CONCLUSION

The concept of verifiable database is a great tool for verifiable EHR storage. However, proof reuse and the technique of proof updating by the server to improve system efficiency fails to achieve data integrity checking. In this work, we propose a novel updatable VDB scheme based on the functional c ommitment that supports privacy-preserving integrity auditing and group member operations, including join and revocation. Two security requirements of EHR are implemented: the server response correctness and the data storage integrity. Our VDB scheme achieves the desired security goals without incurring too much Computational increase. And our VDB scheme provides the minimum communication cost for the terminal with limited performance. To design a functional commitment scheme that applies to our program, two algorithms are added to make the FC scheme updatable. A practical improved concrete VDB scheme under computational l −BDHE assumption is presented. In addition, batch auditing for our VDB scheme supports multi-cloud server, multi-user and multi-storage vector scenarios. It makes the auditing process more efficient. Furthermore, we prove that our functional commitment scheme with updates and our VDB scheme can achieve the desired security properties. The performance of our scheme is more efficient compared with other different algorithms.