Decentralized Password Generator Using Cryptography

Our system is generating OTP in a random way that can be said in a decentralized manner using cryptography. Details of this are explained below:

Clients: There are 4 clients in our system(We can increase as much as we want). Every client generates a unique code that is then sent to the server. Then the server writes a text file named vault.txt.

Before going further, I'm explaining another thing. The vault.txt is generating a unique hash code after every change inside it. By this, we can record every track in a cryptographic way.

Our system is Both centralized and decentralized. The Clients are generating the unique codes on their own side using their logic. This part is decentralized. Then that code/key is sent to the server. The server then stores them in Vault.txt and from this password is generated randomly. This part can be called centralized.

One extra facility is added to our system. Even though every client's logic is known to the hacker, hackers can't know the API-generating code that is done from the server side. We've also added this facility. By this, Clients and API generate different keys and it'll increase the security of our system.

There is a possibility to improve our system in a large manner. We can make our system fully decentralized which is pretty tough. We can also increase the alternative like the API key-generating process.

As our system generates OTP, We can implement this system for KDC(KEY DISTRIBUTION CENTER). There are lots of sites where the user is provided a single sign-in facility. We can implement this facility in a very efficient way for KDC.