How do server confirms that balaji is a good guy and not a bot?

like server, client (browser) will also generate a key and cert and it happens backend.

All these setup is called as PKI. public key Infrastructure

Naming Analogy:-

Certificate (public key) *.crt
*.pem.

server.crt

server.pem.

client.crt

client.pem.

Certificate (private key) *.key
*.key.pem.

server.key

server-key.pem

client-key

client-key.pem