Dear Editor and Reviewers:

Thank you very much for the third time review of my manuscript titled "*A New Lightweight and Efficient FPGA based Architecture for AES Algorithm Targeting IoT Security*" and providing me valuable comments as well as helpful and encouraging feedback. The comments have greatly helped to improve the quality of the paper. Below, I present responses to address all the review comments. Accordingly, I have modified the manuscript based on the review comments that require actions.

Reviewer A:

Dear Author

The author has considered my comments and made some modifications in the manuscript and meet my expected requirements, without changing the main content of the paper.

For future work, my suggestion to the author is to perform "Post-Implementation Timing Simulation" with some other process corners and analyse the results (Vivado: Simulation Settings -> Netlist -> process corner). Moreover, I think the author is aware that the estimative for system maximum clock frequency, obtained after simulation by calculations with data in Vivado "routed design timing summary report", does not account for signal delay in the path at FPGA external interface.

I express my congratulations to the author for the achievements in the current work.

Response: I'm grateful for your insightful comments, understanding and encouragement. I really appreciate your valuable considerations, the information and advice you have shared. Based on your comments, in my future work, I will perform Post-implementation Timing Simulation, to analyze the implementation results that include routing delays.

Reviewer B:

The problem associated with the frequency of the implementation remains. The frequencies are too high for a valid circuit in the FPGA. -The architecture of the full circuit under test should have been included. -How is data sent to the FPGA? Is the source code available?

Response: Thank you very much for your useful comments that helped me to reconsider my work and improve it. Regarding your comments, the reported results in this paper are post-synthesis timing analysis results and not post place-and-rout (PAR) simulation outcomes. I used the achieved clock periods to compute the frequencies. With the post synthesis timing simulation, the design is not fully routed; then, only some statistical information regarding the routing delay might be used (may be including cell-delays). In this case, I assume that the post synthesis simulation might result in shorter delays specifically for this simplified AES specification that involves only the encryption part, rather than the post place-and-rout (PAR) simulation, which also consider full routing delays in addition to cell-delays.

Regarding the architecture of the synthesized circuit, I removed it based on a review comment.

Reviewer C:

Most of the comments that I pointed out in my previous review were satisfactorily addressed by the author. However, there are still two important issues that must be addressed by the author before the manuscript can be accepted for publication:

1 - The implementation results presented in section VI report to the synthesis procedure or to the full FPGA implementation, including the routing to I/O pins? This must be clarified in the paper, due to its implications on the maximum operating frequency of the design and, consequently, on its throughput.

2 - The maximum operating frequencies reported in tables II, III, and IV for the proposed architecture are somewhat higher than the maximum values announced by the FPGA manufacturer for each of the considered devices. This must be clarified, because it puts into question the presented results and conclusions.

Regarding the presentation and style of this revised manuscript, it has greatly improved. Nonetheless, there are still some clerical errors, grammar issues, and other minor issues regarding text formatting that must be further addressed (see PDF file in attach).

Response: Thank you very much for all of your insightful comments. I really appreciate the great effort you exerted to review and improve my manuscript. Your valuable review comments have again greatly helped to improve the quality of the manuscript. I have addressed all of your comments including the language issues and typo-errors and changed the manuscript accordingly.

Concerning the achieved frequencies and the related results, the reported results in this paper are post-synthesis timing analysis results and not post place-and-rout (PAR) simulation. I used the achieved clock periods to compute the frequencies. With the post synthesis timing simulation, the design is not fully routed; then, only some statistical information regarding the routing delay might be used (may be including cell-delays). In this case, I assume that the post synthesis simulation might result in shorter delays specifically for this simplified AES specification that involves only the encryption part, rather than the post place-and-rout (PAR) simulation, which also consider full routing delays in addition to cell-delays.

I have also reflected this in the manuscript in both the “*Result Comparisons and Analysis*” and “*Conclusions*” sections.

I meticulously tried to improve the quality of the manuscript based on the review comments, and made some modifications in the manuscript. The modifications will not change the main content and the paper’s framework. I appreciate for Editor’s/Reviewers’ commitments and warm work earnestly, and hope that the corrections will meet the expected requirements.

Thank you again!

Best regards,

sincerely,

Abiy Tadesse Abebe.