(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 April 2009 (16.04.2009)

PCT

(10) International Publication Number
WO 2009/048191 A1

(51) International Patent Classification:
H04L 9/32 (2006.01) *G06F 15/00* (2006.01)
G06F 17/00 (2006.01)

(21) International Application Number:
PCT/KR2007/004983

(22) International Filing Date: 11 October 2007 (11.10.2007)

(25) Filing Language: Korean

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **INFORTIX CO., LTD** [KR/KR]; #303, Kwangwoon Business Incubation, Center, 447-1, Wolgye-Dong, Nowon-Gu, Seoul 139-701 (KR).

(72) Inventor: **GUEH, How Kiap**; Block 53, New Upper Changi Road, #13-1472, Singapore 461053 (SG).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **HAHN, Eun-ho** [KR/KR]; #323, BrownStone Junggye, Junggye2-Dong, Nowon-Gu, Seoul 139-222 (KR).

(74) Agent: **MI PATENT & LAW FIRM**; 5th Fl., Hongeun Bldg., 824-22, Yeoksam-Dong, Gangnam-Gu, Seoul 135-080 (KR).

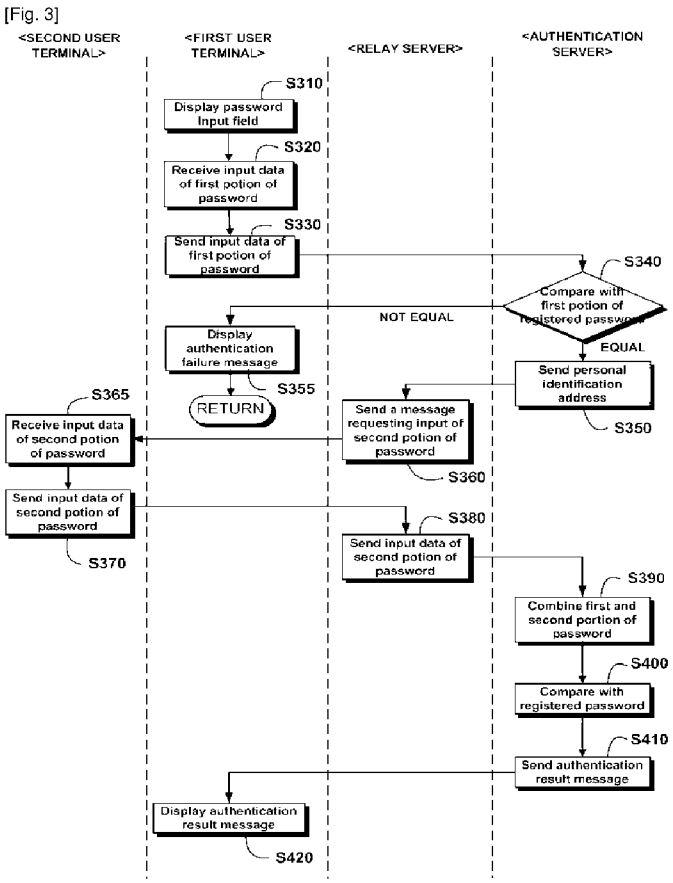
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL,

[Continued on next page]

(54) Title: SECURITY AUTHENTICATION METHOD AND SYSTEM

[Fig. 3]



(57) Abstract: This invention is for a method and system of authenticating personal identification, involving: receiving first portion of password corresponding to user id from first user terminal; sending personal identification address corresponding to the user id to relay server if the received first portion of password equals to the registered first portion of password; receiving second portion of password from the relay server; authenticating the password by combining first portion and second portion of password. Even if third party obtains password, the method provides enhanced anti-fraud protection by sending password with it being divide into tow or more portions depending on the user setup according this invention.

WO 2009/048191 A1

PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

Description

SECURITY AUTHENTICATION METHOD AND SYSTEM

Technical Field

[1] The present invention relates to a system and/or method in the field of security authentication. More particularly, the present invention relates to a system and/or method in the field of security authentication in order to strengthen security performance by sending personal information to authentication server with it being divided through different channels.

Background Art

[2] As Internet is being positioned to necessity for modern life, Internet services such as e-commerce, Internet banking and online game have become increasingly prevalent. Users wanting to utilize such Internet services have to subscribe to them as a member by via of user authentication. User authentication generally includes steps of; user entering ID and password to web browser of user terminal; sending them to server; server checking them to authenticate the user identification.

[3] In addition, user may input not only password but also social security number, credit card number, account number, mobile phone number to web browser on the user terminal to be authenticated by server.

[4] In the meantime, there increasingly occur damages due to leakage of personal information along with distribution of Internet. That is to say, cases that disreputable persons misuse social security number, password, credit card number, account number, mobile phone number at various internet services by obtaining them illegally are increasingly occurring.

[5] In addition, disreputable persons may misuse others' credit card number for various micro-payment services by obtaining it through sales slip following payment by use of credit card, or by obtaining credit card number or social security number directly.

[6] Many security programs have been developed to prevent others' social security number, password, credit card number, account number and mobile phone number from being misused for micro-payment at e-commerce transaction sites.

[7] For example, one previous attempt to solve the security problem has been Secure Electronic Transaction (SET) Technology. This technology requires a credit card to be authenticated via a smart chip reader installed on the user's computer system before the impending transaction.

[8] For Internet banking, users are required to, in advance, install public certificate issued by transaction server by entering user ID and social security number, and to enter password of the public certificate for payment.

[9] In these cases, it is a troublesome that users have to security program to user terminal in advance, and third party who obtained others' personal information can easily use it to carry out e-commerce transactions, lowering security.

Disclosure of Invention

Technical Problem

[10] The present invention has been made in an effort to provide a security authentication method and system in order to strengthen security performance.

Technical Solution

[11] An exemplary a method of authenticating personal identification according to an embodiment of the present invention comprises : receiving first portion of password corresponding to user id from first user terminal; sending personal identification address corresponding to the user id to relay server if the received first portion of password equals to first portion of registered password; receiving second portion of the password from the relay server; authenticating the password by combining first portion and second portion of password.

[12] The relay server may send request for input of second portion of the password through the personal identification address, and may receive second portion of the password from second user terminal.

[13] The personal identification address may include number of second user terminal or email address registered by user.

[14] The first user terminal and the second user terminal may be equal device.

[15] The first portion and the second portion of the password is transferred through separate two channels respectively.

[16] The second user terminal may be wireless handset.

[17] In one embodiment, the method may include sending result of authenticating the password to first user terminal.

[18] The first portion and the second portion of the password may include numbers or characters for additional services.

[19] An exemplary a method of authenticating personal identification according to other embodiment of the present invention comprises : receiving personal identification address corresponding to user id from authentication server that received first portion of password corresponding to the user id; sending request for input of second portion of the password through the personal identification address; receiving second portion of password from user terminal; sending the second portion of the password to the authentication server.

[20] The method may include sending request for input of second portion of the password is sent to the user terminal using Automatic calling System(ACS) if the personal iden-

tification address is number of the user terminal.

[21] The method may include sending request for input of second portion of the password is sent to the user terminal using Short Message Service(SMS) if the personal identification address is number of the user terminal.

[22] The method may include sending request for input of second portion of the password is sent to the user terminal using call back URL SMS if the personal identification address is number of the user terminal.

[23] The method may include sending request to access the web messenger is sent to the user terminal if the personal identification address is number of the user terminal.

[24] The method may include sending request for input of second portion of the password is sent to the email address or web messenger if the personal identification address is the email address.

[25] An exemplary a method of authenticating personal identification according to another embodiment of the present invention comprises : receiving first portion of password corresponding to user id from first user terminal; sending request for input of second portion of the password through personal identification address corresponding to the user id if the received first portion of password equals to the registered first portion of password; receiving second portion of the password from second user terminal; authenticating the password by combining first portion and second portion of the password.

[26] An exemplary a system of authenticating personal identification according to an embodiment of the present invention comprises : authentication server that receives first portion of password corresponding to user id from first user terminal and sends personal identification address corresponding to the user id if the received first portion of password equals to the first portion of registered password; and relay server that sends request for input of second portion of the password through received personal identification address, receives second portion of the password from second user terminal and sends second portion of the password to the authentication server.

[27] The authentication server may authenticate the password by combining first portion and second portion of the password, and may send result of authentication for the password to the first user terminal.

[28] An exemplary a system of authenticating personal identification according to other embodiment of the present invention comprises : authentication server that receives first portion of password corresponding to user id from first user terminal and sends request for input of second portion of the password to personal identification address corresponding to the user id if the received first portion of password equals to the first portion of registered password.

[29]

Advantageous Effects

[30] According to the present invention, even if third party obtains password, this invention provides anti-fraud protection by sending password with it being divide into two or more portions depending on the user setup.

[31] Furthermore according to another embodiment of this invention, if it is applied to approval system, senior level person can enter second portion of password to provide final approval for staff' planning or access to important company assets. Accordingly, this invention can serves as a system to restrict availability given to staffs, enhancing the security of in-house confidential items.

Brief Description of the Drawings

[32] FIG. 1 is a schematic representation of block diagram to illustrate authentication system according to first embodiment of this invention.

[33] FIG. 2 illustrates an example of login screen including password input field according to first embodiment of the present invention.

[34] FIG. 3 is a schematic representation of flow chart to illustrate user authentication process according to first embodiment of this invention.

[35] FIG. 4 is a schematic representation of block diagram to illustrate authentication system according to second embodiment of this invention.

[36] FIG. 5 is a schematic representation of flow chart to illustrate user authentication process according to second embodiment of this invention.

[37] FIG. 6 is a schematic representation of block diagram to illustrate authentication system according to third embodiment of this invention.

[38] FIG. 7 is a schematic representation of flow chart to illustrate user authentication process according to third embodiment of this invention.

Best Mode for Carrying Out the Invention

[39] Hereinafter, with reference to the drawings, embodiments of the present invention are provided so that knowledgeable persons in the technical field in which this invention is included can understand it easily.

[40] With reference to FIG. 1, authentication system according to first embodiment of this invention is described in detail firstly.

[41] FIG. 1 is a schematic representation of block diagram to illustrate authentication system according to first embodiment of this invention.

[42] With reference to FIG. 1, the security authentication system according to first embodiment of present invention includes first user terminal(110), second user terminal(120), authentication server(200) and relay server(300).

[43] The first user terminal(110) communicates with the authentication server(200), transferring information through communication networks(not seen in the figure) by

accessing them. The first user terminal(110) includes devices that provides operation capability by featuring memory devices and micro processor, such as desktop computers, notebook computers, workstations, palmtop computers, PDAs(Personal Digital Assistant), web pads, ATMs(Automatic Teller Machines) and remote civil affaire document issuers.

[44] The first user terminal(110) includes a client/server type program, or a browsers(not seen in the figure) for using internet communication network.

[45] The browser installed into the first user terminal(110) provides various functions, depending on user operation, by accessing service system and authentication server(200) through communication network. Examples of browser includes Internet Explorer from Microsoft, Netscape, Mozilla, Firefox, but not limited to them, whatever provides function to be able to communicate with internet service system and authentication server(200).

[46] The browser displays web page including password input field, based on web page information transferred from authentications server(200).

[47] The user who wants to access internet services provided by authentications server(200) becomes a member by submitting personal information such as ID(or other user identifications), password, credit card number, account number and social security number to service provider operating authentication server(200), enabling user to use internet service.

[48] And, the user who wants to go to security authentication through authentication server(200) requests to log into the system by entering user ID and first portion of password.

[49] After the user logs into the system, user requests user authentication by entering first portion of password into the password input field. For example, the user who wants to do electronic transaction with authentication server(200) requests user authentication by entering a portion of credit card number, account number or social security number, depending on the service, into the password input field on the first user terminal(110).

[50] The second user terminal(120) communicates with the relay server(300), transferring information through communication networks(not seen in the figure) with relay server(300) .

[51] The second user terminal(120) includes devices that provides operation capability by featuring memory devices and micro processors, such as wireless mobile handsets, notebook computers, workstations, palmtop computers, PDAs(Personal Digital Assistant) and web pads.

[52] The user who want to log into the authentication server(200) or to do electronic transaction service provided by authentication server(200) requests user authentication by sending a portion of password, credit card number, account number or social

security number, depending on the service, to relay server(300) through second user terminal(120) after the second user terminal receives a message from relay server(300).

[53] The authentication server(200) managed by financial institutions, web service organizations or public organizations provides web services such as portal service, electronic transaction service, internet banking or web service, depending on their purposes, to first user terminal(110).

[54] And, authentication server(200) provides web pages related to internet service, including password input page, to first user terminal by responding request from first user terminal(110), enabling first user terminal(110) to display internet service pages including password input page.

[55] Authentication server(200) includes user information database(201)(here inafter "user information DB") and authentication module(202) as shown in FIG.1.

[56] Not only ID registered to authentication server(200) but also personal identification address corresponding to each ID are stored to user information DB(201).

[57] Personal identification address specified by user, where request message from relay server is destined, includes reception number of second user terminal(120) and email address.

[58] More specifically, personal identification address corresponding to ID is also stored into user information DB(201) when user registers to a service with ID, allowing user to receive message from relay server(300).

[59] For example, if user wants to receive message through second user terminal(120), user registers number of second user terminal(120) to user information DB(201) as a user information for the purpose. Here, second user terminal(120) includes wireless mobile handsets such as mobile phone and PDA.

[60] If user wants to receive massage through email or messenger, user registers the corresponding email address to user information DB(201) as a user information for the purpose.

[61] User stores password that can be used to authenticate user identification, depending on the purpose of web services, into the user information DB(201).

[62] Here, password to check user identification corresponds to user ID and include not only password, credit card number, social security number, account number but also all unique characters or numbers or their combination that can be used to check user identification for the purpose. Password can also be a type of phrase for the purpose, depending on web services.

[63] For user information DB(201), it is desirable to store password, credit card number, social security number, account number using hash program such as Message Digest 5(MD5) than themselves for the security.

[64] In addition, user information DB(201) can provide personal identification address to

authentication server(200) by being located between authentication server(200) and relay server(300).

[65] Authentication module(202) performs user authentication by combining two portions of password transferred from first user terminal(110) and second user terminal(120) and checking if the combined password equals to the one registered to the user information DB(201).

[66] When request is received from authentication server(200), relay server(300) transfers the message using personal identification address. More specifically if relay server(300) receives number of second user terminal(120) from authentication server(200), it sends message requesting input of second portion of password to second user terminal(120) using the number.

[67] And if relay server(300) receives email address from authentication server(200), it sends message requesting input of second portion of password to the email address through wireless internet.

[68] And when second portion of password is entered from second user terminal(120), relay server(300) sends it to authentication server(200).

[69] With reference to FIG. 2, the process user requests login by entering password is as follows.

[70] FIG. 2 illustrates an example of login screen including password input field according to first embodiment of the present invention.

[71] As shown in FIG. 2, the login screen(114) displayed on first user terminal(110) can include ID input field, password input field(116), ID storage checkbox(117) and login submit button(118). The login screen(114) can include addition menus such as 'member registration' and 'Search ID/password' as well.

[72] User can request login by entering user ID and password into ID input field(115) and password input field(116) respectively, and clicking the login submit button(118) or pressing Enter. If login is successfully performed while ID storage checkbox(117) is checked, ID is continuously displayed at ID input field(115).

[73] While user ID is displayed at ID input field(115) as it is("Patent" in FIG.2), password is displayed as black circles at password input field(116) for the security.

[74] According an embodiment of this invention password is divided into two portions. User enters only first portion of password at the password input field(116), then second portion of password is entered through relay server(300).

[75] Assuming password is 7 characters(or numbers or their combination), user enters only first 4 characters corresponding to first portion of password into the password input field as shown in FIG. 2.

[76] The residual 3 characters of password input field, which corresponds to second portion of password, will be entered through second user terminal.

[77] In FIG.2, user enters first portion of password to log into web page. Furthermore when user uses web services such as portal service, e-commerce, internet banking, online game while user has been logged into the system, personal information such as credit card number, social security number and account number can be served as a type of password as in FIG. 2, meaning they can be used for the purpose depending on services with them being divided into two portions. While password is simply divided into two portions in FIG. 2, first portion and second portion of password can be expanded for additional services.

[78] That is to say, user can enter numbers or characters for additional services as well numbers(or characters or their combination) corresponding to second portion of password through second user terminal(120).

[79] Assuming, for example, second portion of password is '567', user can enter not only '567' but also an identifier(in this invention, it is assumed to '*') and login session request time(in this invention, it is assumed to 1 hour) continuously for the purpose depending on embodiments of invention.

[80] If user enters '567*1' through second user terminal, authentication server(200) authenticates the user using '567' that corresponds to second portion of password and sets the session interval to 1 hour.

[81] From now the process to authenticate user identification is described, with reference to FIG.3.

[82] FIG. 3 is a schematic representation of flow chart to illustrate user authentication process according to first embodiment of this invention.

[83] We assume user of first user terminal(110) is a member to be able to access web pages provided by authentication server(200), and user ID has been registered to authentication server(200).

[84] Web page displayed on first user terminal(110) includes password input field(116)(S310).

[85] Password input field(116) can be one for input of user password to log on, or one for input of user credit card number, social security number or account number depending on the purpose of services.

[86] When user enters first portion of password into the password input field(116), first user terminal(110) receives input data of first portion of password(S320).

[87] First user terminal(110) sends the input data including first portion of password to authentication server(200) (S330). If password input field(116) is one for login request, first user terminal(110) sends the entered user ID as well.

[88] After authentication server(200) receives the data, it compares it with first portion of password corresponding to user ID registered to the user information DB(201)(S340).

[89] If the transferred data equals to first portion of password registered to the user in-

formation DB(201), authentication server(200) sends personal identification address corresponding to user ID (or user identification data) to relay server(300)(S350).

[90] More specifically, authentication server(200) sends number of second user terminal(120) or email address stored to user information DB(201) to relay server(300).

[91] If the transferred data does not equal to first portion of password registered to the user information DB(201), authentication server(200) sends authentication failure message to first user terminal and then first user terminal(110) displays the message received from authentication server(200)(S355).

[92] Once relay server(300) receives personal identification address from authentication server(200), it sends a message requesting input of second portion of password to the personal identification address(S360).

[93] For example if relay server(300) receives number of second user terminal(120) from authentication server(200), relay server(300) can send a massage requesting input of second portion of password to second user terminal, using Auto Calling System(ACS).

[94] Depending on user setup, relay server(300) can alternatively send a massage requesting input of second portion of password to second user terminal(120), using Short Message Service(SMS).

[95] Alternatively depending on the user setup, relay server(300) can send a massage requesting input of second portion of password to second user terminal, using call back URL SMS.

[96] Once relay server(300) receives email address registered by user from authentication server(200), it sends a message requesting input of second portion of password to the email address.

[97] In addition, once relay server(300) receives email address registered by user from authentication server(200), it sends a message requesting input of second portion of through messenger for the purpose.

[98] And if user enters numbers(or characters or combination of them) corresponding to second portion of password, second user terminal(120) receives input date for second portion of password(S365).

[99] The second user terminal(120) sends the input data including second portion of password to relay server(300) (S370).

[100] More specifically if second user terminal(120) is called through ACS, user enters numbers(or characters or combination of them) corresponding to second portion of password into second user terminal(120).

[101] In addition, if second user terminal(120) receives a SMS message through SMS server, user enters numbers(or characters or combination of them) corresponding to second portion of password into second user terminal(120).

[102] Additionally if second user terminal(120) receives a SMS message through call back URL SMS server, user enters numbers(or characters or combination of them) corresponding to second portion of password by pressing call button and accessing the wireless internet site. Hence, second user terminal(120) sends numbers(or characters or combination of them) corresponding to second portion of password to relay server(300) through Wireless Application Protocol(WAP) including GSM, TDMA, CDMA and CDPD.

[103] In one embodiment, if a message requesting input of second portion of password is received through email, user enters numbers(or characters or combination of them) corresponding to second portion of password through email.

[104] In addition, if a message requesting input of second portion of password is received through messenger, user enters numbers(or characters or combination of them) corresponding to second portion of password through messenger by accessing messenger with corresponding ID.

[105] Relay server(300) receives second portion of password from second user terminal(120), and sends it to authentication server(200)(S380).

[106] Authentication server(200) receives second portion of password, and combines it with first portion of password(S390). And authentication module(202) compares the combined password with password registered into user information DB(201)(S400).

[107] Depending on the comparison result, authentication server(200) sends success or failure message to first user terminal(110)(S410).

[108] More specifically if the combined password equals to the password registered to authentication server(200), authentication server(200) sends authentication success message to first user terminal(110) or sends authentication failure message to first user terminal(110).

[109] First user terminal(110) displays authentication message received from authentication server(200)(S420).

[110] If authentication success message is received through first user terminal(110), user can use services provided by the site or goes to next sate of authentication process.

[111] Whereas if authentication success message is received through first user terminal(110), user can retry authentication process by entering first portion of password through first user terminal(110).

[112] Although authentication server(200) and relay server(300) is separated from each other according to first embodiment of this invention, it is possible to use only first user terminal, second user terminal and authentication server for the security authentication without relay server(300).

[113] FIG. 4 is a schematic representation of block diagram to illustrate authentication system according to second embodiment of this invention, and FIG. 5 is a schematic

representation of flow chart to illustrate user authentication process according to second embodiment of this invention.

[114] With reference to FIG. 4, authentication system according to second embodiment of this invention includes first user terminal(111), second user terminal(121) and authentication server(210).

[115] In the second embodiment of this invention, the authentication process is same as that of first embodiment except that second user terminal communicates with authentication server(210) directly without relay server.

[116] With reference to FIG. 5, authentication processes of from S510 to S540 is substantially same as those of from S310 to S340 in the first embodiment of this invention mentioned above.

[117] If the received first portion of password equals to first portion of registered password, authentication server(210) sends a message requesting input of second portion of password to second user terminal using registered personal identification address(S550).

[118] More specifically as is the case with first embodiment of this invention, authentication server(210) sends a message requesting input of second portion of password using ACS, SMS, call back URL SMS, email address or messenger, depending on the purpose for the service.

[119] If the transferred data does not equal to first portion of password registered to the user information DB(201), authentication server(200) sends authentication failure message to first user terminal(111) and then first user terminal(111) displays the message received from authentication server(200)(S555).

[120] Once second user terminal(121) receives input request message from authentication server(210), second user terminal(120) receives input data for second portion of password if user enters number(or characters or combination of them) corresponding to second portion of password into the password input field(116)(S560).

[121] The second user terminal(121) sends the input data including second portion of password to authentication server(210) (S565).

[122] Authentication server(210) receives second portion of password, and combines it with first portion of password(S570). And authentication module(212) compares the combined password with password registered into user information DB(211)(S580).

[123] Depending on the comparison result, authentication server(200) sends success or failure message to first user terminal(111)(S590).

[124] The first user terminal(111) displays authentication message received from authentication server(200)(S600).

[125] According to another embodiment of this invention, user terminals rather than two user terminal can be used to authenticate user identification through authentication

server and relay server.

[126] FIG. 6 is a schematic representation of block diagram to illustrate authentication system according to third embodiment of this invention, and FIG. 7 is a schematic representation of flow chart to illustrate user authentication process according to third embodiment of this invention.

[127] With reference to FIG. 6, the security authentication system according to third embodiment of present invention includes user terminal(130), authentication server(220) and relay server(302).

[128] In this case, authentication process is the same as that of first or second embodiments of this invention except one user terminal is comprehensively used instead of first user terminal and second user terminal.

[129] User terminal(130) shown in FIG.6 plays a role of communicating with both authentication server(220) and relay server(302) on DBDM(Double Band Double Mode).

[130] With reference to FIG. 7, authentication processes of from S710 to S755 are substantially same as those of from S310 to S355 in the first embodiment of this invention mentioned above.

[131] Relay server(302) receives personal identification address from authentication server(220) and sends a message requesting input of second portion of password through the personal identification address(S760).

[132] Once user terminal(130) receives input request message from relay server(302), user terminal(130) receives input date for second portion of password if user enters numbers(or characters or combination of them) corresponding to second portion of password(S765).

[133] Then first user terminal(130) sends the input data including second portion of password to relay server(302) (S770).

[134] When a user, for example, uses phone banking or telebanking service through user terminal(130) featuring mobile messenger, the user sends first portion of password to authentication server(220) through user terminal(130).

[135] When user terminal(130) receives a message requesting access to messenger from relay server(302) in this embodiment, user access the mobile messenger by pressing the call button and enters numbers(or characters or combination of them) corresponding to second portion of password.

[136] Accordingly if the user terminal(130) is a mobile phone featuring mobile messenger function, first portion of password is sent to authentication server(220) through wireless communication on user terminal(130) and second portion of password is sent to relay server(302) through wireless internet by accessing it.

[137] In addition, When a user uses home shopping, home banking or online game service through user terminal(130) featuring remote control function, the user enters first

portion of password into IPTV(Internet Protocol Teleivsion)(not shown in the figure) or DTV(Digital Television)(not shown in the figure) using user terminal(130) as a remote controller.

[138] IPTV or DTV is an interactive TV that communicates with authentication server(220), meaning that entered first portion of password is sent to authentication server(220) when they have been set to channel connected to authentication server(220).

[139] When user terminal(130) receives a message requesting access to messenger from relay server(302) in this embodiment, user access the mobile messenger by pressing the call button and enters numbers(or characters or combination of them) corresponding to second portion of password.

[140] Accordingly if the user terminal(130) is a mobile phone featuring remote control function, first portion of password is sent to authentication server(220) through RF communication or internet communication and second portion of password is sent to relay server(302) through wireless internet.

[141] Hence, first portion of password and second portion of password can be sent to authentication server(220) and relay server(302) through separate channels respectively by using user terminal(130) featuring DBDM function.

[142] As well, first portion of password and second portion of password can be sent to authentication server(220) and relay server(302) through separate channels respectively by using user terminal(130) featuring WiBro/WiMax function and CDMA function, or WiBro/WiMax function and WLAN function, or WiBro/WiMax and DMB function.

[143] While third embodiment of this invention describes that one user terminal(130) sends first portion of password and second portion of password to authentication server(220) and relay server(302) through different channels, they can be sent to authentication server(220) and relay server(302) through 1 channel at another embodiment.

[144] When a user, for example, uses phone banking or telebanking service through user terminal(130), the user sends first portion of password to authentication server(220) through user terminal(130).

[145] If first portion of password is matched, user terminal(130) is called from relay server(302) through ACS and user terminal(130) goes to the call waiting status. Here, user can enter numbers(or characters or combination of them) into user terminal(130).

[146] Hence, first portion of password and second portion of password can be sent to authentication server(220) and relay server(302) through one channel respectively by using one user terminal(130) .

[147] Relay server(302) receives second portion of password from user terminal(130), and sends it to authentication server(220)(S780).

[148] Authentication server(220) receives second portion of password, and combines it

with first portion of password(S790). And then authentication module(222) compares the combined password with password registered into user information DB(221)(S800).

[149] Depending on the comparison result, authentication server(220) sends success or failure message to user terminal(130)(S810).

[150] Then user terminal(130) displays authentication message received from authentication server(220)(S820).

[151] According to third embodiment of present invention, user terminal(130) represents wireless mobile handset such as mobile phone and PDA, and personal identification address represents number of user terminal(130) in terms of embodiment that relay server(302) sends a message requesting input of second portion of password to user terminal(130), and first portion and second portion of password are entered through user terminal(130).

[152] While the third embodiment of this invention describes that security authentication is performed through authentications server(220) and relay server(302) by using one user terminal(130), only user terminal(130) and authentication server(220) can be used for the security authentication without relay server(302) at another embodiment.

[153] In addition, password can be divided into three or more portions to enhance the security performance depending on authentication server setup or user setup.

[154] Yet the location which password is divided at is also changeable depending on authentication server setup or user setup.

[155] In addition, First user terminal that first portion of password is entered, and second user terminal that second portion of password is entered are changeable in terms of application order. For example, first portion of password can be requested to be entered into wireless handset or PDA mentioned as second user terminal above, and second portion of password can be requested to be entered into computer desktop mentioned as first user terminal above.

[156] Modifications within the spirit and scope of the invention may readily be effected by persons skilled in the art. It is to be understood, therefore, that this invention is not limited to the particular embodiments described by way of example hereinabove.

Industrial Applicability

[157] The prsent invention is applicable to a security authentication method and system in order to strengthen security performance.

[158]

[159]

Claims

[1] A method of authenticating personal identification, comprising : receiving first portion of password corresponding to user id from first user terminal; sending personal identification address corresponding to the user id to relay server if the received first portion of password equals to first portion of registered password; receiving second portion of the password from the relay server; authenticating the password by combining first portion and second portion of the password.

[2] The method of claim 1, wherein the relay server sends request for input of second portion of the password to the personal identification address, and receives second portion of the password from second user terminal.

[3] The method of claim 2, wherein the personal identification address includes number of the second user terminal or email address registered by user.

[4] The method of claim 3, wherein the first user terminal and the second user terminal are equal device.

[5] The method of claim 4, wherein the first portion of password and second portion of password are received through separate two channels respectively.

[6] The method of claim 5, wherein the second user terminal includes mobile device.

[7] The method of claim 1, including the result of authenticating the password is sent to the first user terminal.

[8] The method of claim 1, wherein the first portion and second portion of the password include numbers or characters for additional services.

[9] A method of authenticating personal identification, comprising : receiving personal identification address corresponding to user id from authentication server that received first portion of password corresponding to the user id; sending request for input of second portion of the password to the personal identification address; receiving second portion of password from user terminal; sending the second portion of the password to the authentication server.

[10] The method of claim 9, wherein request for input of second portion of the password is sent to the user terminal using Automatic calling System(ACS) if the personal identification address is number of the user terminal.

[11] The method of claim 9, wherein request for input of second portion of the password is sent to the user terminal using Short Message Service(SMS) if the personal identification address is number of the user terminal.

[12] The method of claim 9, wherein request for input of second portion of the password is sent to the user terminal using call back URL SMS if the personal identification address is number of the user terminal.

[13] The method of claim 9, wherein request to access the web messenger is sent to

the user terminal if the personal identification address is number of the user terminal.

[14] The method of claim 9, wherein request for input of second portion of the password is sent to the email address or messenger if the personal identification address is the email address.

[15] A method of authenticating personal identification, comprising : receiving first portion of password corresponding to user id from first user terminal; sending request for input of second portion of the password through personal identification address corresponding to the user id if the received first portion of password equals to first portion of registered password; receiving second portion of the password from second user terminal; authenticating the password by combining first portion and second portion of the password.

[16] The method of claim 15, wherein the personal identification address includes number of the second user terminal or email address registered by user.

[17] The method of claim 16, wherein the first user terminal and the second user terminal are equal device.

[18] The method of claim 17, wherein the first portion of password and second portion of password are received through separate two channels respectively.

[19] The method of claim 15, wherein the first portion and second portion of the password include numbers or characters for additional services.

[20] A system for undertaking authentication of personal identification, comprising : authentication server that receives first portion of password corresponding to user id from first user terminal and sends personal identification address corresponding to the user id if the received first portion of password equals to the first portion of registered password; and
relay server that sends request for input of second portion of the password through received personal identification address, receives second portion of the password from second user terminal and sends second portion of the password to the authentication server.

[21] The system of claim 20, wherein the personal identification address includes number of the second user terminal or email address registered by user.

[22] The system of claim 20, wherein the authentication server authenticates the password by combining first portion and second portion of the password, and sends result of the authentication for the password to the first user terminal.

[23] The system of claim 22, wherein the first user terminal and the second user terminal are equal device.

[24] The system of claim 23, wherein the first portion of password and second portion of password are received through separate two channels respectively.

[25] The system of claim 24, wherein the second user terminal is mobile device.

[26] The system of claim 20, wherein the first portion and second portion of the password include numbers or characters for additional services.

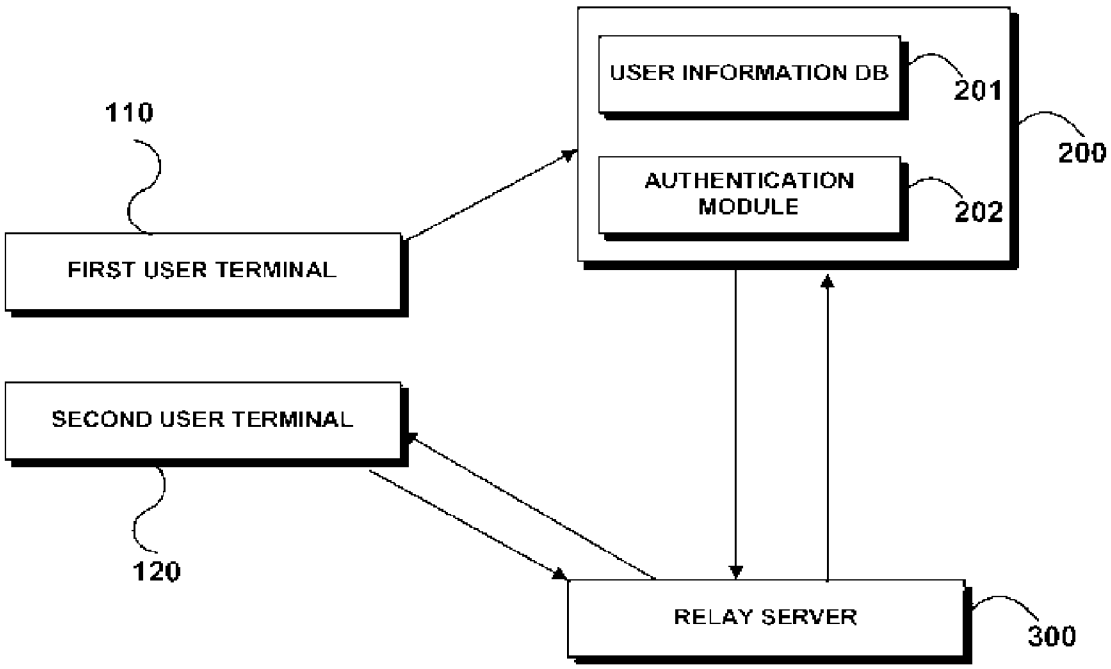
[27] A system for undertaking authentication of personal identification, comprising of authentication server that receives first portion of password corresponding to user id from first user terminal and sends request for input of second portion of the password to personal identification address corresponding to the user id if the received first portion of password equals to the first portion of registered password.

[28] The system of claim 27, wherein the personal identification address includes number of the second user terminal or email address registered by user.

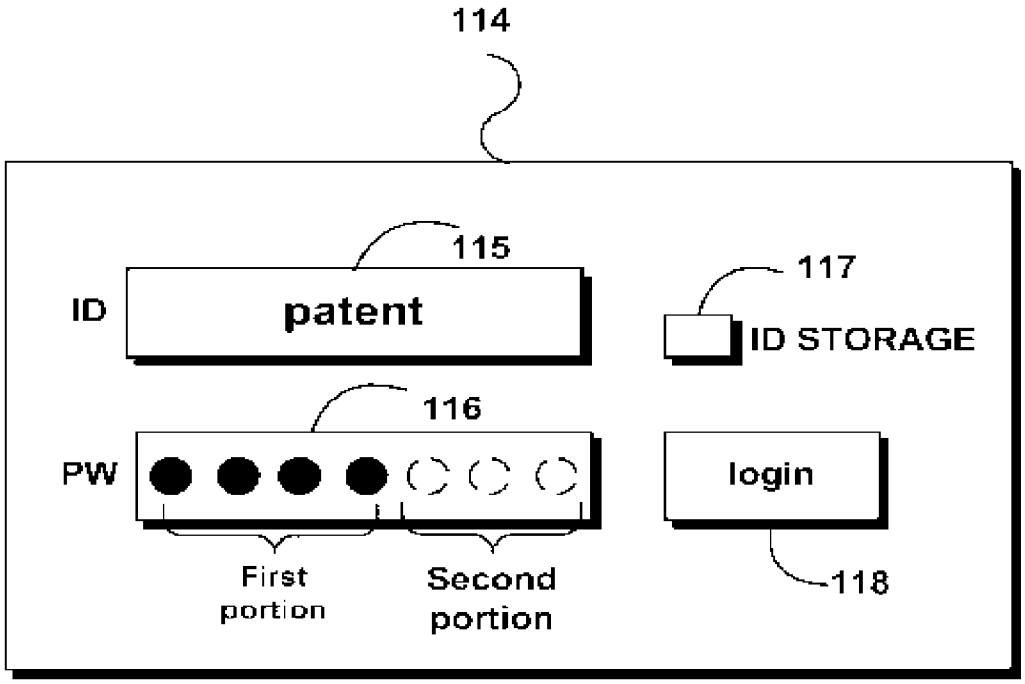
[29] The system of claim 28, wherein the authentication server receives second portion of the password from second user terminal, and authenticates the password by combining first portion and second portion of the password.

[30] The system of claim 29, wherein the authentication server sends the result of authenticating the password to the first user terminal.

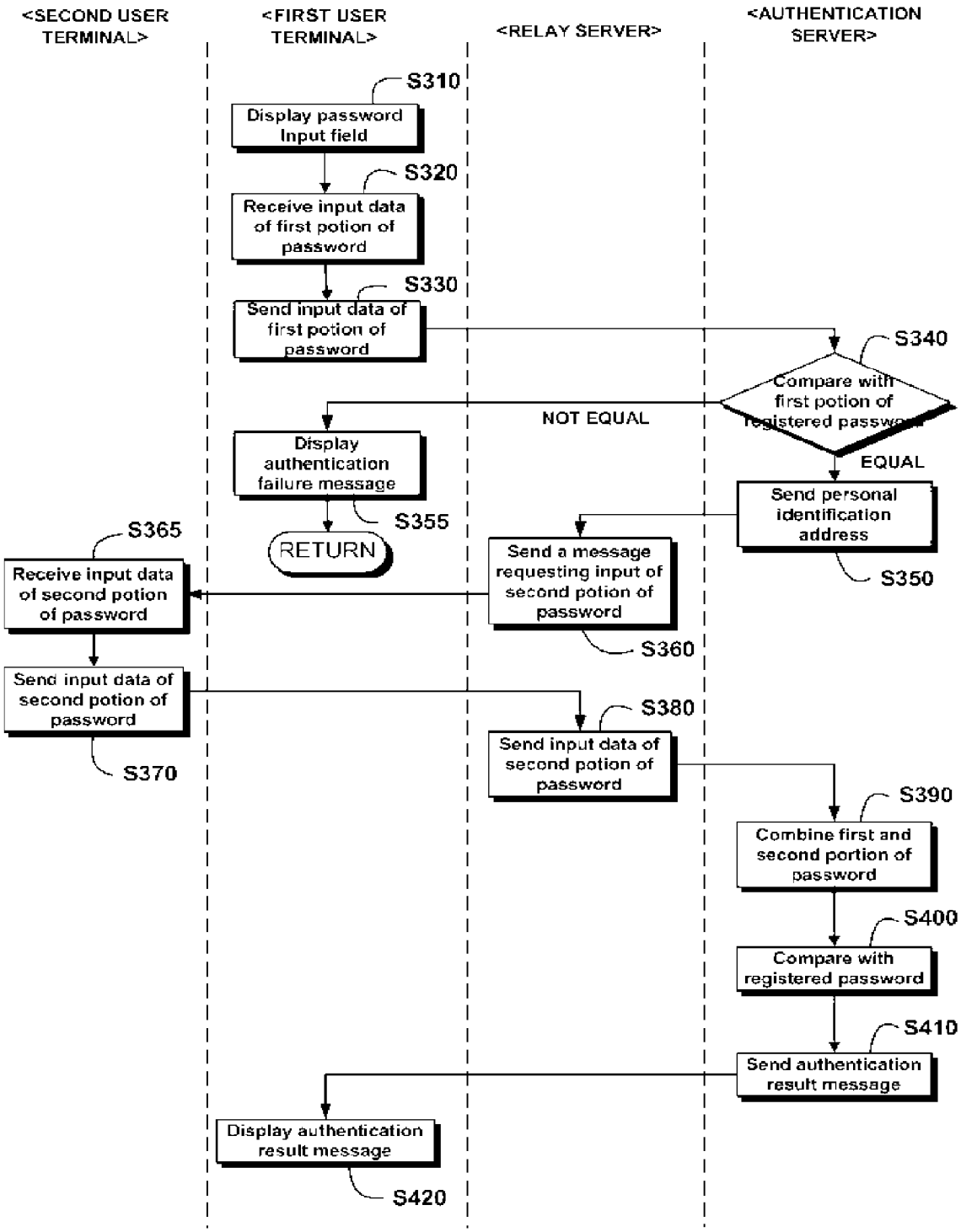
[Fig. 1]


USER INFORMATION DB
201
200
110
AUTHENTICATION MODULE
202
FIRST USER TERMINAL
SECOND USER TERMINAL
120
RELAY SERVER
300

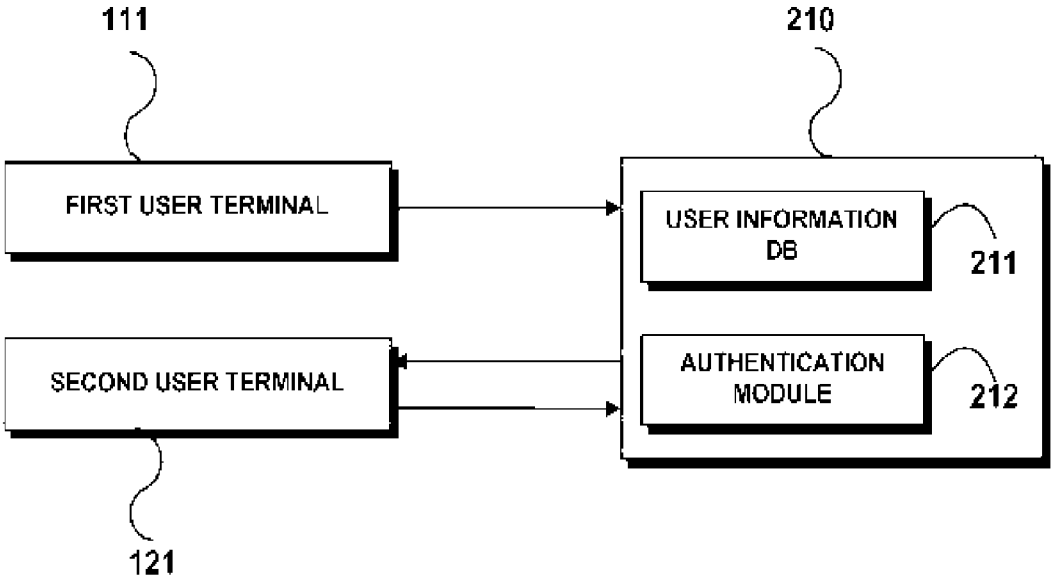
[Fig. 2]


114
115
ID
patent
117
ID STORAGE
116
PW
login
First portion
Second portion
118

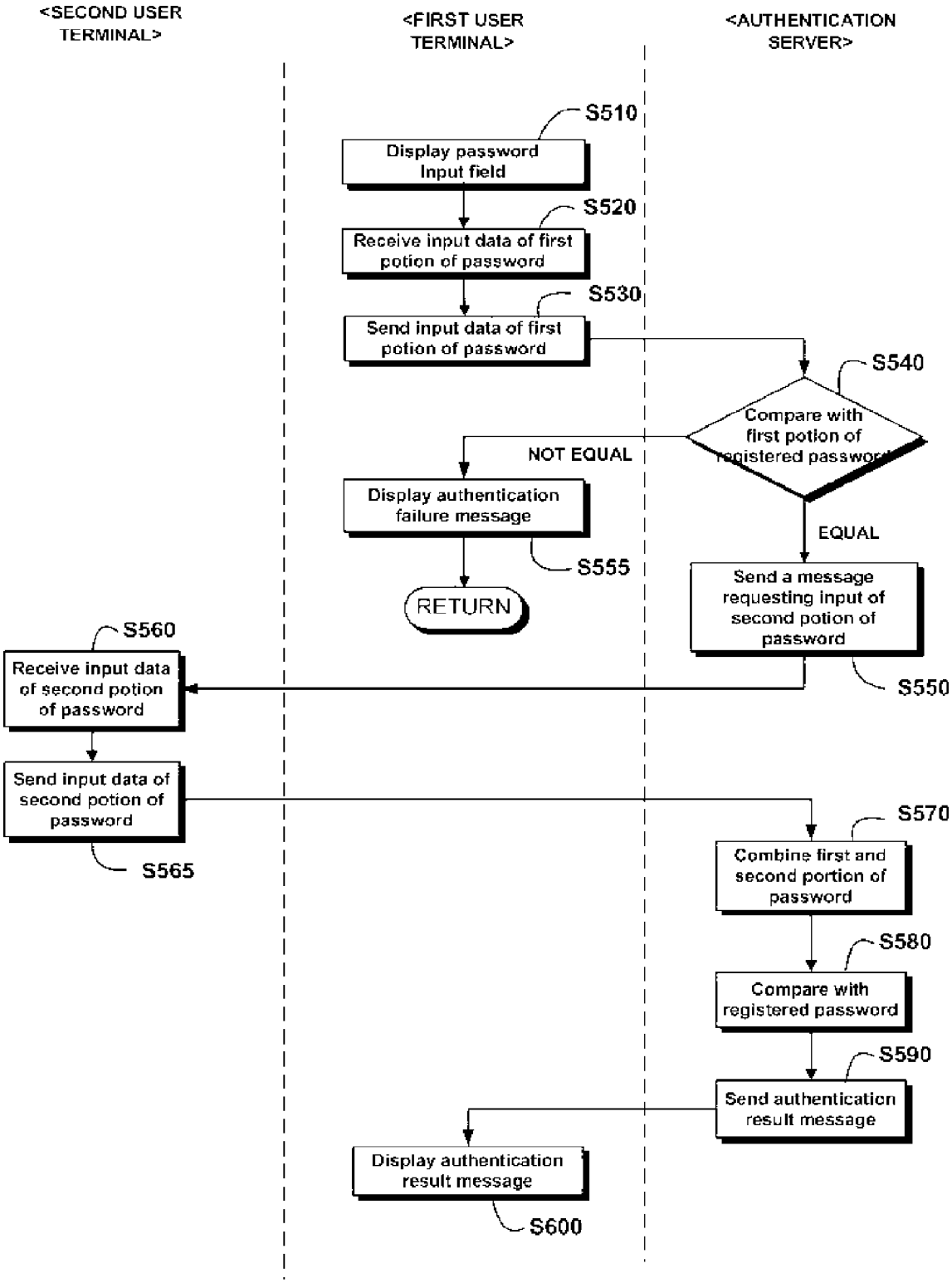
[Fig. 3]


<SECOND USER TERMINAL>
<FIRST USER TERMINAL>
<RELAY SERVER>
<AUTHENTICATION SERVER>
S310
Display password Input field
S320
Receive input data of first potion of password
S330
Send input data of first potion of password
S340
Compare with first potion of registered password
NOT EQUAL
EQUAL
Display authentication failure message
S355
RETURN
Send personal identification address
S350
Send a message requesting input of second potion of password
S360
S365
Receive input data of second potion of password
Send input data of second potion of password
S370
S380
Send input data of second potion of password
S390
Combine first and second portion of password
S400
Compare with registered password
S410
Send authentication result message
Display authentication result message
S420

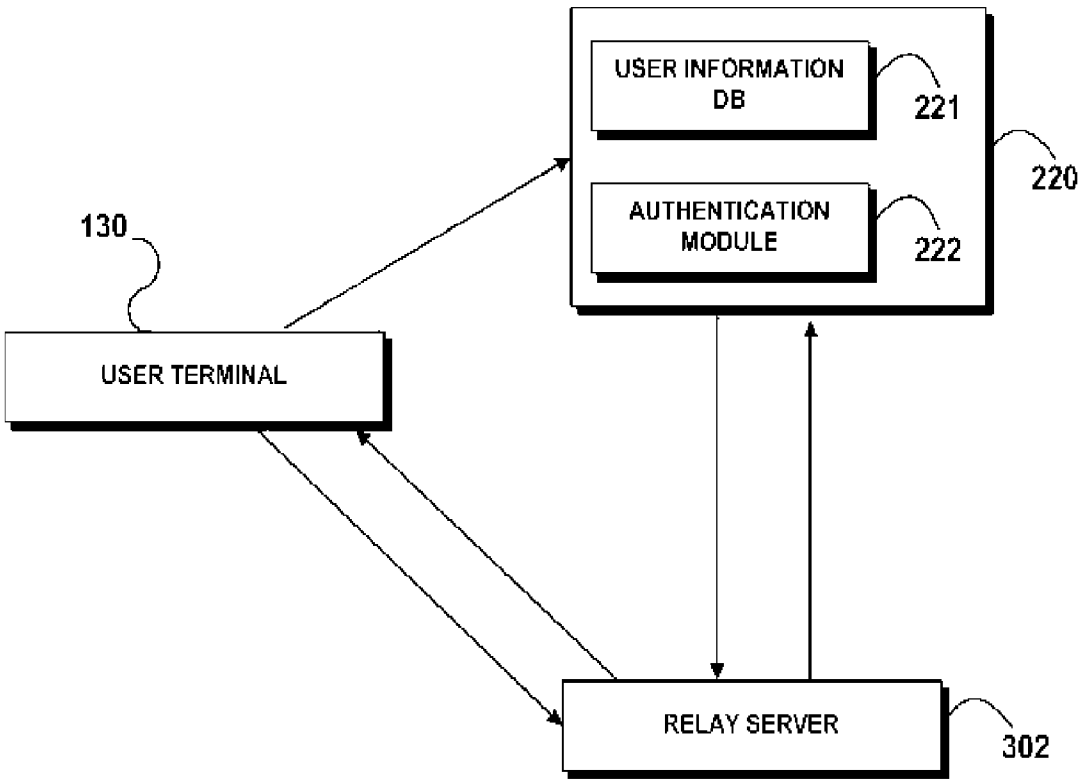
[Fig. 4]


111
210
FIRST USER TERMINAL
USER INFORMATION DB
211
SECOND USER TERMINAL
AUTHENTICATION MODULE
212
121

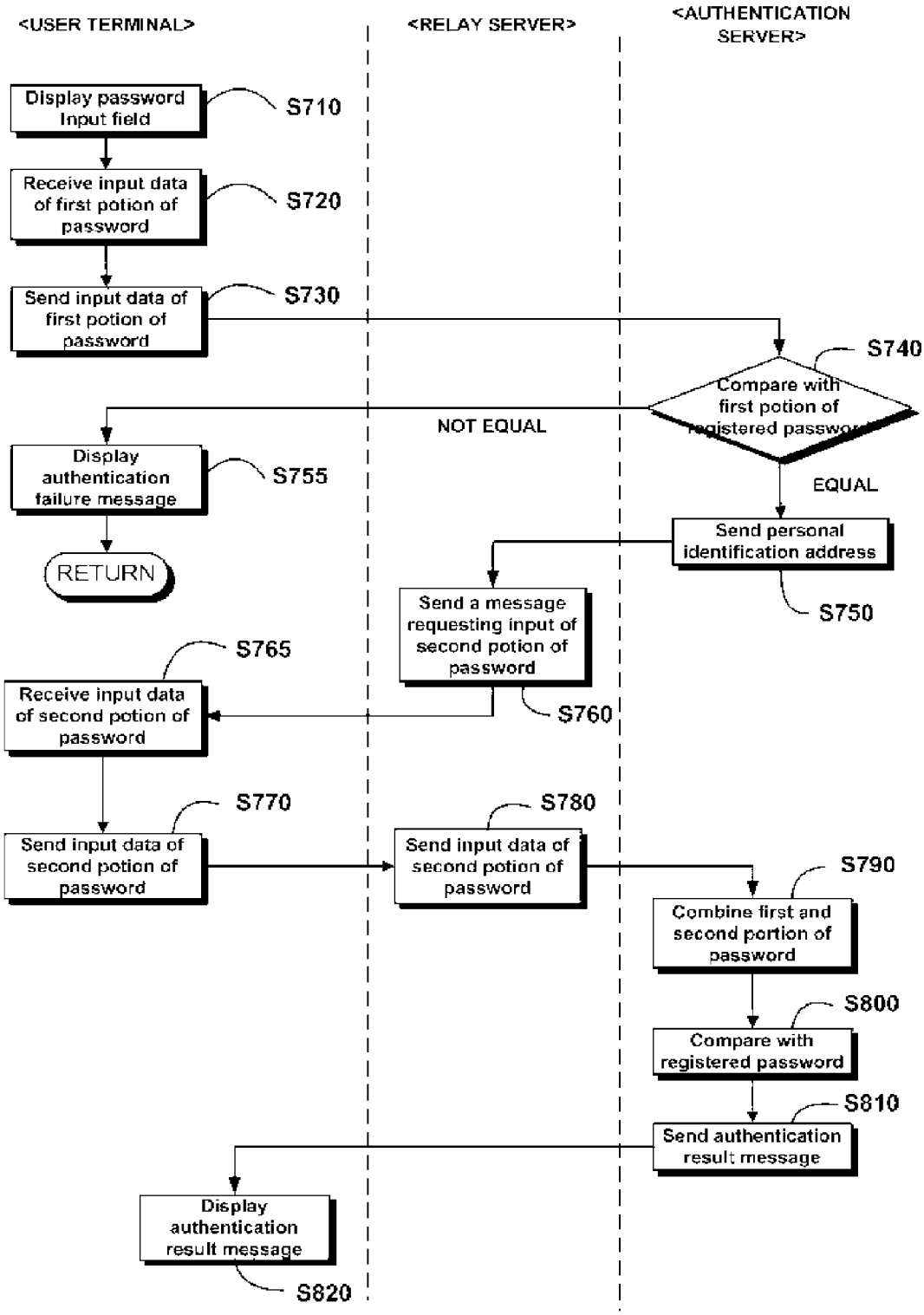
[Fig. 5]


<SECOND USER TERMINAL>
<FIRST USER TERMINAL>
<AUTHENTICATION SERVER>
S510
Display password Input field
S520
Receive input data of first potion of password
S530
Send input data of first potion of password
S540
Compare with first potion of registered password
NOT EQUAL
Display authentication failure message
S555
RETURN
EQUAL
Send a message requesting input of second potion of password
S550
S560
Receive input data of second potion of password
Send input data of second potion of password
S565
S570
Combine first and second portion of password
S580
Compare with registered password
S590
Send authentication result message
Display authentication result message
S600

[Fig. 6]


USER INFORMATION DB
221
220
AUTHENTICATION MODULE
222
130
USER TERMINAL
RELAY SERVER
302

[Fig. 7]


<USER TERMINAL>
<RELAY SERVER>
<AUTHENTICATION SERVER>
Display password Input field
S710
Receive input data of first potion of password
S720
Send input data of first potion of password
S730
S740
Compare with first potion of registered password
NOT EQUAL
EQUAL
Display authentication failure message
S755
RETURN
Send personal identification address
S750
Send a message requesting input of second potion of password
S760
S765
Receive input data of second potion of password
S770
Send input data of second potion of password
S780
Send input data of second potion of password
S790
Combine first and second portion of password
S800
Compare with registered password
S810
Send authentication result message
Display authentication result message
S820

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2007/004983

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i, G06F 17/00(2006.01)i, G06F 15/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 8 G06F 1/, G06F 15/, H04L 9/

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models since 1975

Japanese Utility models and applications for Utility models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKIPASS(KIPO internal) "security, password, first, second, channel"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5881226 A (BRIAN J. VENEKLASE) 9 MAR. 1999 See abstract and figure 1.	1 - 30
A	US 5402492 A (AST RESEARCH INC.) 28 MAR. 1995 See abstract and figure 1.	1 - 30
A	JP 2001-344037 A (SHARP CORP.) 14 DEC. 2001 See abstract and figure 1.	1 - 30
A	JP 2005-070931 A (MASUSHITA ELECTRIC IND. CO., LTD.) 17 MAR. 2005 See abstract and figure 1.	1 - 30

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 JULY 2008 (11.07.2008)	**11 JULY 2008 (11.07.2008)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

MA, Jung Youn

Telephone No. 82-42-481-5679

Form PCT/ISA/210 (second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2007/004983

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5881226 A	09.03.1999	CA 2219344 AA	28.04.1998
		EP 0844551 A2	27.05.1998
		US 2004-054932 A1	18.03.2004
US 5402492 A	28.03.1995	NONE	
JP 2001-344037 A	14.12.2001	NONE	
JP 2005-070931 A	17.03.2005	NONE	