(19) LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

(11) N° de publication : **LU102259**

(12) **BREVET D'INVENTION** **B1**

(21) N° de dépôt: LU102259

(51) Int. Cl.:
G06F 21/44, H04L 9/08

(22) Date de dépôt: 04/12/2020

(30) Priorité:

(43) Date de mise à disposition du public: 09/06/2021

(47) Date de délivrance: 09/06/2021

(73) Titulaire(s):
SHANDONG UNIVERSITY OF SCIENCE AND TECHNOLOGY – 266590 Qingdao, Shandong, (Chine)

(72) Inventeur(s):
Tsu-Yang WU – 266590 Qingdao, Shandong Province, (Chine), Tao Wang – 266590 Qingdao, Shandong Province, (Chine), Chien-Ming CHEN – 266590 Qingdao, Shandong Province, (Chine), Ming-Tai Wu – 266590 Qingdao, Shandong Province, (Chine), Weimin Zheng – 266590 Qingdao, Shandong Province, (Chine), Jeng-Shyang PAN – 266590 Qingdao, Shandong Province, (Chine)

(74) Mandataire(s):
MARKS & CLERK LLP – L-1017 LUXEMBOURG (Luxembourg)

(54) **MOBILE STORAGE-BASED AUTHENTICATION AND KEY AGREEMENT METHOD AND SYSTEM IN MEDICAL ENVIRONMENT.**

(57) The present disclosure provides communication authentication and key agreement method and system. The method includes: receiving a user name and a password entered by a user, and judging whether the user is an owner of the mobile storage device; calculating first transmission data transmitted to a server by a generation random number and a time stamp after determining that the user is the owner of the mobile storage device, and authenticating the mobile storage device by the server according to the first transmission data; receiving second transmission data from the server, and authenticating the server according to the second transmission data; and calculating a session key for communicating with the server after the server is authenticated.

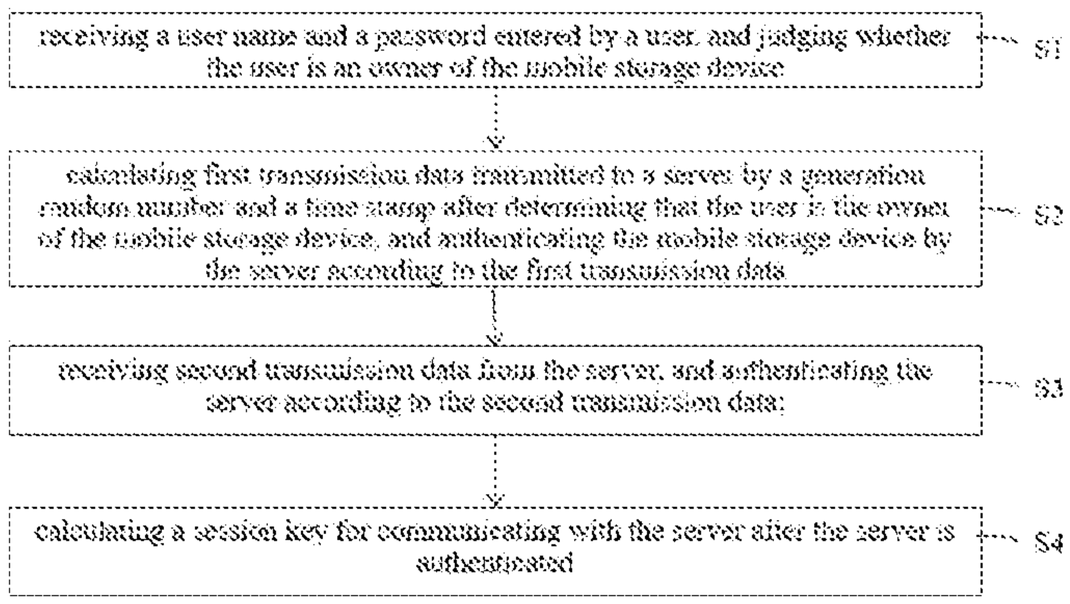

FIG. 1

MOBILE STORAGE-BASED AUTHENTICATION AND KEY AGREEMENT METHOD AND SYSTEM IN MEDICAL ENVIRONMENT

FIELD

[0001] The present disclosure relates the field of data security, and in particular to a mobile storage-based communication authentication and key agreement method and system in a medical environment.

BACKGROUND

[0002] Telecare Medicine Information System (TMIS) provides patients with flexible and convenient medical services. Patients at home submit their data to remote servers in a wired or wireless manner, and doctors in clinical center give corresponding clinical decisions or treatment plans after receiving the data.

[0003] It is necessary to verify and encrypt the data transmitted between patients and doctors as the data often contains user's privacy. Therefore, a large number of authentication and key exchange schemes are designed and applied to the service systems.

[0004] However, insecure factors, such as offline password guessing attacks, user impersonation attacks, man-in-the-middle attacks, and the like, exist in the existing authentication and key exchange schemes. Therefore, how to improve the security of data transmission between two parties in the authentication and key exchange scheme has always

SUMMARY

[0005] The present disclosure aims to provide highly secure and efficient communication authentication and key agreement method and system.

[0006] In one aspect, the present disclosure provides a communication authentication and key agreement method, which is applied to a mobile storage device. The method includes:

[0007] receiving a user name and a password entered by a user, and judging whether the user is an owner of the mobile storage device;

[0008] calculating first transmission data transmitted to a server by a generation random number and a time stamp after determining that the user is the owner of the mobile storage device, and authenticating the mobile storage device by the server according to the first transmission data;

[0009] receiving second transmission data from the server, and authenticating the server according to the second transmission data; and

[0010] calculating a session key for communicating with the server after the server is authenticated.

[0011] In some embodiments, before the operation "receiving a user name and a password entered by a user", the method further includes:

[0012] calculating $HPW_i = h(PW_i \parallel b)$ by the user name ID_i and the password PW_i selected by the user and the generation random number b, transmitting $\{ID_i, HPW_i\}$ as registration

information to the server, calculating by the server $A_i = h(ID_i \parallel k_s)$, $B_i = h(h(ID_i$LU102259 $HPW_i) \, mod \, m)$ and $C_i = A_i \oplus HPW_i \oplus B_i$ through one generation random number $m(2^4 < m < 2^8)$ after receiving the registration information, and storing a parameter $\{B_i, C_i, m, K_s, E_s(\cdot), D_s(\cdot), h\,(\cdot)\}$ as storage data in the mobile storage device and returning the storage data to the user, $h(\cdot)$ is a hash function, $\parallel$ is a connection operation, k_s is a private key of the server, K_s is a public key of the server, $K_s = k_s \cdot P$, $E_s(\cdot)$ is an encryption function, $D_s(\cdot)$ is a decryption function, P is a base point on an elliptic curve, and $\oplus$ is an exclusive OR operation.

[0013] In some embodiments, the operation of "judging whether the user is an owner of the mobile storage device according to the user name and the password entered by the user" includes:

[0014] entering by the user the user name ID_i and password PW_i;

[0015] calculating $HPW_i = h(PW_i \parallel b)$ and $B_i^* = h(h(ID_i \parallel HPW_i) \, mod \, m)$, and comparing whether B_i^* is equal to B_i;

[0016] if yes, determining that the user is the owner of the mobile storage device; and

[0017] if no, terminating a session.

[0018] In some embodiments, the operation of "calculating first transmission data transmitted to a server by a generation random number and a time stamp" includes:

[0019] generating the generation random number r_c and the time stamp T_1;

[0020] calculating $A_i = C_i \oplus HPW_i \oplus B_i$, $R_c = r_c A_i P$, $k1 = r_c A_i K_s$, and $H_i = E_{k1}(realm \parallel ID_i \parallel A_i \parallel T_1)$; and

[0021] transmitting $\{H_i, R_c\}$ as the first transmission data to the server;

[0022] wherein, the operation of "authenticating the mobile storage device by the server according to the first transmission data" includes:

[0023] after the server receiving the first transmission data $\{H_i, R_c\}$, calculating $k2 = k_s R_c$, and decrypting H_i by a calculated result to acquire $realm \parallel ID_i \parallel A_i \parallel T_1$;

[0024] verifying by the server a legitimacy of the time stamp T_1;

[0025] if the time stamp T_1 is legal, calculating $A_i^* = h(ID_i \parallel k_s)$ and verifying $A_i^* ? = A_i$; if the two values are equal, passing by the server the authentication of the mobile storage device; otherwise, terminating the session; and

[0026] generating by the server the generation random number r_s and the time stamp T_2, calculating $R_s = r_s \cdot P$, $J_i = r_s R_c$, $SK = h(J_i \parallel T_1 \parallel T_2)$, and $L_i = E_{k2}(ID_i \parallel R_s \parallel J_i \parallel T_2 \parallel realm)$, and transmitting $\{L_i\}$ as the second transmission data to the mobile storage device.

[0027] In some embodiments, the operation of "authenticating the server according to the second transmission data" includes:

[0028] after receiving the second transmission data $\{L_i\}$, decrypting L_i through $r_c A_i K_s$ to acquire $ID_i \parallel R_s \parallel J_i \parallel T_2 \parallel realm$, and verifying whether the time stamp T_2 is legal;

[0029] if the time stamp T_2 is legal, calculating $J_i' = r_c A_i R_s$ and verifying $J_i' ? = J_i$; and

[0030] if the two values are equal, passing by the server the authentication of the mobile storage device.

[0031] In some embodiments, the operation of "calculating a session key for communicating with the server" includes:

[0032] calculating the session key for communicating with the server as $SK = h(J_i' \| T_1 \| 102259 \| T_2)$.

[0033] In another aspect, the present disclosure provides a communication authentication and key agreement system, which is applied to a mobile storage device. The system includes:

[0034] a judging module, configured for receiving a user name and a password entered by a user, and judging whether the user is an owner of the mobile storage device;

[0035] a transmitting module, configured for calculating first transmission data transmitted to a server by a generation random number and a time stamp after determining that the user is the owner of the mobile storage device, and authenticating the mobile storage device by the server according to the first transmission data;

[0036] a verifying module, configured for receiving second transmission data from the server, and authenticating the server according to the second transmission data; and

[0037] a calculating module, configured for calculating a session key for communicating with the server after the server is authenticated.

[0038] In some embodiments, the system further includes:

[0039] a registering module, configured for calculating $HPW_i = h(PW_i \| b)$ by the user name ID_i and the password PW_i selected by the user and the generation random number b, transmitting $\{ID_i, HPW_i\}$ as registration information to the server, calculating by the server $A_i = h(ID_i \| k_s)$, $B_i = h(h(ID_i \| HPW_i)\ mod\ m)$ and $C_i = A_i \oplus HPW_i \oplus B_i$ through one generation random number $m(2^4 < m < 2^8)$ after receiving the registration information, and storing a

parameter $\{B_i, C_i, m, K_s, E_s(\cdot), D_s(\cdot), h(\cdot)\}$ as storage data in the mobile storage device and returning the storage data to the user, $h(\cdot)$ is a hash function, $\|$ is a connection operation, k_s is a private key of the server, K_s is a public key of the server, $K_s = k_s \cdot P$, $E_s(\cdot)$ is an encryption function, $D_s(\cdot)$ is a decryption function, P is a base point on an elliptic curve, and $\oplus$ is an exclusive OR operation.

[0040] In some embodiments, the judging module is specifically configured for:

[0041] entering by the user the user name ID_i and password PW_i;

[0042] calculating $HPW_i = h(PW_i \| b)$ and $B_i^* = h(h(ID_i \| HPW_i) \, mod \, m)$, and comparing whether B_i^* is equal to B_i;

[0043] if yes, determining that the user is the owner of the mobile storage device; and

[0044] if no, terminating a session.

[0045] In some embodiments, the transmitting module is specifically configured for:

[0046] generating the generation random number r_c and the time stamp T_1;

[0047] calculating $A_i = C_i \oplus HPW_i \oplus B_i$, $R_c = r_c A_i P$, $k1 = r_c A_i K_s$, and $H_i = E_{k1}(realm \| ID_i \| A_i \| T_1)$; and

[0048] transmitting $\{H_i, R_c\}$ as the first transmission data to the server;

[0049] wherein, the operation of "authenticating the mobile storage device by the server according to the first transmission data" includes:

[0050] after the server receiving the first transmission data $\{H_i, R_c\}$, calculating $k2 = k_s R_c$, and decrypting H_i by a calculated result to acquire $realm \| ID_i \| A_i \| T_1$;

[0051] verifying by the server a legitimacy of the time stamp T_1;

[0052] if the time stamp T_1 is legal, calculating $A_i^* = h(ID_i \| k_s)$ and verifying $A_i^* ?= A_i$; if the two values are equal, passing by the server the authentication of the mobile storage device; otherwise, terminating the session; and

[0053] generating by the server the generation random number r_s and the time stamp T_2, calculating $R_s = r_s \cdot P$, $J_i = r_s R_c$, $SK = h(J_i \| T_1 \| T_2)$, and $L_i = E_{k2}(ID_i \| R_s \| J_i \| T_2 \| realm)$, and transmitting $\{L_i\}$ as the second transmission data to the mobile storage device,.

[0054] In some embodiments, the verifying module is specifically configured for:

[0055] after receiving the second transmission data $\{L_i\}$, decrypting L_i through $r_c A_i K_s$ to acquire $ID_i \| R_s \| J_i \| T_2 \| realm$, and verifying whether the time stamp T_2 is legal;

[0056] if the time stamp T_2 is legal, calculating $J_i' = r_c A_i R_s$ and verifying $J_i' ?= J_i$; and

[0057] if the two values are equal, passing by the server the authentication of the mobile storage device.

[0058] In some embodiments, the calculating module is specifically configured for:

[0059] calculating the session key for communicating with the server as $SK = h(J_i' \| T_1 \| T_2)$.

[0060] In the embodiments of the present disclosure, an elliptic curve cryptosystem is adopted in the process of realizing identity verification and key agreement. Under the same security level, the elliptic curve cryptosystem requires less storage and computing resources, and can be better adapted to resource-constrained devices. The embodiments of the present

disclosure provide user anonymity and untraceability, and can also better resist common network attacks, such as offline password guessing attacks, user impersonation attacks, man-in-the-middle attacks, and the like.

BRIEF DESCRIPTION OF THE DRAWINGS

[0061] In order to more clearly illustrate the embodiments of the present disclosure or the technical solutions in the related art, the drawings to be used in the embodiments or description of the related art will be briefly described below. Obviously, the drawings in the following description are only certain embodiments of the present disclosure, and other drawings may be obtained according to the structures shown in the drawings without any creative work for a person having ordinary skill in the art.

[0062] FIG. 1 is a flowchart of a communication authentication and key agreement method according to an embodiment of the present disclosure.

[0063] FIG. 2 is a schematic structural diagram of a communication authentication and key agreement system according to an embodiment of the present disclosure.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0064] The embodiments of the present disclosure will be described in detail below. Examples of the embodiments are shown in the accompanying drawings, wherein the same or similar reference numerals indicate the same or similar components, or components with the same or similar functions. The embodiments described below with reference to the

accompanying drawings are exemplary, and are intended to explain the present disclosure, but should not be construed as limiting the present disclosure.

[0065] Referring to FIG. 1, the method includes the following operations. Meanwhile, for ease of description, the reference numerals in the method are shown in Table 1.

Table 1 Description of the reference numerals

Reference numeral	Description
ID_i	User name
PW_i	User's password
P	Base point on an elliptic curve
k_s	Public key of the server
K_s	Private key of the server
$h(\cdot)$	Secure hash function
$\|$	Connection operation
$\oplus$	Exclusive OR operation
$E_s(\cdot)$	Encryption function
$D_s(\cdot)$	Decryption function

[0066] The present disclosure is a mobile storage-based authentication and key exchange scheme designed in a telecare medicine environment, which mainly includes four stages: an initialization stage, a user registration stage, a login and authentication stage, and a password modification stage.

[0067] Initialization stage: in the stage the server is configured to initialize related

parameters. An elliptic curve and a base point P on the elliptic curve are chosen. A hash function $h(\cdot)$is chosen. An encryption and decryption function $E_s(\cdot)/D_s(\cdot)$ is chosen. A private key $k_s$is chosen. And $K_s = k_s \cdot P$ is calculated.

[0068] User registration stage: user must register with the server before enjoying services provided by the server.

[0069] Login and authentication stage: the registered user can send a login request to the server, and the session key for this communication is established after the two-way identity authentication between the user the server is finished.

[0070] Password modification stage: user can modify the password in this stage when user perceives that the password is at risk of leaking. No assistance from the server is required at the stage.

[0071] The communication authentication and key agreement method shown in FIG. 1 is applied to a mobile storage device and configured to implement communication authentication and key agreement with the remote server. The method includes operations S1 to S4.

[0072] In operation S1, receiving a user name and a password entered by a user, and judging whether the user is an owner of the mobile storage device.

[0073] In the present embodiment, before the operation "receiving a user name and a password entered by a user", the method further includes the user registration stage which specifically includes:

[0074] calculating $HPW_i = h(PW_i \parallel b)$ by the user name ID_i and the password PW_i selected

by the user and the generation random number b, transmitting $\{ID_i, HPW_i\}$ as registration information to the server, calculating by the server $A_i = h(ID_i \| k_s)$, $B_i = h(h(ID_i \| HPW_i) \, mod \, m)$ and $C_i = A_i \oplus HPW_i \oplus B_i$ through one generation random number $m(2^4 < m < 2^8)$ after receiving the registration information, and storing a parameter $\{B_i, C_i, m, K_s, E_s(\cdot), D_s(\cdot), h(\cdot)\}$ as storage data in the mobile storage device and returning the storage data to the user, $h(\cdot)$ is a hash function, $\|$ is a connection operation, k_s is a private key of the server, K_s is a public key of the server, $K_s = k_s \cdot P$, $E_s(\cdot)$ is an encryption function, $D_s(\cdot)$ is a decryption function, P is a base point on an elliptic curve, and $\oplus$ is an exclusive OR operation.

[0075] When the user receives the mobile storage device returned by the server, b is stored in the mobile storage device.

[0076] In the present embodiment, the operation of "judging whether the user is an owner of the mobile storage device according to the user name and the password entered by the user" specifically includes:

[0077] entering by the user the user name ID_i and password PW_i;

[0078] calculating $HPW_i = h(PW_i \| b)$ and $B_i^* = h(h(ID_i \| HPW_i) \, mod \, m)$, and comparing whether B_i^* is equal to B_i;

[0079] if yes, determining that the user is the owner of the mobile storage device; and

[0080] if no, terminating a session.

[0081] In operation S2, calculating first transmission data transmitted to the server by a generation random number and a time stamp after determining that the user is the owner of the

mobile storage device, and authenticating the mobile storage device by the server according to the first transmission data.

[0082] In the present embodiment, the operation of "calculating first transmission data transmitted to the server by a generation random number and a time stamp" includes:

[0083] generating the generation random number r_c and the time stamp T_1;

[0084] calculating $A_i = C_i \oplus HPW_i \oplus B_i$, $R_c = r_c A_i P$, $k1 = r_c A_i K_s$, and $H_i = E_{k1}(realm \parallel ID_i \parallel A_i \parallel T_1)$; and

[0085] transmitting $\{H_i, R_c\}$ as the first transmission data to the server;

[0086] wherein, the operation of "authenticating the mobile storage device by the server according to the first transmission data" includes:

[0087] after the server receiving the first transmission data $\{H_i, R_c\}$, calculating $k2 = k_s R_c$, and decrypting H_i by a calculated result to acquire $realm \parallel ID_i \parallel A_i \parallel T_1$;

[0088] verifying by the server a legitimacy of the time stamp T_1;

[0089] if the time stamp T_1 is legal, calculating $A_i^* = h(ID_i \parallel k_s)$ and verifying $A_i^* ?= A_i$; if the two values are equal, passing by the server the authentication of the mobile storage device; otherwise, terminating the session; and

[0090] generating by the server the generation random number r_s and the time stamp T_2, calculating $R_s = r_s \cdot P$, $J_i = r_s R_c$, $SK = h(J_i \parallel T_1 \parallel T_2)$, and $L_i = E_{k2}(ID_i \parallel R_s \parallel J_i \parallel T_2 \parallel realm)$, and transmitting $\{L_i\}$ as the second transmission data to the mobile storage device.

[0091] In operation S3, receiving second transmission data from the server, and

authenticating the server according to the second transmission data.

[0092] In the present embodiment, the operation of "authenticating the server according to the second transmission data" includes:

[0093] after receiving the second transmission data $\{L_i\}$, decrypting L_i through $r_c A_i K_s$ to acquire $ID_i \parallel R_s \parallel J_i \parallel T_2 \parallel realm$, and verifying whether the time stamp T_2 is legal;

[0094] if the time stamp T_2 is legal, calculating $J_i' = r_c A_i R_s$ and verifying $J_i' \stackrel{?}{=} J_i$; and

[0095] if the two values are equal, passing by the server the authentication of the mobile storage device.

[0096] In operation S4, calculating a session key for communicating with the server after the server is authenticated.

[0097] In the present embodiment, the operation of "calculating a session key for communicating with the server" includes:

[0098] calculating the session key for communicating with the server as $SK = h(J_i' \parallel T_1 \parallel T_2)$.

[0099] In the present embodiment, the password modification stage includes: modifying by the user the password when the user perceives that the password is at risk of leaking. No assistance from the server is required at the stage. The main operations are as follow:

[00100] (1) entering by the user the user name ID_i and the password PW_i, calculating $HPW_i = h(PW_i \parallel b)$ and $B_i^* = h(h(ID_i \parallel HPW_i) \bmod m)$ by the mobile storage device, and comparing whether B_i^* is equal to B_i; if yes, determining that the user is the owner of the mobile storage

device, and proceeding to the next operations; if no, terminating the password modification requirement.

[00101] (2) entering by the user a new password PW_i^{new}, calculating by the mobile storage device a parameter $HPW_i^{new} = h(PW_i^{new} \| b)$, $B_i^{new} = h(h(ID_i \| HPW_i^{new}) \bmod m)$, and $C_i^{new} = C_i \oplus HPW_i \oplus B_i \oplus HPW_i^{new} \oplus B_i^{new}$; then replacing B_i^{new} and C_i^{new} with B_i and C_i。

[00102] Referring to FIG. 2, which shows a schematic structural diagram of a communication authentication and key agreement system 10 according to an embodiment of the present disclosure.

[00103] In the present embodiment, the communication authentication and key agreement system 10 is applied to a mobile storage device, and configured to implement communication authentication and key agreement with the remote server. The communication authentication and key agreement system 10 includes: a registering module 11, a judging module 12, a transmitting module 13, a verifying module 14, and a calculating module 15.

[00104] The registering module 11 is configured for calculating $HPW_i = h(PW_i \| b)$ by the user name ID_i and the password PW_i selected by the user and the generation random number b, transmitting $\{ID_i, HPW_i\}$ as registration information to the server, calculating by the server $A_i = h(ID_i \| k_s)$, $B_i = h(h(ID_i \| HPW_i) \, mod \, m)$ and $C_i = A_i \oplus HPW_i \oplus B_i$ through one generation random number $m(2^4 < m < 2^8)$ after receiving the registration information, and storing a parameter $\{B_i, C_i, m, K_s, E_s(\cdot), D_s(\cdot), h(\cdot)\}$ as storage data in the mobile storage device and returning the storage data to the user, $h(\cdot)$ is a hash function, $\|$ is a connection operation, k_s is a

private key of the server, K_s is a public key of the server, $K_s = k_s \cdot P$, $E_s(\cdot)$ is an encryption function, $D_s(\cdot)$ is a decryption function, P is a base point on an elliptic curve, and $\oplus$ is an exclusive OR operation.

[00105] The judging module 12 is configured for receiving a user name and a password entered by a user, and judging whether the user is an owner of the mobile storage device;

[00106] In the present embodiment, the judging module 12 is specifically configured for:

[00107] entering by the user the user name ID_i and password PW_i;

[00108] calculating $HPW_i = h(PW_i \parallel b)$ and $B_i^* = h(h(ID_i \parallel HPW_i) \bmod m)$, and comparing whether B_i^* is equal to B_i;

[00109] if yes, determining that the user is the owner of the mobile storage device; and

[00110] if no, terminating a session.

[00111] The transmitting module 13 is specifically configured for calculating first transmission data transmitted to a server by a generation random number and a time stamp after determining that the user is the owner of the mobile storage device, and authenticating the mobile storage device by the server according to the first transmission data.

[00112] In the present embodiment, the transmitting module 13 is specifically configured for:

[00113] generating the generation random number r_c and the time stamp T_1;

[00114] calculating $A_i = C_i \oplus HPW_i \oplus B_i$, $R_c = r_c A_i P$, $k1 = r_c A_i K_s$, and $H_i = E_{k1}(realm \parallel ID_i \parallel A_i \parallel T_1)$; and

[00115] transmitting $\{H_i, R_c\}$ as the first transmission data to the server;

[00116] wherein, the operation of "authenticating the mobile storage device by the server according to the first transmission data" includes:

[00117] after the server receiving the first transmission data $\{H_i, R_c\}$, calculating $k2 = k_s R_c$, and decrypting H_i by a calculated result to acquire $realm \parallel ID_i \parallel A_i \parallel T_1$;

[00118] verifying by the server a legitimacy of the time stamp T_1;

[00119] if the time stamp T_1 is legal, calculating $A_i^* = h(ID_i \parallel k_s)$ and verifying $A_i^* ? = A_i$; if the two values are equal, passing by the server the authentication of the mobile storage device; otherwise, terminating the session; and

[00120] generating by the server the generation random number r_s and the time stamp T_2, calculating $R_s = r_s \cdot P$, $J_i = r_s R_c$, $SK = h(J_i \parallel T_1 \parallel T_2)$, and $L_i = E_{k2}(ID_i \parallel R_s \parallel J_i \parallel T_2 \parallel realm)$, and transmitting $\{L_i\}$ as the second transmission data to the mobile storage device.

[00121] The verifying module 14 is configured for receiving second transmission data from the server, and authenticating the server according to the second transmission data.

[00122] In the present embodiment, the verifying module 14 is specifically configured for:

[00123] after receiving the second transmission data $\{L_i\}$, decrypting L_i through $r_c A_i K_s$ to acquire $ID_i \parallel R_s \parallel J_i \parallel T_2 \parallel realm$, and verifying whether the time stamp T_2 is legal;

[00124] if the time stamp T_2 is legal, calculating $J_i' = r_c A_i R_s$ and verifying $J_i' ? = J_i$; and

[00125] if the two values are equal, passing by the server the authentication of the mobile storage device.

[00126] The calculating module 15 is configured for calculating the session key for

communicating with the server after the server is authenticated.

[00127] In the present embodiment, the calculating module 15 is specifically configured for:

[00128] calculating the session key for communicating with the server as $SK = h(J_i' \| T_1 \| T_2)$.

[00129] In the embodiments of the present disclosure, an elliptic curve cryptosystem is adopted in the process of realizing identity verification and key agreement. Under the same security level, the elliptic curve cryptosystem requires less storage and computing resources, and can be better adapted to resource-constrained devices. The embodiments of the present disclosure provide user anonymity and untraceability. The embodiments of the present disclosure can also better resist common network attacks, such as offline password guessing attacks, user impersonation attacks, man-in-the-middle attacks, and the like.

[00130] In the description of the specification, the description with reference to terms "one implementation", "some implementations", "one embodiment", "some embodiments", "example", "specific examples", or "some examples" and the like means that the specific features, structures, materials or characteristics described in conjunction with the embodiments or examples are included in at least one embodiment or example of the present disclosure. In this specification, the schematic representations of the above terms do not necessarily refer to the same embodiment or example. Moreover, the described specific features, structures, materials or characteristics may be combined in any one or more embodiments or examples in a suitable manner.

[00131] The above content is a further detailed description of the present disclosure in combination with specific embodiments, and it cannot be considered that the specific implementation of the present disclosure is limited to these descriptions. For those of ordinary skill in the art to which the present disclosure belongs, a number of simple deductions or substitutions can also be made without departing from the concept of the present disclosure. LU102259

CLAIMS

What is claimed is:

1. A communication authentication and key agreement method, applied to a mobile storage device, comprising:

receiving a user name and a password entered by a user, and judging whether the user is an owner of the mobile storage device;

calculating first transmission data transmitted to a server by a generation random number and a time stamp after determining that the user is the owner of the mobile storage device, and authenticating the mobile storage device by the server according to the first transmission data;

receiving second transmission data from the server, and authenticating the server according to the second transmission data; and

calculating a session key for communicating with the server after the server is authenticated.

2. The method according to claim 1, wherein before the operation “receiving a user name and a password entered by a user”, the method further comprises:

calculating $HPW_i = h(PW_i \parallel b)$ by the user name ID_i and the password PW_i selected by the user and the generation random number b, transmitting $\{ID_i, HPW_i\}$ as registration information to the server, calculating by the server $A_i = h(ID_i \parallel k_s)$, $B_i = h(h(ID_i \parallel HPW_i)\ mod\ m)$ and $C_i = A_i \oplus HPW_i \oplus B_i$ through one generation random number $m(2^4 < m < 2^8)$ after receiving the

registration information, and storing a parameter $\{B_i, C_i, m, K_s, E_s(\cdot), D_s(\cdot), h(\cdot)\}$ as storage data in the mobile storage device and returning the storage data to the user, $h(\cdot)$ is a hash function, $\|$ is a connection operation, k_s is a private key of the server, K_s is a public key of the server, $K_s = k_s \cdot P$, $E_s(\cdot)$ is an encryption function, $D_s(\cdot)$ is a decryption function, P is a base point on an elliptic curve, and $\oplus$ is an exclusive OR operation.

3. The method according to claim 2, wherein the operation of "judging whether the user is an owner of the mobile storage device according to the user name and the password entered by the user" comprises:

entering by the user the user name ID_i and password PW_i;

calculating $HPW_i = h(PW_i \| b)$ and $B_i^* = h(h(ID_i \| HPW_i) \, mod \, m)$, and comparing whether B_i^* is equal to B_i;

if yes, determining that the user is the owner of the mobile storage device; and

if no, terminating a session.

4. The method according to claim 3, wherein the operation of "calculating first transmission data transmitted to a server by a generation random number and a time stamp" comprises:

generating the generation random number r_c and the time stamp T_1;

calculating $A_i = C_i \oplus HPW_i \oplus B_i$, $R_c = r_c A_i P$, $k1 = r_c A_i K_s$, and $H_i = E_{k1}(realm \parallel ID_i \parallel A_i \parallel T_1)$; and

transmitting $\{H_i, R_c\}$ as the first transmission data to the server;

wherein, the operation of "authenticating the mobile storage device by the server according to the first transmission data" comprises:

after the server receiving the first transmission data $\{H_i, R_c\}$, calculating $k2 = k_s R_c$, and decrypting H_i by a calculated result to acquire $realm \parallel ID_i \parallel A_i \parallel T_1$;

verifying by the server a legitimacy of the time stamp T_1;

if the time stamp T_1 is legal, calculating $A_i^* = h(ID_i \parallel k_s)$ and verifying $A_i^* ? = A_i$; if the two values are equal, passing by the server the authentication of the mobile storage device; otherwise, terminating the session; and

generating by the server the generation random number r_s and the time stamp T_2, calculating $R_s = r_s \cdot P$, $J_i = r_s R_c$, $SK = h(J_i \parallel T_1 \parallel T_2)$, and $L_i = E_{k2}(ID_i \parallel R_s \parallel J_i \parallel T_2 \parallel realm)$, and transmitting $\{L_i\}$ as the second transmission data to the mobile storage device.

5. The method according to claim 4, wherein the operation of "authenticating the server according to the second transmission data" comprises:

after receiving the second transmission data $\{L_i\}$, decrypting L_i through $r_c A_i K_s$ to acquire $ID_i \parallel R_s \parallel J_i \parallel T_2 \parallel realm$, and verifying whether the time stamp T_2 is legal;

if the time stamp T_2 is legal, calculating $J_i' = r_c A_i R_s$ and verifying $J_i' ? = J_i$; and

if the two values are equal, passing by the server the authentication of the mobile storage

device.

6. The method according to claim 5, wherein the operation of "calculating a session key for communicating with the server" comprises:

calculating the session key for communicating with the server as $SK = h(J_i' \| T_1 \| T_2)$.

7. A communication authentication and key agreement system, applied to a mobile storage device, wherein the system comprises:

a judging module, configured for receiving a user name and a password entered by a user, and judging whether the user is an owner of the mobile storage device;

a transmitting module, configured for calculating first transmission data transmitted to a server by a generation random number and a time stamp after determining that the user is the owner of the mobile storage device, and authenticating the mobile storage device by the server according to the first transmission data;

a verifying module, configured for receiving second transmission data from the server, and authenticating the server according to the second transmission data; and

a calculating module, configured for calculating a session key for communicating with the server after the server is authenticated.

8. The system according to claim 7, wherein the system further comprises:

a registering module, configured for calculating $HPW_i = h(PW_i \parallel b)$ by the user name ID_i and the password PW_i selected by the user and the generation random number b, transmitting $\{ID_i, HPW_i\}$ as registration information to the server, calculating by the server $A_i = h(ID_i \parallel k_s)$, $B_i = h(h(ID_i \parallel HPW_i)\, mod\, m)$ and $C_i = A_i \oplus HPW_i \oplus B_i$ through one generation random number $m(2^4 < m < 2^8)$ after receiving the registration information, and storing a parameter $\{B_i, C_i, m, K_s, E_s(\cdot), D_s(\cdot), h(\cdot)\}$ as storage data in the mobile storage device and returning the storage data to the user, $h(\cdot)$ is a hash function, $\parallel$ is a connection operation, k_s is a private key of the server, K_s is a public key of the server, $K_s = k_s \cdot P$, $E_s(\cdot)$ is an encryption function, $D_s(\cdot)$ is a decryption function, P is a base point on an elliptic curve, and $\oplus$ is an exclusive OR operation.

9. The system according to claim 8, wherein the judging module is specifically configured for:

entering by the user the user name ID_i and password PW_i;

calculating $HPW_i = h(PW_i \parallel b)$ and $B_i^* = h(h(ID_i \parallel HPW_i)\, mod\, m)$, and comparing whether B_i^* is equal to B_i;

if yes, determining that the user is the owner of the mobile storage device; and

if no, terminating a session.

10. The system according to claim 9, wherein the transmitting module is specifically configured for:

generating the generation random number r_c and the time stamp T_1;

calculating $A_i = C_i \oplus HPW_i \oplus B_i$, $R_c = r_c A_i P$, $k1 = r_c A_i K_s$, and $H_i = E_{k1}(realm \parallel ID_i \parallel A_i \parallel T_1)$; and

transmitting $\{H_i, R_c\}$ as the first transmission data to the server;

wherein, the operation of "authenticating the mobile storage device by the server according to the first transmission data" comprises:

after the server receiving the first transmission data $\{H_i, R_c\}$, calculating $k2 = k_s R_c$, and decrypting H_i by a calculated result to acquire $realm \parallel ID_i \parallel A_i \parallel T_1$;

verifying by the server a legitimacy of the time stamp T_1;

if the time stamp T_1 is legal, calculating $A_i^* = h(ID_i \parallel k_s)$ and verifying $A_i^* ?= A_i$; if the two values are equal, passing by the server the authentication of the mobile storage device; otherwise, terminating the session; and

generating by the server the generation random number r_s and the time stamp T_2, calculating $R_s = r_s \cdot P$, $J_i = r_s R_c$, $SK = h(J_i \parallel T_1 \parallel T_2)$, and $L_i = E_{k2}(ID_i \parallel R_s \parallel J_i \parallel T_2 \parallel realm)$, and transmitting $\{L_i\}$ as the second transmission data to the mobile storage device.

11. The system according to claim 10, wherein the verifying module is specifically configured for:

after receiving the second transmission data $\{L_i\}$, decrypting L_i through $r_c A_i K_s$ to acquire $ID_i \parallel R_s \parallel J_i \parallel T_2 \parallel realm$, and verifying whether the time stamp T_2 is legal;

if the time stamp T_2 is legal, calculating $J_i' = r_c A_i R_s$ and verifying $J_i' \stackrel{?}{=} J_i$; and

if the two values are equal, passing by the server the authentication of the mobile storage device.

12. The system according to claim 11, wherein the calculating module is specifically configured for:

calculating the session key for communicating with the server as $SK = h(J_i' \| T_1 \| T_2)$.

REVENDICATIONS

1. Procédé d'authentification de communications et d'accord sur des clés, appliqué à un dispositif de stockage mobile, comprenant:

la réception d'un nom d'utilisateur et d'un mot de passe entrés par un utilisateur, et le jugement du fait que l'utilisateur est un propriétaire du dispositif de stockage mobile;

le calcul de premières données d'émission émises à un serveur par un nombre aléatoire de génération et un marquage d'horodatage après la détermination que l'utilisateur est le propriétaire du dispositif de stockage mobile, et l'authentification du dispositif de stockage mobile par le serveur selon les premières données d'émission;

la réception de secondes données d'émission du serveur, et l'authentification du serveur selon les secondes données d'émission; et

le calcul d'une clé de session pour la communication avec le serveur après que le serveur est authentifié.

2. Procédé selon la revendication 1, dans lequel avant que l'opération de « réception d'un nom d'utilisateur et d'un mot de passe entrés par un utilisateur », le procédé comprenant en outre:

le calcul $HPW_i = h(PW_i \| \mathrm{b})$ par le nom d'utilisateur ID_i et le mot de passe PW_i sélectionnés par l'utilisateur et le nombre aléatoire de génération b, la transmission $\{ID_i, HPW_i\}$ comme informations d'inscription au serveur, le calcul par le serveur $A_i = h(ID_i \| k_s)$, $B_i = h(h(ID_i \| HPW_i) \ mod \ m)$ et $C_i = A_i \oplus HPW_i \oplus B_i$ à travers un nombre aléatoire de génération $m(2^4 < m < 2^8)$ après la réception des informations d'inscription, et le stockage d'un paramètre $\{B_i, C_i, m, K_s, E_s(\cdot), D_s(\cdot), h(\cdot)\}$ comme données de stockage dans le dispositif de stockage mobile et le retour des données de stockage à l'utilisateur, $h(\cdot)$ est une fonction de hachage, $\|$ est une opération de connexion, k_s est une clé privée du serveur, K_s est une clé publique du serveur, $K_s = k_s \cdot P$, $E_s(\cdot)$ est une fonction de chiffrement, $D_s(\cdot)$ est une fonction de déchiffrement, P est un point de base sur une courbe elliptique, et $\oplus$ est une opération OU exclusif.

3. Procédé selon la revendication 2, dans lequel l'opération de « jugement du fait que l'utilisateur est un propriétaire du dispositif de stockage mobile selon le nom d'utilisateur et le mot de passe entrés par l'utilisateur » comprend:

l'entrée par l'utilisateur du nom d'utilisateur ID_i et du mot de passe PW_i;

le calcul $HPW_i = h(PWi \| b)$ et $B_i^* = h(h(ID_i \| HPW_i) \ mod \ m)$, et la comparaison si B_i^* est égal à B_i;

si oui, la détermination que l'utilisateur est le propriétaire du dispositif de stockage mobile; et

si non, la clôture d'une session.

4. Procédé selon la revendication 3, dans lequel l'opération de « calcul de premières données d'émission émises à un serveur par un nombre aléatoire de génération et un marquage d'horodatage » comprend:

la génération du nombre aléatoire de génération r_c et de marquage d'horodatage T_1;

le calcul $A_i = C_i \oplus HPW_i \oplus B_i$, $R_c = r_c A_i P$, $k_1 = r_c A_i Ks$, et $H_i = Ek_1(domaine \| ID_i \| A_i \| T_1)$; et

l'émission $\{H_i, R_c\}$ comme premières données d'émission au serveur;

dans lequel, l'opération d'« authentification du dispositif de stockage mobile par le serveur selon les premières données d'émission » comprend:

après que le serveur a reçu les premières données d'émission $\{H_i, R_c\}$, le calcul $k_2 = k_s R_c$, et le déchiffrement H_i par un résultat calculé pour acquérir $domaine \| ID_i \| A_i \| T_1$;

la vérification par le serveur d'une légitimité de marquage d'horodatage T_1;

si le marquage d'horodatage T_1 est légitime, le calcul $A_i^* = h(ID_i \| k_s)$ et la vérification $A_i^* ? = A_i$; si les deux valeurs sont égales, le passage par le serveur de l'authentification du dispositif de stockage mobile; sinon, la clôture de la session; et

la génération par le serveur du nombre aléatoire de génération r_s et de marquage d'horodatage T_2, le calcul $R_s = r_s \mathrm{P}$, $J_i = r_s R_c$, $SK = h(J_i \| T_1 \| T_2)$, et $L_i = Ek_2(ID_i \| R_s \| J_i \| T_2 \| domaine)$, et l'émission $\{L_i\}$ comme les secondes données d'émission au dispositif de stockage mobile.

5. Procédé selon la revendication 4, dans lequel l'opération d'« authentification du serveur selon les secondes données d'émission » comprend:

après la réception des secondes données d'émission $\{L_i\}$, le déchiffrement L_i à travers $r_c A_i Ks$ pour acquérir $ID_i \| R_s \| J_i \| T_2 \| \mathrm{domaine}$, et la vérification du fait que le marquage d'horodatage T_2 est légitime;

si le marquage d'horodatage T_2 est légitime, le calcul $J_i' = r_c A_i R_s$ et la vérification $J_i' ? = J_i$; et

si les deux valeurs sont égales, le passage par le serveur de l'authentification du dispositif de stockage mobile.

6. Procédé selon la revendication 5, dans lequel l'opération de « calcul d'une clé de session pour la communication avec le serveur » comprend:

le calcul de la clé de session pour la communication avec le serveur comme $SK = h(J_i' \| T_1 \| T_2)$.

7. Système d'authentification de communications et d'accord sur des clés, appliqué à un dispositif de stockage mobile, dans lequel le système comprend:

un module de jugement, configuré pour recevoir un nom d'utilisateur et un mot de passe entrés par un utilisateur, et le jugement du fait que l'utilisateur est un propriétaire du dispositif de stockage mobile;

un module d'émission, configuré pour le calcul de premières données d'émission émises à un serveur par un nombre aléatoire de génération et un marquage d'horodatage après la détermination que l'utilisateur est le propriétaire du dispositif de stockage mobile, et l'authentification du dispositif de stockage mobile par le serveur selon les premières données d'émission;

un module de vérification, configuré pour la réception de secondes données d'émission du serveur, et l'authentification du serveur selon les secondes données d'émission; et

un module de calcul, configuré pour calculer une clé de session pour la communication avec le serveur après que le serveur a été authentifié.

8. Système selon la revendication 7, dans lequel le système comprend en outre:

un module d'enregistrement, configuré pour le calcul $HPW_i = h(PW_i||b)$ par le nom d'utilisateur ID_i et le mot de passe PW_i sélectionnés par l'utilisateur et le nombre aléatoire de génération b, la transmission $\{ID_i, HPW_i\}$ comme informations d'inscription au serveur, le calcul par le serveur $A_i = h(ID_i||k_s)$, $B_i = h(h(ID_i||HPW_i)\ mod\ m)$ et $C_i = A_i \oplus HPW_i \oplus B_i$ à travers un nombre aléatoire de génération $m(2^4 < m < 2^8)$ après la réception des informations d'inscription, et le stockage d'un paramètre $\{B_i, C_i, m, K_s, E_s(\cdot), D_s(\cdot), h(\cdot)\}$ comme données de stockage dans le dispositif de stockage mobile et le retour des données de stockage à l'utilisateur, $h(\cdot)$ est une fonction de hachage, $||$ est une opération de connexion, k_s est une clé privée du serveur, K_s est une clé publique du serveur, $Ks = k_s \cdot P$, $E_s(\cdot)$ est une fonction de chiffrement, $D_s(\cdot)$ est une fonction de déchiffrement, P est un point de base sur une courbe elliptique, et $\oplus$ est une opération OU exclusif.

9. Système selon la revendication 8, dans lequel le module de jugement est spécifiquement configuré pour:

l'entrée par l'utilisateur du nom d'utilisateur ID_i et du mot de passe PW_i;

le calcul $HPW_i = h(PW_i||b)$ et $B_i^* = h(h(ID_i||HPW_i)\ mod\ m)$, et la comparaison du fait que B_i^* est égal à B_i;

si oui, la détermination que l'utilisateur est le propriétaire du dispositif de stockage mobile; et

si non, la clôture d'une session.

10. Système selon la revendication 9, dans lequel le module d'émission est spécifiquement configuré pour:

la génération du nombre aléatoire de génération r_c et du marquage d'horodatage T_1;

le calcul $A_i = C_i \oplus HPW_i \oplus B_i$, $R_c = r_c A_i P$, $k_1 = r_c A_i K_s$, et $H_i = Ek_1(\text{domaine}||ID_i||A_i||T_1)$; et

l'émission $\{H_i, R_c\}$ comme premières données d'émission au serveur;

dans lequel, l'opération d'« authentification du dispositif de stockage mobile par le serveur selon les premières données d'émission » comprend:

après la réception par le serveur des premières données d'émission $\{H_i, R_c\}$, le calcul $k_2 = k_s R_c$, et le déchiffrement H_i par un résultat calculé pour acquérir le domaine$\|ID_i\|A_i\|T_1$;

la vérification par le serveur d'une légitimité de marquage d'horodatage T_1;

si le marquage d'horodatage T_1 est légitime, le calcul $A_i^* = h(ID_i\|k_s)$ et la vérification $A_i^*? = A_i$; si les deux valeurs sont égales, le passage par le serveur de l'authentification du dispositif de stockage mobile; sinon, la clôture de la session; et

la génération par le serveur du nombre aléatoire de génération r_s et du marquage d'horodatage T_2, le calcul $R_s = r_s P$, $J_i = r_s R_c$, $SK = h(J_i\|T_1\|T_2)$, et $L_i = Ek_2(ID_i\|R_s\|J_i\|T_2\|\text{domaine})$, et l'émission $\{L_i\}$ comme secondes données d'émission au dispositif de stockage mobile.

11. Système selon la revendication 10, dans lequel le module de vérification est spécifiquement configuré pour:

après la réception des secondes données d'émission $\{L_i\}$, le déchiffrement L_i à travers $r_c A_i Ks$ pour acquérir $ID_i\|R_s\|J_i\|T_2\|$domaine, et la vérification du fait que le marquage d'horodatage T_2 est légitime;

si le marquage d'horodatage T_2 est légitime, le calcul $J_i' = r_c A_i R_s$ et la vérification $J_i'? = J_i$; et

si les deux valeurs sont égales, le passage par le serveur de l'authentification du dispositif de stockage mobile.

12. Système selon la revendication 11, dans lequel le module de calcul est spécifiquement configuré pour:

le calcul de la clé de session pour la communication avec le serveur comme $SK = h(J_i'\|T_1\|T_2)$.

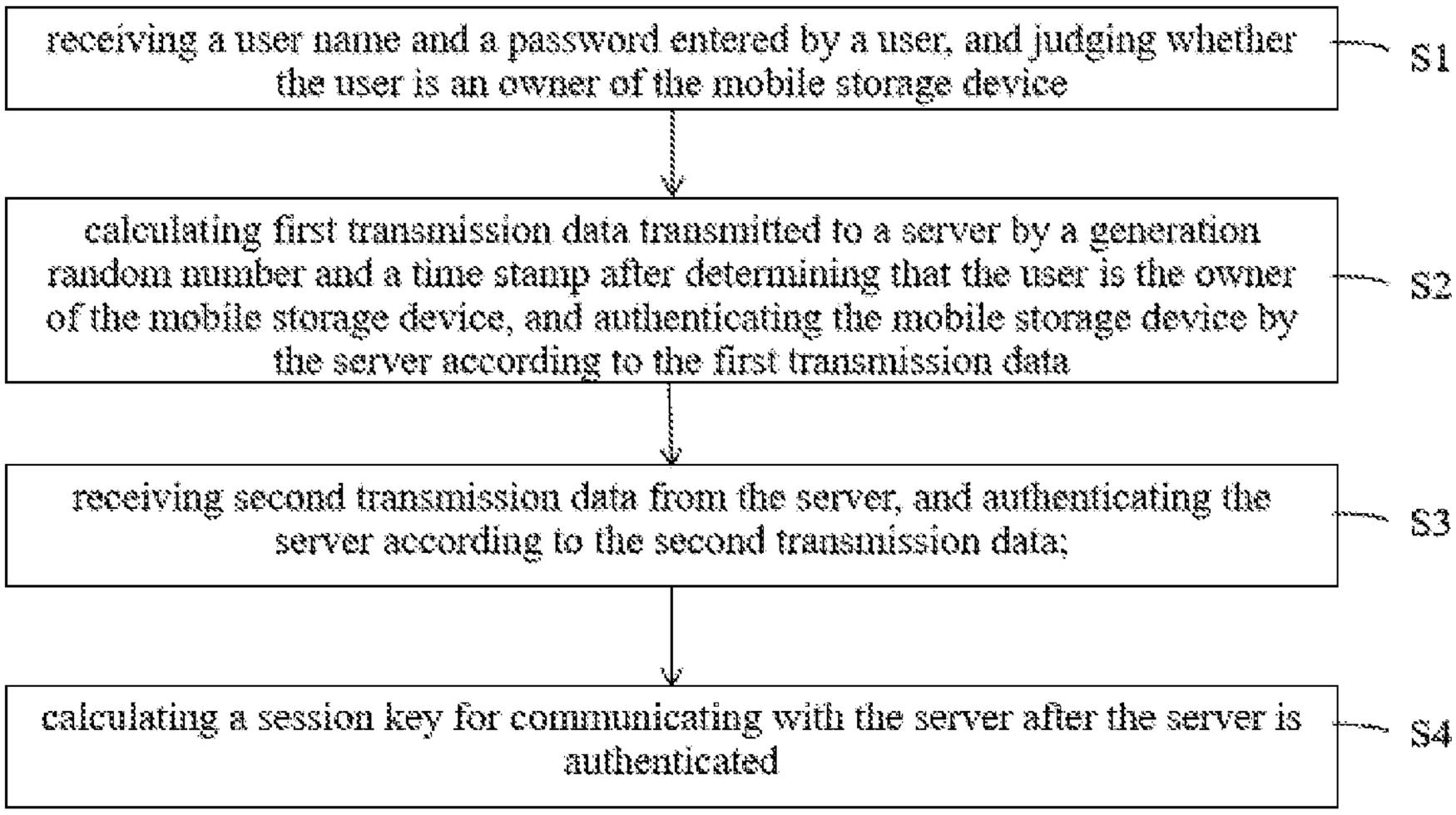
receiving a user name and a password entered by a user, and judging whether the user is an owner of the mobile storage device
S1
calculating first transmission data transmitted to a server by a generation random number and a time stamp after determining that the user is the owner of the mobile storage device, and authenticating the mobile storage device by the server according to the first transmission data
S2
receiving second transmission data from the server, and authenticating the server according to the second transmission data;
S3
calculating a session key for communicating with the server after the server is authenticated
S4

FIG. 1

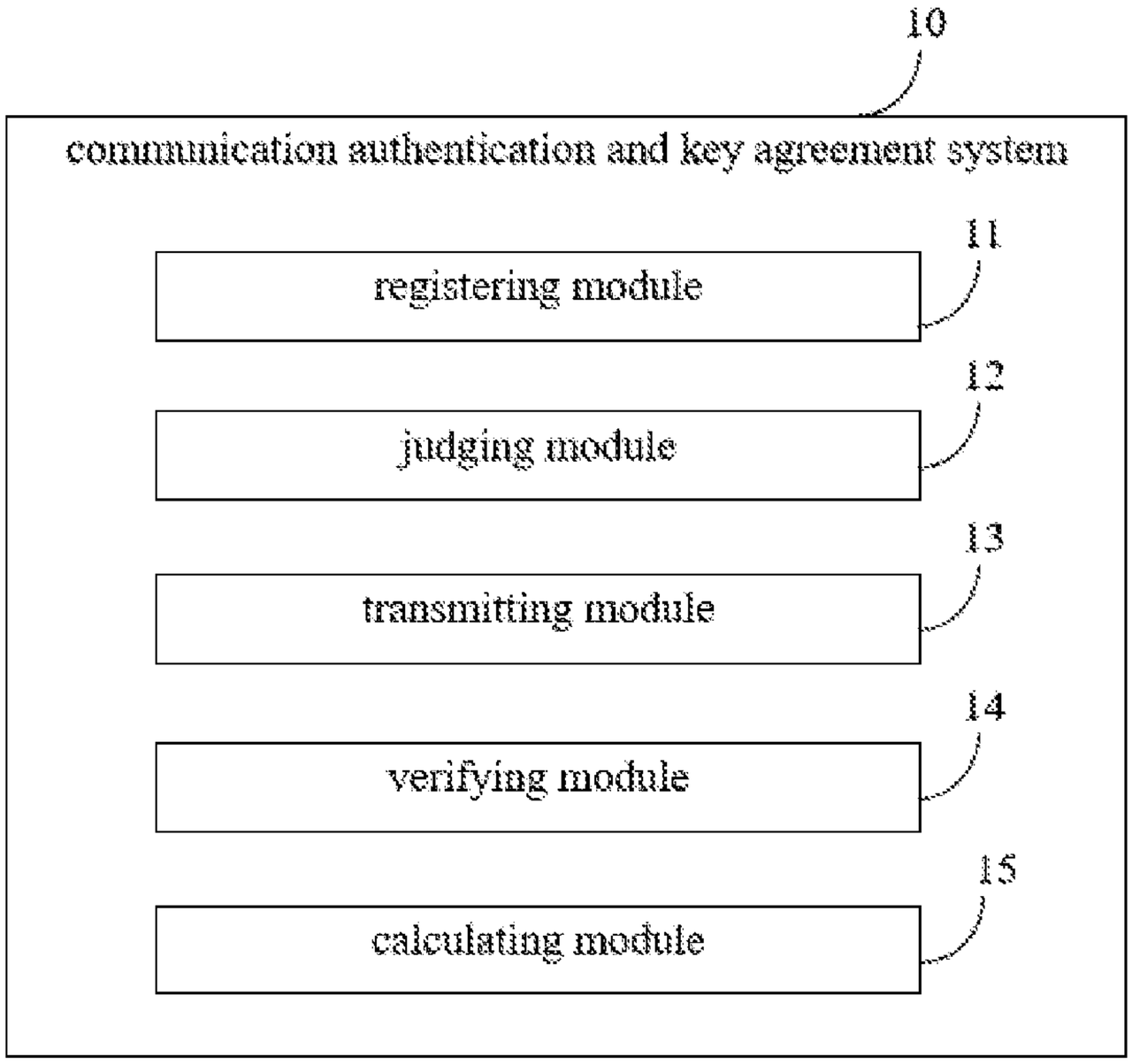
10
communication authentication and key agreement system
11
registering module
12
judging module
13
transmitting module
14
verifying module
15
calculating module

FIG. 2