Scientific Research Publishing

Journal of Information Security, 2022, 13, 66-75
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Measuring the Impact of DoS Attack on Availability: Empirical Study Based on Accessibility

Suhail Qadir[1], Uzair Bashir[2]

[1]Directorate of IT & SS, University of Kashmir, Srinagar, India
[2]Computer Science, DSE, Srinagar, India
Email: suhailmir@uok.edu.in, ub.cs@uok.edu.in

How to cite this paper: Qadir, S. and Bashir, U. (2022) Measuring the Impact of DoS Attack on Availability: Empirical Study Based on Accessibility. *Journal of Information Security*, **13**, 66-75.
https://doi.org/10.4236/jis.2022.132004

Received: February 4, 2022
Accepted: April 8, 2022
Published: April 11, 2022

Abstract

Information Security is determined by three well know security parameters *i.e.* Confidentiality, Integrity and Availability. Availability is an important pillar when it comes to security of an information system. It is dependent upon the reliability, timeliness and accessibility of the Information System. This paper presents an analytical view of the fact that when Accessibility is degraded during the presence of an ongoing attack, the other factors reliability and timeliness can also get affected, therefore creating a degrading impact on the overall Availability of the system, which eventually leads to the Denial of Service Attack and therefore affecting the security of the System.

Keywords

Security, Availability, Reliability, Timeliness, Accessibility, DoS Attack

1. Introduction

From the perspective of the user there are two views of an Information System; one is the external view of the system *i.e.* the set of services and functionalities the system provides to the users of the Information System. The other is the inside view of the Information System *i.e.* the design and architecture of the system, how the different software/hardware components interact with each other in order to provide the services and functionalities to the users of the information system. The external view is also called the system level (service level) view in the realm of information system technology. The well-established principles/attributes at the service level that determine/impact Availability of an Information System existent in theory and practice are *Reliability*, *Timeliness* and *Accessibility* [1]. The determinants provide us with a platform to understand, analyse and measure Availability of an information system at the service level with the help of certain well known metrics.

Linked to the system level determinants that impact Availability there is also a second line of factors that can impact *Availability* indirectly [1] (also known as the second order determinants) *i.e. Security Policy*, *Physical Security*, *Auditing and System Effectiveness Evaluation*, *Redundancy*, *System Monitoring and Operational Controls*, *Backups* and *Business Continuity.* Figure 1 presents the picture of Availability w.r.t determinants and other security attributes of the CIA triad. The determinants, Reliability, Timeliness and Accessibility [2] and the respective metrics [3] are very critical in understanding, measuring and analysing *Availability* of an *Information System.* Keeping in mind the three determinants mentioned above availability can be either 0 or 1 [4]. 0 means no availability and 1 means any acceptable level of availability. But in practice whenever Availability is discussed the security practitioners and stakeholders are more inclined towards first two determinants *i.e.* Reliability and Timeliness [5]. Accessibility is certainly not ignored but is discussed the least and is not taken as seriously as a measuring entity as the first two are taken. This surely does not mean Accessibility is not important. Accessibility describes more the behavioural aspect of the system rather than a serious system defining metric. The focus of the paper is to analyse how the Accessibility is impacted by DoS attacks. For this purpose a discussion on the system level factors that impact Availability is presented first and followed by an experimental evaluation of the impact of DoS attacks on accessibility.

2. Determinants of Availability

The attributes that determine Availability of an Information System at the service level are:

Reliability is the extent to which an information system performs its expected function over a given duration of time [6] and [7]. Reliability is not the only factor or the lead factor that impacts availability and it should be noted that the measurement of reliability alone cannot be taken as the measurement of availability of

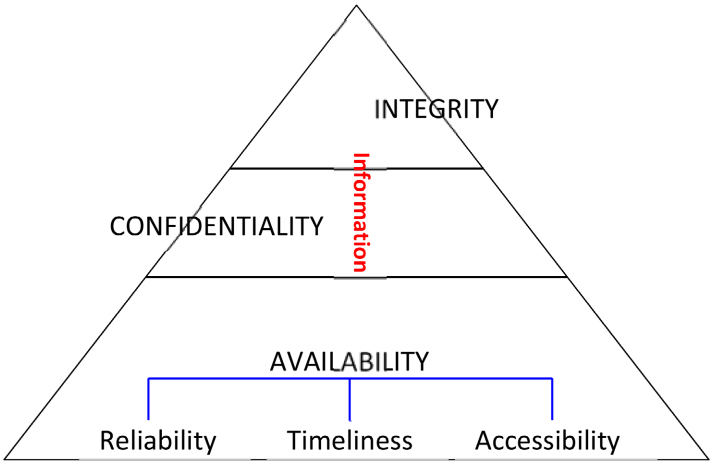

Figure 1. System level determinants of availability and the CIA triad.

an information system *i.e.* 99% reliability of an information system does not mean 99% availability of the information system. Reliability is the ability of an information system to perform its function nonstop while as the goal of Availability is much broader and is the ability of the information system to provide services to the legitimate clients whenever and wherever demanded. Reliability of an information system provides us with a metric that tells us about the failures of a component. The component (Hardware/Software) is most reliable when the component is in its "Useful Life". The metric for reliability [8] [9] and [10] is trifold *Mean Time between Failures* (*MTBF*), *Mean Time to Failure* (*MTTF*) and *Failure Rate.*

Timeliness is the response of an information system to a user request in a suitable amount of time. Delayed response is equivalent to no-response in today's world, given the speed and efficiency at which information processing and communicating systems work these days. Given the criticality of time w.r.t Availability, this metric is the most used and mentioned in determining the Availability of an information system. There are two things to be seen here, one is the individual time of each request/message and the second is the overall time all the requests/messages (includes idle time as well). Generally when it comes to measuring Availability we are interested in the second one *i.e.* the overall time or better put as the extent (time) to which an information system or resource is processing or working without any interruption or outage (*Uptime*) [11] and [12]. We are also interested in the time when the information system or resource is not processing or working (*Downtime*) *i.e.* outage, repairing time or the time during up gradation of a system, or any other time when the system is down. Availability is measured in terms of *Uptime Ratio*, which gives us the nearest approximation of the most commonly quoted availability metric *i.e.* The *Steady State Availability* [8]. *Uptime Ratio* is the percentage of the system being available without any interruption during the useful life. *Uptime Ratio* is calculated as follows [5]:

$$\text{Uptime Ratio} = \frac{T_u}{T_u + T_d} \text{ or } A = \frac{T_u}{T_u + T_d}$$

where

T_u: Uptime,

T_d: Downtime,

A: Availability.

Another most commonly used Availability metric related to *downtime* is *downtime per year in minutes* and the Information Systems are classified based on the number of 9 s as given in **Table 1** [12].

Accessibility is the extent to which an information system is used concurrently by as many number of users viable without making any changes (like adding new hardware for more users) to the Information System. All the concurrent users should be in active state and should be subscribed and authorized to whatever services the Information System provides. Now to grant access to an

Table 1. The availability league (six 9's).

Availability %	Downtime %	Downtime per Year
98%	2%	7.3 days
99%	1%	3.65 days
99.8%	0.2%	17 hours, 30 minutes
99.9%	0.1%	8 hours, 45 minutes
99.99%	0.01%	52.5 minutes
99.999%	0.001%	5.25 minutes
99.9999% (Six 9 s)	0.0001%	31.5 seconds

Information System we need gate keeping for letting only authorized users to access the resources. Such gatekeeping is provided by means of *Authentication and Authorization.* Now Accessibility will get impacted if the information requested by the user is unavailable. There can be number of reasons for the information being un-available *i.e.* the server is not responding, network connectivity issues, scheduled maintenance or some malicious attack on the network or server infrastructure. Irrespective of the reasons behind the non-availability of information/network resource, accessibility will be impacted and degraded in any manner and as a result the overall reliability of the system will be impacted significantly.

This paper presents an analytical view of the fact that when *Accessibility* is degraded during the presence of an ongoing attack, the other factors like *reliability* and *timeliness* can also get impacted, therefore impacting the overall *Availability* of the system, which eventually leads to the *Denial of Service Attack.*

3. Experiment

For the explanation of the effect of DoS attack on *Accessibility* we conduct a small scale experiment using a simple network topology given in **Figure 2**. We demonstrate this by stress testing the windows server using *Siege* 2.70 [13], a HTTP/HTTPS based stress testing framework. The objective is to demonstrate how much data or requests the target system can handle concurrently and at the same time give an indication about the systems *Availability* (Accessibility). Overloading the system with requests and data generated through siege may also result in a DoS attack, but primarily here we are more interested in the number of connections that the server can handle concurrently. The tool allows us to strike the server with pre-configured number of concurrent simulated users. The tools give us various performance measures which will be discussed further in the experiment.

3.1. Experiment Setup

The experiment is carried out under controlled conditions on a Local Area Network consisting of a server and a client computer. The configuration of the

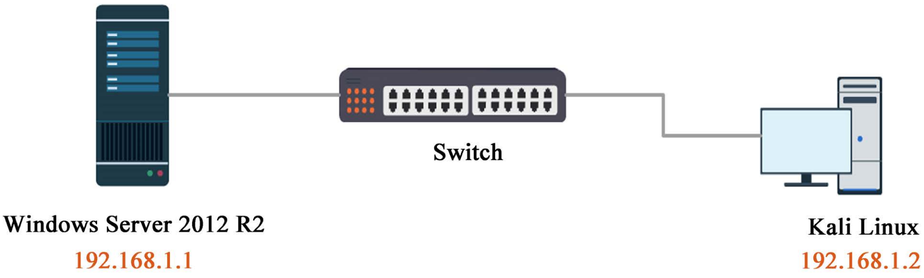

Figure 2. Experiment setup for understanding the effect of DoS attack.

Table 2. System configurations used in experiment.

Machine	Operating System	Hardware Configuration
192.168.1.1 (victim)	Windows server 2012 R2 (6.3 build 9600)	Intel® Core™ 2 Duo 2 GHz, 1 GB RAM
192.168.1.2 (Attacker Machine)	Kali Linux 1.1.0	Intel® Core™ i5 2.8 GHz, 4 GB RAM

machines are presented in Table 2. The server (192.168.1.1) is at the receiving end of the traffic generated by the attacker machine (192.168.1.2). The server machine is configured as an application server and a web server. Besides HTTP, the server is running a number of well-known services like *i.e.* HTTPS, DHCP, FTP, SMTP, Telnet, DNS, NETBIOS, POP3, and MSRPC etc. The windows server is running on *VMware Player V7* [14], hosted on windows 8.1 machine (6.3 build 9600) with Intel® Core™ i5 2.8 GHz, 4 GB RAM, with Intel® Core™ i5 2.8 GHz, 4 GB RAM.

The Siege load testing framework is launched from the machine running Kali Linux (192.168.1.2). Siege has three modes of operation, *internet simulation*, *regression testing* and *brute force*. We will be using brute force for validating the accessibility component of *Availability*. The tool tests the server and bench-marks the server for various performance measurements carried out during the load testing.

3.2. Results and Discussion

After configuring Siege on Kali Linux for load testing we use the following configuration of the tool to test the strength of the target machine:

```
siege -c500 -t10 192.168.1.1
** SIEGE 2.70
** Preparing 500 concurrent users for battle.
The server is now under siege...      done.
```

We created 5 instances of the above configuration and each configuration prepares 500 concurrent simulated users to test the strength of the server for 10 seconds. That means when all the five configurations run concurrently, we are actually striking with a force of 2500 concurrent users. The experiment was repeated 3 times with same configurations under same conditions. The measurements returned are Transactions, Availability, Elapsed time, Data Transferred, Response time, Transaction rate, Concurrency and Failed Transactions, out of which we are only interested in 3 measurements, Availability, Response time and Concurrency. Availability here is different than *Availability* [2] we have been discussing so far, here in *Siege* testing framework it is the percentage of successfully handled socket connections by the server. It is the result of socket failures (including timeouts) divided by the sum of all connection attempts. Response time is the average processing time it took to process each simulated user's requests. Concurrency is the average number connections from each simulated user. The experiment was run with same configurations in all the instances across all the 3 runs.

In the data collected after putting the windows server under siege, in the first instance of the first run, we have 277 successful transactions done with the server by 500 concurrent simulated users. The availability value measured in this configuration is 18%, the average response time of every connection is 6.26 seconds and the number of concurrent connections for the same is 208. Important thing to observe here is the response time, which is well above the permitted Round Trip Time (RTT) [15] is case of an HTTP web request. The availability measured in the second instance is higher at 33%, the average response time of every connection is 5.07 seconds and the number of concurrent connections for the same is 246. Response time is still above the permissible limit in case of HTTP web request. If we go on and analyse all the values of these three parameters (Availability, Response time and Concurrency) in the first run, we find an interesting trend, decrease in response time leads to increase in availability and concurrency as well. Two observation where the response time was under the permissible limit was in instance 4 and instance 5 and in both the cases the concurrency was highest among the other entries in the group. From the first run we deduce that high availability percentage and a lower value of response time produces a higher number of concurrent connections for the server and low availability percentage and a higher value of response time produces a lower number of concurrent connections for the server.

The graphical analysis of the above mentioned facts is done in **Figure 3** and **Figure 4**. In the second run of the experiment a similar trend is observed in the three parameters *i.e.* when the availability if high, the response time is low and low response time also means higher rates in concurrency and the vice versa as well. The response times in instance 2 and 3 are above the permissible limits and in both the cases the availability and concurrency is at lower ends in the group. The highest rate of concurrency is achieved in instance 5 and the lowest response time is also from the same instance. The graphical analysis of these facts is done in **Figure 5** and **Figure 6**.

The third run of the experiment showed a similar trend as the preceding experiments, Availability and Concurrency showed maximum growth when the response time was lowest.

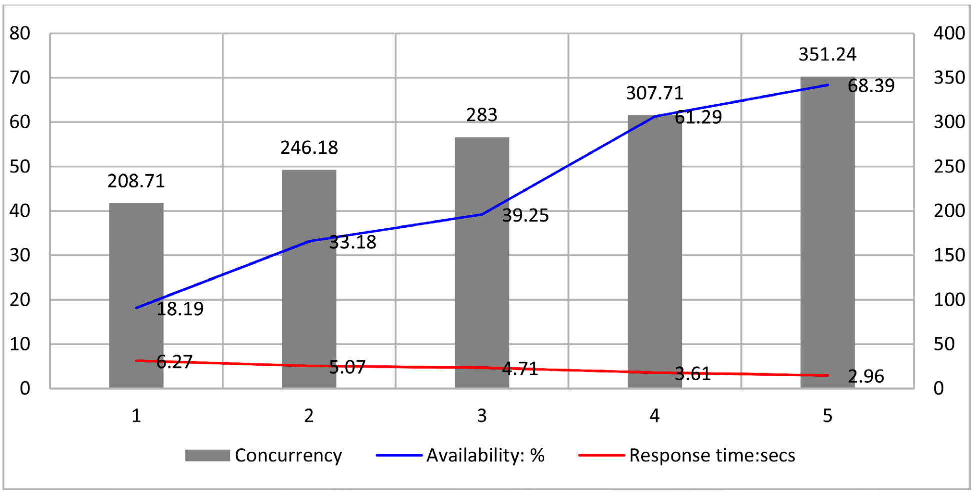

Figure 3. Run 1, measurements of concurrency, availability and response time.

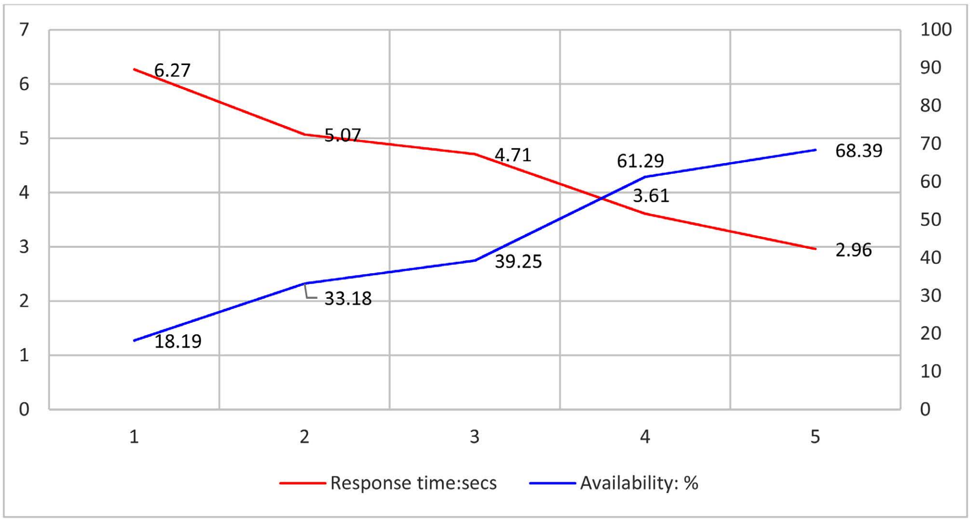

Figure 4. Run 1, comparison of availability and response time.

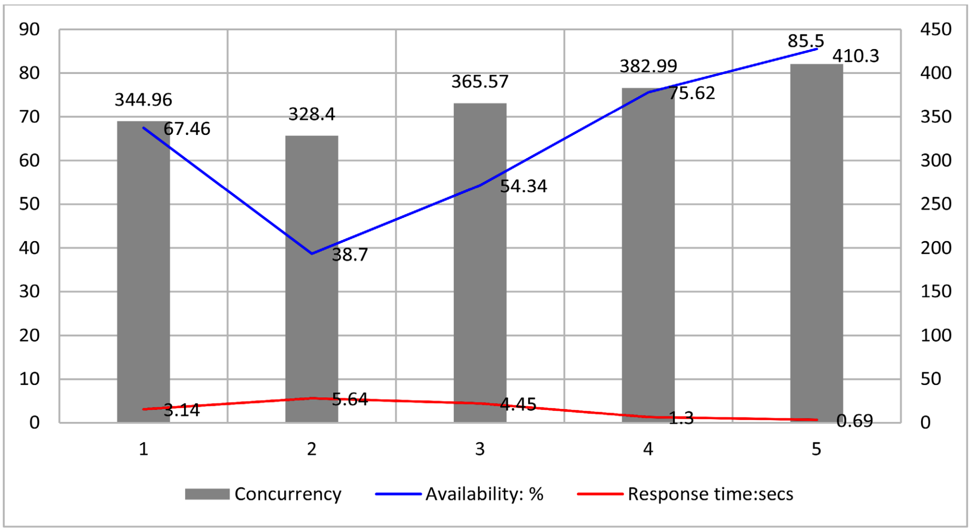

Figure 5. Run 2, measurements of concurrency, availability and response time.

The first two instances achieved 100% availability and in both the cases the response time was well within the limits of universally accepted values. The concurrency was highest in the fifth instance and no surprises for response time being the lowest here among the group. The graphical analysis of these facts is done in Figure 7 and Figure 8. Also this run produced the highest number of successful transactions and the lowest number of failed transactions.

4. Conclusion

With respect to using the siege framework for evaluating the *Accessibility* of an information system *i.e.* the number of concurrent connections that a server supports, we conclude with the fact that there exists a relation between *Concurrency*, *Response Time and Availability*. Higher number of concurrent connections

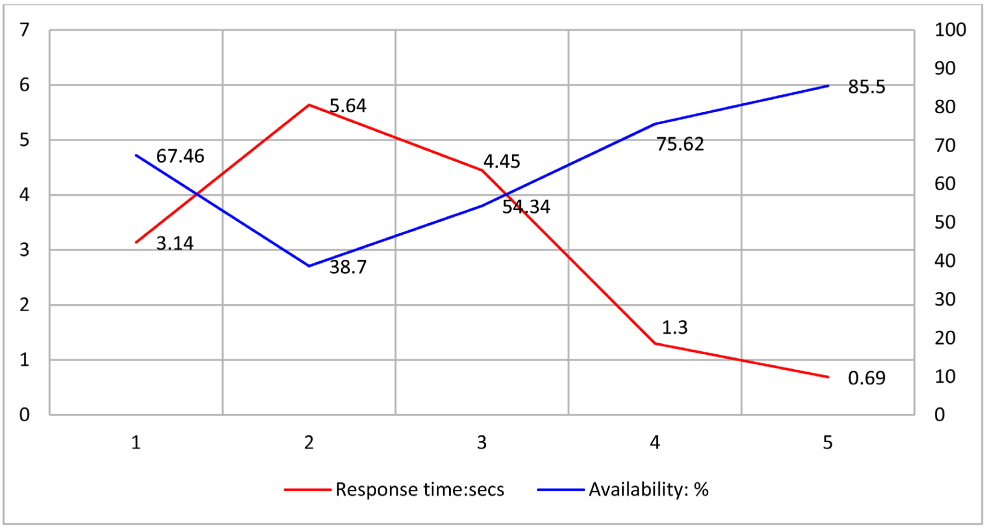

Figure 6. Run 2, comparison of availability and response time.

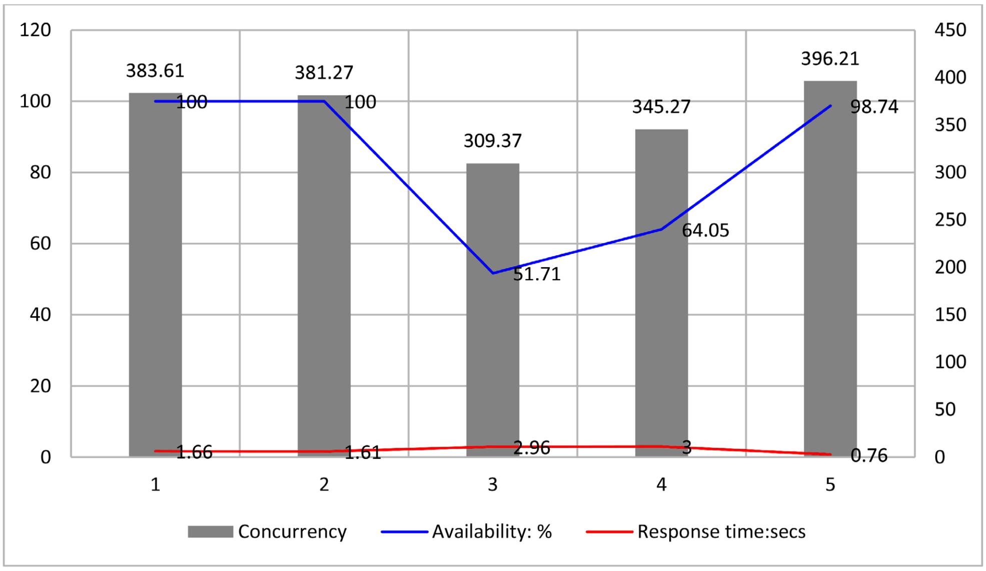

Figure 7. Run 3, measurements of concurrency, availability and response time.

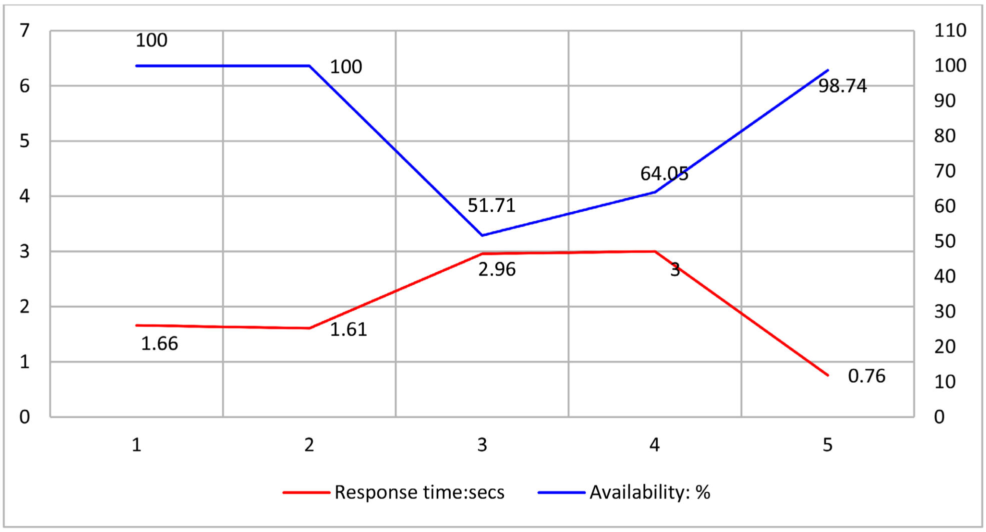

Figure 8. Run 3, comparison of availability and response time.

are possible only when the response time of every user request is low, preferably below the universally accepted mark (refer to [15] for universal standard operation requirement). The vice versa is true as well, when the response time is high, the concurrency is low. Now under normal conditions in the system the response time will mostly be under permissible limits, which therefore won't affect the number of concurrent connections that a server can support. But going by the results of experiment, a DoS attack can severely impact the response time (ICMP response time or RTT) and in the table we have seen how the response time jumped beyond the permissible limits once the attack was launched. It even reached infinite (server unreachable). Now once the response time starts increasing, the availability and concurrency start decreasing. In other words the increase in response time leads to decrease in the number of concurrent connections that a server can support. In worst cases very high response time will lead to no concurrent connections or no connections at all, leading to what we call as a Denial of Service Attack and therefore in the process affecting *Accessibility*.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Khazanchi, D. and Martin, A.P. (2009) Information Availability. In: Gupta, J.N.D. and Sharma, S., Eds., *Handbook of Research on Information Security and Assurance*, IGI Global, Hershey, 230-239. https://doi.org/10.4018/978-1-59904-855-0.ch019

[2] Qadir, S. and Quadri, S.M.K. (2016) Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, **7**, 185-194. https://doi.org/10.4236/jis.2016.73014

[3] Mir, S.Q. and Quadri, S.M.K. (2019) Component Based Metric for Evaluating

Availability of an Information System: An Empirical Evaluation. *International Journal of Information Technology*, **11**, 277-285.
https://doi.org/10.1007/s41870-018-0220-2

[4] Mir, S.Q. and Quadri, S.M.K. (2017) Metric for Evaluating Availability of an Information System: A Quantitative Approach Based on Component Dependency. *International Journal of Network Security & Its Applications*, **9**, 1-11.
https://doi.org/10.5121/ijnsa.2017.9201

[5] Mir, S.Q. (2018) Ensuring Availability of Information by Preventing Denial of Service Attack. Doctoral Dissertation, University of Kashmir, Kashmir.

[6] Lyu, M.R. (1996) Handbook of Software Reliability Engineering.

[7] Sahu, K. and Srivastava, R.K. (2019) Revisiting Software Reliability. In: *Data Management*, *Analytics and Innovation*, Springer, Berlin, 221-235.
https://doi.org/10.1007/978-981-13-1402-5_17

[8] Rohani, H. and Roosta, A.K. (2014) Calculating Total System Availability. Information Services Organization, Amsterdam.

[9] Kone, D. (2021) High Availability Systems. Master's Thesis, University of Helsinki, Helsinki.

[10] Wang, A.J.A. (2005) Information Security Models and Metrics. *Proceedings of the* 43*rd Annual Southeast Regional Conference*, Volume 2, 178-184.
https://doi.org/10.1145/1167253.1167295

[11] Engelmann, C., Scott, S.L., Leangsuksun, C. and He, X. (2008) Symmetric Active/Active High Availability for High-Performance Computing System Services: Accomplishments and Limitations. 2008 *Eighth IEEE International Symposium on Cluster Computing and the Grid* (*CCGRID*), Lyon, 19-22 May 2008, 813-818.
https://doi.org/10.1109/CCGRID.2008.78

[12] Marcus, E. and Stern, H. (2003) Blueprints for High Availability. John Wiley & Sons, Hoboken.

[13] (2022) Siege (Software). Wikipedia, the Free Encyclopaedia.
https://en.wikipedia.org/w/index.php?title=Siege_(software)&oldid=722155219

[14] Bugnion, E., Devine, S., Rosenblum, M., Sugerman, J. and Wang, E.Y. (2012) Bringing Virtualization to the x86 Architecture with the Original VMware Workstation. *ACM Transactions on Computer Systems* (*TOCS*), **30**, 12.
https://doi.org/10.1145/2382553.2382554

[15] Mirkovic, J., Fahmy, S., Reiher, P., Thomas, R., Hussain, A., Schwab, S. and Ko, C. (2006) Measuring Impact of Dos Attacks. In *Proceedings of the* 2*nd ACM Workshop on Quality of Protection*, June 2006, 53-58.