US 20240214225A1

(19) United States

(12) Patent Application Publication

Lindskog et al.

(10) Pub. No.: US 2024/0214225 A1

(43) Pub. Date: Jun. 27, 2024

(54) **STORAGE DEVICE UTILIZING PHYSICALLY UNCLONABLE FUNCTION (PUF) BASED SECRET SHARING SCHEME FOR DATA ENCRYPTION/DECRYPTION**

(71) Applicant: **TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)**, Stockholm (SE)

(72) Inventors: **Niklas Lindskog**, Lund (SE); **Håkan Englund**, Lund (SE)

(21) Appl. No.: **18/567,722**

(22) PCT Filed: **Jun. 7, 2021**

(86) PCT No.: **PCT/IB2021/054991**

§ 371 (c)(1),
(2) Date: **Dec. 6, 2023**

Publication Classification

(51) **Int. Cl.**

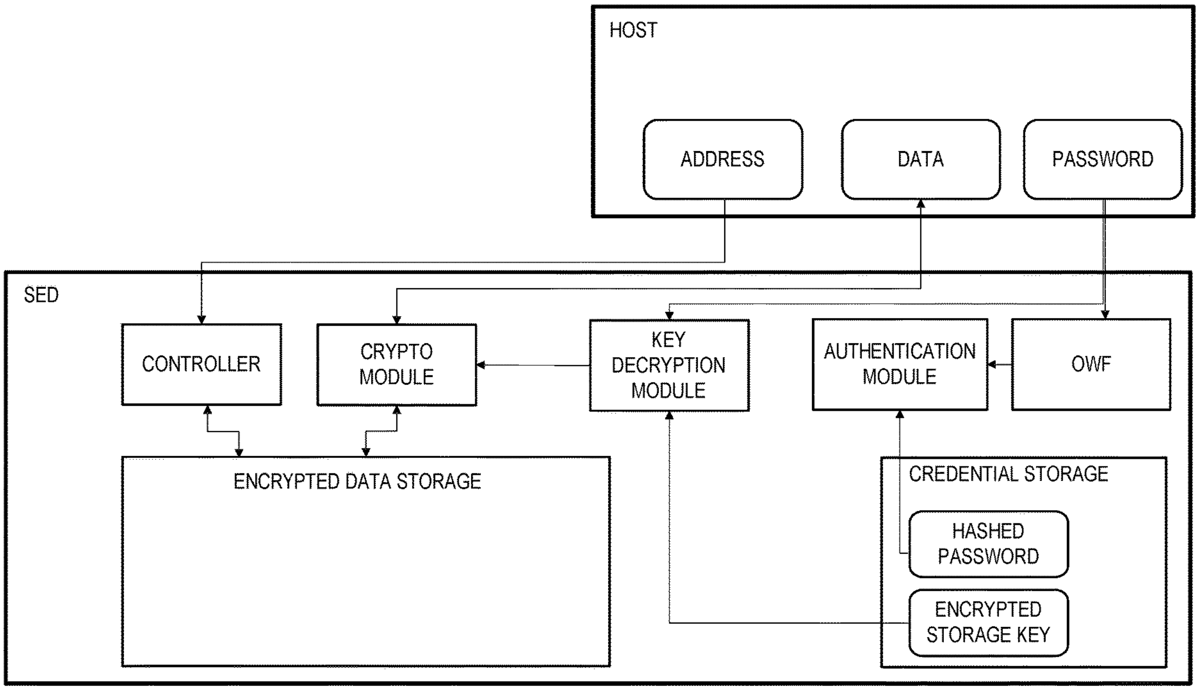
H04L 9/32	(2006.01)
G06F 21/78	(2006.01)
H04L 9/08	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 9/3278*** (2013.01); ***G06F 21/78*** (2013.01); ***H04L 9/085*** (2013.01)

(57) **ABSTRACT**

Systems and methods are disclosed herein for protecting data in a storage device by encrypting or decrypting the data with a Data Encryption Key (DEK). The storage device is communicatively coupled to a host and is locked with the host by secret sharing. In one example, the storage device comprises a Physically Unclonable Function (PUF) configured to, during a key generation phase of operation, generate a set of DEK responses based on a set of DEK challenges (chalDEK) and an assembler configured to obtain a set of SED DEK secret shares (SS_{SED}) based on the first set of DEK responses, receive additional data, and assemble at least the set of SED DEK secret shares (SS_{SED}) and the additional data to create a DEK master secret. The storage device also comprises a crypto module configured to receive a DEK based on the master secret and perform encryption and/or decryption of data using the DEK.


HOST
ADDRESS
DATA
PASSWORD
SED
CONTROLLER
CRYPTO MODULE
KEY DECRYPTION MODULE
AUTHENTICATION MODULE
OWF
ENCRYPTED DATA STORAGE
CREDENTIAL STORAGE
HASHED PASSWORD
ENCRYPTED STORAGE KEY