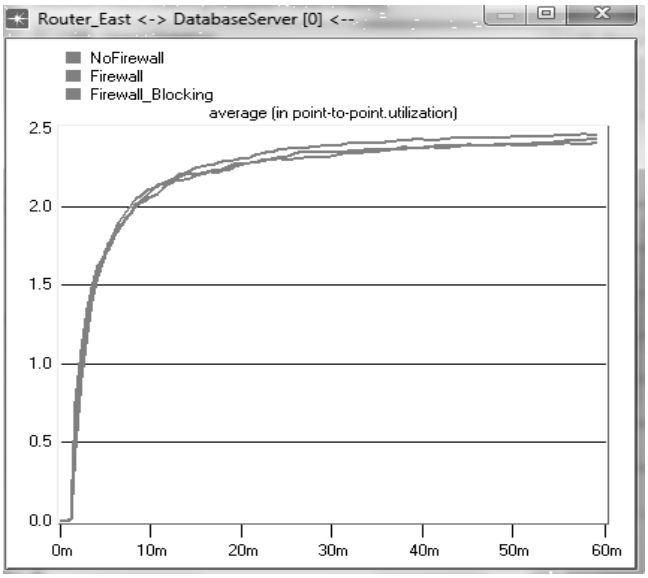


Fig. 6: Graph of Database server point to point utilization

From the above graph of figure 6 it is clear that the overall cloud utilization rate has increased over the secured scenario.

C. Cloud utilization

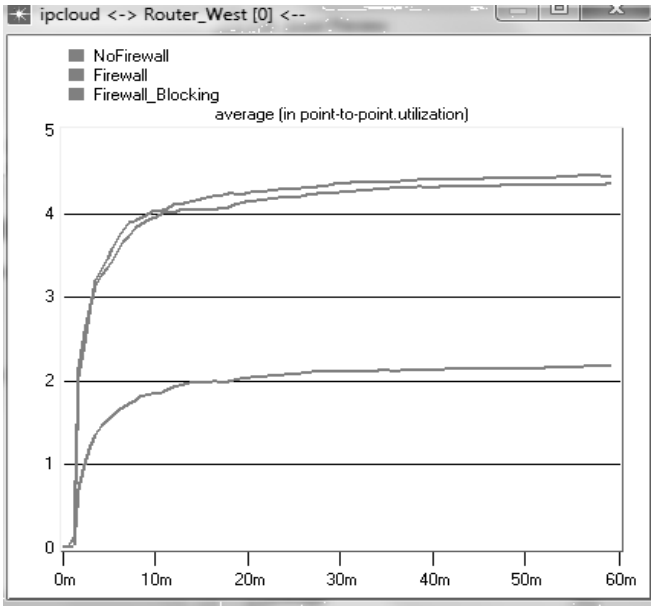


Fig. 7: Graph of Cloud Utilization

As the graph shows, Cloud utilization has improved a lot across the secured scenarios when compared to other scenarios.

IV. CONCLUSION

The main aim of this research is to enhance the security model of data storage across cloud computing. There are many issues to be considered while improving security for the data storage and in this research availability of data is considered as the main aspect. OPNET simulation tool is used for simulating internet based clouds. Three scenarios are used across the simulation where the first scenario has no security constraints, second scenario has firewall routers and the third scenario has configurations that block the unauthorized web traffic. From the simulation results it is clear that performance of the database availability is improved a lot and even the unauthorized web access is blocked. Database response time, database server utilization and the overall cloud storage utilization is improved.

ACKNOWLEDGMENT

I would like to thank all my family members and friends who supported me in developing this research. I am glad to thank my professor Mr. P Rama Krishna MTECH ECE department in providing ample research scope and guidance.

REFERENCES

[1] John W. Rittinghouse, James F. Ransome, "Introduction", Cloud Computing- Implementation, management & security, Ed. Taylor & Francis Group, LLC ,2010, pp.27-29.
[2] Cor-Paul Bezemer, Andy Zaidman, "Multi-Tenant SaaS Applications: Maintenance Dream or Nightmare?", Delft University of Technology Software Engineering Research Group Technical Report Series, 2010, http://www.se.ewi.tidelft.nl/techreports, pp 1-5.
[3] Uma Somani, Kanika Lakhani, Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010), pp.211-216.
[4] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou, "Security and Privacy in Cloud Computing: A Survey", 2010 Sixth International Conference on Semantics, Knowledge and Grids, pp. 105-112.
[5] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Security Issues for Cloud Computing", International Journal of Information Security and Privacy, 4(2), April-June 2010, pp 39-51.
[6] Jianfeng Yang, Zhibin Chen, "Cloud Computing Research and Security Issues", International Conference on Computational Intelligence and Software Engineering(CiSE), Wuhan, 10-12 Dec. 2010, pp 1-3.
[7] Shuai Zhang, Shufen Zhang, "Cloud Computing Research and Development Trend", 2010 Second International Conference on Future Networks,ICFN'10 , 2010, pp 93-97
[8] The Force.com Multitenant Architecture: Understanding the Design of Salesforce.com Internet Application Development Platform. http://www.salesforce.com/au/assets/Force.com_Multitenancy_WP_101508.pdf.
[9] David Banks, John S. Erickson, Michael Rhodes, "Multitenancy in Cloud-based Collaboration Services", Hewlett- Packard Development Company, L.P., February 21, 2009 http://www.hpl.hp.com /techreports/2009/HPL-2009-17.pdf.
[10] "Implementing SaaS Multi-tenancy with EMC Documentum 6.5- Best Practices planning", EMC2, http://www.emc.com/collateral/software/white-papers/h4701-oem-multitenancywp.pdf.

