When I create an EC2 instance, I either use an AWS-generated key pair. The **public key** from that key pair is stored on the EC2 instance, and I keep the **private key** (usually a .pem file) on my local machine. When I SSH into the instance, the EC2 server uses the public key to verify that my private key is valid. This ensures secure, key-based authentication.