International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 4, Issue 1, 2025
DOI: https://doi.org/10.5281/zenodo.14745473

Evaluating the Impact of AES-256 Encryption on Network Performance: An Analysis of Transfer Time, Latency and Throughput

Chinwe Chizoba Eromosele[1]

[1] Glasgow Caledonian University (GCU)

Publication Date: 2025/02/06

Abstract

➢ *Background and objectives-*

The file size of plain text impedes network performance. This level of impairment should be used as the benchmark for evaluation of encryption algorithms. The objective of this study is primarily to compare the effects of plain text and AES-256 encryption on network performance. Additionally, it will determine the effect of the encryption on plain text data size and the relationship between data size and selected network performance metrics.

➢ *Materials and methods-*

Plain text and AES-256 encrypted text of various data sizes were categorized into two groups- small to medium data size (10-100MB) and very small data size (0.1-0.9MB). The percentage increase in file size caused by encryption was recorded for each data. They were serially transmitted through EVENG simulated network environment. Transfer time, latency, and throughput were determined. The results were further evaluated using comparison of means, Pearson and Spearman's correlations, line graphs and scatter plots.

➢ *Results-*

The increases in file size after encryption varies from 0.031% at 0.1MB to 0.00003% at 100MB. Graph lines of the metrics against data size are predominantly coincident but differ in pattern between the two categories. Scatter plots and correlation coefficients show a significant ($p<0.05$) positive correlation between transfer time and data size of each text in both categories, latency in the 10-100MB but not in the 0.1-0.9MB categories ($p>0.05$), or throughput in general. Curiously, a significant ($p<0.05$) strong positive correlation exists between throughput and data size in the 0.1-0.5MB range. A throughput saturation value starts at 60 MB for plain text and at 30 MB for cipher text.

➢ *Conclusion-*

AES-256 encrypted text and plain text have similar effects on network performance probably because of the former's negligible effect on data size. Data size positively correlates with transfer time. Similar correlation exists with latency only in the 10-100MB range but not in the 0.1-0.9 MB range and not with throughput. An early, but, transient correlation occurs between data size and throughput in the 0.1-0.9MB range.

➢ *Keywords and Abbreviations:*

Keywords : AES-256 Encryption, Cipher Text, Cryptography, Data Security, Latency, Network Performance, Packet Loss, Throughput.

Abbreviations: AES (Advanced Encryption Standard), PT (Plain Text), CT (Cipher Text), FTP (File Transfer Protocol), WAN (Wide Area Network)

Eromosele, C. C. (2025). Evaluating the Impact of AES-256 Encryption on Network Performance: An Analysis of Transfer Time, Latency and Throughput. *International Journal of Scientific Research and Modern Technology*, *4*(1), 49–58. https://doi.org/10.5281/zenodo.14745473

I. INTRODUCTION

Transmission and storage of data over a network by organizations and individuals is fraught with danger because of malevolent third-party activities. Increasing use of Internet globally, digitalization of world economies and rise in the use of remote work environment during and after Covid 19 pandemic have been associated with rise in cybercrimes. These include attacks on cyber security and data security. Cyber security refers to the protection of technology assets- devices and services, while data security protects information assets (1). Between 2005 and 2022 the reported number of incidents of data security breaches in the United States rose from 157 to approximately 1800 (2). Similarly, in 2022, data breach cost, on the average, $9.44 million in the US, and $4.35 million globally (3). These data highlight the need for robust data security to keep ahead of the increasing sophistication of hackers. Since there is a trade-off between data security techniques and network performance the search for enhanced security must take cognizance of its effect on network performance.

Current data security is derived from three concepts- cryptography, steganography, and a combination of both also known as crypto-steganography (crypto-stego). Cryptography, which is the subject of interest in this report, is a data security technique that scrambles information into a format useful only to authorized parties. It is the oldest and most used of the three data security technologies. Stefnisson estimated that more than 65% of global traffic data was encrypted in 2017 (4).

Encryption ensures confidentiality, integrity, non-repudiation, availability, and authentication of data. During encryption, a normal intelligible plain text (PT) is transcribed into an incomprehensible cipher text (CT) which is reversed during decryption with an appropriate key by the recipient into normal text (5).

Since the adoption of Data Encryption Standard (DES), created by IBM by the National Bureau of standards in 1977 (6) many algorithms have been created. This spurred a rash of comparative studies analyzing their strengths and weaknesses (7-10). The findings of these studies indicate that Advanced Encryption Standard (AES), trumps the rest with respect to efficiency, flexibility, security, and performance. Currently it is considered the strongest encryption algorithm available as there is no evidence that it has been cracked till date (11).

The impact of cryptography on network performance has been examined by many authors, sometimes with conflicting results (12-18). Significantly most of these studies did not compare the effects of encryption and unencrypted data on network performance. This is considered necessary because it is widely believed that data size affects network performance. The larger the data size the more likely it will increase transfer time and cause network congestion. Therefore, plain text, by the sheer size of the data being transmitted, is expected to affect network performance. This effect should be considered normal and used as a bench mark for comparing the degradation of network performance caused by encryption algorithms.

Network performance is an evaluation of the quality of service experienced by its users such as speed of message delivery or document retrieval. Its metrics include transfer time, latency, throughput, bandwidth, packet loss, jitter, efficiency, round trip delay, retransmission, uptime, bandwidth delay, and packet delay.

A delicate balance must be struck between data security and network performance because the latter affects the efficiency of communication across the network. Consequently, poor network performance will adversely affect an organization's operations and staff morale.

The objective of this study is three-fold. The first is to determine by comparative analysis if there are significant differences between the degradation of network performance caused by transmission of plain text and AES-256 encrypted text. This will enable users of AES-256 algorithm carry out an objective cost benefit analysis.

The second objective is to establish the effect of AES-256 encryption on data size of plain text. Lastly, the study will attempt to define the relationship between data size and transfer time, latency or throughput. The results of these will give an inkling into the principles underlying the effects of cryptography on network performance.

II. MATERIALS AND METHODS

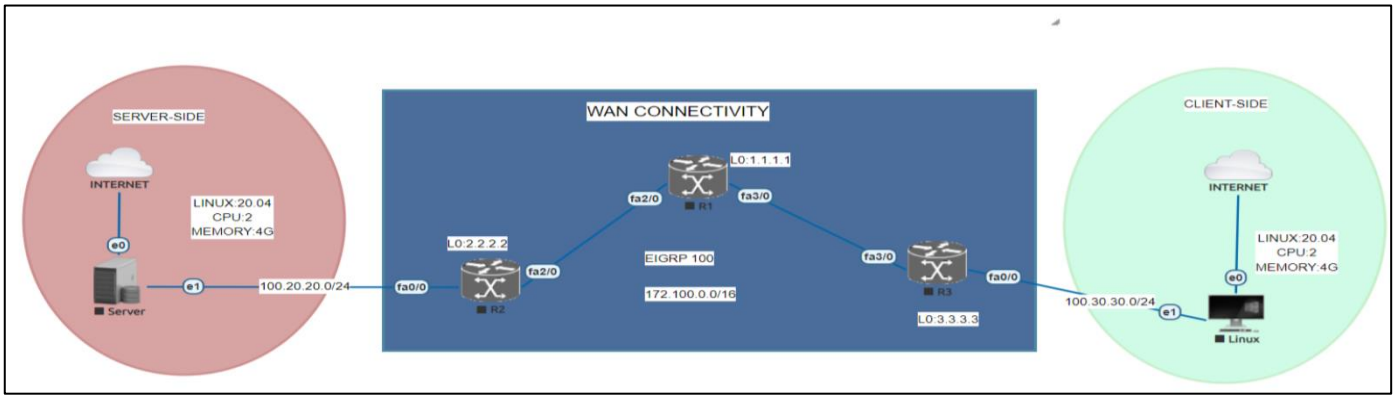

Fig 1 Network Topology used for this Simulation

The experiment was conducted using the EVE-NG network simulator to create a virtualized network environment. The setup consisted of three Cisco routers configured with the Enhanced Interior Gateway Routing Protocol (EIGRP) and two Ubuntu 20.04 systems acting as sender and recipient. The network topology included:

A Cisco router and an Ubuntu system at both the sender and recipient ends.

A third Cisco router representing Wide Area Network (WAN) connectivity, serving as the intermediary between the sender and recipient.

To facilitate encryption and performance measurements, OpenSSL and Netperf were installed and configured on the Ubuntu systems.

➢ *Simulation Procedure:*

The procedure was divided into three stages:

- *Data Preparation:*

Plain Text File Generation: Plain text files with different sizes were created using the dd command in Linux. Encrypted File Creation: Files were encrypted using the AES-256 algorithm via OpenSSL.

- *Data Transmission:*

Data was transmitted from the server (sender) to the client (recipient) using the File Transfer Protocol (FTP). Both plain text and encrypted files were transmitted to observe variations in network performance metrics.

- *Performance Measurement:*

During data transmission, three key network performance metrics—latency, throughput, and transfer time—were monitored and measured using FTP for throughput and transfer time and Netperf for latency.

Data transmission and performance measurement were performed simultaneously to capture real-time impacts of the encryption on network performance.

➢ *Data Categorization and Transmission*

The experiment analysed the transmission of plain text and AES-256 encrypted files across two distinct data size categories:

- Small Files: Ranging from 0.1 MB to 0.9 MB.
- Large Files: Ranging from 10 MB to 100 MB.

➢ *Definition of Terms.*

- *Transfer Time (Seconds*)-

The time it took for data to move from source to destination.

- *Latency,* in Milliseconds (ms)-

The delay in packet transmission from source to destination and back to destination from source

- *Throughput (MB/Second)-*

The quantity of information units a system can handle in a specific length of time.

The results are displayed in tabular and graphic forms as appropriate. Pearson and Spearman's coefficients have been used to determine the strength of relationship between variables while t-test has been used to compare differences in mean values. Probability value of < 0.05 determines the level of statistical significance. Statistical calculations have been done at the website of Social Science Statistics (19), while graphs were drawn using Excel.

III. RESULTS

➢ *Effect of AES-256 Encryption on Plain Text Data Size.*

The sizes of plain text and AES-256 generated cipher text data are recorded in tables 1a and b. The corresponding line graphs are depicted in figures 2a and 2b.

Table 1a Increase in Data Size Associated with Cipher Text for Data Size (10 -100) MB.

Data Size MB	Plain text (PT) bytes	Cryptography Text (CT) bytes	Increase bytes	Increase %
10	10000000	10000032	32	0.00032
20	20000000	20000032	32	0.00016
30	30000000	30000032	32	0.00011
40	40000000	40000032	32	0.00008
50	50000000	50000032	32	0.00006
60	60000000	60000032	32	0.00005
70	70000000	70000032	32	0.00005
80	80000000	80000032	32	0.00004
90	90000000	90000032	32	0.00004
100	100000000	100000032	32	0.00003

Table 1b Increase in Data Size Associated with Cipher Text for Data Size (0.1-0.9) MB.

Data Size MB	Plain text (PT) bytes	Cryptography text (CT) bytes	Increase	Increase %
0.1	100000	100032	32	0.032
0.2	200000	200032	32	0.016
0.3	300000	300032	32	0.011
0.4	400000	400032	32	0.008
0.5	500000	500032	32	0.006
0.6	600000	600032	32	0.005
0.7	700000	700032	32	0.005
0.8	800000	800032	32	0.004
0.9	900000	900032	32	0.004

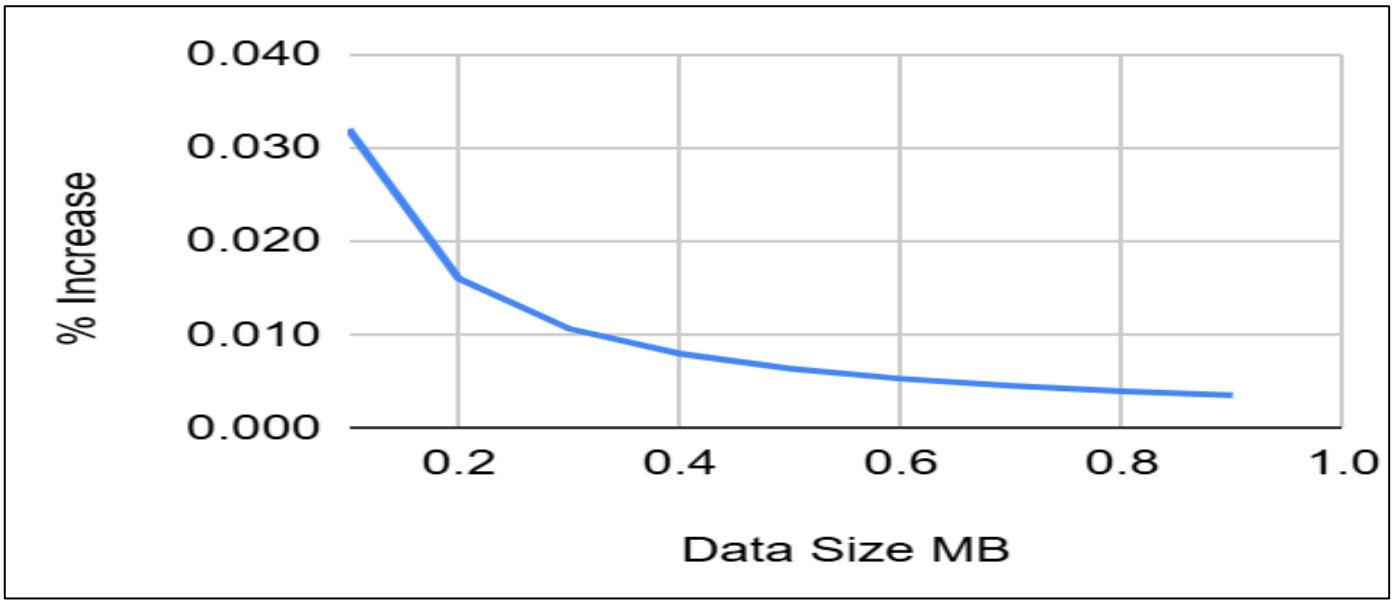

Fig 2a Increase in Data Size Associated with Cipher Text for Data Size (10 – 100) MB.

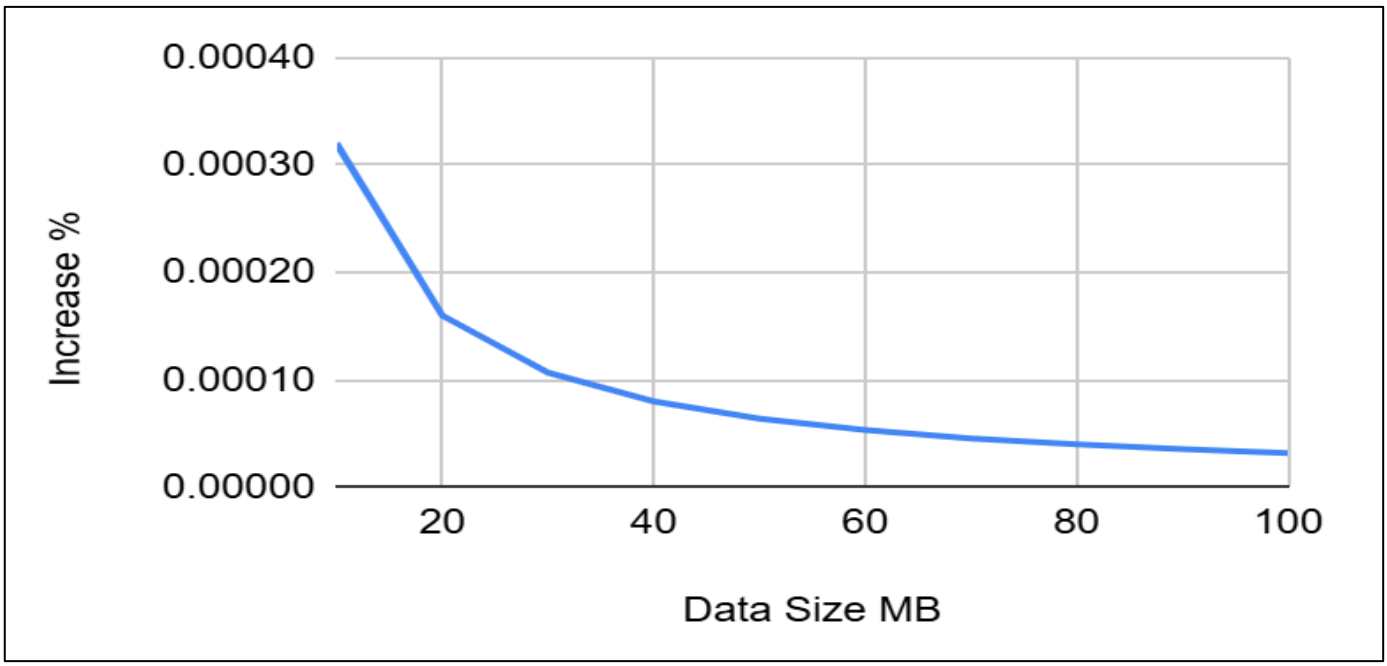

Fig 2b Increase in Data Size Associated with Cipher Text for Data Size (0.1 – 0.9) MB.

As a result of encryption additional 32 bytes have been added to each data size. These extra bytes which contain all information necessary for decryption except the key are also collectively referred to as payload. The line graph of percentage increase against data size shows a curve with an initial rapid decrease which gradually levels towards a minimum as the data size increases (figures 2a and b). The percentage increase varies from (0.03%) at 0.1 MB to < (0.01%) at 100 MB.

➢ *Transfer Time, Latency and Throughput.*

The values of transfer time, latency, and throughput are recorded in tables 2a and b.

Table 2a Transfer Time, Latency, and Throughput for 10 – 100 MB

Data Size MB	Transfer time (sec) PT	Transfer time (sec) CT	Latency (ms) PT	Latency (ms) CT	Throughput (MB/s) PT	Throughput (MB/s) CT
10	373.96	240.37	180.32	171.74	26.37	26.45
20	379.53	378.22	185.9	189.6	52.23	81.26
30	558.58	557.69	269.5	281.4	52.45	52.53
40	773.25	814.3	386.1	415.9	50.52	47.97
50	1007.54	997.79	498.4	453.1	48.46	48.94
60	1248.15	1078.57	618.8	610.1	46.95	54.33
70	1375.16	1370.3	687.5	687.1	49.71	49.89
80	1636.58	1577.77	810.1	790.4	47.74	49.52
90	1755.46	1705.22	824.7	805.1	50.07	52.82
100	1987.31	1959.58	976.6	971.99	49.14	49.83

Table 2b Transfer Time, Latency, and Throughput for 0.1 – 0.9 MB

Data Size MB	Transfer Time (sec) PT	Transfer Time (sec) CT	Latency (ms) PT	Latency (ms) CT	Throughput (MB/s) PT	Throughput (MB/s) CT
0.1	0.15	0.18	48.76	51.9	0.67	0.56
0.2	0.29	0.25	51.12	52.21	0.68	0.79
0.3	0.24	0.27	53.21	48.93	1.2	1.09
0.4	0.3	0.32	47.58	47.5	1.32	1.24
0.5	0.38	0.4	52.84	52.83	1.28	1.22
0.6	0.51	0.54	53.76	52.03	1.16	1.08
0.7	0.52	0.78	50.58	49.58	1.31	0.89
0.8	0.74	0.67	51.34	48.12	1.05	1.16
0.9	0.92	0.76	57.11	50.86	0.97	1.16

- *Transfer time*

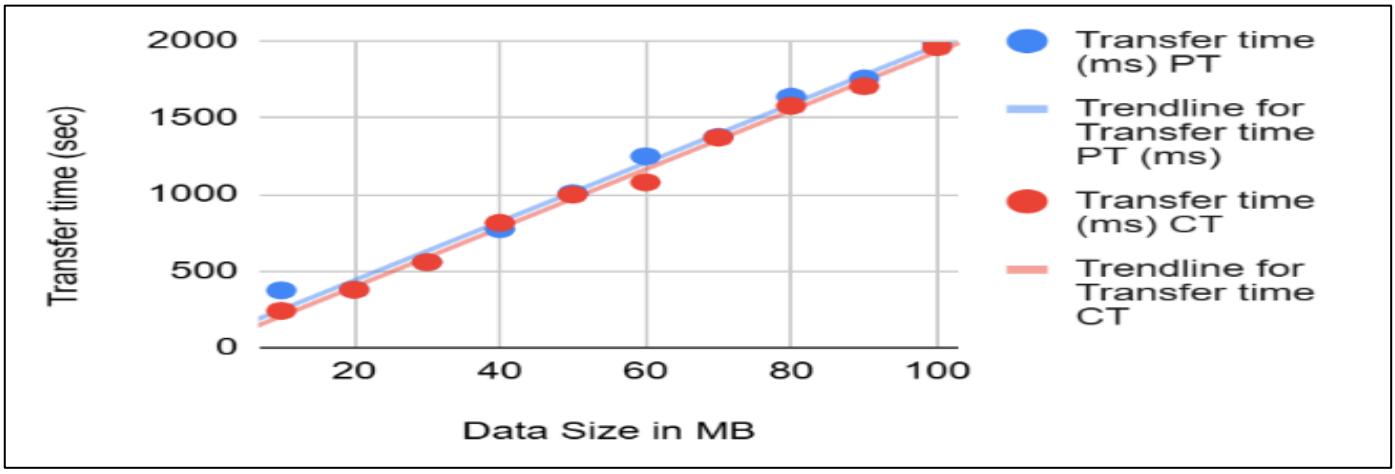

Fig 3a Transfer Time for Plain and Cipher Text for Data Size (10 - 100) MB.

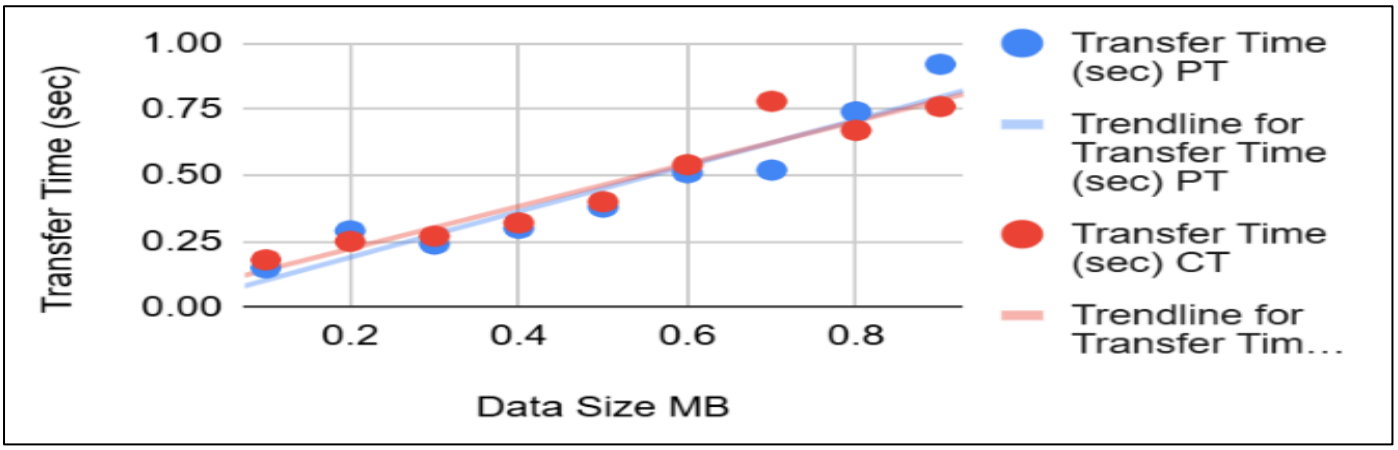

Fig 3b Transfer Time for Plain and Cipher Text for Data Size (0.1 – 0.9)MB.

The scatter plots show that transfer time has a strong positive correlation with data size for plain text and cipher text in both data categories. The relationship in the 10 – 100MB group is linear (figures 3a and b). In the 10 - 100MB group the Pearson coefficient of correlation (r) is 0.995 and 0.998 for both plain text and cipher text respectively. The probability (p) value is < 0.01 for each text.

In the 0.1-0.9MB group r is 0.95 and 0.96, for plain text and cipher text respectively. The p-value is < 0.01 for each. These indicate that there is a strong, positive, statistically highly significant correlation between data size and transfer time in both data categories.

In the 10-100MB group the mean transfer time is 1109.55 sec and 1067.98 sec for plain text and cipher text respectively. The t-value is 0.16 with a p-value of 0.44. In the 0.1-0.9MB group the mean transfer time is 0.45 sec and 0.46 sec respectively for plain text and cipher text. The t-value is 0.12 with a p-value of 0.45. The differences in mean transfer time are statistically insignificant.

- *Latency*

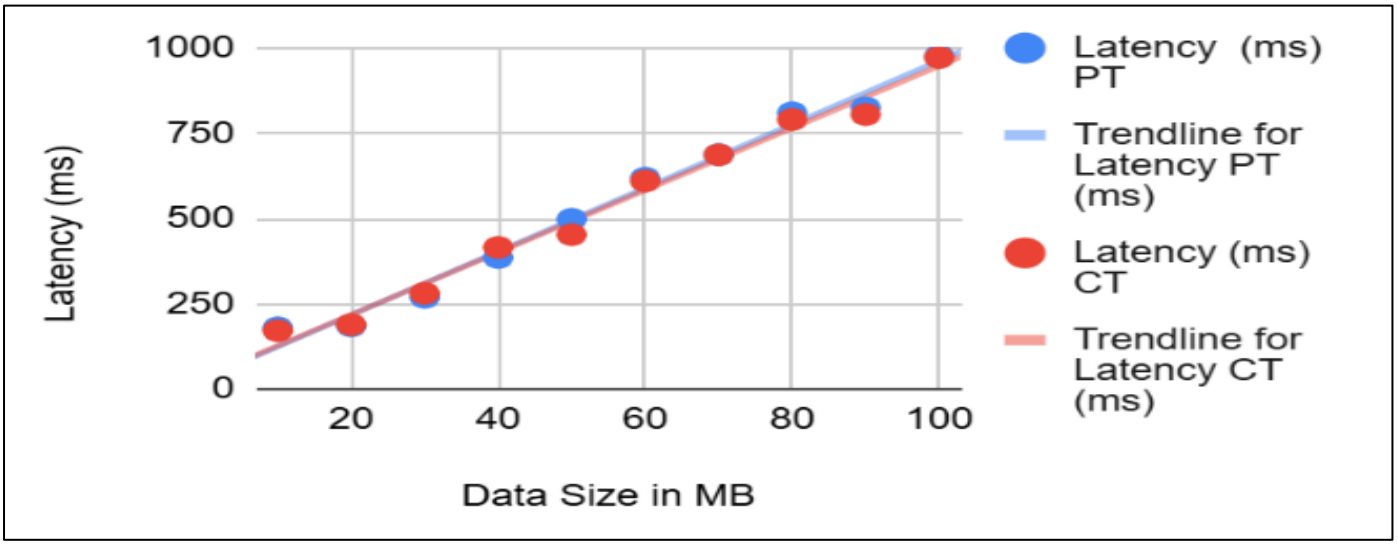

Fig 4a Latency for Plain and Cipher Text or Data Size (10 - 100) MB.

Fig 4b Latency for Plain and Cipher Text for Data Size (0.1 – 0.9) MB.

The scatter plot for the 10-100MB data group shows that latency has an essentially linear relationship with data size for plain text and cipher text (figures 4a). The r value is 0.99 for both plain text and cipher text. While the p - value for each is < 0.01.

In the 0.1-0.9MB group the latency against data size is non- monotonic for both text. Spearman's correlation (r_s) of 0.5 and -0.23 with p value of 0.17 and 0.55 for plain text and cipher text respectively indicates lack of statistically significant association between the two variables.

In the 10 – 100MB category the mean latency is 543.79 ms and 537.64 ms for plain text and cipher text respectively. The t-value is 0.049 and p-value 0.48. In the 0.1-0.9MB group, the mean latency is 51.81 ms and 50.44 ms for plain text and cipher text respectively. The t-value is 1.19, while the p-value is 0.13. The p-values of > 0.05 indicates that the differences in the mean latency in both data categories are statistically insignificant.

- *Throughput.*

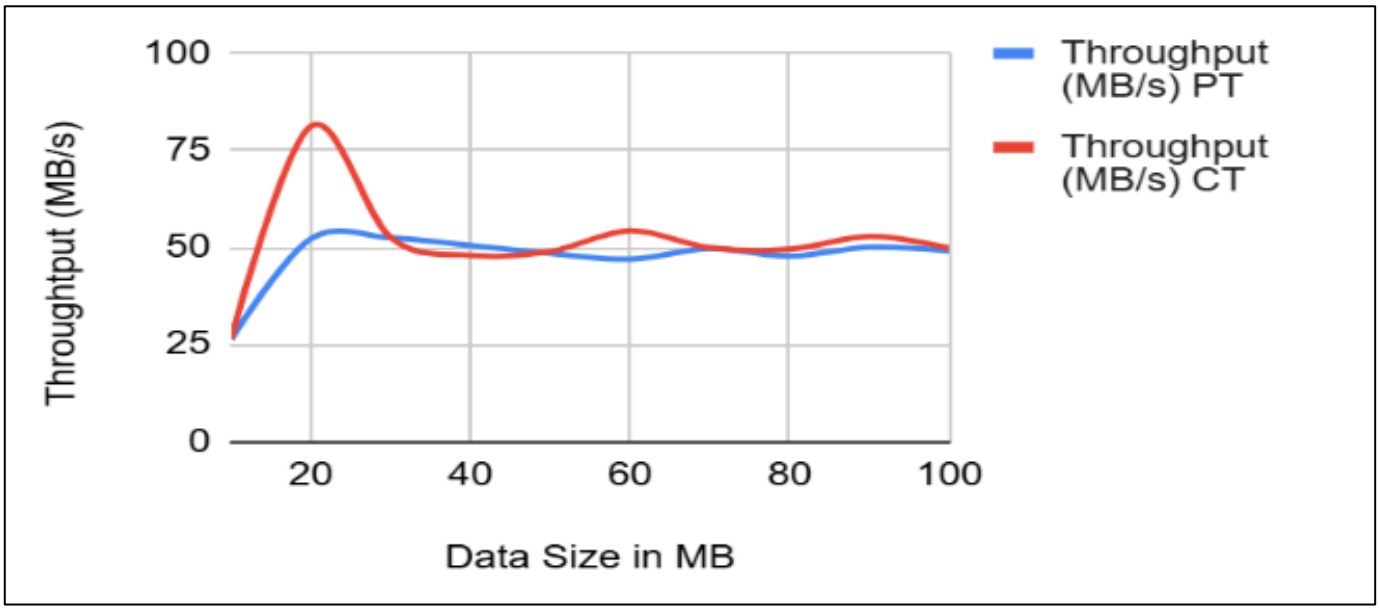

Fig 5a Throughput for Plain and Cipher Text for Data Size (10 – 90) MB.

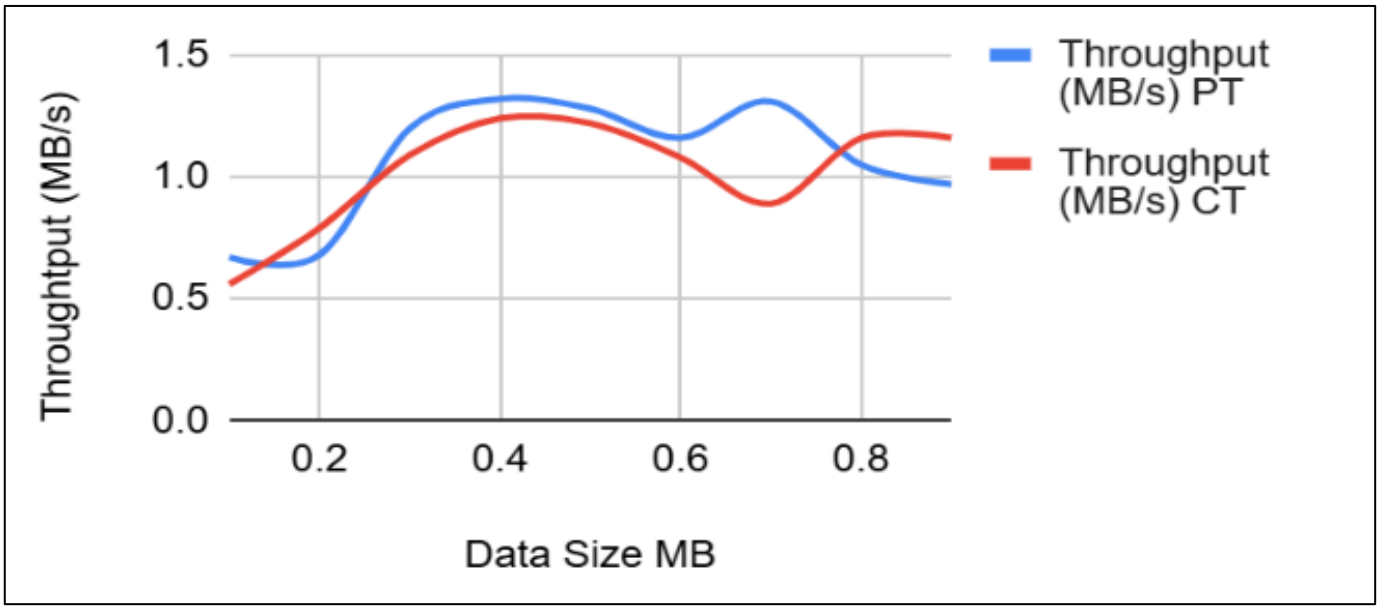

Fig 5b Throughput for Plain and Cipher Text for Data Size (0.1 – 0.9)M

The graphs of throughput against data size are non-monotonic but differ in line patterns. In the 10-100MB data range, the graph line of plaintext throughput against data size shows a peak at 30 MB, followed by a gradual decline till 60 MB after which it maintains minor inconsistent rise. The graph line of ciphertext throughput against data size peaks at 20 MB and rapidly declines till 30 MB, with a gradual decline at 40MB after which it shows occasional minor inconsistent rises (figure 5a). In the 0.1-0.9MB range the graph lines have an undulating pattern (figure 5b).

Spearman's correlation (r_s) is -0.13 and 0.15 (p= 0.68 and 0.73) respectively for plain text and cipher text in the 10-100MB range while In the 0.1-0.9MB range r_s is 0.23 and 0.44 with p of 0.55 and 0.23 for plain text and cipher text respectively. These indicate that there is no statistically significant association between data size and throughput in both categories.

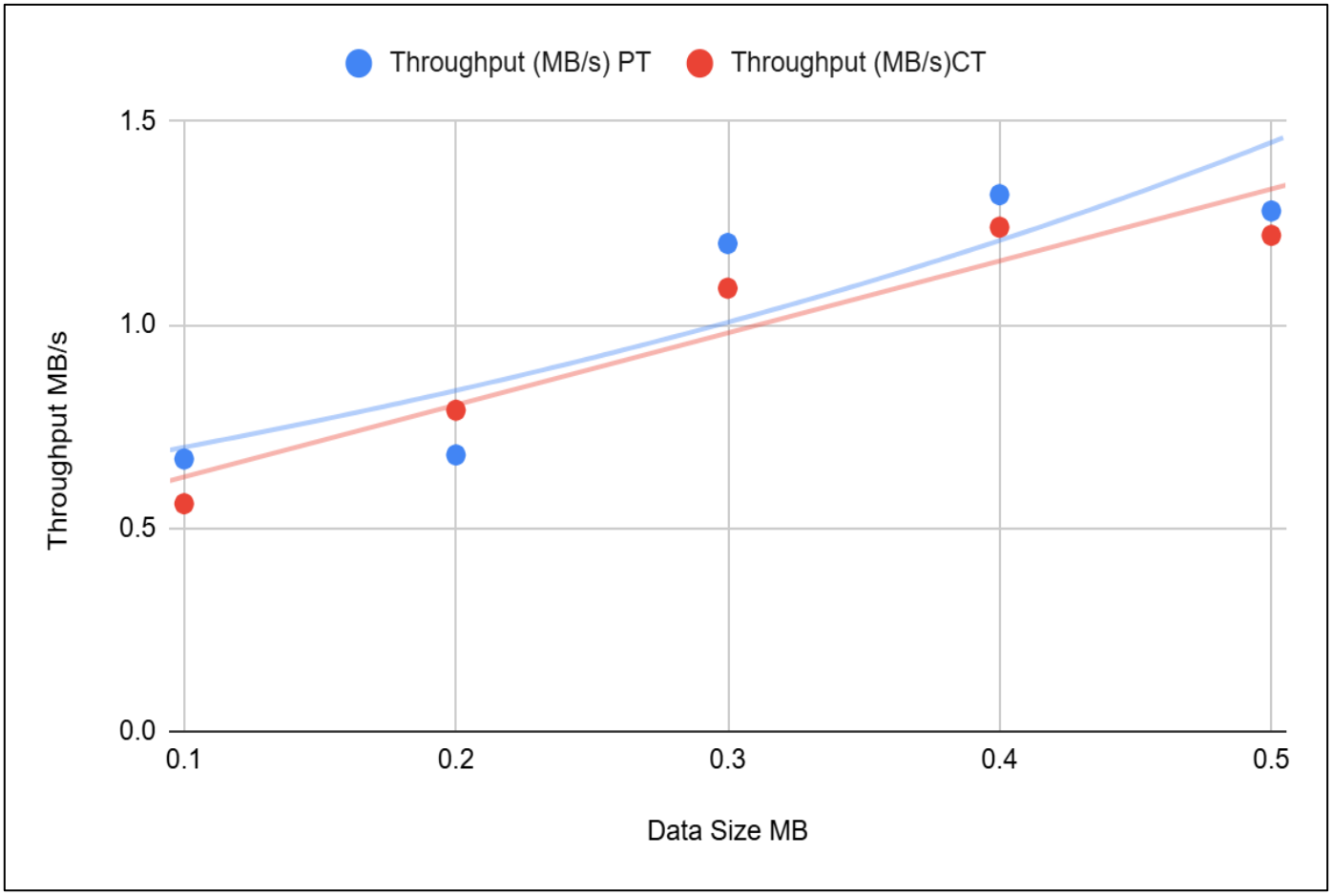

Fig 5c Throughput for Plain and Cipher Text for Data Size (0.1 – 0.5) MB.

However, scatter plot highlights a strong linear correlation between throughput and data size in the 0.1-0.5MB range (figure 5c). R for plain text is 0.9 with p=0.04. For ciphertext r is 0.95 and p is 0.02. This indicates a strong positive correlation between the two variables within this data range.

In 10-100MB data range the mean throughput is 47.36 Mb/sec and 51.35 Mb/sec for plain text and cipher text respectively with a t-value of 0.83 and p-value of 0.21. In 0.1-0.9MB range the mean throughput for plaintext is 1.07mb/s and for cipher text 1.02mb/s. The t-value of 0.44 and p-value is 0.33. These indicate that there is no statistically significant difference in the mean throughput of both text in the two data categories.

➢ *Relationship between Transfer Time and either Latency or Throughput*

- *Transfer time and latency*

Correlation analysis yielded r values of 0.99 and 0.9 respectively for plain text and ciphertext in the 10-100MB category. The p value is less than 0.01. These indicate that there is strong positive statically highly significant correlation between data size and transfer time in the 10-100MB. In the 0.1-0.9MB data range (r_s) is 0.47 and -0.32 with p values of 0.47 and 0.4 respectively for plain text and cipher text. These indicates there is no statically significant association between transfer time and latency in this group.

- *Transfer time and throughput.*

In the 10-100MB category, (r_s) is -0.22 and 0.15 with p-values of 0.53 and 0.68 respectively for plain text and cipher text. In the 0.1-0.9MB category, (r_s) is 0.17 and 0.33 with p-values of 0.53 and 0.68 respectively for plaintext and ciphertext. These indicate that there is no statically significant association between transfer time and throughput in both data categories.

IV. DISCUSSION

The statically insignificant differences in the mean values of transfer time, latency, and throughput in both data categories indicate that both cipher text and plain text have similar impact on network performance. Consequently, the users of AES-256 encryption can enjoy its robust protection without bothering about a significant trade-off with network performance.

The results further indicate that data size affects both transfer time and latency in the 10-100MB range. Presumably data size indirectly affects latency through its effect on transfer time. Therefore, it is proposed that the effect of encryption algorithms on latency is dependent on their effect on data size. Expectedly only algorithms which significantly increase the plain text data size will markedly degrade network performance.

Consistent with previous report (20), AES-256, a symmetric algorithms, caused extremely negligible (< 0.05%) increase in plain text data size. This is considered a major contributory factor to the insignificant difference in the impacts of AES-256 encrypted data and that of unsecured data on network performance.

Transfer time has a direct relationship with data size in both categories of data size. This lends credence to results of Abolade whose data ranged from 0.25 to 2 Kb (21). Interestingly critical analysis of his results shows an insignificant difference in the transfer time of unsecured and encrypted data in line with the findings of this study.

Despite the strong correlation between transfer time and data size in the 0.1-0.9MB data range there is no significant association between latency and data size or transfer time in this category. This may be attributed to the very short transfer time (<1 second). Expectedly, very short transfer time will cause minimal latency. In this study, the difference between two consecutive latency values varies from 1 to 6ms with a median of 2.5ms for plaintext and from 0 to 5ms with a median of 2.13ms for ciphertext. If the latency values are expressed in seconds, they will be constant at 0.05 second. This suggests that the latency observed in this group falls within the range of minimum latency for the experimental network environment.

Considering the findings in both data categories, it may be deduced that there is a critical threshold of data size necessary to cause a remarkable increase in latency. Predictably, this lies between 1 and 10MB.

Bianchi (22) has defined throughput saturated value as "the limit reached by the system throughput as the offered load increases and it represents the maximum load that the system can carry in stable conditions" .In this study, this value probably starts at 60 MB and 30 MB for plaintext and ciphertext respectively.

Inexplicably, throughput has a strong positive correlation with data size in the range of 0.1 to 0.5 MB. This suggests that an initial positive correlation between throughput and data size disappears as data size increases.

V. CONCLUSION

The study has shown that AES-256 encryption, adjudged to be the strongest algorithm available in the market, has no significant adverse effect on network performance. Consequently, its users will enjoy the benefit of its strong protection without the inconvenience of significant degradation of network performance.

Furthermore, it has extremely negligible effect on data size. Its purported increase in latency and transfer time is related to effect of data size rather than the effect of encryption per se. There is a transient positive correlation between throughput and data size in the very low data range.

ACKNOWLEDGEMENT

This paper is an extract from my MSc thesis submitted to Glasgow Caledonian University (GCU). I would like to thank my academic supervisors and the faculty of the School of Computing, Engineering, and Built Environment at GCU for their guidance and support throughout the research. I also acknowledge the use of the EVE-NG simulator and other open-source tools, which were instrumental in conducting this research.

➢ *Contribution Statement and Patent Information*

As the sole author, responsible for all aspects of the research, including conceptualization, methodology design, data analysis, and manuscript preparation. No patents are associated with the findings or methodology presented in this paper.

➢ *Funding*

No financial support was received for the conduct of this research or the preparation of this manuscript.

- *Author Contribution Statement*

This research was independently conducted by who carried out the entire process from initial concept and experiment design to data collection, analysis, and writing of the manuscript.

- *Declaration of Interest*

The author declares no conflict of interest related to this research.

REFERENCES

[1]. Keck, M., Gillani, S., Dermish, A., Grossman, J., & Ruhmann, F. (2022). The role of cybersecurity and data security in the digital economy. Retrieved from https://policyaccelerator.uncdf.org/policy-tools/brief-cybersecurity-digital-economy.

[2]. Statista. (2023). Cybercrime: Number of compromises and impacted individuals in US 2005-2022. Retrieved from https://www.statista.com.

[3]. IBM. (2022). Cost of a Data Breach. Retrieved from https://www.ibm.com.

[4]. Stefánsson, S. (2017). Private, but not secure: HTTPS is hiding cybercrime. *Security Week*. Retrieved from https://www.securityweek.com.

[5]. Wagner, L. (2021, September 8). What is Cryptography? A complete overview. *Boot.dev*. Retrieved from https://blog.boot.dev/cryptography/what-is-cryptography.

[6]. IBM. (2022). Cost of a Data Breach. Retrieved from https://www.ibm.com.

[7]. Semwal, P., & Sharma, M. K. (2017). Comparative study of different cryptographic algorithms for data security in cloud computing. *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)*, 1-7. https://doi.org/10.1109/ICACCAF.2017.8344738.

[8]. Abood, O. G., & Guirguis, S. K. (2018). A survey on cryptography algorithms. *International Journal*

of Scientific and Research Publications, 8(7). https://doi.org/10.29322/ijsrp.8.7.2018.p7978.

[9]. Hamouda, B. E. H. H. (2020). Comparative study of different cryptographic algorithms. *Journal of Information Security, 11*(3), 138–148. https://doi.org/10.4236/jis.2020.113009.

[10]. Saini, H. (n.d.). 8 strongest data encryption algorithms in cryptography. *Analytics Steps*. Retrieved from https://www.analyticssteps.com/blogs/8-strongest-data-encryption-algorithms-cryptography.

[11]. Hammad, B. T., Sagheer, A. M., Ahmed, I., & Jamil, N. (2020). A comparative review on symmetric and asymmetric DNA-based cryptography. *Bulletin of Electrical Engineering and Informatics, 9*(6), 2484–2491. https://doi.org/10.11591/eei.v9i6.2470.

[12]. Boulmalf, M., Barka, E., & Lakas, A. (2007). Analysis of the effect of security on data and voice traffic in WLAN. *Computers and Communications, 30*(11), 2468–2477. https://doi.org/10.1016/j.comcom.2007.04.024.

[13]. Turab, N., & Moldoveanu, F. (2008). The impact of various security mechanisms on the WLAN performance. *Series C, 70*(4), 21–36.

[14]. Kolahi, S. S., Li, P., Argawe, M., & Safdari, M. (2012). WPA2 security-bandwidth trade-off in 802.11n peer-peer WLAN for IPv4 and IPv6 using Windows XP and Windows 7 operating systems. *IEEE Symposium on Computers and Communications (ISCC)*. https://doi.org/10.1109/ISCC.2012.6249358.

[15]. Siwamogsatham, S., Hiranpruek, K., Luangingkasut, C., & Srilasak, S. (2008). Revisiting the impact of encryption on performance of IEEE 802.11 WLAN. *IEEE Xplore*. https://doi.org/10.1109/ECTICON.2008.4600451.

[16]. Lepaja, S., Maraj, A., Efendiu, I., & Berzati, S. (2018). The impact of the security mechanisms in the throughput of the WLAN networks. *7th Mediterranean Conference on Embedded Computing (MECO)*, 1–5. https://doi.org/10.1109/MECO.2018.8406067.

[17]. Forenbacher, I., Husnjak, S., Jovović, I., & Bobić, M. (2021). Throughput of an IEEE 802.11 wireless network in the presence of wireless audio transmission: A laboratory analysis. *Sensors, 21*(8), 2620. https://doi.org/10.3390/s21082620.

[18]. Asare, S., Yaokumah, W., Gyebi, E. B. B., & Abdulai, J. (2022). Evaluating the impact of cryptographic algorithms on network performance. *International Journal of Cloud Applications and Computing, 12*(1), 1–15. https://doi.org/10.4018/ijcac.309937.

[19]. SocSciStatistics. (n.d.). Social science statistics. Retrieved from https://www.socscistatistics.com.

[20]. Elbayoumy, A., & Shepherd, S. (2005, March). A high grade secure VoIP system: The tiny encryption algorithm. In Proceedings of 7th Annual International Symposium on Advanced Radio Technologies (pp. [page range]). Boulder, Colorado.

[21]. Abolade, O., Okandeji, A., Oke, A., Osifeko, M., & Oyedeji, A. (2021). Overhead effects of data encryption on TCP throughput across IPSEC secured network. *Scientific African, 13*, e00855. https://doi.org/10.1016/j.sciaf.2021.e00855.

[22]. Bianchi, G. (1998). IEEE 802.11-saturation throughput analysis. *IEEE Communications Letters, 2*(12), 318–320. https://doi.org/10.1109/49.740860.