Definição de Biometria

É uma tecnologia que utiliza características físicas ou comportamentais únicas que pode ser usada para identificar indivíduos na autenticação, refere-se à utilização de características próprias de um indivíduo para proceder à sua autenticação e/ou identificação perante um SI de uma organização.

Na prática, a biometria permite substituir ou complementar métodos tradicionais de segurança, como senhas ou cartões, ao transformar o corpo ou o comportamento de uma pessoa na "chave" de acesso a sistemas, dispositivos ou locais. Ela é amplamente utilizada para aumentar a segurança em áreas como acesso a dispositivos eletrônicos, controle de entrada em edifícios e proteção de informações sensíveis.

Aplicação na Autenticação

Quando um indivíduo tenta acessar um sistema ou serviço protegido, o dispositivo (como um scanner de impressões digitais, uma câmera para reconhecimento facial etc.) captura a característica biométrica.

O sistema, então, compara a característica capturada com um banco de dados previamente armazenado. Se houver uma correspondência, o acesso é concedido; caso contrário, ele é negado. **Autenticação**: Verificar se o usuário é quem diz ser, permitindo ou negando acesso a sistemas, dados ou locais. **Identificação**: Determinar quem é o usuário, comparando seus dados biométricos com todos os registros disponíveis no banco de dados.

Métricas de Avaliação

As **métricas de avaliação** em sistemas de autenticação biométrica são usadas para medir a eficácia, precisão e aceitabilidade do método de autenticação utilizado. As principais métricas incluem:

**1. FAR (False Acceptance Rate - Taxa de Falsas Aceitações):**

* **Definição:** Indica a frequência com que o sistema aceita erroneamente uma pessoa não autorizada como sendo autorizada.
* **Importância:** Uma alta taxa de FAR compromete a segurança, pois permite acessos indevidos.

**2. FRR (False Rejection Rate - Taxa de Falsas Rejeições):**

* **Definição:** Mede a frequência com que o sistema rejeita erroneamente uma pessoa autorizada.
* **Importância:** Uma alta taxa de FRR afeta a conveniência e a experiência do usuário, pois impede o acesso de pessoas legítimas.

**3. CER (Crossover Error Rate - Taxa de Intersecção de Erros):**

* **Definição:** Ponto onde as taxas de falsas aceitações (FAR) e falsas rejeições (FRR) são iguais. Representa um equilíbrio entre segurança e usabilidade.
* **Importância:** Quanto mais baixo o CER, mais preciso é o sistema biométrico, indicando um bom equilíbrio entre segurança e conveniência.

Tipos de Biometria:​

-Física​: Impressão digital, reconhecimento facial, geometria da mão, leitura de íris e retina.

-Comportamental​: Reconhecimento de voz, padrões de digitação, assinatura.

Critérios para escolha da Biometria

1. Segurança e Precisão:

Escolha uma biometria que identifique corretamente as pessoas autorizadas e rejeite as não autorizadas com precisão.

2. Custo:

Considere o custo total para implementar, incluindo equipamentos, software e manutenção.

3. Conforto e Aceitação:

Escolha um método que seja fácil e confortável para os usuários e que eles aceitem bem.

4. Adequação ao Ambiente:

Certifique-se de que a biometria funcione bem no local de uso, como em ambientes internos ou externos.

5. Facilidade de Integração:

Verifique se a biometria pode ser integrada facilmente aos sistemas e dispositivos existentes.

6. Velocidade:

A tecnologia deve autenticar rapidamente, especialmente em locais movimentados.

7. Privacidade e Leis:

Escolha uma tecnologia que respeite a privacidade dos usuários e siga as leis de proteção de dados.

8. Resistência a Fraudes:

Prefira tecnologias mais seguras e difíceis de enganar ou falsificar.

9. Escalabilidade:

Considere se a solução pode ser expandida para muitos usuários.

10. Durabilidade:

A tecnologia deve ser resistente e durar por bastante tempo, mesmo com uso frequente.

Processo de Autenticação Biométrica

1. Captura de Dados Biométricos:

Os dados biométricos do usuário (como impressão digital, rosto, voz, íris etc.) são capturados usando um dispositivo específico, como um scanner de impressão digital ou uma câmera.

2. Extração de Características:

As características únicas do dado biométrico capturado (pontos específicos de uma impressão digital, formato do rosto, padrões de voz etc.) são extraídas e convertidas em um formato digital.

3. Criação de um Modelo Biométrico:

Os dados extraídos são processados para criar um "modelo" biométrico, que é um conjunto de dados que representa as características únicas da pessoa.

4. Armazenamento Seguro do Modelo:

O modelo biométrico é armazenado de forma segura em um banco de dados ou em um dispositivo local, geralmente criptografado para evitar acesso não autorizado.

5. Comparação com o Modelo Existente:

Quando o usuário tenta se autenticar, uma nova amostra biométrica é capturada e um novo modelo é gerado. Este modelo é comparado com o modelo previamente armazenado.

6. Verificação e Decisão:

O sistema verifica se o novo modelo corresponde ao modelo armazenado dentro de um limite aceitável de semelhança. Se a correspondência for positiva, o acesso é concedido; caso contrário, o acesso é negado.

7. Resposta ao Usuário:

O usuário é notificado sobre o resultado da autenticação, recebendo acesso ao sistema ou sendo solicitado a tentar novamente.