

DISTRIBUTED BIOMETRIC COMPARISON FRAMEWORK

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] None.

BACKGROUND

5 [0002] In current methods and systems it is standard practice to obtain a first biometric template from a user so that the user can later authenticate themselves by inputting a second biometric template. The first biometric template is encrypted and stored in a central repository (i.e., a database) or a user's device. The central repository and the user's device can be secured by state-of-the-art encryption
10 techniques. However, the central repository and the user's device serve as a single point of vulnerability for the stored biometric templates. In the case of the central repository, a single security breach (e.g., by a malicious party) will result in thousands or even millions of biometric templates being compromised. This is problematic because the user cannot change their biometric associated with the compromised biometric
15 template.

[0003] Additionally, upon receiving an encrypted second biometric template, the central repository or the user's device must decrypt the encrypted second biometric template. This is because the central repository or the user's device compares the first biometric template and the second biometric template, not the encrypted biometric
20 templates. The encrypted first biometric template that was previously stored is also be decrypted. The decrypted first biometric template is then compared to the decrypted second biometric template. For example, an identification operation, such as a 1:N comparison, will result in the decryption of thousands or even millions of stored templates during the comparison phase. During this phase, the decrypted biometric
25 templates are vulnerable to being compromised since the biometric templates no longer have the security of being encrypted.

[0004] Another problem is that a complete biometric template is encrypted and stored in the central repository or the user's device. If the encrypted complete biometric template were to be compromised by a malicious party, they would have access to the complete biometric template.

- 5 **[0005]** Embodiments of the invention address these and other problems individually and collectively.

SUMMARY

[0006] One embodiment of the invention is directed to a method comprising: receiving, by an authentication node, a plurality of encrypted match values, wherein the
10 plurality of encrypted match values were formed by a plurality of worker nodes that compare a plurality of encrypted second biometric template parts derived from a second biometric template to a plurality of encrypted first biometric template parts derived from a first biometric template; decrypting, by the authentication node, the plurality of encrypted match values resulting in a plurality of decrypted match values; and
15 determining, by the authentication node, if a first biometric template matches the second biometric template using the plurality of decrypted match values.

[0007] Another embodiment of the invention is directed to an authentication node comprising: a processor; a memory device; and a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the
20 processor for implementing a method comprising: receiving a plurality of encrypted match values, wherein the plurality of encrypted match values were formed by a plurality of worker nodes that compare a plurality of encrypted second biometric template parts derived from a second biometric template to a plurality of encrypted first biometric template parts derived from a first biometric template; decrypting the plurality
25 of encrypted match values resulting in a plurality of decrypted match values; and determining if a first biometric template matches the second biometric template using the plurality of decrypted match values.

[0008] Another embodiment of the invention is directed to a method comprising: storing, by a worker node, an encrypted first biometric template part; comparing, by the worker node, the encrypted first biometric template part and an encrypted second biometric template part resulting in an encrypted match value; and transmitting, by the worker node, the encrypted match value to an authentication node.

[0009] Another embodiment of the invention is directed to a worker node comprising: a processor; a memory device; and a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing a method comprising: storing an encrypted first biometric template part; comparing the encrypted first biometric template part and an encrypted second biometric template part resulting in an encrypted match value; and transmitting the encrypted match value to an authentication node.

[0010] These and other embodiments are described in further detail below, with reference to the Figures and Detailed Description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1 shows a block diagram of a system according to an embodiment of the invention.

[0012] FIG. 2 shows a block diagram of an authentication node according to an embodiment of the invention.

[0013] FIG. 3 shows a block diagram of an enrollment node according to an embodiment of the invention.

[0014] FIG. 4 shows a block diagram of a worker node according to an embodiment of the invention.

[0015] FIG. 5 shows a flow diagram illustrating a method of enrolling a biometric template.

[0016] FIG. 6 shows a flow diagram illustrating an alternate method of enrolling a biometric template.

[0017] FIG. 7 shows a flow diagram illustrating a method of authenticating a biometric template.

5 **[0018]** FIG. 8 shows a block diagram of an access system according to an embodiment of the invention.

DETAILED DESCRIPTION

[0019] Prior to discussing embodiments of the invention, some terms can be described in further detail.

10 **[0020]** A “node” may be a device or system attached to or within a network. A node may be used for communicating with other nodes, a communication network, or any other suitable system. A node may generally be located in any suitable location, such as at the location of a user. A node may be in any suitable form. Some examples of nodes include POS or point of sale devices (e.g., POS terminals), cellular phones,
15 personal digital assistants (PDAs), personal computers (PCs), tablet PCs, hand-held specialized readers, wearable devices (e.g., smart watches), vehicles with communication capabilities (e.g., smart cars), home assistant devices, household appliances, household devices (e.g., TV), set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks,
20 security systems, access systems, and the like. In some embodiments, a node can be a user device. In some embodiments, where a node may comprise a smart phone, any suitable smart phone may be used and may include a biometric reader, a processor, and a computer-readable medium. In some embodiments, a node may be an enrollment node, an authentication node, or a worker node.

25 **[0021]** An “enrollment node” may be a node capable of performing enrollment. An enrollment node may allow a user to enroll a biometric template. An enrollment node may be in any suitable form and may generally be located in any suitable location,

such as at the location of a user. In some embodiments, the enrollment node may be a smartphone operated by the user.

[0022] An "authentication node" may be a node capable of performing authentication. An authentication node may allow a user to authenticate a biometric template with a previously stored biometric template. An authentication node may generally be located in any suitable location, such as at the location of a user. Authentication nodes may be in any suitable form. In some embodiments, the authentication node may be a smartphone operated by a user. The authentication node may prompt the user to input a biometric sample when the user has initiated an interaction that requires authentication, such as a transaction with a merchant.

[0023] A "worker node" may be a node capable of performing computations. A worker node may store encrypted biometric template parts. A worker node may be capable of comparing an encrypted first biometric template part to an encrypted second biometric template part. In some embodiments, there may be a plurality of worker nodes. The plurality of worker nodes may be in any suitable configuration. The plurality of worker nodes may be located at any suitable location, such as at a user's residence. In some embodiments, the worker nodes of the plurality of worker nodes may be at different locations from one another. In some embodiments, the plurality of worker nodes may be devices owned by the user. For example, the worker nodes may be the user's laptop computer, the user's smart watch, the user's television, and the user's home assistant device.

[0024] An "application" may be a computer program or piece of software that is used for a specific purpose. An application may be programmed using any suitable computer language such as, for example, Java, C, C++, C#, Objective-C, Swift, or scripting language such as Perl or Python using, for example, conventional or object-oriented techniques. For example, an application may be a payment application configured to perform a payment transaction. In some embodiments, an application may be stored in a memory of a device or node.

[0025] A "user" may include an individual. In some embodiments, a user may be associated with one or more personal accounts and/or user devices.

[0026] A "key" may refer to a piece of information that is used in a cryptographic algorithm to transform input data into another representation. A cryptographic algorithm
5 can be an encryption algorithm that transforms original data into an alternate representation, or a decryption algorithm that transforms encrypted information back to the original data. Examples of cryptographic algorithms may include triple data encryption standard (TDES), data encryption standard (DES), advanced encryption standard (AES), etc.

10 **[0027]** A "public key" may include a cryptographic key that may be obtained and used by an entity to encrypt information. The public key may be designed to be shared and may be configured such that any information encrypted with the public key may only be decrypted using a private key associated with the public key (i.e., a public/private key pair).

15 **[0028]** A "private key" may include a cryptographic key that may be protected and secure. For example, the private key may be securely stored at an entity that generates a public/private key pair and may be used to decrypt any information that has been encrypted with the associated public key of the public/private key pair. A private key may be configured such that it may decrypt information.

20 **[0029]** A "public/private key pair" may include a pair of linked cryptographic keys generated by an entity. The public key may be used for encrypting information to send to the entity or for verifying a digital signature which was supposedly made by the entity. The private key, on the other hand may be used for decrypting received information or applying a digital signature. The public key will usually be authorized by a body known
25 as a certification authority (i.e., certificate authority) which may store the public key in a database and may distribute it to any other entity which requests the public key. The private key may typically be kept in a secure storage medium and will usually only be

known to the entity. However, the cryptographic systems described herein may feature key recovery mechanisms for recovering lost keys and avoiding data loss.

[0030] The term “secure multi-party computation” may refer to a multi-party computation which is secure. Multi-party computation may allow multiple parties to perform a computation amongst themselves. In many cases, in secure multi-party computation, the parties do not share information or other inputs with one another. Secure multi-party computation may allow the parties to jointly compute a function over their inputs while keeping those inputs private. As an example, two parties may wish to know which one of them is more wealthy, without revealing their wealth to each other.

The two parties could use a secure multi-party computation technique, such as garbled circuits, in order to accomplish this.

[0031] A “biometric” may be any human characteristic that is unique to an individual. For example, a biometric may be a person’s fingerprint, voice sample, face, DNA, retina, etc.

[0032] A “biometric reader” may include a device for capturing data from an individual’s biometric sample. Examples of biometric readers may include fingerprint readers, front-facing cameras, microphones, and iris scanners.

[0033] A “biometric sample” may include data obtained by a biometric reader. The data may be either an analog or digital representation of the user’s biometric, generated prior to determining distinct features needed for matching. For example, a biometric sample of a user’s face may be image data. In another example, a biometric sample of a user’s voice may be audio data.

[0034] A “biometric template” or “biometric sample template” may include a file containing distinct characteristics extracted from a biometric sample that may be used during a biometric authentication process. For example, a biometric template may be a binary mathematical file representing the unique features of an individual’s fingerprint, eye, hand, or voice needed for performing accurate authentication of the individual.

[0035] The term “interaction” may be a reciprocal action, effect, or influence. An interaction, for example, could be an exchange or transaction between two or more parties. Examples of transactions can include payment transactions, data access transactions, and location access transactions.

5 **[0036]** A “processor” may refer to any suitable data computation device or devices. A processor may comprise one or more microprocessors working together to accomplish a desired function. The processor may include a CPU comprising at least one high-speed data processor adequate to execute program components for executing user and/or system-generated requests. The CPU may be a microprocessor such as
10 AMD's Athlon, Duron and/or Opteron; IBM and/or Motorola's PowerPC; IBM's and Sony's Cell processor; Intel's Celeron, Itanium, Pentium, Xeon, and/or XScale; and/or the like processor(s).

[0037] A “memory” may be any suitable device or devices that can store electronic data. A suitable memory may comprise a non-transitory computer readable
15 medium that stores instructions that can be executed by a processor to implement a desired method. Examples of memories may comprise one or more memory chips, disk drives, etc. Such memories may operate using any suitable electrical, optical, and/or magnetic mode of operation.

[0038] “Access data” may include any suitable data that can be used to access a
20 resource or create data that can access a resource. In some embodiments, access data may be account information for a payment account. Account information may include a PAN (primary account number or “account number”), payment token, expiration date, card verification values (e.g., CVV, CVV2), dynamic card verification values (dCVV, dCVV2), etc. In other embodiments, access data could include data that
25 can be used to access a location or to access secure data. Such information may be ticket information for an event, data to access a building, transit ticket information, passwords, biometrics or other credentials to access secure data, etc.

[0039] An “authorization request message” may be an electronic message that requests authorization for an interaction. In some embodiments, it is sent to a transaction processing computer and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some
5 embodiments may comply with International Organization for Standardization (ISO) 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a user using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization
10 request message may also comprise additional data elements corresponding to “identification information” including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), a PAN, a payment token, a user name, an expiration date, etc. An authorization request message may also comprise “transaction information,” such as any information associated with a
15 current transaction, such as the transaction amount, merchant identifier, merchant location, acquirer bank identification number (BIN), card acceptor ID, information identifying items being purchased, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0040] An “authorization response message” may be a message that responds to
20 an authorization request. In some cases, it may be an electronic message reply to an authorization request message generated by an issuing financial institution or a transaction processing computer. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval -- transaction was approved; Decline -- transaction was not approved; or Call Center --
25 response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the transaction processing computer) to the merchant's access device (e.g. POS

equipment) that indicates approval of the transaction. The code may serve as proof of authorization.

[0041] An “authorizing entity” may be an entity that authorizes a request. Examples of an authorizing entity may be an issuer, a governmental agency, a document repository, an access administrator, etc. An authorizing entity may operate an authorizing entity computer. An “issuer” may refer to a business entity (e.g., a bank) that issues and optionally maintains an account for a user. An issuer may also issue payment credentials stored on a user device, such as a cellular telephone, smart card, tablet, or laptop to the consumer.

[0042] A “merchant” may typically be an entity that engages in transactions and can sell goods or services, or provide access to goods or services. In some embodiments, a merchant may be a resource provider and may be associated with a resource provider computer.

[0043] An “acquirer” may typically be a business entity (e.g., a commercial bank) that has a business relationship with a particular merchant or other entity. Some entities can perform both issuer and acquirer functions. Some embodiments may encompass such single entity issuer-acquirers. An acquirer may operate an acquirer computer, which can also be generically referred to as a “transport computer”.

[0044] A “processing computer” may be any suitable computation apparatus that can process data. In some embodiments, processing computers may be remotely located with respect to any external computers that may be requesting that data be processed. Exemplary processing computers may include a transport computer, a network computer, and an authorizing entity computer.

[0045] FIG. 1 shows a block diagram of a system 100 comprising a number of components according to an embodiment of the invention. The system 100 comprises an authentication node 102, an enrollment node 104, a plurality of worker nodes 106 including a first worker node 106A, a second worker node 106B, and an Nth worker

node 106C, as well as a resource provider computer 108, a transport computer 110, a network computer 112, and an authorizing entity computer 114.

[0046] The plurality of worker nodes 106 may be in operative communication with the enrollment node 104 and the authentication node 102. The enrollment node 104
5 may be in operative communication with the authentication node 102 and the plurality of worker nodes 106 including the first worker node 106A, the second worker node 106B, and the Nth worker node 106C. Further, the authentication node 102 may be in operative communication with the resource provider computer 108. The resource provider computer 108 may be in operative communication with the transport computer
10 110 which may be in operative communication with the network computer 112. The network computer 112 may be in operative communication with the authorizing entity computer 114.

[0047] For simplicity of illustration, a certain number of components are shown in FIG. 1. It is understood, however, that embodiments of the invention may include more
15 than one of each component. For example, there may be many worker nodes. In one example, there may be five worker nodes, in another, there may be fifty worker nodes.

[0048] The components in system 100 may be in operative communication with each other through any suitable communication channel or communications network. Suitable communications networks may be any one and/or the combination of the
20 following: a direct interconnection; the Internet; a Local Area Network (LAN); a Metropolitan Area Network (MAN); an Operating Missions as Nodes on the Internet (OMNI); a secured custom connection; a Wide Area Network (WAN); a wireless network (e.g., employing protocols such as, but not limited to a Wireless Application Protocol (WAP), I-mode, and/or the like); and/or the like. Messages between the computers,
25 networks, and devices may be transmitted using a secure communications protocols such as, but not limited to, File Transfer Protocol (FTP); HyperText Transfer Protocol (HTTP); Secure Hypertext Transfer Protocol (HTTPS), Secure Socket Layer (SSL), ISO (e.g., ISO 8583) and/or the like.

[0049] The authentication node 102 may be configured to authenticate biometric templates. In some embodiments, the authentication node 102 may be operated by a user. For example, the authentication node 102 may be a smart phone operated by the user, wherein the user initiates an interaction that requires the user to authenticate their identity. In some embodiments, the authentication node 102 may be in operative communication with the resource provider computer 108, the enrollment node 104, and the plurality of worker nodes 106.

[0050] The enrollment node 104 may be configured to enroll biometric templates. In some embodiments, the enrollment node 104 may be operated by the user. For example, the enrollment node 104 may be a laptop computer operated by the user, wherein the user initiates enrollment of a biometric template.

[0051] In some embodiments, the enrollment node 104 and the authentication node 102 may be the same node. For example, the user may enroll a first biometric template using a personal computer and then, later, authenticate a second biometric template using the personal computer. In this way, the personal computer may be the enrollment node 104 during enrollment and may be the authentication node 102 during authentication.

[0052] The first worker node 106A, the second worker node 106B, and the Nth worker node 106C of the plurality of worker nodes 106 may be configured to compare encrypted biometric template parts. In some embodiments, the second worker node 106B and the Nth worker node 106C may have similar characteristics to the first worker node 106A.

[0053] In other embodiments, the first worker node 106A may have previously been an enrollment node 104 or an authentication node 102. For example, the user may enroll a first biometric using a personal computer, and then authenticate a second biometric template using a smart watch as the authentication node 102. In this case, the laptop computer may be first used as the enrollment node 104, but then may be used as the first worker node 106A during authentication. In some embodiments, each

worker node of the plurality of worker nodes 106 may be in operative communication with one another.

[0054] The resource provider computer 108 may be operated by an entity such as a merchant. In some embodiments, the resource provider computer 108 may be a server computer. The resource provider computer 108 may be in operative communication with the authentication node 102 and the transport computer 110. In some embodiments, the resource provider computer 108 may host a resource provider host site that allows users to conduct interactions.

[0055] In some embodiments, the resource provider host site may be a Website. The authentication node 102 may be capable of communicating with the resource provider host site and/or the resource provider computer 108.

[0056] In other embodiments, the resource provider of the resource provider computer 108 may create a resource provider application and may provide the resource provider application to the authentication node 102. The resource provider application may allow the user to initiate an interaction with the resource provider computer 108 via the resource provider application.

[0057] The transport computer 110 may be located between (in an operational sense) the resource provider computer 108 and the network computer 112. The transport computer 110 may be operated by an entity such as an acquirer. An acquirer can maintain an account of any merchants with which users may wish to interact. In some embodiments, the transport computer 110 may be a server computer.

[0058] The network computer 112 may route or switch messages between a number of transport computers including the transport computer 110, and a number of authorizing entity computers including the authorizing entity computer 114. The network computer may be a processing network computer in some embodiments. The processing network computer may be configured to provide authorization services, and clearing and settlement services for payment transactions. A processing network computer may include data processing subsystems, networks, and operations used to

support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions.

- 5 VisaNet™, in particular includes a Visa Integrated Payments (VIP) system which processes authorization requests and a Base II system which performs clearing and settlement services. Furthermore, the payment processing network may include a server computer and may use any suitable wired or wireless telecommunications network, including the Internet. In some embodiments, the processing network
10 computer may forward an authorization request received from the transport computer 110 to the authorizing entity computer 114 via a communication channel. The processing network computer may further forward an authorization response message received from the authorizing entity computer 114 to the transport computer 110.

- [0059]** The authorizing entity computer 114 may be configured to authorize any
15 suitable request, including access to data, access to a location, or approval for a payment. In some embodiments, the authorizing entity computer 114 may be operated by an account issuer. Typically, the issuer is an entity (e.g., a bank) that issues and maintains an account of a user. The account may be a credit, debit, prepaid, or any other type of account.

- 20 **[0060]** FIG. 2 shows a block diagram of an authentication node 102 according to an embodiment of the invention. The authentication node 102 may comprise a processor 102A, a network interface 102B, an output element 102C, an input element 102D, a memory 102E, a biometric reader 102F, and a computer readable medium 102G comprising an encryption module 102G-1, a biometric template division module
25 102G-2, a decryption module 102G-3, and a match result computation module 102G-4, as well as a secure key generator and storage 102H.

[0061] The processor 102A may be operatively coupled to the network interface 102B, the output element 102C, the input element 102D, the memory 102E, the

biometric reader 102F, the computer readable medium 102G, and the secure key generator and storage 102H.

[0062] The network interface 102B may include an interface that can allow the authentication node 102 to communicate with external computers or other nodes. For example, the network interface 102B may comprise a contact, Bluetooth, or Wi-Fi interface. In some embodiments, the network interface 102B may be configured to allow secure transmissions between the authentication node 102 and the enrollment node 104 as well as the plurality of worker nodes 106.

[0063] The output element 102C may comprise any suitable devices that may output data. Examples of the output element 102C may include display screens, speakers, and data transmission devices.

[0064] The input element 102D may include any suitable device capable of inputting data into the authentication node 102. Examples of the input element 102D may include buttons, touchscreens, touch pads, microphones, biometric scanners, etc.

[0065] The memory 102E may be coupled to the processor 102A and may store data, applications, keys, and any other suitable information. The memory 102E may be in the form of one or more memory devices (e.g., RAM, EEPROM, ROM chips), using any suitable mode of data storage. In some embodiments, the memory 102E in the authentication node 102 may also include a secure storage area for storing sensitive data. For example, the memory 102E may be part of or may contain a secure element.

[0066] The computer readable medium 102G may comprise code, executable by the processor 102A. The computer readable medium 102G may contain any number of applications, modules, and code. The computer readable medium 102G may comprise a number of modules such as the encryption module 102G-1, the biometric template division module 102G-2, the decryption module 102G-3, and the match result computation module 102G-4. The computer readable medium 102G may comprise code, executable by the processor 102A for implementing a method comprising: receiving a plurality of encrypted match values, wherein the plurality of encrypted match

values were formed by a plurality of worker nodes that compare a plurality of encrypted second biometric template parts derived from a second biometric template to a plurality of encrypted first biometric template parts derived from a first biometric template; decrypting the plurality of encrypted match values resulting in a plurality of decrypted match values; and determining if a first biometric template matches the second biometric template using the plurality of decrypted match values.

[0067] The encryption module 102G-1 may be capable of encrypting a second biometric template. For example, the encryption module 102G-1 may access the secure key generator and storage 102H to obtain an authentication node public key.

The encryption module 102G-1 may use the authentication node public key to encrypt the second biometric template.

[0068] In other embodiments, the encryption module 102G-1 may be capable of encrypting a plurality of second biometric template parts. The encryption module 102G-1 may encrypt each second biometric template part of the plurality of second biometric template parts separately. For example, if there are three second biometric template parts, the encryption module 102G-1 may encrypt a first part, a second part, and a third part. The encryption module 102G-1 may use any of the described methods of encryption to encrypt the second biometric template parts, for example, encrypting with the authentication node public key. Other methods of encrypting may be through the use of secure multi-party computation. Secure multi-party computation may include techniques such as Yao based protocols, oblivious transfer, etc. The use of garbled circuits are explained by *"How to generate and exchange secrets," Foundations of Computer Science, 1986., 27th Annual Symposium on. IEEE: 162–167* which is hereby incorporated by reference.

[0069] The biometric template division module 102G-2 may be capable of dividing the second biometric template resulting in a plurality of second biometric template parts. The second biometric template may be divided into any suitable number of parts.

[0070] In some embodiments, the second biometric template may be divided into parts based on a fixed policy. For example, a fixed policy may state that if the second biometric template represents the user's face, then the second biometric template may be divided into second biometric template parts relating to facial regions such as eye, nose, mouth, etc. In some embodiments, the fixed policy may be predetermined by an entity. The fixed policy may determine how the second biometric template is divided into parts, based on the type of biometric template (i.e., face, fingerprint, retina, etc.), the number of available worker nodes, a location of the enrollment node 104, network connectivity, etc.

[0071] In some embodiments, the biometric template division module 102G-2 may determine the fixed policy that was used to divide a first biometric template. The second biometric template may be divided in a same or similar way to the first biometric template. In some embodiments, the same fixed policy may be used. In other embodiments, the fixed policy may be stored in the memory 102E.

[0072] In some embodiments, the biometric template division module 102G-2 may divide the second biometric template by splitting the second biometric template into a number of consecutive equally sized parts. For example, if the second biometric template is a face template that is represented by a two-dimensional array, then the two-dimensional array may be divided into 4 equally sized quadrants, resulting in four second biometric templates. In another example, the face template may be a one-dimensional array, wherein the one-dimensional array may be divided into four parts including a first fourth, a second fourth, a third fourth, and a last fourth. This may be done, for example, with the face template array of faceTemplateArr[0100111001010010000001101001], which may be split into faceTemplatePartOne[0100111], faceTemplatePartTwo[0010100], faceTemplatePartThree[1000000], and faceTemplatePartFour[1101001].

[0073] In some embodiments, the biometric template division module 102G-2 may divide the second biometric template through the methods of splitting biometric templates described in US 9,847,997, hereby incorporated by reference.

[0074] The decryption module 102G-3 may be capable of decrypting a plurality of encrypted match values resulting in a plurality of decrypted match values. In some embodiments, the encrypted match values may have been encrypted with an authentication node public key. The decryption module 102G-3 may decrypt the encrypted match values with an authentication node private key, wherein the authentication node public key and the authentication node private key form a public/private key pair. In other embodiments, the decryption module 102G-3 may use secure multi-party computation techniques as described above.

[0075] For example, the authentication node 102 may receive a plurality of encrypted match values from a plurality of worker nodes 106. The plurality of encrypted match values may include any number of encrypted match values. For example, if there are 5 encrypted match values, then the decryption module 102G-3 may decrypt the 5 encrypted match values sequentially, resulting in 5 decrypted match values.

[0076] The match result computation module 102G-4 may be capable of determining if a first biometric template matches a second biometric template using a plurality of decrypted match values.

[0077] In some embodiments, determining if the first biometric template matches a second biometric template using a plurality of decrypted match values may further comprise determining, by the match result computation module 102G-4 a weight associated with each decrypted match value of the plurality of decrypted match values. In some embodiments, the match result computation module 102G-4 may determine an overall authentication threshold. The match result computation module 102G-4 may compare a number of worker nodes that responded to a number of needed responses. The match result computation module 102G-4 may determine if an overall decision based on the weights and the decrypted match values is greater than or equal to the overall authentication threshold. The determination of whether the first biometric template matches the second biometric template is described in more detail below.

[0078] The biometric reader 102F may include a device for capturing data from an individual's biometric sample. Examples of biometric readers may include fingerprint readers, front-facing cameras, microphones, and iris scanners.

[0079] The secure key generator and storage 102H may be secure database that securely stores cryptographic keys as well as generates public/private key pairs. For example, the secure key generator and storage 102H may generate an authentication node public key and an authentication node private key. The secure key generator and storage 102H may securely store the authentication node public key and the authentication node private key. In some embodiments, the authentication node public key may be shared with other devices, such as the enrollment node 104.

[0080] FIG. 3 shows a block diagram of an enrollment node 104 according to an embodiment of the invention. The enrollment node 104 may comprise a processor 104A, a network interface 104B, an output element 104C, an input element 104D, a memory 104E, a biometric reader 104F, and a computer readable medium 104G comprising a first biometric template encryption module 104G-1 and a first biometric template division module 104G-2.

[0081] The network interface 104B may have similar characteristics to the network interface 102B. In some embodiments, the network interface 104B may be configured to allow secure transmissions between the enrollment node 104 and the authentication node 102 as well as the plurality of worker nodes 106.

[0082] The output element 104C may have similar characteristics to the output element 102C. The input element 104D may have similar characteristics to the input element 104D. The memory 104E may be coupled to the processor 104A. The memory 104E may have similar characteristics to the memory 102E.

[0083] The computer readable medium 104G may comprise code, executable by the processor 104A. The computer readable medium 104G may contain any number of applications, modules, and code. The computer readable medium 104G may comprise

a number of modules, such as a first biometric template encryption module 104G-1 and a first biometric template division module 104G-2.

[0084] The first biometric template encryption module 104G-1 may be capable of encrypting a first biometric template. In some embodiments, the first biometric template encryption module 104G-1 may be capable of encrypting the first biometric template using an authentication node public key. In other embodiments, the first biometric template encryption module 104G-1 may be capable of encrypting the first biometric template using secure multi-party computation techniques as described above.

[0085] In other embodiments, the first biometric template encryption module 104G-1 may be capable of encrypting a plurality of first biometric template parts. For example, the plurality of first biometric template parts may include 3 first biometric template parts, i.e., first biometric template part one, first biometric template part two, and first biometric template part three. The first biometric template encryption module 104G-1 may encrypt the first biometric template part one, the encrypt the first biometric template part two, and then encrypt the first biometric template part three. The first biometric template encryption module 104G-1 may be capable of encrypting any number of first biometric template parts.

[0086] The first biometric template division module 104G-2 may be capable of dividing a first biometric template resulting in first biometric template parts. The first biometric template division module 104G-2 may divide the first biometric template using the techniques described above for the biometric template division module 102G-2. In some embodiments, the first biometric template division module 104G-2 may be capable of dividing an encrypted first biometric template.

[0087] The biometric reader 104F may have similar characteristics to the biometric reader 102F.

[0088] FIG. 4 shows a block diagram of a first worker node 106A according to an embodiment of the invention. The first worker node 106A may comprise a processor 106A-1, a network interface 106A-2, an output element 106A-3, an input element 106A-

4, a memory 106A-5, and a computer readable medium 106G comprising an encrypted biometric template division module 106A-6A and an encrypted biometric template part comparison module 106A-6B, as well as a database 106A-7 including an encrypted first biometric template part 106A-7A.

5 **[0089]** The processor 106A-1 may be operatively coupled to the network interface 106A-2, the output element 106A-3, the input element 106A-4, the memory 106A-5, and the computer readable medium 106A-6. The first worker node 106A may be operatively coupled to the database 106A-7.

10 **[0090]** The network interface 106A-2 may have similar characteristics to the network interface 102B. In some embodiments, the network interface 106A-2 may be configured to allow secure transmissions between the worker node 106 and the authentication node 102 as well as the enrollment node 104.

15 **[0091]** The output element 106A-3 may have similar characteristics to the output element 102C. The input element 106A-4 may have similar characteristics to the input element 102D. The memory 106A-5 may be coupled to the processor 106A-1. The memory 106A-5 may have similar characteristics to the memory 102E.

20 **[0092]** The computer readable medium 106A-6 may comprise code, executable by the processor 106A-1. The computer readable medium 106A-6 may contain any number of applications, modules, and code. The computer readable medium 106A-6 may comprise a number of modules, such as the encrypted biometric template division module 106A-6A and the encrypted biometric template part comparison module 106A-6B. The computer readable medium 106A-6 may comprise code, executable by the processor for implementing a method comprising: storing an encrypted first biometric template part; comparing the encrypted first biometric template part and an encrypted
25 second biometric template part resulting in an encrypted match value; and transmitting the encrypted match value to an authentication node.

[0093] The encrypted biometric template division module 106A-6A may be capable of dividing encrypted biometric templates resulting in a plurality of encrypted

biometric template parts. In some embodiments, the encrypted biometric template division module 106A-6A may divide the encrypted biometric template based on the fixed policy. For example, the fixed policy may state that the encrypted biometric template division module 106A-6A may split the encrypted biometric template into thirds
5 and keep the middle third for storage.

[0094] In other embodiments, the encrypted biometric template division module 106A-6A may divide the encrypted biometric template into any suitable number of encrypted biometric templates. For example, if the encrypted biometric template is encBioTemp[f156p69w2bcv6751k613mb8u], then the encrypted biometric template
10 division module 106A-6A may split encBioTemp into three parts of encBioTempPartOne[f156p69w], encBioTempPartTwo[2bcv6751], and encBioTempPartThree[k613mb8u]. In some embodiments, the first worker node 106A may store one of the encrypted biometric template parts. In other embodiments, the encrypted biometric template parts may not be equally sized.

[0095] The biometric template comparison module 106A-6B may be capable of comparing the encrypted first biometric template part 106A-7A to an encrypted second biometric template part. The encrypted biometric template part comparison module 106A-6B may be capable of comparing two encrypted template parts through the use of homomorphic secret sharing. Homomorphic secret sharing may be a type of sharing
20 algorithm in which the secret is encrypted using homomorphic encryption. Homomorphic encryption may be a form of encryption that allows computation on ciphertexts, and generates an encrypted result which, when decrypted, matches the result of the computations as if they had been performed on the plaintext. Homomorphic encryption may be described in more detail in Armknecht, Frederik, et al.
25 "A Guide to Fully Homomorphic Encryption." *IACR Cryptology ePrint Archive* 2015 (2015): 1192, hereby incorporated by reference.

[0096] The database 106A-7 may be a conventional, fault tolerant, relational, scalable, secure database such as those commercially available from Oracle™ or Sybase™. The database 106A-7 may store the encrypted first biometric template part

106A-7A. In some embodiments, the database 106A-7 may store any suitable number of encrypted first biometric template parts.

[0097] ENROLLMENT

[0098] FIG. 5 shows a flow diagram illustrating a method of enrolling a biometric template according to an embodiment of the invention. The method illustrated in FIG. 5 will be described in the context of a user operating nodes owned by the user. It is understood, however, that the invention can be applied to other circumstances (e.g., nodes at various locations, with devices owned by various entities, etc.) in which the ability to enroll and authenticate are needed. Although the steps are illustrated in a specific order, it is understood that embodiments of the invention may include methods that have the steps in different orders. In addition, steps may be omitted or added and may still be within embodiments of the invention.

[0099] Step S502 may occur when the user of the enrollment node 104 initiates the enrollment of a first biometric template. In some embodiments, the user may be prompted to enter a biometric sample. The user may input the first biometric sample using the biometric reader 104H of the enrollment node 104. For example, the user may be prompted to take a photograph of the user's face using a camera on the user's mobile phone.

[0100] At step S502, the enrollment node 104 may generate a first biometric template from the first biometric sample. In some embodiments, features of the first biometric sample may be extracted and used to generate the first biometric template. Features may be characteristics or unique aspects of a biometric sample. For example, a biometric sample of a fingerprint may include features of the ridges, groves, and directions of the lines on the finger. There may be many ways to extract the features of the first biometric sample in order to generate the first biometric template. For example, three different methods may be minutiae based techniques, correlation based techniques, and pattern based techniques.

[0101] At step S504, the enrollment node 104 may divide the first biometric template into a plurality of first biometric template parts. In some embodiments, the first biometric template may be divided into parts based on a fixed policy. For example, a fixed policy may state that if the first biometric template represents the user's face, then the first biometric template may be divided into first biometric template parts relating to facial regions such as eye, nose, mouth, etc. In some embodiments, a biometric template may be divided by any of the methods described above.

[0102] In some embodiments, the fixed policy may be predetermined by an entity before enrollment. The fixed policy may determine how the first biometric template is divided into parts, based on the type of biometric template (i.e., face, fingerprint, retina, etc.), the number of available worker nodes, a location of the enrollment node 104, network connectivity, etc. For example, the enrollment node 104 may determine, using the fixed policy, to divide the first biometric template into five parts if five worker nodes are available.

[0103] At step S506, after dividing the first biometric template into a plurality of first biometric template parts, the enrollment node 104 may encrypt the plurality of first biometric template parts resulting in a plurality of encrypted first biometric template parts. In some embodiments, the plurality of first biometric template parts may be encrypted with an authentication node public key. In other embodiments, the plurality of first biometric template parts may be encrypted using secure multi-party computation techniques, wherein the parties involved may be the enrollment node 104, the authentication node 102, and the plurality of worker nodes 106. The secure multi-party computation techniques may involve any of the previously mentioned secure multi-party computation techniques.

[0104] Next, the enrollment node 104 may respectively transmit the plurality of encrypted first biometric template parts to the plurality of worker nodes 106.

[0105] At step S508, the enrollment node 104 may transmit an encrypted first biometric template part to the first worker node 106A. At step S510, the enrollment

node 104 may transmit an encrypted first biometric template part to the second worker node 106B. At step S512, the enrollment node 104 may transmit an encrypted first biometric template part to the Nth worker node 106C.

[0106] For example, if the plurality of encrypted first biometric template parts includes an encrypted eye template part, an encrypted nose template part, and an encrypted mouth template part, then each different encrypted template part may be sent to a different worker node. The encrypted eye template part may be transmitted to the first worker node 106A (the user's personal computer), the encrypted nose template part may be transmitted to the second worker node 106B (the user's smart watch), and the encrypted mouth template part may be transmitted to the Nth worker node 106C (the user's home assistant device). There may be any number of worker nodes capable of receiving an encrypted first biometric template part from the enrollment node 104.

[0107] In some embodiments, the worker nodes of the plurality of worker nodes 106 may be pre-registered with the enrollment node 104. The user may select to connect the enrollment node 104 with a worker node. For example, the user may be presented with a list of available devices, available via Bluetooth connection, wherein the user may select a device on the list of available devices.

[0108] In other embodiments, there may be a known worker node table stored in the memory 104E of the enrollment node 104. The known worker node table may include a list of worker nodes that the enrollment node 104 has previously connected to. In some embodiments, the user of the enrollment node 104 may add a worker node to the known worker node table. In some embodiments, the known worker node table may include the type of connection with the worker node (i.e., Wi-Fi, Bluetooth, etc.) and may include a device identifier of the worker node.

[0109] In some embodiments, the enrollment node 104 may transmit a connection request message to the first worker node 106A. After receiving the connection request message, the first worker node 106A may generate and transmit a connection response message to the enrollment node 104. The enrollment node 104

may determine if a connection response message has been received from the first worker node 106A. In some embodiments, if the enrollment node 104 receives the connection response message, then the enrollment node 104 may determine that the first worker node 106A is active, or otherwise online. In other embodiments, if the enrollment node 104 does not receive the connection response message, then the enrollment node 104 may determine that the first worker node 106A is not active, or otherwise offline. After determining that the first worker node 106A is active, the enrollment node 104 may transmit the encrypted first biometric template part to the first worker node 106A.

10 **[0110]** In some embodiments, the enrollment node 104 may randomly assign the plurality of encrypted first biometric template parts to the plurality of worker nodes 106 and then respectively transmit the plurality of encrypted first biometric template parts to the assigned worker nodes 106. For example, the encrypted mouth template part may not always be transmitted to the user's home assistant device.

15 **[0111]** After respectively receiving the plurality of encrypted first biometric template parts, the plurality of worker nodes 106 may respectively store the plurality of encrypted first biometric template parts in a plurality of worker nodes 106.

[0112] At step S514, the first worker node 106A may store the encrypted first biometric template part into the database 106A-7. At step S516, the second worker node 106B may store the encrypted first biometric template part into a database. At step S518, the Nth worker node 106C may store the encrypted first biometric template part into a database.

20 **[0113]** Each worker node of the plurality of worker nodes 106 may store a different encrypted first biometric template part of the plurality of encrypted first biometric template parts.

[0114] In some embodiments, the plurality of encrypted first biometric template parts may be transmitted between worker nodes 106 securely to further improve security. The plurality of encrypted first biometric template parts may be transmitted

between worker nodes 106 on a schedule (e.g., once every day) or randomly. For example, the first worker node may transmit the encrypted eye template to the second worker node, the second worker node may transmit the encrypted nose template to the third worker node, and the third worker node may transmit the encrypted mouth
5 template to the first worker node. The respective destination (worker node) of the plurality of encrypted first biometric template parts may be determined by a pattern or randomly.

[0115] In other embodiments, the enrollment node 104 may store at least one encrypted first biometric template part of the plurality of encrypted first biometric
10 template parts. The enrollment node 104 may then later be used as a worker node of the plurality of worker nodes 106.

[0116] FIG. 6 shows a flow diagram illustrating an alternate method of enrolling a biometric template according to an embodiment of the invention. FIG. 6 includes a smartphone 602 that may be the enrollment node 104, a laptop computer 604 that may
15 be the first worker node 106A, a television 606 that may be the second worker node 106B, and a home assistant device 608 that may be the Nth worker node 106C. It is understood that the enrollment node 104, the first worker node 106A, the second worker node 106B, and the Nth worker node 106C may be other devices and are not limited to a smartphone, a laptop computer, a television, and a home assistant device. Although
20 the steps are illustrated in a specific order, it is understood that embodiments of the invention may include methods that have the steps in different orders. In addition, steps may be omitted or added and may still be within embodiments of the invention.

[0117] Step S602 may occur when the user of the smartphone 602 initiates the enrollment of a biometric template. In some embodiments, the user may be prompted
25 to enter a first biometric sample. The user may input the first biometric sample using a biometric reader of the smartphone 602. For example, the user may be prompted to scan the user's fingerprint using a fingerprint scanner on the user's smartphone 602.

[0118] At step S602, the smartphone 602 may generate a first biometric template from the first biometric sample. The generation of the first biometric template from the first biometric sample may be done in the previously described ways.

[0119] At step S604, the smartphone 602 may encrypt the first biometric template resulting in an encrypted first biometric template. In some embodiments, the first biometric template may be encrypted with an authentication node public key. In other embodiments, the first biometric template may be encrypted using secure multi-party computation techniques. Encrypting the first biometric template may be performed in similar ways to the previously described encrypting of the plurality of first biometric template parts.

[0120] At step S606, the smartphone 602 may transmit the encrypted first biometric template to laptop computer 604. At step S608, the smartphone 602 may transmit the encrypted first biometric template to the television 606. At step S610, the smartphone 602 may transmit the encrypted first biometric template to the home assistant device 608.

[0121] In some embodiments, the smartphone 602 may be connected to the plurality of worker nodes 106, including the laptop computer 604, the television 606, and the home assistant device 608, by any suitable means. For example, the user may have previously connected the smartphone 602 to the laptop computer 604 via a Bluetooth connection. The connection may be stored in a table of known worker nodes in the memory of the smartphone 602.

[0122] After receiving the encrypted first biometric template, the plurality of worker nodes 106 may divide the encrypted first biometric template into a plurality of encrypted first biometric template parts.

[0123] At step S612, the laptop computer 604 may divide the encrypted first biometric template into a plurality of encrypted first biometric template parts. At step S614, the television 606 may divide the encrypted first biometric template into a plurality of encrypted first biometric template parts. At step S616, the home assistant device 608

may divide the encrypted first biometric template into a plurality of encrypted first biometric template parts.

[0124] In some embodiments, each of the plurality of worker nodes 106 may divide the encrypted first biometric template into the plurality of encrypted first biometric template parts using a method known to that worker node 106 or a fixed policy. In some embodiments, the encrypted first biometric template may be divided differently at each worker node 106 of the plurality of worker nodes 106.

[0125] For example, the fixed policy of the worker node 106 may be to divide the encrypted first biometric template into a number of parts. The encrypted first biometric template may be divided into three parts, a first third, a second third, and a last third. The encrypted first biometric template may be divided into any number of parts. The worker node 106 may determine to use one of, or some of, the plurality of encrypted first biometric template parts during authentication. In some embodiments, the fixed policy may include any of the previously mentioned methods for dividing an encrypted biometric template.

[0126] The plurality of worker nodes 106 may respectively store the plurality of encrypted first biometric template parts in a memory or database.

[0127] At step S618, the laptop computer 604 may store the encrypted first biometric template into a database. At step S620, the television 606 may store the encrypted first biometric template into a database. At step S622, the home assistant device 608 may store the encrypted first biometric template into a database.

[0128] In some embodiments, a worker node of the plurality of worker nodes 106 may store any number of the encrypted first biometric template parts of the plurality of encrypted first biometric template parts.

[0129] In some embodiments, the plurality of encrypted first biometric template parts may be transmitted between worker nodes 106 securely to further improve security. The plurality of encrypted first biometric template parts may be transmitted between worker nodes 106 on a schedule (e.g., once every day) or randomly.

[0130] In some embodiments, a heartbeat message may be utilized. The heartbeat message may be a message sent from the worker node to the enrollment node 104 or the authentication node 102 that enables the destination to identify if and when the worker node fails or is no longer available. For example, the plurality of worker nodes 106 may transmit a heartbeat message to the enrollment node 104 on a predetermined schedule (i.e., once every 10 minutes, once every hour, etc.). If the enrollment node 104 does not receive the respective heartbeat message during an anticipated arrival period, the enrollment node 104 may determine that the respective worker node may have failed, shutdown, or may generally be unavailable. In some embodiments, the enrollment node 104 may transmit the encrypted first biometric template to the plurality of worker nodes 106 from which the enrollment node 104 has received heartbeat messages from.

[0131] AUTHENTICATION

[0132] FIG. 7 shows a flow diagram of an authentication method according to an embodiment of the invention. The method illustrated in FIG. 7 will be described in the context of a user initiating a transaction with a merchant via the merchant's Website. It is understood, however, that the invention can be applied to other circumstances (e.g., requesting access to a building, a data access transaction, etc.) in which the ability to authenticate is needed. Although the steps are illustrated in a specific order, it is understood that embodiments of the invention may include methods that have the steps in different orders. In addition, steps may be omitted or added and may still be within embodiments of the invention.

[0133] Step S702 may occur when the user of the authentication node 102 initiates an interaction with the resource provider computer 108 or the resource provider host site. In some embodiments, the interaction may be a transaction. For example, the user may select items for purchase on the resource provider host site.

[0134] At step S702, the authentication node 102 may transmit an interaction request message to the resource provider computer 108. The interaction request

message may include an item the user wants to purchase. In some embodiments, the interaction request message may include a request to initiate an interaction. In other embodiments, the interaction request message may be a transaction request message and may include a request to initiate a transaction.

5 **[0135]** At step S704, the resource provider computer 108 may transmit an authentication request message to the authentication node 102. The authentication request message may include a request for access data. In some embodiments, the authentication request message may include a request for the user to authenticate themselves.

10 **[0136]** For example, the resource provider computer 108 may transmit the authentication request message including a request for payment credentials. The user may be able to provide payment credentials that are stored on the authentication node 102 by authenticating the user's identity. For example, the payment credentials may be stored in a secure storage. The payment credentials may be accessed after
15 authentication.

[0137] At step S706, after receiving the authentication request message, the authentication node 102 may prompt the user to authenticate. In some embodiments, the authentication node 102 may prompt the user to enter a second biometric sample. The user may input the second biometric sample using the biometric reader 102F of the
20 authentication node 102. For example, the user may initiate the interaction using an application on the user's smart watch, wherein the user may be prompted to input the second biometric sample for authentication. The user may then scan a fingerprint using a fingerprint scanner on the user's smart watch.

[0138] In some embodiments, the user may have previously enrolled the first
25 biometric template. The second biometric sample may relate to the first biometric sample. For example, if the first biometric sample represents the user's fingerprint, then the user may be prompted to input the second biometric sample that may also represent the user's fingerprint.

[0139] In some embodiments, the user may have previously enrolled multiple biometric templates. For example, the user may have enrolled a forefinger template, a ring finger template, and a facial template. The authentication node 102 may prompt the user to enter any biometric sample relating to biometric templates previously enrolled.

[0140] At step S708, the authentication node 102 may generate a second biometric template from the second biometric sample. The generation of the second biometric template from the second biometric sample may similar to the generation of the first biometric template from the first biometric sample.

[0141] At step S710, the authentication node 102 may encrypt the second biometric template resulting in an encrypted second biometric template. In some embodiments, the second biometric template may be encrypted with an authentication node public key. In other embodiments, the second biometric template may be encrypted using secure multi-party computation techniques. In some embodiments, the second biometric template may be encrypted with the same key as the first biometric template. The authentication node 102 may encrypt the second biometric template using any of the previously discussed methods.

[0142] At step S712, the authentication node 102 may transmit the encrypted second biometric template to the first worker node 106A. At step S714, the authentication node 102 may transmit the encrypted second biometric template to the second worker node 106B. At step S716, the authentication node 102 may transmit the encrypted second biometric template to the Nth worker node 106C.

[0143] In some embodiments, there may be a known worker node table stored in the memory 104E of the authentication node 102. The known worker node table may include a list of worker nodes that the authentication node 102 has previously connected to. In some embodiments, the user of the authentication node 102 may add a worker node to the known worker node table. In some embodiments, the known

worker node table may include the type of connection with the worker node (i.e., Wi-Fi, Bluetooth, etc.) and may include a device identifier of the worker node.

[0144] At step S714, after receiving the encrypted second biometric template, the plurality of worker nodes 106 may respectively divide the encrypted second
5 biometric template into a plurality of encrypted second biometric template parts. In some embodiments, each of the plurality of worker nodes 106 may divide the encrypted second biometric template, using a method known to that worker node 106 or a fixed policy. In some embodiments, the plurality of worker nodes may derive their individual encrypted second biometric template parts. The individual encrypted second biometric
10 template parts may be derived from the encrypted second biometric template.

[0145] At step S718, the first worker node 106A may divide the encrypted second biometric template into the plurality of encrypted second biometric template parts. At step S720, the second worker node 106B may divide the encrypted second biometric template into the plurality of encrypted second biometric template parts. At step S722,
15 the Nth worker node 106C may divide the encrypted second biometric template into the plurality of encrypted second biometric template parts.

[0146] In some embodiments, the encrypted second biometric template may be divided differently at each worker node of the plurality of worker nodes 106. In other embodiments, the plurality of worker nodes 106 may respectively divide the encrypted
20 second biometric template in the same way as the plurality of worker nodes 106 respectively divided the encrypted first biometric template. In other embodiments, the encrypted second biometric template may be divided in any of the ways previously described.

[0147] In some embodiments, after step S708 (generating the second biometric
25 template), the authentication node 102 may divide the second biometric template into a plurality of second biometric template parts. In some embodiments, the second biometric template may be divided into parts based on the fixed policy. In other embodiments, the authentication node 102 may divide the second biometric template

into a plurality of second biometric template parts in a same or similar way to how the enrollment node 104 divided the first biometric template into the plurality of first biometric template parts.

[0148] In some embodiments, after the authentication node 102 divides the second biometric template into the plurality of second biometric template parts, the authentication node 102 may encrypt the plurality of second biometric template parts resulting in a plurality of encrypted second biometric template parts. In some embodiments, the plurality of second biometric template parts may be encrypted with an authentication node public key. In other embodiments, the plurality of second biometric template parts may be encrypted using secure multi-party computation techniques. The plurality of second biometric template parts may be encrypted in the same way as the plurality of first biometric template parts, step S506.

[0149] In some embodiments, after encrypting the plurality of second biometric template parts, the authentication node 102 may transmit the plurality of encrypted second biometric template parts to the plurality of worker nodes 106.

[0150] The plurality of worker nodes 106 may then respectively compare the plurality of encrypted second biometric template parts and the plurality of encrypted first biometric template parts resulting in a plurality of encrypted match results.

[0151] At step S724, the first worker node 106A may compare the encrypted second biometric template part and the encrypted first biometric template part resulting in an encrypted match value. At step S726, the second worker node 106B may compare the encrypted second biometric template part and the encrypted first biometric template part resulting in an encrypted match value. At step S728, the Nth worker node 106C may compare the encrypted second biometric template part and the encrypted first biometric template part resulting in an encrypted match value.

[0152] In some embodiments, the plurality of encrypted second biometric template parts and the plurality of encrypted first biometric template parts may not be decrypted. In other embodiments, they may be compared in an encrypted domain

through the use of homomorphic comparison techniques. For example, the worker node 106 may have previously stored an encrypted fingerprint template part and now may have an encrypted second fingerprint template part. The worker node 106 may compare the encrypted fingerprint template part and the encrypted second fingerprint
5 template part.

[0153] In some embodiments, the comparison of an encrypted second biometric template part and an encrypted first biometric template part may result in an encrypted match value of the plurality of encrypted match values. The encrypted match value, when decrypted into a decrypted match value, may be in a fixed range (i.e., 1-100). In
10 other embodiments, the encrypted match value, when decrypted into the decrypted match value, may be a decision (i.e., "match," "no match"). The encrypted match value may be based on a threshold of each worker node 106 of the plurality of worker nodes 106. The threshold may be predetermined based on false acceptance rates, false rejection rates, acceptance rates, rejection rates, etc. In some embodiments, each
15 worker node of the plurality of worker nodes 106 may have a different threshold. Some worker nodes may have a more stringent threshold while others are more relaxed.

[0154] The comparison of the encrypted second biometric template part and the encrypted first biometric template part may be done through the use of homomorphic comparison as described above.

20 **[0155]** After comparing the encrypted first biometric template parts to the encrypted second biometric template parts, the plurality of worker nodes 106 may transmit the plurality of encrypted match values to the authentication node 102.

[0156] At step S730, the first worker node 106A may transmit the encrypted match value to the authentication node 102. At step S732, the second worker node
25 106B may transmit the encrypted match value to the authentication node 102. At step S734, the Nth worker node 106C may transmit the encrypted match value to the authentication node 102.

[0157] In some embodiments, the authentication node 102 may receive a number of encrypted match values (k') less than or equal to the number of worker nodes (N). For example, there may be ten worker nodes, but worker node five is offline, therefore the authentication node 102 may receive nine encrypted match values rather than ten.

5 **[0158]** At step S736, after receiving the plurality of encrypted match values, wherein the plurality of encrypted match values were formed by the plurality of worker nodes 106 that compare the plurality of encrypted second biometric template parts derived from the second biometric template to the plurality of encrypted first biometric template parts derived from the first biometric template, the authentication node 102
10 may decrypt the plurality of encrypted match values, resulting in a plurality of decrypted match values. In some embodiments, an authentication node private key may be used to decrypt the plurality of encrypted match values. In other embodiments, the plurality of encrypted match values may be decrypted using secure multi-party computation techniques.

15 **[0159]** At step S738, the authentication node 102 may determine if the first biometric template and the second biometric template match using the plurality of decrypted match values. In some embodiments, the authentication node 102 may determine if the first and second biometric templates match based on the following equation:

20 **[0160]** $m_1*s_1 + m_2*s_2 + m_3*s_3 + \dots + m_{k'}*s_{k'} \geq s$, where $k' \geq K$ and $s = f(K, k')$

where $m_1, m_2, \dots, m_{k'}$ may be weights assigned to the decrypted match value from each worker node, $s_1, s_2, \dots, s_{k'}$ may be the decrypted match values of the plurality of decrypted match values, s may be the overall authentication threshold, $+$ may be a decision fusion operator, $*$ may be an operator to combine the weight of each node with
25 the associated decrypted match value, k' may be a number of worker nodes that the authentication node 102 received the encrypted match value from, and K may be a number of needed responses.

[0161] In some embodiments, a weight may be a value. The weights may be different for each worker node 106. The authentication node 102 may determine the weight associated with each decrypted match value of the plurality of decrypted match values. In some embodiments, the authentication node 102 may determine the weights
5 based on the associated worker node 106. For example, the authentication node 102 may determine a small weight to be associated with the decrypted match value of the associated worker node if the associated worker node does not have an accurate comparison method. The weights may be determined on a relative or on an absolute scale.

10 **[0162]** $s_1, s_2, \dots, s_k$ may be the decrypted match values. For example, s_1 may be the decrypted match value associated with the first worker node, while s_3 may be the decrypted match value associated with the third worker node.

[0163] The overall authentication threshold (s) may be a value used to determine if the first biometric template matches the second biometric template. The overall
15 authentication threshold may be the threshold of the authentication node 102. In some embodiments, the authentication node 102 may determine the overall authentication threshold. In other embodiments, the overall authentication threshold may be predetermined. In yet other embodiments, the overall authentication threshold may be the same between different authentication nodes. For example, the overall
20 authentication threshold may be equal to a value of 75 whether the authentication node 102 is the user's personal computer or is the user's smart watch.

[0164] The operator to combine the weight of each node with the associated decrypted match value may combine the weights and the decrypted match values in any suitable way. In some embodiments, the operator to combine may perform the
25 multiplication operation. For example, the weights and the decrypted match values may be numerical values, in which case the operator to combine may multiply the weight of each node with the associated decrypted match value. In other embodiments, the operator to combine may be an arithmetic combination of multiplication and addition. In some embodiments, the decrypted match values may be binary or integer values.

[0165] The decision fusion operator may combine the weight and decrypted match value of one worker node with the weight and decrypted match value of another worker node. In some embodiments, the decision fusion operator may perform the addition operation. In other embodiments, the decision fusion operator may be an arithmetic combination of multiplication and addition.

[0166] For example, there may be four decrypted match values of "1," "1," "1," and "0," where, in this example, a value of 1 indicates a match and a value of 0 does not indicate a match. The four decrypted match values may be associated with the weights of 0.4, 0.1, 0.3, and 0.2, respectively. Applying the equation: $(0.4) * (1) + (0.1) * (1) + (0.3) * (1) + (0.2) * (0) \geq s$. Which is $0.8 \geq s$. If s is less than 0.8 then the authentication node 102 may determine that the first biometric template matches the second biometric template.

[0167] The authentication node 102 may determine if $k' \geq K$. The authentication node 102 may compare the number of worker nodes that responded (k') to the number of needed responses (K). For example, the authentication node 102 may require receiving at least K encrypted match values and may receive k' encrypted match values. If the authentication node 102 determines that $k' \geq K$ then the authentication node 102 may proceed with determining if the second biometric template matches the first biometric template. If the authentication node 102 determines that $k' < K$ then the authentication node 102 may re-perform the previous steps until a predetermined criteria, such as until $k' \geq K$ or until a certain amount of time has passed. For example, the number of needed responses may be six, but the number of worker nodes that responded may be four. In this case, the authentication node 102 may determine that $k' < K$ and then wait until the authentication node 102 receives at least two more encrypted match values from different worker nodes. In some embodiments, the number of needed responses may be predetermined by an entity.

[0168] The left hand side of the equation (i.e., $m_1*s_1 + m_2*s_2 + m_3*s_3 + \dots + m_k*s_k$) may be the overall decision. The authentication node 102 may determine if the overall decision based on the weights and the decrypted match values is greater than or

equal to the overall authentication threshold (s). If the overall decision is greater than or equal to the overall authentication threshold, then the authentication node 102 may determine that the second biometric template and the first biometric template match. In some embodiments, after the authentication node 102 determines that the second
5 biometric template and the first biometric template match, the authentication node 102 may determine to authenticate the interaction.

[0169] If the overall decision is less than the overall authentication threshold, then the authentication node 102 may determine that the second biometric template and the first biometric template do not match. In some embodiments, after the authentication
10 node 102 determines that the second biometric template and the first biometric template do not match, the authentication node 102 may determine to not authenticate the interaction. In other embodiments, the authentication node 102 may prompt the user to reenter the second biometric sample.

[0170] In some embodiments, determining if the first biometric template and the second biometric template match may result in an overall match result. In some
15 embodiments, the overall match result may be the overall decision. In other embodiments, the overall match result may be a "yes match" or a "no match." The overall match result may be a value or characters that relate to the overall decision. For example, the overall decision may be a value of 95 (out of 100), then the overall match
20 result may be 95, or may be "yes match."

[0171] At step S740, after determining if the first biometric template and the second biometric template match, the authentication node 102 may generate an authentication response message. The authentication response message may include the overall match result and access data. In some embodiments, the authentication
25 response message may be in response to the authentication request message.

[0172] At step S742, the authentication node 102 may transmit the authentication response message to the resource provider computer 108.

[0173] At step S744, after receiving the authentication response message, the resource provider computer 108 may generate an authorization request message. The resource provider computer 108 may transmit the authorization request message to the transport computer 110. The authorization request message may include access data.
5 In some embodiments, the authorization request message may also include the overall match result.

[0174] In other embodiments, the authentication node 102 may generate the authorization request message and then transmit the authorization request message to the resource provider computer 108. In some embodiments, the authentication node
10 102 may transmit the authorization request message to the authorizing entity computer 114 via the resource provider computer 108, the transport computer 110, and the network computer 112.

[0175] At step S746, the transport computer 110 may transmit the authorization request message to the network computer 112. In some embodiments, the transport
15 computer 110 may be associated with the resource provider computer 108 and may manage authorization requests on behalf of the resource provider computer 108.

[0176] At step S748, the network computer 112 may transmit the authorization request message to the authorizing entity computer 114.

[0177] The network computer 112, the transport computer 110, and the
20 authorizing entity computer 114 may operate suitable routing tables to route authorization request messages using payment credentials, payment tokens, and/or other suitable identifiers.

[0178] At step S750, after receiving the authorization request message, the authorizing entity computer 114 may determine to authorize the interaction.

[0179] The authorizing entity computer 114 may issue and manage a payment
25 account to the user which in some embodiments may be associated with the authentication node 102. The authorizing entity computer 114 may also represent a verification entity that may choose to verify the user. In some embodiments, the

authorizing entity computer 114 may be able to authorize transactions that involve the payment account. Before authorizing a transaction, the authorizing entity computer 114 may authenticate access data, such as payment credentials, received in the authorization request message, and check that there is available credit or funds in an associated payment account. The authorizing entity computer 114 may also receive and/or determine a risk level associated with the transaction, and may weigh the risk when deciding whether or not to authorize the interaction.

[0180] At step S752, after approving or declining the interaction, the authorizing entity computer 114 may generate an authorization response message communicating the approval or decline of the transaction.

[0181] At steps S754-S760, the authorizing entity computer 114 may transmit the authorization response message to the authentication node 102 via the network computer 112, the transport computer 110, and the resource provider computer 108. The authentication node 102 may receive the authorization response message from the authorizing entity computer 114.

[0182] In some embodiments, at the end of the day or at any other suitable period of time after the authorization response message is received by the resource provider associated with the resource provider computer 108, a clearing and settlement process may be performed between an acquirer associated with the transport computer 110, the entity associated with the network computer 112, and an authorizing entity represented by authorizing entity computer 260.

[0183] After the authentication node 102 receives the authorization response message, the authentication node 102 may proceed with the interaction with the resource provider computer 108 if the authorizing entity computer 114 authorized the interaction.

[0184] FIG. 8 shows a block diagram of an access system 800 comprising a number of components according to an embodiment of the invention. The access system 800 comprises the authentication node 102, the enrollment node 104, the

plurality of worker nodes 106 including the first worker node 106A, the second worker node 106B, and the Nth worker node 106C, as well as a central server computer 802, and an access authorizing computer 804.

[0185] The authentication node 102, the enrollment node 104, and the plurality of worker nodes 106 may be in operative communication as described in FIG. 1. Further, the authentication node 102 may be in operative communication with the central server computer 802, which may be in operative communication with the access authorizing computer 804.

[0186] For simplicity of illustration, a certain number of components are shown in FIG. 8. It is understood, however, that embodiments of the invention may include more than one of each component. For example, there may be many worker nodes. In one example, there may be five worker nodes, in another, there may be fifty worker nodes.

[0187] The components in the access system 800 may be in operative communication with each other through any suitable communication channel or communications network. Suitable communications networks may be any one and/or the combination of the following: a direct interconnection; the Internet; a Local Area Network (LAN); a Metropolitan Area Network (MAN); an Operating Missions as Nodes on the Internet (OMNI); a secured custom connection; a Wide Area Network (WAN); a wireless network (e.g., employing protocols such as, but not limited to a Wireless Application Protocol (WAP), I-mode, and/or the like); and/or the like. Messages between the computers, networks, and devices may be transmitted using a secure communications protocols such as, but not limited to, File Transfer Protocol (FTP); HyperText Transfer Protocol (HTTP); Secure Hypertext Transfer Protocol (HTTPS), Secure Socket Layer (SSL), ISO (e.g., ISO 8583) and/or the like.

[0188] The authentication node 102, the enrollment node 104, the plurality of worker nodes 106 including the first worker node 106A, the second worker node 106B, and the Nth worker node 106C have been described previously and need not be repeated here.

[0189] The central server computer 802 may be a server computer. In some embodiments, the user of the authentication node 102 may initiate an interaction with the central server computer 802 via the authentication node 102. In some embodiments, the central server computer 802 may generally be located at a building.

5 The central server computer 802 may control access to the building via locks on the entryways.

[0190] The access authorizing computer 804 may be a server computer operated by an entity associated with the central server computer 802. The access authorizing computer 804 may be capable of authorizing access. For example, the access

10 authorizing computer 804 may be capable of authorizing a user to enter a building.

[0191] In some embodiments, a user may initiate an interaction with the central server computer 802 via the authentication node 102. The interaction may be a request to enter a building. For example, the user may have previously entered a first biometric template with an enrollment node 104, such as a computer supplied by their landlord.

15 When attempting to enter the building, the user may scan their fingerprint on an authentication node 102, such as a fingerprint scanner on a security device at the building. The security device may divide the entered second biometric template (template of the user's fingerprint) into a plurality of second biometric template parts. The security device may then encrypt the plurality of second biometric template parts

20 and may transmit the plurality of encrypted second biometric template parts to a plurality of worker nodes throughout the building. The plurality of worker nodes may respectively compare the two encrypted biometric template parts and then transmit the resulting encrypted match values to the security device. The security device may then transmit an authorization request message to a central computer which may route the

25 authorization request message to the access authorizing computer 804. The access authorizing computer 804 may determine to authorize the user to enter the building. The access authorizing computer 804 may transmit an authorization response message to the authentication node 102, via the central server computer 802. The authentication node 102 may then unlock a door to the building if the user was authorized to enter.

The user may then enter the building if their fingerprint matches a fingerprint stored in the plurality of worker nodes and they have been authorized to enter.

[0192] In some embodiments, the security device may determine to allow the user to enter the building without generating the authorization response message, depending on if only authentication is needed. In other embodiments, both authentication and authorization may be needed.

[0193] Embodiments of the invention have a number of advantages. One advantage is that once the biometric templates are encrypted, there is no need to decrypt the biometric templates. This is highly beneficial over current systems in which the stored encrypted biometric template must be decrypted in order to be compared with a decrypted second biometric template. Since the encrypted biometric templates are not decrypted they cannot be easily compromised by malicious parties.

[0194] Further, the plurality of worker nodes that store the encrypted biometric template parts need not be trusted since the biometric templates are never decrypted. A worker node of the plurality of worker nodes does not have access to the plain text biometric template or the biometric template parts.

[0195] Embodiments of the invention have another advantage of dividing the biometric templates into encrypted biometric template parts. Since no worker node ends with the whole encrypted biometric template, even if the worker node were malicious, that node would only be able to compromise a biometric template part rather than the whole biometric template.

[0196] Further, if the malicious party were to try to use a compromised biometric template part to perform authentication they would be unable to do so, since the authentication node determines if the number of responses is greater than or equal to the number of needed responses. The malicious party would have to compromise many worker nodes, even though they would have no knowledge of which worker nodes to compromise. Furthermore, each worker node of the plurality of worker nodes may

have different encryption keys, thus making it even more difficult to compromise many worker nodes.

[0197] Another advantage is that this framework allows for having heterogeneous biometric comparison algorithms being used by different worker nodes. Each worker node and even the authentication node may be oblivious to the underlying algorithms being used, as long as they can use a normalized output/score from the comparison function.

[0198] It should be understood that any of the embodiments of the present invention can be implemented in the form of control logic using hardware (e.g. an application specific integrated circuit or field programmable gate array) and/or using computer software with a generally programmable processor in a modular or integrated manner. As used herein, a processor includes a single-core processor, multi-core processor on a same integrated chip, or multiple processing units on a single circuit board or networked. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement embodiments of the present invention using hardware and a combination of hardware and software.

[0199] Any of the software components or functions described in this application may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C, C++, C#, Objective-C, Swift, or scripting language such as Perl or Python using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions or commands on a computer readable medium for storage and/or transmission, suitable media include random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a compact disk (CD) or DVD (digital versatile disk), flash memory, and the like. The computer readable medium may be any combination of such storage or transmission devices.

[0200] Such programs may also be encoded and transmitted using carrier signals adapted for transmission via wired, optical, and/or wireless networks conforming to a variety of protocols, including the Internet. As such, a computer readable medium according to an embodiment of the present invention may be created using a data
5 signal encoded with such programs. Computer readable media encoded with the program code may be packaged with a compatible device or provided separately from other devices (e.g., via Internet download). Any such computer readable medium may reside on or within a single computer product (e.g. a hard drive, a CD, or an entire computer system), and may be present on or within different computer products within a
10 system or network. A computer system may include a monitor, printer, or other suitable display for providing any of the results mentioned herein to a user.

[0201] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with
15 reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0202] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

20 **[0203]** As used herein, the use of "a," "an," or "the" is intended to mean "at least one," unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
 - 2 receiving, by an authentication node, a plurality of encrypted match
 - 3 values, wherein the plurality of encrypted match values were formed by a plurality of
 - 4 worker nodes that compare a plurality of encrypted second biometric template parts
 - 5 derived from a second biometric template to a plurality of encrypted first biometric
 - 6 template parts derived from a first biometric template;
 - 7 decrypting, by the authentication node, the plurality of encrypted match
 - 8 values resulting in a plurality of decrypted match values; and
 - 9 determining, by the authentication node, if the first biometric template
 - 10 matches the second biometric template using the plurality of decrypted match values,
 - 11 and wherein the method further comprises:
 - 12 encrypting, by the authentication node, the second biometric template
 - 13 resulting in an encrypted second biometric template; and
 - 14 transmitting, by the authentication node, the encrypted second biometric
 - 15 template to the plurality of worker nodes, wherein the plurality of worker nodes derive
 - 16 the encrypted second biometric template parts.
- 1 2. The method of claim 1, wherein determining, by the authentication
- 2 node, if the first biometric template matches the second biometric template using the
- 3 plurality of decrypted match values, further comprises:
 - 4 determining, by the authentication node, a weight associated with each
 - 5 decrypted match value of the plurality of decrypted match values;
 - 6 determining, by the authentication node, an overall authentication
 - 7 threshold;
 - 8 comparing, by the authentication node, a number of worker nodes that
 - 9 responded to a number of needed responses; and

10 determining, by the authentication node, if an overall decision based on
11 the weights and the decrypted match values is greater than or equal to the overall
12 authentication threshold.

1 3. The method of claim 1 further comprising:
2 transmitting, by the authentication node, if the first biometric template
3 matches the second biometric template, an authorization request message to an
4 authorizing entity computer; and
5 receiving, by the authentication node, an authorization response message
6 from the authorizing entity computer.

1 4. An authentication node comprising:
2 a processor;
3 a memory device; and
4 a computer-readable medium coupled to the processor, the computer-
5 readable medium comprising code executable by the processor for implementing a
6 method comprising:
7 receiving a plurality of encrypted match values, wherein the plurality of
8 encrypted match values were formed by a plurality of worker nodes that compare a
9 plurality of encrypted second biometric template parts derived from a second biometric
10 template to a plurality of encrypted first biometric template parts derived from a first
11 biometric template;
12 decrypting the plurality of encrypted match values resulting in a plurality of
13 decrypted match values; and
14 determining if the first biometric template matches the second biometric
15 template using the plurality of decrypted match values, and wherein the method further
16 comprises:
17 encrypting the second biometric template resulting in an encrypted second
18 biometric template; and

19 transmitting the encrypted second biometric template to the plurality of
20 worker nodes, wherein the plurality of worker nodes derive the encrypted second
21 biometric template parts.

1 5. The authentication node of claim 4, wherein the step of
2 determining, if the first biometric template matches the second biometric template using
3 the plurality of decrypted match values, further comprises:
4 determining a weight associated with each decrypted match value of the
5 plurality of decrypted match values;
6 determining an overall authentication threshold;
7 comparing a number of worker nodes that responded to a number of
8 needed responses; and
9 determining if an overall decision based on the weights and the decrypted
10 match values is greater than or equal to the overall authentication threshold.

1 6. The authentication node of claim 4, wherein the method further
2 comprises:
3 transmitting if the first biometric template matches the second biometric
4 template, an authorization request message to an authorizing entity computer; and
5 receiving an authorization response message from the authorizing entity
6 computer.

1 7. A method comprising:
2 storing, by a worker node, an encrypted first biometric template part;
3 comparing, by the worker node, the encrypted first biometric template part
4 and an encrypted second biometric template part resulting in an encrypted match value;
5 and
6 transmitting, by the worker node, the encrypted match value to an
7 authentication node, and wherein the method further comprises:

8 receiving, by the worker node, an encrypted second biometric template,
9 wherein the authentication node encrypts a second biometric template resulting in the
10 encrypted second biometric template; and
11 deriving, by the worker node, from the encrypted second biometric
12 template, the encrypted second biometric template part.

1 8. The method of claim 1, wherein the first biometric template is a
2 binary mathematical file containing distinct characteristics of a biometric sample.

1 9. The method of claim 1, wherein the first biometric template is
2 derived from a face of a user.

1 10. The method of claim 1, wherein the decrypted match values are
2 within a fixed range.

1 11. The method of claim 10, wherein the fixed range is from 1-100.

1 12. The method of claim 1, wherein the decrypted match values
2 comprise match or no match values.