IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Enhancing Social Media Security Through Three-Step Verification

[1]Omkar Santosh Kadam, [2]Aditya Arjun Kadam, [3]Siddhant Dhanaji Kadam,[4]Mrs.Nutan Vikas Patil

[1,2,3]Students, [4]Assistant Professor,

[1,2,3,4] Computer Science And Engineering Department,

Abstract: Since social media platforms are still necessary for worldwide communication, strong security measures are now imperative. A three-step verification procedure is recommended by this study to increase the security of user accounts on social networking sites. The conventional username-password authentication mechanism may be vulnerable to a variety of cyber threats, of which phishing attempts and password leaks are just two examples. The initial stage establishes a foundational security layer using traditional username-password authentication. The second stage introduces MFA.the suggested three-step verification system reduces the danger of illegal access. Conventional username-password authentication is used in the first phase to create a basic security layer. In the second phase, MFA is introduced. It provides an extra layer of authentication to prevent hacked login credentials by sending OTPs to the user's registered.

Keywords **– Mulitfactor Aurthentication (MFA),one-time passwords(OTP),Addharcard verification.**

I. Introduction

A subset of artificial intelligence called machine learning gives a machine the ability to learn from data automatically, perform better based on past performance, and make predictions. A collection of algorithms used in machine learning process vast amounts of data. These algorithms are fed data to train them, and then they use the training data to develop a model and carry out a specified task. 1.1 Machine learning types: With cutting-edge hashing and secure government ID integration in our cutting-edge social media platform, we are reinventing digital interactions. By assessing and reducing the impact of negative remarks, machine learning algorithms actively promote a positive online environment. Our welcoming interface encourages inclusive interest based groups and a variety of multimedia content, strengthening user connections. Users are empowered by transparent data privacy options, and upcoming features will push the limits of online interaction with augmented reality filters and virtual reality venues. By fusing security, authenticity, and engaging experiences, we are at the vanguard of social media, changing digital relationships for a self-assured and imaginative community.

II. OBJECTIVE

- To awareness about social responsibility.
- To add the new authentication level.
- To secure the social network.
- To protection from attacks.

III. SYSTEM ARCHITECTURE

The user inputs their personal information, including their password, username, and other identifying details. The system uses a cryptographic hash function to transform the user's data into a fixed-size hash value. The hash value is kept by the system in a database or another safe place. A mathematical algorithm known as the hash function converts a variable-length input into a fixed-length output. The result is referred to as a message digest or hash value. The following qualities of a good hash function are present:

•Originality:Two distinct inputs ought to yield two distinct hash values.

• Collision resistance: Finding two distinct inputs that result in the same hash value ought to be challenging.

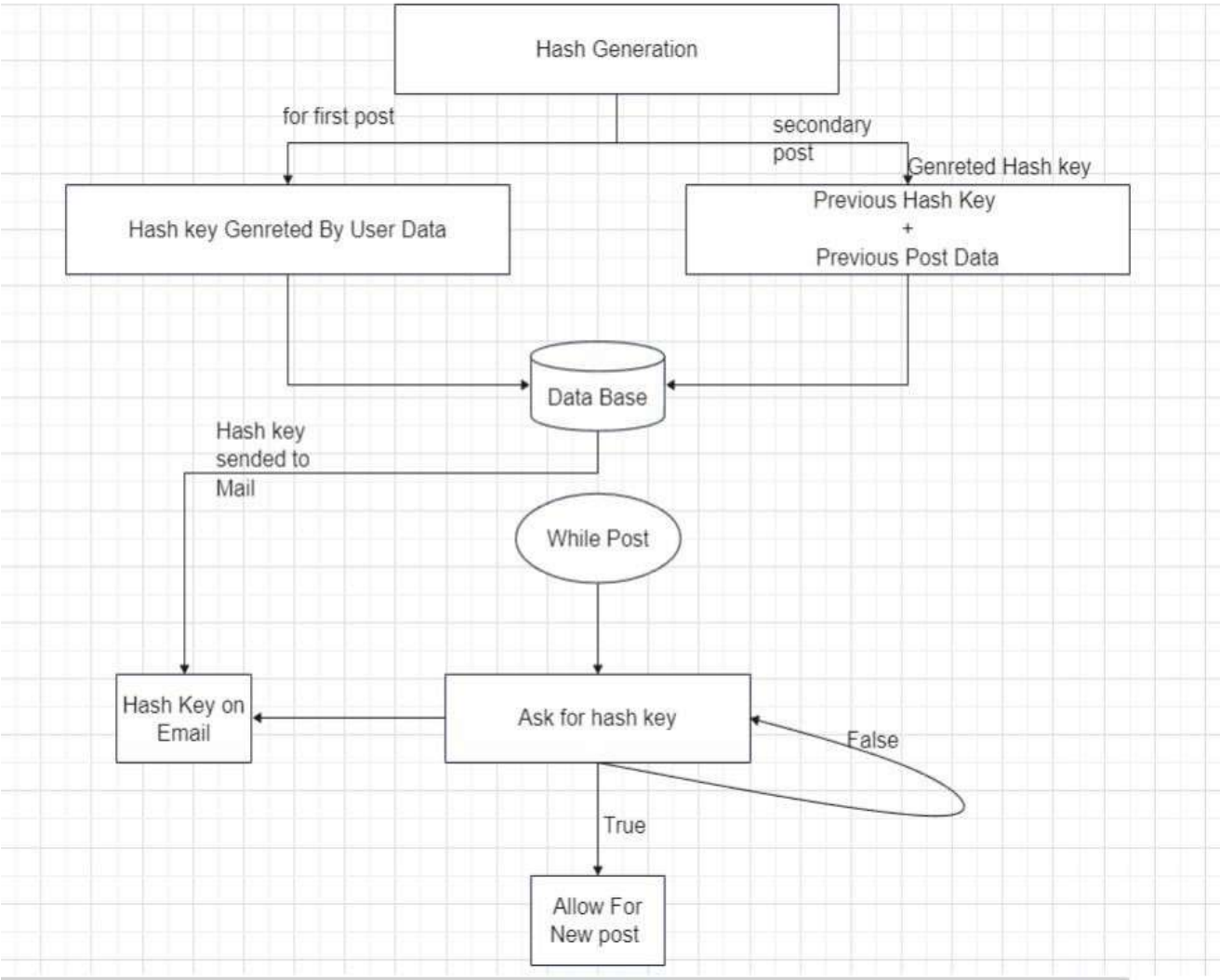

FIG.2.1. SYSTEM ARCHITECTURE

I. RESEARCH METHODOLOGY

3.1Data Flow Diagram

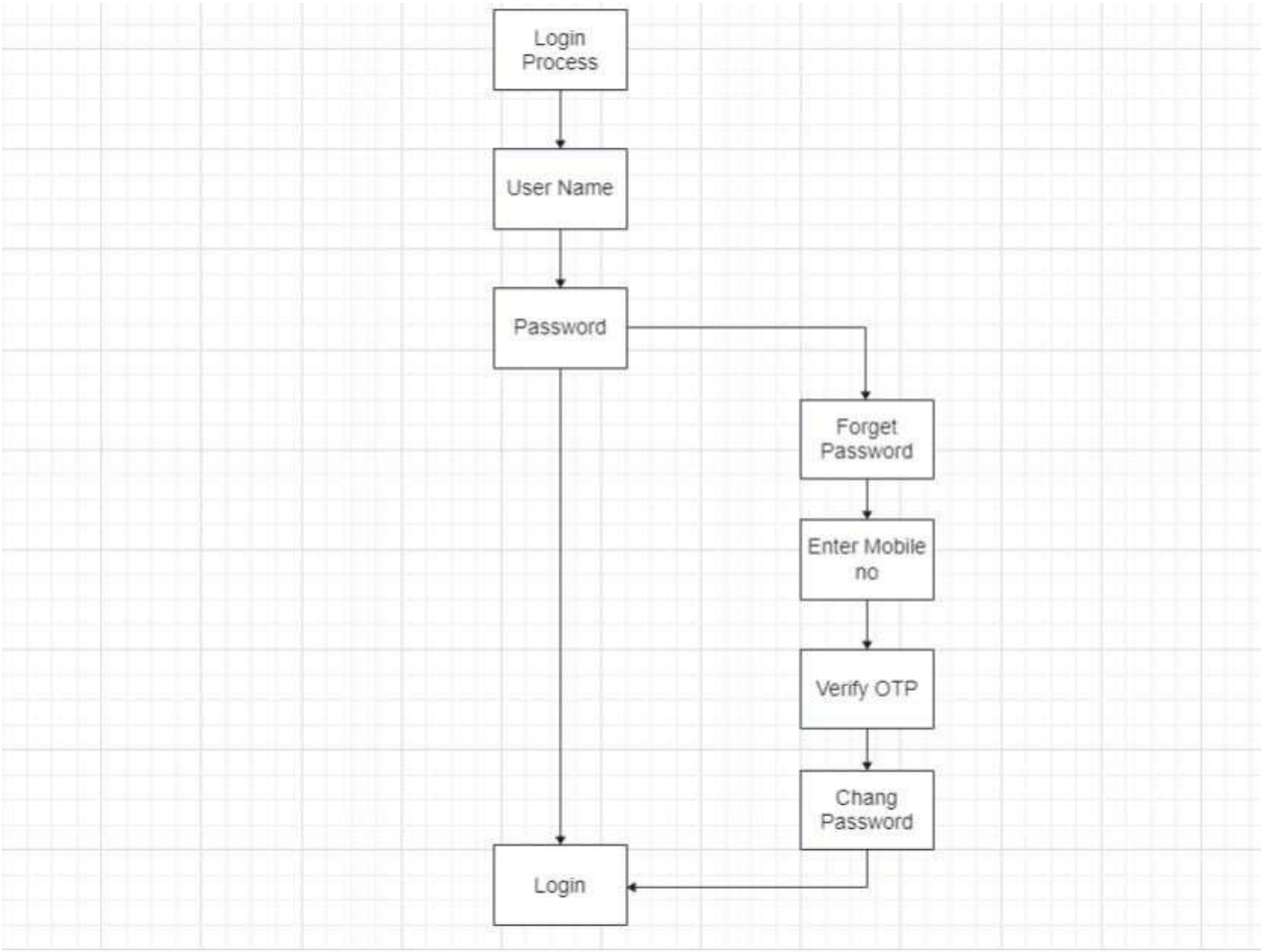

Fig 3:1 Data Flow Diagram

Users interact with the website by entering their username and password into the login form. Upon submission, the website processes this information by verifying the provided credentials against its database. If the credentials match an existing user record, indicating they are valid, the user is successfully logged in and granted access to their account. However, if the credentials do not match any records in the database, indicating they are invalid, the user is prompted to try again, typically by displaying an error message. Additionally, the website offers two supplementary options for users who encounter issues with their password. If a user forgets their password, they can initiate a password reset process by selecting the "Forgot Password" option. This typically involves confirming the user's identity through email verification or security questions before allowing them to set a new password. Similarly, users who wish to change their password for security reasons or personal preference can do so by selecting the "Change Password" option. This option typically requires the user to authenticate themselves by entering their current password before allowing them to specify a new one. These additional options provide users with mechanisms to manage their account security and regain access to their account in the event of a forgotten password.

3.2 Use Case Diagram

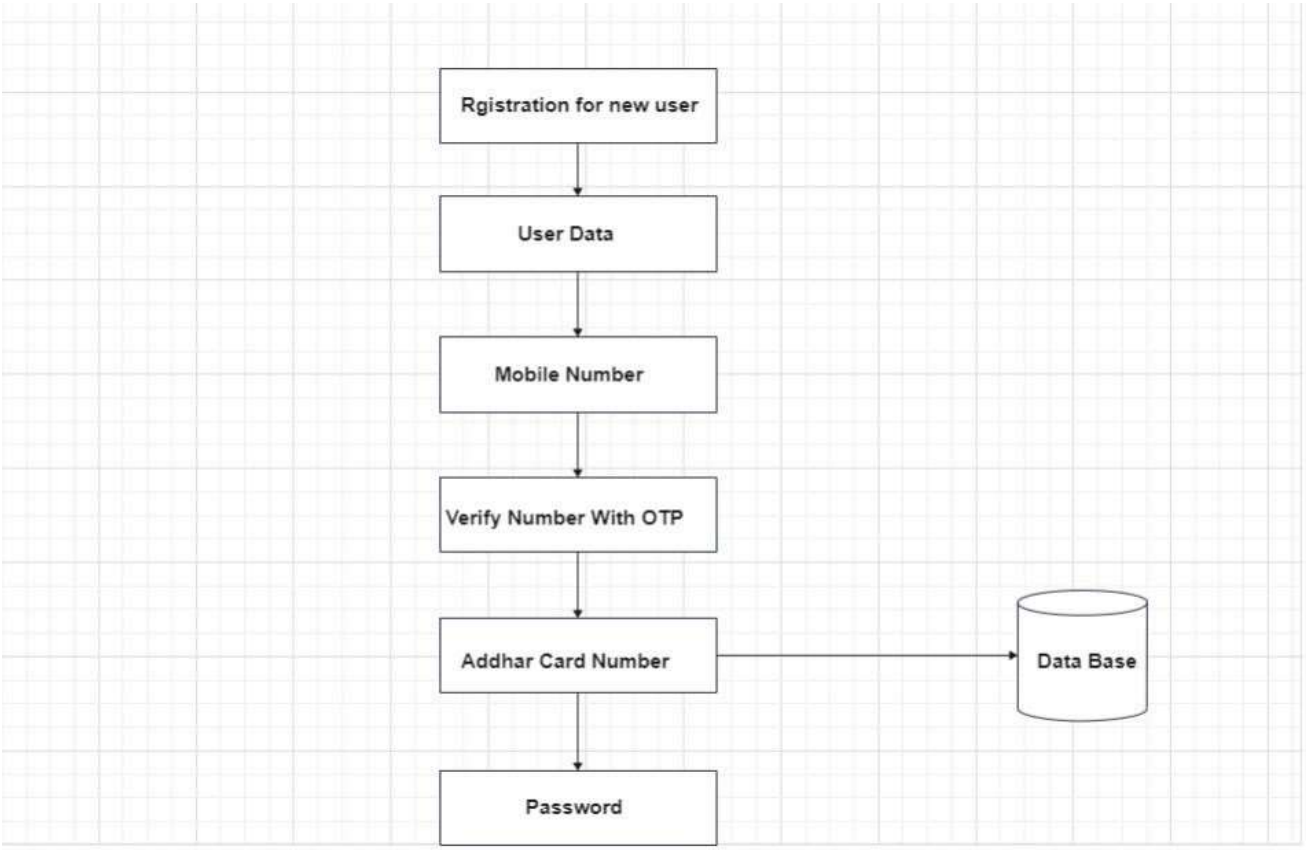

Fig 3:2 Use Case Diagram

The registration process begins with users entering their personal details such as name, email address, and other relevant information. This data is essential for creating their account and enabling access to the website or application. Following this, users are prompted to input their mobile number, which serves as a pivotal step for identity verification. (OTP) is sent to the provided mobile number to authenticate the user's identity. Upon receiving the OTP, users must input it into the system to confirm access to the registered mobile number. Next, users are required to input their Aadhaar card number, a unique identification number issued to Indian citizens. This step is crucial for completing the registration process. Subsequently, all provided user data is securely stored in the website or application's database. This stored data is then utilized for user authentication and to facilitate account access. Finally, users are prompted to set a password for their account, which acts as a protective measure to safeguard their account. Through these sequential steps, users can successfully register and establish their account within the platform.

IV. RESULTS AND DISCUSSION

4.1 Register Page

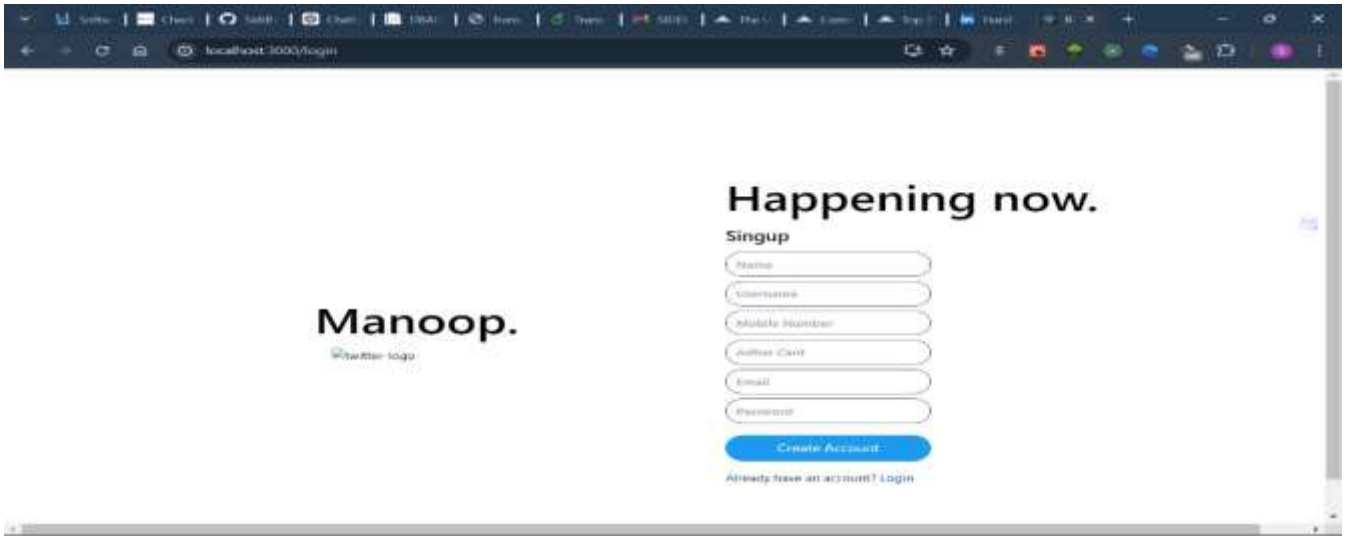

Fig 4:1 Register page

Sign Up To enhance the security and authenticity of user onboarding, a robust sign-up page can be designed incorporating Aadhaar card verification and OTP (One-Time Password) verification for mobile numbers. During the sign-up process, users provide their Aadhaar card details, which are then verified against the UIDAI (Unique Identification Authority of India) database to confirm their identity. Concurrently, an OTP is sent to the user's registered mobile number to ensure that the provided contact information is valid. This dual-layer verification process helps in reducing fraudulent activities and ensures the reliability of the user data collected. Implementing Aadhaar and OTP verification not only strengthens security but also complies with regulatory requirements, providing users with a secure and seamless sign-up experience.

4.2 Login Page

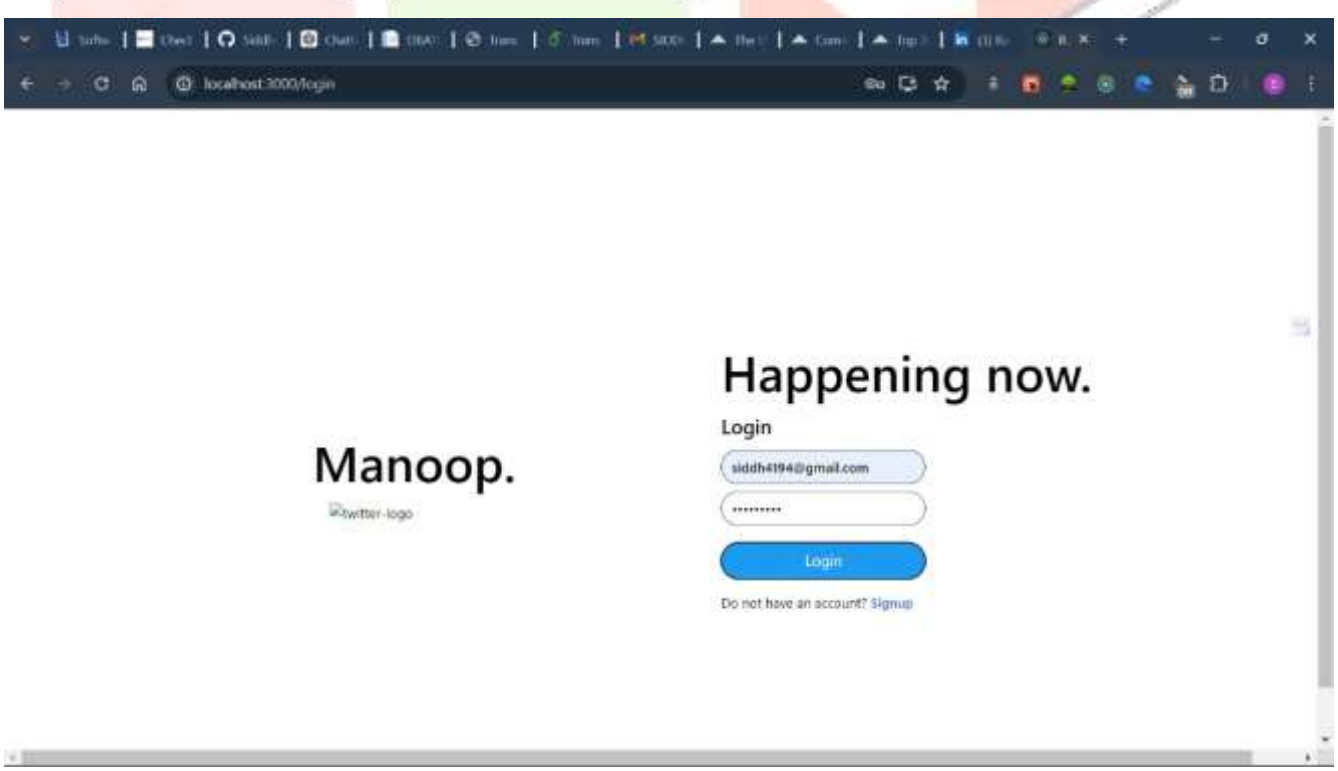

Fig 4.2. Login Page

After authentication user's profile will get created. Then user can be login this system with username and password. Click the green "Login" button to submit your credentials and access your account.

4.3 OTP Page

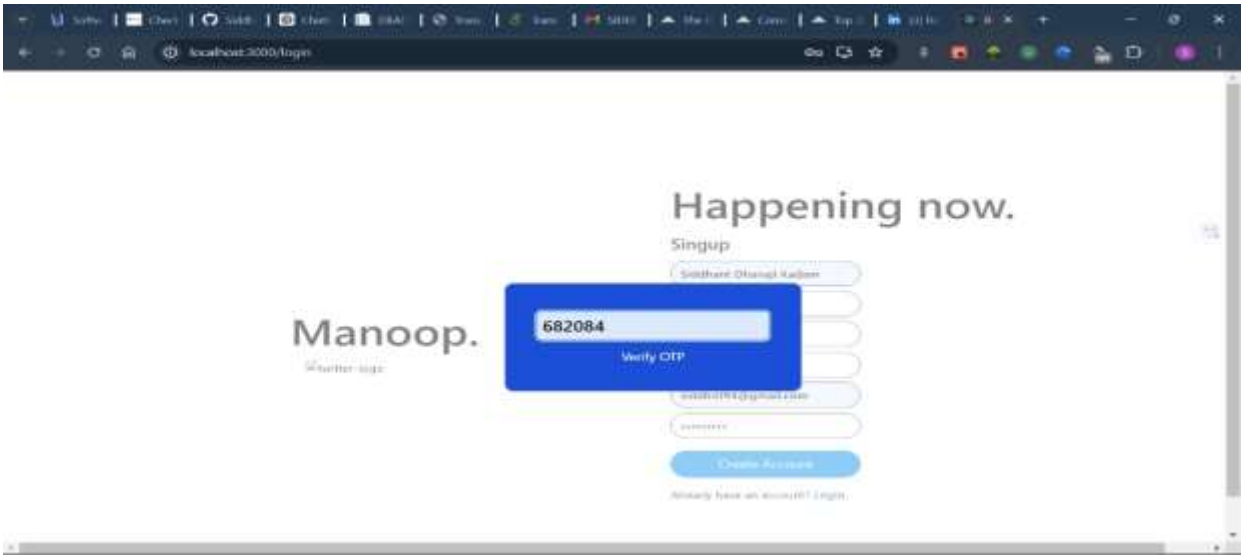

Fig 4.3 OTP Page

Twilio JS is utilized for generating and validating OTPs (One-Time Passwords) to ensure secure mobile number verification. It seamlessly integrates with the sign-up process, sending OTPs to users' mobile numbers and validating them upon entry. This enhances security and user trust by adding a reliable verification layer.

4.4 Hash Key

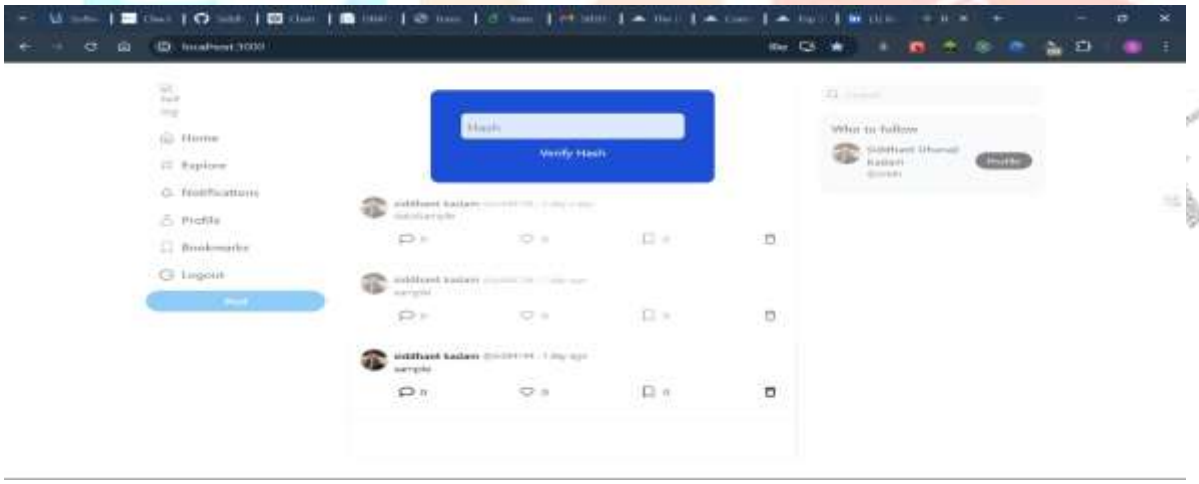

Fig 4.4 Hash kay

As part of the third step of the verification process, a unique hash key is required for every post made on the platform. This hash key is shared with users via email to ensure secure communication and identity confirmation. For new users, a hash key is generated based on their provided information during the sign-up process. Users must then enter this hash key into a dedicated input field to verify their identity. Only upon successful verification of the hash key can users proceed to the next step, such as creating or interacting with posts. This additional security measure ensures that only verified users can engage fully with the platform, significantly reducing the risk of unauthorized access and enhancing overall trust and security. By incorporating this step, the platform demonstrates a strong commitment to safeguarding user data and maintaining the integrity of interactions.

IV. CONCLUSION

Implementing a three-step Aadhar card verification process on social media platforms represents a commendable initiative to enhance user authentication and security. In the first step, users would be required to link their Aadhar card to their social media accounts, providing a robust foundation for identity validation. Subsequently, a biometric verification step could be introduced, leveraging Aadhar's biometric data to ensure a more foolproof authentication process. Finally, a one-time password (OTP) sent to the mobile number linked with the Aadhar card could serve as the third and final verification step, adding an additional layer of security. This three-step process not only streamlines the verification procedure but also significantly reduces the risk of impersonation and unauthorized account access. In conclusion, the integration of Aadhar card verification in social media authentication processes promises to fortify digital identities, mitigate fraud, and bolster the overall security posture of online platforms.

REFERENCES

[1]M. M. Rahman , Muhammad Abdullah Adnan; “Two Step Verification System of Highly Secure Social Media: Possible to Breach the Security”, Department of CSE, BUET. 5-8 January, 2017

[2]McKringle Xolani Mhlanga; Richard Rabin Maiti; Bennet Hammer“Privacy and Security Matters Related To Use Of Mobile Devices and Social Media” , INSPEC Accession 10-13 March 2021

[3]Ruslan Shevchuk; Yaroslav Pastukh; “Improve the Security of Social Media Accounts” INSPEC Accession,2019

[4]caroline Oehri, Stephanie Teufel, “ Social Media Security Culture The Human Dimension in Social Media Managemen”, INSPEC Accession: 15-17 August 2018

[5]Lei Li; Kai Qian;“ Using Real-Time Fear Appeals to Improve Social Media Security INSPEC Accession , 10-14 June

[6]Heidi Wilcox; Maumita Bhattacharya; “A framework to mitigate social engineering through social media within the enterprise” INSPEC Accession /2018