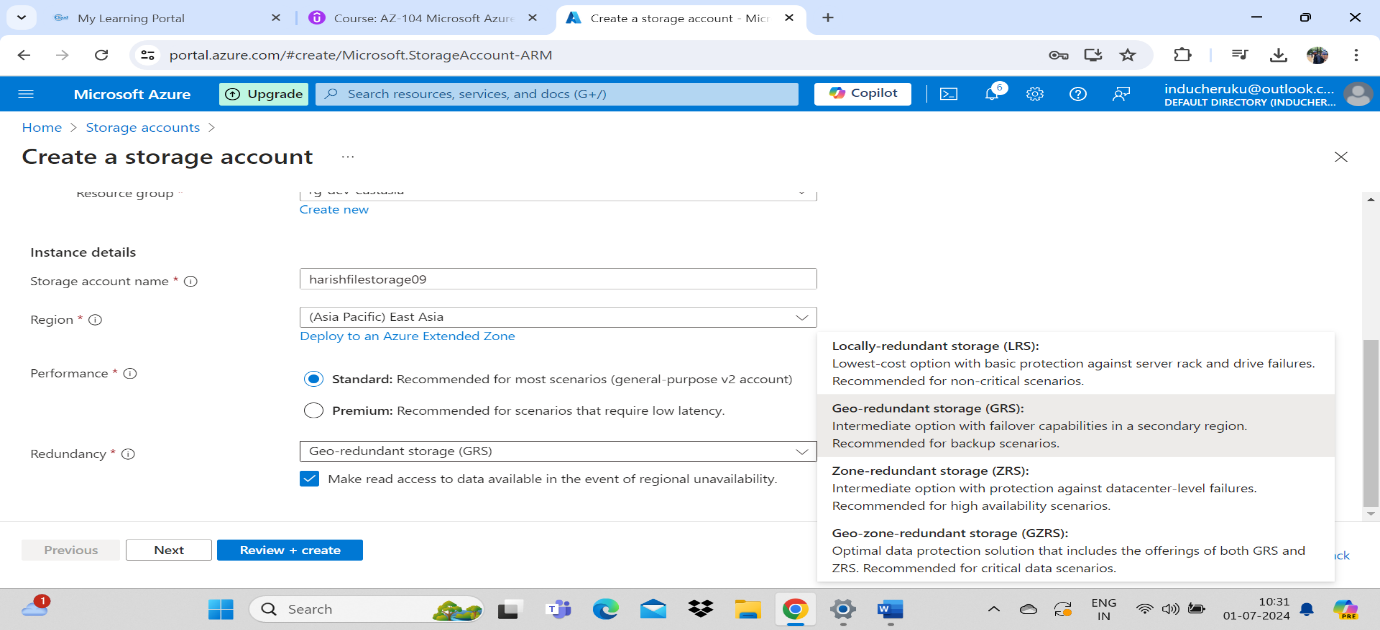
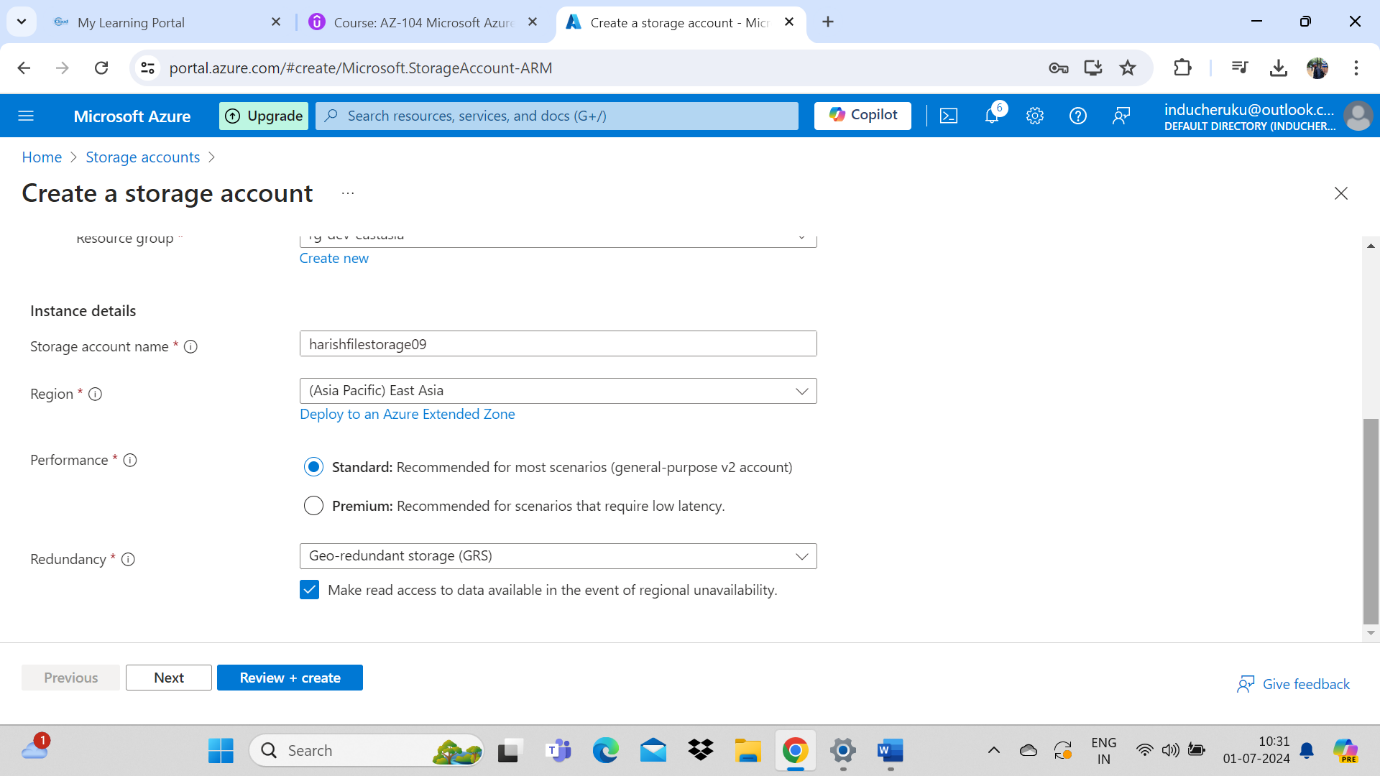
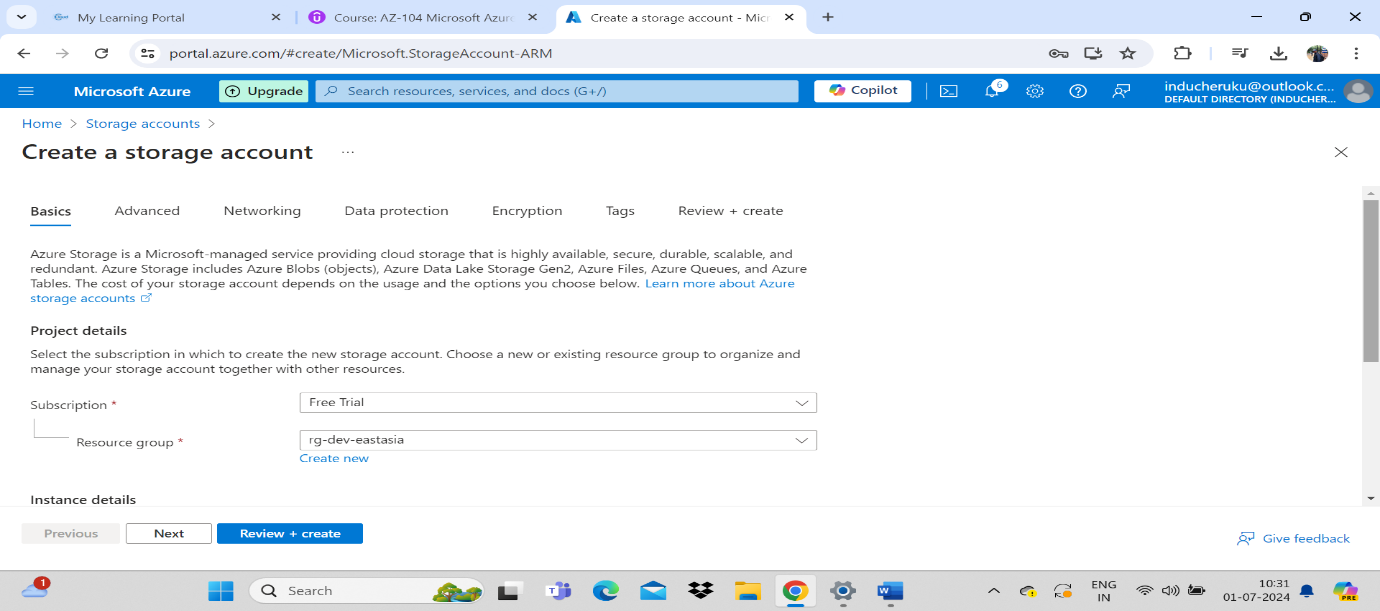
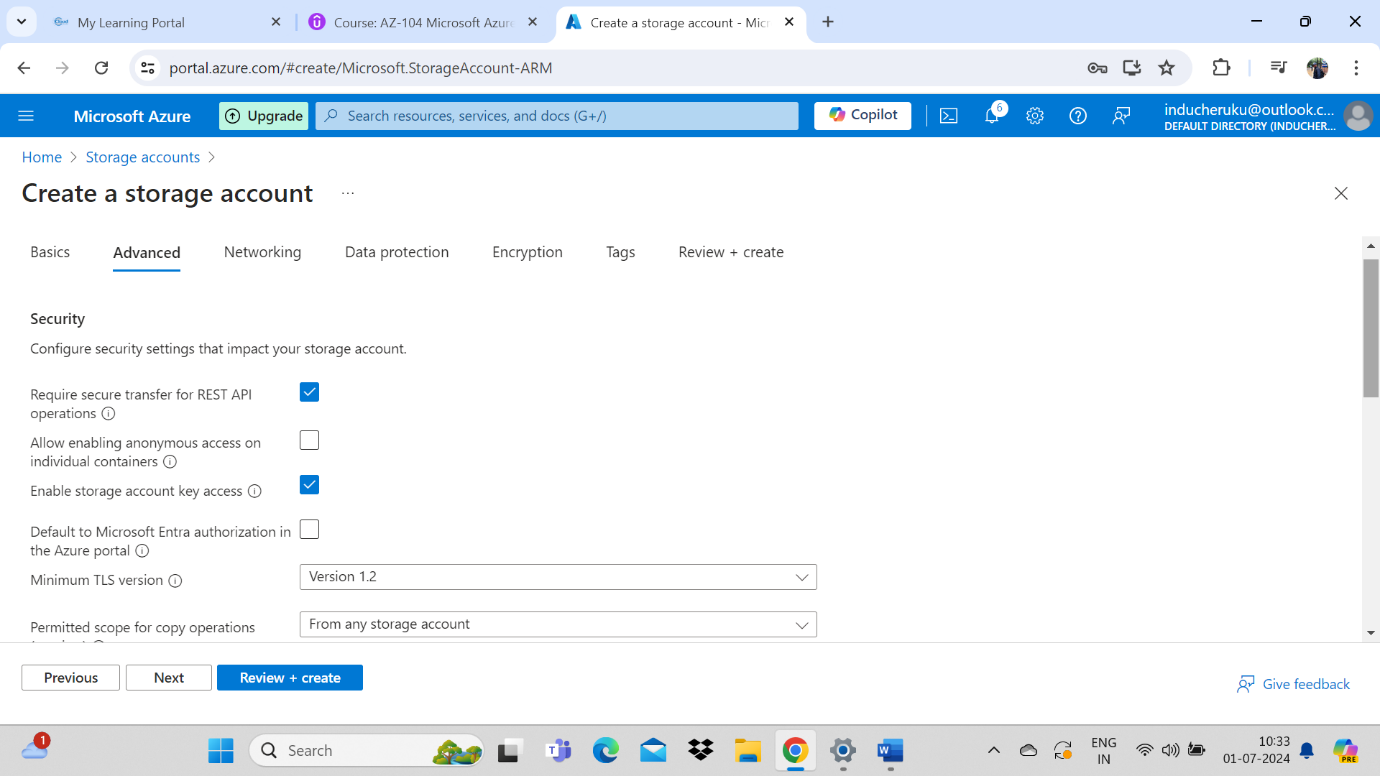
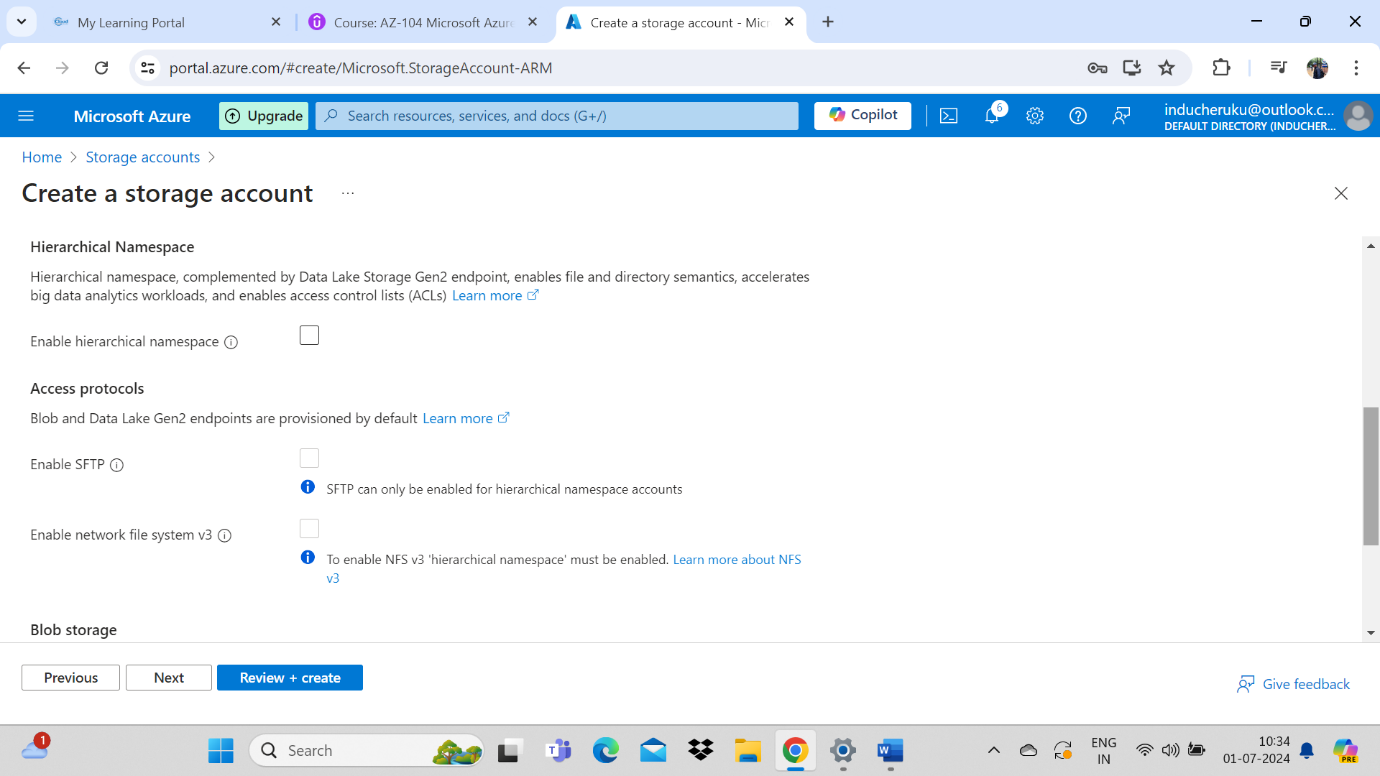
Storage Account:



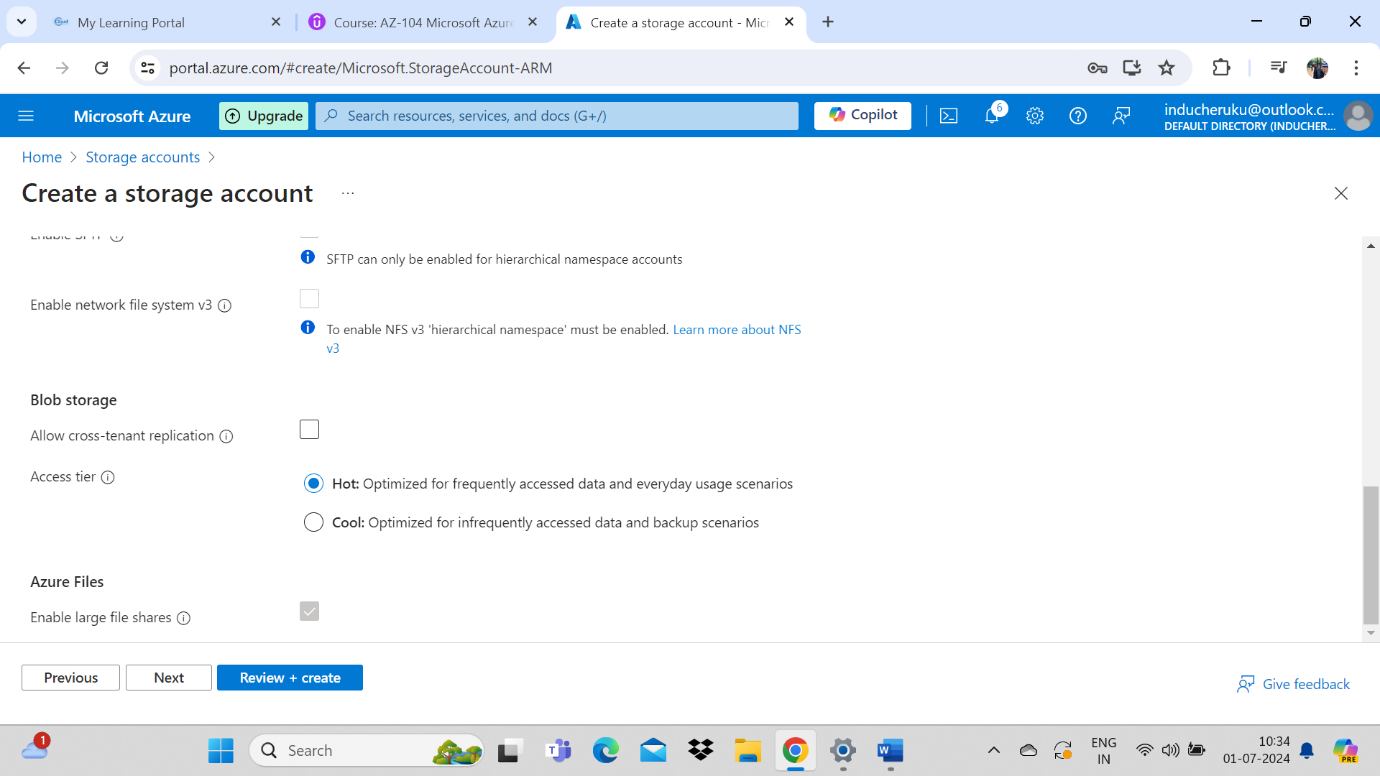
Advanced Tab : Require secure transfer for REST API operations :

The secure transfer option enhances the security of your storage account by only allowing REST API operations on the storage account using HTTPs. Any requests using HTTP will be rejected when this setting is enabled. When you are using the Azure file service, connections without encryption will fail, including scenarios using NFS v4.1, SMB 2.1, SMB 3.0 without encryption, and some flavors of the Linux SMB client. Because Azure storage doesn’t support HTTPs for custom domain names, this option is not applied when using a custom domain name. Connections via NFSv3 for blobs over TCP will succeed but will not be secured



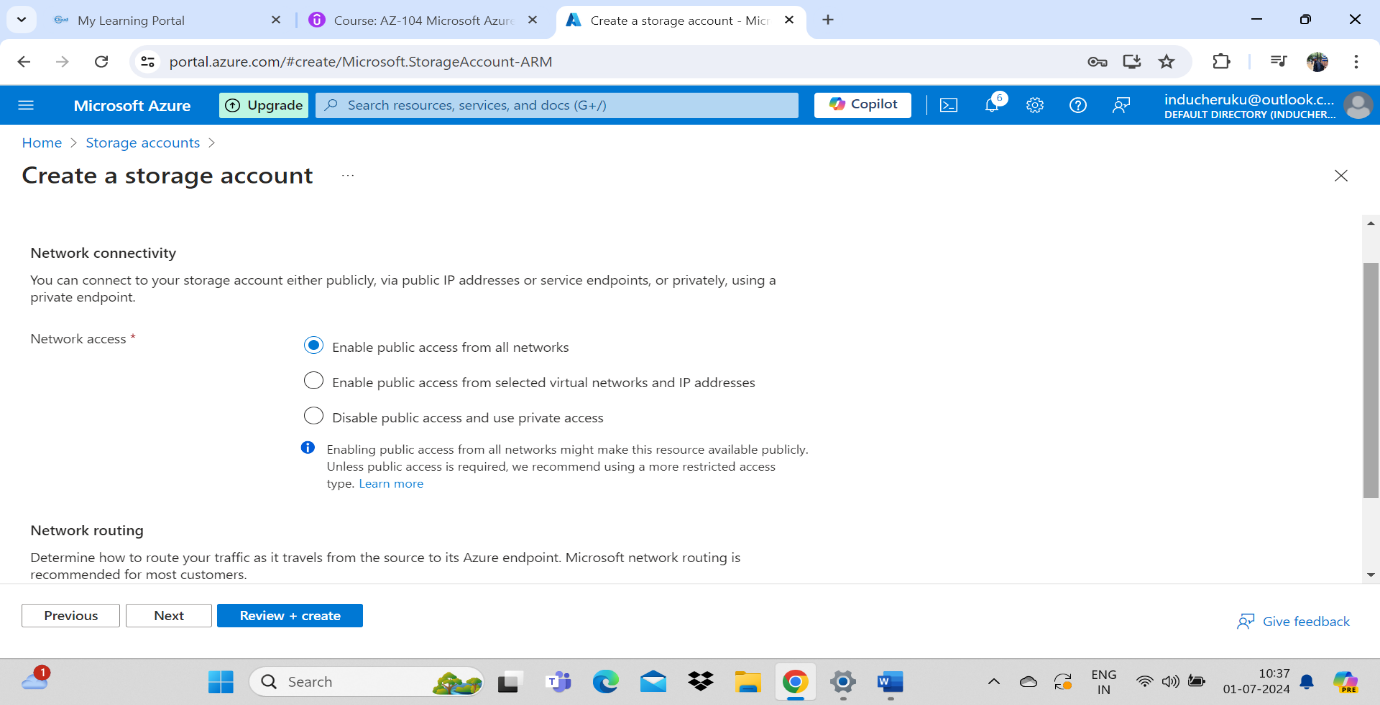


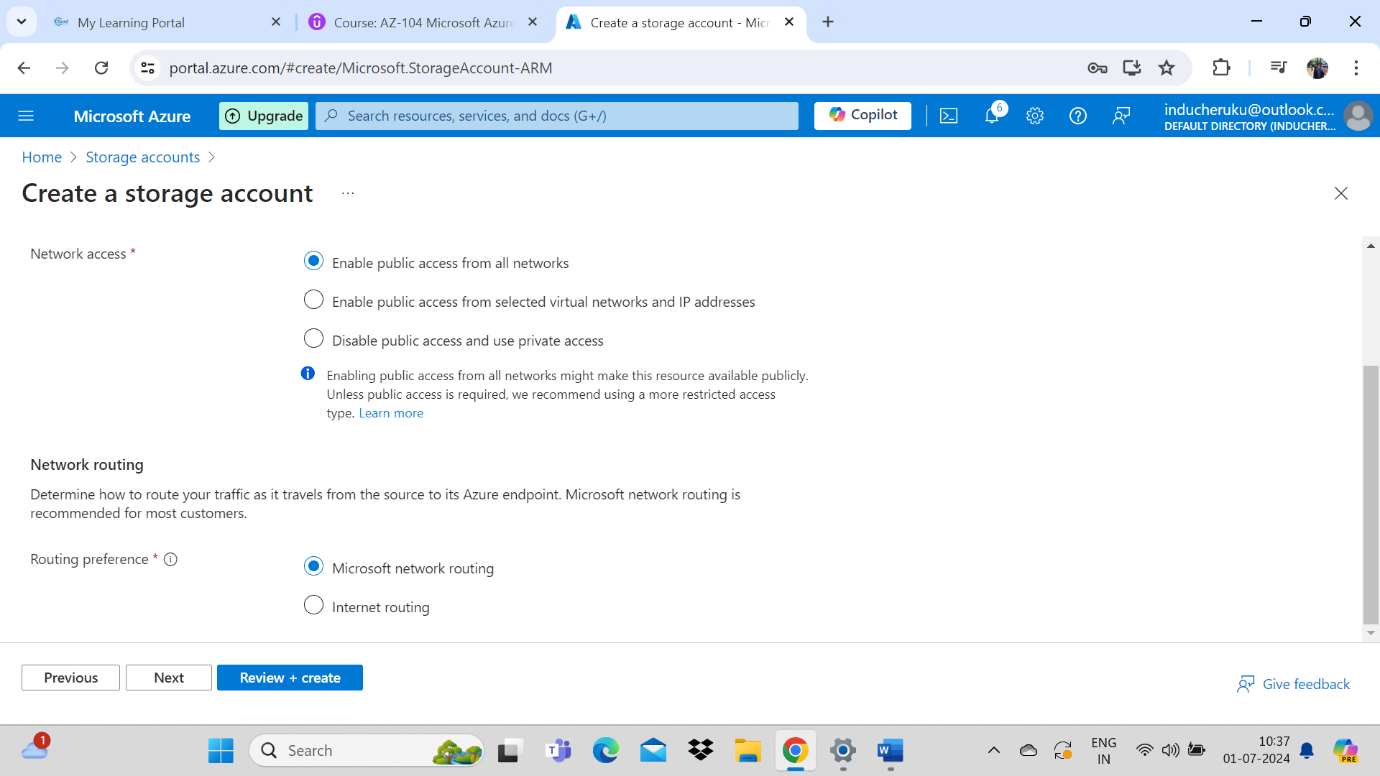
**Allow cross-tenant replication :**  
Allow object replication to copy blobs to a destination account on a different Microsoft Entra tenant. Not enabling cross-tenant replication will limit object replication within the same Microsoft Entra tenant.



**Access tier :**  
The account access tier is the default tier that is inferred by any blob without an explicitly set tier. The hot access tier is ideal for frequently accessed data, the cool access tier is ideal for infrequently accessed data, and the cold access tier is ideal for rarely accessed data. The archive access tier can only be set at the blob level and not on the account.

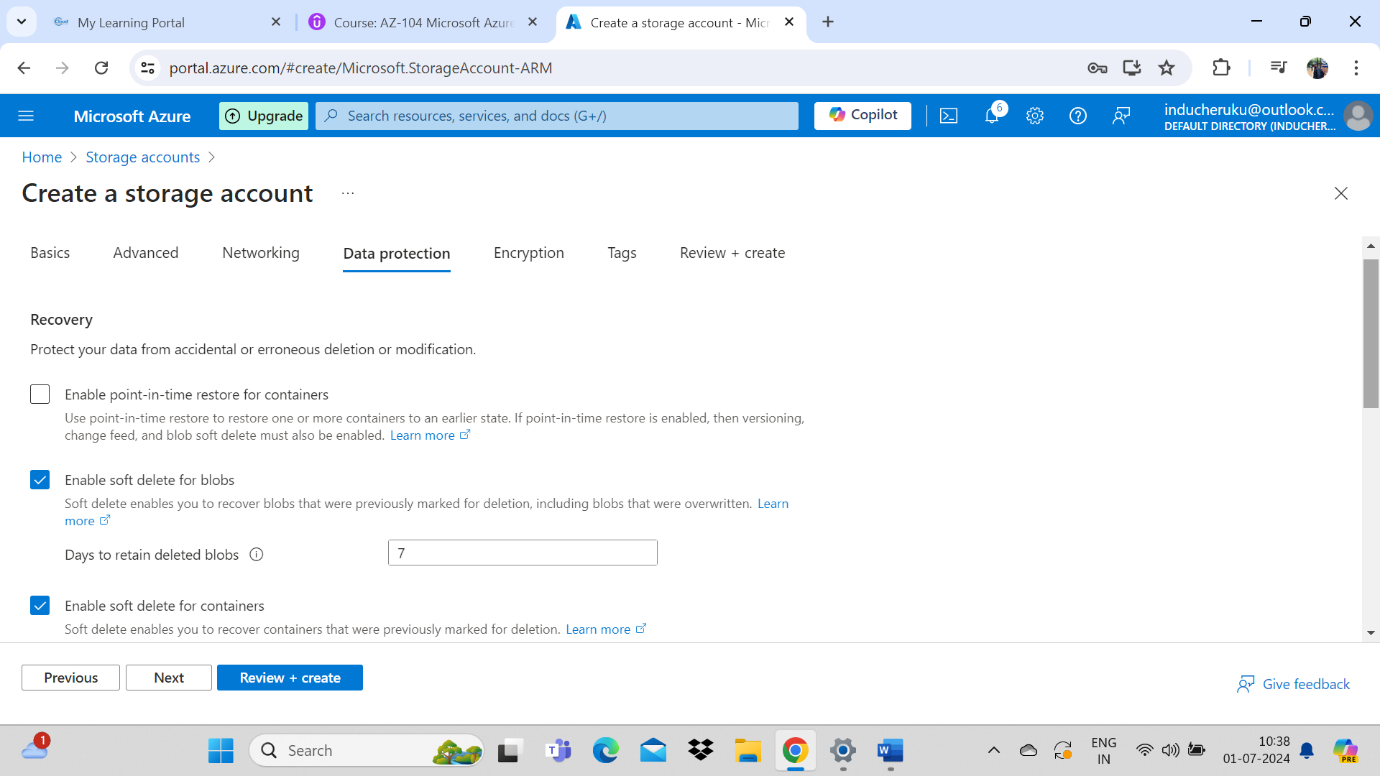
Networking tab :

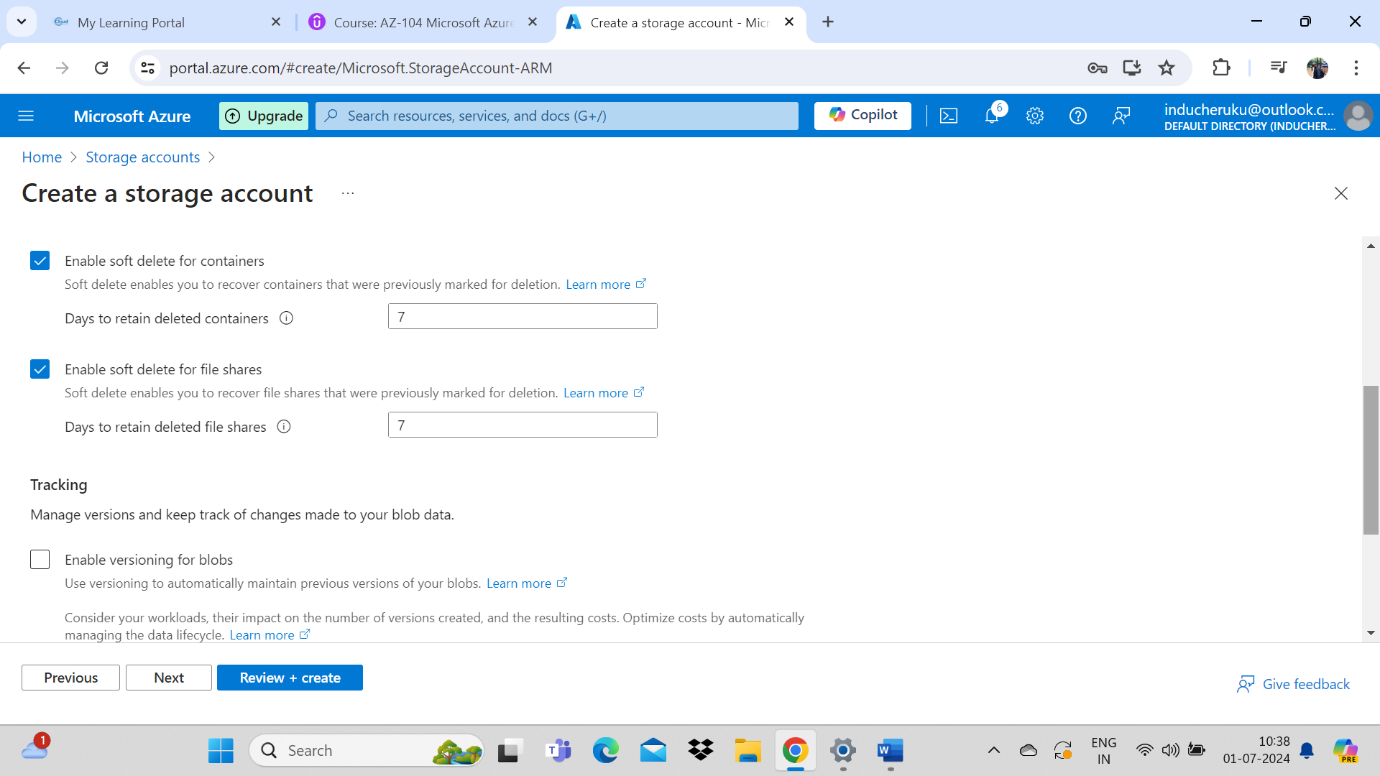


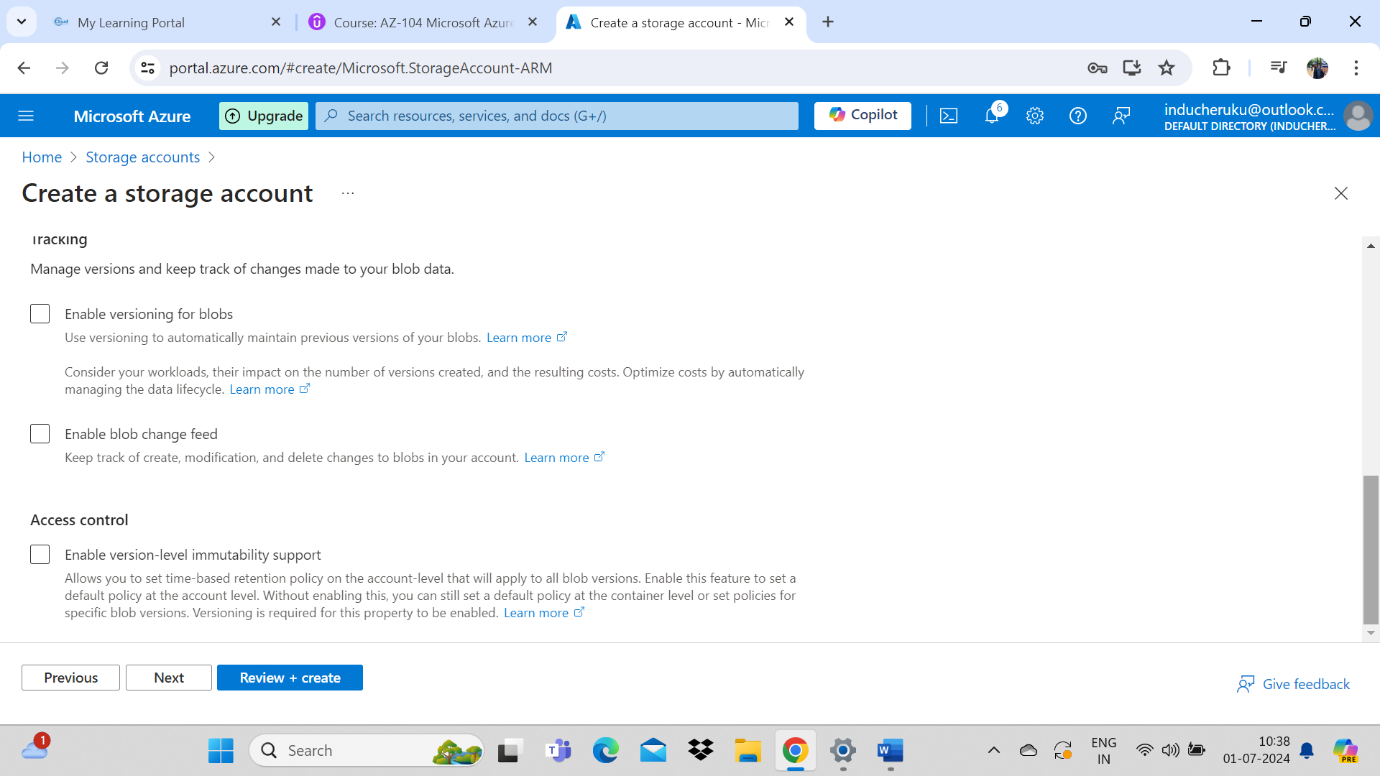


Microsoft network routing will direct your traffic to enter the Microsoft cloud as quickly as possible from its source. Internet routing will direct your traffic to enter the Microsoft cloud closer to the Azure endpoint.

Data protection tab :



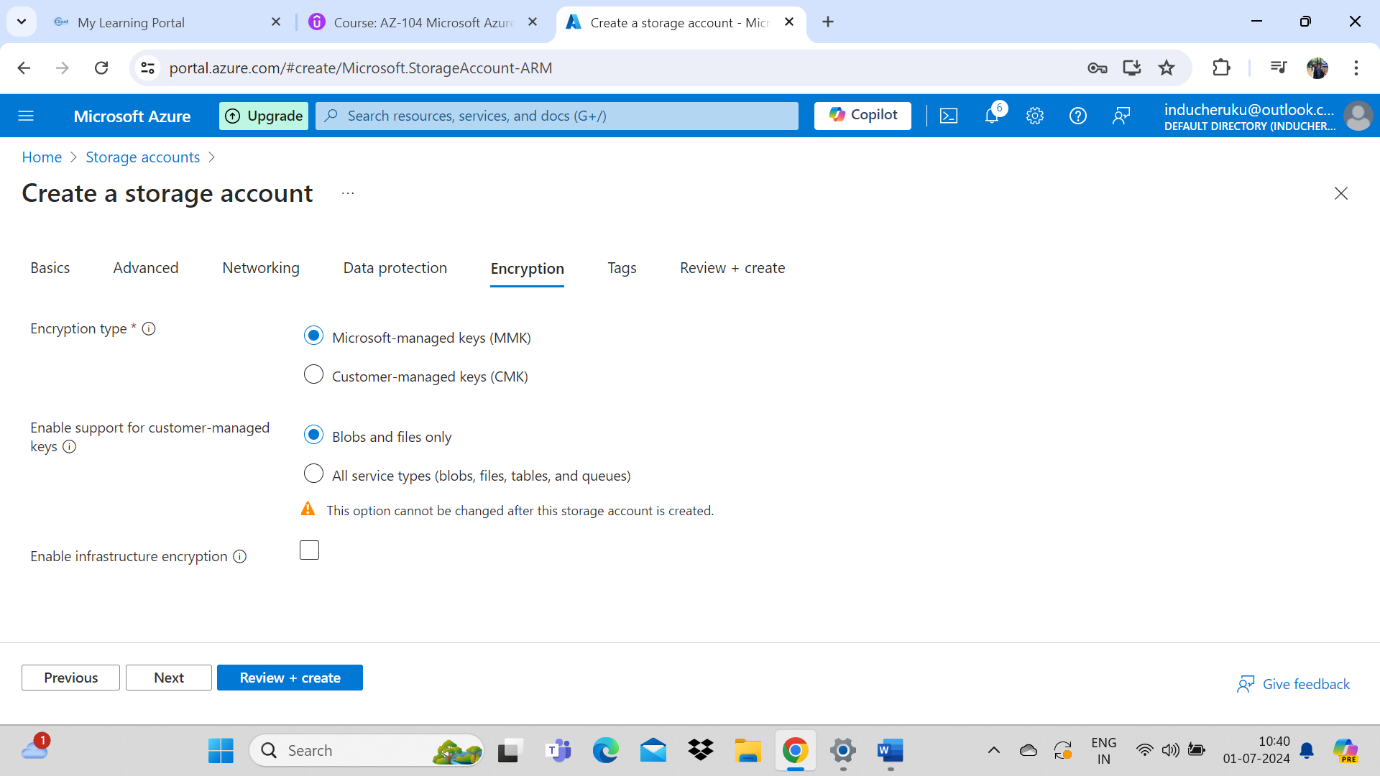




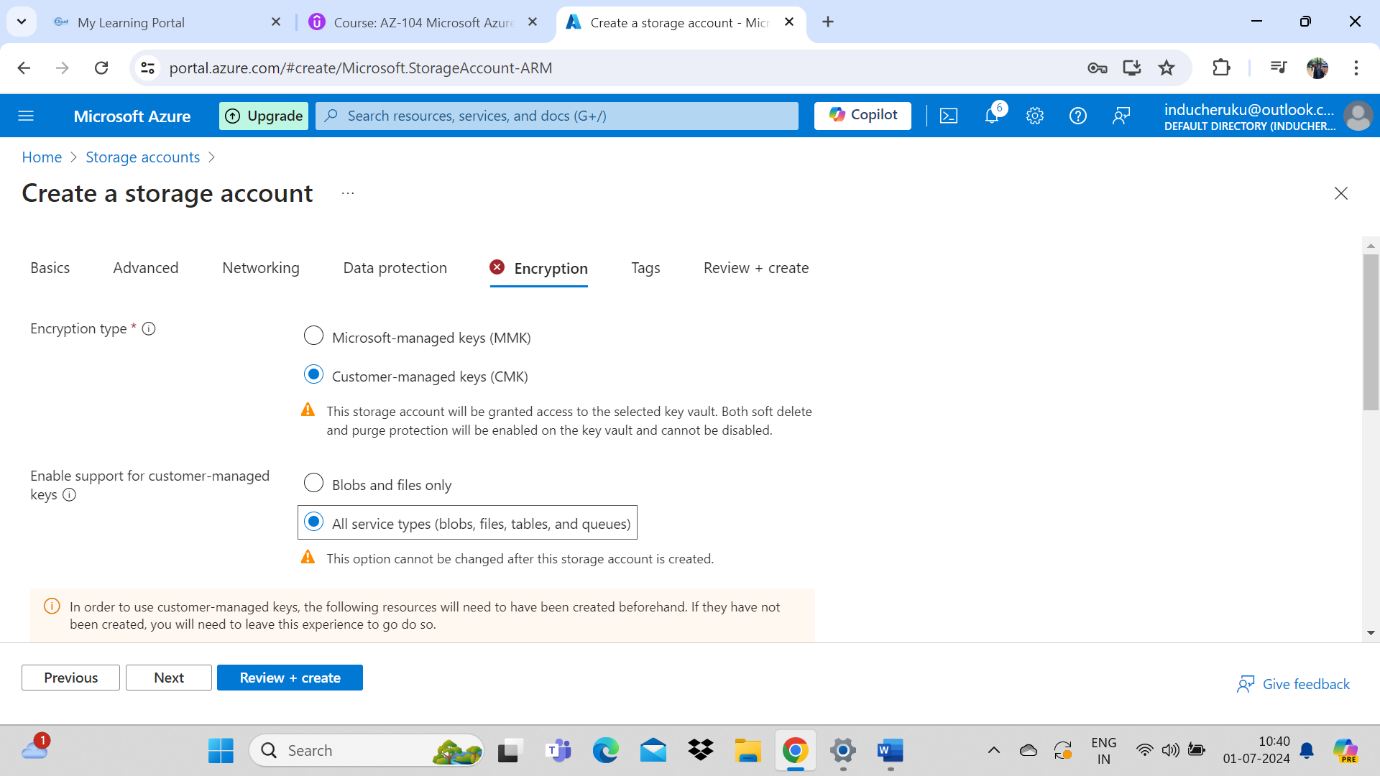
Encryption Tab :

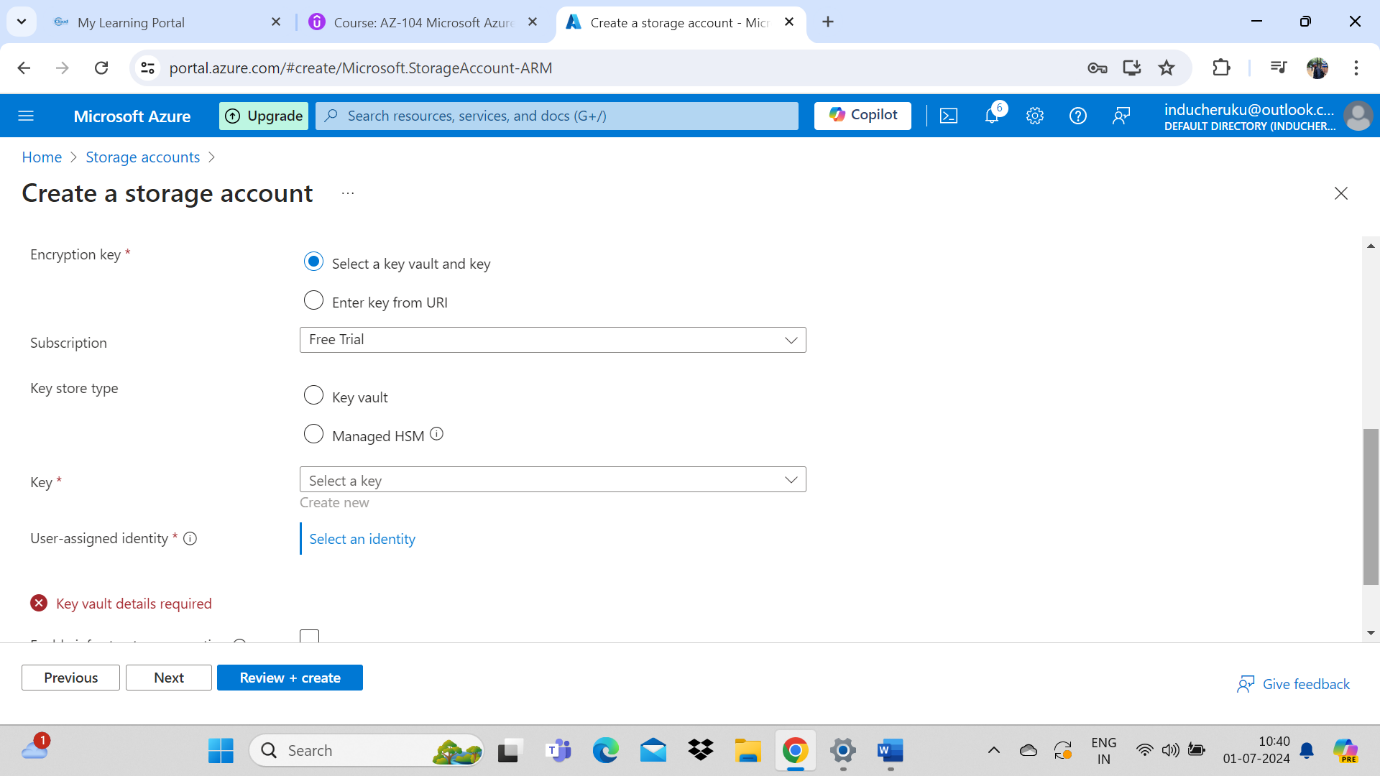
Your data is encrypted by default using Microsoft-managed keys. For additional control over your data, encrypt using customer-managed keys via the Azure Key Vault

MMK :



CMK :





Enable infrastructure encryption:

By default, Azure encrypts storage account data at rest. Infrastructure encryption adds a second layer of encryption to your storage account’s data.

