**CONCLUSION**

The intent of this survey is to study the various techniques based on the authentication structures used for data integrity verification in the cloud and fog environment and to analyze their pitfalls. This paper gives the classification of various integrity verification schemes. The classifications are root signature-based, BF-based, tag regeneration-based and tablebased schemes. This survey concludes that root signature based schemes are suitable for integrity verification in a single copy of dynamic data, BF-based schemes are suitable for a single copy of static data, tag regeneration-based schemes are suitable for IoT data and table-based schemes are suitable for multiple copies of dynamic data. Existing cloud data integrity verification methods are not suitable for fog environment because of its cryptographic nature. So there is a need for a lightweight scheme to verify the data integrity in the fog environment. In the future, a lightweight protocol based on erasure coding techniques will be proposed for integrity verification and corrupted data retrieval in the fog environment.