US 20240214361A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2024/0214361 A1

Ollikainen et al. (43) Pub. Date: Jun. 27, 2024

(54) **DISTRIBUTED DATA CONTENT PROTECTION**

(71) Applicant: **Rovi Guides, Inc.**, San Jose, CA (US)

(72) Inventors: **Ville Ollikainen**, Vihti (FI); **Markku Kylanpaa**, Helsinki (FI); **Anni Karinsalo**, Oulu (FI); **Pekka Koskela**, Oulu (FI)

(21) Appl. No.: **18/088,295**

(22) Filed: **Dec. 23, 2022**

Publication Classification

(51) **Int. Cl.**
H04L 9/40 (2006.01)
H04L 67/1097 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/0435*** (2013.01); ***H04L 67/1097*** (2013.01)

(57) **ABSTRACT**

Systems and methods are described for encrypting and decrypting data in a distributed storage environment. Such systems and methods for encryption may divide a data payload into slices, the slices including a first slice and a subsequent slice, employ a content encryption key and an initialization vector, encrypt the first slice using the content encryption key and the initialization vector, generate a subsequent initialization vector for the subsequent slice based upon the initialization vector and the unencrypted content of the first slice, and encrypt the subsequent slice using the subsequent initialization vector and the content encryption key. The systems and methods may then generate a list of the encrypted slices into which the data payload has been generated, and publish to a secure storage location, the slice list, the content encryption key and the initialization vector for the first slice in the slice list, with the slices outputted to the distributed storage environment. Systems and methods for decryption may receive, from a secure storage location, a slice list, a content encryption key, and an initialization vector, determine the encrypted slices to be received from the distributed storage environment. The systems and methods may receive, from the distributed storage environment, at least encrypted first slice and the encrypted subsequent slice, and decrypt the first slice using the content encryption key and the initialization vector, to generate a decrypted first slice, and generate a subsequent initialization vector for the subsequent slice based upon the initialization vector and the decrypted first slice, decrypt the subsequent slice using the subsequent initialization vector and the content encryption key, and combine the first slice and the subsequent slice into a data payload.