Review of: "Se-PKSE: Secure Public-Key Searchable Encryption for Cloud-Assisted Lightweight Platforms"

Li Shuai

Potential competing interests: The author(s) declared that no potential competing interests exist.

The authors proposed a dynamic ranked PKSE framework over encrypted cloud data named "Secure" Public-Key Searchable Encryption (Se-PKSE).

The paper deals with an interesting problem.

However, there are still lot of work to be done and the manuscript need to be revised carefully, including the organizations and writing.

Here are some comments for modifications:

In Page2/Second column/Paragraph "We propose...", the authors said "Document producers can encrypt using the public key (partial homomorphic encryption), upload, and then remove the documents".

However, in Page8/Second column/Paragraph "Documents produced...", the authors said "Documents produced by the document producers can be encrypted using any standard file encryption technique."

So, which encryption method is used to encrypt the document?

Is it "partial homomorphic encryption" or "standard file encryption technique".

If it is "partial homomorphic encryption", whether it can be realized on the lightweight platform?

If it is "standard file encryption technique", is it AES or another algorithm?

If it is symmetric encryption such as AES, how to solve the key management problem?

Thus, the authors should explain this problem in detail.

Compared with the existing scheme, the characteristic of the proposed scheme in this paper may be "dynamic ranked" rather than "Secure".

In fact, all the authors who study searchable encryption claim that their proposed scheme is "Secure".

I suggest the authors rename the proposed scheme.

In Abstract and elsewhere in the manuscript, "Amazon EC2" is used without explanation.

The authors should explain "Amazon EC2".

In Page4/Second column/Paragraph "The document policy...", the authors replaced trapdoors with key wordsearch procedure and ciphertexts with document policies.

The use of the term“document policie” is confusing.

The authors should elaborate.

In Page5/Second column/Paragraph "Setup..." , there is a redundant parenthesis.

In Page8/System Description, the authors should indicate who performs the algorithm "setup" and "keygen".

In Page8/Second column/Equation (6) and elsewhere in the manuscript" , the function "enc" is missing the key as input.

In Performance Evaluation, the authors took the lowest possible AWS instance t2.nano (Intel Xeon 3.3 GHz processor with 1 core and 0.5GiB ram) instance for document producer. Obviously, it has more powerful computing and storage capabilities than a real lightweight platform (like sensors, mobile devices, wearable devices, drones, and other smart devices).

The author should experiment with some real lightweight platforms.

In Performance Evaluation/Figure 10, the legend "Xia et al. [6] and Peng et al. [8]" should be "Xia et al. [9] and Peng et al. [11]".