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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 August 2016 (11.08.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/126151 A1

(51) International Patent Classification:
H04L 9/00 (2006.01) *H04W 12/00* (2009.01)
H04L 12/00 (2006.01)

(21) International Application Number:
PCT/MY2016/000006

(22) International Filing Date:
5 February 2016 (05.02.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2015700366 5 February 2015 (05.02.2015) MY

(71) Applicant: **MTOUCHE TECHNOLOGY BERHAD** [MY/MY]; Suite 39-06 Menara Citibank, 165 Jalan Ampang, 50450 Kuala Lumpur (MY).

(72) Inventors: **Kenneth Kong Seh Kiang**; 32A Jalan Awan Biru, Taman Yarl, 58200 Kuala Lumpur (MY). **Janice Ng Dz Yun**; 113, Jalan BRP 7/3, Bukit Rahman Putra, 47000 Sungai Buloh, Selangor (MY). **Leong Yee Ling**; 17, Jalan 92/26, Taman Sri Rampai, Setapak 53300 Kuala Lumpur (MY). **Yang Zhuo**; Blok A, Unit 16-01, Menara Megah Condo, Jalan Kolam Air, Off Jalan Ipoh, 51200 Kuala Lumpur (MY). **Randall Low**; Suite 39-06 Menara Citibank, 165 Jalan Ampang, 50450 Kuala Lumpur (MY). **Melvyn Tan Hong Keat**; 16, Jalan 33/157A, Kemuning Avenue, 40460 Shah Alam, Selangor (MY).

(74) Agent: **MOHAN K.**; A-39-10, Penthouse, Menara UOA Bangsar, No. 5, Jalan Bangsar Utama 1, 59000 Kuala Lumpur (MY).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Continued on next page]

(54) Title: SYSTEM FOR ESTABLISHING SECURE COMMUNICATION BETWEEN MULTIPLE ELECTRONIC COMMUNICATION DEVICES

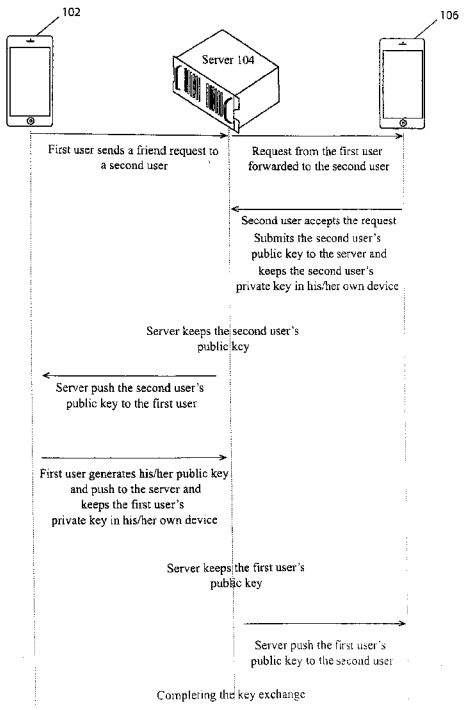

FIG. 4

(57) Abstract: Disclosed system (100) for establishing secure communication between multiple electronic communication devices comprises at least one electronic communication device (102, 106) installed with an application capable of performing an encrypted or decrypted data transfer and a server (104) for establishing a secure connection between the electronic communication devices (102, 106) over a communication network (108). The application allows transferring encrypted or decrypted data including text, multimedia, email, video calls and Voice over IP (VoIP) data through the server (104). The system (100) and the method associated with the application running in the electronic communication devices (102, 106) forms an all-in encrypted or decrypted communication means for text, instant chat, multimedia, email, video calls and VoIP data and allows the user to send and receive encrypted or decrypted messages with self-destruct function. The application prevents hackers and intruders to decrypt the contents of the data send through the application, even if they gain access to the server (104).

WO 2016/126151 A1

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

SYSTEM FOR ESTABLISHING SECURE COMMUNICATION BETWEEN MULTIPLE ELECTRONIC COMMUNICATION DEVICES

FIELD OF INVENTION

The present invention relates to a system for secure multimode communication. More particularly, the present invention relates to a software messaging system for secure multimode communication between multiple electronic communication devices.

BACKGROUND

Users of electronic communication devices increasingly desire to communicate privately and securely with one another. The communication means for communicating with two or multiple users includes text messaging, instant chat, etc. The present systems and methods uses different applications installed on the electronic communication devices for handling one or more communication methods such as text messaging, instant chat, etc. Unfortunately, there is no single application that can handle all forms of communication over an encrypted channel for securing communications. Also the existing systems have difficulties when a sender of a communication intends for the communication to be received by multiple entities over an encrypted channel.

Electronic mail (email), short message service (SMS, or text), instant chats, email, voice communication by voice over IP means, video calling, group video chat and so forth (collectively, "electronic communication") are now common and perhaps indispensable methods of communication. These tools are used for both personal communication and business communication. Many applications exists that offer secured mode of communication between two or more devices. It is commonly believed that the content of such communications through these applications are relatively secure and private. However, in many circumstances, an expectation of security and privacy is not well founded. The applications for such communications offer a limited number of communication methods such as text messaging or instant chat and are relatively easy to intercept. The communication service providers often provide archiving of messages and instant chats that may be accessed,

easily or with varying degrees of effort and authority. Communications are often retained, at least temporarily, on a user's hardware device, such as a cellular telephone, tablet computer, and so on. Therefore, a misplaced or stolen device may give others access to communications retained thereon.

In another approach, the sender encrypts a message using a key. The receiver has a corresponding key, which is used to decrypt the message when received. There are many variations of this encryption-decryption scheme, such as private keys, public key exchange, and so on. Problems with the encryption-decryption approach include the need for processing resources to perform the encryption-decryption on the sending and receiving devices, and the risk of loss of security of the key or the device that performs the encryption-decryption. Furthermore, encryption usually converts a human-readable message into a jumble of numbers and letters that is not readable other than after decoding. However, the jumble of letters and numbers then appears to be just what it is an encrypted message. An unauthorized user can therefore quickly identify the message as being encrypted, and hence a target for efforts at decryption, coerced or otherwise.

Another technique for lending security to electronic communication is to permit communication only between pre-authorized devices. In certain versions of such schemes, a message contains code that prevents it from being delivered to, opened by or read on a machine other than one identified in that code. In other versions, limiting access to a network carrying the electronic communications only to approved devices ensures security. There are many other access-limiting schemes for enabling secure communication. However, problems with these approaches in general include the potential inability or difficulty to include new users in a communication, the need to expose a user's device id when sending or receiving a message, and since the message may in fact be encoded until the authenticity of the receiving device is confirmed, the presence of an encoded message may be apparent, identifying it as a target for decryption efforts.

There exist separate applications for sending email, video chat and instant text chat over a communication channel using many techniques for improving the level of security and

privacy in electronic communication. One method employs encrypting the messages send through an application. Encryption offers fair level of security to the contents. These communications may be difficult to be intercepted in transit. However, the existing applications only allow one or two communication methods such as instant text chat and multimedia messaging for sending in an encrypted format.

Users sometimes use the user's electronic communication device to place voice calls, place video calls, VoIP calls, group video chat, instant chats, emails or to send messages to other user devices. There exists a need for a system and method for communicating a user device with devices owned by one more users for transferring voice calls, video calls, VoIP calls, group video chat, instant chats, emails and messages. The needed system and method would send and receive the information over a secured communication channel. In addition, the information would be encrypted before transferring. Further, the needed system and method would employ a single application to transfer place voice calls, place video calls, VoIP calls, group video chat, instant chats, emails and to send messages to other user devices. In addition, the needed system would allow the data to be encrypted for preventing hacking, thereby protecting potentially sensitive and private information. The present invention addresses such a need.

SUMMARY

The present disclosure is directed to systems and methods for providing secure electronic communications from one device to another that is both secure, in the sense of encryption, and protected, in the sense that third parties cannot access the contents of the secure message. The present invention is a system for establishing secure communication between multiple electronic communication devices. The system comprises a first electronic communication device installed with an application capable of performing an encrypted or decrypted data transfer, at least one second electronic communication device installed with the application capable of performing an encrypted or decrypted data transfer, at least one server capable of establishing a secure connection between the first electronic communication device and the second electronic communication device for transferring at least one encrypted or decrypted data. The application installed in the first electronic communication device and the second

electronic communication device is capable of transferring encrypted or decrypted data including text, multimedia, email, video calls and Voice over IP (VoIP) data through the at least one server. A communication network transfers the encrypted or decrypted text, multimedia, email and VoIP data from the application running in the first electronic communication device to the at least one second electronic communication device through the at least one server.

The system offers multiple modes of security layers by introducing AES256 military-grade encryption algorithm, RSA (1024bit) for key exchange, Hash (SHA256) for unique message signature and transferring the encrypted or decrypted data via Secure Socket Layer (SSL). The system and the method associated with the application running in the electronic communication device forms an all-in communication application that allows the user to send and receive encrypted or decrypted messages with self-destruct function. The application running in the electronic communication devices allows the users to send and receive chats with encryption, email with encryption, encrypted or decrypted VoIP, encrypted or decrypted video calls, etc. Thereby the text, multimedia, email, video calls and Voice over IP (VoIP) information can be securely transferred between the two or more electronic communication devices using a single application and it would be difficult for the hackers and intruders to decrypt the contents of the messages, even if they gain access to the server. The user can send the data even if the second electronic communication device kept in an offline mode. In that case the server forms a central repository to store the data and synchronizes the data stored in the central repository with the application running in the at least one second electronic communication device when the device comes online.

Other objects and advantages of the embodiments herein will become readily apparent from the following detailed description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTIONS OF THE DRAWINGS

FIG. 1 illustrates the system for establishing a secure communication for transferring data including text, multimedia, email, video calls and Voice over IP (VoIP) data between a first

electronic communication device and at least one second electronic communication device, according to a preferred embodiment of the present invention.

FIG. 2 illustrates a block diagram of the electronic communication device for sending and receiving data including text, multimedia, email, video calls and Voice over IP (VoIP) data, according to a preferred embodiment of the present invention.

FIG. 3 illustrates a block diagram of an authentication server of the system for establishing a secure communication for transferring data, according to a preferred embodiment of the present invention.

FIG. 4 illustrates a diagram showing a general process of authorizing a user for establishing secure communication between a pair of electronic communication devices.

FIG. 5A illustrates a diagram showing a one-time process of secure key registration for authorizing at least one user to establish secure communication using the application installed in his/her electronic communication device.

FIG. 5B to **5C** illustrates a diagram showing a process of secure key exchange for authorizing at least one user to establish secure communication between a pair of electronic communication devices, according to a preferred embodiment of the present invention.

FIG. 6 illustrates a diagram showing a process of establishing secure chat communication with encryption between a pair of electronic communication devices of a first user and second user alone.

FIG. 7 is a flowchart describing the complete message generation when the first user sends a message to the second user.

FIG. 8 is a flowchart describing the complete message decryption when the second user receives a message from the first user.

FIG. 9A to **9C** illustrates a diagram showing a process of secure key exchange for authorizing multiple users to establish secure communication between a pair of electronic communication devices in a group chat using the present application installed in the electronic devices, according to a preferred embodiment of the present invention.

FIG. 10A illustrates a diagram showing a process of sending a message between a pair of electronic communication devices in a group chat using the present application installed in the electronic devices, according to a preferred embodiment of the present invention.

FIG. 10B illustrates a diagram showing a process of receiving and decrypting a message using an electronic communication device in a group chat using the present application installed in the electronic device according to a preferred embodiment of the present invention.

FIG. 11A illustrates a diagram showing a process of sending an email using the present application installed in the electronic device according to a preferred embodiment of the present invention.

FIG. 11B illustrates a diagram showing a process of receiving an email using the present application installed in the electronic communication device, according to a preferred embodiment of the present invention.

FIG. 12 illustrates an architecture diagram for electronic communication device installed with the mobile application capable of transferring data including text, multimedia, email, video calls and Voice over IP (VoIP) data between the first electronic communication device and the second electronic communication device, according to a preferred embodiment of the present invention.

FIG. 13 illustrates an architecture diagram for the server capable of establishing a secure connection for transferring data including text, multimedia, email, video calls and Voice over IP (VoIP) data between mobile applications installed in the first electronic communication

device and the second electronic communication device, according to a preferred embodiment of the present invention.

DETAILED DESCRIPTION

In the following detailed description, a reference is made to the accompanying drawings that form a part hereof, and in which the specific embodiments that may be practiced is shown by way of illustration. These embodiments are described in sufficient detail to enable those skilled in the art to practice the embodiments and it is to be understood that the logical, architectural and other changes may be made without departing from the scope of the embodiments. The following detailed description is therefore not to be taken in a limiting sense.

In this document, the terms "a" or "an" are used, as is common in patent documents, to include one or more than one. In this document, the term "or" is used to refer to a nonexclusive "or," such that "A or B" includes "A but not B," "B but not A," and "A and B," unless otherwise indicated. Furthermore, all publications, patents, and patent documents referred to in this document are incorporated by reference herein in their entirety, as though individually incorporated by reference. In the event of inconsistent usages between this document and those documents so incorporated by reference, the usage in the incorporated reference(s) should be considered supplementary to that of this document; for irreconcilable inconsistencies, the usage in this document controls.

The description provided herein is complete and sufficient for those skilled in the arts of computer systems, software application development, mobile application development and web development to implement the methods as described. One embodiment of this system for establishing secure communication between multiple electronic communication devices may employ a server running an operating system such as Windows, Linux, web-server software such as Apache, and database such as MySQL, with methods implemented through a software development language such as PHP or Java. However, the invention should not be limited to

these types of software operating system, web-server software, database software, software development language, server or client hardware.

The present invention provides a system for transferring data by enabling efficient secure authentication between various portable communication devices. The present invention overcomes inadequacies of the prior art by creating a novel architecture for secured transfer of multiple forms of data including, but not limited to, text, instant chat, multimedia, email, video calls and Voice over IP (VoIP) data using a single messaging facility in form of messages. The present invention sends the plurality of information including, but not limited to, text, instant chat, multimedia, email, video calls and Voice over IP (VoIP) data in form of encrypted formats, thereby improving the security of the information transferred between multiple portable electronic communication devices. However, the methods and system provided herein are also capable of transferring data in decrypted format.

The present invention is a system (100) for establishing secure communication between multiple electronic communication devices. According to a preferred embodiment, the system (100) disclosed in the present inventions is used for establishing a secure communication for transferring data including text, multimedia, email, video calls and Voice over IP (VoIP) data between applications running in the multiple electronic communication devices over a wireless communication network. The data to be transferred may be in encrypted or decrypted format. **FIG. 1** illustrates the system (100) for establishing a secure communication for transferring encrypted data including text, multimedia, email, video calls and Voice over IP (VoIP) data between a first electronic communication device (102) and at least one second communication device (106), according to a preferred embodiment of the present invention. In one embodiment, the system (100) transfers decrypted data between the first communication device (102) and the second (106) communication device. The system (100) includes the first electronic communication device (102) installed with an application capable of performing an encrypted or decrypted data transfer, at least one second electronic communication device (106) installed with the application capable of performing an encrypted or decrypted data transfer and at least one server (104) capable of establishing a secure connection between the first electronic communication device (102) and the at least one second electronic

communication device (106) for transferring at least one encrypted or decrypted data over a communication network (108). The application installed in the first electronic communication device (102) and the at least one second electronic communication device (106) is capable of performing encrypted or decrypted data transfer of information such as, but not limited to, text, multimedia, email, video calls and Voice over IP (VoIP) data through the server (104). The communication network (108) for transferring encrypted or decrypted text, multimedia, email and VoIP data from the application running in the first electronic communication device (102) to the at least one second electronic communication device (106) can be a wireless communication network such as but not limited to, cellular communication, Wi-Fi etc.

Before describing aspects of the present invention in detail, it is helpful to first discuss the environment in which embodiments of the invention operate. Referring now to **FIG. 2**, the electronic communication device (102, 106) such as, but not limited to, a Smartphone, tablet, ultrabook, laptop, smart wearable device including Google Glass, Smartwatch etc., runs a number of applications including the mobile application for transferring encrypted or decrypted data including text, multimedia, email, video calls and Voice over IP (VoIP) data. The electronic communication device (102, 106) comprises the at least one processing unit (200) that is equipped with a control unit (206) and an Arithmetic Logic Unit (ALU) (208), a memory unit (210), a storage unit (212), a plurality of networking devices (214) and a plurality input/output (I/O) devices (204). The electronic communication device (102, 106) can be composed of multiple homogeneous and/or heterogeneous cores, multiple CPUs of different kinds, special media and other accelerators. The processing unit (200) may also include a memory that stores data. The processing unit (200) might include only one of a type of component e.g. one microprocessor, or may contain multiple components of that type e.g. multiple microprocessors. The processing unit (200) could be composed of a plurality of separate circuits and discrete circuit elements. In some embodiments, the processing unit (200) will essentially comprise solid-state electronic components such as a microprocessor e.g. microcontroller. The processing unit (200) may be mounted on a single board in a single location or may be spread throughout multiple locations, which cooperate to act as processing unit (200). In some embodiments, the processing unit (200) may be located in a single location e.g. in proximity and/or on a common circuit carrying element such as a circuit board and/or

all the components of the processing unit (200) will be closely connected. The mobile application has an encryption module and an algorithm for encrypting the input data including text, multimedia, email, video calls and Voice over IP (VoIP) data. The processing unit (200) is responsible for processing the instructions of the algorithm. The processing unit (200) receives commands from the control unit (206) in order to perform its processing. Further, the plurality of processing units (200) may be located on a single chip or over multiple chips. In addition, any logical and arithmetic operations involved in the execution of the instructions are computed with the help of the ALU (208).

Further, the electronic communication device (102, 106) includes a variety of hardware and associated software components, where the variety of hardware components include the at least one processing unit (200) designed to control various other circuits such as information displayed on a display (202). The display (202) can display the user interface of the mobile application with options for selecting a desired service such as instant chat, text messaging, multimedia, email, video calls and Voice over IP (VoIP). The display (202) may be a touch screen display allowing the plurality of users to control the user interface of the mobile application using at least one gesture or touch. The processing unit (200) may control the information based on inputs received from various input/output (I/O) devices (204) of the electronic communication device (102, 106) e.g. hard keys, a touch screen, voice commands from a microphone or a microphone connected to headset jack, camera and/or from some other user input device. The mobile application has the capability to launch the at least one camera module of the device for sending encrypted or decrypted data including multimedia messages, images or video through instant chat and for making video calls and Voice over IP (VoIP) call.

The mobile application installed in the electronic communication device (102, 106) allows the plurality of users to login to send or receive an encrypted or decrypted data including instant chat text, multimedia, email, video calls and Voice over IP (VoIP) data through a user interface. The processing unit (200) processes the text, multimedia, email, video calls and Voice over IP (VoIP) data inputs received from the first electronic communication device (102), encrypts the information and transfers the information to the server (104). The server

(104) authenticates the receiver device and the encrypted or decrypted data is forwarded the second electronic communication device (106). In an embodiment of the present invention, the at least one processing unit (200) is configured to process a plurality of instructions received from the server (104). The server (104) can act as a central repository for receiving and storing the encrypted or decrypted data. The mobile application allows the users to submit a plurality of information in form of text, instant chat, multimedia, email, video calls and Voice over IP (VoIP) data through the user interface and the data is encrypted or decrypted by the application before sending to the at least one second electronic communication device (106) through the server (104).

FIG. 3 illustrates a block diagram of an authentication server (104) of the system (100) for user authentication and for establishing a secure communication for transferring encrypted or decrypted data including text, instant chat, multimedia, email, video calls and Voice over IP (VoIP) data, according to a preferred embodiment of the present invention. The server (104) runs an application for user authentication and for transferring the encrypted or decrypted data to the second user or users, in case of a group chat, group messaging, group call and video call. The electronic communication devices (102), (106) used to access the server (104) provides the network-based and other features discussed below, uses one or multiple applications. Such access may be by way of a computer network or communication networks (108), such as the network of networks commonly known as the Internet. In some cases, the communication network (108) includes a local and/or wide area network or mobile communication network. In other instances, the communication network (108) may be a local area network (LAN) of an enterprise and/or a virtual LAN, which is instantiated over the Internet or other networks of networks. The server (104) is communicatively coupled to a database, which may store records concerning user credentials.

The server (104) includes similar hardware as in a computer system, which includes the processing unit (306), a network communication unit (314), at least one memory unit (304), a storage unit (308) and a plurality of I/O devices (320) for connecting to a plurality of peripheral devices including a display unit. The server (104) is run by operating system software, Firmware and includes an application for user authentication (310) and transferring

of encrypted or decrypted data including text, instant chat, multimedia, email, video calls and Voice over IP (VoIP) data from the mobile application running in the electronic communication devices (102, 106). The processing unit (306) processes the instructions (312) of the application for user authentication (310) for establishing secure communication between the first electronic device (102) and one or more second electronic devices (106).

The system (100) and the method associated with the application running in the electronic communication device (102, 106) can be employed to send encrypted or decrypted messages, instant chats, email, video and voice over IP calls from the devices through the server (104). In addition, the application forms an all-in communication application that allows the user to send and receive encrypted or decrypted messages with self-destruct function. The application running in the electronic communication devices (102, 106) allows the users to send and receive chats with encryption, email with encryption, encrypted or decrypted VoIP, encrypted or decrypted video calls, etc. Thus the information can be securely transferred between the two or more electronic communication devices (102), (106) and it would be difficult for the hackers and intruders to decrypt the contents of the messages, even if he or she gains access to the server (104) or the sending and receiving electronic communication devices (102, 106).

The system (100) offers multiple modes of security layers by introducing AES256 military-grade encryption algorithm, RSA (1024bit) for key exchange, Hash (SHA256) for unique message signature and transferring the encrypted or decrypted data via Secure Socket Layer (SSL). The encryption offered by the system (100) includes the process of encoding a message including text, instant chat, multimedia, email, video calls and Voice over IP (VoIP) data that can only be decrypted by the authorized receiving device (106). **FIG. 4** illustrates a diagram showing a general process of authorizing a user for establishing secure communication between a pair of electronic communication devices (102, 106). A first user sends a request for establishing a connection with a second user. The request is send from the mobile application running in the first electronic communication device (102) of the first user. The server (104) receives the request and forwards the request to the second user as a notification. Upon receiving the notification, the second user launches the secure communication application

installed in the device (106) and accepts the request. When the second user accepts the request, the secure communication application running the device (106) instructs to submit the device's (106) public key to the server (104) and a private key corresponding to the generated public key will be stored in the device (106). The server (104) now receives the public key send from the device (106) of the second user. The server (104) keeps the second user's device (106) public key and push forward the public key to the first user's device (102). After receiving the public key of the second electronic communication device (106), the first electronic communication device (106) automatically generates its own public key and pushes it to the server (104). At the same time a private key corresponding to the generated public key will be stored in the first electronic communication device (106). The server (104) keeps the first user's device (102) public key and pushes the same public key to the second electronic communication device (106). This completes a key exchange for establishing secure communication connection between the electronic communication device (102) of the first user and the electronic communication device (106) of the second user.

FIG. 5A illustrates a diagram showing a one-time process of secure key registration for authorizing at least one user to establish secure communication using the application installed in his/her electronic communication device. The electronic communication device (102) of the first user generates three sets of RSA keys, and only the public key is send to the server (104). The server (104) receives and acknowledges back to the first electronic communication device (102) that the RSA public key has received. This secure key registration process is performed only one time i.e. when the application is launched for the first time from the electronic communication devices (102) or (106) and register the user to the server (104). **FIG. 5B** to **5C** illustrates a diagram showing a process of secure key exchange for authorizing users to establish secure communication between a pair of electronic communication devices (102, 106). **FIG. 5B** illustrates a diagram showing a process of first part of secure key exchange for authorizing at least one user to establish secure communication. When the first user sends a friend request to a second user from the mobile application running in the first electronic communication device (102), the following process is performed in the background for a secure key exchange. First the first user sends an http request of "addIdentity" to the server (104). Upon receiving the http request, the server (104) generates and returns RSA encrypted

data. In an embodiment, the server (104) generates and returns decrypted data. Then the first user device (102) decrypts the first layer of encryption using first user's RSA Private key and then the first user sends over the decrypted content via Extensible Messaging and Presence Protocol (XMPP) to the second user.

The second user receives the content and approves the request by selecting "Approved" and the second user sends an "Identity check" http request back to the server (104) as shown in **FIG. 5C**. The server (104) then generates the Hash of first user's Public key 2 and second user's Public Key 2 and returns the result to the second user. Then the second user verifies that both the hash value from the server (104) and that from the first user are identical. Then the second user stores the first user's RSA public key 3 (Pub3A). The second user decrypts the content obtained in the last step of **FIG. 5B** using the second user's RSA Private Key 2 and compares the Hash value. Upon successful verification, the second user will send http request "Identity Approve" to the server (104). After the server (104) is verified, it generates and returns the RSA encrypted data to the second user. In an embodiment, the server (104) generates and returns decrypted data to the second user. In case, the encrypted data is generated and returned to the second user, the second user decrypts the first layer of encryption using second user's RSA Private key 2. Then the second user sends over the decrypted content via xmpp to the first user followed by the second user will send an http request "Identity Approve". Upon successful verification, the server (104) will respond acknowledgement. Now the first user will store the second user's RSA public key 3 (Pub3B) and thereby establishes a secure connection between the devices (102, 106) of first user and second user.

FIG. 6 describes the message component and the breakdown. The first user sends the information using the application installed in his device (102). The format of encrypted message includes CipherMessage and CipherInfo ensuring a completely encrypted message. Here the format of CipherMessage includes PublicKey of second user (AesKey) + Aes(PlainMessage), which forms the encrypted content of the message. The format of CipherInfo includes CipherIdentity and version, which forms the info of the message. The info is used for message verification and also for versioning. The format of CipherIdentity includes

PrivateKey of first user (Hash of (PlainMessage) + OwnJid), which is the identity of the message and is used for message verification.

FIG. 7 describes the complete message generation when the first user sends a message to the second user. The first user launches the application from his or her device then inputs plain message and sends to the second user. A random Aes - 256bits Key is now generated. The generated Aes Key is used to encrypt the plain message. Now, the second user's Public 1 Key (Pub1B) and the key version are obtained via http request or from local storage. The Aes Key generated in step 2, i.e. while sending the plain message, is encrypted using Pub1B. Then the plain message is hashed using SHA-256. The hash result is combined with the first user's Jid and the resulting output is encrypted with the first user's Public Key 3. The results comprising the hash result with the first user's Jid that then encrypted with the first user's Public Key 3, encrypted Aes Key using Pub1B, and key version from second user's Public 1 Key (Pub1B) obtaining step is combined to get the encrypted message.

FIG. 8 describes the complete message decryption process when the second user receives a message from the first user. The process starts when the second user receive message from the first user. In step 1 the second user receives the complete encrypted message from the first user. Then in step 2, the second user decrypt the Pub1B (Aes Key) using the second user's RSA Private key 1. In a 3rd step, the second user decrypt Aes (Plain Message) using key obtained from step 2. Now the second user will get the plain message in step 4. But the second user still has other steps to verify the received message. In a 5th step, the second user will generate the Hash of Plain Message using SHA-256. In a following 6th step, the second user verifies the Pub1Bs Key version with key stored locally. Then in step 7, the second user decrypt Pri3A(SHA(PlainMessage) + first user's Jid) using the first user's Public Key 3 obtained during key exchange. From the decrypted data in step 7, the second user verifies the first user's JID. From the decrypted data in step 7, the second user verifies the SHA(Plain Message) with the Hash generated in step 5. Successful completion of the above steps allows the second user to accept the plain message send by the first user.

FIG. 9A to **9C** illustrates a diagram showing a process of secure key exchange for authorizing multiple users to establish secure communication between a pair of electronic communication devices in a group chat using the present application installed in the electronic devices (102, 106) according to a preferred embodiment of the present invention. **FIG. 9A** illustrates a diagram showing a process of secure key generation while creating the group. When the first user create a group with the second user, the first user sends a request to server (104) to get the second user's latest Public key 1. The server (104) returns the second user's latest Public Key 1 (Pub1B). Now the first user generates a random AesKey and encrypts the key with the first user's Public Key 1 and second user's Public Key 1 separately. Both the key will be uploaded to server (104). The server (104) responds by acknowledgement and the group key version.

FIG. 9B illustrates a diagram showing a process of secure key generation while the group admin adding new member into the existing group. The first user, who being the admin of the group, sends request to the server (104) to get the new user's latest Public key 1. The server (104) returns the new user's latest Public Key 1 (Pub1C). Now the first user generate a new random aesKey and encrypts the key with the first user's Public Key 1, and the second user's Public Key 1 and the new user's Public Key 1 separately. The entire keys will be uploaded to the server (104). Upon receiving all the keys, the server (104) responses with acknowledgement and the new group key version.

FIG. 9C illustrates a diagram showing a process of secure key generation while the group admin removes a member from the existing group. The first user, who being the admin of the group, can remove a member whenever desired. The first user generates a new random aesKey and encrypts the key with the first user's Public Key 1 and the second user's Public Key 1 separately. The entire keys will be uploaded to the server (104). The server (104) responds with acknowledgement and the new group key version.

FIG. 10A illustrates a diagram showing a process of sending a message between a pair of electronic communication devices in a group chat using the present application installed in the electronic devices (102, 106) according to a preferred embodiment of the present invention. The following steps are performed when the first user sends a message to the group. The first

user inputs the plain message and select send from the application installed in the electronic device (102). The group Aes key will be obtained either from local DB or from the server (104). The group Key version is obtained from the local DB. The plain message is encrypted with Aes Key obtained in the second step and combined with group key version from the third step. Thus the Aes encryption is performed and the encrypted message includes the Plain message, Aes Key provided with the group key version.

FIG. 10B illustrates a diagram showing a process of receiving and decrypting a message using an electronic communication device in a group chat using the present application installed in the electronic device (102, 106) according to a preferred embodiment of the present invention. The process with the following steps is preformed when the second user receives the group message. In a first step the second user obtains the encrypted message. Now in a second step, the second user verified the Group key version with the key stored in local DB. If the key is different then the second user detects a different Group Key version and sends request to the server (104), which is step 3. The second user decrypt Pub1B(AesKey) to get the group Key. In step 2, if the Group key version with the key stored in local DB is same, then the second user obtain the group key either from step 3 or direct from local DB, which is step 4. The second user will now decrypt the encrypted message in step 1 and decrypt using the Aes Key from step 3 or 4.

FIG. 11A illustrates a diagram showing a process of sending an email using the present application installed in the electronic communication device (102) according to a preferred embodiment of the present invention. The below example explains the process of sending an email by the first user to the second user using the present application installed in the electronic communication device (102). The first user inputs the plain message and select send from the application installed in the first electronic communication device (102). Then a random Aes key is generated. The second user's Public Key 1 is obtained from the server (104) or local storage. The generated Aes Key is encrypted with the first user's Public Key 1 and second user's Public Key 1 separately. The Plain Message is now encrypted with Aes Key and combined with content generated in the above step.

FIG. 11B illustrates a diagram showing a process of receiving an email using the present application installed in the electronic communication device (104) according to a preferred embodiment of the present invention. The second user receives the email send in steps of **FIG. 11A** through the application installed in the first electronic communication device (102). The second user receives the encrypted email content, then the second user decrypt Pub1B(AesKey) with the second user's Private Key 1 in a second step. The plain message is obtained by decrypting Aes(Plain Message, Aes Key) with Aes key using Aes Key from the second step.

FIG. 12 illustrates an architecture diagram for electronic communication devices (102, 106) installed with the mobile application capable of transferring encrypted data including text, multimedia, email, video calls and Voice over IP (VoIP) data between the first electronic communication device (102) and the at least one second electronic communication device (106), according to a preferred embodiment of the present invention. The mobile applications installed in the electronic communication devices (102, 106) are associated with a database repository for storing user information and for storing the generated public and private keys. The information send through the mobile application is stored in the local storage such as a solid-state memory. The mobile application includes different modules associated with the key management process and the user management processes. The mobile application further includes an encryption module providing encryption levels such as AES256 military-grade encryption algorithm, RSA (1024bit) for key exchange and Hash (SHA256) for unique message signature. The encrypted text, multimedia, email, video calls and Voice over IP (VoIP) data are transferred via SSL (Secure Socket Layer).

FIG. 13 illustrates an architecture diagram for the server (104) capable of establishing a secure connection for transferring encrypted data including text, multimedia, email, video calls and Voice over IP (VoIP) data between mobile applications installed in the first electronic communication device (102) and the at least one second electronic communication device (106), according to a preferred embodiment of the present invention. The server (104) is installed with an application for allowing the communication between users through the mobile applications installed in their individual electronic communication devices (102). The

application installed in the server (104) is associated with a database repository for storing user information and for storing the generated public and private keys. The information send through the mobile application is stored in the local file storage such as a solid-state memory or hard disk of the server (104) in an encrypted form. The server application includes different business logic modules associated with the key management process, the user management, group management, account payment management processes. The server application further includes a module for transferring the encrypted text, multimedia, email, video calls and Voice over IP (VoIP) data via SSL (Secure Socket Layer) between the multiple electronic communication devices (102, 106). The application running in the first electronic communication device (102) allows to send the encrypted text, multimedia, email and VoIP data to the at least one second electronic communication device (106) even when the second device (106) is kept in an offline mode. In that case the at least one server (104) forms a central repository to store the encrypted text, multimedia, email and VoIP data and at least one contact information. The server (104) synchronizes the encrypted text, multimedia, email and VoIP data stored in the central repository with the application running in the at least one second electronic communication device (106) comes online. The application running in the first electronic communication device (102) and the at least one second electronic communication device (106) provides an all-in encrypted communication over the communication network (108). The application is capable of transferring the encrypted text chats, encrypted multimedia, encrypted email, encrypted video calls and encrypted VoIP data between the first electronic communication device (102) and the at least one second electronic communication device (106) through the at least one server (104). In an embodiment of the system (100), the application running in the first electronic communication device (102) and the at least one second electronic communication device (106) includes a self-destruct function to destroy the transferred encrypted messages including the encrypted text chats and the encrypted multimedia. The user can opt in the option from the mobile application user interface to destroy the messages after a certain period of time automatically. Further, in some other embodiments of the system (100), the mobile application running in the first electronic communication device (102) and the at least one second electronic communication device (106) includes a stealth mode to avoid detection by unauthorized users. In an embodiment, the stealth mode is available for Android OS only.

In certain embodiments the application installed in the first electronic communication device (102) and the at least one second electronic communication device (106) includes a payment system, which allows the users to pay for receiving individual services including encrypted text, multimedia, instant chat, email and VoIP data, video call over IP etc. The users can select one or more desired service and can pay for that. For managing the users the server (104) includes a user management module for managing the users, account information of the users and the payment information associated with each user.

The foregoing description of the specific embodiments will so fully reveal the general nature of the embodiments herein that others can, by applying current knowledge, readily modify or adapt for various applications such specific embodiments without departing from the generic concept, and, therefore, such adaptations and modifications should and are intended to be comprehended within the meaning and range of equivalents of the disclosed embodiments. It is to be understood that the phraseology or terminology employed herein is for the purpose of description and not of limitation. Therefore, while the embodiments herein have been described in terms of preferred embodiments, those skilled in the art will recognize that the embodiments herein can be practiced with modification within the scope of the appended claims.

Although the embodiments herein are described with various specific embodiments, it will be obvious for a person skilled in the art to practice the invention with modifications. However, all such modifications are deemed to be within the scope of the claims.

CLAIMS:

1. A system (100) for establishing secure communication between a plurality of electronic communication devices comprises:

a first electronic communication device (102) installed with an application capable of performing an encrypted or decrypted data transfer;

at least one second electronic communication device (106) installed with the application capable of performing the encrypted or decrypted data transfer;

at least one server (104) capable of establishing a secure connection between the first electronic communication device (102) and the at least one second electronic communication device (106) for transferring at least one encrypted or decrypted data,

wherein the application installed in the first electronic communication device (102) and the at least one second electronic communication device (106) being capable of performing encrypted or decrypted data transfer including text, multimedia, instant chat, email, video calls and Voice over IP (VoIP) data through the at least one server (104); and

a communication network (108) for transferring encrypted or decrypted text, multimedia, email and VoIP data from the application running in the first electronic communication device (102) to the at least one second electronic communication device (106) through the at least one server (104).

2. The system (100) of claim 1 wherein the first electronic communication device (102) and the at least one second electronic communication device (106) is installed with the application capable of performing encrypted or decrypted text, multimedia, instant chat, email, video calls, video group chat and Voice over IP (VoIP) data transfer over the communication network (108).

3. The system (100) of claim 1 wherein the at least one server (104) authenticates first electronic communication device (102) and the at least one second electronic communication device (106) for establishing an encrypted or decrypted connection to transfer encrypted or decrypted text, multimedia, instant chat, email, video calls, video group chat and Voice over IP (VoIP) data using the application running in the first electronic communication device (102)

and the at least one second electronic communication device (106) over the communication network (108).

4. The system (100) of claim 1 wherein the application running in the first electronic communication device (102) allows to send the encrypted or decrypted text, multimedia, instant chat, email, video calls, video group chat and Voice over IP (VoIP) data to the at least one second electronic communication device (106) kept in an offline mode.

5. The system (100) of claim 4 wherein the at least one server (104) forms a central repository to store the encrypted or decrypted text, multimedia, instant chat, email, video calls, video group chat and Voice over IP (VoIP) data and at least one contact information.

6. The system (100) of claim 5 wherein the at least one server (104) is capable of synchronizing the encrypted or decrypted text, multimedia, instant chat, email, video calls, video group chat and Voice over IP (VoIP) data stored in the central repository with the application running in the at least one second electronic communication device (106) when the device (106) comes online.

7. The system (100) of claim 1 wherein the application running in the first electronic communication device (102) and the at least one second electronic communication device (106) provides an all-in encrypted communication over the communication network (108),

wherein the application capable of all-in encrypted communication transfers the encrypted text chats, encrypted instant chat, encrypted multimedia, encrypted email, encrypted video calls and encrypted VoIP data between the first electronic communication device (102) and the at least one second electronic communication device (106) through the at least one server (104).

8. The system (100) of claim 1 wherein the application running in the first electronic communication device (102) and the at least one second electronic communication device (106) includes a self-destruct function to destroy the transferred encrypted or decrypted messages including the encrypted or decrypted text chats and the encrypted or decrypted

multimedia.

9. The system (100) of claim 1 wherein the application running in the first electronic communication device (102) and the at least one second electronic communication device (106) includes a stealth mode to avoid detection by unauthorized users.

10. A method for establishing secure communication between a plurality of electronic communication devices, the method comprises the steps of:

providing a first electronic communication device (102) and at least one second electronic communication device (106) installed with an application capable of performing an encrypted or decrypted data transfer,

wherein the application installed in the first electronic communication device (102) and the at least one second electronic communication device (106) being capable of performing encrypted or decrypted data transfer including text, multimedia, instant chat, email, video calls, video chat and Voice over IP (VoIP) data through the at least one server (104);

authorizing the at least one second electronic communication device (106) by the first electronic communication device (102) for establishing secure communication using the application,

wherein a process of authorizing the at least one second electronic communication device (106) by the first electronic communication device (102) comprises the steps of:

registration of the first electronic communication device (102) with a central server (104);

approval of the at least one second electronic communication device (106) by the first electronic communication device (102); and

exchange of public parameters between the first electronic communication device (102) with the central server (104) and the at least one second electronic communication device (106);

sending at least one information from the first electronic communication device (102) to the at least one second electronic communication device (106) via the server (104),

wherein the at least one information includes text, multimedia, instant chat, email,

video calls, video chat and Voice over IP (VoIP) data in an encrypted or decrypted message format; and

receiving, verifying and decrypting the at least one information from the first electronic communication device (102) by the at least one second electronic communication device (106).

11. The method of claim 10 wherein the application is capable of transferring encrypted or decrypted text chats, encrypted or decrypted instant chat, encrypted or decrypted multimedia, encrypted or decrypted email, encrypted or decrypted video calls and encrypted or decrypted VoIP data between the first electronic communication device (102) and the at least one second electronic communication device (106) through the server (104).

12. The method of claim 10 wherein the application running in the first electronic communication device (102) and the at least one second electronic communication device (106) includes a self-destruct function to destroy the transferred encrypted or decrypted messages including the encrypted or decrypted text chats and the encrypted or decrypted multimedia.

13. The method of claim 10 wherein the application running in the first electronic communication device (102) and the at least one second electronic communication device (106) includes a stealth mode to avoid detection by unauthorized users.

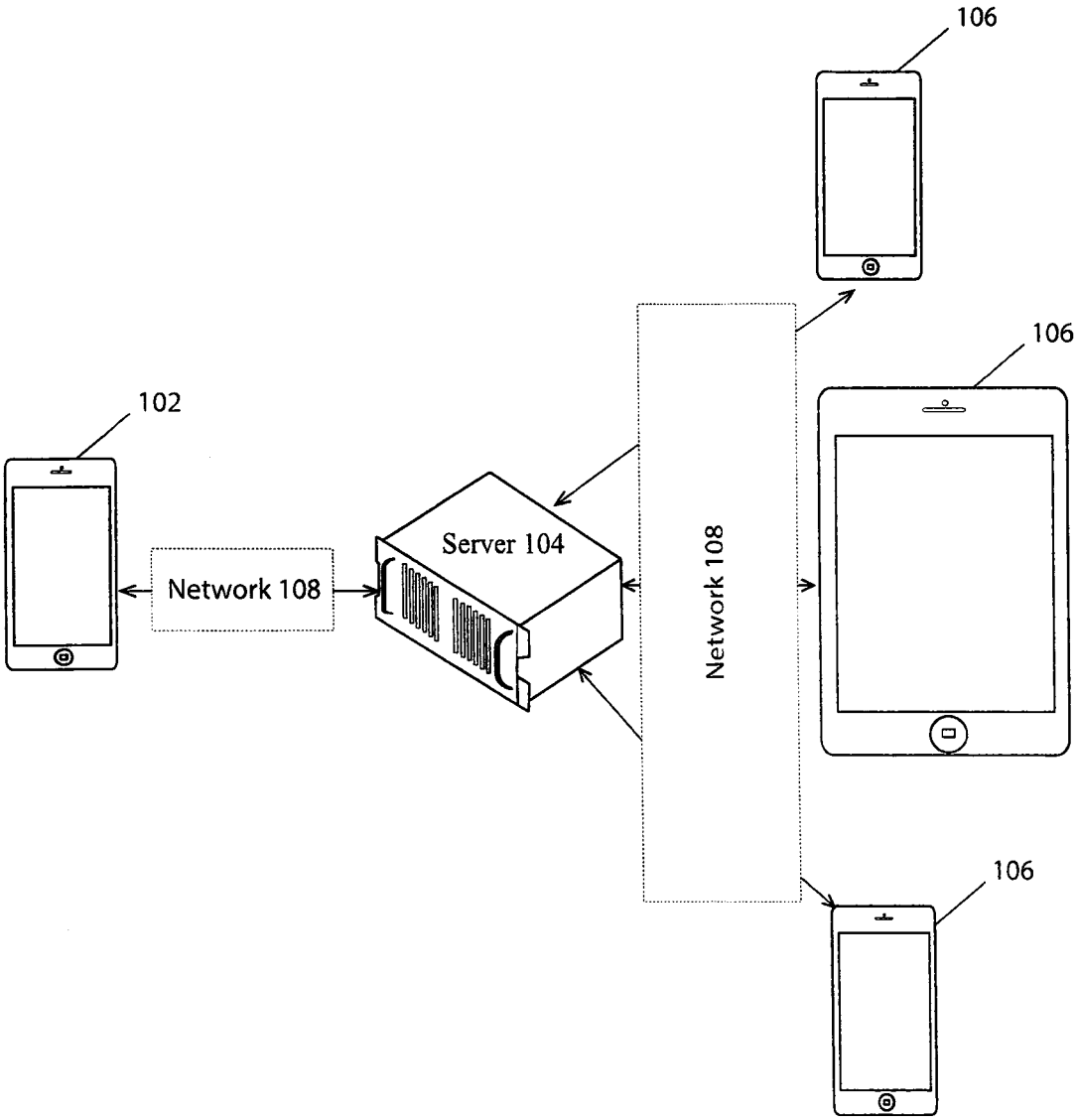

FIG. 1

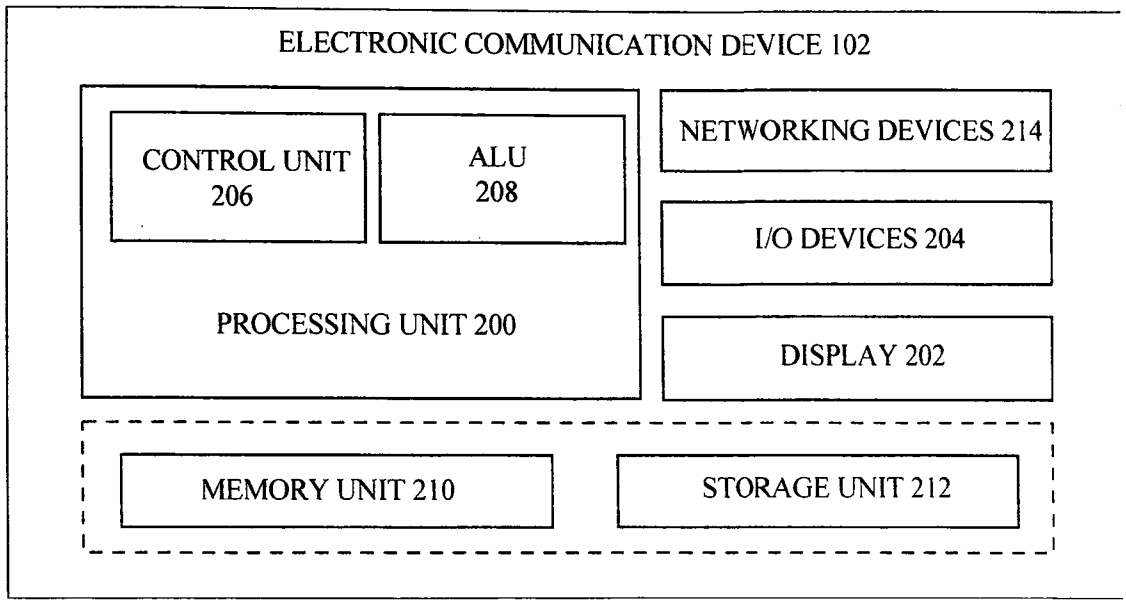
ELECTRONIC COMMUNICATION DEVICE 102
CONTROL UNIT 206
ALU 208
PROCESSING UNIT 200
NETWORKING DEVICES 214
I/O DEVICES 204
DISPLAY 202
MEMORY UNIT 210
STORAGE UNIT 212

FIG. 2

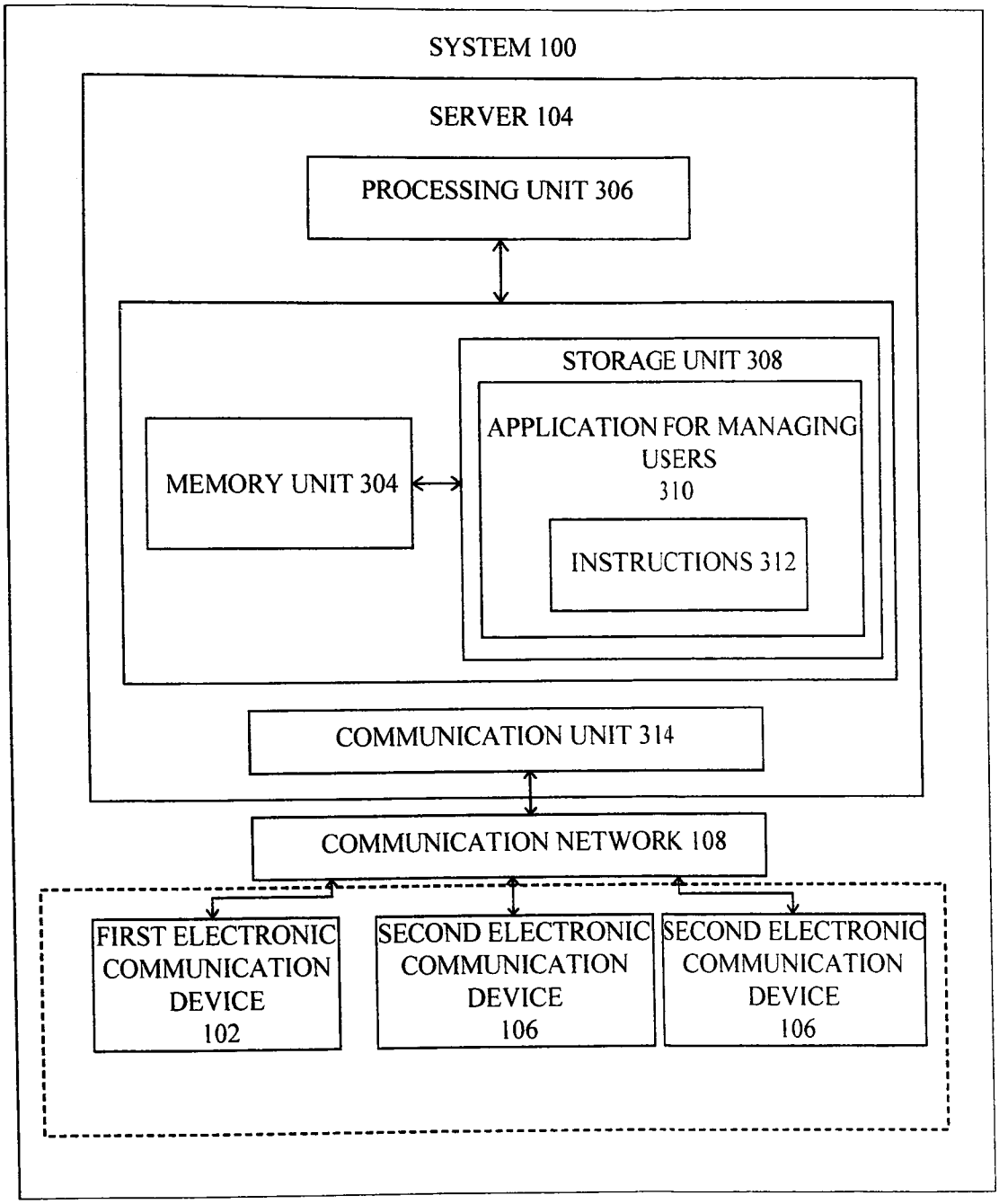
SYSTEM 100
SERVER 104
PROCESSING UNIT 306
STORAGE UNIT 308
APPLICATION FOR MANAGING USERS 310
INSTRUCTIONS 312
MEMORY UNIT 304
COMMUNICATION UNIT 314
COMMUNICATION NETWORK 108
FIRST ELECTRONIC COMMUNICATION DEVICE 102
SECOND ELECTRONIC COMMUNICATION DEVICE 106
SECOND ELECTRONIC COMMUNICATION DEVICE 106

FIG. 3

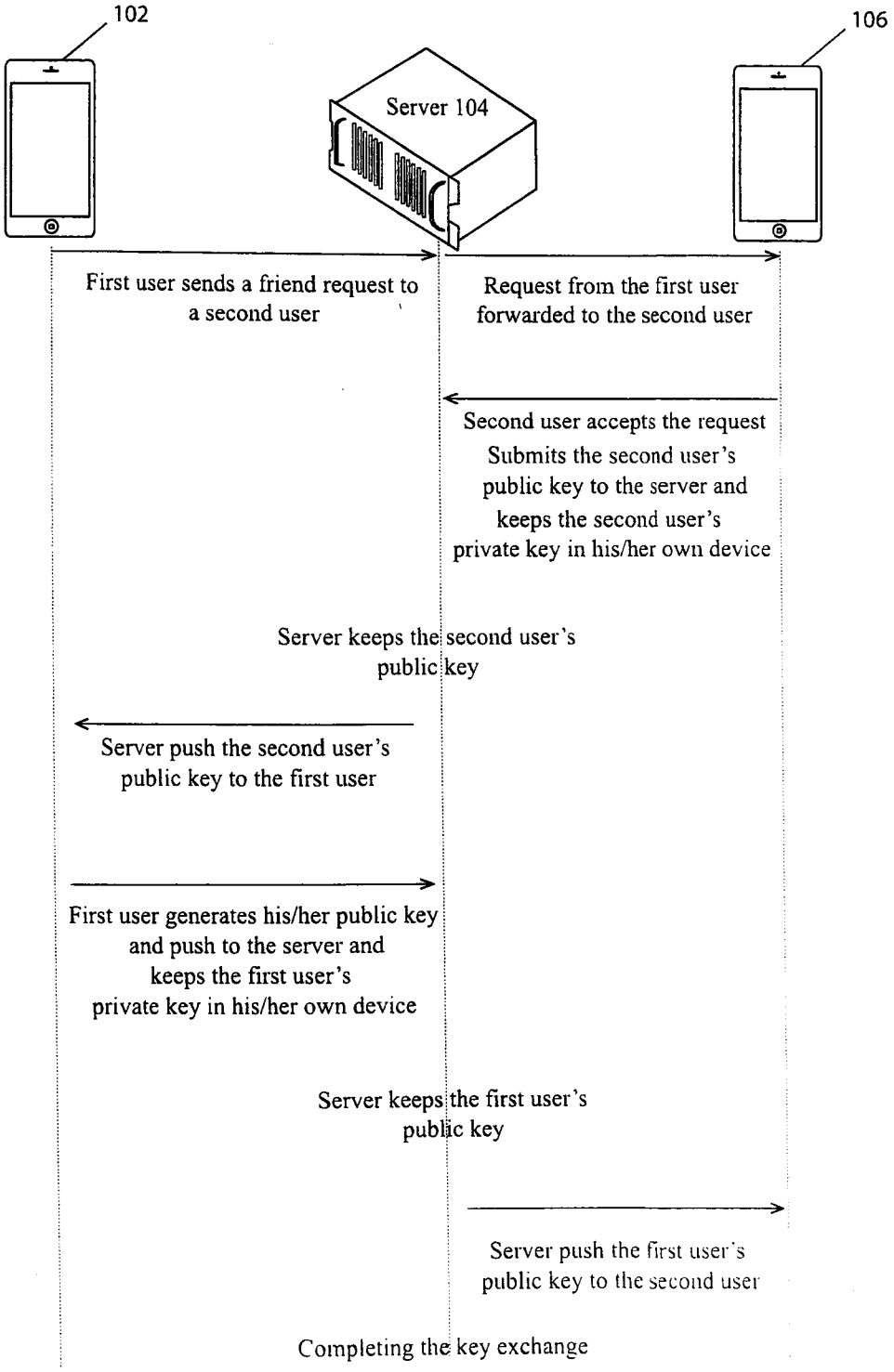
102
Server 104
106
First user sends a friend request to a second user
Request from the first user forwarded to the second user
Second user accepts the request
Submits the second user's public key to the server and keeps the second user's private key in his/her own device
Server keeps the second user's public key
Server push the second user's public key to the first user
First user generates his/her public key and push to the server and keeps the first user's private key in his/her own device
Server keeps the first user's public key
Server push the first user's public key to the second user
Completing the key exchange

FIG. 4

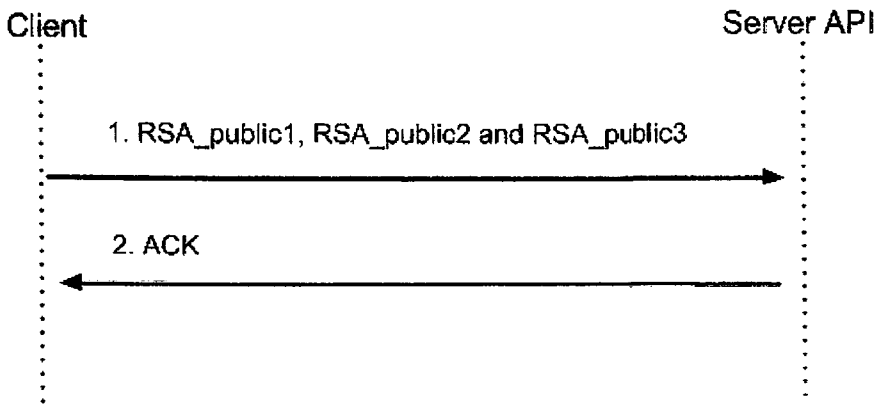
Client
Server API
1. RSA_public1, RSA_public2 and RSA_public3
2. ACK

FIG. 5A

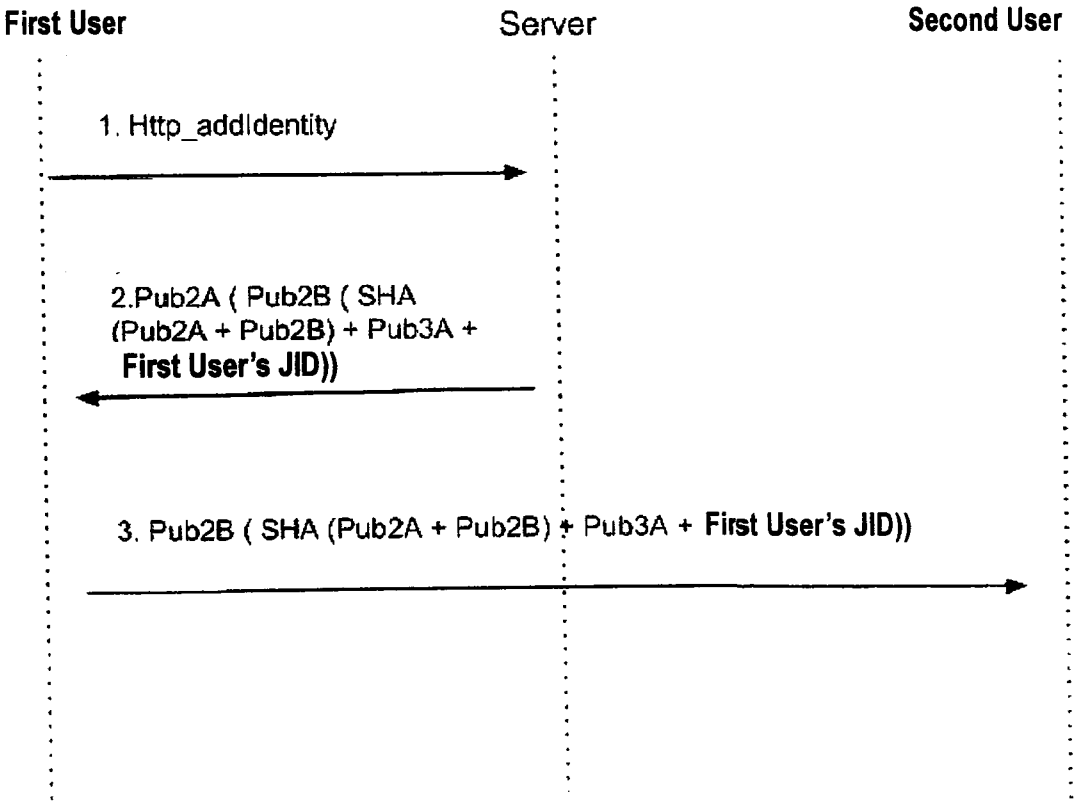
First User
Server
Second User
1. Http_addIdentity
2.Pub2A (Pub2B (SHA (Pub2A + Pub2B) + Pub3A + First User's JID))
3. Pub2B (SHA (Pub2A + Pub2B) + Pub3A + First User's JID))

FIG. 5B

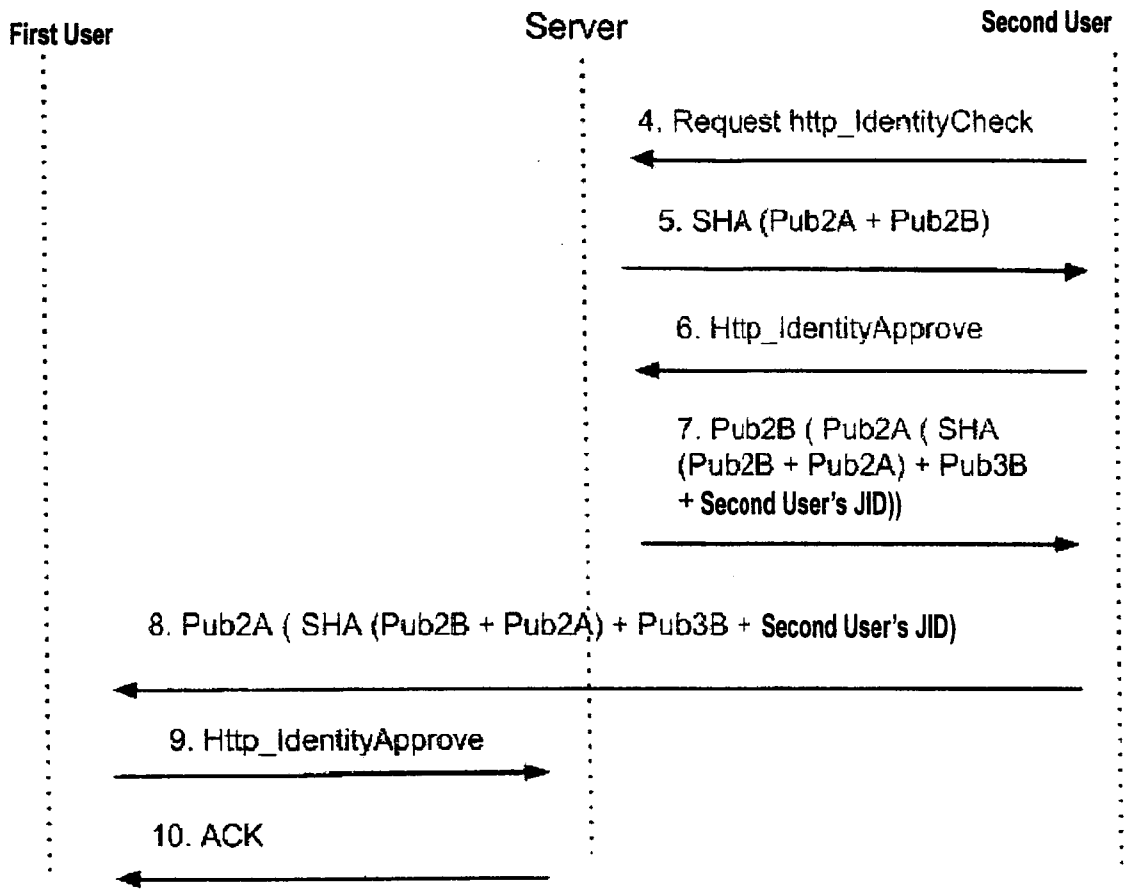
First User
Server
Second User
4. Request http_IdentityCheck
5. SHA (Pub2A + Pub2B)
6. Http_IdentityApprove
7. Pub2B (Pub2A (SHA (Pub2B + Pub2A) + Pub3B + Second User's JID))
8. Pub2A (SHA (Pub2B + Pub2A) + Pub3B + Second User's JID)
9. Http_IdentityApprove
10. ACK

FIG. 5C

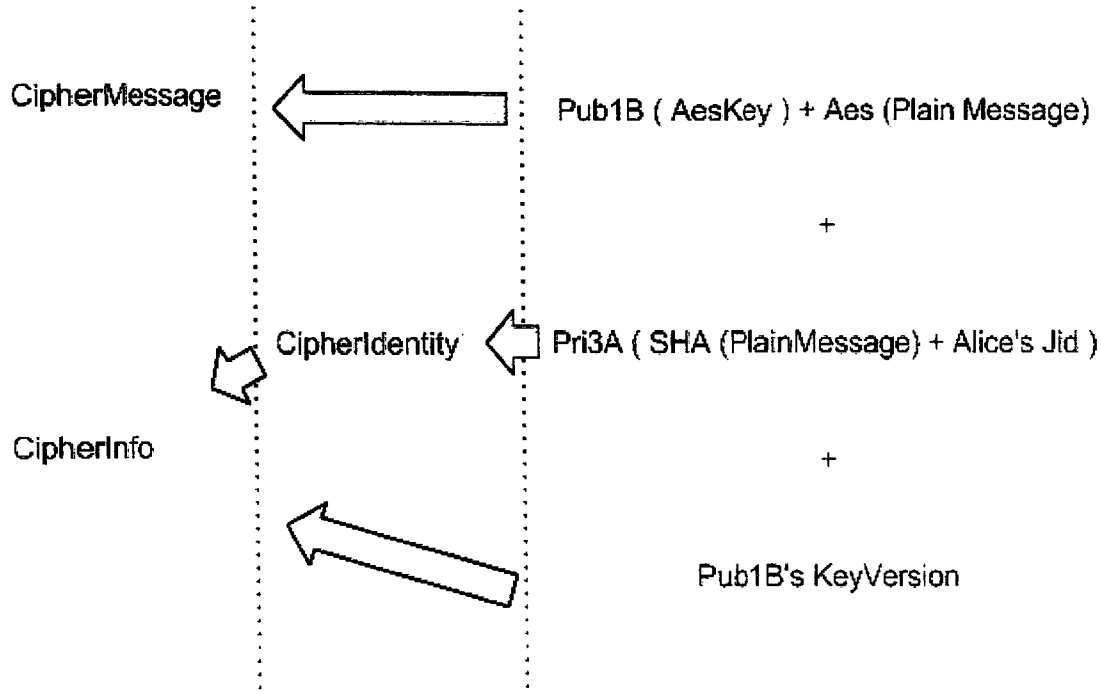
CipherMessage
Pub1B (AesKey) + Aes (Plain Message)
+
CipherIdentity
Pri3A (SHA (PlainMessage) + Alice's Jid)
CipherInfo
+
Pub1B's KeyVersion

FIG. 6

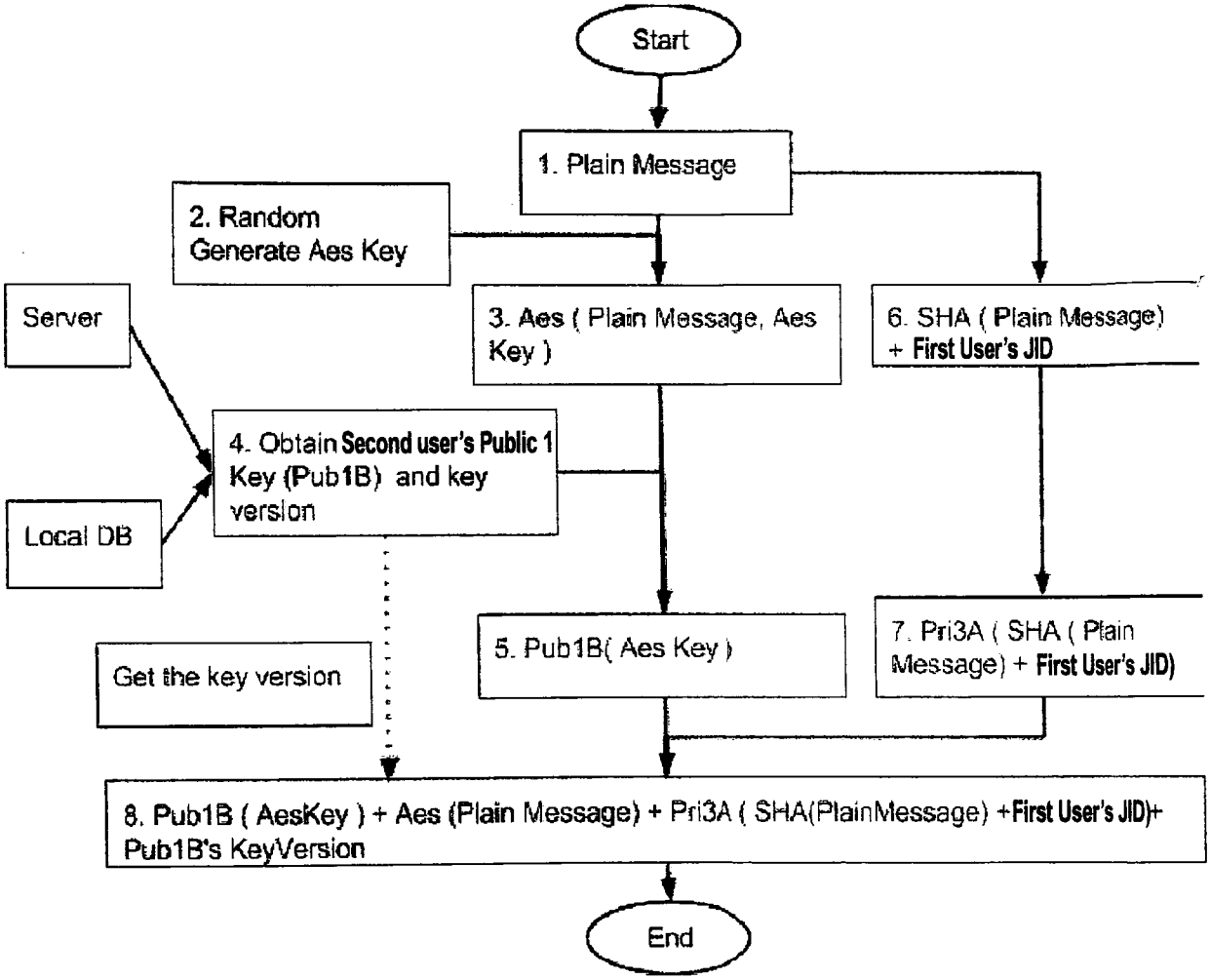
Start
1. Plain Message
2. Random Generate Aes Key
Server
3. Aes (Plain Message, Aes Key)
6. SHA (Plain Message) + First User's JID
4. Obtain Second user's Public 1 Key (Pub1B) and key version
Local DB
Get the key version
5. Pub1B(Aes Key)
7. Pri3A (SHA (Plain Message) + First User's JID)
8. Pub1B (AesKey) + Aes (Plain Message) + Pri3A (SHA(PlainMessage) +First User's JID)+ Pub1B's KeyVersion
End

FIG. 7

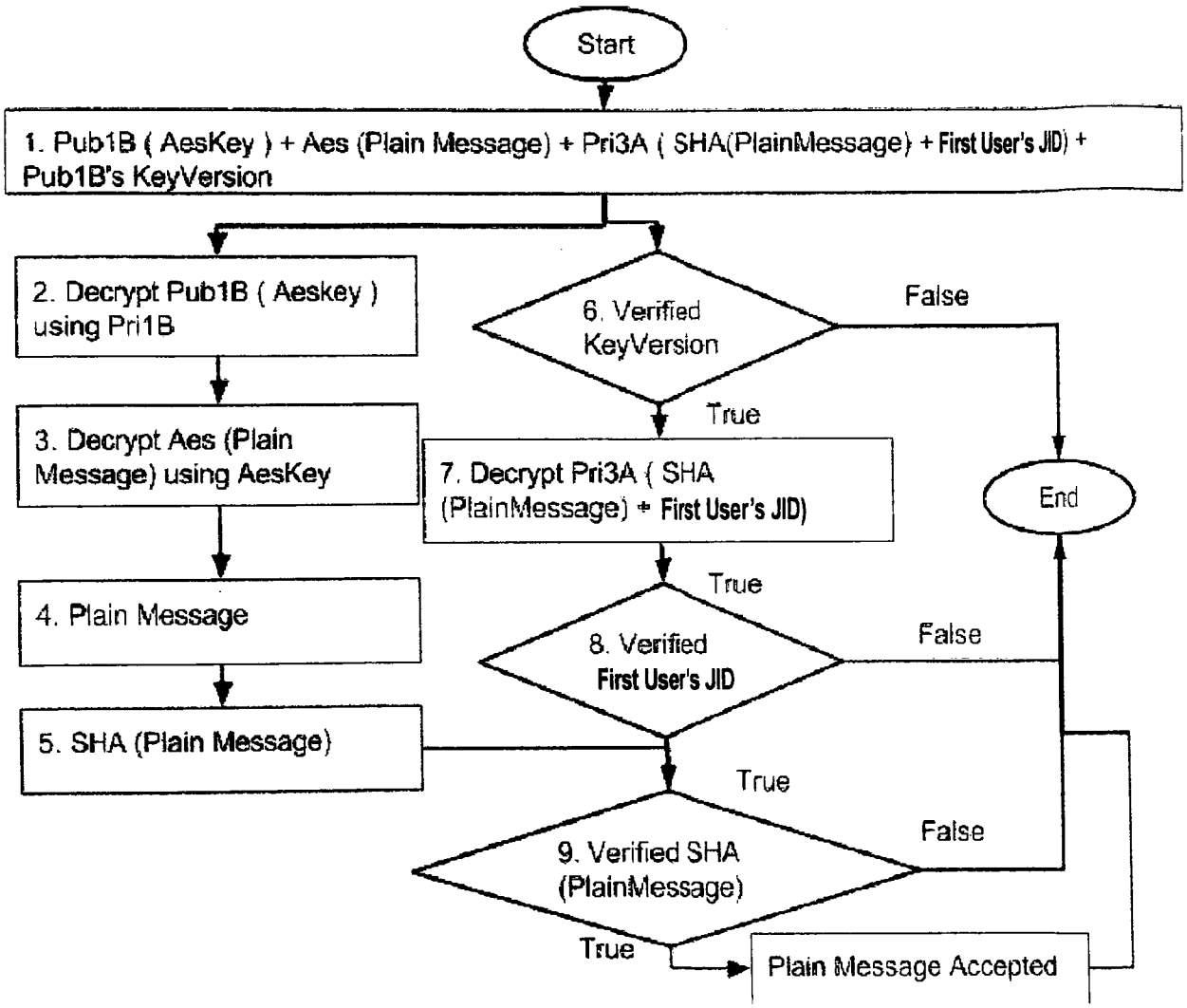
Start
1. Pub1B (AesKey) + Aes (Plain Message) + Pri3A (SHA(PlainMessage) + First User's JID) + Pub1B's KeyVersion
2. Decrypt Pub1B (Aeskey) using Pri1B
3. Decrypt Aes (Plain Message) using AesKey
4. Plain Message
5. SHA (Plain Message)
6. Verified KeyVersion
False
True
7. Decrypt Pri3A (SHA (PlainMessage) + First User's JID)
True
8. Verified First User's JID
False
True
9. Verified SHA (PlainMessage)
False
True
Plain Message Accepted
End

FIG. 8

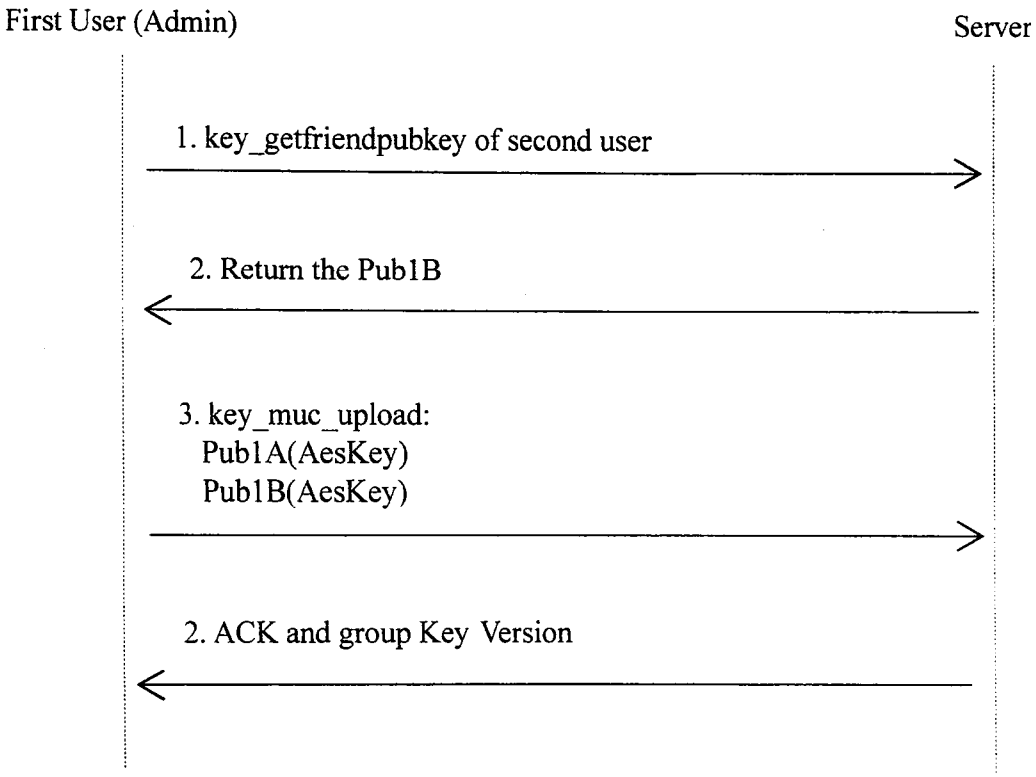
First User (Admin)
Server
1. key_getfriendpubkey of second user
2. Return the Pub1B
3. key_muc_upload:
Pub1A(AesKey)
Pub1B(AesKey)
2. ACK and group Key Version

FIG. 9A

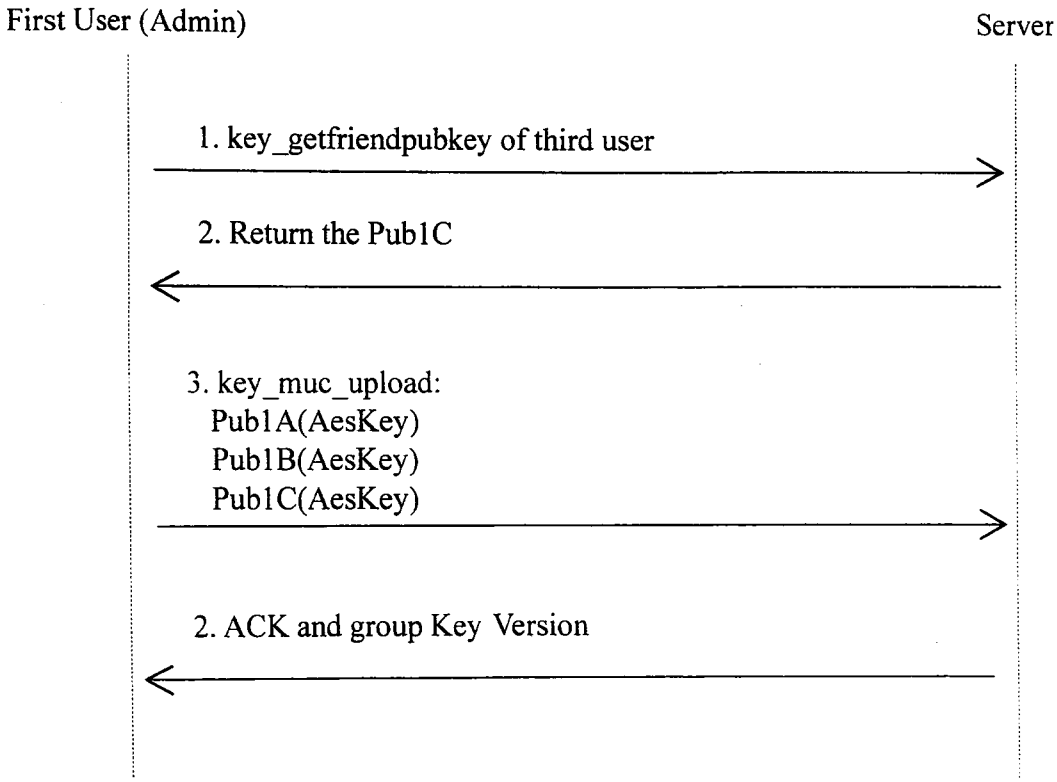
First User (Admin)
Server
1. key_getfriendpubkey of third user
2. Return the Pub1C
3. key_muc_upload:
Pub1A(AesKey)
Pub1B(AesKey)
Pub1C(AesKey)
2. ACK and group Key Version

FIG. 9B

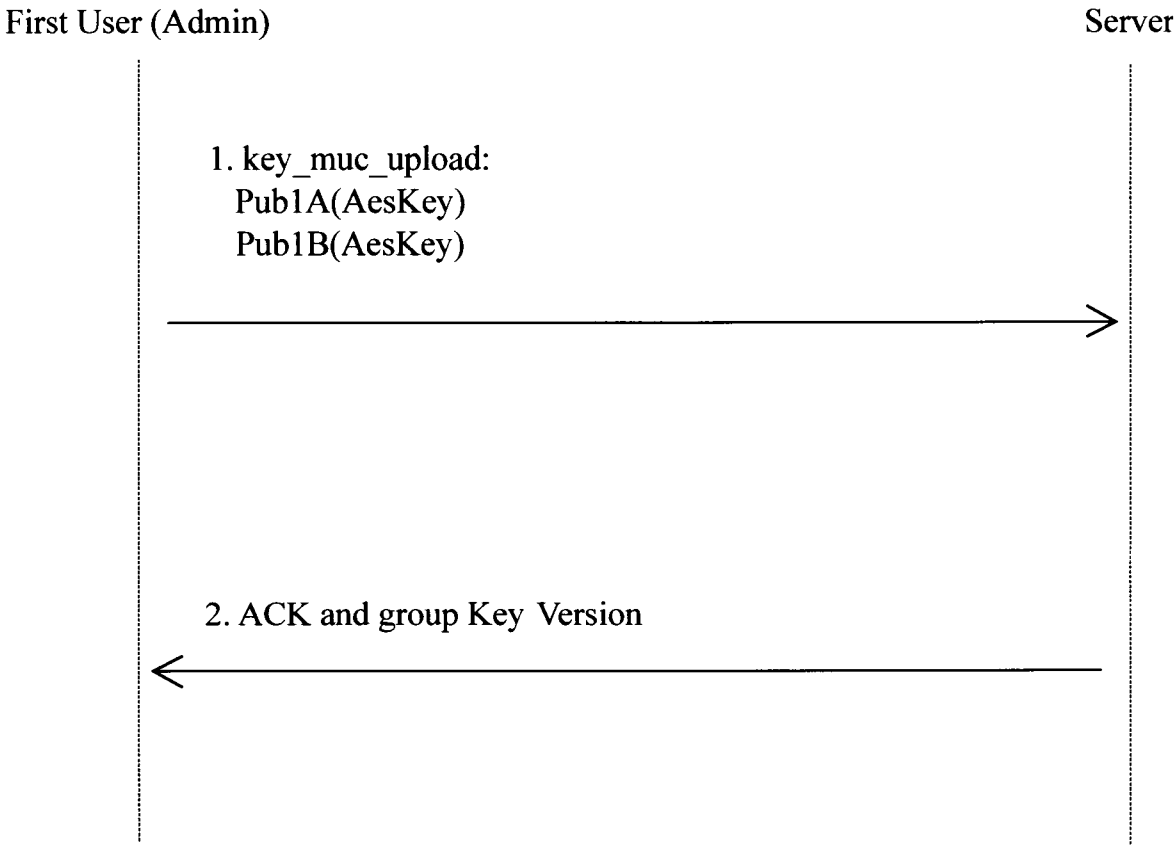
First User (Admin)
Server
1. key_muc_upload:
Pub1A(AesKey)
Pub1B(AesKey)
2. ACK and group Key Version

FIG. 9C

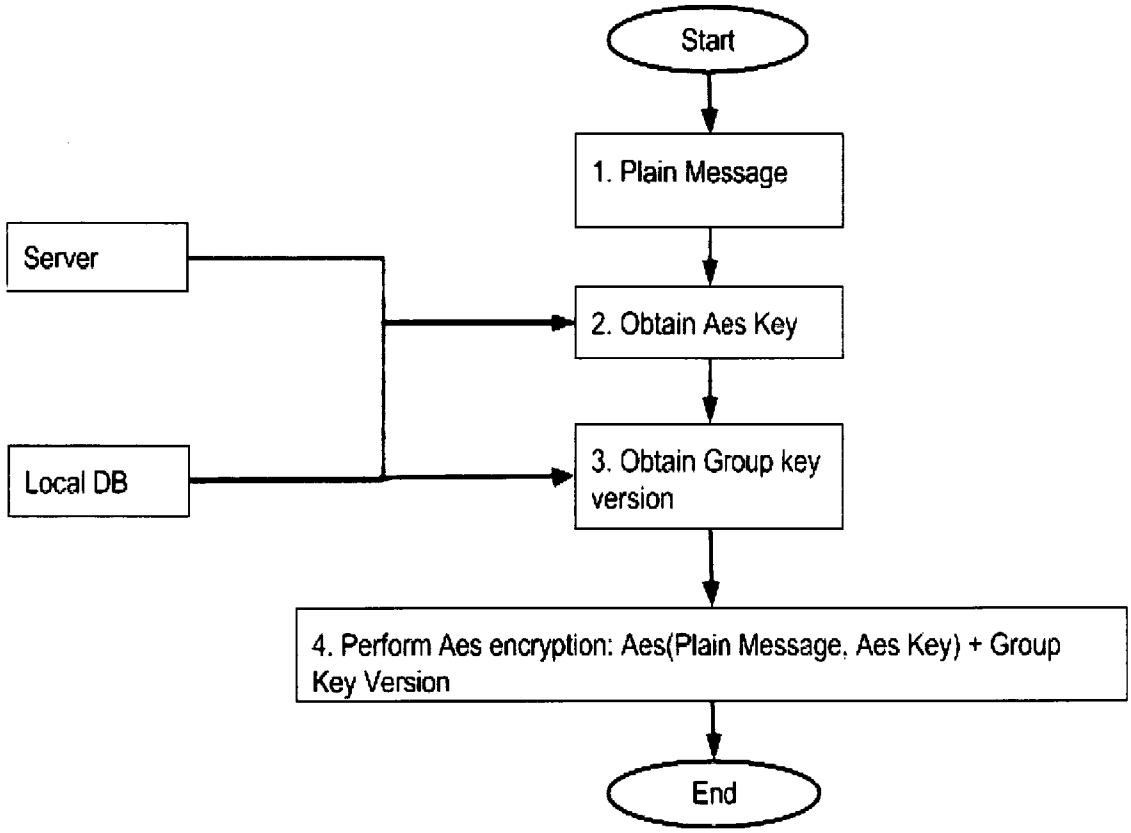
Start
1. Plain Message
Server
2. Obtain Aes Key
Local DB
3. Obtain Group key version
4. Perform Aes encryption: Aes(Plain Message, Aes Key) + Group Key Version
End

FIG. 10A

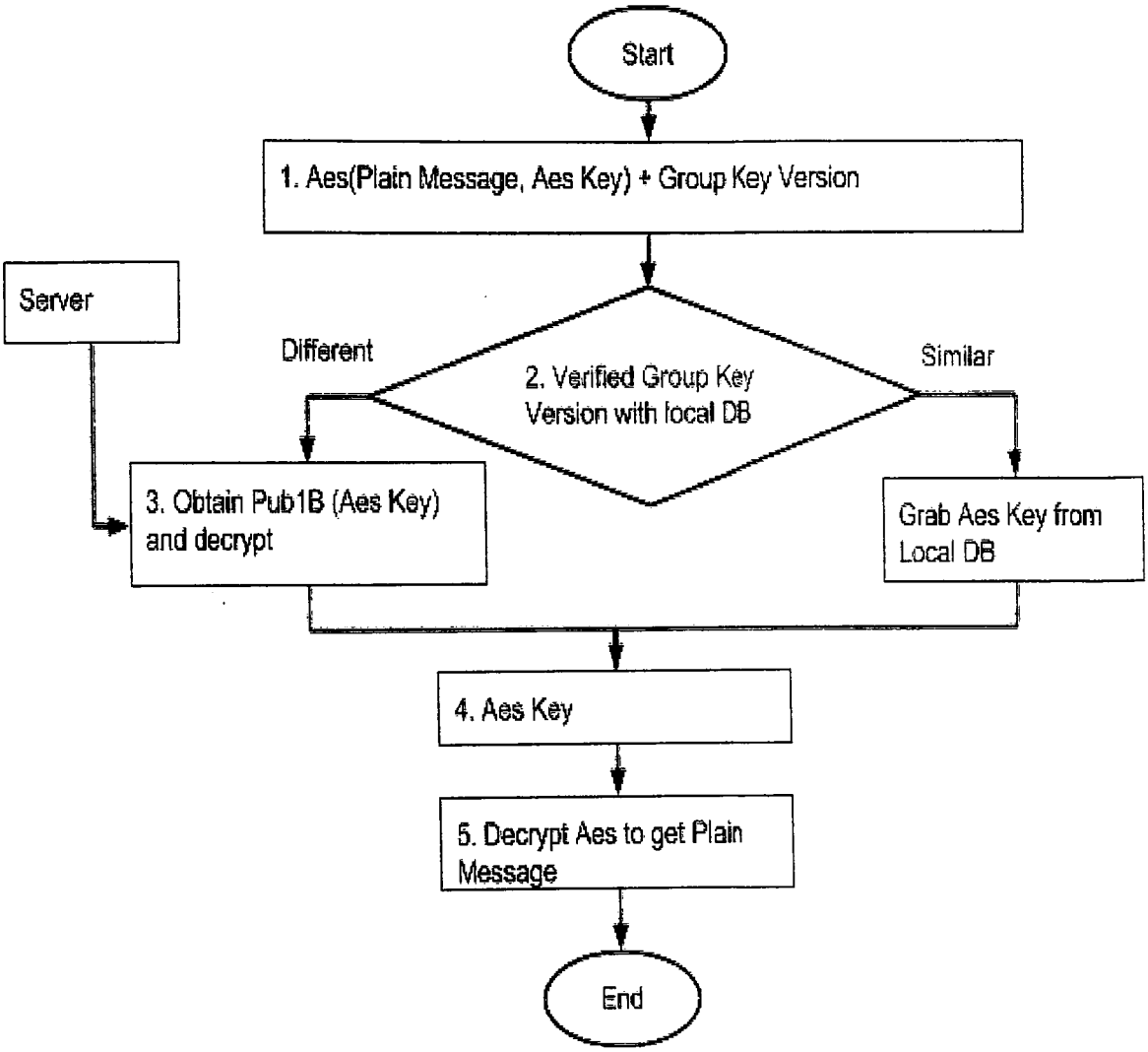
Start
1. Aes(Plain Message, Aes Key) + Group Key Version
Server
Different
2. Verified Group Key Version with local DB
Similar
3. Obtain Pub1B (Aes Key) and decrypt
Grab Aes Key from Local DB
4. Aes Key
5. Decrypt Aes to get Plain Message
End

FIG. 10B

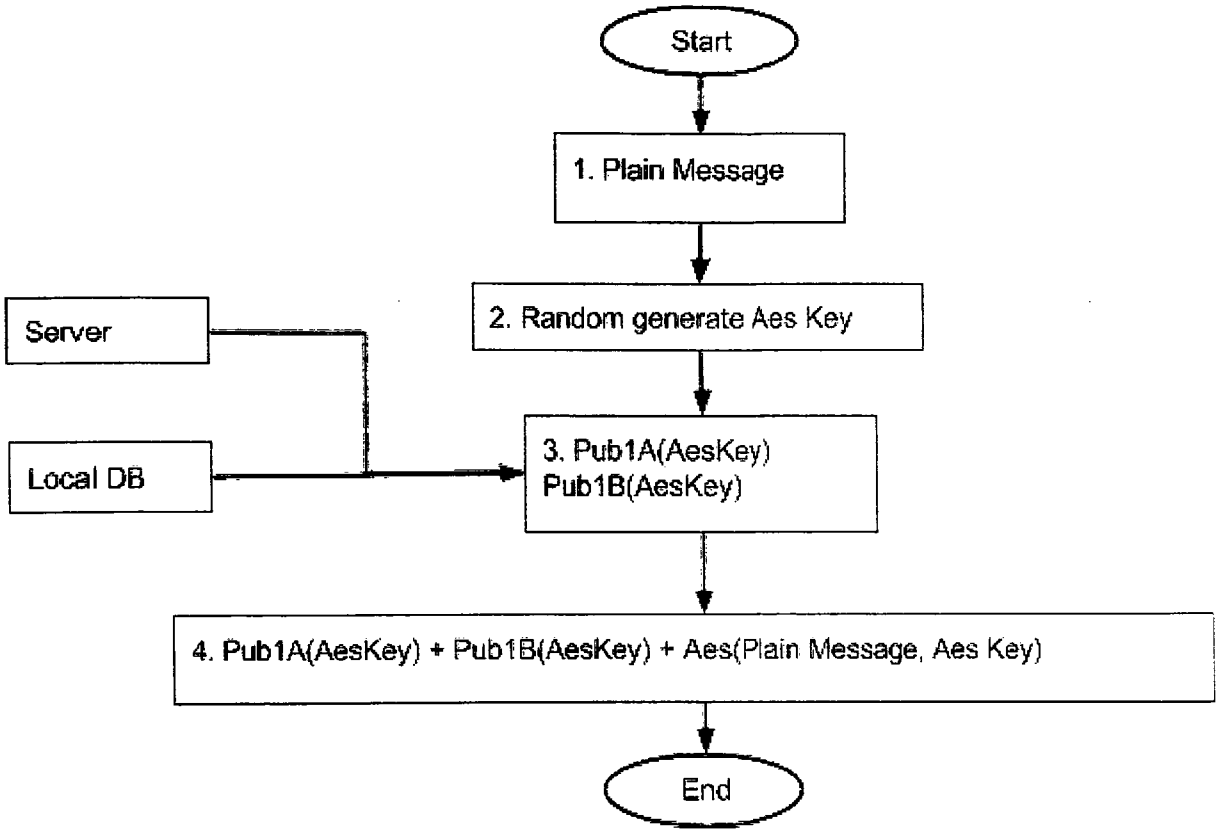
Start
1. Plain Message
2. Random generate Aes Key
Server
Local DB
3. Pub1A(AesKey)
Pub1B(AesKey)
4. Pub1A(AesKey) + Pub1B(AesKey) + Aes(Plain Message, Aes Key)
End

FIG. 11A

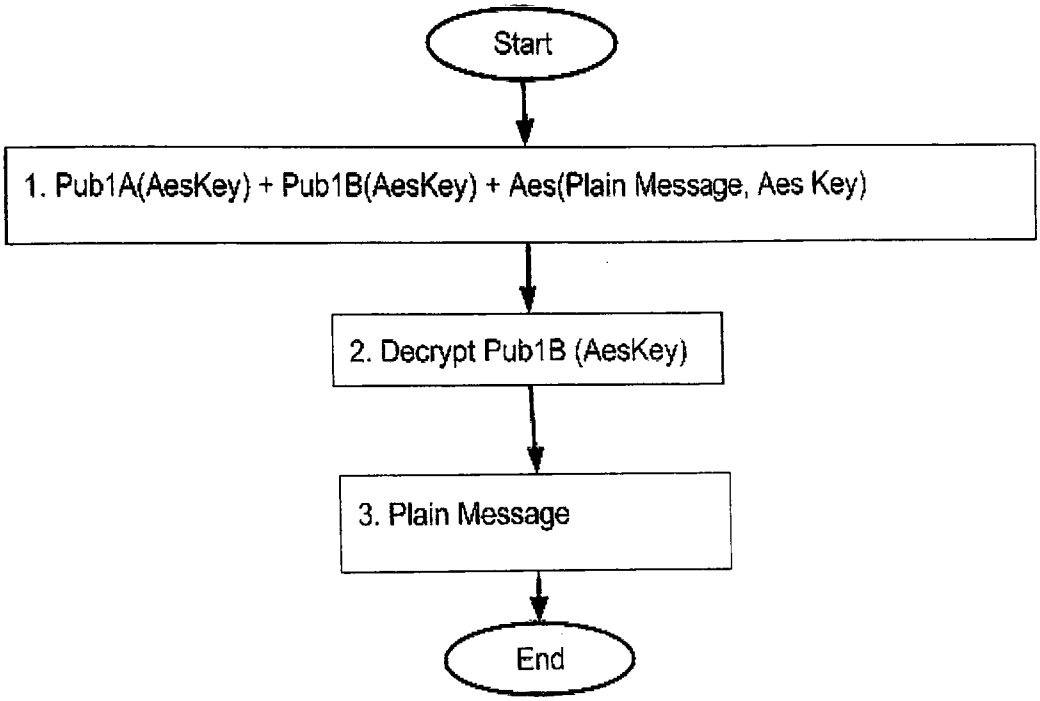
Start
1. Pub1A(AesKey) + Pub1B(AesKey) + Aes(Plain Message, Aes Key)
2. Decrypt Pub1B (AesKey)
3. Plain Message
End

FIG. 11B

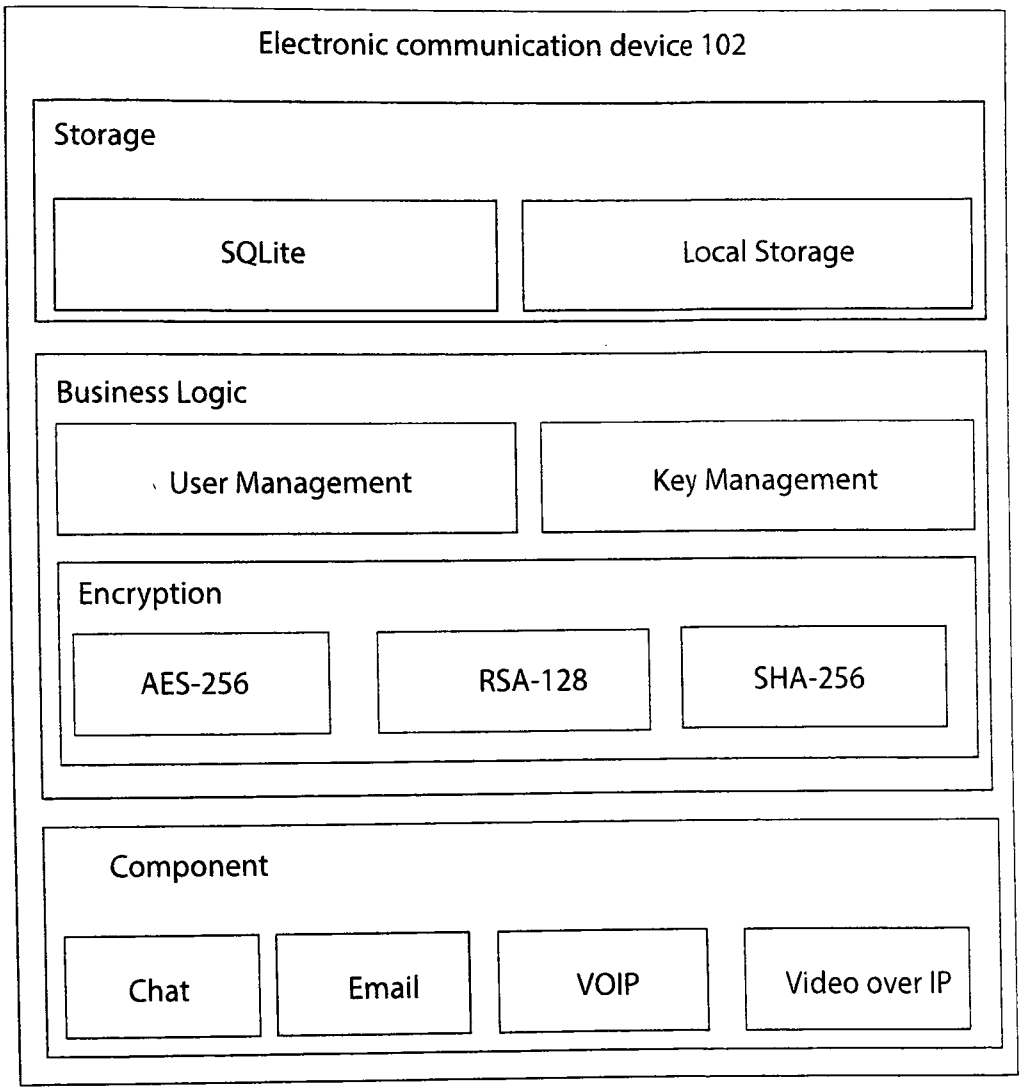
Electronic communication device 102
Storage
SQLite
Local Storage
Business Logic
User Management
Key Management
Encryption
AES-256
RSA-128
SHA-256
Component
Chat
Email
VOIP
Video over IP

FIG. 12

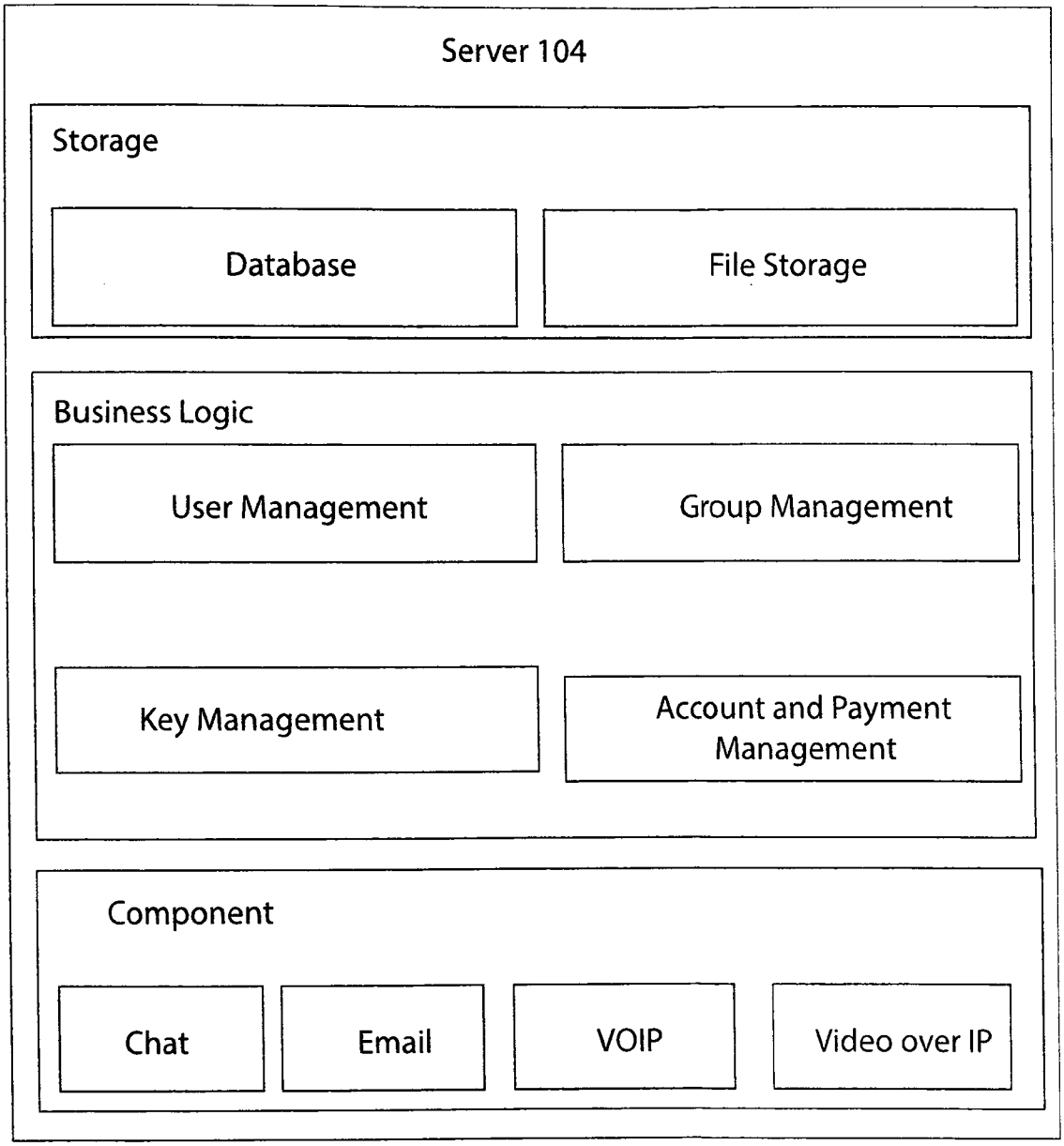
Server 104
Storage
Database
File Storage
Business Logic
User Management
Group Management
Key Management
Account and Payment Management
Component
Chat
Email
VOIP
Video over IP

FIG. 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2016/000006

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00 (2006.01) H04L 12/00 (2006.01) H04W 12/00 (2009.01)

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)

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

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

Databases: EPODOC, WPIAP, INSPEC, TXTE, The LENS, Google Patents, Google, Google Scholar, Espacenet, AusPat and internal databases provided by IP Australia.
IPC and CPC Marks: H04L 9/00, H04L 12/00, H04W 12/00.
Keywords: Secure, Communication, Application, Server, Encryption, Decryption, Key, Public, Private, Transmit, Receive, Data transfer, Device, Message, Voice over IP, Authentication, Registration, Approve, Source, Destination, First, Second, Service, Offline, Online, Synchronise, Stealth, Self-destruction, Mode and like terms.
Applicant Name: "MTOUCHE TECHNOLOGY BERHAD".
Inventor Name: "Kenneth Kong Seh Kiang", "Janice Ng Dz Yun", "Leong Yee Ling", "Yang Zhuo", "Randall Low" and "Melvyn Tan Hong Keat".

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] Further documents are listed in the continuation of Box C [X] 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 another 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
29 April 2016	29 April 2016
Name and mailing address of the ISA/AU	**Authorised officer**
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au	Yogita Chapre AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. 0262223638

INTERNATIONAL SEARCH REPORT C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		International application No. **PCT/MY2016/000006**
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/0138660 A1 (HAYNES et al.) 03 June 2010 Title; Abstract; Para[0001], [0012]-[0019], [0030], [0032], [0037], [0047]-[0056], [0058]-[0063], [0068]; Figures 1 and 5-9.	1-13
X	US 2014/0136208 A1 (INTERMEC IP CORP.) 15 May 2014 Abstract; Para[0020], [0023], [0026], [0028], [0038], [0044]-[0048], [0058]; Figures 1-4, 7-8 and 10-14.	1-13
A	US 2013/0268582 A1 (NOKIA CORPORATION) 10 October 2013 Abstract; Para[0002]-[0006].	1-13
A	US 6711608 B1 (OGILVIE) 23 March 2004 Abstract; Col 2, Lines 61-65; Col 3, Lines 17-49; Col 5, Line 44 – Col 6, Line 20; Figure 2.	1-13
A	US 2013/0159877 A1 (BANTI et al.) 20 June 2013 Abstract; Para[0003], [0022].	1-13

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/MY2016/000006**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
US 2010/0138660 A1	03 June 2010	US 2010138660 A1	03 Jun 2010
		US 8990569 B2	24 Mar 2015
US 2014/0136208 A1	15 May 2014	US 2014136208 A1	15 May 2014
US 2013/0268582 A1	10 October 2013	US 2013268582 A1	10 Oct 2013
US 6711608 B1	23 March 2004	US 6711608 B1	23 Mar 2004
		AU 7106200 A	24 Apr 2001
		EP 1116126 A1	18 Jul 2001
		US 6324569 B1	27 Nov 2001
		US 2002026487 A1	28 Feb 2002
		US 6487586 B2	26 Nov 2002
		US 6701347 B1	02 Mar 2004
		US 6757713 B1	29 Jun 2004
		WO 0017768 A1	30 Mar 2000
		WO 0122243 A1	29 Mar 2001
US 2013/0159877 A1	20 June 2013	US 2013159877 A1	20 Jun 2013

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.