

**METHODS AND SYSTEMS FOR ESTABLISHING AN OPERATION
BETWEEN USERS BASED ON IDENTIFICATION OF ONE OR MORE USER
ACTIONS**

FIELD OF THE INVENTION

5 The present invention relates generally to establishing communication between a plurality of users. In particular, the present invention relates to methods and systems for establishing an operation between the users based on identification of one or more user actions.

BACKGROUND OF THE INVENTION

10 The use of wireless communication systems has rapidly evolved from predominantly voice-only communications to the transmission of data, such as Internet and multimedia content and execution of a payment transaction. There are ongoing efforts to find more effective ways to share data and initiate communication between the smart devices connected through the network. Several mechanisms and technologies
15 have developed to transfer data to, or to conduct a transaction with another device such as a smart device. As such, a first smart device may be able to display, manipulate, or store data from a second smart device, provided that the data is transferred from the second device to the first device. Though a user may have access to two similarly capable smart devices, sharing data between the two devices may involve a number of
20 steps, each of which may vary in difficulty. The process of transferring data or establishing a communication for executing any operation between the devices may include many user decisions, such as which data to save, where the data to be saved, which formats each device may be capable of processing, how to interconnect the devices for a most effective data transfer, how to securely initiate a commercial
25 transaction, etc. Such complexity may also increase the difficulty or time spent transferring data between two electronic devices. The existing mechanisms of establishing communication between two smart devices have drawbacks when it comes to initiating an operation securely between two smart devices. Therefore, what is desired in an approach that will enable a user to securely initiate a transaction or operation
30 between two smart devices. The system and process should be easy to implement, cost effective and adaptable to existing environments. A secure mechanism is desired to initiate an operation between a plurality of users.

SUMMARY OF THE INVENTION

The present invention provides methods and system to initiate an operation between a first user and a second user belonging to a same network using one or more user actions. The operation may be initiated by any of the users in a network. The operation that include, but not limited to, transfer of files (photos, songs, videos, documents or any piece of data), exchange of information, payments, or sharing any content over a digital medium. The operation is initiated by means of one or more pre-configured actions performed by the user in real-time, on the smart wearable device or mobile device and/or both. The actions include, but not limited to, entering a pin (numeric), password (alpha-numeric, special), One Time Password (OTP), gesture patterns, sensor values or any combination thereof. These actions performed by the user are appropriately captured by the I/O modules, sensor modules configured in both smart wearable device and mobile device. In an embodiment, the operation may be initiated by the user, through the combined operation of the smart wearable device and mobile device.

In another embodiment, a method of initiating an operation between a first user and a second user is provided. The method includes the steps of: receiving one or more first input actions from said first user and one or more second input actions from said second user, wherein said one or more first input actions are responsible for validating and authenticating said first user and said one or more second input actions are responsible for validating and authenticating said second user; comparing said one or more first input actions and one or more second input actions respectively with corresponding pre-configured authentication actions for validating and authenticating said first user and said second user respectively; receiving one or more third input actions associated with said first user, wherein said one or more third input actions are responsible for triggering initiation of one or more operations with the second user; determining type of one or more operations associated with said one or more third input actions; receiving one or more fourth input actions from the second user, wherein said one or more fourth input actions are responsible for establishing a connection for initiating one or more determined operations with the first user; ascertaining if said one or more fourth input actions matches with pre-configured actions required for initiating said one or more determined operations between the first and the second user; initiating said one or more determined operations between the first and the second user on positive ascertaining.

In an embodiment, the present invention provides methods and systems for establishing communication between a first mobile device and second mobile device through the values of accelerometer, gyroscope, location and time stamps, and by simply tapping these mobile devices.

It is an object of the invention to provide methods and system for easy and quick identification of two parties in a range or part of a same network.

It is another object of the invention to provide a secure mechanism to initiate an operation between a plurality of users.

To further clarify advantages and features of the present invention, a more particular description of the invention will be rendered by reference to specific embodiments thereof, which is illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail with the accompanying drawings.

BRIEF DESCRIPTION OF FIGURES

These and other features, aspects, and advantages of the present invention will become better understood when the following detailed description is read with reference to the accompanying drawings in which like characters represent like parts throughout the drawings, wherein:

Figure 1 illustrates a block diagram of a system level environment in accordance with an embodiment of the present invention;

Figure 2 illustrates block diagram of exemplary components of smart wearable device in accordance with an embodiment of the present invention;

Figure 3A illustrates direct connection between the smart wearable device and application server in accordance with an embodiment of the present invention;

Figure 3B illustrates direct connection between mobile device and application server in accordance with an embodiment of the present invention;

Figure 3C illustrates the connection (establishment) between the smart wearable device and application through a mobile device in accordance with an embodiment of the present invention;

Figure 4 illustrates a flowchart for a method of initiating an operation between a first user and a second user in accordance with an embodiment of the present invention;

Figure 5 illustrates a flowchart illustrating the reception of inputs from both smart wearable and mobile device, for the first time, in accordance with an embodiment of the present invention;

Figure 6 illustrates a flowchart describing the identification of first user based on the subject user action in accordance with an embodiment of the present invention.

Figure 7 illustrates an exemplary method of authorization followed by the application by the application server in accordance with an embodiment of the present invention;

Figure 8 illustrates an exemplary flow chart to authorize gesture control in accordance with an embodiment of the present invention;

Figure 9 illustrates an exemplary flowchart of a method of authorization by the application server in accordance with another embodiment of the present invention.

Figure 10A, Figure 10B and Figure 10C illustrate an example operation performed by the user in accordance with an embodiment of the present invention;

Figure 11 is a flowchart illustrating a method of establishing the connection between first and second mobile devices in accordance with an embodiment of the present invention; and

Figure 12 illustrates a block diagram of a system for initiating an operation between a first user and a second user in accordance with an embodiment of the present invention.

Further, skilled artisans will appreciate that elements in the drawings are illustrated for simplicity and may not have been necessarily been drawn to scale. For example, the flow charts illustrate the method in terms of the most prominent steps involved to help to improve understanding of aspects of the present invention. Furthermore, in terms of the construction of the device, one or more components of the device may have been represented in the drawings by conventional symbols, and the drawings may show only those specific details that are pertinent to understanding the embodiments of the present invention so as not to obscure the drawings with details that will be readily apparent to those of ordinary skill in the art having benefit of the description herein.

DETAILED DESCRIPTION:

For the purpose of promoting an understanding of the principles of the invention, reference will now be made to the embodiment illustrated in the drawings and specific language will be used to describe the same. It will nevertheless be understood that no

limitation of the scope of the invention is thereby intended, such alterations and further modifications in the illustrated system, and such further applications of the principles of the invention as illustrated therein being contemplated as would normally occur to one skilled in the art to which the invention relates.

5 It will be understood by those skilled in the art that the foregoing general description and the following detailed description are exemplary and explanatory of the invention and are not intended to be restrictive thereof.

Reference throughout this specification to “an aspect”, “another aspect” or similar language means that a particular feature, structure, or characteristic described in
10 connection with the embodiment is included in at least one embodiment of the present invention. Thus, appearances of the phrase “in an embodiment”, “in another embodiment” and similar language throughout this specification may, but do not necessarily, all refer to the same embodiment.

The terms "comprises", "comprising", or any other variations thereof, are
15 intended to cover a non-exclusive inclusion, such that a process or method that comprises a list of steps does not include only those steps but may include other steps not expressly listed or inherent to such process or method. Similarly, one or more devices or sub-systems or elements or structures or components preceded by "comprises...a" does not, without more constraints, preclude the existence of other
20 devices or other sub-systems or other elements or other structures or other components or additional devices or additional sub-systems or additional elements or additional structures or additional components.

Unless otherwise defined, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this
25 invention belongs. The system, methods, and examples provided herein are illustrative only and not intended to be limiting.

Embodiments of the present invention will be described below in detail with reference to the accompanying drawings.

Figure 1 shows a block diagram of system level environment in accordance with
30 an embodiment of the present invention. The system 100 includes a smart wearable device 102, a mobile device 104, an application server 106 and a database 108. The smart wearable device 102 may be any smart device which is capable of sending commands, instructions to the mobile device 104 and application server 106. The smart wearable device 102 may include, but not limited, to a smart watch, smart fitness bands,

smart shoes, smart glass, smart earphones/ headphones, smart clothing, smart jewellery to name a few. The mobile device 104 is connected to the application server 106 through a first communication network (not shown). The communication network may be one of, but not limited to, WiFi, Near Field Communication or any wired/wireless communication standards. Further, a mobile application is configured in the mobile device 104 to appropriately receive user input actions and to transfer the data, to the application server 106. The mobile application is capable of handling any user related data with the application server 106 and the database 108. The database 108 is configured to securely store data received from smart wearable device 102, mobile device 104 and application server 106. The database 108 is also configured to securely store any data relating to the processed and analyzed, at the application server 106 and the mobile device 104. The database 108 further creates tables to store and separately maintain user related data such as profiles, operations, communications, transactions etc. The users are connected to the application server, forming a network, who can perform any type of operations through their smart wearable device 102 or mobile device 104. Further, the application server 106 also maintains the overall list of users in the network. The application server 106 monitors the network and perform necessary actions/steps when required, based on the policies and rules.

In an embodiment, the smart wearable device 102 is directly connected to the application server 106. In another embodiment, the smart wearable device 102 is connected to the application server 106 through the mobile device (paired device) 104.

In an embodiment, the data is being stored in different clusters of the database 108, pertaining to different user profiles. In another embodiment, the user profile includes data relating to user such as, unique user id, unique user input action, name, age, gender, user status (active, inactive, idle), GPS data, bank account details (bank account number, name of bank, IFSC code, Branch details, payment limit etc), card details (debit/credit card number, expiry date, cvv number, name on card etc), personal identification details (such as, driving license or any identification details accepted by the system), user pattern details (initiation pattern and/or authorization pattern). In an embodiment, each user profile may have an exclusive operation initiation pattern and operation authorization pattern. In one example, the user pattern details may include, but not limited to input actions of the user, such as pin, password, accelerometer/gyro values, gesture pattern values, or any device related sensor values etc. In another embodiment, the exclusive pattern of users ensures the operation to occur in a smooth, sophisticated

and authorized manner. In an embodiment, while connecting to the network for the first time, every user must select and input the operation initiation pattern and operation authentication pattern. These patterns are appropriately stored in the profile data. This data is different from mobile application authentication details. The user can input a
5 unique action for a first time, to validate his identity and to use the subject smart wearable or mobile device, so that, the device will recognize the subject user. In an embodiment, the smart wearable device 102 must receive a unique action (preconfigured by the user), before the start of any process in the smart wearable device 102 or mobile device 104. For example, enabling a gesture-controlled peer detection/authorization
10 when smart wearable device 102 is worn for the first time or smart wearable device 102 is used first time in a day.

In an example, when the operation is a 'Payment transaction', the database 108 has complete payment transaction history of the user, which include, payment received/made by the first user from the second user, amount being transacted, date and
15 time stamp of such payment, the input action performed by the users to authorize such transaction. In another example, the operation is a 'transfer of files'. In an embodiment, the database 108 has complete history of transferring files that include, but not limited to, name of files being transferred, location of transfer of files, size of the files, file type being shared. The database 108 is configured to store the data of the user in a safe and
20 secure way in the dedicated data clusters. The operational details are compared by the application server 106 when any one of the user is initiating any operation with another user, in real-time, in the same network. In another embodiment, the application server 106 compares the authorizations received from both the users and analyzes the patterns of input actions. If found, the authorization details are matching (in real-time), then the
25 transaction is authorized, otherwise, the operation is automatically declined by the application server. The transfer of data from one device (smart wearable device 102 or mobile device 104) to another device may happen by fastest means (some operations does not require, routing the data through server). The direct operations will occur through any one of communication standards that include but not limited to Wi-Fi,
30 Bluetooth.

Figure 2 illustrates a block diagram of exemplary components of smart wearable device in accordance with an embodiment of the present invention. Figure 2 shall be explained in conjunction with the devices referred in Figure 1. The smart wearable device 102 (as referred in Figure 1) includes a controller 202, a communication module

204, a sensor module 206, a power supply unit 208 and an I/O unit 210. The sensor module 206 is further configured with gesture recognition module 212, accelerometer module 214, a gyroscope module 216 and other sensor units 218. The accelerometer module 214 and gyroscope module 216 determine the position and orientation of the smart wearable device 106 respectively. In other words, the accelerometer module 214 measures the displacement of a mass with a position-measuring interface circuit. This measurement is further converted into a digital electrical signal through an analog-to-digital converter (ADC) for digital processing. In addition to that, the acceleration creates a force which is captured by the force-detection mechanism of the accelerometer. Thus, the accelerometer module 214 really measures force, not acceleration and basically measures acceleration indirectly through a force applied to one of the accelerometer's axes (x, y, and z). Whereas, the gyroscope module 216 measures both the displacement of the resonating mass and its frame because of the Coriolis acceleration. The controller 202 is capable of analyzing the values from communication module 204, I/O unit 210 and sensor modules 206 and determining the suitable output. The power supply unit 208 is configured to supply power to various modules and units of the smart wearable device 102. The I/O unit 210 is configured to receive inputs from the user.

In an embodiment, the mobile device 104 is also configured with similar/same set of arrangement. The smart wearable device 102 and mobile device 104 are configured with suitable communication modules 204 which can capable of establishing the connection, through various wired/wireless communication standards, that include but not limited to Bluetooth, Wi-Fi, near field communication. In another embodiment, the smart wearable device 102 and mobile device 104 can work independently, capturing, the sensor information (actions of the user) and transmitting them to the application server 106. In another embodiment, the mobile device 104 is configured with a mobile application which can capable of detecting, monitoring and capturing the sensor module values in real-time. In yet another embodiment, the mobile application is further configured to share the corresponding values of sensor modules 206 with the application server 106 in real-time.

Figure 3A illustrates direct connection between the smart wearable device and application server. Each of the smart wearable device 102₂, 102₄,...102_n is in direct connection with the application server 106. Figure 3B illustrates direct connection between mobile device and application server. Each of the mobile device 104₂, 104₄,...104_n is in direct connection with the application server 106. Figure 3C illustrates

the connection (establishment) between the smart wearable device and application through a mobile device. The smart wearable device 102₂, 102₄...102_n is connected to the application server 106 through the mobile device (paired device) 104₂, 104₄...104_n.

Referring to Figure 4, a flowchart for a method of initiating an operation between
5 a first user and a second user in accordance with an embodiment of the present invention is illustrated. The method 400 includes the step 402 of receiving one or more first input actions from said first user and one or more second input actions from said second user, wherein said one or more first input actions are responsible for validating and authenticating said first user and said one or more second input actions are responsible
10 for validating and authenticating said second user. The input actions may be received using a smart wearable device or a paired mobile device or using both smart wearable device and mobile device. The one or more first and second actions may include, but not limited to, include entering of a unique pin, entering of a unique password, shaking of a smart wearable device or a mobile device in a particular manner, performing gesture
15 actions using the smart wearable device or mobile device or both, capturing of sensor values using the smart wearable device or mobile device or both, performing a particular sequence or pattern of any of the above input actions or combination thereof. Once the input actions are received, one or more first input actions and one or more second input actions respectively are compared with corresponding pre-configured authentication
20 actions for validating and authenticating said first user and said second user respectively in step 404. Both the first user and the second user have pre-configured suitable one or more actions that required for authenticating the identity of the respective user/smart wearable. Further, the pre-configured input actions relating to user identity validation and authentication are fetched from the database and matched with the input actions
25 received from the first and second user respectively. In case the input actions do not match with the pre-configured input actions, the user is prompted to redo the input action again. In case the users are validated and authenticated as a result of the comparison in step 404, one or more third input actions associated with said first user are received in step 406, wherein said one or more third input actions are responsible for triggering
30 initiation of one or more operations with the second user. The one or more operations may include, but not limited to, file and data transfer, payment transaction, communication message transfer, remote access of user devices.

Thereafter, the method 400 includes determining type of one or more operations associated with said one or more third input actions in step 408. The one or more operations to be initiated on detecting or receiving one or more actions are pre-configured. The user may pre-configure and associate a particular operation with a particular action. From example, moving a smart device in a particular manner may be associated with a file transfer operation. Once the operation is determined, the method 400 includes step 410 of receiving one or more fourth input actions from the second user, wherein said one or more fourth input actions are responsible for establishing a connection for initiating one or more determined operations with the first user. The one or more fourth actions from the second user are received in response to establishing a connection to initiate the operations determined in step 408. The one or more third and fourth actions may include, but not limited to, include entering of a unique pin, entering of a unique password, shaking of a smart wearable device or a mobile device in a particular manner, performing gesture actions using the smart wearable device or mobile device or both, capturing of sensor values using the smart wearable device or mobile device or both, performing a particular sequence or pattern of any of the above input actions or combination thereof. Thereafter, it is ascertained in step 412 if the one or more fourth input actions correspond with pre-configured actions required for initiating the one or more determined operations between the first and the second user. On positive ascertaining, the method 400 initiates the one or more determined operations between the first and the second user in step 414. In the event of negative ascertaining in step 414, the second user may be provided with an option to re-input another input action to initiate the operation. In the event of negative ascertaining exceeding pre-defined number of times, the initiation of the operation may be completely declined and a fresh initiation request would be required from the first user.

In an embodiment, the method 400 further includes receiving one or more first and second actions from the first user and the second user respectively for validating and authenticating said first user and said second user respectively; and configuring said one or more first and second actions from the first user and the second user respectively such that the reception of said one or more actions from the first user and the second user respectively validates and authenticates said first user and said second user respectively.

In an embodiment, the method 400 further includes receiving one or more third and fourth actions from the first user and the second user respectively for initiating one or more operations; configuring said one or more third and fourth actions from the first

user and the second user respectively such that execution of said one or more third and fourth actions from the first user and the second user respectively triggers initiation of one or more operations by said first user and said second user respectively.

5 In an embodiment, the one or more input actions by first user and second user are same. In another embodiment, the one or more input actions by first user and second user are different. In yet another embodiment, the one or more actions include at least two actions. The two actions may include actions performed using smart device only, mobile device only or combination of both smart wearable device and mobile device

10 In an embodiment, the method 400 includes determining if one or more fourth input actions matches with the one or more third input actions received from said first user, wherein said matching includes matching at least one or more of the type of input actions, sequence of input actions, particular sequence or pattern of input actions. For example, the sequence of input actions means, performing one or more input action in a sequential manner (one after the other) to initiate an operation. The sequence of input
15 actions includes at least two inputs from the user to initiate the subject operation. Further, the sequence of input actions needs to be performed within the pre-configured time. In one example, inputting a pin and gesture action by the user to be completed within 30 seconds.

20 In an embodiment, the method 400 includes prompting the first user or the second user to perform one or more actions in the event of mis-match with their respective associated actions pre-configured for validating, authenticating and to initiate an operation.

25 In an embodiment, the method 400 includes ascertaining if one or more operations to be initiated require a second level of authorization of the users. On positive ascertaining, the method 400 includes requesting the first user and the second user respectively to perform their respective one more additional actions for second level authentication. The one or more additional actions performed by the first user and second user are matched with the respective pre-configured second level of authorization actions. On matching, the authorization is complete, the operation proceeds further. Such
30 second level of authorization may be involved especially during payment transactions.

In an embodiment, the input action of both users may be same and may be validated by the application server in real-time. In another embodiment, the users can configure a common authorization input action pattern, so that, whenever, the operation to be authorized, both users shall perform the same set of authorization input action

pre-configured input actions) of both smart wearable device and mobile device, at any time. In an embodiment, the smart wearable device or mobile device may send categorized input actions to the application server for effective processing of subject actions. Further, the smart wearable device and/or mobile device may maintain a user
5 configured list of input actions. The users can set one or more input actions, to perform and initiate the operation. In an embodiment, the first user can every time perform at least one of the input action to initiate the operation (for example, payment transaction), with the second user. The payment transaction (transaction details) may include, amount to be transferred/received, reason of transaction, transaction id, to whom the payment to
10 be made (unique user id), user input action (to authenticate the subject transaction, for example, the way in which the mobile device to be rotated). The second user performs its own set of input actions to initiate an operation. In an embodiment, the actions performed by both users are analyzed and accepted by the application server. Then, connection is established. In another embodiment, the second user can perform the same set of input action (the one performed by the first user), to acknowledge and initiate the
15 operation between them. Besides, the application server primarily checks the input action performed by the users, while performing the operation. Following are the steps involving storing the user action pattern for operation initiation and authorization. User can store one or more input actions for operation initialization and operation
20 authorization.

In step 506, the application server checks whether it received a first pattern of input action from the first user. In an embodiment, the first pattern of input action may be entering a 'PASSWORD'. If yes, then the control is transferred to step 508 and the application server stores the first pattern of input action as first set of data. Otherwise,
25 the control is transferred to step 510. In step 510, the application server checks whether it received a second pattern of input action from the first user. In an embodiment, the second pattern of input action may be entering a 'PIN'. If yes, then the control is transferred to step 512 and the application server stores the second pattern of input action as second set of data. Otherwise, the control is transferred to step 514. In step 514, the
30 application server checks whether it received a third pattern of input action from the first user. In an embodiment, the third pattern of input action may be values from accelerometer and/or gyroscope values (shake or motion observed in smart wearable and/or mobile device). If yes, then the control is transferred to step 516 and the application server stores the third pattern of input action as third set of data. Otherwise,

the control is transferred to step 518. In step 518, the application server checks whether it received a fourth pattern of input action from the first user. In an embodiment, the fourth pattern of input action may be 'GESTURE' action of first user. In another embodiment, the same gesture action to be performed by the second user to acknowledge and proceed with the operation (for example, payment process, either transfer or reception of money). If yes, then the control is transferred to step 520 and the application server stores the fourth pattern of input action as fourth set of data. Otherwise, the control is transferred to step 522. In step 522, the application server checks whether it received any of the combination of pattern of input action from the first user. In an embodiment, the pattern of input may include, combination of entering a pin, password, accelerometer/gyro values, gesture input action of first user. If yes, then the control is transferred to step 524 and the application server stores the combinational pattern of input action as fifth set of data. Otherwise, the control is transferred to step 526. In step 526, the application server could not able to recognize the input pattern performed by the first user. In an embodiment, the application server may store a copy of all input actions performed by the users, for every operation. In another embodiment, the application server further shares the operation details and input actions with the second user (the user, to whom the operation is being initiated by the first user).

Figure 6 illustrates a flowchart describing the identification of first user based on the subject user action in accordance with an embodiment of the present invention. The flow chart 600 begins in step 602. In step 602, the application server receives the first input pattern action performed by the first and second user. In an embodiment, the user input actions are captured either by the smart wearable or mobile device. The application server receives the subject input action from the user to initiate an operation. In step 604, the application server analyzes whether first input pattern matches with the preconfigured data of first and second user. In an embodiment, the application server separately compares the preconfigured data (operation initiation input action) with the received data of first user. Similarly, the preconfigured data of second user is being compared with the received data. If the received data is matching with the preconfigured data then the control is transferred to step 606, otherwise, the control is transferred to step 602. In step 606, the application server identifies the first user and second user based on the input actions performed by them and retrieves their profiles.

In step 608, after the retrieval of subject user profiles, the application server also checks with the users, whether they would like to continue the operation in secure manner or authorized manner. If users would like to continue with the authorizations, then the control is transferred to step 612, otherwise, the control is transferred to step 5 610. In step 610, the application server further initiates the operation between the first and second user. In step 612, the application server requests the users to enter the authorization input action pattern. In step 614, the application server further receives the authorization input action pattern from the first and second user, by means of a smart wearable and/or a mobile device. In step 616, the application server analyzes the 10 authorization input action pattern, stored in their respective profiles. If the authorization is successful, then the control is transferred to step 618, otherwise the control is transferred to step 612. In step 618, the application server authenticates and authorizes both users. Further, it establishes and initiates the operation between first and second user in a secure or encrypted way.

15 Figure 7 illustrates an exemplary method of authorization followed by the application by the application server in accordance with an embodiment of the present invention. This is a continuation to Figure 6, when authorization input action pattern is being analyzed by the application server. The flow chart 700 begins in step 702. In step 702, the application server receives the authorization input action from first and second 20 user. In an embodiment, the users may have a same or different authorization input actions. In step 704, the application server checks whether, the input action of users belongs to same action ('PIN'), if so, whether their authorization data stored in their respective profiles are matching with one another. If, the 'PIN' details are matching with their respective preconfigured authorization input action pattern (stored in the database), 25 then the control is transferred to step 706, otherwise, the control is transferred to step 708. In step 706, the application server authorizes both users and initiates the transaction in a safe and encrypted way. In step 708, the application server checks whether, the input action of users belongs to same action ('PASSWORD'), if so, whether their authorization data stored in their respective profiles are matching with one another. If, 30 the 'PASSWORD' details are matching with their respective preconfigured authorization input action pattern (stored in the database), then the control is transferred to step 706, otherwise, the control is transferred to step 710.

In step 710, the application server checks whether, the input action of users belongs to same action ('accelerometer and gyro values'), if so, whether their authorization data stored in their respective profiles are matching with one another. If, the 'accelerometer and gyro values' details are matching with their respective preconfigured authorization input action pattern (stored in the database), then the control is transferred to step 706, otherwise, the control is transferred to step 712.

In step 712, the application server checks whether, the input action of users belongs to same action ('gesture data'), if so, whether their authorization data stored in their respective profiles are matching with one another. If, the 'gesture data' details are matching with their respective preconfigured authorization input action pattern (stored in the database), then the control is transferred to step 706, otherwise, the control is transferred to step 714.

In step 714, the application server checks whether, the input action of users involves sequential in nature. In other words, the input action of the user involves one or more actions (a combination of one or more actions or combination of input actions for initiation and authorization, as in the following table). If, the input sequential data is matching with their respective preconfigured authorization input action pattern (sequentially stored in the database), then the control is transferred to step 706, otherwise, the control is transferred to step 716. In an embodiment, the application server simultaneously checks the profiles of the user and their respective user input action patterns.

The example combinations include,

Combination of Input actions
Password + PIN,
Password + Gesture values,
Password + Accelerometer/gyro values,
PIN + Accelerometer/gyro values,
PIN + Gesture values,
Gesture + Accelerometer/gyro values,
Password + PIN + Accelerometer/gyro values,
Password + PIN + Gesture values,
PIN + Accelerometer/gyro values + Gesture

values
Password + PIN + Accelerometer/gyro values + Gesture values

The application server receives the above possible combination of input actions from the first or second user connected devices (either a smart wearable device, or mobile device or both). The application server further analyzes (above combinations in real-time) and compares the subject input from the users and authorizes them to perform the subject operation. In step 716, the application server checks whether the authorization user input action is different from the one which is stored and preconfigured by the user. In other words, the application server checks whether authorization input action pattern matches with the preconfigured authorization input action pattern of the same user. If, the data is not matching then the control is transferred to step 718, otherwise, the step is transferred to step 722. In step 718, the application server does not authorize the subject operation between the first and second user, since the authorization parameters are not matching with their subject preconfigured authorization patterns as stored in the database. In step 720, the application server requests the subject user (who has not correctly inputted the authorization input action pattern) to re-enter the authorization input action. In step 722, the application server could not able to recognize the input actions performed by the users and hence the authorization of subject operation cannot be performed.

Referring to Figure 8, an exemplary flow chart to authorize gesture control is provided. The flow chart 800 begins in step 802 where a PIN is received from the user. In step 804, it is checked if the authorization PIN entered by the user matches with pre-configured authorization PIN stored in the database. If the PIN entered by the user matches with the pre-configured authorization PIN, the control is transferred to step 806 else the control is transferred back to step 802 where the user is requested to re-enter the PIN again. In step 806, the gesture control is monitored and authorized till the device (for instance, a smart wearable device worn by the user, which is capable of detecting gesture actions of user) is removed from the hand. A time limit may be set for monitoring and authorizing the gesture control, for instance 6 hours/12hours (the duration is counted from the time in which the user wears the smart wearable device). In an embodiment, when the user removes the smart wearable device, the user further has

to enter the PIN once again, whenever he is wearing smart wearable device again. Once the gesture control is authorized, the gesture control information is transferred to the application server in step 808.

Figure 9 illustrates an exemplary flowchart of a method of authorization by the application server in accordance with another embodiment of the present invention. The method 900 begins at step 902 where authorization input action pattern of a plurality of users is detected by the application server (meaning, user inputs the action pattern for operation initialization/authorization, and smart wearable device or mobile device which captures the user action send the information to the application server). In step 904, the detected authorization input action pattern is matched with the preconfigured authorization input action pattern of the same user (the application server also finds if any of the user, who has sent the data to initiate the operation between the first user, and the application server checks for such similar action from other users). If the match is positive (i.e. if other user is found), the control is transferred to step 906 else the control goes back to step 902 where another authorization input action pattern is detected and checked. At step 906, it is checked whether required input action pattern is received from any user for initiating the operation. If not, the control is transfer back to step 904 else the control is transferred to step 908. In step 908, the received input action pattern is matched with the preconfigured input action pattern required for authorizing initiating the operation. If authorized, the control is transferred to step 910 else the control is transferred back to 906 where a new input action pattern may be received from the user. In step 910, it is checked whether a 2nd factor/ level of authorization is required for initiating the operation. If not, the control is transferred to step 912 where the operation is initiated, else the control is transferred to step 914. In step 914, the 2nd factor/ level of authorization pattern is received and authorized. On authorization, the control is transferred to step 912 where the operation is initiated. Once the operation is initiated, a message in respect of the operation is sent to the user devices.

Figure 10A, Figure 10B and Figure 10C illustrate an example operation performed by the user in accordance with an embodiment of the present invention;

In Figure 10A, the first user taps the first mobile device against the second mobile device of second user. In Figure 10B, these mobile devices which are tapped undergo a vibration/shock (internally) for a while and this vibration by means of acceleration is being appropriately captured by accelerometer. The values (signature) of accelerometer of both mobile devices are captured and processed to perform at least one

action by any one of the user. The first mobile application (in both mobile devices) shares these accelerometer values along with the location, gyroscope values and time stamps with application server. The application sever in turn compares these values and initiates a connection process between these mobile devices (first and second mobile devices). In another embodiment, when tapping the mobile phones against each other, the values of accelerometer may be same (at that particular time instant), but opposite in direction (hence, may have a negative value). Further, the mobile application uses gyroscope values to determine the actual angle alignment between first and second mobile devices. Following are example accelerometer values (x, y and z axis components) in an embodiment of the present invention,

Accelerometer axis	First Mobile device	Second Mobile device
Ax	1.2	-1.2
Ay	10.1	-10.1
Az	8.2	-8.2

As shown in above table, the axis values (x,y and z) accelerometer with respect to first mobile device and second mobile device matches with one another, but opposite in direction (negative values).

In Figure 10C, illustrates the communication establishment between first mobile device and second mobile device through the values of accelerometer, gyroscope, location and time stamps, and by simply tapping these mobile devices. The communication module of first mobile device shall connect with the communication module of second mobile device. Further, the communication between these two mobile devices may happen through Bluetooth, Wi-Fi or through any other communication standards.

In yet another embodiment, the application server additionally compares the profile data of first user with that of second user. The application server further analyzes the actions to be performed, operations to be carried out, when the accelerometer values of these mobile devices matches with one another. In another embodiment, the entire operation of connecting a first mobile device with the second mobile device is pre-programmed and stored in the database. The pre-programmed set of

instructions/operations are shared immediately and updated in the mobile applications of first and second mobile devices.

In an embodiment, with the same accelerometer values, the mobile application can be used to perform any number of operations/activities/applications in real-time, that include, but not limited to, transferring of files, payments etc, from one device to another. In another embodiment, a VPA (virtual payment address) of both mobile devices are shared with one another to initiate and perform any payment related activity in their mobile devices. For example, if the first user wants to pay to second user, then the first user opens the mobile application, and taps the first mobile device (of first user) with that of the second mobile device (of second user). The accelerometer values (signature), location and time stamp (of tapping the mobile phones) are validated at the application server (the mobile application shares these data with the application server). The connection between first mobile device and second mobile device is established and the first user can transfer a payment to second user (for example, through VPA). In an embodiment, a common pin/OTP/password/codeword is provided to both the users to securely complete the payment process.

Figure 11 is a flowchart illustrating a method of establishing the connection between first and second mobile devices in accordance with an embodiment of the present invention; The flow chart 1100 begins in step 1102. In step 1102, the mobile application configured in first and second mobile devices monitor the first and second data. The first and second data includes accelerometer data, gyroscope data, time stamp, location of respective mobile devices. In step 1104, the first and second mobile devices are tapped against each other. In step 1106, the mobile application collects the first and second data from first and second mobile devices. In an embodiment, the mobile application detects a change in first data and second data. In step 1108, the mobile application (in both mobile devices) further shares the first and second data having accelerometer data values, gyroscope data values with the time stamp (of tapping the mobile devices), and location of both mobile devices (data) to the application server. In step 1110, the application server compares the first and second data, received from first and second mobile devices in real-time. In step 1112, the first data from first mobile device is matched with the second data from the second mobile device. When the first data is equal to second data then the control is transferred to step 1114, otherwise, the control is transferred to step 1104. In Step 1114, the application server sends notifications to both mobile devices and establishes a connection between first and

second mobile devices, in real-time. Otherwise, the mobile devices should be tapped once again to establish such connection as in step 1104.

Referring to Figure 12, a block diagram system for initiating an operation between a first user and a second user in accordance with an embodiment of the present invention is illustrated. The system 1200 includes a receiving unit 1202 for receiving one or more first input actions from said first user and one or more second input actions from said second user, wherein said one or more first input actions are responsible for validating and authenticating said first user and said one or more second input actions are responsible for validating and authenticating said second user. The input actions are received from the first and second user are analyzed by the sensor modules of the smart wearable devices and mobile devices and communicated by their respective communication modules. On receiving the details pertaining to the input actions, a comparator circuitry 1204 compares the one or more first input actions and one or more second input actions respectively with pre-configured authentication actions for validating and authenticating said first user and said second user respectively. The pre-configured authentication actions corresponding to each user are stored in a database 1206 of system 1200. The receiving unit 1202 is further configured to receive one or more third input actions associated with said first user, wherein said one or more third input actions are responsible for triggering initiation of one or more operations with the second user. A processing unit 1208 is provided for determining type of one or more operations associated with said one or more third input actions. The type of operations to be performed on reception of one or more input actions are pre-configured during the configuration stage. The type of operation and the corresponding input action are stored in database 1206. The receiving unit 1202 is further configured to receive one or more fourth input actions from the second user, wherein said one or more fourth input actions are responsible for establishing a connection for initiating one or more determined operations with the first user. The system 1200 further includes an ascertaining unit 1210 for ascertaining if said one or more fourth input actions matches with pre-configured actions required for initiating said one or more determined operations between the first and the second user. On positive ascertaining, a controlling unit 1212 for initiating said one or more determined operations between the first and the second user on positive ascertaining. An I/O unit 1214 is configured to receive inputs from the user for changing the configuration settings. The system 1200 further includes a power supply unit 1216 configured to supply power to various modules and units of the system 1200. A

communication module 1218 is provided for establishing communication with one or more smart wearable devices, mobile devices.

The actions performed by the user are appropriately captured by the I/O modules, sensor modules configured in both smart wearable and mobile device. In an embodiment, the operation may be initiated by the user, by combined operation of smart wearable and mobile device. In another embodiment, the second user may receive the operation details (incoming request, and other details of the operation) in the mobile device (an exclusive mobile application configured). In another embodiment, the second user must acknowledge and accept the operational details sent by the first user. Upon, acknowledgement, the subject operation is being initiated between the first and second user (for example, transfer of files, amount, payments etc). In yet another embodiment, both the first user and the second user should perform a same or similar set of actions (for example, one action or sequence of actions) at the same time to initiate or establish or authorize the operation. The application server is capable of analyzing the actions performed by the first user and second user, in real-time, further it shall identify the users, and authorize the subject operations (optional) and authorization is user configurable. Also, in case of secure operations (to perform the operations in a secure manner) the application server compares the actions performed by the first user and second user, and if the pre-defined actions (of the users) are matching, then the operation is authorized, otherwise, the application server requests the users to re-perform the appropriate action in a precise way.

The drawings and the foregoing description give examples of embodiments. Those skilled in the art will appreciate that one or more of the described elements may well be combined into a single functional element. Alternatively, certain elements may be split into multiple functional elements. Elements from one embodiment may be added to another embodiment. For example, orders of processes described herein may be changed and are not limited to the manner described herein. Moreover, the actions of any flow diagram need not be implemented in the order shown; nor do all of the acts necessarily need to be performed. Also, those acts that are not dependent on other acts may be performed in parallel with the other acts. The scope of embodiments is by no means limited by these specific examples. Numerous variations, whether explicitly given in the specification or not, such as differences in structure, dimension, and use of material, are possible. Benefits, other advantages, and solutions to problems have been described above with regard to specific embodiments.

Claims

We claim:

1. A method for initiating a task-based operation between a first communication device and a second communication device, the method comprising:
 - receiving, by a first receiving unit (1202), a request to initiate the task-based operation between the first communication device and the second communication device;
 - identifying, by a processing unit (1208), pre-defined instructions pertaining to one or more authentication patterns for initiation of the task-based operation;
 - sending, by a transmitting unit, a request to at least one of the first communication device and the second communication device to generate an authentication pattern to initiate the task-based operation;
 - receiving, by a second receiving unit, authentication pattern generated by at least one of the first communication device and the second communication device, wherein receiving authentication pattern includes of capturing the authentication pattern of vibrations generated upon tapping of the first communication device with the second communication device and receiving the authentication pattern of vibrations, gyroscope values and time stamps of the first communication device and the second communication device;
 - determining, by an authentication engine, the authentication patterns, if received authentication patterns are in accordance with the pre-defined instructions, wherein determining the authentication patterns includes of comparing the authentication pattern of vibrations, gyroscope values and time stamps in accordance with the pre-defined instructions;
 - initiating, by a controlling unit (1212), the task-based operation between the first communication device and the second communication device if received authentication patterns are found to be in accordance with the pre-defined instructions, wherein initiating the task-based operation includes of determining, by a gyroscope module (216), an angle alignment between first and second communication devices using the gyroscope values; and
 - initiating the task-based operation between the first communication device and the second communication device when there is a match of angle alignment between the first and second communication devices.
2. The method as claimed in claim 1, wherein the pre-defined instructions comprises details pertaining to execution of one or more authentication patterns for initiating the task-based

operation, and wherein said details include type of authentication patterns for initiating a task based operation; a sequence of authentication patterns to be executed initiating a task based operation; type of devices to be used for executing authentication patterns for initiating a task based operation; priority order of tasked based operation to be initiated in case of a plurality of task based operations.

3. The method as claimed in claim 1, wherein the task-based operation is initiated between the first communication device and the second communication device if the authentication pattern generated by the first communication device matches with authentication pattern generated by the second communication device, or if the authentication pattern generated by the first communication device and the second communication device matches with a pre-defined authentication pattern.
4. The method as claimed in claim 1, wherein the task-based operation is initiated between the first communication device and the second communication device if the authentication pattern generated by the first communication device and the second communication device are generated within a pre-defined time frame.
5. The method as claimed in claim 1, wherein the task-based operation is initiated between the first communication device and the second communication device if the first communication device and the second communication device are in closed proximity or in contact with each other.
6. The method as claimed in claim 1, wherein the task-based operation is initiated between the first communication device and the second communication device if the authentication pattern generated by the first communication device and the second communication device are generated through devices of same type.
7. The method as claimed in claim 1, wherein the authentication pattern is selected from one or more of: entering of a unique pin, entering of a unique password, shaking of a smart wearable device (102) or a mobile device (104) in a particular manner, performing gesture actions using the smart wearable device (102) or mobile device (104), capturing of sensor values using the smart wearable device (102) or mobile device (104) or both, performing a particular sequence or pattern of any of the above input actions.
8. The method as claimed in claim 1, comprising:
 - accessing profile of the first user and the second user;
 - initiating the task-based operation between the first communication device and the second communication device in accordance with the profile of the user.

9. The method as claimed in claim 1, wherein the task-based operation includes at least one or more of a file and data transfer, payment transaction, communication message transfer, and a remote access.
10. The method as claimed in claim 1, comprising:
 - receiving authentication requests from the first communication device for a first user and from the second communication device for a second user respectively;
 - authenticating the first and the second user respectively in accordance with at least one pre -configured authentication method selected by the first user and the second user, said pre -configured authentication method involving execution of one or more authentication patterns.
11. The method as claimed in claim 10, wherein said one or more authentication patterns are different or similar from authentication patterns for initiation of said task based operation.
12. The method as claimed in claim 1, comprising: defining said pre-defined instructions, wherein defining includes one or more of: defining type of authentication patterns for initiating a task based operation; defining a sequence of authentication patterns to be executed initiating a task based operation; defining type of devices to be used for executing authentication patterns for initiating a task based operation; defining priority order of tasked based operation to be initiated in event of a plurality of task based operations, defining proximal distance or contact values between first communication device and the second communication device for initiating task based operation.
13. A system for initiating a task-based operation between a first communication device and a second communication device, the system comprising:
 - a first receiving unit (1202) for receiving a request to initiate the task-based operation between the first communication device and the second communication device;
 - a processing unit (1208) for identifying pre-defined instructions pertaining to one or more authentication patterns for initiation of the task-based operation;
 - a transmitting unit for sending a request to at least one of the first communication device and the second communication device to generate an authentication pattern to initiate the task-based operation;
 - a second receiving unit for receiving authentication pattern generated by at least one of the first communication device and the second communication device, wherein the second receiving unit for capturing the authentication pattern of vibrations generated upon tapping of the first communication device with the second communication device

and receiving the authentication pattern of vibrations, gyroscope values and time stamps of the first communication device and the second communication device;

an authentication engine for determining the authentication patterns if received authentication patterns are in accordance with the pre-defined instructions, wherein the authentication engine for comparing the authentication pattern of vibrations, gyroscope values and time stamps in accordance with the pre-defined instructions; and

a controlling unit (1212) for initiating the task-based operation between the first communication device and the second communication device if received authentication patterns are found to be in accordance with the pre-defined instructions, wherein the controlling unit (1212) for determining, by a gyroscope module (216), an angle alignment between first and second communication devices using the gyroscope values; and initiating the task-based operation between the first communication device and the second communication device when there is a match of angle alignment between the first and second communication devices.

14. The system as claimed in claim 13, wherein the controlling unit (1212) is configured to initiate task-based operation between the first communication device and the second communication device on meeting one or more of: if the authentication pattern generated by the first communication device matches with authentication pattern generated by the second communication device; if the authentication pattern generated by the first communication device and the second communication device matches with a pre-defined authentication pattern; if the authentication pattern generated by the first communication device and the second communication device are generated within a pre-defined time frame; if the authentication pattern generated by the first communication device and the second communication device are generated through devices of same type, if the first communication device and the second communication device are in closed proximity or in contact with each other.
15. The system as claimed in claim 13, wherein the authentication pattern is selected from one or more of: entering of a unique pin, entering of a unique password, shaking of a smart wearable device or a mobile device in a particular manner, performing gesture actions using the smart wearable device (102) or mobile device (104), capturing of sensor values using the smart wearable device (102) or mobile device (104) or both, performing a particular sequence or pattern of any of the above input actions, wherein the

authentication pattern is performed using at least one of a smart wearable device (102), and a smart phone.

16. The system as claimed in claim 13, wherein the task-based operation includes at least one or more of a file and data transfer, payment transaction, communication message transfer, and a remote access.

METHODS AND SYSTEMS FOR ESTABLISHING AN OPERATION BETWEEN USERS BASED ON IDENTIFICATION OF ONE OR MORE USER ACTIONS

ABSTRACT

The present invention provides methods and system to initiate an operation between a first user and a second user belonging to a same network using one or more user actions. The operation may be initiated by any of the users in a network. The operation that include, but not limited to, transfer of files (photos, songs, videos, documents or any piece of data), exchange of information, payments, or sharing any content over a digital medium. The operation is initiated by means of one or more pre-configured actions performed by the user in real-time, on the smart wearable device or mobile device and/or both. The actions include, but not limited to, entering a pin (numeric), password (alpha-numeric, special), One Time Password (OTP), gesture patterns, sensor values or any combination thereof.

[Figure 4]