Reviewer 1

This paper presents the method to detect the Cyber-attack Detection Using Gradient Clipping Long Short-Term Memory Networks in Internet of Things:where the memory is very low. Here the new method is used compared to related works with higher accuracy. However, I would like the authors to add small changes as follows:

1. Please fix error red underline in fig.1. (DoS and FoG)
   Response: Thank you for pointing that out. I will correct the error with the red underline in Figure 1 (DoS and FoG) and update the document accordingly
2. Please discuss on the difference between DDOS TCP, UDP, HTTP? How it impacts on the intrusion.
3. **Response:** Thank you for your comment. I'll provide a detailed discussion on the differences between DDoS attacks targeting TCP, UDP, and HTTP protocols, as well as their respective impacts on intrusion

4. Please also discuss on the drawback of GC-LSTM compared to RNN and ANN?

   Response: Thank you for your suggestion. This comparison will help highlight the relative advantages and limitations of GC-LSTM in different contexts. I'll update the document accordingly

Reviewer 2

1. Excellent work on developing the GC-LSTM approach for cyber-attack detection in IoT networks. The performance improvements over existing methods are impressive and well-demonstrated.
   Response: Thank you so much for your kind words and positive feedback. I'm glad to hear that the GC-LSTM approach and its performance improvements were well-received.
2. The paper's relevance to current IoT security challenges is clear and well-articulated. Consider expanding on the potential real-world implications of your findings, particularly in critical sectors like healthcare or smart cities.
   Response: Thank you for your insightful feedback. I will include the potential real-world implications of the findings, particularly in critical sectors such as healthcare and smart cities (page-no5).
3. Your use of the Bot-IoT dataset for multi-class classification is a strength. You might consider elaborating on why this dataset was chosen and how it compares to other available datasets in the field.
   Response: Thank you for highlighting the strength of using the Bot-IoT dataset for multi-class classification. I will elaborate on why this particular dataset was chosen, including its unique features and advantages over other available datasets in the field.
4. The presentation of results is generally clear, but you could enhance the abstract by including some specific performance metrics to immediately highlight your achievements.

Response: Thank you for your valuable feedback. I will enhance the abstract by including specific performance metrics to better highlight the achievements of the study.

5. The technical explanation of the GC-LSTM model is good, but consider adding a brief explanation or diagram illustrating how gradient clipping specifically addresses the challenges in IoT security contexts. This could make your innovation more accessible to a broader audience.
   Response: Thank you for your suggestion. I will add a brief explanation or diagram illustrating how gradient clipping addresses specific challenges in IoT security contexts.
6. Your comparison with RNN and ANN methods is valuable. Consider discussing any limitations of your approach or scenarios where these other methods might still be preferable.
   Response: Thank you for your insightful feedback. I will include a discussion of any limitations of the GC-LSTM approach and explore scenarios where RNN and ANN methods might still be preferable.
7. The suggestion for future work in IoHT is intriguing. You might expand slightly on the specific challenges or modifications needed to apply your method in healthcare IoT contexts.
   Response: Thank you for your feedback. I will expand on the specific challenges and modifications needed to apply the GC-LSTM method in healthcare IoT contexts
8. While the overall presentation is clear, a final proofreading pass could help eliminate minor grammatical issues and further polish the writing.
   Response: Thank you for your suggestion. I will conduct a final proofreading pass to address any minor grammatical issues and further polish the writing. Your feedback is appreciated, and I'll ensure the presentation is as clear and refined as possible
9. Consider adding a brief discussion on the computational requirements of your method compared to existing approaches, as this could be relevant for practical implementation in resource-constrained IoT environments.
   Response: Thank you for your suggestion. I will add a brief discussion on the computational requirements of the GC-LSTM method compared to existing approaches
10. Your work provides a solid foundation for future research. You might suggest some specific next steps or open questions that could build upon your findings. Overall, this is a strong paper with significant contributions to the field of IoT security. These suggestions aim to further enhance its impact and clarity.
    Response: Thank you for your kind words and constructive feedback. I will suggest specific next steps and open questions that could build upon the findings of this work. This will help outline potential avenues for future research and enhance the paper's impact and clarity.