Privacy and security of data on the cloud have been a hot research topic. Attribute-based encryption (ABE) is widely adopted in cloud scenarios. However, most ABE schemes suffer from key escrow problem as the private key is provided by a third party entity - key generation center (KGC), which may lead to security issues. It is also considered that if the private key is leaked it will severely compromise data confidentiality. The authors propose a forward-secure decentralized attribute-based encryption scheme using puncture encryption to protect data privacy and the generation of the private key does not depend on the KGC. Security proofs demonstrate the confidentiality of their scheme. They show the performance of six algorithms: Setup, KeyGen, Extract, Puncture, Encrypt, and Decrypt. Experiments show that their scheme is effective but the article has a number of problems. More detailed comments are given as follows.

-On page 2, Fig 1. The text above the arrows between the entities generally represents what is being sent. The “encrypt” and “decrypt” marked by the author look like they should be algorithms running on some entity, rather than ciphertexts, private keys, or something that can be sent.

-On page 2, section I.B. The authors mention a lot of work related to punctured encryption which is used to implement forward security. The authors could introduce some other related techniques for implementing forward security.

-On page 3, Table I. The table looks very confusing and not clear enough. The authors could write the relevant properties directly into the table instead of labeling them in small print below.

-On page3. Fig.2 has a similar problem as Fig.1. The authors need to make a clear distinction between the algorithm run by the entity and the file passed on the network to avoid misunderstanding by the reader. At the two circular arrows, it's a bit confusing whether the entity passes the puncture keys or performs the Puncture algorithm.

-On page 3. In attribute-based encryption, the data owner decides who can access the data by specifying the access structure in the ciphertext. It's strange that the author leaves it up to the data owner to generate and send private keys to the data users. It's true that the data owner has the privilege to specify who can access the data, but why would the author use attribute-based encryption if it's the data owner who can just send the decryption key to the specified person?