

Multiple Account Detection

Sinisandal¹, Arhath Kumar²

¹Student, Department of MCA, NMAM Institute of Technology, Karkala, India

²Professor, Department of MCA, NMAM Institute of Technology, Karkala, India

Abstract: Multiple account detection is an application that allows the system to track the location when first time the account is created. And compare the distance. If it possible to cover the distance, then it would be considered as normal operation else it would be blocked.

Keywords: multiple account detection

1. Introduction

Multiple account detection is an application where it will check where first time the account was created. For example, assume that you have created your first account in Bangalore, that time it detects the location. In this case, each login will track the location and compare the distance of the login. If it's possible to cover the distance of the time difference between the two logins then it would be considered as a normal operation else it would be blocked.

It will filter the words which it considers as vulgar. The users can store the words which they consider as vulgar in the database. If the message contains the words stored in the database then those words will be filtered out. That is those words will be in the form of asterisk.

2. Literature survey

[1] Respiration rate, electrocardiograph, blood pressure and galvanic skin resistance were used as features with mechanical scribbles for deception detection by Yong et al in 2011. Multimodal dataset consisting of physiological, thermal and visual responses of subject under the three scenarios of deception i.e. Mock Crime, Best Friend and Abortion were also found to be suitable for deception detection.

[2] Statistical analysis of differences between deceptive and truthful settings using physiological and thermal response were presented in Polygraph test (Deception) at airport by thermal image captured at different stages i.e. acquisition, physiological correlation and classification was conducted in Warmelink et al. pointed increment in the liars skin temperature as compared to the truth tellers. They reported 64 % of non-deception and 69% of deception correctly.

[3] The thermal image camera increases the performance to 72 % of truth and 77 % of liars correctly. Thermodynamic modeling of images acquired by thermal camera for finding the blood flow rate at the face of the subject was also reported.

3. Problem description

For a social media environment, which often involves database with large volumes of data, the case of blocked users initiating new accounts, often called sock puppetry are widely known and past efforts which have attempted to detect such users, have been primarily based on verbal behavior. Although these methods yield a high detection accuracy rate they are computationally inefficient for the social media environment.

4. System security

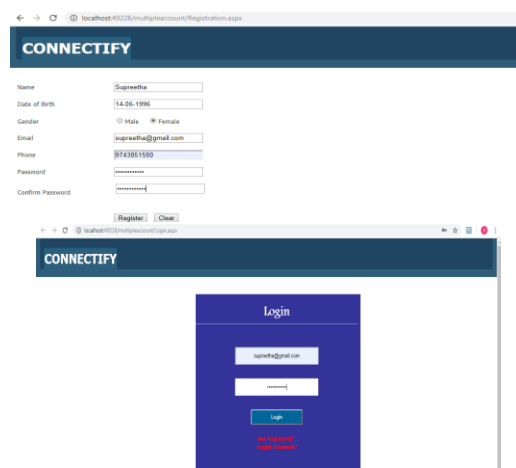
A. Email verification

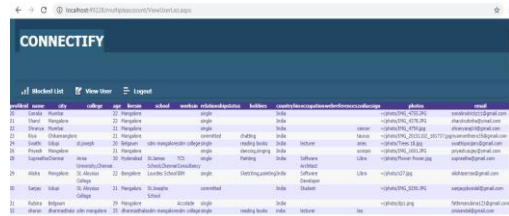
When the users register into the application for the first time, he has to fill all the required information to precede registration. Once registered, an OTP number will be sent to his Email for verification, without verifying his mail, the user cannot login to the particular application. When the user enter the OTP into the application and click ok, then registration will be completed and user can login to the application.

B. Phone number verification

When the users register into the application for the first time, he has to fill all the required information to precede registration. Once registered, an OTP number will be sent to his phone for verification, without verifying his phone, the user cannot login to the particular application. When the user enter the OTP into the application and click ok, then registration will be completed and user can login to the application.

5. Screenshots



id	name	email	age	gender	location	relationship	status	phone
21	Carla	carla@gmail.com	22	Female	Surabaya	single	single	+629121234567
22	Wati	wati@gmail.com	21	Female	Surabaya	single	single	+629121234567
23	Shara	shara@gmail.com	21	Female	Surabaya	single	single	+629121234567
24	Rani	rani@gmail.com	21	Female	Surabaya	single	single	+629121234567
25	Shafa	shafa@gmail.com	21	Female	Surabaya	single	single	+629121234567
26	Frank	frank@gmail.com	21	Male	Surabaya	single	single	+629121234567
27	Yusuf	yusuf@gmail.com	21	Male	Surabaya	single	single	+629121234567
28	Yusuf	yusuf@gmail.com	21	Male	Surabaya	single	single	+629121234567
29	Yusuf	yusuf@gmail.com	21	Male	Surabaya	single	single	+629121234567
30	Yusuf	yusuf@gmail.com	21	Male	Surabaya	single	single	+629121234567
31	Yusuf	yusuf@gmail.com	21	Male	Surabaya	single	single	+629121234567
32	Yusuf	yusuf@gmail.com	21	Male	Surabaya	single	single	+629121234567
33	Yusuf	yusuf@gmail.com	21	Male	Surabaya	single	single	+629121234567
34	Yusuf	yusuf@gmail.com	21	Male	Surabaya	single	single	+629121234567
35	Yusuf	yusuf@gmail.com	21	Male	Surabaya	single	single	+629121234567

Fig. 1. Implementation

6. Conclusion

Despite the explosive growth of social media applications and networks, deception in social media environment is an area that has not received commensurate attention from researchers, designers, and developers. There are automated solutions that guarantee higher detection rates than human detection but the computational challenges of monitoring verbal communications are many. Non-verbal behavior monitoring for deception detection is an alternative path that can be used as a leading or complimentary detection solution. A coordinated effort is required to test these solutions on different platforms and advance the field of social media identity deception detection.

References

- [1] M. Tsikerdekis and S. Zeadally, "Multiple Account Identity Deception Detection in Social Media Using Nonverbal Behavior," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 8, pp. 1311-1321, Aug. 2014.
- [2] M. Tsikerdekis and S. Zeadally, "Online deception in social media," *Commun. ACM*, vol. 57, no. 9, Sep. 2014.
- [3] X. (Sherman) Shen, "Security and privacy in mobile social network," *IEEE Netw.*, vol. 27, no. 5, pp. 2-3, Sep/Oct. 2013.