Every Hour 100$ is getting depleted.   
  
Probable reasons -

* web exploits and bots - There are common web exploits and bots that may affect availability, compromise security, or consume excessive resources. If that is the case then we should implement a WAF service that can protect the system against specific ip’s that are responsible for exploits attacks.
* There may be issues on session ttl where login session ttl is very less, due to this user needs to login multiple times in a time interval and otp service is getting called for each login session.
* There may be issues at the system level where multiple otps are getting triggered for a single login call.

What to do -

* We will need to check on the third party sms provider sms analytics part, we can get which mobile number otp service is getting called frequently and we can check the same on system logs if their login activity is valid or analyze sms logs and check for which mobile numbers otp is getting sent multiple times in a short interval.
* We can implement WAF system and add rules to check which ip’s are triggering specific apis to generate otp.
* We can increase access-token ttl time so that users will be logged in for a longer time and otp service will not get called multiple times.