

The following question was asked on our Telegram channel:

"Is it possible to 'ask' the nodes to remove a certain dataset and then check if they performed the action?" - Stathis

Here is Guy's response:

"Like everything in security (and generally in life), it depends on the assumptions you make. (a) For TEEs - if you trust that they cannot be tampered with, then it is possible. The enclave can prove this. (b) For MPC, if you assume that at most T nodes are bad ($T \geq 1$), then the answer is also yes. You simply ask the nodes to destroy their shares - if enough nodes do this then the data is effectively deleted.

Note that because T could be defined as low as $T=1$, then it's enough for only the original owner of the data so be honest here. However, there is a tradeoff with redundancy.

In any case, deletion is not an attributable action. Nodes can't prove to you that they deleted the data, so making these assumptions is the best you can do."