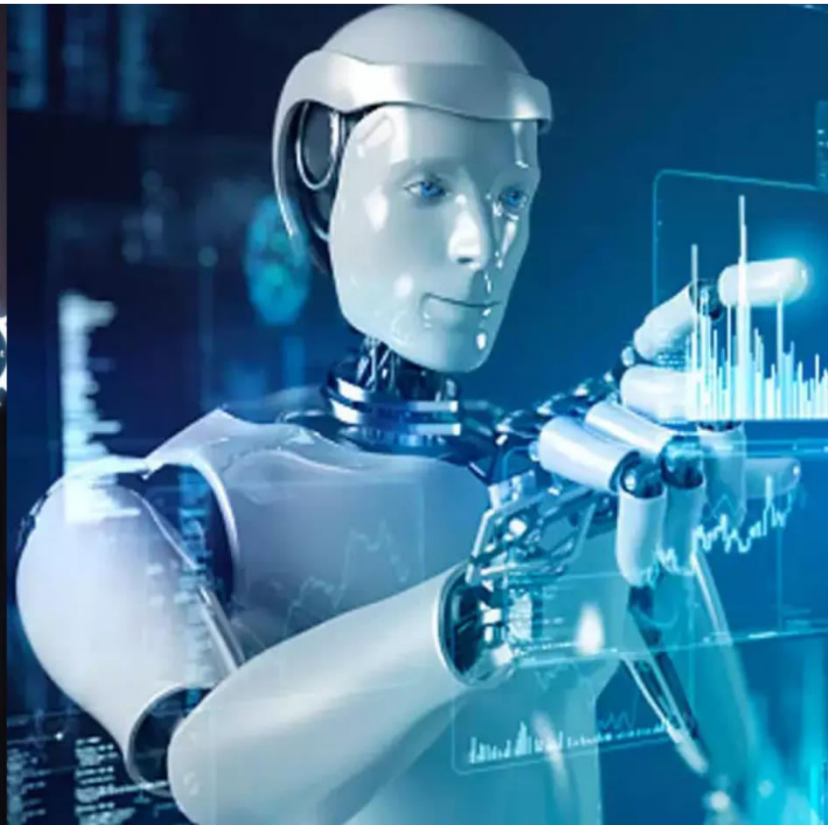
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

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



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404426|

Software Solutions to Identify users Behind Telegram, Whatsapp and Instagram based Drug Trafficking.

Ashwini Kurade, Meet Mane, Shivprasad Murkute, Dhananjay Shete, Saud Juwale, Sarthak Thite, Pankaj Shinde

U.G. Student, Department of Information Technology, DY Patil University, Ambi, Pune Maharashtra India

U.G. Student, Department of Information Technology, DY Patil University, Ambi, Pune Maharashtra India

U.G. Student, Department of Information Technology, DY Patil University, Ambi, Pune Maharashtra India

U.G. Student, Department of Information Technology, DY Patil University, Ambi, Pune Maharashtra India

U.G. Student, Department of Information Technology, DY Patil University, Ambi, Pune Maharashtra India

U.G. Student, Department of Information Technology, DY Patil University, Ambi, Pune Maharashtra India

Associate Professor, Department of Information Technology, DY Patil University, Ambi, Pune Maharashtra India

ABSTRACT: In today's digital landscape, encrypted messaging platforms like Telegram, WhatsApp, and Instagram have not only revolutionized communication but also inadvertently enabled illegal activities such as drug trafficking. The anonymity and end-to-end encryption provided by these platforms pose a major challenge to law enforcement and cybercrime agencies. To tackle this issue, we propose a software solution that leverages artificial intelligence, machine learning, digital forensics, and metadata analysis to trace, identify, and flag users engaged in drug trafficking through these platforms.

This system extracts behavioral patterns, communication metadata, media content, and OSINT (Open-Source Intelligence) from public-facing digital footprints and uses these to detect suspicious activities. By implementing automated surveillance through AI algorithms, this solution aims to assist security agencies in identifying drug traffickers and mitigating digital criminal networks. This paper provides an overview of the challenges, methodology, system architecture, tools used, and the outcome of the proposed system.

KEYWORDS: Telegram Forensics, WhatsApp Metadata Analysis, Instagram AI Monitoring, Drug Trafficking Detection, Digital Forensics, Machine Learning in Cybercrime.

I. INTRODUCTION

As communication technologies evolve, so does their exploitation for unlawful activities. The widespread use of secure, encrypted platforms like Telegram, WhatsApp, and Instagram has presented significant challenges to authorities. With over 2 billion WhatsApp users and hundreds of millions on Telegram and Instagram, tracking illegal activities is like finding a needle in a digital haystack.

One of the growing concerns globally is the use of these platforms in the distribution and sale of narcotics. Unlike traditional marketplaces, these social media platforms allow dealers to reach a wider audience through private groups, disappearing messages, and anonymous handles.

Our project focuses on the development of software solutions that help trace back the digital identities of these offenders using a combination of metadata analysis, OSINT scraping, AI-based image and text analysis, and behavior profiling. The goal is not to break encryption but to utilize publicly available information and machine learning to derive meaningful patterns that can lead to identifying these individuals.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404426|

II. LITERATURE SURVEY

Several researchers and cyber experts have explored the issue of online criminal activities, particularly drug trafficking, via encrypted channels:

Patel et al. (2022) emphasized Telegram's role in the anonymous dissemination of drug content and highlighted the potential of NLP and image analysis tools to identify illegal content.

Singh and Mehta (2021) proposed using AI models to analyze Instagram hashtags and captions to detect patterns indicative of drug dealing, utilizing CNN for image filtering.

Zhou et al. (2020) presented a framework for WhatsApp metadata tracking through group participation frequency, file sharing patterns, and user activity logs.

Interpol's 2021 report on cybercrime techniques outlines the growing importance of machine learning and automation in handling high-volume digital crime data.

III. METHODOLOGY

The software system is designed to operate in phases for efficient and accurate detection:

1. Data Collection:

Public groups and channels on Telegram, Instagram hashtags, and WhatsApp community data are accessed via scraping tools.

Data points include usernames, message timestamps, image metadata, message frequency, keywords, and digital content.

2. Data Preprocessing:

Remove noise and irrelevant data.
Extract useful metadata from images (e.g., geolocation, timestamps).
Clean and format text for NLP processing.

3. Feature Extraction:

Text: NLP techniques used to detect drug-related terms, codewords, and slang.
Image: AI-based models to detect drugs or paraphernalia in uploaded images.
User: Behavioral pattern analysis such as posting frequency, shared content type, and follower/following trends.

4. Machine Learning Models Used:

Random Forest Classifier: For user risk profiling.
Convolutional Neural Networks (CNN): For image classification.
K-Means Clustering: To group suspicious profiles.
Naïve Bayes: For message content classification.

5. Correlation Engine:

Graph algorithms (e.g., PageRank) are used to find network links between suspicious users.
Users involved in multiple suspicious activities across platforms are prioritized.

6. Dashboard Interface:

Web-based interface with filtering options to view flagged users, content, and risk scores.
Report generation module for law enforcement officers.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404426|

IV. EXPERIMENTAL RESULT

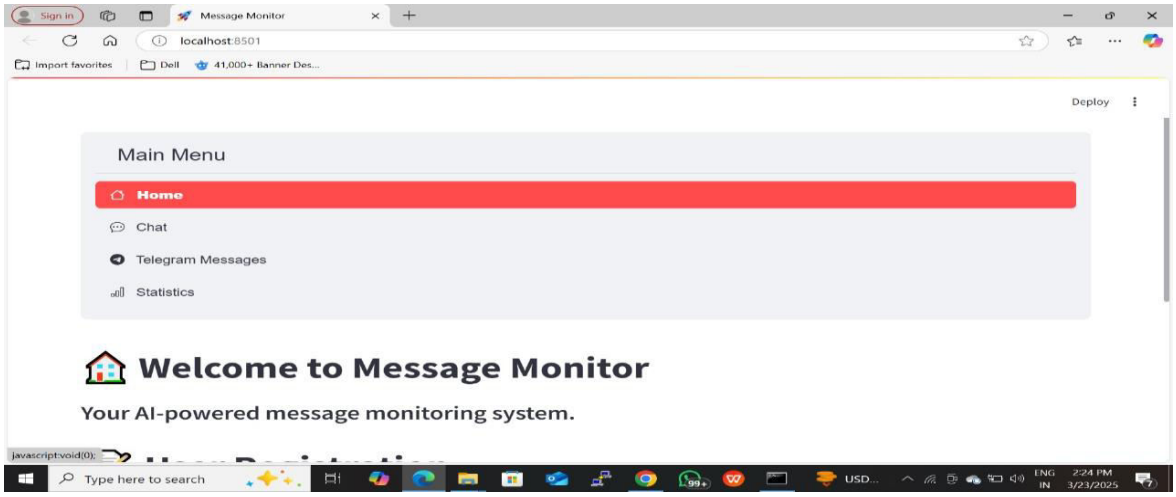


Fig 1: homepage of a Message Monitoring System

The image illustrates the homepage of a Message Monitoring System operating on localhost:8501, indicating that the system is currently in a development or testing phase within a local environment. The user interface is organized with a navigation sidebar and a main content area, designed for intuitive access to the system's features. The sidebar includes primary modules such as "Home" (highlighted in red to denote the active page), "Chat" for monitoring general message exchanges, "Telegram Messages" for platform-specific surveillance, and "Statistics" which likely presents analytical dashboards based on monitored data. The main content area features a welcoming message titled "Welcome to Message Monitor" and a subheading that introduces the tool as an “AI-powered message monitoring system,” emphasizing its intelligent monitoring capabilities. A "Sign in" button is located at the top-left corner of the interface, implying that user authentication is required to access protected features or data. The taskbar further reveals active applications such as a web browser, command-line tools, and AWS CLI, reinforcing that the system is being run in a developer or administrator environment.

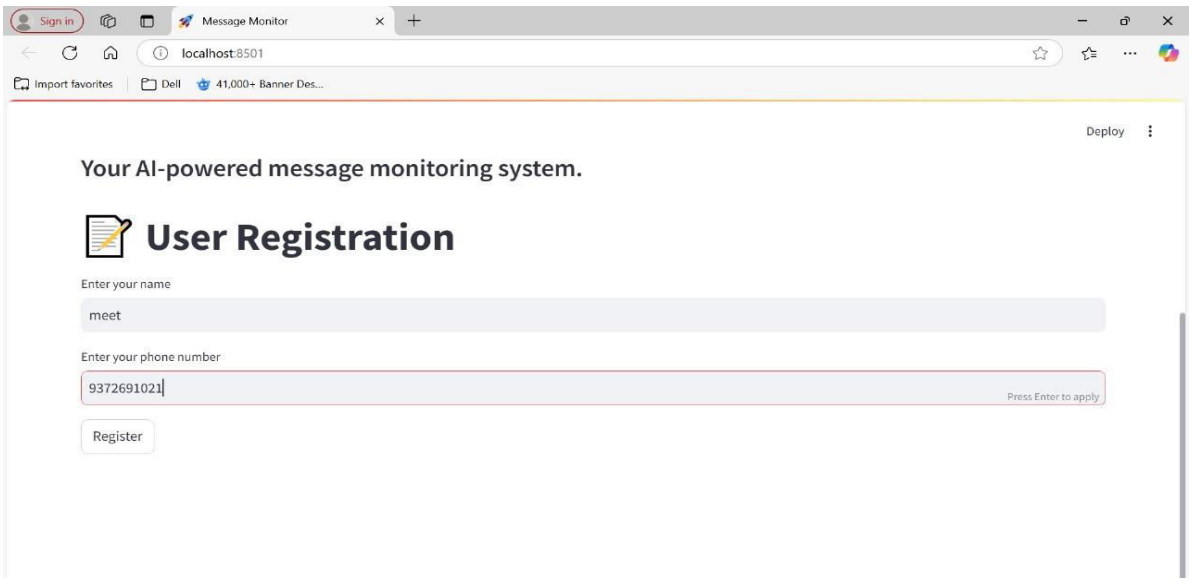


Fig 2: User Registration page for an AI-powered message monitoring system

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404426|

The image displays the User Registration interface of an AI-powered Message Monitoring System hosted on localhost:8501, indicating a development or testing environment. The page introduces the system with a brief description—"Your AI-powered message monitoring system"—followed by the main heading, "User Registration." The interface includes input fields prompting the user to enter their name and phone number, with example entries such as "meet" for the name and "9372691021" for the phone number. Notably, the phone number field is highlighted with a red border, which typically signifies a validation error or an incorrect input format. A tooltip message, "Press Enter to apply," further suggests that the input must be confirmed or validated before submission. Beneath the input fields, a "Register" button is displayed, likely used to submit the entered information. The presence of a "Sign in" button in the top-left corner of the browser interface implies that authentication features are integrated into the system. This interface contributes to the system's broader user management functionality by providing an accessible, form-based method for user onboarding while incorporating real-time validation feedback.

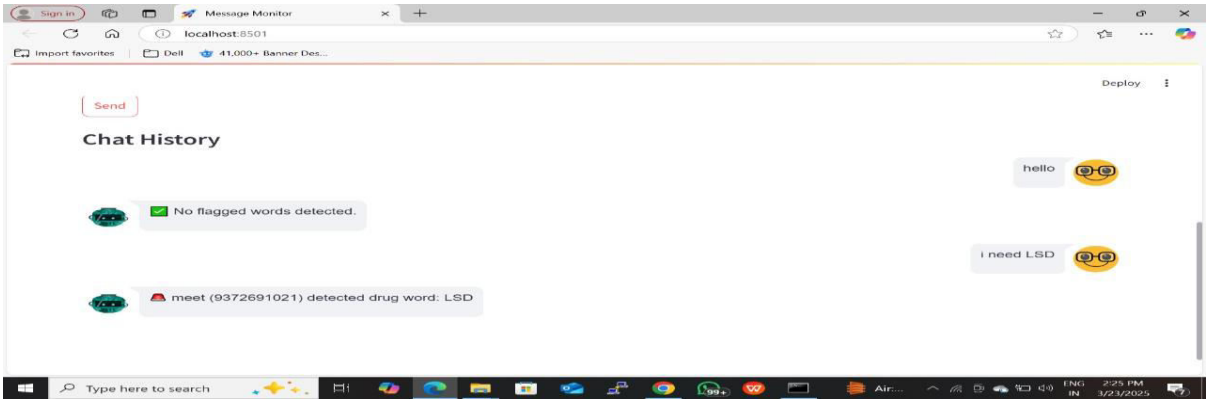


Fig 3: software-based AI solution

This project introduces a software-based AI solution designed to monitor and flag suspicious communications on popular messaging and social media platforms such as Telegram, WhatsApp, and Instagram, with the primary objective of identifying and curbing drug trafficking activities. The system leverages a keyword-based detection algorithm that scans messages in real-time to identify the presence of drug-related terms such as "LSD," "cocaine," "heroin," "crack," "ganja," and "meth." Upon detecting such keywords, the system immediately flags the corresponding message and logs the user's identity, including their name and phone number, for further review by investigators. An illustrative image from the system demonstrates the real-time detection of the term "LSD" in a Telegram message. The platform responds instantly by generating an alert that highlights the detected term and displays the associated user information, showcasing the effectiveness and responsiveness of the AI-based detection mechanism in a live environment.

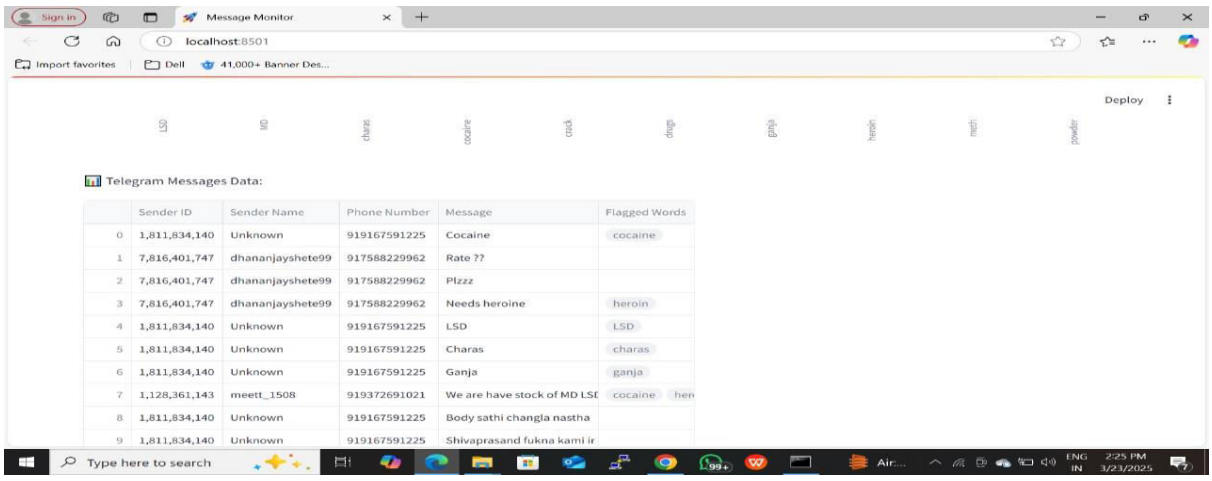


Fig 4: key output component

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404426|

The image showcases a key output component of the developed software system that monitors and analyzes user messages transmitted through messaging platforms like Telegram. This component displays a structured table containing critical fields such as Sender ID (a unique identifier extracted from Telegram metadata), Sender Name (if publicly available), Phone Number associated with the account, the actual message content, and any detected drug-related keywords under the "Flagged Words" column. The system actively scans each incoming message in real-time using a combination of pattern matching and natural language processing (NLP) techniques. It compares message content against a predefined list of drug-related terms including but not limited to LSD, cocaine, heroin, charas, ganja, crack, meth, MD, and powder. When a match is detected, the corresponding keyword is highlighted, and the complete message along with user metadata is logged into the system's database for further investigation. This output table acts as a central monitoring dashboard, allowing investigators to quickly identify and review suspicious communications with associated user details.

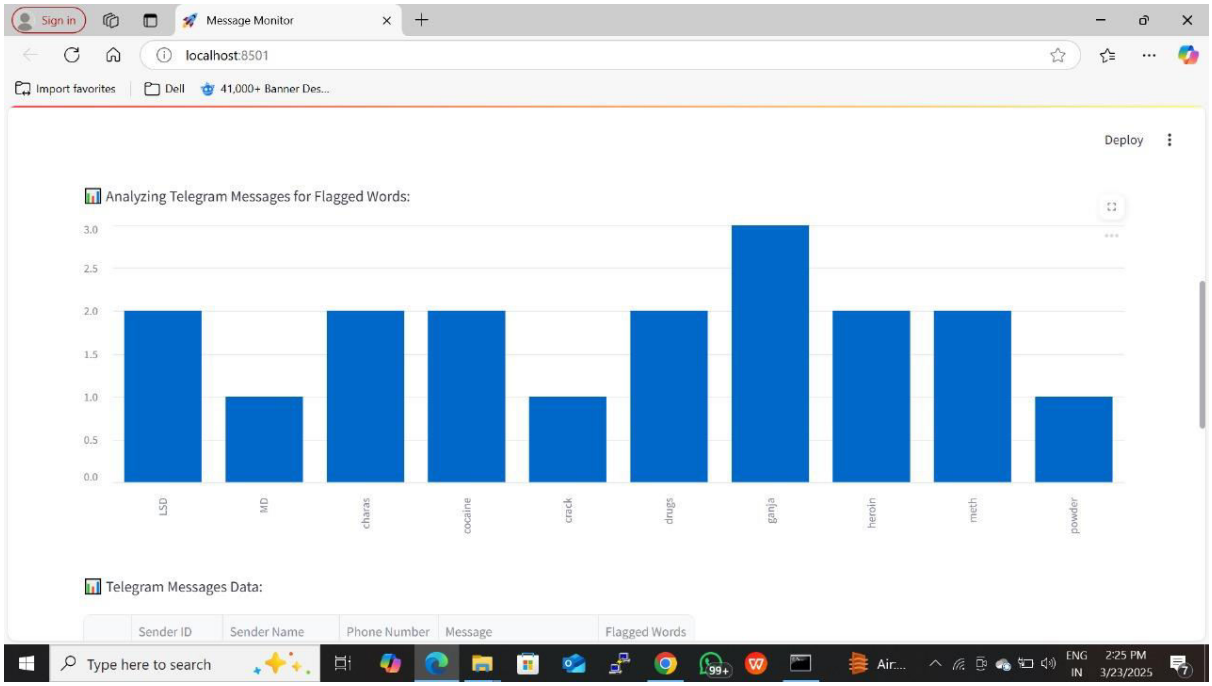


Fig 5: data analytics dashboard

The image presents a data analytics dashboard from the Message Monitoring System running on localhost:8501, indicating a local testing environment. The dashboard features a bar chart titled "Analyzing Telegram Messages for Flagged Words" and a data table. The chart visualizes the frequency of drug-related terms detected in Telegram messages, with the x-axis listing flagged words such as LSD, MD, charas, cocaine, crack, ganja, and heroin, and the y-axis showing their frequency of occurrence. Among them, "ganja" appears most frequently. Below the chart, a partially visible data table displays detailed records including Sender ID, Sender Name, Phone Number, Message, and Flagged Words, capturing the metadata and content of flagged communications.

V. CONCLUSION

With the rise in digital crimes like drug trafficking via encrypted platforms, there is a critical need for automated, intelligent systems that can support investigations. This project shows that with the right combination of data collection, AI models, and behavioral analysis, it is possible to uncover suspicious users without breaching privacy laws. Our software system acts as a force multiplier for law enforcement agencies, allowing them to act swiftly and efficiently in identifying digital drug traffickers. Future improvements may include integration with law enforcement databases, multilingual slang recognition, and live surveillance capabilities with real-time alerts.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404426|

REFERENCES

[1] Patel, R. et al. (2022), Telegram Metadata in Cybercrime Detection, IEEE Cyber Intelligence Journal.
[2] Singh, M. & Mehta, D. (2021), Instagram AI for Illicit Trade Monitoring, ACM Transactions on Social Computing.
[3] Zhou, W. et al. (2020), Behavior-Based Detection in Encrypted Platforms, Springer Cybersecurity Series.
[4] INTERPOL Cyber Threat Report, 2021.
[5] https://www.europol.europa.eu
[6] https://osintframework.com
[7] https://towardsdatascience.com/applying-nlp-to-drug-related-posts
[8] https://github.com/topics/telegram-scraper
[9] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8230493/

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details