IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

LEA OSINT Bot and Website: An Advanced Open-Source Intelligence Platform for Law Enforcement Agencies

Sourav Singh, Mradul Chauhan, Mr. Brijesh Kumar Mishra
Students, Department of CSE(IOT)
Department of CSE(Iot), RKGIT
Raj Kumar Goel Institute of Technology, Ghaziabad, India
sourav5670s@gmail.com, chauhanmradul492@gmail.com, bkmishraengg@gmail.com

Abstract: *This paper covers LEAOSINT Bot and Website, an open source intelligence (OSINT) platform built out to address an urgent requirement for basic investigative tools that could assist Law Enforcement Agencies (LEAs) in their investigations across digital communications and internet-based communications. It assembles the design and development of 45+ intelligence modules across 10 distinct functional categories (Personal Info, Financial Intelligence, Vehicle info, UPI &Payments, Digital Security, Email Intelligence, Social Media, Domain &Network, Location Services, Advanced Analytics) into a single Dashboard to generate over 500+ unique data points. Fully integrated existing capabilities like zero-click device fingerprinting, GPS geodes, Telegram bot alerts, multi-layer progressive OSINT collection have been employed as key system features. Under Indian jurisdiction and IT Act 2000, the system outputs have resulted in significant gains on investigation turn-around, multi-source data correlation and field action intelligence. A high level overview of system architecture, feature set, data dictionary, security measures and use-case scenario is presented.*

Keywords: OSINT, Law Enforcement Intelligence, Digital forensic, Computer forensic, Cybercrimes, Telecom analytical tools, Camera Fingerprinting Devices, Geolocation Intelligence, Open Source Intelligence Platform

I. INTRODUCTION

Open-Source Intelligence is proving to be a vital component of contemporary criminal investigations. The astonishing volume of personal information trails individuals and businesses leave across telecommunication systems, social networking sites, financial transactions, and the internet provides both an unparalleled source of evidence and a daunting task for investigators. Current methods of manual correlation of dispersed data are ineffective against the high level of sophistication on display in cyber criminal, commercial fraud, and border security investigations

The LEA OSINT Bot and Website addresses this deficiency by gathering intelligence from more than 45 separate lookup modules into one close integrated platform, allowing their law enforcement operators to efficiently perform a multidimensional profiling operation on a single focus, in record time through combined lookups from a number of personal identification logs, financial tools, motoring registers, social networking sites, and network infrastructure.

The engine is designed as an inherently serverless, stateless system that is highly resilient, rapidly deployable, and without any single points of failure. A major innovation of the platform is the Advanced Device Intelligence Protocol (ADIP), a three-tier, zero-click device fingerprinting and geolocation tracking engine that can be embedded into custom tracking links, for uses such target ID verification, counter- intelligence sweeps, and hostage/missing person geolocation

This paper is structured as follows: section II presents the related work in OSINT; section III describes the solution architecture; section IV covers the the categories of information, and the data dictionary; section V describes the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 10, April 2026 Impact Factor: 8.2

Advanced Device Intelligence Protocol; section VI discusses security and compliance controls; section VII describes the operational use case; and section VIII concludes the paper.

II. PROBLEM STATEMENT

Despite the proliferation of new intelligence tools and open sources of data, law enforcement agencies have been plagued with many challenges seeking to obtain and analyze open source intelligence in an efficient manner. Their prevalent issues are:

- Disjointed and unintegrated OSINT tools
- Increased dependencies on manual file analysis and individual data collection procedures
- Reduction in the ability to effectively triangulate data points derived from various digital sources
- Time lag in providing a ready shot to intelligence and pictorial reports; and
- Absence of a centralized platform to facilitate seamless and successful investigations within the boundaries of statutory regulations

Such issues highlight the fact that current investigative techniques and infrastructure are ill-equipped to deal with, and overwhelmed by, the quantity of digital information that we now must collect. We need a solitary, automated solution like the LEA OSINT Bot and Website that is capable of capturing, analyzing and visualizing data to allow for faster, more accurate, and within legal boundaries, investigations.

III. OBJECTIVES

The main objectives of the proposed LEA OSINT Bot and Website system are as follows:

- Achieve a consolidated Open Source Intelligence (OSINT) platform that aggregates various intelligence modules into a unified interface.
- To harness the data available from digital sources through the use of open source data collection systems.
- Increase the speed and accuracy of information collection for law enforcement investigation.
- To allow instant correlation and visualization of data for better decision making.
- To guarantee the safe, reliable, and legally compliant dispatch of investigative data.
- To assist cyber crime investigation, digital forensics and intelligence operation with modern OSINT techniques

IV. RELATED WORK

OSINT has gained a significant amount of interest from academia and practitioners over the past ten years. Glassman and Kang [4] describe OSINT as intelligence that is derived from publicly available information and that is collected, exploited and disseminated in a timely fashion to the right audience to meet a specific intelligence requirement. They group OSINT sources into five main areas; the media, internet, public government information, professional and academic publications and commercial data.

Automated, graphical OSINT collection has been explored using tools like Maltego [5] and Shodan [6], but they are targeted towards the cyber security research community, and do not have any Indian law enforcement oriented integrations that are specifically tailored to the Indian government identity databases (Aadhaar, PAN, Voter ID, Vehicle Registration databases etc.)

BinHassan et al.‘s [7] social media OSINT research points to cross-platform correlation – associating a person‘s identities across Facebook, Instagram, WhatsApp and Telegram – as a vital investigation technique, and the LEA OSINT Bot contains a dedicated module for each.

An earlier effort toward device fingerprinting, by Eckersley [8] provided the underlying theory for unique identification of the browser device. The Advanced Device Intelligence Protocol builds on Eckersley‘s technique by providing implementation of GPS geolocation capture and silent camera visual verification that builds upon the implementation techniques shown by Acar et al. [9] for cross device tracking.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

V. SYSTEM ARCHITECTURE

A. Overall Architecture

The LEA OSINT Bot and Website is an entirely serverless, stateless architecture. By utilizing this design there is zero overhead from maintaining a database, allows seemingly unlimited horizontal scalability, and presents zero attack surface from persistent server side infrastructure. The system is built of the following five components:

• Web Interface: Browsers in a control room displaying a frontend that translates questions from intelligence operators into structured forms and presents the structured web results.

• OSINT API Gateway: Manages requests for 45+ intelligence modules, brings responses together and normalises them.

• Telegram Bot Integration:Provides instant intelligence reports for operators in the field through a private Telegram Chat.

• Serverless Proxy Layer: Tunnels all data through a global proxy grid, obscuring source IPs and avoiding CORS limitations.

• Advanced Device Intelligence Protocol: An engine for zero click fingerprinting and geolocation tracking utilizing dynamically generated tracking URLs.

B. Data Flow

When an operator types in an intelligence query (eg a mobile number in the Mobile Lookup module), the system (1) checks that the syntax is correct and the operator is authorised; (2) makes parallel API calls to all data sources; (3) recombines, deduplicates and formats the responses; (4) renders a tabled report on the web front-end; and (5) sends a formatted version of the report to the operator‘s designated Telegram Bot Telegram channel. The module for the Deep OSINT Report is more complex, executing in parallel over 12+ API calls between them to return a 12+ source multi-intelligence report [3].

VI. FEATURE CATEGORIES AND DATA DICTIONARY

The platform is structured into ten different feature categories consisting of 45 different intelligence modules and greater than 500 data fields. A brief breakdown on each of these categories can be found in Table I.

TABLE I: Summary of Feature Categories

Category	Modules	Key Data Points
Personal Information	Mobile Lookup, Aadhaar Search, PAN Search, Voter ID, Driving Licence, Family Details, Ration Card, Age & Gender Verification,	Name, DOB, Address, Bank Details, IFSC, Facebook url, PAN, Aadhar, Voter EPIC, Driving licence, Family members.
Financial Intelligence	Bank Account Verify. IFSC Finder. GSTIN Lookup. GST to PAN. BIN Lookup. IBAN Lookup. Director DIN Info. Udyog Aadhaar	Account Status, Holder Name, UPI ID, IFSC, MICR, SWIFT, Business Constitution, Director Details, BIN Card Scheme
Vehicle Intelligence	Vehicle Advanced, Challan Info, Fastag Info	Owner Name, Make / Model, Chassis/Engine No., Insurance, RC Expiry, Traffic Challans, Fastag Balance
UPI & Payments	UPI Mobile Lookup, UPI Info Basic	UPI ID, Account Holders Name, PSP, IFSC, Bank Name, Account Type
Digital Security	Email Breach Check, Email Validator, Phone Validation, IP	History of Breach, Fraud Score, Risk Flags, IP Threat Intel, IMEI Device Information, URL

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 10, April 2026 Impact Factor: 8.2

	Scanner, IMEI Lookup, URL Scanner	Location...
Email Intelligence	Email OSINT, Gmail OSINT (GHunt)	Linked Records,Gai a ID,Google Services,Maps Profile,Calendar, Cover Photo
Social Media	Truecaller Lookup, Mobile to Facebook, Instagram Footprint, IG OSINT, WhatsApp Lookup, Telegram OSINT.	Call ID Facebook Profile Instagram Stats WhatsApp Status Telegram User Mapping
Domain & Network	Domain WHOIS, DNS Records, MX Lookup	Registrar, Name Servers, DNSSEC, A/AAAA/MX/TXT/CNAME Records
Location Services	Zipcode Lookup, Reverse Geolocation, Cell Tower Lookup	GPS Co-ordinates, Address, Cell Tower CGI, MCC/MNC/LAC, Azimuth, Google Maps Link
Advanced	Deep OSINT Report, MNP Lookup, PAK OSINT, Advanced	12+ API Parallel Aggregation, Device Fingerprint, GPS, Camera Photo, MNP Operator

A. Personal Information Category

The Personal Information category consists of 8 modules which provide information of a person‘s identity and identity proof itself. Mobile Lookup module takes mobile number as input and outputs 17 data items such as name, father‘s name, address, email, alternate mobile number, aadhaar number, Pan number, date of birth, gender, bank name, bank account number, IFSC code, MICR code, Facebook url, source database. Aadhaar Search module takes enterprise‘s aadhaar number from input and returns the personal details and contact details of that aadhaar number. Driving Licence Info module provides details of driving license holders like photo, blood group, citizenship, vehicle class, address details: permanent address, temporary address, respective pins.

B. Financial Intelligence Category

There are 8 modules in the financial intelligence category. Bank Account Verify module checks the existence of the account and returns account holder name, UPI ID and IMPS reference. The GSTIN Lookup module returns the complete GST registration details like legal name, trade name, business constitution, GST type, jurisdiction, registration &cancellation dates, business activities, and full address. BIN Lookup module returns card scheme (Visa/Mastercard), card type, card level, issuer details and country from the Bank Identification Number. Director DIN Info module returns director details like father‘s name, DOB, nationality, DIN status, PAN, email, address, companies &c Directors with Designation.

VII. ADVANCED DEVICE INTELLIGENCE PROTOCOL

The most advanced technical element of the LEA OSINT platform is the Advanced Device Intelligence Protocol. This is a three stage, zero-click progressive data capture pipeline that will be used in high value law enforcement situations.

A. Stage 1: Zero-Click Device Fingerprinting

Step 1 is entirely passive. When the target opens a tracking URL created by us, there are no actions required to be performed by the target and no prompts are displayed. In less than a few hundred milliseconds after the page load, it sends the full hardware and network fingerprint to the operator‘s dashboard in Telegram. This fingerprint includes IP address and ISP/ASN data, full user-agent string, OS and platform details, RAM amount and CPU cores count, screen resolution and color depth, touch screen supported, device pixel ratio, browser language, timezone and UTC offset, network connection type and estimated speed, Canvas fingerprint (unique hash), WebGL renderer and vendor strings, Web Audio Context hardware hash, WebRTC local IP address, battery status and charge state, Ad Blocker detection

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 10, April 2026 Impact Factor: 8.2

results, platform architecture bits. This happens even before the page load is complete if the user will close the browser, we'll still get the data.

B. Stage 2: Precision Geolocation Capture

For Stage 2, the use of smart fallback UI gestures is used to invoke native OS-level GPS permission dialogs in a well-designed user experience flow. After location permission access is granted, high accuracy GPS data (lat, lon, radius of location accuracy meter, Altitude, Altitude accuracy, Heading, Speed (if the target is moving), Google Maps pre-computed direct link) along with an auto-generated reverse geocoded address is streamed right back to the operator dashboard.

C. Stage 3: Silent Visual Verification

Stage 3 presents a clear camera overlay of the person authorizing the tracking link's verification photo. At the same time, all online media hardware (e.g. microphone, webcam, speaker, etc.) is enumerated, matching device names, hardware IDs, number of audio input and output channels, and media device group IDs. The photo is then encoded using Base64 and pushed to the operator's Telegram dashboard along with data from stage1 and stage 2.

D. Progressive Submission Architecture

At each stage, data is relayed immediately as it becomes available. This incremental submission design allows usable intelligence to be gleaned from incomplete sessions. If the target closes the browser midway through Stage 1, yet before reaching Stage 2, the operator will still acquire an entire device fingerprint. The tracking infrastructure is a serverless proxy running on Vercel, obfuscating the origin infrastructure IP and providing a geographic spread of servers for low-latency operation across the globe. Distinct tracking URLs are produced and have payload IDs base64 encoded within them, since there are no server-side sessions or database lookups.

VIII. SECURITY AND COMPLIANCE

Designed with security as top priority, this system ensures every individual data and file is protected by TLS1.3 encryption through transit while at rest they are encrypted with AES-256, and all API calls are secured using HTTPS with certificate pinning. Systems uses multi-layered role based permissions controls with all operator access secured by API keys and JWT tokens and supervision- (super-admins) enables precise control over permission assignments per user for specific usage or features [10].

Fully auditable record of all access, queries and data exports. Auditable, immutable audit trail provides complete accountability and traceability. Cloud infrastructure on enterprise grade providers (via network segregation, aided by DDoS protection and a WAF.).

All these operations are carried out exclusively as per the provisions of the IT Act 2000 (as amended in 2008) and relevant rules made thereunder named IT Rules 2021 and Indian Penal Code, by (1) the platform having a MoU with the requesting organization; (2) receipt of the NOC from the requesting organization; (3) where the request is being directed on the receiving end, the request has been rerouted using an authorized nodal officer acting on official credential of the Indian government. All investigations were carried out upon lawful authority.

IX. OPERATIONAL USE CASES

A. Cyber Crime Investigation

For online fraud investigations, investigators can quickly be connected to the suspect's mobile Number with the Mobile Lookup module. Within a single query, investigators are able to retrieve associated Citibank, Facebook, Aadhaar and PAN Number. Once downloaded, 12+ APIs from Deep OSINT Report module can then be triggered to run concurrently, collating a subject dossier in live time. UPI Mobile Lookup & UPI info Basic modules can additionally help to establish payment identities to follow digital trails.

B. Target Location and Identity Verification

In missing person or fugitive location case, Advanced Device Intelligence Protocol can be employed by creating a tracking link and sharing it through SMS, WhatsApp, email, or social media; when the target opens the link, the field

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 10, April 2026 Impact Factor: 8.2

team receives GPS coordinates up to meter accuracy, real-time picture of the target, and full device fingerprint allowing rapid response teams to determine positions without requiring active searches.

C. Financial Fraud Investigation

Application modules like Bank Account Verify, IFSC Finder, GSTIN Lookup, and BIN Lookup are used for instant financial identity check for financial fraud investigations. GST to PAN application module is used for crosschecking business identities with identity documents. Director DIN Info and Udyog Aadhaar modules can be used for investigating fake/business entities and their directors.

D. Counter-Intelligence Operations

Tracking links for counter intelligence operations can be distributed in suspected breached communication channels. The system can then observe what devices open the links, match the device fingerprint with existing profiles, and reveal unauthorized persons inside secure networks. The cell tower lookup module allows geolocating the targets on telecom network data with Cell Global Identity (CGI) records.

X. RESULTS AND DISCUSSION

There are a few distinct advantages of the LEA OSINT Bot and Website over old traditional investigative practices. Firstly, the consolidation of 45+ intelligence modules within a single user experience drastically decreases the time required to create a subject intelligence dossier. In comparison, investigators needed to query many parallel databases and cross-reference results manually. Secondly, the parallel APIs execution feature of the Deep OSINT Report module allows rapid subject profiling through phone validation, Truecaller lookup, UPI account discovery, WhatsApp status, MNP detail, family tree reconstruction, and Gmail OSINT all through a single holistic request.

Third, the four stage incremental capture architecture of Advanced Device Intelligence Protocol guarantees exhaustive data capture in even worst case circumstances if the target aborts session prematurely. The entirely serverless and stateless design of Internet Protocol‘s architecture will provide operational security from infrastructure attacks for law enforcement deployments. Fourth, Telegram Bot integration provides formatted intelligence reports to field operatives on a regular basis and can be incorporated in operational scenarios so as to avoid accessing web interfaces from the field.

Coverage of India-specific data sources (such as Aadhaar, PAN, Voter ID (EPIC), Driving Licence, Ration Card, GSTIN, Udyog Aadhaar, UPI, Fastag, Vehicle Registration systems etc.) is a differentiator with respect to general purpose OSINT tools and an attractive feature for Indian law enforcement use cases. The coverage of Cell Tower Lookup with azimuth-based direction finding and map overlays is comparable to commercial telecom intelligence tools.

XI. CONCLUSION

This paper has introduced LEA OSINT Bot & Website, an all-in-one open-source intelligence platform targeted for authorized law enforcement / internal intelligence uses. It offers an all-in-one open-source-based intelligence delivery platform by synching 45+ modules of personal identity, financial, vehicle, social media, computer security, domain authority as well as geolocation into one single unified real-time intelligence platform.

Technical achievement: advanced device intelligence protocol: Zero click device fingerprinting, GPS geotagging of precisely georeferenced points (precise GPS), and silent visual id/vouching using an advanced three stage progressive capture architecture. Serverless, stateless architecture of the platform to ensure scalability, fast time-to-market and security of operations. According to IT Act 2000 requirements of formal ‘State permission’ were fulfilled.

The next phase of development will likely involve further extension of the integration to other Indian Government databases, modification of the association mapping process using machine learning algorithms for automated link analysis, and development of graph-based visualisation tools for multisubject investigations. This platform represents one of the first full-fledged OSINT systems available in Indian law enforcement that can hold its own against the analytic tools provided to most global intelligence services.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

REFERENCES

[1]. M. Glassman and M. J. Kang, 'Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT)," Computers in Human Behavior 28 (2), 673–682, 2012.

[2]. R. Hassan and G. Hijazi, A comprehensive survey of open source intelligence (OSINT) tools and techniques, Journal of cyber security technology,5(3), 101– 127.

[3]. K. Sharma and P. Verma, "Serverless Architecture for Real Time Intelligence Platforms designed and Secured," International Journal of Computer Application, vol. 183, no. 12, pp. 15 22, 2021.

[4]. D. Steele, "Open Source Intelligence", in Handbook of Intelligence Studies, L. K. Johnson, Ed., New York: Routledge, 2007, pp. 129–147.

[5]. Maltego Technologies. "Maltego Transform Hub and Intelligence Platform," Maltego GmbH, Munich, 2023. [Online]. Available: https://www.maltego.com

[6]. J. Matherly, Complete Guide to Shodan: Collect. Analyze. Visualize. Make Internet Intelligence Work for You, Shodan, LLC, 2016.

[7]. M. Bin Hassan, A. Azmi, and R. Ismail conducted an empirical review on how social media OSINT is used in law enforcement investigations, published in IEEE Access in 2021.

[8]. P. Eckersley explored the uniqueness of web browsers in a chapter for Privacy Enhancing Technologies, published by Springer in 2010.

[9]. G. Acar and colleagues discussed persistent tracking methods on the web in a paper presented at ACM SIGSAC CCS in 2014.

[10]. N. Tamma, C. Malin, S. Hayes, and J. Erickson wrote the second edition of a book on analyzing Android activities and data with forensic tools, published by Packt Publishing in 2018