

Web-based facial authentication has seen significant development in recent years thanks to the autonomous advancements of Artificial Intelligence and Computer Vision technologies giving birth to a plethora of solutions that present some advantages and limitations and that can be categorized as presented below .

- Face Recognition APIs
  - Cloud-based APIs provided by big tech companies : Microsoft Azure Face API, Amazon Rekognition, and Google Cloud Vision API ..
  - Present and sell facial recognition as a service in a B2B and B2C context allowing the integration of facial recognition into web applications .

**Advantages :**

- **Ease of Integration** :They are easy to incorporate into web applications without starting from scratch.
- **Regular updates and Maintenance** : Users benefit from frequent updates and maintenance without needing to manage them.
- **Scalability** : These APIs can handle varying levels of traffic and processing demands effectively.
- **Advanced Features** : They offer additional functionalities like emotion detection, gender recognition , and age estimation.

**Limitations :**

- **Bias and Accuracy**: Algorithms can be biased and inaccurate, especially for certain demographic groups.
- **Legal and Ethical Challenges**: Compliance with regulations and ethical considerations is necessary and can be complex.
- **Dependency**: Relying on external providers for essential functionality poses risks.
- **Privacy Concerns**: Users may be worried about sharing biometric data due to privacy issues.

- Open Source Libraries

Some computer vision and deep learning open source libraries like [OpenCV](#) and [dlib](#) have emerged providing facial recognition functionalities .

**Advantages :**

- **Cost-Effective:** Free to use, accessible for developers on a budget.
- **Customization:** Developers can tailor the library to suit their specific needs.
- **Platform Independence:** Cross-platform compatibility across different systems.
- **Community Support:** Large and active communities, providing extensive documentation, tutorials, and support forums.

#### Limitations :

- **Legal Considerations:** Users need to be aware of licensing agreements and potential legal implications when using OS libraries.
- **Maintenance and Updates:** Community-driven maintenance may lead to slower updates and compatibility issues.
- **Performance:** While OS libraries can offer powerful functionalities, they may not always achieve the same level of performance or optimization as proprietary solutions.
- Custom Machine Learning Models  
Some Organizations developed custom machine learning models tailored to their systems and trained specifically for their web-based facial authentication needs .

#### Advantages :

- **Tailored Accuracy:** Specifically designed for the organization's needs, potentially offering higher accuracy.
- **Competitive Advantage:** Developing proprietary models can provide a competitive edge by offering unique features or better performance than off-the-shelf solutions.
- **Control and Flexibility:** Organizations have full control over development and can adapt the model as needed.

#### Limitations :

- **Resource Intensive:** Requires significant expertise, time, and resources for development and maintenance.
- **Data Bias:** May inherit biases from training data, leading to inaccuracies.
- **Generalization Challenges:** Difficulty in adapting to diverse scenarios or user populations.
- Biometric Authentication Platforms  
Some platforms like FaceTec and BioID offer web-based facial authentication solutions that comply with industry standards and regulations.

#### Advantages :

- **Accuracy:** Biometric authentication offers high accuracy in verifying user identity, enhancing security.

- **User Convenience:** Users find biometric authentication convenient, as it eliminates the need for remembering passwords or carrying physical tokens.
- **Security:** Biometric data is unique to each individual, making it difficult to replicate or spoof.

#### Limitations :

- **Reliability on Hardware:** Some biometric authentication methods require specific hardware, limiting accessibility for users without compatible devices.
- **User Acceptance:** Not all users may feel comfortable with biometric authentication methods, leading to potential resistance or adoption challenges.
- **Regulatory Compliance:** Adhering to regulations and standards, such as GDPR, may impose additional complexities and requirements on biometric authentication platforms.
- Browser-based solutions  
Native facial authentication characteristics are supported by some modern web browsers through APIs like [WebAuthn](#) .

#### Advantages :

- **Convenience:** Authenticate directly in the browser without extra steps.
- **Security:** Enhanced security using device-specific hardware and encryption.
- **User-friendly:** Easy and intuitive for users, improving the login experience.
- **Compatibility:** Works with modern browsers and devices without additional software.

#### Limitations :

- **Device Dependency:** Works only on devices with compatible hardware.
- **Privacy Concerns:** Users may worry about their facial data privacy.
- **Accuracy Variability:** Performance may differ based on algorithms and hardware.
- **Security Risks:** Vulnerable to potential security threats despite enhanced security measures.
- Blockchain-based solutions  
These solutions rely on the principles of blockchain technology in order to provide users with greater experiences .

#### Advantages :

- **Security:** Enhanced security with decentralized and tamper-proof records.
- **Transparency:** Clear and trustworthy transactions visible to all parties.

- **Data Integrity:** Ensured data accuracy and trust through cryptographic methods.
- **Decentralization:** Reduced reliance on middlemen, leading to cost savings and efficiency.

**Limitations :**

- **Scalability:** Slower processing times due to consensus requirements.
- **Complexity:** Requires specialized knowledge and resources for implementation.
- **Energy Consumption:** Some methods consume a lot of energy, raising environmental concerns.

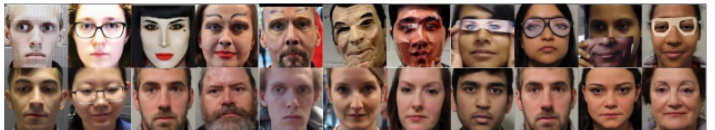
Despite the advancements and diverse array of solutions in the realm of web-based facial authentication, it's crucial to be mindful of the potential threats and vulnerabilities that face recognition systems may encounter , that's why we present an overview of the threats and attacks that a facial authentication system may face .

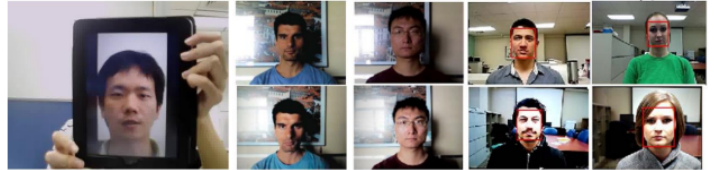

## Threats Towards Face Recognition Systems

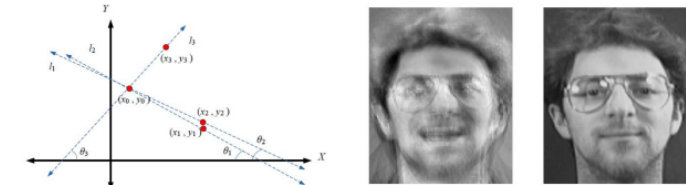
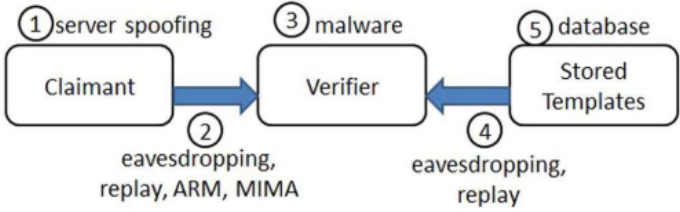
Threats towards facial authentication systems can be grouped into 5 categories depending on their nature :

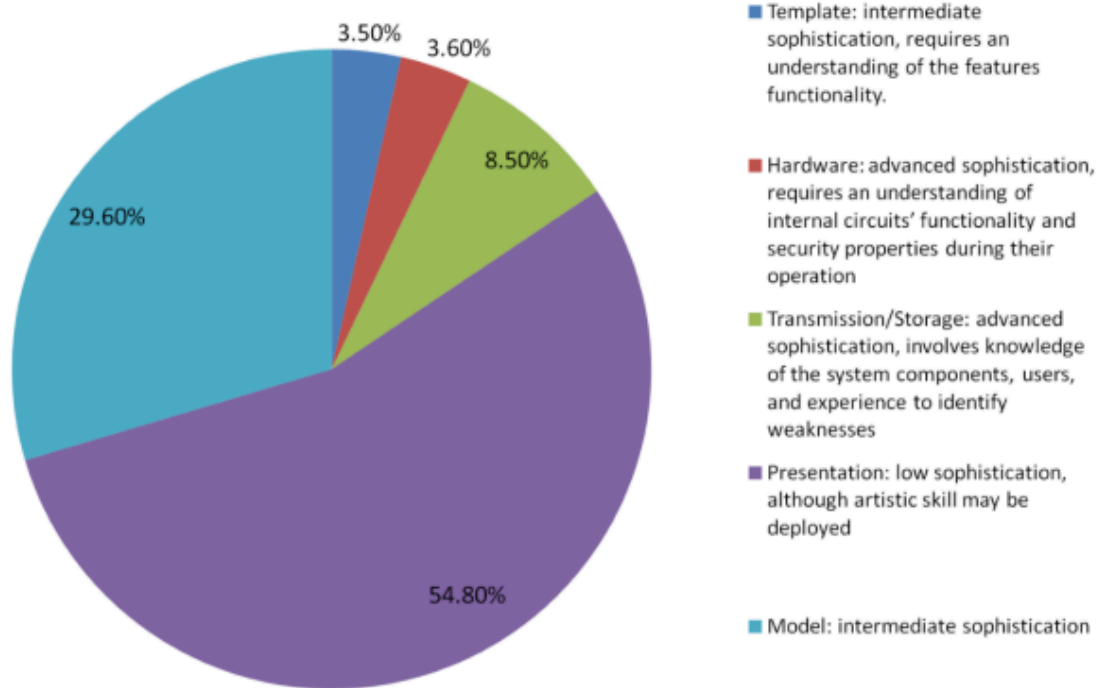
- Presentation group
- Template group
- Model group
- Hardware group
- Transmission/Storage group

## Types of Attacks :

Type of attack	Concept	Details and Examples
Presentation	producing a fabricated/tampered sample to bypass the system's authentication	Social media platforms and public websites are plentiful resources, as they comprise free available samples sometimes without the victim's knowledge. Samples can also be obtained live in person without the victim's consent (pictures can be taken in public places without being a privacy violation) . The next step is to generate the image replica which will be used to bypass the system. These images will eventually lead to impersonating a specific subject (spear impersonation) or any person that uses the FRS (random impersonation).
Printouts	Creating a replica that requires only a sample image of the victim and a high-quality printer	<p>- High-definition printouts present a problem for FRS</p> <p>-These attacks require little level of sophistication once the victim has been identified.</p>  <p>“ Printout samples to perform impersonation attacks. First row printout, second row live targets ”</p>

		<p>-These attacks require little level of sophistication once the victim has been identified.</p>
VideoReplay	<p>Having a video of the intended victim and providing it as a sample to the FRS.</p>	<p>-used because some authentication methods imply detecting whether the face is actually alive : liveness detection methods .</p> <p>- Because some spoofing detection methods are based on motion detection , these require computing motion characteristics, e.g., optical flow, and tracking facial landmarks to determine whether the subject is alive.</p>  <p><i>“ Video replay samples to perform impersonation attacks. First row live samples, second row device’s video. “</i></p>
Masks	<p>generating masks using wax , silicone or using 3D masks</p>	<p>-Liveness-based methods are not easy to fool with this technology</p> <p>-Wax techniques require sophisticated artistic skills</p> <p>-Silicone masks have the potential capability of adding dynamic facial characteristics, particularly regarding eyes and mouth.</p> <p>-3D-masks are considered a serious threat as recent technological advances have made 3D printing accessible .</p>  <p><i>“ Image example for each technique “</i></p>

<p>Template</p>	<p>Exploiting vulnerabilities from image features which implies potential vulnerabilities in the feature space and finding samples that closely resemble bonafide templates.</p>	<div data-bbox="899 247 1581 478">  <p>(a) Random Slope to conceal the feature matching process [106].</p> <p>(b) An image recovered using a new model inversion attack [175]</p> </div> <p>Here is an example of such an attack, known as an <b><u>“inversion attack”</u></b>: the attacker may reverse the matching process to find templates that cause the system to accept samples via low similarity scores.</p>
<p>Model</p>	<p>Potential attacks aimed at features processing : corrupting the data and creating adversarial samples</p>	<p>-Can be separated into various categories including poisoning , backdoor , evasion , inversion , registration ..</p> <p>-Feasible because of the ever growing need for pre-processed data. The lack of control of the training process, reference data and model structure are fertile ground for model vulnerabilities.</p>
<p>Hardware</p>	<p>Targeting the physical components of a face recognition system aiming to manipulate or exploit them to compromise security or disrupt functionality .</p>	<p>-Can occur at various levels, including the sensor, processing unit, and storage devices.</p> <p>-A famous example is <b><u>“ Sensor Tampering Attack”</u></b> and it includes manipulating the facial recognition system's sensor to compromise its functionality and bypass authentication.</p>
<p>Transmission</p>	<p>Threatening data during the handling process</p>	<p>-Include data replay and data breaches via <b><u>“man-in-the-middle attack”</u></b>.</p> <p>- Databases can be hacked and analyzed for personal information and cross-matching attacks. -Privacy is threatened as the individual’s control over the collection, use, and disclosure of his biometric data is compromised.</p> <div data-bbox="883 1562 1559 1772">  <pre> graph LR     Claimant[Claimant] -- "1 server spoofing" --&gt; Verifier[Verifier]     Verifier -- "2 eavesdropping, replay, ARM, MIMA" --&gt; Claimant     Verifier -- "3 malware" --&gt; Claimant     Verifier -- "4 eavesdropping, replay" --&gt; DB[(5) database Stored Templates]     DB -- "5 database" --&gt; Verifier </pre> </div>



### Attacks by Proportion Groups