Protecting User Data in Profile Matching Social Networks

Sheikh Mudasir Rashid[1], Farmaan Feroz[2], M Kesavan[3], Binita Pun Magar[4]
[1,2,3,4]*Dept. of Information Science and Engineering, HKBK College of Engineering, Bengaluru, India*

***Abstract*— The project "Protecting User Data in Profile Matching Social Networks: A Matrimony-Inspired Approach" aims to improve online interactions' security and privacy, which is a pressing necessity. For current users, the platform provides secure authentication by utilizing facial recognition technology. To prevent unauthorized access, new users must go through a laborious registration process that requires them to submit 100 facial photographs and personal information. To protect user data, the system has an alarm mechanism that notifies administrators of any illegal login attempts. Users that successfully authenticate are granted access to an intuitive dashboard where they may browse project information and see other users' profiles. Sending requests to possible matches will cause notifications and approval messages to be sent back. Users who have been approved can use a Telegram bot to start secure chats and view complete profiles. This all-inclusive strategy offers a smooth and safe online interaction experience, similar to a marriage-matching website, while also safeguarding user data.**

I. INTRODUCTION

Ensuring user data security and privacy is crucial in the digital era, particularly on social media sites. Motivated by the requirement for a safe online space similar to a marriage agency, this project seeks to create a strong framework for user data protection. The site uses strict registration criteria and facial recognition technologies for authentication in an effort to prevent unwanted access and improve user privacy. The project has an intuitive interface that makes it easy for users to view project data and use the platform. Facial recognition simplifies authentication for current users and offers a safe login procedure. In order to guard against unwanted access and safeguard user data from potential breaches, new users must go through a thorough registration process that includes providing personal information and face photographs. In order to provide proactive security measures, the platform also has an alert system that notifies administrators of any illegal login attempts.

II. LITERATURE SURVEY

1. Match Prediction Matrimonial Web Application

- *Title:* Match Prediction Matrimonial Web Application
- *Year:* 2020
- *Author:* Snehal Kharde1, Sonal Kharde2, Pranita Pawale3, Namrata Dushing4
- *Description:* This literature explores the development and implementation of a predictive algorithm within a matrimonial web application. The focus is on leveraging machine learning techniques to enhance the matchmaking process, providing users with accurate compatibility predictions based on various parameters.
- *Limitations:* The study may face limitations in terms of the diversity of data used for training the prediction model. Ethical concerns related to privacy and data security are also considered.

2. Sentiment Analysis using machine learning

- *Title:* Sentiment Analysis Using Machine Learning
- *Year:* 2020
- *Author:* Omkar Kadlag, Dhanashri Kalaskar, Kareena Shahani
- *Description:* This literature review investigates the application of sentiment analysis in the context of matrimonial websites. It explores how machine learning algorithms can be employed to analyze user-generated content, such as profile descriptions and communication logs, to gauge the sentiment and emotional tone. The goal is to enhance the matchmaking process by understanding users' emotional states and preferences.
- *Limitations:* The study acknowledges challenges related to the accuracy of sentiment analysis, especially when dealing with nuanced or ambiguous language. It also considers potential biases in training data affecting the analysis results.

3. Matrimony Website using Blockchain for Tracking Authenticity of Profiles

- *Title:* Matrimony Website using Blockchain for Tracking Authenticity of Profiles
- *Year:* 2019
- *Author:* Raju Talwar, Raju Talikoti
- *Description:* This literature survey explores the integration of blockchain technology into matrimonial websites for ensuring the authenticity of user profiles. The study delves into the decentralized nature of blockchain, its role in preventing fake profiles and unauthorized access, and the overall enhancement of security and trust in the matrimony platform.
- *Limitations:* The study acknowledges potential challenges in terms of scalability and user adoption. It also discusses the need for addressing regulatory concerns related to data protection and privacy within the blockchain framework.

4. Matrimonial Website

- *Title:* Matrimonial Website
- *Year:* 2020
- *Author:* Priya Doshi, Sneha Shinde
- *Description:* This literature review provides a comprehensive overview of existing matrimonial websites, focusing on their features, functionalities, and user experiences. It explores the evolution of online matchmaking platforms and discusses the various technological aspects employed to facilitate successful matches.
- *Limitations:* The review acknowledges the challenge of balancing user preferences with algorithmic recommendations. It also considers potential biases in the platform's user base and the evolving nature of societal norms impacting matchmaking criteria.

5. Fake Profile Detection Using Machine Learning Techniques

- *Title:* Fake Profile Detection Using Machine Learning Techniques
- *Year:* 2021
- *Author:* R
- *Description:* This literature survey investigates the application of machine learning techniques in identifying and preventing fake profiles on matrimonial websites. The study explores different approaches, including pattern recognition and anomaly detection, to enhance the platform's security and reliability. It also considers the impact of fake profiles on user trust and satisfaction.
- *Limitations:* The study addresses challenges related to the dynamic nature of fake profiles and the need for continuous model adaptation. It also discusses the ethical considerations associated with profile scrutiny and potential false positives in detection algorithms.

III. EXISTING SYSTEM

The existing system lacks robust security measures and fails to adequately protect user data, leaving users vulnerable to unauthorized access and potential breaches. The current authentication process is often based on weak credentials, such as passwords, which can be easily compromised. Additionally, the registration process is not stringent, allowing for the creation of fake or duplicate accounts. These shortcomings result in a lack of trust among users and hinder the overall user experience.

DEMERITS*:*

1. Weak authentication system using passwords.
2. Lack of stringent registration process, leading to potential fake accounts.

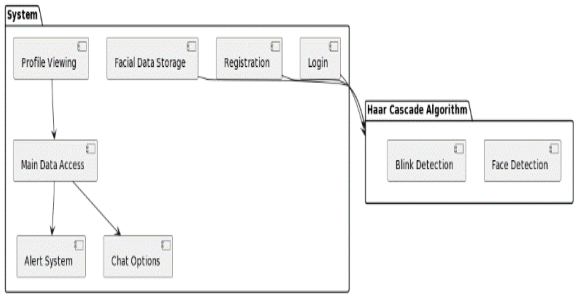
III. PROPOSED SYSTEM

The proposed system aims to revolutionize user data protection in social media, setting new standards for security and privacy. Through the implementation of cutting-edge facial recognition technology, the system ensures foolproof authentication, eliminating the risk of unauthorized access entirely. The registration process for new users is rigorous, requiring not only personal details but also 100 facial images for verification, ensuring that only legitimate users gain access. The platform features a user-friendly dashboard where users can access project information and explore profiles of other users securely. Additionally, an alert system is in place to notify administrators of any suspicious activity, further enhancing the platform's security measures. Overall, the proposed system sets a new benchmark for secure online interactions, guaranteeing user privacy and data protection like never before.

ADVANTAGES*:*

1. Enhanced security through facial recognition authentication.
2. Rigorous registration process to prevent fake accounts.
3. User-friendly dashboard for easy navigation.
4. Secure messaging through Telegram bot.
5. Proactive alert system for unauthorized access detection.

IV. ARCHITECTURE DIAGRAM



1. *Haar Cascade Algorithm:* This component handles the face detection and blink detection processes for user authentication. It is used during login and registration to ensure the presence of a live person.
2. *Login:* This component manages the user authentication process, which includes utilizing the Haar Cascade algorithm for face detection.
3. *Registration:* Here, the Haar Cascade algorithm is used for face detection to register new users securely.
4. *Profile Viewing:* After successful login, users can view profiles of others, initiating requests for further interaction.
5. *Main Data Access:* This component controls access to main data, requiring approval. It interacts with the alert system for unauthorized access detection.
6. *Alert System:* This component is triggered if an unknown person attempts to log in, ensuring the security of the system.
7. *Chat Options:* Upon approval, users can engage in secure chat sessions. This component facilitates communication within the platform.
8. *Facial Data Storage:* This component stores facial data securely for future use, enabling efficient authentication.

V. ALGORITHM

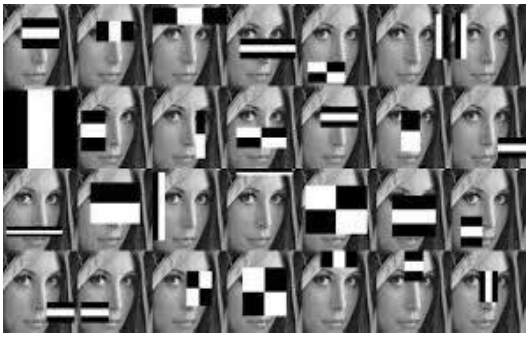
Haar Cascade Face Detection Algorithm Steps:

1.Preprocessing of Input Images:

- Convert the input image from the webcam to grayscale to reduce computational complexity.
- Normalize the image to enhance contrast and lighting conditions.

2.Load Haar Cascade Classifier:

- Load the pre-trained Haar Cascade classifier designed for face detection. These classifiers are XML files that OpenCV provides for detecting various body parts, including faces.



3.Face Detection:

- Apply the Haar Cascade classifier to the preprocessed image.
- The classifier scans the image using a moving window, calculating Haar features for each window section.
- An integral image concept is used to speed up the feature calculation, allowing the algorithm to operate in real time.

4.Analyze Detection Results:

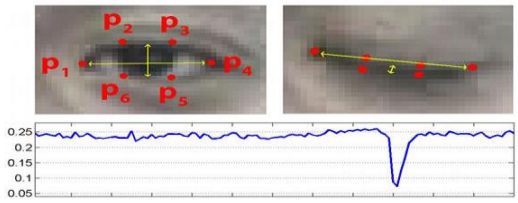
- For each section of the image, the classifier assesses whether there are features matching a face.

- A series of classifiers (cascade) are applied; if a section passes all stages, it's marked as a face candidate.

5.Post-processing:

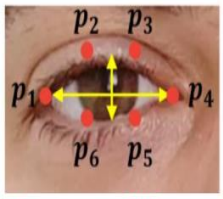
- Apply additional criteria (like minimum size of the detected face) to filter out false positives.
- If multiple faces are detected, use heuristics or additional checks to identify the primary user's face.

Blink Detection Steps:

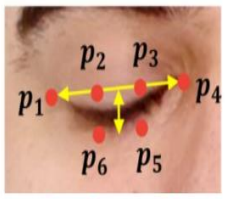


1. Eye Region Detection:

- Within each detected face, identify the regions corresponding to the eyes using a similar Haar Cascade specifically trained for eye detection.



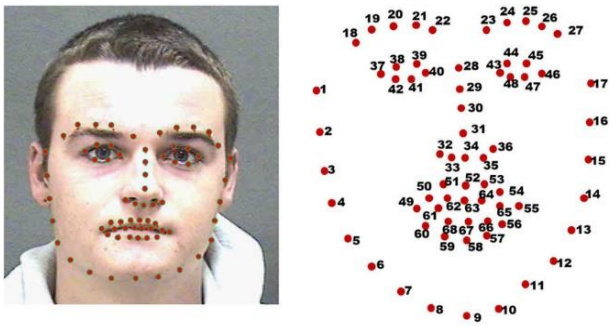
Open eye will have more EAR



Closed eye will have less EAR

2.Blink Detection:

- Monitor the eye regions over a sequence of frames to detect closure and reopening, indicative of a blink.
- This can involve analyzing the aspect ratio of the eye regions; a significant decrease would suggest a blink.



(a) (b)

Authentication and Access Control:

1.Identity Verification:

- Compare the detected face against a database of known faces. This might involve feature comparison or more sophisticated machine learning models.
- If the system includes liveness detection, ensure the blink detection step confirms the subject's presence.

2.Access Granting:

- If the face matches an existing user profile and liveness is confirmed, grant access to the user.
- Log the access event and any other relevant security data.

3.Alerts for Unauthorized Attempts:

- If the authentication fails, trigger an alert mechanism. This could involve notifying system administrators or the user via email or a mobile notification.

VI. DISCUSSION

"PROTECTING_USER_DATA_SOCIAL_MEDIA" project represents a significant advancement in the realm of online security and privacy on social media platforms, particularly for sensitive sectors like matrimonial services. By leveraging the robustness of the Haar Cascade algorithm for facial recognition and incorporating blink detection, the system introduces a novel layer of security that goes beyond traditional password-based authentication methods. This approach not only mitigates the risk of unauthorized access but also paves the way for a more secure and user-friendly experience. The project's comprehensive modules, from user authentication to secure chat functionalities, showcase a holistic approach to

protecting user data. However, the project also prompts discussions on the balance between security and user convenience, the ethical considerations of facial recognition technology, and the potential need for regulatory compliance. As the project moves forward, these discussions will be crucial in refining its approach to ensure it not only meets the technical and security expectations but also addresses broader societal and ethical concerns.

VII. CONCLUSION

"PROTECTING USER DATA IN PROFILE MATCHING SOCIAL NETWORKS" project has demonstrated a pioneering approach to enhancing security and privacy on social media platforms, particularly within the context of matrimonial services. By integrating advanced facial recognition technologies with a comprehensive suite of user interaction and data protection features, the project sets a new standard in safeguarding user data against unauthorized access. Its success lies not just in its technological innovations, such as the use of the Haar Cascade algorithm for secure login and blink detection for live person verification but also in its commitment to user privacy and secure communication. As the project concludes, it stands as a testament to the potential of combining cutting-edge technology with robust data protection practices to create safer online spaces for users. The insights gained and the challenges overcome during this project pave the way for future endeavors in the field of online security and privacy.

FUTURE SCOPE

The future scope of the project is vast and promising, offering numerous avenues for enhancement and expansion. As technology evolves, integrating more advanced AI and machine learning algorithms could significantly improve facial recognition accuracy and user authentication processes. The potential for incorporating real-time behavior analysis to detect and prevent fraudulent activities further underscores the project's commitment to security. Additionally, exploring decentralized data storage solutions, such as blockchain, could offer even greater levels of data privacy and security, setting a new benchmark in user data protection. The project's adaptable architecture also allows for the integration of emerging technologies and platforms, ensuring its relevance and effectiveness in a rapidly changing digital landscape. Overall, the project is well-positioned to lead innovations in online security and privacy, making it a crucial model for future developments in social media and beyond.

REFERENCE

1. Dictionary.com: Definition of Reciprocal. http://dictionary.reference.com/browse/reciprocal, visited on 2015-05-09.
2. Statistics Finland: Finland in Figures (2013). http://www.stat.fi/ tup/suoluk/suoluk_vaesto_en.html, visited on 2015-02-23.
3. Adomavicius, Gediminas and Tuzhilin, Alexander: Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions. IEEE Transactions on Knowledge and Data Engineering, 17(6):734–749, June 2005.
4. Agrawal, Manish, Karimzadehgan, Maryam, and Zhai, ChengXian: An Online News Recommender System for Social Networks. In Proceedings of the Workshop on Search in Social Media, 2009, ISBN 3838315642.
5. Akehurst, Joshua, Koprinska, Irena, Yacef, Kalina, Pizzato, Luiz, Kay, Judy, and Rej, Tomasz: CCR - A Content-Collaborative Reciprocal Recommender for Online Dating. In Proceedings of the 22nd International Joint Conference on Artificial Intelligence, pages 2199–2204, 2011.
6. Akehurst, Joshua, Koprinska, Irena, Yacef, Kalina, Pizzato, Luiz, Kay, Judy, and Rej, Tomasz: Explicit and Implicit User Preferences in Online Dating. In New Frontiers in Applied Data Mining, pages 15–27. 2012. Amatriain, Xavier, Pujol, Josep M, and Oliver, Nuria: I Like It... I Like It Not: Evaluating User Ratings Noise in Recommender Systems. In User Modeling, Adaptation, and Personalization, pages 247–258. 2009.
7. Auer, Peter, Cesa-Bianchi, Nicolò, and Fischer, Paul: Finite-time Analysis of the Multiarmed Bandit Problem. Machine Learning, 47(2-3):235–256,2002.