**SVKM'S NMIM’S Nilkamal School of Mathematics, Applied Statistics & Analytics**

**Master of Science (Data Science)**

Practical-6 Implementing MFA

**Writeup:-**

# • MFA

Multi-factor authentication (MFA) is a multi-step account login process that requires users to enter more information than just a password. For example, along with the password, users might be asked to enter a code sent to their email, answer a secret question, or scan a fingerprint. A second form of authentication can help prevent unauthorized account access if a system password has been compromised.

BENEFITS:

Reduces security risk

Multi-factor authentication minimizes risks due to human error, misplaced passwords, and lost devices.

Enables digital initiatives

Organizations can undertake digital initiatives with confidence. Businesses use multi-factor authentication to help protect organizational and user data so that they can carry out online interactions and transactions securely.

Improves security response

Companies can configure a multi-factor authentication system to actively send an alert whenever it detects suspicious login attempts. This helps both companies and individuals to respond faster to cyberattacks, which minimizes any potential damage.

# • Types of MFA

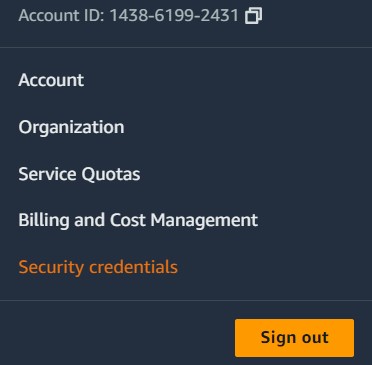
SMS-Based MFA: In this method, after entering the username and password, the user receives a one-time code via SMS (Short Message Service) on their registered mobile phone. They then enter this code to complete the authentication process.

Time-Based One-Time Password (TOTP): TOTP is a type of MFA where a temporary numeric code is generated based on the current time and a shared secret key. This code is typically generated by a smartphone app such as Google Authenticator or Authy. The user must enter this code along with their username and password to authenticate.

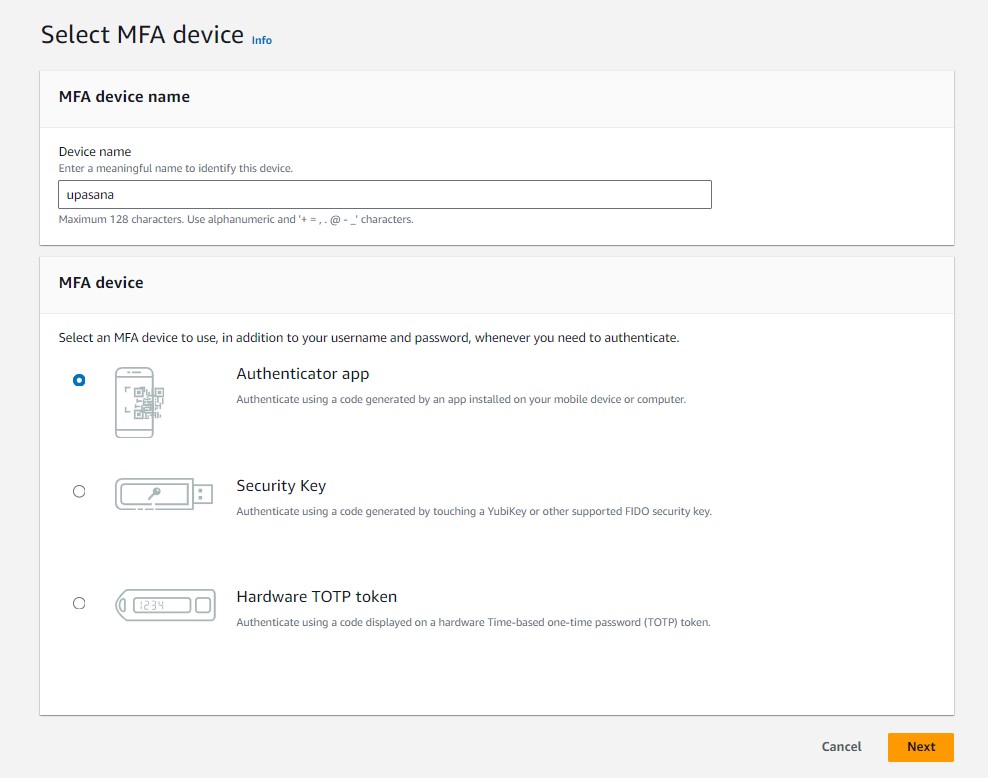
Hardware Tokens: Hardware tokens are physical devices that generate one-time passwords. These tokens can be USB tokens, smart cards, or key fobs. When a user needs to authenticate, they simply press a button on the token, and it generates a unique code that they enter along with their other credentials.

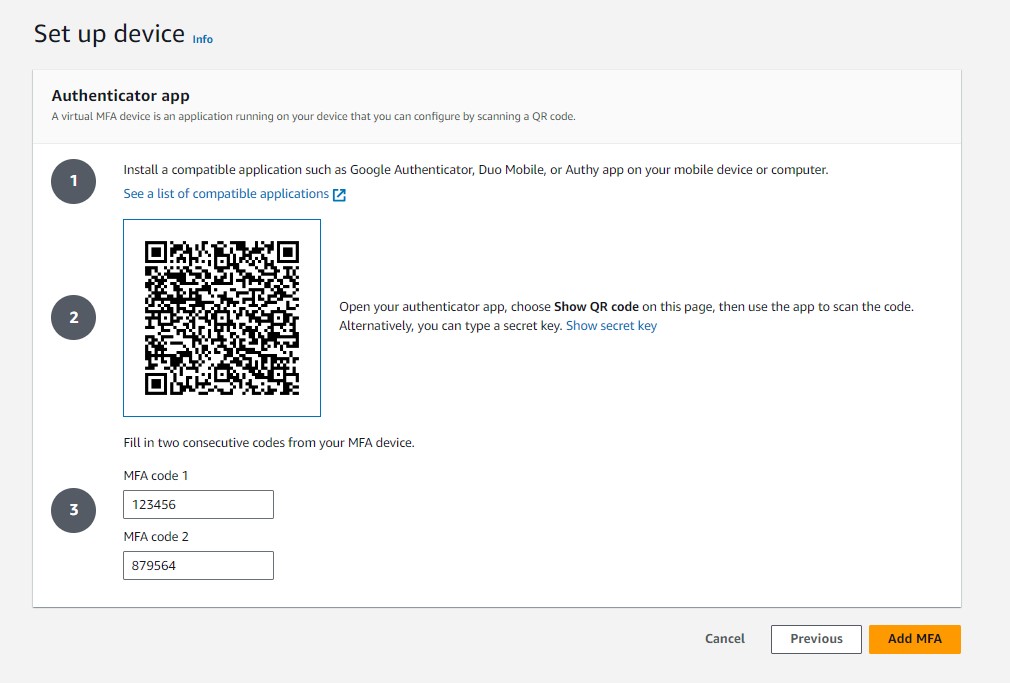
**PRACTICAL IMPLEMENTATION USING GOOGLE AUTHENTICATOR.**

# Study and implement MFA in the environment of popular Cloud Service Provider









# CREATE USER AND ASSIGN MFA

