CHAPTER 7

EXPERIMENTAL RESULTS

This chapter analyzes the results obtained after performing the network and application level DDoS attacks on the Single tier and three tier infrastructures. The criteria for analyzing the success and failure of the architectures is based on Real User Monitoring parameters as ICMP Response, Browser Throughput, Page Load Response and Application server response.

7.1 PERFORMANCE RESULTS - SINGLE TIER ARCHITECTURE

Real User Monitoring parameter values for ICMP, Page Load, Browser Throughput and Application Server Response obtained before and during the DDoS attacks on Single Tier Architecture are presented in the Figure 7.1 below.

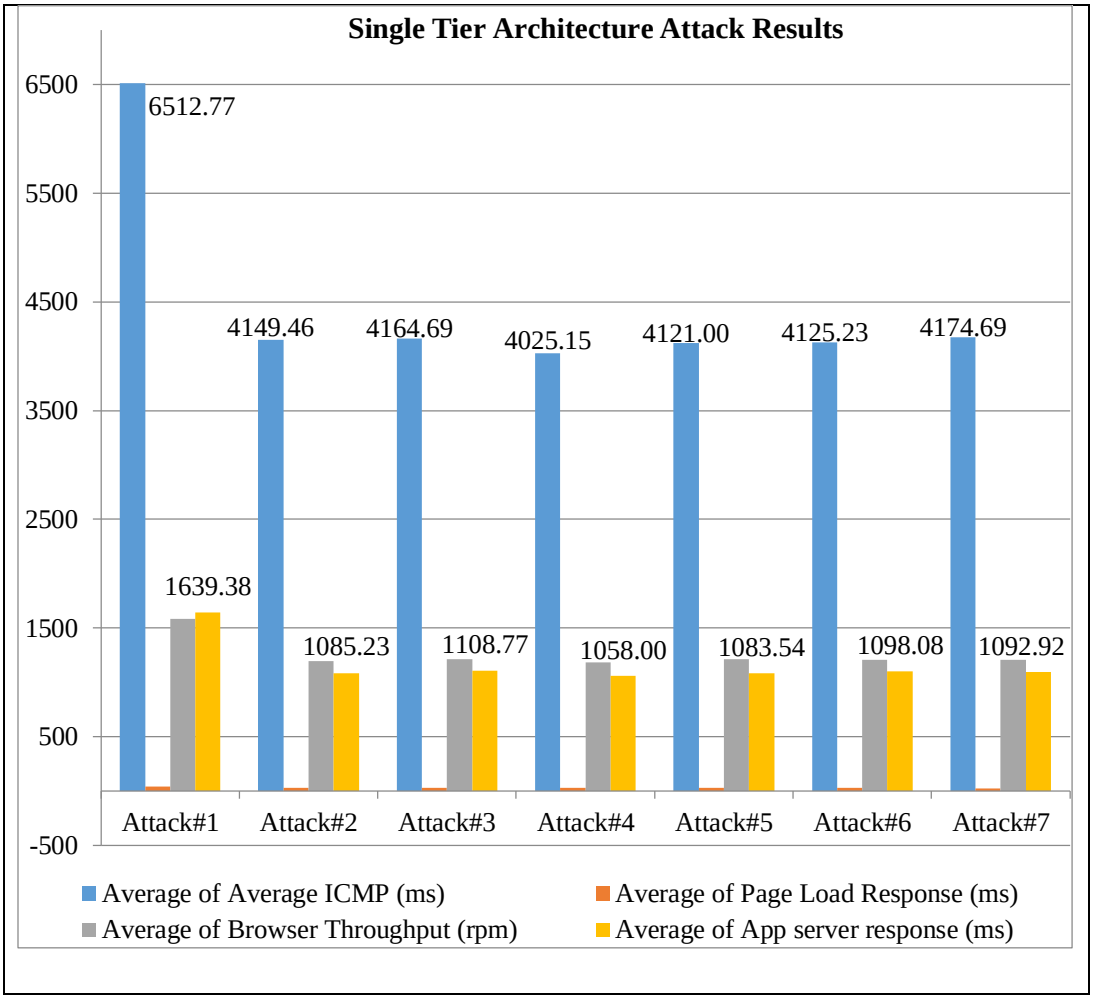

Figure 7.1 Single Tier Architecture Attack Results

7.2 PERFORMANCE RESULTS - THREE TIER ARCHITECTURE

Real User Monitoring parameter values for ICMP, Page Load, Browser Throughput and Application Server Response obtained before and during the DDoS attacks on the Three Tier Architecture are presented in the Figure 7.2 below.

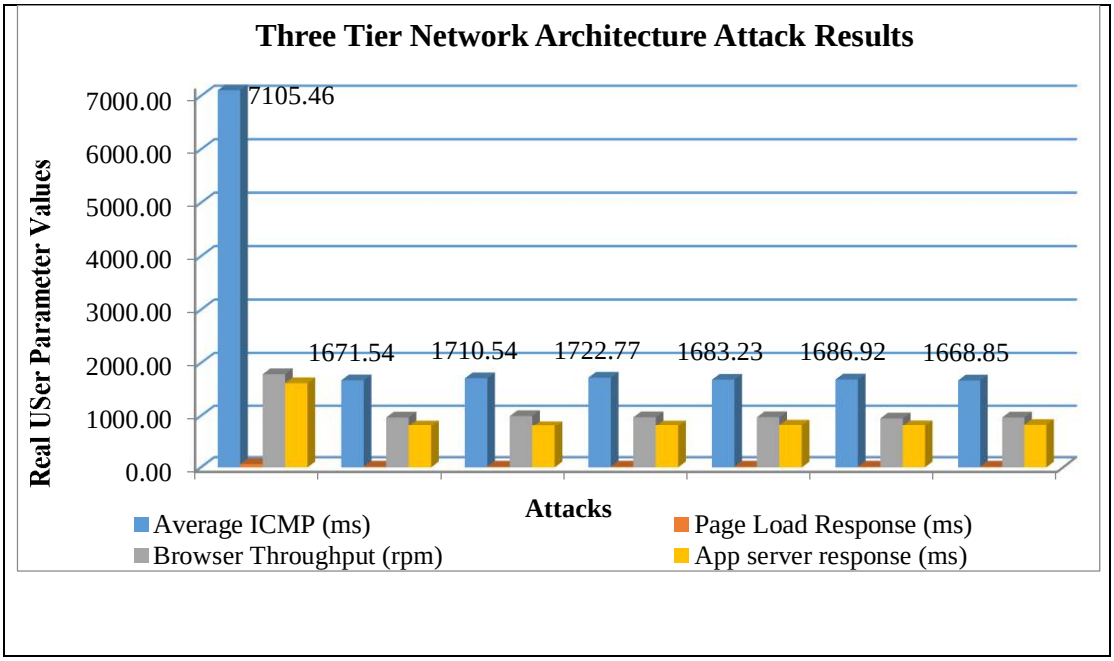

Figure 7.2: Three Tier Network Architecture Attack Results

Comparing Single Tier and Three Tier Architecture results for ICMP Responses during and after the DDoS attack are presented in the Figure 7.3.

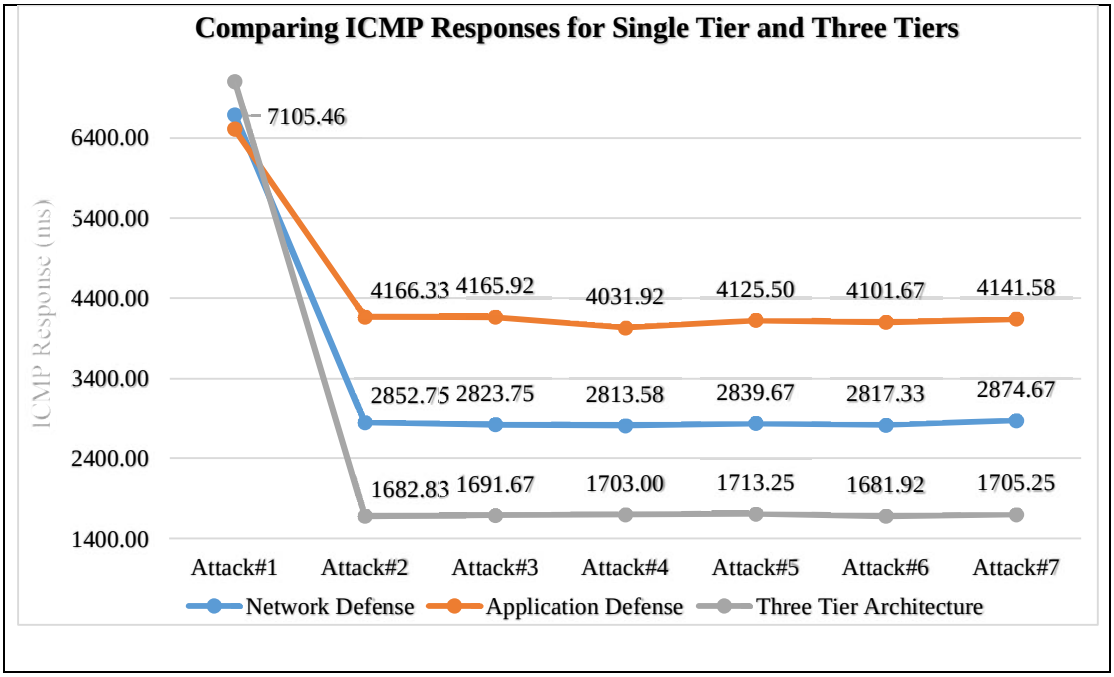

Figure 7.3: ICMP Response comparison results

Comparing Single Tier and Three Tier Architecture results for Page Load Responses during and after the DDoS attack are presented in the Figure 7.4.

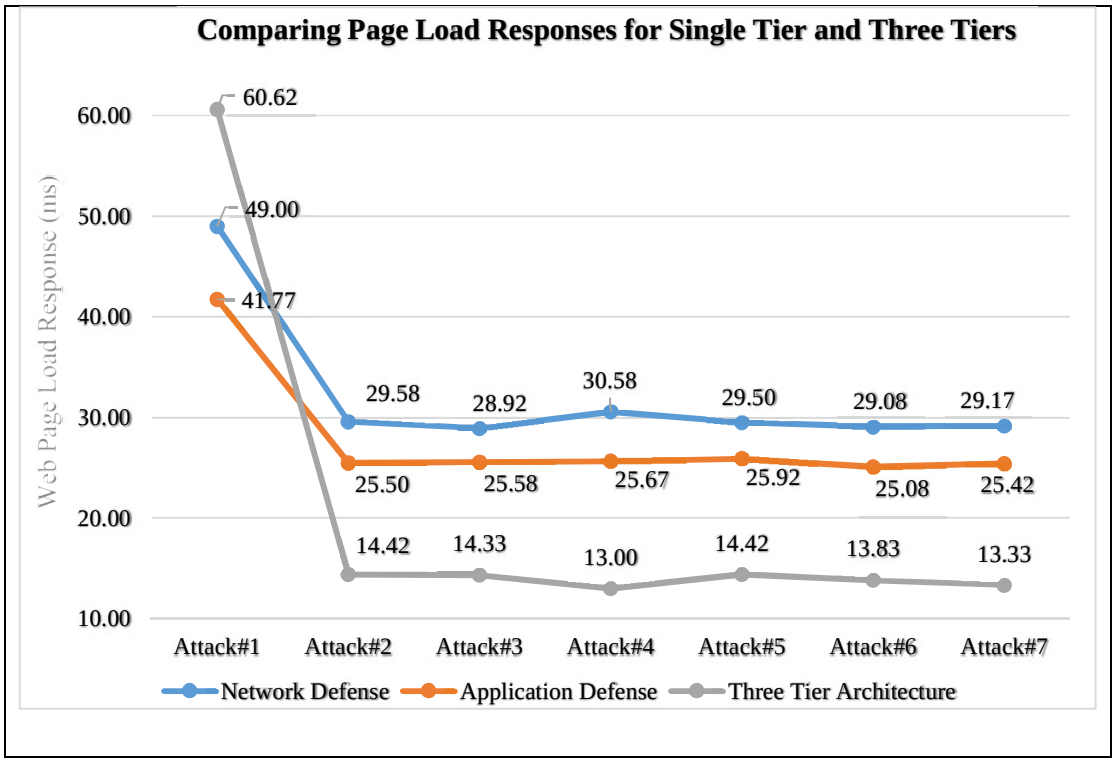

Figure 7.4: Page Load response results

Comparing Single Tier and Three Tier Architecture results for Browser Throughput during and after the DDoS attack are presented in the Figure 7.5.

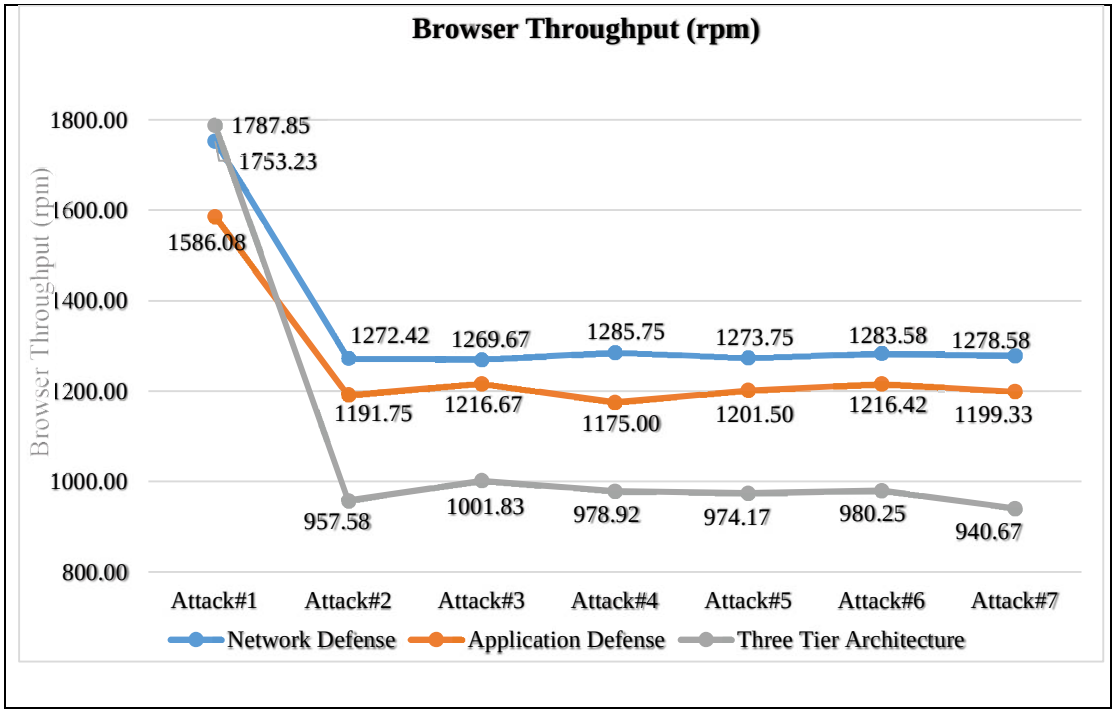

Figure 7.5: Browser Throughput comparison results

Comparing Single Tier and Three Tier Architecture results for ICMP Responses during and after the DDoS attack are presented in the Figure 7.6.

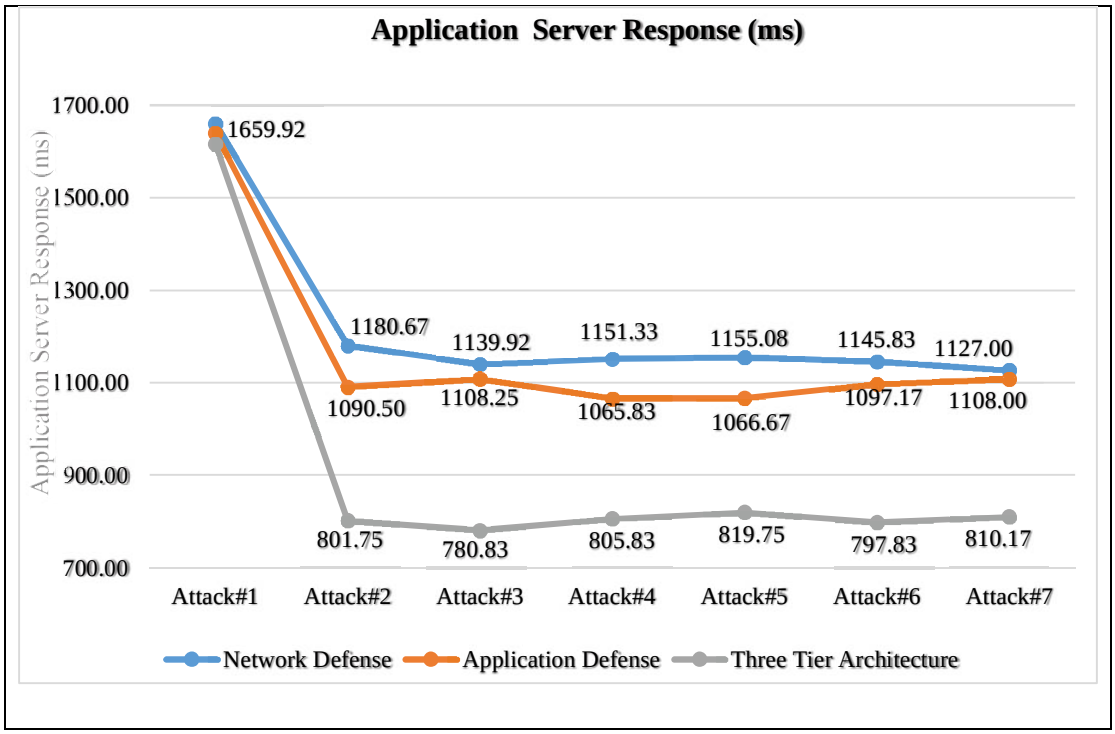

Figure 7.6: Real User Monitoring – Application Server Response

7.3 VALIDATING TEST RESULTS

The author performed Parametric Statistic T-test to ensure the Real User Monitoring data obtained from Single and Three Tier architectures has no violations for the data presented in a random sample from the test population, the distribution of the sample mean is normal and the variances of different real user parameter very similar. The null hypo is assumed that if the data violates these assumptions, then it is assumed the author committed a Type I error which is more or less often than the alpha probability and the T-Test results are interpreted as follows.

T	denotes the T-Test
DF(x)	denotes the degree of freedom for # of test performed
x.xx	denotes the 'T-Static' value of the calculations
$p \leq 0.05$	Not likely to be a result of chance and A ≠ B Which implies difference is significant → Null hypo is incorrect Hence Null is rejected, relationship between A and B
$p \geq 0.05$	Likely chance and A = B Which signifies no significant difference → Null hypo is correct Hence fail to reject the Null, no relationship between A and B

Table 7.1: T Test Validation parameters

7.3.1 T-TEST VALIDATION FOR AVERAGE ICMP RESPONSE

	Average ICMP (ms)		
Attack#	**Network Defense**	**Application Defense**	**Three Tier Architecture**
Attack#1	6690.08	6512.77	7105.46
Attack#2	2852.75	4166.33	1682.83
Attack#3	2823.75	4165.92	1691.67
Attack#4	2813.58	4031.92	1703.00
Attack#5	2839.67	4125.50	1713.25
Attack#6	2817.33	4101.67	1681.92
Attack#7	2874.67	4141.58	1705.25

Table 7.2: Average ICMP for Single Tier and Three Tier Infrastructures

T-Test Summary for Average ICMP Response:

Variable	Observations	With missing data	Without missing data	Minimum	Maximum	Mean	Standard Deviation
6545	90	0	90	2618.000	6995.000	3342.400	1330.157
7655	90	0	90	1523.000	7993.000	2406.511	1860.344

Table 7.3: T-Test Summary for Average ICMP

95% Confidence interval (CI) on difference between the two means:

] 806.553, 1065.225 [

Difference	**935.889**
Observed value (t)	**14.378**
Critical value (|t|)	**1.987**
Degree of Freedom (DF)	**89**
Two-tailed P-value	**< 0.0001**
The ALPHA	**0.05**

Table 7.4: T-test for Two Paired Single Tier and Three Tier Data

Test Interpretation:

H0: difference between two means = 0

Ha: difference between two means $\neq 0$

Since the P-value is less than the significance level alpha (0.05) → hence the Null Hypo (H0) is rejected and the Alternative Hypo (Ha) is accepted.

7.3.2 T-TEST VALIDATION FOR PAGE LOAD RESPONSE

	Page Load Response (ms)		
Attack#	**Network Defense**	**Application Defense**	**Three Tier Architecture**
Attack#1	49.00	41.77	60.62
Attack#2	29.58	25.50	14.42
Attack#3	28.92	25.58	14.33
Attack#4	30.58	25.67	13.00
Attack#5	29.50	25.92	14.42
Attack#6	29.08	25.08	13.83
Attack#7	29.17	25.42	13.33

Table 7.5: Page Load Response for Single Tier and Three Tier Infrastructure

T-Test Summary for Page Load Response:

Variable	Observations	With missing data	Without missing data	Minimum	Maximum	Mean	Standard Deviation
45	90	0	90	27.000	55.000	32.000	7.213
50	90	0	90	10.000	72.000	20.311	16.593

Table 7.6: T-Test Summary for Page Load Response

95% Confidence interval (CI) on difference between the two means:

] 9.551, 13.827 [

Difference	**11.689**
t (Observed value)	**10.865**
|t| (Critical value)	**1.987**
DF	**89**
P-Value (Two-tailed)	**< 0.0001**
ALPHA	**0.05**

Table 7.7: T-test for Two Paired Single Tier and Three Tier Data

Test Interpretation:

H0: difference between two means = 0

Ha: difference between two means $\neq 0$

Since the P-value is less than the significance level alpha (0.05) → hence the Null Hypo (H0) is rejected and the Alternative Hypo (Ha) is accepted.

7.3.3 T-TEST SUMMARY FOR BROWSER THROUGHPUT

	Browser Throughput (rpm)		
Attack#	**Network Defense**	**Application Defense**	**Three Tier Architecture**
Attack#1	1753.23	1586.08	1787.85
Attack#2	1272.42	1191.75	957.58
Attack#3	1269.67	1216.67	1001.83
Attack#4	1285.75	1175.00	978.92
Attack#5	1273.75	1201.50	974.17
Attack#6	1283.58	1216.42	980.25
Attack#7	1278.58	1199.33	940.67

Table 7.8: Browser Throughput for Single Tier and Three Tier Infrastructure

T-Test Summary for Browser Throughput:

Variable	Observations	With missing data	Without missing data	Minimum	Maximum	Mean	Standard Deviation
1800	90	0	90	1203.000	1856.000	1339.233	169.120
1775	90	0	90	850.000	1887.000	1080.478	287.208

Table 7.9: T-Test Summary for Browser Throughput

95% Confidence interval (CI) on difference between the two means:

] 228.425, 289.086 [

Difference	**258.756**
Observed value (t)	**16.951**
Critical value (|t|)	**1.987**
DF	**89**
Two-tailed P-value	**< 0.0001**
The ALPHA	**0.05**

Table 7.10: T-test for Two Paired Single Tier and Three Tier Data

Test Interpretation:

H0: difference between two means = 0

Ha: difference between two means $\neq 0$

Since the P-value is less than the significance level alpha (0.05) → hence the Null Hypo (H0) is rejected and the Alternative Hypo (Ha) is accepted.

7.3.4 T-TEST SUMMARY FOR APPLICATION SERVER RESPONSE

	Application Server Response (ms)		
Attack#	**Network Defense**	**Application Defense**	**Three Tier Architecture**
Attack#1	1659.92	1639.38	1616.38
Attack#2	1180.67	1090.50	801.75
Attack#3	1139.92	1108.25	780.83
Attack#4	1151.33	1065.83	805.83
Attack#5	1155.08	1066.67	819.75
Attack#6	1145.83	1097.17	797.83
Attack#7	1127.00	1108.00	810.17

Table 7.11: Application Server Response for Single Tier and Three Tier Infrastructure

T-Test Summary for Application Server Response:

Variable	Observations	With missing data	Without missing data	Minimum	Maximum	Mean	Standard Deviation
1636	90	0	90	1001.000	1833.000	1221.733	196.171
1528	90	0	90	701.000	1692.000	913.744	286.449

Table 7.12: T-Test Summary for Application Server Response

95% confidence interval on the difference between the means:

] 276.857, 399.120 [

Difference	**307.989**
Observed value (t)	**19.657**
Critical value (|t|)	**1.987**
DF	**89**
Two-tailed P-value	**< 0.0001**
The ALPHA	**0.05**

Table 7.13: T-test for Two Paired Single Tier and Three Tier Data

Test Interpretation:

H0: difference between two means = 0

Ha: difference between two means $\neq 0$

Since the P-value is less than the significance level alpha (0.05) → hence the Null Hypo (H0) is rejected and the Alternative Hypo (Ha) is accepted.

CHAPTER SUMMARY

With Network firewall configured on the first tier and the Web Application Firewall configured on the second tier, network and application attack trend and real user monitoring graphs display a positive response for three tier as compared to the single tier design when comparing ICMP TTL, Browser throughput, Page load response and Application response. The graph in Figure 7.7 below displays the availability trend metrics obtained after performing the DoS attacks on the two architectures for network and application layer design.

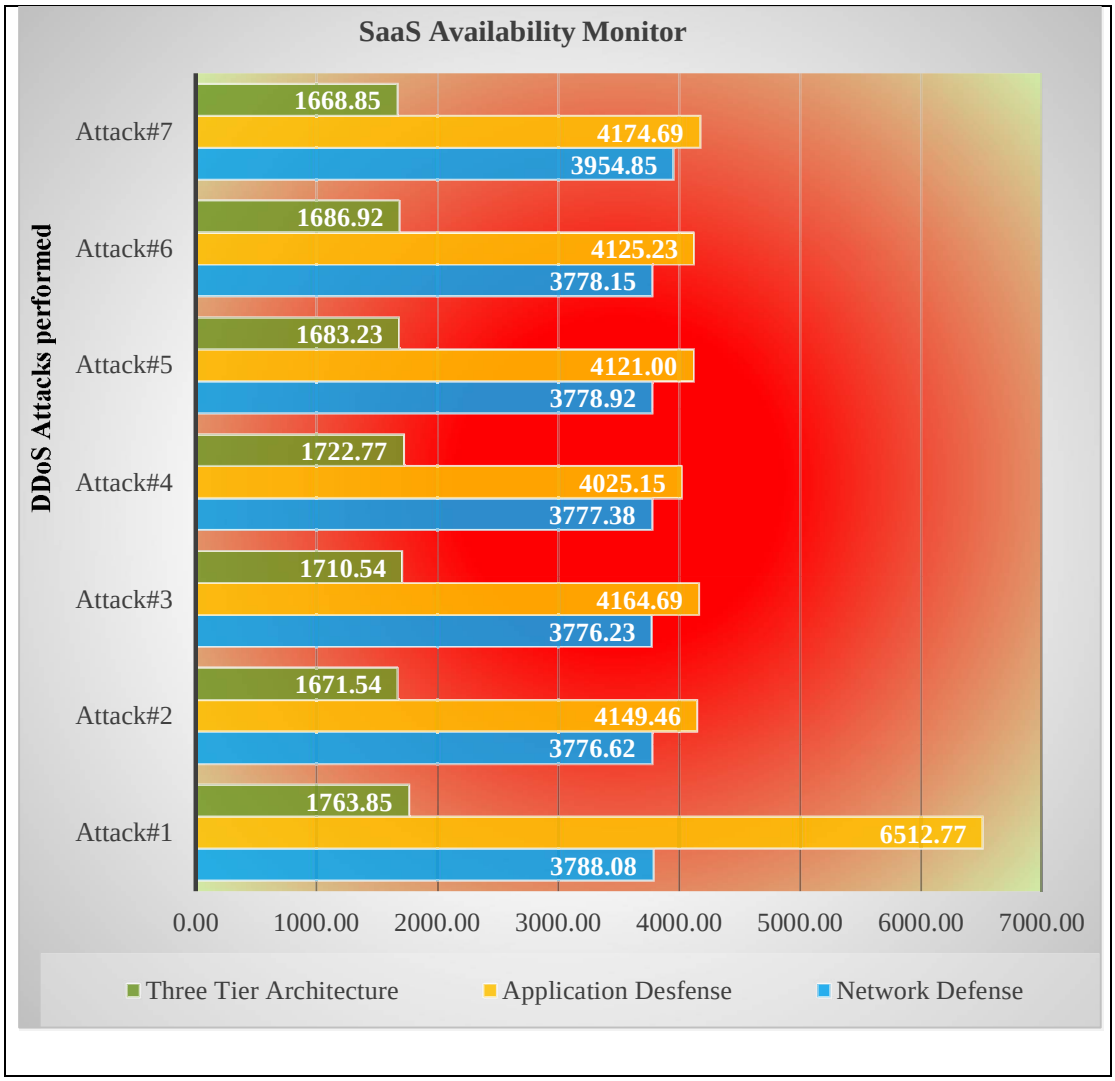

Figure 7.7: Real User Monitoring – SaaS Availability Threshold

Having only the network defense in place in form of a firewall, the SaaS availability takes a major hit during DDoS attacks and the average real user response is always over 3700ms which indicates the application availability is a huge issue. If using only the

application defense, during DDoS attacks the average real user response goes even beyond 4100ms – which clearly indicates the application might not be available.

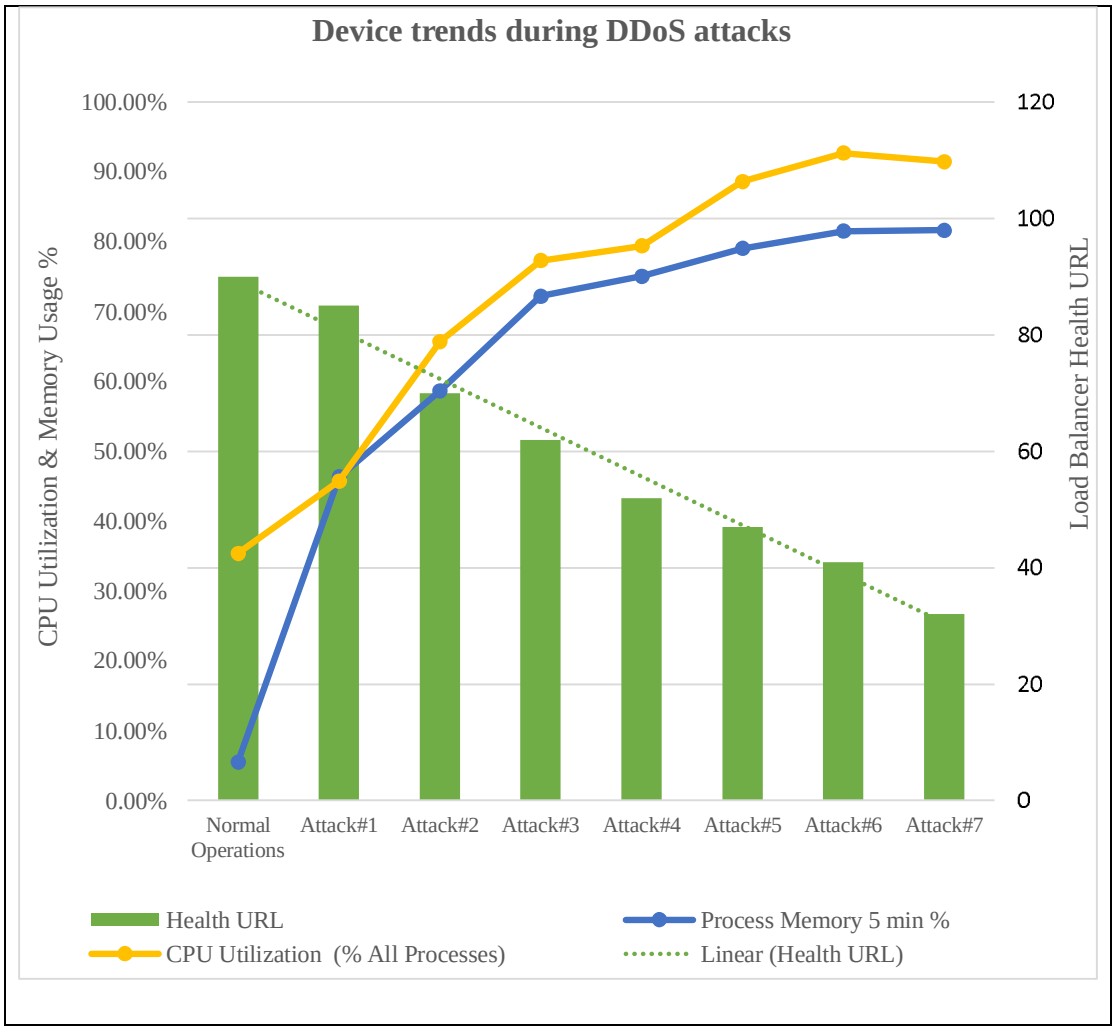

Figure 7.8: Device trends during DDoS attacks

At the same time, with the proposed three tier architecture of network and application defense as separate tiers, for the same DDoS attack, the SaaS average real time response is always around 1600ms – which indicates a healthy, responsive performance is guaranteed. As the size and scope of attacks increase the network devices like Router and Load Balancer also start to show the strain, data for which is illustrated in the Figure 7.8 below, from CPU Utilization %, Process Memory (5 minute) and Load Balancer URL Health.