US008533493B1

(12) **United States Patent**
Tzeng et al.

(10) **Patent No.: US 8,533,493 B1**
(45) **Date of Patent: Sep. 10, 2013**

(54) **METHOD OF SECURING TRANSMISSION DATA**

(75) Inventors: **Jeng-Nan Tzeng**, New Taipei (TW); **I-Te Chen**, Kaohsiung (TW); **Jer-Min Tsai**, Kaohsiung (TW)

(73) Assignees: **National Chengchi University**, Taipei (TW); **Kaohsiung Medical University**, Kaohsiung (TW); **Kun Shan University**, Tainan (TW)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **13/422,159**

(22) Filed: **Mar. 16, 2012**

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
USPC **713/189**; 380/44

(58) **Field of Classification Search**
USPC 726/26, 29; 713/189, 193, 153; 380/278, 44, 45, 46
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,731,754 B1 * 5/2004 Ito 380/28

* cited by examiner

Primary Examiner — Edward Zee
(74) *Attorney, Agent, or Firm* — Davidson Berquist Jackson & Gowdey LLP

(57) **ABSTRACT**

A method is provided for securing transmission data between an upload device and a download device. The upload device is configured to generate a first matrix, a second matrix and a re-encryption vector, to encrypt a plaintext data file using the first matrix to obtain a ciphertext data file, to transmit the ciphertext data file and the re-encryption vector to a server, and to transmit the second matrix to the download device. The server is configured to re-encrypt the ciphertext data file using the re-encryption vector to obtain a re-encrypted data file that can be decrypted using the second matrix to obtain a decrypted data file, and to allow the download device to download the re-encrypted data file therefrom.

9 Claims, 4 Drawing Sheets