Revocation plays a crucial role in attribute-based encryption as it allows data owners to control and manage decryption privileges for data users based on their preferences. The authors' research on revocable attribute-based encryption is highly significant and relevant in the field of data security and access control on the cloud. The authors' approach of using a cloud server to perform revocation is commendable because of the convenience it brings to the data owner. However, it is worrisome that the server may compromise the integrity of the encrypted data during the revocation process in order to save its own computational resources, which may hinder practical applications. To address this challenge, the authors introduce an efficient RFAME-DI scheme that solves the data integrity problem while maintaining computational efficiency. They implement an revocable mechanism based on FAME that protects data integrity and enables data users to verify the revoked ciphertext generated by the cloud server. The authors provide a comprehensive and convincing security analysis of their scheme that ensures data confidentiality and integrity. In addition, performance evaluation demonstrates the efficiency benefits of their proposed scheme.

There are some suggestions:

1. In the $\rm{Encrypt}$ algorithm, the public parameter $PP$ is used when the data owner encrypts the message, so $PP$ should be added to the input of the $\rm{Encrypt}$ algorithm.
2. In the $\rm{Decrypt\_{or}}$ and $\rm{Decrypt\_{re}}$ algorithms, the conditions for the output message $m$ are not described accurately enough. According to the authors' scheme, it is not only necessary for the set of attributes to satisfy the access structure, but it is also necessary to pass the validation of the $csum$. The relevant description should be added.
3. The acronym CP-ABE should be used instead of the ciphertext-policy attribute-based encryption, in line 53 (left column) on page 2.
4. In line 58-59 (right column) on page 4, the symbol $a\_z$ is considered to be the symbol $\alpha\_z$. Similarly, in line 27 (right column) on page 5, $a\_t$ and $d\_t$ are considered to be $\alpha\_t$ and $\gamma\_t$ respectively.
5. In line 56-57 (right column) on page 5, the parameter $\widetilde{\mathbb{A}} =(\widetilde{M},\widetilde{\tau})$ in the delegate DG has already appeared earlier, and it is straightforward to write it as access structure $\widetilde{\mathbb{A}}$. Similarly on page 6, line 2 (left column).
6. In line 47 (left column) on page 6, “... the fourth part of the original cipheretext $CT\_{csum} ...$” , this expression may cause misunderstandings among readers, so it is better to modify it to “... the checksum in the original cipheretext $CT\_{csum} ...”.

Overall, the authors' work deserves recognition for its contribution to the field of attribute-based encryption. While there are some minor errors and symbolism issues in the article that need addressing, the authors' novel approach and experimental results make this research paper acceptable with the suggested revisions.