A Searchable Secure Encrypted Block Storage Service

Este Projeto tem como objetivo o design e implementação de um Serviço de Armazenamento de Blocos Encriptados de forma a conseguir procurá-los. O projeto teve como base a arquitetura TCP/IP, onde o cliente é responsável por toda a parte da encriptação e desencriptação, onde o servidor não tem conhecimento dos dados que armazena.

Foram implementados três algoritmos, **AES-256/GCM**, **AES-256/CBC** com **HMAC-SHA256** e **ChaCha20-Poly1305.** Para derivar chaves seguras para a KeyStore, foram utilizadas as passwords dos utilizadores, com o PBKDF2 com HMAC-SHA256 onde foram feitas 100000 iterações o que garante a resistência a *Brute Force Attacks*. Estas chaves são guardadas numa *Keystore* (JCEKS), e são associadas ao nome do ficheiro.

A Integridade e autenticidade são asseguradas por HMACs, gerados por cada bloco, onde existe uma verificação durante a desencriptação. Se esta verificação falhar, o cliente não realiza a transferência do ficheiro. Para assegurar a integridade, no caso do AES-256/CBC, foi feito inicialmente a encriptação para confidencialidade e posteriormente o HMAC para integridade.

A pesquisa por ficheiros é realizada através da encriptação das *keywords* a pesquisar, que são posteriormente enviadas para o servidor. O servidor retorna o valor pretendido utilizando a *trapdoor* enviada pelo cliente.

Relativamente ao testes, nem todos os métodos da nossa classe de testes CLTest funcionam, portanto recomendamos a realização dos testes através do lado do cliente fornecido visto que, por essa classe todos os mecanismos funcionam.

Ainda assim, enviamos a classe de teste de forma a comprovar que grande parte destes métodos funcionam.