

Fake Social Media Accounts and Their Detection

- Problem Statement ID – SIH1775
- Problem Statement Title- Fake Social Media Accounts and Their Detection.
- Theme- Blockchain & Cybersecurity
- PS Category- Software
- Team ID- 1958



Fake Social Media Accounts and Their Detection

❖ Proposed Solution

- Fake social handle detection can be brought into the experiment by considering the point where a user is supposed to sign in to an app with a few of his details like his/her Full Name, Email, Password, Gender, Birth date, and a unique Username the one has to be identified with, by analyzing these data and figuring out if the user's Full Name is somewhere completely distinct than his/her email ID.
- As the full name and email ID domain of a legit user should generally match, a completely different domain indicates that the person is either running a company and is using his business domain there or he has created an unauthorized email with his pen name as his email domain or the user is just looking out to hide his/her identity by providing an illegitimate email id, or vice versa in the case if one is making it with his/her Name.
- To add to this, the phone no. user is registering his/her account with can be checked if it is already connected to any other account. Most of the time an illegitimate user can manage to fake his/her email ID and his/her name and email ID, but generally switching between phone numbers is not a casual thing until the case is about a bigger scam. After a user trespasses these criteria he/she is to be added to the database under the "Red Flag Users" node.

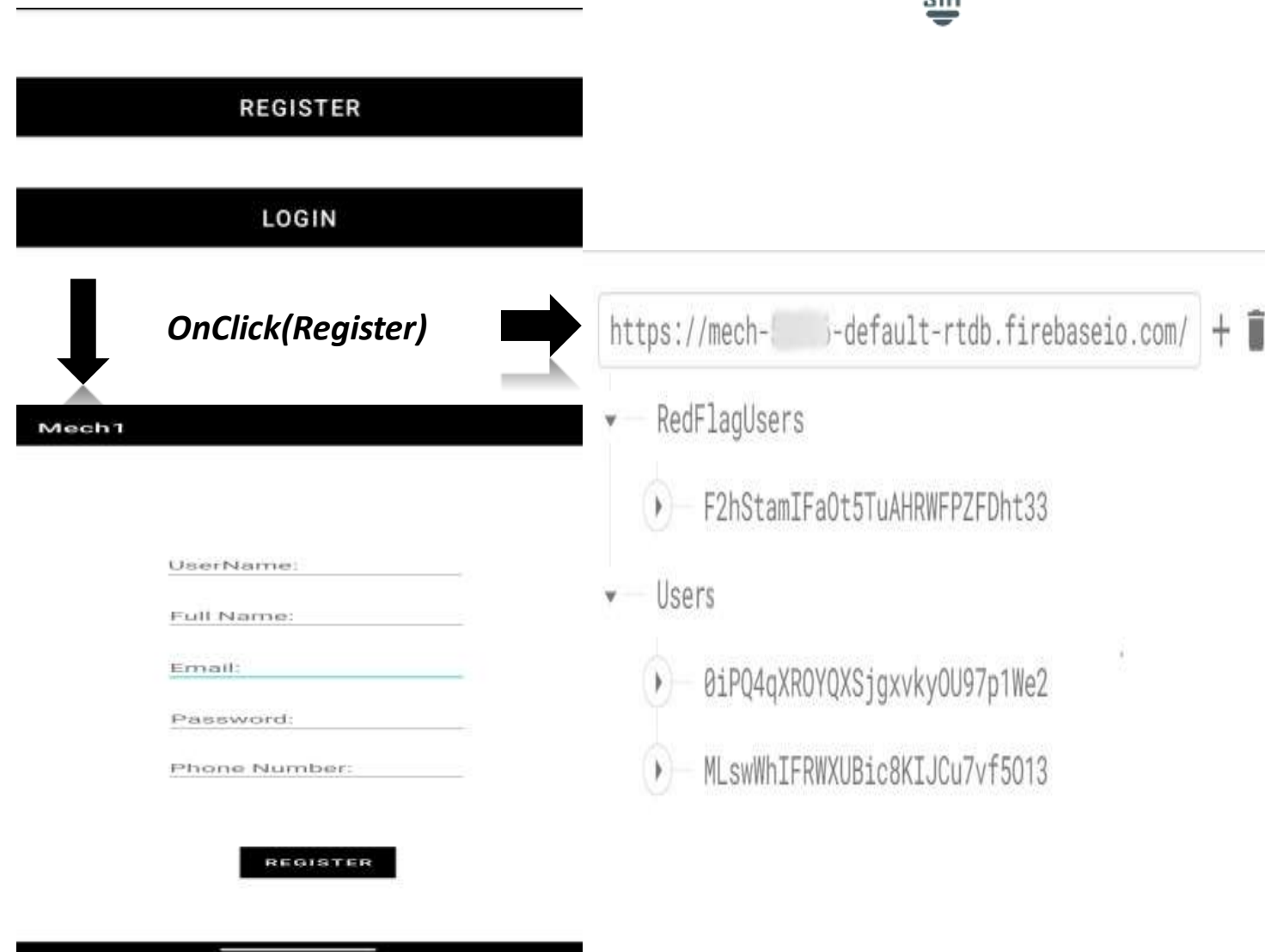
TECHNICAL APPROACH

- The fake profile detection app will leverage Firebase for authentication, database management, and real-time tracking.
- Upon user registration, the submitted credentials (such as name, email, and other details) will be checked against existing records. If the credentials match to a reasonable extent, the user is considered legit. If significant discrepancies are found, the system will flag the account with an orange alert, stored in the Firebase database.
- If additional reports are submitted against the orange-flagged account, the flag will escalate to red. The app will primarily monitor red-flagged users, tracking their activities for further investigation, while both orange- and red-flagged profiles will be maintained in categorized collections for continuous tracking and analysis.
- The application will also feature a user-friendly interface for reporting suspicious profiles, with Firebase handling the data sync and updates in real-time.



FEASIBILITY AND VIABILITY

- Here's a blueprint of our app's data collecting interface.
- Next to it is an image illustrating the required user credentials for app sign-in.
- Once the user submits this data his/her **UserName**, **Full Name**, and **Email ID** are analyzed, if these three have any connecting dots between them.
- Based on the analysis, the user data is pushed to the database and categorized into “**Users**” and “**Red Flag Users**”.



How is Red Flag helping me?

- For an account registered under Red Flag Users, if another user encounters this type of profile, the user on this end is notified about the possibility of the other user maintaining a fake account. This notification is typically indicated by a red flag marker somewhere on the suspicious user's profile.
- However, as mentioned earlier every Red Flag User shouldn't be directly considered as a fraud. Some users may be operating business profiles or promotional channels without being well-versed in the use of verified or business accounts for these purposes.
- But not every nerd is actually innocent, so here comes the role of "The Red Flag". This works for a genuine user exercising him to be cautious beforehand while making any contact with such profiles.

What is My Role?

- While you are on social media, it is important to take care not to exceed the limits of access to your personal data.
- Being social is a trend, but anything beyond a certain limit is hazardous. The way similar thing is to be considered before sharing each and every update of your daily schedules or posting and updating profiles with the photos which are actually meant to be kept in-box.
- The most important role of a genuine user is to never ever share any of his/her personal details while communicating with a Red Flag User. Consider adjusting your privacy settings to hide your posts from such accounts.

RESEARCH AND REFERENCES



- The proposed fake profile detection system draws inspiration from the operational framework of the Truecaller app, particularly in its approach to identifying and categorizing potentially malicious users.
- Much like Truecaller flags phone numbers based on crowdsourced reports and historical data, this system flags user accounts based on credential mismatches and community reports.
- Just as Truecaller escalates user classifications from unknown to spam based on frequency and severity of reports, this system transitions users from an orange flag to a red flag, indicating a higher risk of fraudulent behavior. The Firebase backend serves as the foundation for real-time flagging and database management, similar to how Truecaller relies on cloud-based infrastructure to update its data dynamically.