Code and data stored remotely on a cloud can be manipulated and tampered by untrustable entities or attackers. One way to verify data integrity is to use authenticated data structures (ADS). With ADS a client can make sure that his data is secure, intact and up to date by querying in the form of a challenge and evaluating the received response. Current approaches rely on the transmission of metadata to the clients for integrity check. In a cloud-based service this would mean updating the numerous clients accessing the same data structure with the same metadata. One solution to this problem is to verify the integrity of the data locally on the cloud. This can be achieved only if we have a trusted entity on the cloud. In this regard, the Trusted Execution Environment (TEE) provided by the Intel CPUs are very useful. Intel provides Software Guard eXtensions (SGX) which runs parts of an application in a secure environment (called Enclave). In this thesis, we develop an application prototype which uses Intel SGX features. The application demonstrates (a) Attestation of the system (b) Integrity protection of code and data (c) Confidentiality protection of the data. This thesis also measures the performance penalty incurred by running the application inside Intel SGX enclaves.