User Credential Storage ADR

CONTEXT:

User Credential Storage is seen as an important step in security. Hashing is a one-way function which ensures credential safety if the database is compromised.

PROBLEM:

Not storing User Credential in plaintext.

SOLUTION:

Crypto is a Node module which allows for hashing and ciphers.

When a User registered, a salt(random string) is generated. The salt is then used in a cipher function to encrypt the password. SHA512 is the current security standard for hashing passwords. The Users passwords are encrypted with a SHA512 function and the salt and hash are both stored in the Users profile.

When a user tries to Log In, the salt of the user will be retrieved from the database and the input is put in the SHA512 hashing function. The output of the function is compared to the hash stored in the database.