the at least one issuer, a consent or a dissent for authenticating second payment transaction using the one or more authentication techniques; and identifying, by at least one processor, the one or more authentication techniques having the consent of the at least one issuer. In some non-limiting embodiments or aspects, the one or more authentication techniques comprise at least one of a first type of authentication technique, and one or more issuer authentication techniques.

[0012] In some non-limiting embodiments or aspects, providing the one or more authentication techniques to the application comprises: computing, by at least one processor, a risk value for each of the determined one or more authentication techniques based on at least one of merchant information, issuer information, and user information; and modifying the consent of the determined one or more authentication techniques based on the computed risk value, wherein the determined one or more authentication techniques are provided to the application. In some non-limiting embodiments or aspects, facilitating the processing of the second payment transaction request when the one of the one or more authentication techniques selected by the user is a first type of authentication technique comprises: receiving, by at least one processor, the second payment transaction request including at least a device attestation response, a payment amount, a second token, merchant information, payment card information, a payment authentication request, and a payment authorization request; and generating, by at least one processor, a third token upon processing the payment authentication request and the payment authorization request, wherein the generated third token is provided to the device for authenticating a third payment transaction.

[0013] In some non-limiting embodiments or aspects, provided is a payment server for authenticating digital transactions, comprising: at least one processor; and a memory communicatively coupled to the at least one processor, wherein the memory stores processor instructions, which, upon execution, causes the at least one processor to: receive a device registration request and a device attestation response including at least a device integrity status from a device; in response to the device registration request, provide a device registration response to the device, based on validation of the device integrity status; receive a first payment transaction request and an enrolment request from the device via an application to authenticate a second payment transaction request using a first type of authentication technique; and enroll the device to the first type of authentication technique and provide a second token to

departing from the spirit and scope of the subject matter described herein. Furthermore, the method may be implemented in any suitable hardware, software, firmware, or combination thereof.

[0080] In some non-limiting embodiments or aspects, and at step (301), the payment server (105), receives the device registration request and the device attestation response including at least the device integrity status from the device (102). In some non-limiting embodiments or aspects, the SDK (102B) in the device (102) provides to the second server (104) the device attestation request including at least the first token, upon receiving the device registration request including at least the merchant information from the application (102A). The first token or nonce is generated in the device (102) by the SDK (102B) using one or more cryptographic techniques. In some non-limiting embodiments or aspects, the first token or nonce is generated by the payment server (105) and provided to the SDK (102B) in the device (102). A person skilled in the art may appreciate the use of one or more pseudo random number generation techniques for generating the first token. For example, the first token may be “R2Rra24fVm5xa2Mg”.

[0081] In some non-limiting embodiments or aspects, SDK (102B) in the device (102) receives, from the second server (104), the device attestation response including at least the device integrity status based on the first token. For example, the device attestation response (401) shown in Fig. 4A includes a timestamp of the response generated by the second server (104) (e.g., timestamp), the first token or nonce, a name of the application (102A) (e.g., PackageName), a cryptographic hash or digital certificate associated with the application (102A) and/or with the device (102) indicative of the integrity of the application (102A) (e.g., CertificateDigestSha256), and the device integrity status (e.g., ProfileMatch and Integrity).

[0082] The device (102), upon receiving the device attestation response (401) from the second server (104), provides the device registration request and the device attestation response (401) via the SDK (102B). For example, the device registration request may include at least one of a merchant card alias, the application identification value, a merchant customer identification value, the mobile number associated with the device (102), $\text{encrypted}_{\text{v_static_public_key}}$ ($\text{signed}_{\text{device_private_key}}$ (first token, device_public_key, device key type, device key size, the device attestation response (401))), and a v_static_public_key reference identification value, where $\text{encrypted}_{\text{v_static_public_key}}$ indicates an encryption using one or more cryptographic

include specialized processing units such as integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

[0100] The processor (702) may be disposed in communication with one or more input/output (I/O) devices (not shown) via an I/O interface (701). The I/O interface (701) may employ communication protocols/methods such as, without limitation, audio, analog, digital, monaural, RCA, stereo, IEEE-1394, serial bus, universal serial bus (USB), infrared, PS/2, BNC, coaxial, component, composite, digital visual interface (DVI), high-definition multimedia interface (HDMI), RF antennas, S-Video, VGA, IEEE 802.1 n /b/g/n/x, Bluetooth®, cellular (e.g., code-division multiple access (CDMA), high-speed packet access (HSPA+), global system for mobile communications (GSM), long-term evolution (LTE), WiMax®, or the like), etc.

[0101] Using the I/O interface (701), the computer system (700) may communicate with one or more I/O devices. For example, an input device (710) may be an antenna, keyboard, mouse, joystick, (infrared) remote control, camera, card reader, fax machine, dongle, biometric reader, microphone, touch screen, touchpad, trackball, stylus, scanner, storage device, transceiver, video device/source, etc. An output device (711) may be a printer, fax machine, video display (e.g., cathode ray tube (CRT), liquid crystal display (LCD), light-emitting diode (LED), plasma, Plasma display panel (PDP), Organic light-emitting diode display (OLED), or the like), audio speaker, etc.

[0102] In some non-limiting embodiments or aspects, the computer system (700) is connected to the service operator through a communication network (709). The processor (702) may be disposed in communication with the communication network (709) via a network interface (703). The network interface (703) may communicate with the communication network (709). The network interface (703) may employ connection protocols including, without limitation, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/Internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. The communication network (709) may include, without limitation, a direct interconnection, e-commerce network, a peer to peer (P2P) network, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, Wi-Fi®, etc. Using the network interface (703) and the communication network (709), the computer system (700) may communicate with the one or more service operators.

modifying the consent of the determined one or more authentication techniques based on the computed risk value, wherein the determined one or more authentication techniques are provided to the application.

12. The method of claim 8, wherein facilitating the processing of the second payment transaction request when the one of the one or more authentication techniques selected by the user is a first type of authentication technique comprises:

receiving, by at least one processor, the second payment transaction request including at least a device attestation response, a payment amount, a second token, merchant information, payment card information, a payment authentication request, and a payment authorization request; and

generating, by at least one processor, a third token upon processing the payment authentication request and the payment authorization request, wherein the generated third token is provided to the device for authenticating a third payment transaction.

13. A payment server for authenticating digital transactions, comprising:

at least one processor; and

a memory communicatively coupled to the at least one processor, wherein the memory stores processor instructions, which, upon execution, causes the at least one processor to:

receive a device registration request and a device attestation response including at least a device integrity status from a device;

in response to the device registration request, provide a device registration response to the device, based on validation of the device integrity status;

receive a first payment transaction request and an enrolment request from the device via an application to authenticate a second payment transaction request using a first type of authentication technique; and

enroll the device to the first type of authentication technique and provide a second token to the device based on a result of the first payment transaction request, wherein the second token is used for authenticating the second payment transaction request.