

# RISK ASSESSMENT MATRIX

Likelihood	<b>Unlikely (1)</b>	Low risk. No further action	Low risk. No further action	Low risk. No further action	Low risk. No further action	Medium risk. Further action optional
	<b>Seldom (2)</b>	Low risk. No further action	Low risk. No further action	Medium risk. Further action optional	Medium risk. Further action optional	High risk. Further action necessary
	<b>Occasional (3)</b>	Low risk. No further action	Medium risk. Further action optional	Medium risk. Further action optional	High risk. Further action necessary	Extreme risk. Act now
	<b>Likely (4)</b>	Medium risk. Further action optional	Medium risk. Further action optional	High risk. Further action necessary	Extreme risk. Act now	Extreme risk. Act now
	<b>Definite (5)</b>	Medium risk. Further action optional	High risk. Further action necessary	Extreme risk. Act now	Extreme risk. Act now	Extreme risk. Act now
		<b>Insignificant (A)</b>	<b>Marginal (B)</b>	<b>Moderate (C)</b>	<b>Critical (D)</b>	<b>Catastrophic (E)</b>
Consequence						

Technical Risks:

Algorithm Accuracy: The accuracy of smile detection software may not be high due to improper dataset of SMILE , a simple algorithm.

Hardware Compatibility: The system may not be compatible with all smartphones or cameras, limiting its usability.

Resource Limitations: The processing power of the server on which the model is deployed is not quite high to handle many users

Data Privacy Concerns: If the user agrees to sharing of data , and the data is leaked , then we would be responsible for it .

Operational Risks:

User Acceptance: Users may not be give us permission to capture selfie

Environmental Conditions: The system's performance may vary under different lighting conditions, affecting its reliability.

False Positives: Due to unbalanced dataset , the software would be biased towards non-smiling faces reducing the f1-score . However, weighing the dataset will take care of it .

Schedule Risks:

Development Delays: Deploying the ML model online on a website will be challenging for us .

Testing and Iteration: Extensive testing and iteration may be required to ensure the system's accuracy and reliability, potentially extending the development timeline.

Regulatory Risks:

Compliance Requirements: The system may need to comply with regulations related to data privacy, image processing, and user consent, which could pose legal and regulatory challenges if not adequately addressed.

SR NO.	Risk	Probability (%)	Impact	Level
1	Algorithm Accuracy	10	Mo	low
2	Hardware Compatibility	15	Mo	low
3	Resource Limitations	30	S	high
4	Data privacy	40	S	high
5	User Acceptance	10	Mi	low
6	Environmental Conditions	25	Mo	Medium
7	False Positives	20	Mo	low
8	Development Delays	40	S	high
9	Compliance Requirements	80	Mi	medium
10				

Privacy Concerns: Users can become uncomfortable having their selfies taken without their express permission, which could result in legal problems or privacy complaints.

Solution: Prior to taking any pictures, use consent prompts and obvious alerts.

Inaccurate Detection: Frustration or inaccurate data collecting may result from the ML model interpreting expressions wrongly.

Continually train and enhance the model to increase accuracy, and before taking a selfie, offer a manual confirmation option.

Security Flaws: There's a chance that the software will be hacked or misused, giving unwanted access to private information.

Solution: To safeguard taken photos, put strong encryption in place and routinely check the system for security flaws.

Ethical Issues: Using facial recognition technology may have ethical ramifications, particularly if it is done so without the users' knowledge or agreement.

Solution: Give consumers choices to opt out of the functionality if they so want and guarantee openness regarding the usage of the collected data.

Bias and Discrimination: Especially against specific demographics, the ML model may show bias, producing erroneous or discriminating results.

Use a variety of representative training data, routinely check the model for bias, and use bias mitigation strategies while training the model.

Personality

Give fifteen chances at the very least.

DiscussionGPT

Indeed, the following list of fifteen possible hazards is connected to the grin detection software:

**Privacy Breach:** Unauthorised access to or abuse of selfies taken by users could jeopardize their privacy.

Solution: For data stored, put in place stringent access restrictions and encryption.

**False Positives:** Frustration and discontent from incorrectly identifying a smile could result.

The solution is to keep raising the accuracy of the machine learning model by means of extensive testing and feedback systems.

**False Negatives:** Ignoring to recognize a real smile could lead to lost chances or erroneous data analysis.

Solution: Improve the detection algorithm to reduce false negatives while keeping specificity.

Depending on the lighting conditions, grin detection accuracy could change.

Solution: Include algorithms with adaptability to various lighting situations.

**Performance Decline with Time:** As the machine learning model comes across novel, unexplored situations, its performance may suffer.

To preserve performance, apply frequent updates and retraining of the model with new data.

**Data bias:** Unrepresentative training data used to build the machine learning model could produce biased outcomes.

Gather inclusive and varied training data, then routinely check the model for bias.

**Hardware Compatibility:** The program might not function well with every kind of camera or device.

Test every device and platform in-depth for compatibility.

**Legal Compliance:** There could be consequences for breaking facial recognition or privacy rules.

The solution is to keep up with pertinent laws and guarantee complete adherence to them in all data handling activities.

**User Acceptance:** Because they are uncomfortable with facial recognition or have privacy concerns, users could oppose or reject the feature.

Solution: Provide users choice over when and how to use the function and provide concise explanations of its advantages.

**Resource Intensiveness:** Device performance may be impacted by the software's possible large computational resource consumption.

Solution: Give consumers the ability to change how much resources are used and optimise algorithms for effectiveness.

**Accessories:** Correct smile detection may be hampered by items like glasses or face masks. Adapt algorithms to various facial combinations and accessories is the solution.

**Attacks by Adversaries:** By use of spoofing methods or adversarial inputs, malicious actors may try to control the system.

Solution: Put strong security protocols into place, such anomaly detection and image authentication.

**Psychological Impact:** Ongoing observation of users' facial expressions may prompt worries about invasion or surveillance.

Offer open lines of communication on data use and stress user choice and permission.

**Cultural Sensitivity:** The appropriateness and precision of grin detection may be impacted by cultural variances in facial expressions.

Solution: Give consumers customizing choices and take cultural quirks into account when developing the detecting system.

Software flaws or malfunctions may cause unexpected behavior or system failure.

Solution: Set up efficient bug reporting and resolving procedures and carry out extensive testing at every development phase.

## Risk Assessment Matrix

1				6	
2		7	4		
3		9	12	2 3	1
4		10	5		13
5			11	8	
	A	B	C	D	E

### Legends:

Likelihoods

Consequences

1- Unlikely

2- Seldom

3- Occasional

4- Likely

5- Definite

A - Insignificant

B - Marginal

C - Moderate

D - Critical

E - Catastrophic

### Color Legends:

Low risk - No Further Action	Medium risk - Can take action	High Risk - Further Action Necessary	Extreme Risk- Act Now
------------------------------	-------------------------------	--------------------------------------	-----------------------

1. Privacy Breach:
2. ML Model Inaccuracies
3. Performance Decline with Time:
4. Data bias:
5. Hardware Compatibility:
6. Legal Compliance:
7. Resource Intensiveness:
8. Accessories:
9. Psychological Impact:
10. Cultural Sensitivity:
11. Monitoring and updates all the time
12. Testability
13. Server Maintenance