US 20240214222A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2024/0214222 A1

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

(54) **TLS-BASED AUTHENTICATION METHOD WITHOUT INTERVENTION OF CERTIFICATE AUTHORITY**

(71) Applicant: **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE**, Daejeon (KR)

(72) Inventor: **Daegeun YOON**, Daejeon (KR)

(73) Assignee: **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE**, Daejeon (KR)

(21) Appl. No.: **18/393,479**

(22) Filed: **Dec. 21, 2023**

(30) **Foreign Application Priority Data**

Dec. 21, 2022 (KR) 10-2022-0180265
Nov. 20, 2023 (KR) 10-2023-0161066

Publication Classification

(51) **Int. Cl.**
H04L 9/32 (2006.01)
H04L 9/30 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 9/3268*** (2013.01); ***H04L 9/3073*** (2013.01); ***H04L 9/3218*** (2013.01)

(57) **ABSTRACT**

A transport layer security (TLS)-based authentication method according to the present invention includes: receiving, in a web server, a certificate for TLS authentication issued from a certificate authority on a web server; transmitting a delegated request from the web server to a delegated entity; receiving, in the web server, a public key among a public key-private key pair generated by the delegated entity in response to the delegated request; generating, in the web server, delegated data based on the public key; generating, in the web server, delegated proof data of the same version as the delegated data; storing, in the web server, the delegated proof data in a delegated proof data storage; and transmitting the certificate and delegated data from the web server to the delegated entity.