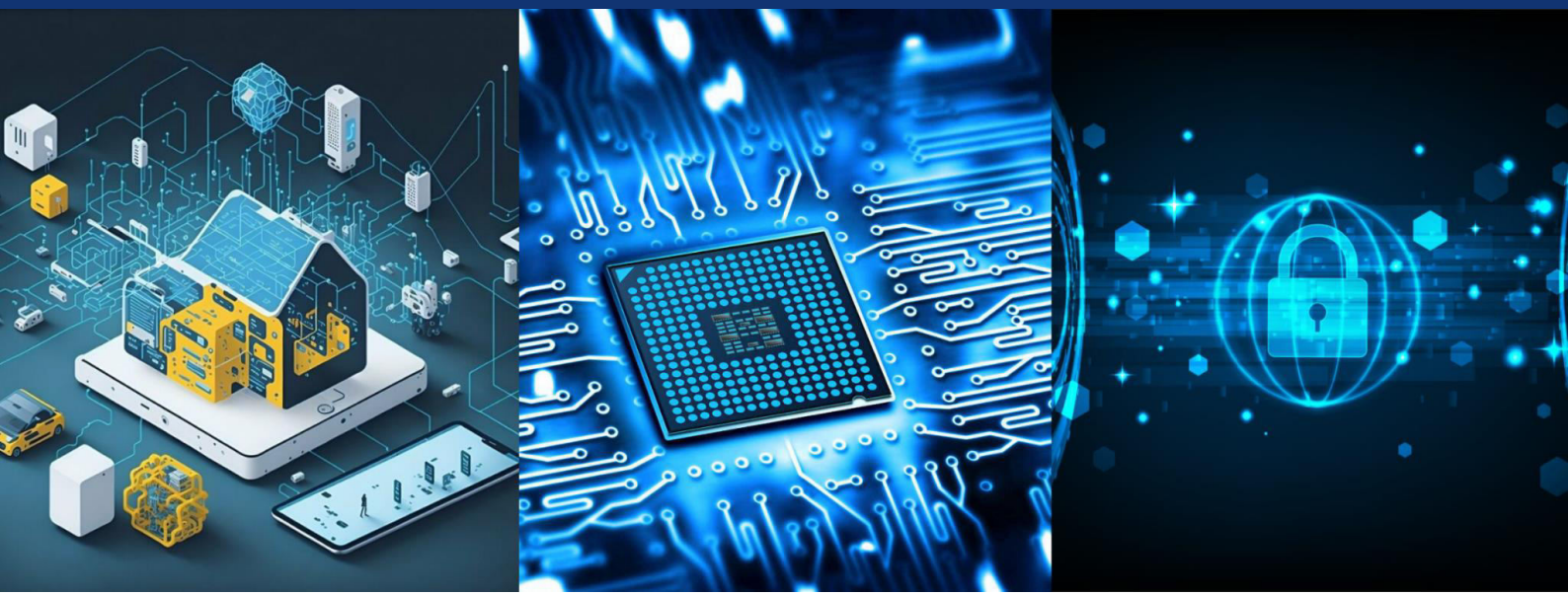
IJIRCCE

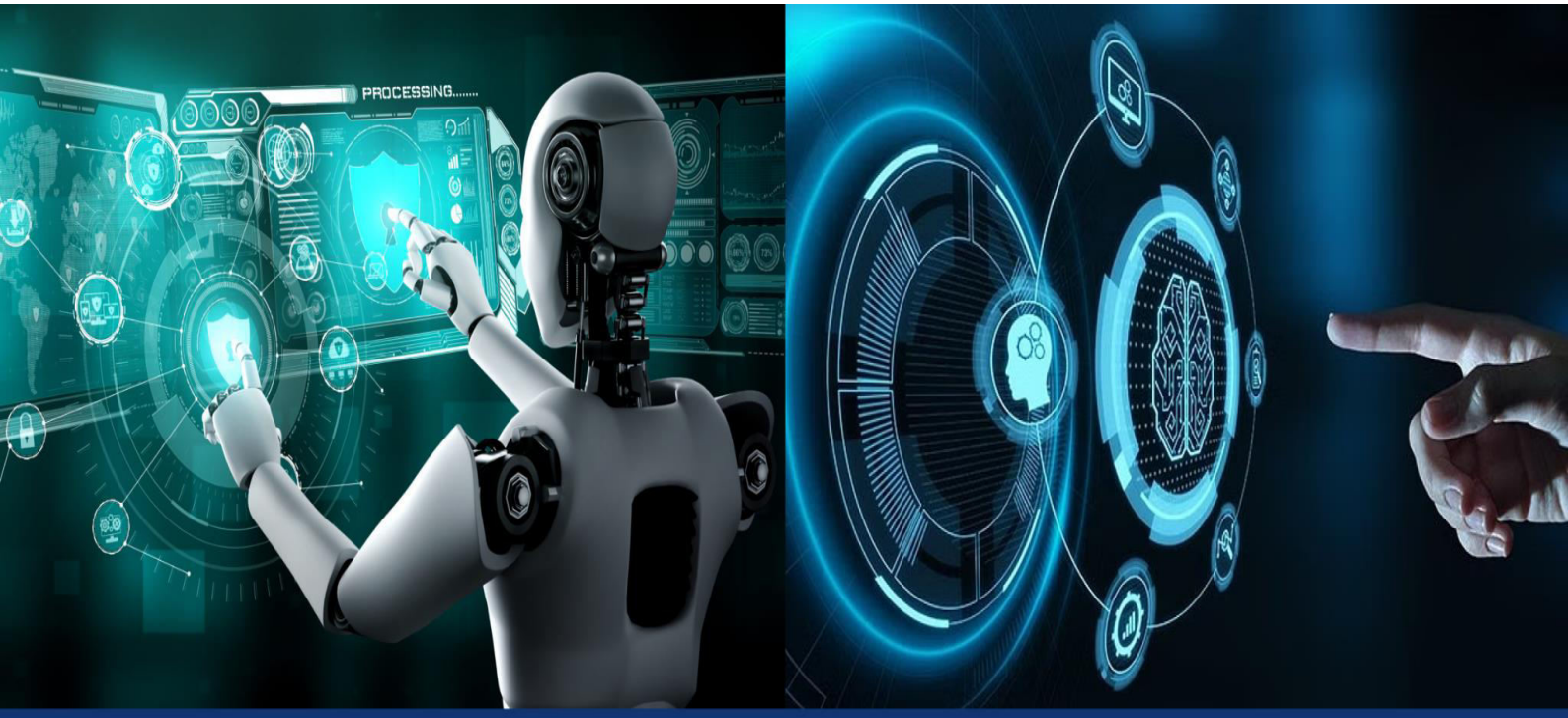
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 5, May 2025

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305192

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Fake ID and Image Forgery Detection in Social Media using Machine Learning

D. Sangeetha[1], Varsha K S[2] Janat Peter[3], Soniya C M [4]

Assistant Professor, Dept. of IT, Jaya Engineering College, Chennai, Tamil Nadu, India[1]

UG Student, Dept. of IT, Jaya Engineering College, Chennai, Tamil Nadu, India[2-4]

ABSTRACT: FaceTrace is a comprehensive, AI-powered web application built to detect and prevent the misuse of digital identities on major social media platforms including Facebook, Instagram, Twitter, and LinkedIn. In an era where fake profiles, impersonation, and manipulated images are increasingly used for cyber fraud, scams, and misinformation, FaceTrace offers an intelligent, multi-layered defense mechanism. The application integrates key technologies such as machine learning, computer vision to assess and validate the authenticity of user profiles. Users begin by securely registering or logging into the system through a backend built with Flask and MongoDB. Once inside, users can input any public social media profile URL or identifier, and the system will fetch corresponding data through connected social media APIs (or dummy datasets when API access is limited). This includes crucial attributes such as the username, display name, email, bio, follower count, and profile image. These collected data points are processed through a trained Support Vector Machine (SVM) classifier, which has been built on real and fake user data patterns to accurately detect anomalies and inconsistencies that typically signify a fake account. Simultaneously, uploaded or retrieved profile pictures are passed through a robust image forgery detection module that leverages OpenCV and MD5 Hashing algorithms. This module detects various forms of image tampering such as copy-move forgery, splicing, or even AI-generated facial images, thereby confirming whether the profile picture is genuine or manipulated. The analysis results from both the machine learning model and the forgery detection engine are combined to give a comprehensive trust score for the profile. The application's frontend is developed using React.js and styled with CSS to provide a smooth, responsive, and user-friendly interface. The dashboard mimics real social media environments, allowing users to navigate intuitively and compare multiple analyzed profiles side by side. Each verification entry is recorded with a timestamp and hashed data, making it impossible to alter previously validated information, thus enhancing trust and traceability in future verifications. To ensure complete functionality, FaceTrace also includes a fully working contact form, enabling users to provide feedback.

KEYWORDS: Machine Learning (ML), Digital Security, Fake ID Detection, Image Forgery Detection, MD5 Hashing, OpenCV.

I.INTRODUCTION

In today's digital world, social media platforms play a crucial role in connecting individuals across the globe. However, with the rapid growth of these platforms, concerns regarding fake identities, image manipulation, and cybersecurity threats have significantly increased. Fraudulent activities such as identity theft, deepfake content, and forged documents have created serious challenges for ensuring authenticity and security in online interactions. The unauthorized use of forged images and fake IDs is widely exploited for illegal activities, ranging from cyber fraud to misinformation campaigns, making it imperative to develop advanced solutions for detection and prevention. Currently, most social media platforms rely on manual verification and user reports to identify fake profiles and image forgery. However, these traditional methods are inefficient, time-consuming, and prone to errors, often failing to detect sophisticated forgeries created using AI-Based deepfake technology. With advancements in machine learning and blockchain, automated detection mechanisms can offer a real-time, reliable, and scalable solution to combat these fraudulent activities. This paper proposes an AI-powered detection system that integrates Convolutional Neural Networks (CNNs), Support Vector Machines (SVMs), and OpenCV for image processing and forgery detection. To enhance security, MD5 hashing is utilized for image integrity verification, while Hyperledger Fabric blockchain technology ensures an immutable record of verified identities. Additionally, a two-step verification mechanism is implemented using Firebase, where an image-based alert system notifies users when an unauthorized attempt is made to upload a fake profile picture, providing an added layer of security. By leveraging AI, cryptographic hashing, and blockchain, this research aims to build a robust system that enhances digital trust, privacy protection, and online

authenticity. The proposed approach is expected to improve the efficiency of social media security systems by providing real-time fraud detection and immediate response mechanisms, reducing the risk of identity theft and misinformation spread.

II.SYSTEM MODEL AND ASSUMPTIONS

The proposed system, FaceTrace, is a comprehensive AI-powered web application designed to detect fake identities and image forgeries on major social media platforms such as Facebook, Instagram, Twitter, and LinkedIn. The system follows a client-server architecture, where the frontend, developed using React.js, facilitates user interaction for registration, login, profile submission, and displaying verification outcomes. The backend, implemented using Python Flask, is responsible for handling API requests, processing user data, and invoking various detection modules. It communicates with a MongoDB database for secure storage of user credentials, profile data, and verification logs. The system integrates multiple intelligent modules. Fake ID detection is performed using a pre-trained Support Vector Machine (SVM) classifier, which analyzes user profile features such as username patterns, follower counts, bio content, and other behavioral indicators to distinguish between genuine and fraudulent accounts. Simultaneously, profile images are subjected to an image forgery detection module that leverages OpenCV-based computer vision techniques and MD5 hashing to identify alterations like splicing, copy-move forgery, and deepfake artifacts. To ensure that the identity verification process remains tamper-proof and auditable, each verification result is hashed and recorded on a Hyperledger Fabric blockchain network. This immutable record helps maintain long-term integrity and trust in the system's outputs.

The system operates under several key assumptions. It assumes that users voluntarily participate by uploading ID images and allowing access to public social media profile data. When APIs are not accessible due to permission limits, structured dummy datasets are used to simulate real-world scenarios. It is assumed that all input images are of sufficient quality to enable forgery detection with high accuracy. The machine learning model is trained on a representative dataset containing both legitimate and fake profiles to ensure generalizability. Additionally, it is presumed that access tokens for social media APIs are valid and that the system operates in a secure and stable network environment. The blockchain component assumes that once data is written, it cannot be modified or deleted, thereby preserving verification history. These assumptions form the foundation for the functional reliability and effectiveness of the FaceTrace system in combating identity-based fraud on social media platforms.

III.EFFICIENT COMMUNICATION

The FaceTrace system ensures efficient communication between its components through asynchronous and parallel processing. The frontend, built using React.js, sends user inputs such as profile URLs and images to the Flask backend via secure HTTPS requests. To reduce response time, the backend executes the Fake ID detection (SVM) and Image Forgery detection (OpenCV) modules concurrently. Social media profile data is retrieved through authorized API calls. If API access fails, the system switches to dummy datasets to maintain flow without delay. Each module processes data independently and shares results back to the frontend in real-time using structured JSON responses. Final outputs, including verification scores and image hashes, are securely stored on a Hyperledger Fabric blockchain. To minimize network overhead, multiple verification entries are batched into a single blockchain transaction. This architecture ensures low latency, high throughput, and secure data handling throughout the verification process.

IV.SECURITY

Security is a fundamental aspect of the FaceTrace system, ensuring the confidentiality, integrity, and authenticity of both user data and verification results. The application incorporates multiple layers of security starting from user authentication, where a secure login and signup system is implemented using encrypted password storage in MongoDB. All data transmission between the frontend and backend is conducted over HTTPS to prevent unauthorized interception or man-in-the-middle attacks.

For detecting profile fraud, the system leverages a machine learning model (SVM) trained on real and fake user data, making it resistant to simple spoofing attempts. Profile images are validated through an image forgery detection module that uses OpenCV and MD5 hashing techniques to identify tampered or AI-generated images. Even minor alterations in image content will result in different hash outputs, ensuring high sensitivity against forgery.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305192

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

To maintain integrity and trust over time, the verification results, including user ID hashes and analysis reports, are securely logged into a private Hyperledger Fabric blockchain. This prevents any tampering or post-verification modification, as each entry becomes immutable once recorded. The system ensures that only verified users can initiate verification requests, and all API tokens and credentials used for social media access are securely managed and expire periodically to reduce security risks.

In addition, FaceTrace implements real-time monitoring and alert mechanisms. Any abnormal verification attempt—such as repeated fake image uploads or access using expired tokens—triggers system-generated alerts to administrators and temporarily restricts the user to prevent abuse. To combat social engineering attempts, user inputs and API responses are validated using strict schema definitions, reducing the chances of injection or manipulation attacks.

The system is also designed to be resilient against future threats such as deepfake images and generative AI-based profile forgeries. By integrating continuous updates to its machine learning models and expanding the training dataset, FaceTrace stays adaptive and responsive to evolving cybersecurity challenges. Furthermore, data minimization techniques are employed—only essential user data is stored, and personally identifiable information is never exposed during processing or logging.

FaceTrace enforces role-based access control (RBAC) to ensure that only authorized users, such as administrators or data analysts, have access to sensitive operational modules. To prevent denial-of-service attacks and API abuse, rate-limiting techniques and CAPTCHA verification are employed at both the client and server ends. The backend also maintains secure logs and audit trails of every verification event, making it possible to trace malicious activity or rollback anomalies during incident response.

The system follows best practices aligned with global data privacy regulations such as the General Data Protection Regulation (GDPR). Backup and disaster recovery mechanisms are also in place to ensure business continuity in the event of system failure or data loss. With this layered approach to cybersecurity—covering infrastructure, application, data, and legal compliance—FaceTrace delivers a secure, trustworthy, and regulation-compliant environment for digital identity verification.

V. RESULT AND DISCUSSION

In the fig 1, it shows the FaceTrace homepage showcasing the platform's AI-driven interface for verifying the authenticity of social media profiles and content.

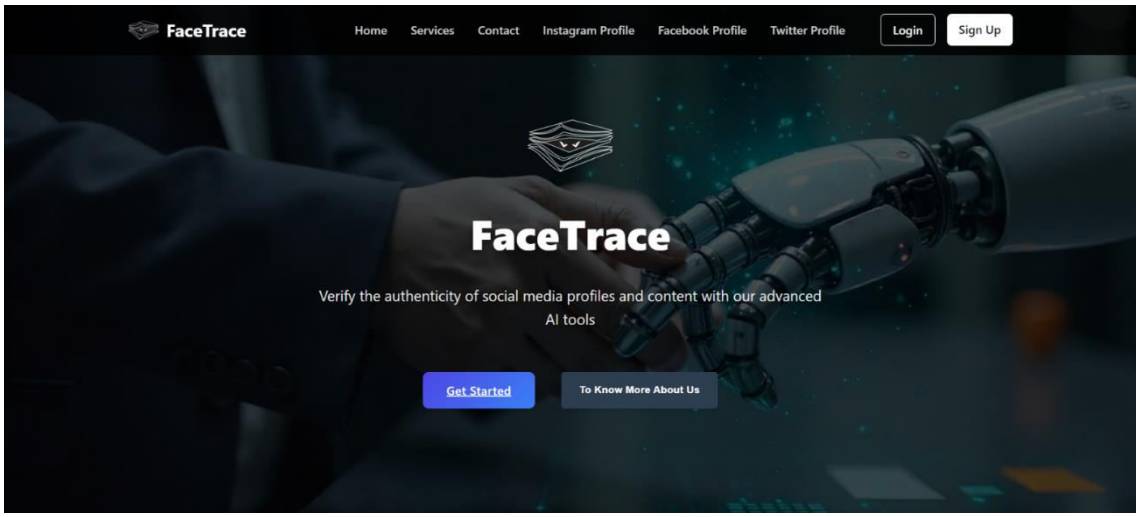


Fig.1 Home Page

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305192

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

In the fig 2, it shows the user registration (sign-up) page for a website called FaceTrace, allowing users to create an account by entering their name, email, and password.

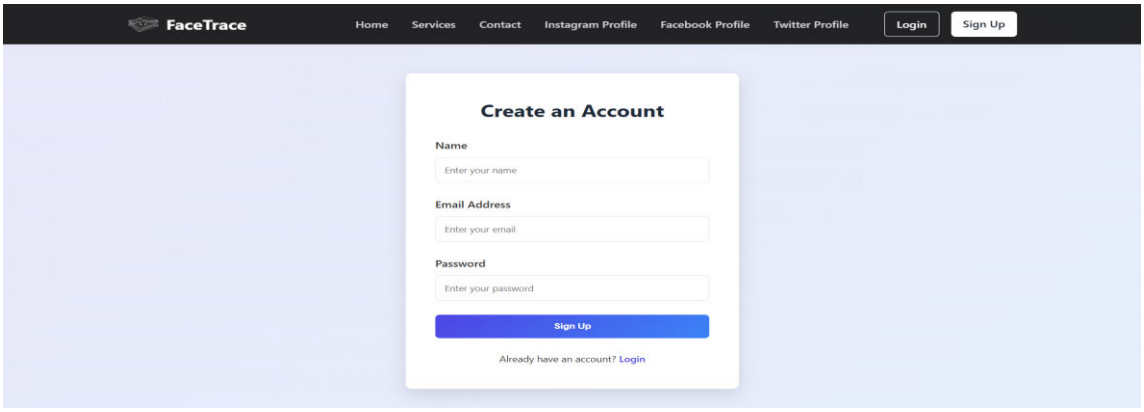


Fig .2 Signup Page

In the fig 3, it shows the user login page for the *FaceTrace* website, allowing users to access their accounts by entering their email and password.

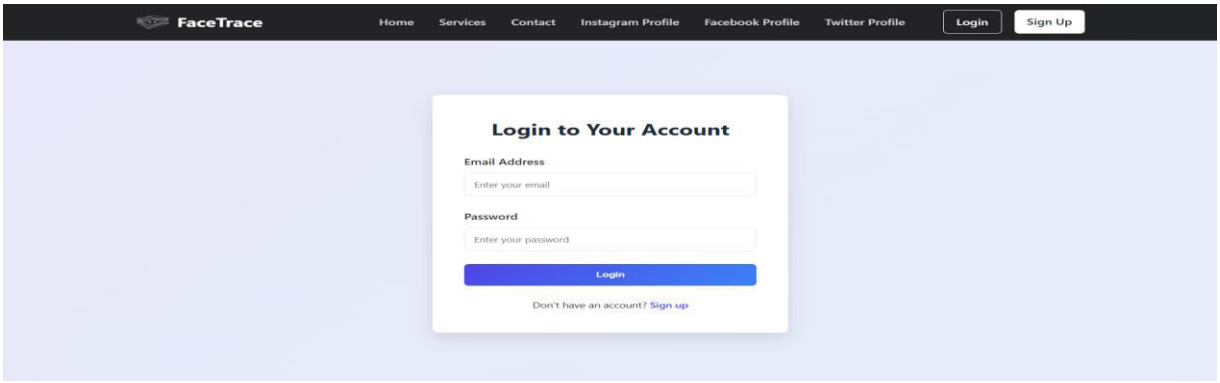


Fig.3 Login Page

In the fig 4, it shows the FaceTrace homepage with a MetaMask login popup, indicating an attempt to connect a decentralized wallet for verifying social media authenticity using AI tools

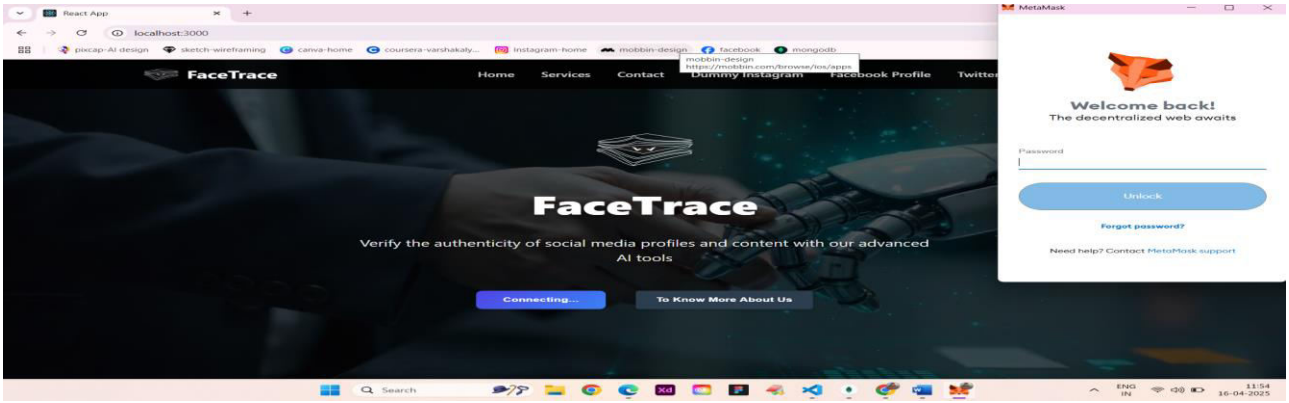


Fig.4 Connect Wallet Page

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305192

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

In the fig 5, it shows the FaceTrace dashboard interface where users can verify the authenticity of social media profiles by selecting a platform and entering a profile URL.

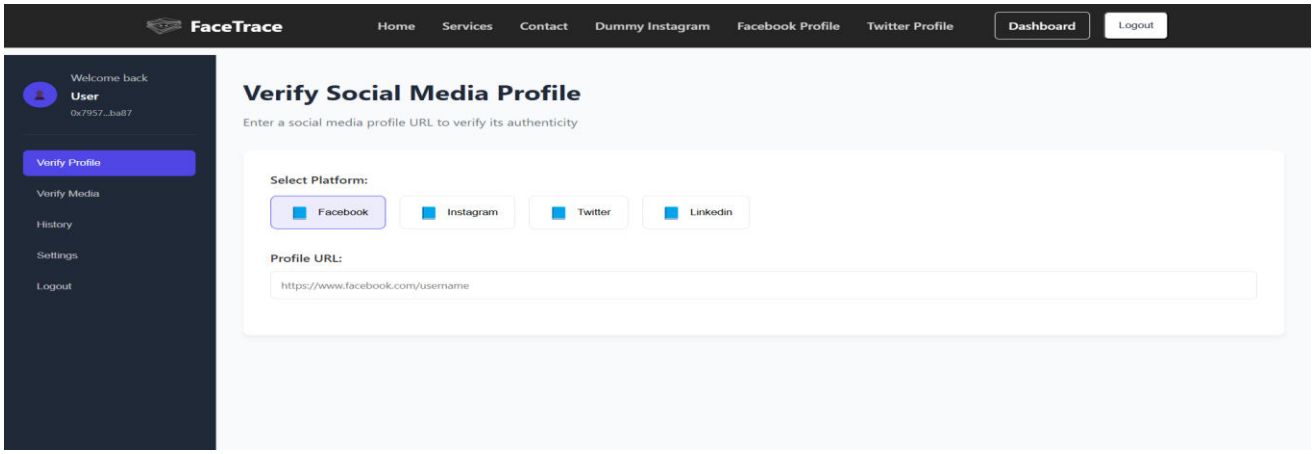


Fig.5 Get Started ID Detection Page

In the fig 6, it shows the FaceTrace interface for verifying the authenticity of social media content by submitting a URL of a specific post.

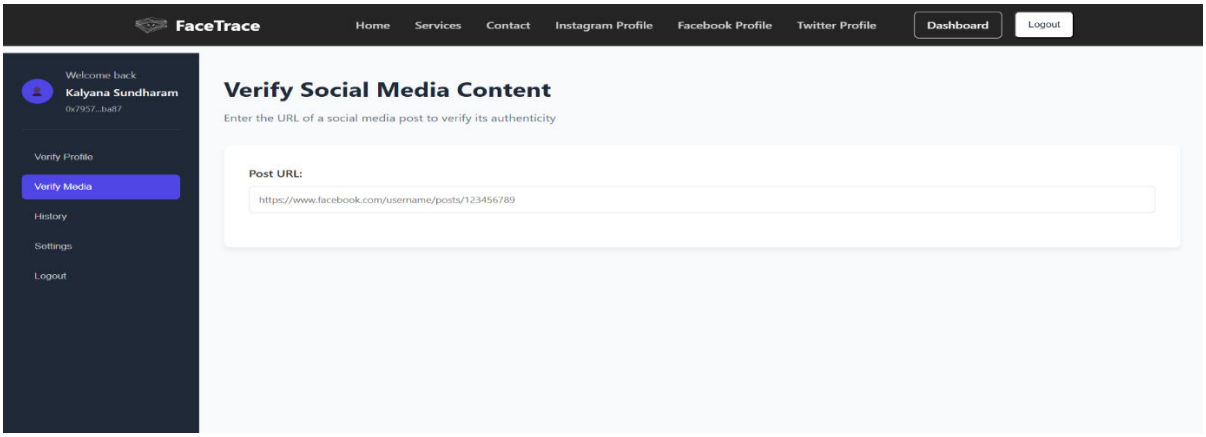


Fig.6 Get Started Media Detection Page

VI.CONCLUSION

This research presents a comprehensive and automated solution for detecting fake IDs and image forgeries using machine learning, image processing, and blockchain technology. The system successfully integrates OpenCV, CNN, SVM, and MD5 hashing for forgery detection, while Hyperledger Fabric ensures data security and integrity. The testing results confirm the system's high accuracy, scalability, and efficiency**,** making it well-suited for large-scale deployment in social media and identity verification platforms. Despite its effectiveness, certain challenges such as reducing false positives, improving deepfake detection, and optimizing system response time remain. Future work will focus on enhancing AI models with more diverse training datasets, refining real-time alert mechanisms, and integrating more advanced fraud detection techniques to improve reliability. By continuously refining detection methodologies and incorporating new advancements, this system lays a strong foundation for secure and trustworthy digital identity verification, contributing to a safer online environment.

REFERENCES

[1] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "A Review on Deepfake Creation and Detection Techniques," *Information Fusion*, Elsevier, 2020, ISSN: 1566-2535.

[2] T. Thakur, K. Singh, and A. Yadav, "Forgery Identification in Digital Images Using Non-Blind Techniques," *International Journal of Computer Applications*, 2018, ISSN: 0975–8887.

[3] N. N. Zanje, A. M. Bongale, and D. Dharrao, "Facial Image Forgery Detection Using Transfer Learning Models," *Int. J. of Advances in Applied Sciences*, 2024, ISSN: 2252-8814.

[4] S. Ghosh and S. Sanyal, "Survey of Image Manipulation Detection Approaches," *International Journal of Computer Applications*, 2021, ISSN: 0975–8887.

[5] I. J. Goodfellow et al., "Generative Models and Adversarial Training," *arXiv preprint*, 2014, arXiv:1406.2661, ISSN: 2331-8422.

[6] C. H. Ravikumar, M. Radha, M. Mahendar, and P. Manasa, "Comparative Study on Deep Learning-Based Forgery Detection Systems," *International Journal of Systematic Innovation*, 2024, ISSN: 2077-8767.

[7] S. A. Naji and Noha, "Forgery Localization in Images with Advanced U-Net Architecture," *Iraqi Journal for Computers and Informatics*, 2023, ISSN: 2520-4912.

[8] Y. Abdalla, M. T. Iqbal, and M. Shehata, "Using Transfer Learning for Digital Forgery Recognition," *Eur. J. Electr. Eng. & Computer Science*, 2023, ISSN: 2736-5751.

[9] F. Siddiqui and M. Suaib, "Detecting Fake Social Media Profiles via Artificial Neural Networks," *Int. J. of Engg. and Management Research*, 2023, ISSN: 2250-0758.

[10] L. Xiu-jian and S. He, "Methods in Image Tampering Detection Using Deep Learning," *Journal of Cyber Security*, 2022, ISSN: 2579-0064.

[11] E. U. H. Qazi, T. Zia, M. Imran, and M. H. Faheem, "Transfer Learning for Deep Image Forgery Detection," *Intelligent Automation & Soft Computing*, 2023, ISSN: 2326-005X.

[12] H. R. Suresh, M. Shanmuganathan, T. Senthilkumar, and B. S. Vidhyasagar, "Image Authentication Using AI-Based Forgery Detection," *Int. J. of Electronic Security and Digital Forensics*, 2024, ISSN: 1751-911X.

[13] K. C. Yang, D. Singh, and F. Menczer, "AI-Generated Fake Profiles on Social Platforms: Analysis and Trends," *Journal of Online Trust and Safety*, 2024, ISSN: 2767-0163.

[14] A. Alharbi, H. Dong, X. Yi, Z. Tari, and I. Khalil, "Survey of Deception Detection in Online Social Identities," *ACM Computing Surveys*, 2021, ISSN: 0360-0300.

[15] Y. Liu et al., "Machine Learning Techniques for Detecting Social Media Fraud: A Critical Review," *arXiv preprint*, 2024, ISSN: 2331-8422.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details