[0157] In some non-limiting embodiments or aspects, the transaction handler receives a transaction from the merchant system with payment card information that is transmitted via a gateway. Transaction service provider system 502 determines types and kinds of information needed to complete the transaction, and keys are exchanged with issuer system 510 (e.g., issuing bank, etc.). In such an example, instead of requiring multiple messages between the POS device 508, transaction service provider system 502, acquirer system 504, and issuer system 510, the POS device 508 includes an MPC that to encrypt with an asymmetric key and sends to acquirer system 504 which includes an HSM.

[0158] In some non-limiting embodiments or aspects, merchant system 506 and acquirer system 504 share an MPC with multiple devices from multiple transactions and reduce the need for HSMs by using a shared HSM to access their transactional data in a remote data repository. When the KEK is used on data at rest, or in a KMS, the KEK is wrapped with a public key of the host, transaction service provider system 502, and have no risk of exposure of a key in the clear, or alternatively, multiple keys, a KEK could remove the HSM from the software at the front, transaction service provider system 502 receives it in the MPC node with two MPCs, unwrap and use to move it in a different database that can be shared with issuer system 510.

[0159] In some non-limiting embodiments or aspects, both the merchant and the issuer use MPC would have two separate nodes. A transaction could come from merchant system 506 through software defined MPC for secure cryptoprocessor 516 of transaction service provider system 502 (e.g., an HSM of a transaction handler). In one example, the transaction includes a pin block, transaction service provider system 502 provides the 2nd MPC to decrypt the pin block, while the first is with merchant system 506, which can then encrypt with another key and send it down to issuer system 510. Merchant system 506 could then decrypt using an MPC and send back a response.

[0160] Multiple instances of MPC servers are available, and in some non-limiting embodiments or aspects, could have more than one instance, such that a quorum is considered when multiple instances of a server are used (e.g., a predetermined number of MPC server instances). To have a quorum does not require multiple instances of the server to communicate to the original office. The quorum may eliminate the original office.

[0161] When the original office is in a foreign country, an instance of an MPC Server in the original office can be denied communications, thereby, effectively placing the data in a protected condition for an indefinite period of time. For example, key management services that are initially provided for multiple colocation key centers including a foreign data center, are denied to the foreign data center when colocation is compromised, to protect the data by making it inaccessible while determining a threat. Domestic processing may keep things separate while using MPC to transmit the encrypted data back and forth. In such an example, a local MPC encrypts a portion then the global data center decrypts the rest of it. If using multiple instances of a server, then only 2 of 3 may be needed to decrypt the domestic data, or alternately, other ratios of server instances or configurations depending on requirements and risks.

[0162] Remote data storage service 208 is configured to decrypt based on a predetermined number of MPC responses of the first entity. Remote data storage service 208 is configured to transmit one or more MPC requests to a plurality of MPC servers (e.g., instances, virtual copies, etc.) associated with entity system 204. As such, accuracy of a security measure is increased, and the number of computations and exposure of security keys is reduced.

[0163] In some non-limiting embodiments or aspects, remote data storage service 208 determines an MPC after receiving one or more MPC responses from the plurality of MPC servers, wherein the stored encrypted data is decrypted based on the received MPC responses satisfying the predetermined number of MPC responses.

[0164] In some non-limiting embodiments or aspects, stored encrypted data is decrypted based at least partially on the second MPC response that has been generated by a second server controlled by an entity controlling a transaction terminal, an issuer bank, or an acquirer bank, a merchant, a transaction handler, that is configured to generate and transmit a second MPC response.

[0165] Referring now to FIG. 6, FIG. 6 is a flowchart of a non-limiting embodiment or aspect of a process 600 for removing a data repository encrypted with an MPC of an entity. In some non-limiting embodiments or aspects, one or more of the steps of process 600 for removing a data repository may be performed (e.g., completely, partially, and/or the like) by cloud provider system 602 (e.g., one or more devices of cloud provider system 602), first entity system 604 (e.g., one or more devices of first entity system 604), communication network 606 (e.g., one or more devices of communication network 606), remote data storage service 608 (e.g., one or more