PSI in SEV Design Document

The PSI is composed of the Client and the Server, and the connection between them.

1. The Client:
   1. hardcode the assigned according to the client id session key for encrypting data sent to the server.
   2. Establish gRPC for connect the client and the server.
   3. Divide data into piece blocks for the VM disk limitation
   4. Encrypt blocks
   5. Send encrypted blocks to the server.
   6. Receive encrypted result from the server
   7. Decrypted and verify the result.
   8. The server will collect the result of all pieces of blocks as the final result.

1. The Server: (VM is already running in the server machine and the IP address is configured and known by the Client.)
   1. get a set of session keys for different clients for encrypting data
   2. a message receiver in SEV VM, receiving the message and save it in the Queue.
   3. decrypt received data with the key corresponding to the client Id.
   4. Sort the coming data.
   5. Intersection of two sorted data.
   6. Encrypt the result with the key corresponding to the client id
   7. Send the result to the client by using gRPC.

1. The connection between the client and the server is established between the client and the VM running in the server directly by using gRPC.
2. Message PSI message{

String clientId;

Bytes data; (encrypted data)

Uint32 size;

}

“data” is composed of 16 bytes mac and ciphertext.

Using byteArrayBuffer as the plain data struct.