International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

© Global Society of Scientific Research and Researchers

http://ijcjournal.org/

Distributed Denial of Service Attack Challenges in Cloud Computing: A Review

Adesegun O. A.[a]*, Izang A. A[b], Nzenwata J. Uchenna[c], Udosen Alfred Akpan[d]

[a,b,c,d]*Department of Computer Science, School of Computing and Engineering Sciences Babcock University, Ilishan-Remo, PMB4005 Ogun State, Nigeria*

[a]*Email: adeseguno@babcock.edu.ng*

[b]*Email: izanga@babcock.edu.ng*

[c]*Email: nzewatau@babcock.edu.ng*

[d]*Email: udosena@babcock.edu.ng*

Abstract

Cloud computing as an ever-evolving technology has appeared to be a new discovery, with a history that can be traced to the 1960s, yet the computing paradigm has not been fully adopted till date. This is due to the security and trust management issues associated with the paradigm. Studies so far have shown remarkable efforts in the area of cloud computing security but has paid little attention to the area of application-based denial of service and its distributed variant. To this end, this paper highlights the Extensive Mark-up Language Denial of Service (XDoS) and the Extensive Mark-up Language Distributed Denial of Service (XDDoS) as one of the security challenges that inhibit the adoption of cloud computing. So many researchers in this field have proposed different solutions to this issues, however, it was observed that there is a need for an efficient and more effective counter-measures solution against XDoS and its distributed variant XDDoS which are application based denial of service that can be found in software as a service (SaaS) cloud computing service model.

Keywords: Cloud Computing; Distributed DoS; Extensive Mark-up Language XDoS; Infrastructure as a Service; Platform as a Service and Software as a Service.

1. Introduction

Cloud computing, which appears to be a new discovery, but it has a history that can be traced to the 1960s. The 1960s was the era of mainframe computers. Innovations of that time led to the change of how mainframe computers were used.

----

* Corresponding author.

Their usage was predicated on direct access, one user at a time to complete the many tasks. After a few years, timesharing was introduced. This implied that multiple users could use the mainframe servers. By the 1970s, mainframe users saw the first implementation of virtualization and symmetric multi-processing. It was during this era that John McCarthy stated that "Computation may someday be organised as a public utility" [1]. There was a further shift in how computing was done by the 1980s from the centralized paradigm of computing to the client server approach. The development of communication systems helped facilitate the shift. As a result companies could have their application software installed on a server and through the communication media, access those applications and data from desktop computers. The disadvantage to this shift was an initial heavy capital expenditure in the purchase of hardware. The Internet and its protocols were standardised in the 1990s and as a result a company named SalesForce was able to host and distribute customer relationship management software over the internet on a subscription basis by 1995. SalesForce on its website force.com was also able to host a platform on their servers that enabled developers to build applications hosted on their servers. It was at this point that virtualization of hardware (that is, the creation of a guest machine inside a host machine) was just gaining popularity [2]. Many definitions have been given in relation to cloud computing but this research having gone through, defines it as an on-demand resource sharing that is based on the internet as the communication medium between devices used. Essentially there is an abstraction between the resources being shared and the architecture the cloud service provider employs to deliver those shared resources. Several resources could be shared ranging from infrastructure, platforms and software among others.

2. Characteristics of Cloud Computing.

Ease of Use: One of the criteria for any computing paradigm to be classified as cloud computing is for resources to be requested for when needed and released to the cloud service provider when not needed [3].

At-Scale/Elasticity: With cloud computing, because users can request for resources as needed there is disillusionment that, there is an infinite amount of resource available for use [4]. For instance, with the use of Dropbox cloud storage facility, one pays for whatever capacity one requires to store data and can increase this storage capacity as the need arises. Abstraction: An important characteristic of the cloud computing model is its reliance on abstraction, such that the details of how the cloud service provider delivers the service is not shown or known by the client; that is, the infrastructural architecture is hidden from the user [2]. For instance, how many racks of servers, routers, and switches and so on which the provider uses in providing its services are not known to the client. All that the client wants is value for services paid for. This has to reach a minimum standard. Usually a legal document called the Service Level Agreement (SLA) is signed by the provider and client to ensure that their money's worth of services are delivered.

Multi-tenancy: A single implementation or set up by a cloud service provider is able to serve several clients [4]. For instance Google Apps can be used by many people at the same time without any conflict.

Hardware virtualization: This is a technological characteristic of cloud computing that helps to maximise cloud service provider resources [3]. It is this characteristic that helps achieve some of the other characteristics listed earlier such as, multi-tenancy and At-Scale. For instance, one server could have several virtual machines dynamically created and paid for by the client. All those virtual machines would have their operating systems and would be used as different computers, thereby maximising the cloud provider resources. This wouldn't have been the case if virtualization were not used.

Automation: Without manual intervention, it is possible for the cloud environment to dynamically allocate more resources to users as needed [2]. For instance, if a user is running a processor intensive task, instead of the program hanging and not responding, the cloud automatically allocates more processing capacity to that virtual machine. Once that program is done, executing the extra processing capacity is withdrawn.

Metered Billing: This is otherwise known as pay as you go. In this characteristic of the cloud computing, cloud service providers' customers/clients are liable to only pay for whatever resources they use [5]. Clients no longer need to worry about the initial cost of purchase of any equipment or commit to a level of usage of resources provided by the cloud service provider. This model makes it easy for small and medium enterprises to have computer resources without too much investment in technological set up of their enterprise. Just like the example above about automatic resource allocation of processing capacity as needed, at the time the server is running a processor intensive task the customer would be billed. As soon as that program is done executing that extra allocation of resource is released, leaving the user to only pay for services rendered. In other words a pay-as–you-go approach is used.

Broad Network Access: Cloud computing resources are available over networks, which encourages the use of thin and thick clients such as tablets, mobile phones, laptops among others [6]. This enables users to access their resources more flexibly. Depending on the architecture users may be able to have access to and use the resource they paid for anywhere in the world through the use of the internet as a medium between the cloud service providers and cloud service providers' client.

2.1 Review of Related Works

Modi and his colleaguesadopted Mell and Grance's definition of cloud computing,that defines the computing paradigm as, a convenient provision of on-demand, network access to a shared pool of configurable computing resources'. The paper highlighted the various service model of cloud computing to be software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS). Example of SaaS includes Google Apps, of PaaS is Google App engine and of IaaS is Amazon web services [1]. The research reported that cloud computing suffers from the same security challenges that the traditional networks have. These security challenges include DoS, DDoS, Flooding, DNS Poisoning, IP Spoofing, Routing Information Protocol attack and so on. Hence the main problem tackled by this research was finding the best intrusion detection system (IDS) algorithm and where to place the IDS on the network in cloud computing. The main objective of the paper was to highlight the need for an intrusion detection system in cloud computing. The paper highlighted the fact that firewalls would be inadequate to solve the current security challenges in cloud computing, as firewalls would not be able to prevent insider attacks. The paper used a survey research design of descriptive study. A thorough literature review was also done which detailed the various techniques of IDS/IPS, its characteristics and its challenges, IDS/IPS types and their various disadvantages. The paper also detailed the existing IDS approaches in the cloud with their various advantages and disadvantages. As a result of the preceding problem statement, objective and methodology the researcher concluded that firewalls are not sufficient to deal with security issues in cloud computing. They made a case for the use of IDS systems in the cloud computing environment. Lonea, Popescu & Tianfield reported that cloud computing has numerous challenges. They highlighted the fact that among these challenges, security issues are major challenges hindering the total adoption of the computing paradigm. As a result the paper alluded to the fact that of all the security issues DDoS is a major security challenge as confirmed by the International Data Corporation (IDC) in August 2008 [2]. The paper highlighted the fact that intrusion detection systems (IDS) are a good way of mitigating DDoS and assuring usable cloud computing services. However the problem with this method is that the IDS sensors generate a lot of false positives. This problem is the main problem their paper tries to address. As an add-on the paper also tries to address the problem analysis of logs generated by the IDS sensors. The main objective of the study was to detect and analyse DDoS attack in cloud computing environment. The researchers intended to complete this objective by completing a thorough review of related works, analysis and understanding the Dempster-Shafer Theory which is the algorithm they proposed in their Virtual Machine (VM)-based IDS. The paper used an experimental research design whereby the researchers used Dempster-Shafer Theory (DST) operations in 3-valued logic and Fault-Tree Analysis (FTA) for each VM- based Intrusion Detection System. The cloud topology as depicted in figure 1 was used in this research.

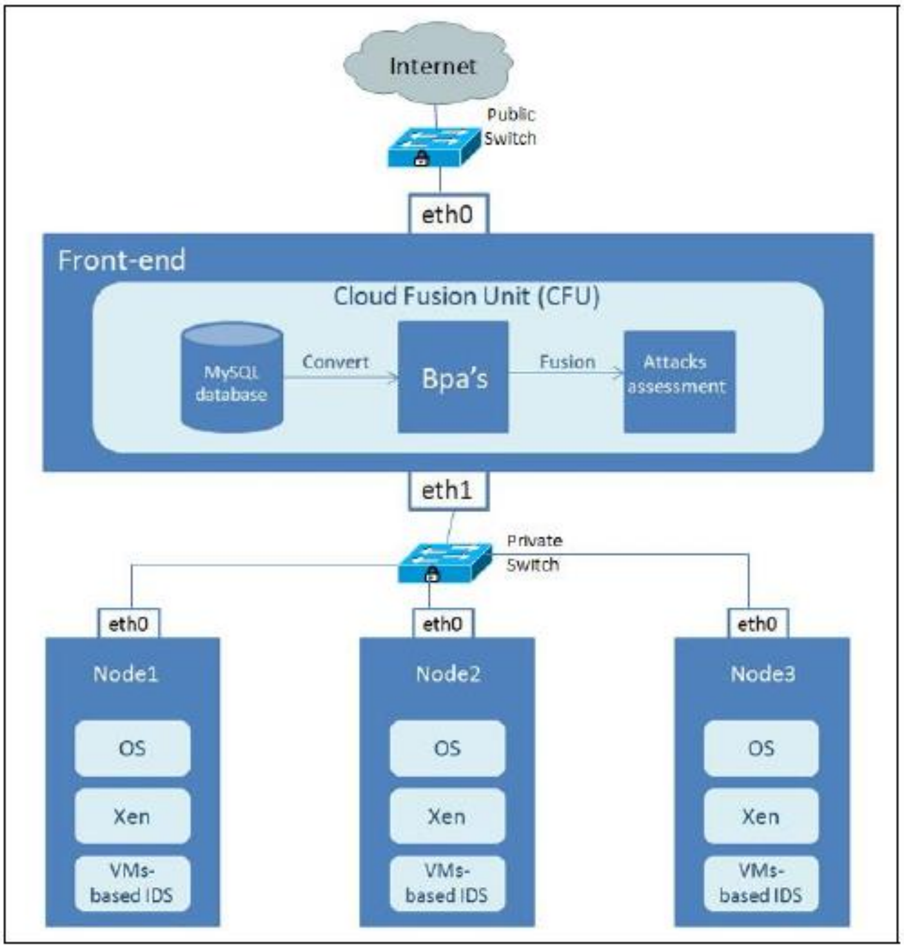

Figure 1: Private Cloud Topology [7]

As a result of the preceding problem, which is to find a solution to distributed denial of service in cloud computing, objective and methodology as stated earlier, their proposed solution incorporated the use of IDS in the virtual machines which eliminates the overloading problem, because network traffic is divided to all IDS. The cold fusion unit as shown in Figure 1 added the capacity to analyse the result of the DST of evidence in 3-valued logic and the Fault-Tree Analysis for the IDS of each virtual machine and at the end was fused using the Dempter's combination rule. Hence, with the use of DST their proposed solution could take care of cases of uncertain state, reduced the amount of false negatives, increase detection rate, resolve conflicts generated by the combination of information provided by multiple sensors and ease the work of analysing different log by the cloud administrator. Reference [7] introduced cloud computing as an internet-based environment that focuses on sharing computations or resources as well as hiding the complexities involved from users of the system. The paper highlights three cloud computing paradigms, namely: private, public and hybrid clouds. It also mentioned Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) as service rendered on the cloud. The researcher mentioned three areas upon which quality of service could be met. They are reliability of data, availability of service and security of the whole setup. There are a few challenges cloud computing face which include but not limited to privacy issues, security, anonymity, telecommunication capacity, government surveillance, reliability and liability. They noted that the most critical task of any cloud service provider is security thus, their paper looked at the problem of security in cloud computing. The main objective of the paper was to highlight the major security threats in cloud computing. In so doing the paper highlighted DDoS as a type of attack that was difficult to tackle by most networks, the example of address resolution protocol (ARP) spoofing at the network layer overcoming virtual machines was given. The paper used a survey research design of descriptive study and a thorough literature review. The paper proposed the use of the cloud against DDoS. The instance of web servers being brought down by many requests was given and that taking that web server to the cloud assures the client of more resource thereby eliminating the DDoS. Subashini & Kavitha, Stated that small medium enterprises (SMEs) are now realising that, cloud computing would increase their profitability. This reduces the amount of money to be invested on information technology (IT) resources as well as the staff to manage those resources. The paper pointed out that 74% IT top executives and chief information officer of organizations would like to adopt cloud computing but for the security issues in the computing paradigm [9]. The paper tried to explain reasons why cloud computing has not been adopted by a lot of enterprises given its apparent advantages. Advantages of cloud computing which include pay-for-use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, greater resiliency, hypervisor protection against network attack and so on. The objective of the paper was to survey security issues in cloud computing delivery models. In order to meet this general objective literature review was conducted. This detailed SaaS, PaaS and IaaS as delivery models. It also detailed some explanations on data security, network security, data locality, data integrity, data segregation, data access, authentication and authorization, data confidentiality, web application security, data breaches, vulnerabilities in virtualization, availability, backup and Identity management and sign-on process as some of the security issues in SaaS. In PaaS, the paper suggests that the ability of the application developer to develop secure application is most important. At the IaaS level the paper suggests that the deployment model such as private, community, public and hybrid affect the level at which one is to be concerned about security. The paper used a descriptive research design, detailing and describing the several components of cloud computing and the security issues therein.

Table 1: Summary of Reviewed work and their shortcomings

SN	Author(Year)	Contribution to Knowledge	Gap
1	[1]	Highlighted cloud security challenges and equated them to traditional network challenges (e.g. DoS, DDoS, RIP attack, IP spoofing) They made a case for IDS systems in cloud computing	Cannot defend against application based denial of service attacks.
2	[2]	Highlighted the fact that IDSs generate a lot of false positives Proposed best algorithm for IDSs to be Dempster-Shafer Theory operation in 3-valued logic and Fault tree Analysis. Proposed VM based IDSs	Cannot defend against application based denial of service attacks.
3	[3]	Highlighted security challenges in cloud The paper proposed the use of cloud against DDoS	Cannot defend against application based denial of service attacks. With the right amount of customers a cloud datacentre can be brought down.
4	[4]	Highlighted Security Challenges in cloud computing delivery models In SaaS availability data segregation, vulnerabilities in virtualization, web application security, backup and identity management to mention a few. In PaaS, ability of the application developer to develop secure applications In IaaS, level of security depends on deployment model	The author did not go into details about the specific types of web application vulnerability.
5	[5]	Showed how HTTP-DoS and XML-DoS and their distributed variants as possible attacks in cloud Proposed a trace back Proposed the use of neural networks in IDS systems.	The author proposed a trace back mechanism which may be inefficient if the IP is spoofed. There is no reference to the dataset used, hence the validity is questionable. The author reported that the main issue is that the response time increased from between 20ms-30ms to 1sec The authors did not publish the detection rate of XDoS They had 91% detection rate in the training dataset for HDoS protection but got a worse detection rate of 88% on the test dataset. The authors did not justify the reasons for using 1000 data points in their training dataset and 1000 data point in their test dataset.

The paper compiled various suggestions by other researchers in the field as well as suggested some solutions to the highlighted problems in cloud computing. Chonka, Xiang, Zhou & Bonti described cloud computing as cloud service providers renting out spaces on their physical machines for a specific amount of time. They pointed out that space on the physical machine could mean dynamic virtual machines and flexible hosted software services. They added that each machine and software share the notion that delivered resources should be allocated and de-allocated on demand and at the same time providing real performance. Studies in this paper, conducted by E-Crime Congress and KPMG showed that online customers are most at risk as time goes by reporting 60% poisoned websites and 40% of their respondents reporting an increase in technical sophistication of attacks. They described DDoS as node systems attacking one node all at the same time, flooding it with messages in order to use up its networking resources or crash the application [10]. Fowler stated that it is usually better for corporations to pay ransoms than to see their systems go off line as a result of DDoS. Their paper tried to establish the fact that there could be other variations of the DDoS such as the Hyper-text Transport Protocol Denial of Service (HTTP-DoS) and Extensible Mark-up Language Denial of Service (XML-DoS) as well as their distributed version which could be from multiple points to a single primary victim. The aim of their study was to show how to protect cloud computing against HTTP-DoS and XML-DoS. In order to meet up with this main objective the researchers did a review of related works, they showed how this kind of attack is possible in the cloud computing environment of SaaS using real attack traffic as provided by the StuPot project and they also showed how to mitigate this problem using their Service Oriented Trace-back Architecture [11].

3. Conclusion

Form the review, it can be observed that most of the proposed solutions to detect or militate against application based DDoS (XDoS and XDDoS) in cloud computing by current researches do not effectively and efficiently solve the problem (see table 1) hence a counter-measure for XDDoS attacks in cloud computing service model is required, so that the cloud computing paradigm can be fully adopted by organisation, knowing that their businesses would not be hampered by XDoS and its distributed variant. Cloud computing as one of the recent trends in the world of Information Technology which has come with numerous benefits as highlighted in the earlier part of this paper has come to stay and should be adopted as a new paradigm by organizations and business owners. Cloud computing as a technology has a lot of challenges and issues associated with it which include, trust issues, security issues, insider threat issues, quality of service of cloud providers, reliability and availability of data, etc. this issues has hindered its adoption for a while now, but despite all this issues, companies keep migrating to the cloud on a daily basis.

4. Recommendation

To this end for this technology to be fully adopted without fear of businesses and normal computer users being attacked with XDoS and its distributed variant, there is a need for continuous research to yield efficient and effective solutions. In our future study we will present a modern solution to the application-based DDoS (XDoS and XDDoS) in software as a service (SaaS) cloud computing service model which will go a long way to increase its usage and adoption worldwide.

References

[1] P. Zaroo, "A Survey of DDoS attacks and some DDoS defense mechanisms," Advanced Information Assurance (CS 626), 2002.

[2] ARBOR, "The Importance of On-Premise DDoS Protection," ARBOR NETWORKS, 2013.

[3] R. Arora and K. S. Bajaj, "Highly Effective Advanced Technology "HEAT" Re-defining Technology for Hospital Management," International Journal of Management & Behavioural Sciences, vol. Special Edition, pp. 68-73, March 2013.

[4] Skillsoft, "Cloud Computing Basics," 2013.

[5] CISCO, "Cisco Cloud Computing - Data Center Strategy, Architecture and Solutions. Point of view white paper for U.S. public sector," Cisco Systems, Inc., 2009.

[6] C. Gong, J. Lui, H. Chen and Z. Gong, "The Characteristics of Cloud Computing," in International Conference on Parallel Processing Workshops, 2010.

[7] F. Fan, F. Lei and J. Wu, "The Integration of Cloud Computing and the intrction," in Networked Computing and Advanced Information Management (NCM), 2011 7th International Conference, Gyeongju, 2011.

[8] P. Mell and T. Grance, "The NIST Definition of Cloud Computing (Recommendations of the National Institute of Standards and Technology)," National Institute of Standards and Technology US Department of Commerce, Gaithersburg, MD 20899-8930, 2011.

[9] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel and M. Rjarajan, "A survey of intrusion detection techniques in cloud," Jornal of Network and Computer Applications, pp. 42-57, 2013.

[10] A. M. Lonea, D. E. Popescu and H. Tianfield, "Detecting DDoS Attacks in Cloud Computing Environment," International Journal of Computing Communication & Control, pp. 70-78, 2013.

[11] F. Sabahi, "Cloud Computing Security Threats and Responses," in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference, Xi'an, 2011.

[12] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications., vol. 34, no. 1, pp. 1-11, 2011.

[13] A. Chonka, Y. Xiang, W. Zhou and A. Bonti, "Cloud Security defence to protect cloud computing against HTTP-DoS and XML-DoS," Journal of Network and Applications, vol. 34, pp. 1097-1107, 2011.

[14] A. Fowler, "Fear in the Fast Lane," 17 08 2009. [Online]. Available: http://www.abc.net.au/4corners/content/2009/s2655088.htm.