8.3.3 Remote user to a cloud service:

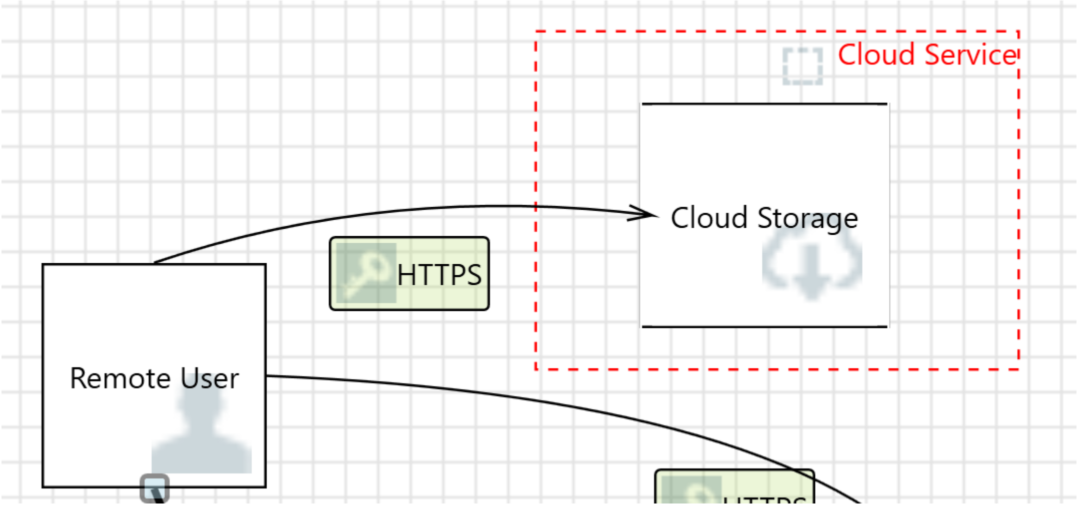

Figure 8: Remote user to cloud service

In Figure 8, remote user access to cloud service is depicted. This could also be an internal user-to-cloud service. Listed below are potential threats and corresponding measures to mitigate them.

Spoofing of Destination Data Store Cloud Storage

Category:	Spoofing
Description:	Cloud Storage may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Cloud Storage. Consider using a standard authentication mechanism to identify the destination data store.
Mitigation:	User authentication will be done through Single Sign On (SSO) with MFA enabled for all external connections (Grassi et al., 2017).

The Cloud Storage Data Store Could Be Corrupted

Category:	Tampering
Description:	Data flowing across HTTPS may be tampered with by an attacker. This may lead to the corruption of Cloud Storage. Ensure the integrity of the data flow to the data store.

Mitigation:	Strong encryption techniques will protect data at rest and in transit. Sensitive data will be encrypted before storing it in the cloud, and data will be transmitted over secure channels using protocols like HTTPS.

Data Store Denies Cloud Storage Potentially Writing Data

Category:	Repudiation
Description:	Cloud Storage claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Mitigation:	User authentication will be done through Single Sign On (SSO) with MFA enabled for all external connections (Grassi et al., 2017).

Data Flow HTTPS Is Potentially Interrupted

Category:	Denial Of Service
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Mitigation:	A Cloud Access Security Broker (CASB) can be used to avoid this attack. A zero-trust approach can be implemented to enhance the security of the CASB solution. This model operates under the assumption that all devices and users are untrusted and must be verified before being granted access to resources. CASB can authenticate and authorise access to such resources (Trend Micro, 2023).