



---

# RavenAI Fusion

Entity-Centric Intelligence Fusion Platform

One platform. Every source. Faster decisions.

By Pivotchain Solution Technologies



**Your adversary's  
decision loop  
is in minutes.  
Yours is in hours.**

RavenAI Fusion — GEOINT O... x  
https://ravenai.duckdns.org:30443j/

Sun, 31 May 2026 21:32:28 UTC

RAVEN AI FUSION GEO OPS COMMAND LIVE FEED AES-256-GCM CONNECTED LIC AI ADMIN admin LOGOUT

NAVIGATION  
Live Map  
Cameras  
Assets  
Threats  
Zones  
Weather Alerts  
Bookmarks

PLATFORM STATUS

9 ASSETS	8 ACTIVE
2 CRITICAL	3 HIGH
6 ZONES	5 ALERTS
131 DATA	508 FLIGHTS
8 DRIPS	6 CAMERAS
20 WEATHER	0 LEVEL OPS
10 INTEL	10 HURRY

ASSETS ACTIVE THREATS CAMERAS / CCTV WEATHER & ENVIRONMENTAL ALERTS

- LoT Demo... ACTIVE
- APC KE... MAINTENANCE
- Radar Station... ACTIVE
- Field Team Br... ACTIVE
- Border Post Al... ACTIVE
- LoC Infiltrat... CRITICAL
- Active Terror... CRITICAL
- Cross-Border Dr... HIGH
- PLA Forward De... HIGH
- Unidentified Ves... HIGH
- Tawang Forward Post Cam ACTIVE
- Pathankot Air Base Perime... ACTIVE
- Mumbai Naval Dock Cam 3 ACTIVE
- Delhi Ops Centre CCTV ACTIVE
- Srinagar Airbase Gate Cam ACTIVE
- Green earthquake... MEDIUM GOACS
- Green earthquake... MEDIUM GOACS
- Green earthquake... MEDIUM GOACS
- Green notification... MEDIUM GOACS
- Green flood alert... MEDIUM GOACS



# The Decision Gap

---

## The **OODA** Loop Gap

- ▶ Your analysts juggle 6 disconnected systems
- ▶ Average time to correlate a multi-source threat: Few hours
- ▶ Each handoff between systems loses context and time
- ▶ By the time a report reaches the commander, it's stale

Every hour lost is a window for the adversary.  
The gap between sensor and decision is where operations fail.



# Key Pain Points

---

Intelligence doesn't fail because of bad analysts.

It fails because of disconnected systems.

## Today's Reality:

- ▶ HUMINT reports in one system
- ▶ OSINT feeds in another
- ▶ GIS / mapping on a third
- ▶ Chat and coordination on a fourth
- ▶ Intel reports and assessments on a fifth

India's C4ISR networks — [AFNET](#), [NCN](#), [ASCON](#) — are not fully interoperable.

- ▶ No single common operating picture exists.
- ▶ Every tool adds overhead.
- ▶ Every handoff loses context.
- ▶ Every silo creates blind spots.



# Data Sovereignty

Foreign  
platforms are  
dependencies  
you can't  
control in a  
crisis.

## It Has Happened to Us

- ▶ **Kargil 1999** — US denied GPS data to India during active conflict. India built NavIC. The lesson: never depend on foreign systems in war.
- ▶ **Pokhran-II 1998** — US sanctions blocked critical technology transfers
- ▶ **Turkey** — removed from F-35 program overnight
- ▶ **S-400** — CAATSA sanctions threatened for sovereign defence purchases

## Foreign SaaS Means

- ▶ Foreign telemetry **on your** operations
- ▶ Foreign kill switches **on your** capability
- ▶ Foreign jurisdiction **on your** data

The question isn't “**can we afford indigenous?**”  
It's “**can we afford not to?**”



# Introducing RavenAI Fusion

Your data never leaves your infrastructure.

## FUSE

Entity-centric fusion  
with confidence  
scoring  
across all INT  
sources

## SEE

Map as intelligence  
control surface with  
temporal replay

## DECIDE

AI-assisted  
assessments  
+ analyst inbox for  
human-in-the-loop  
review

## ACT

Ops rooms, tasking,  
field coordination  
& mobile app

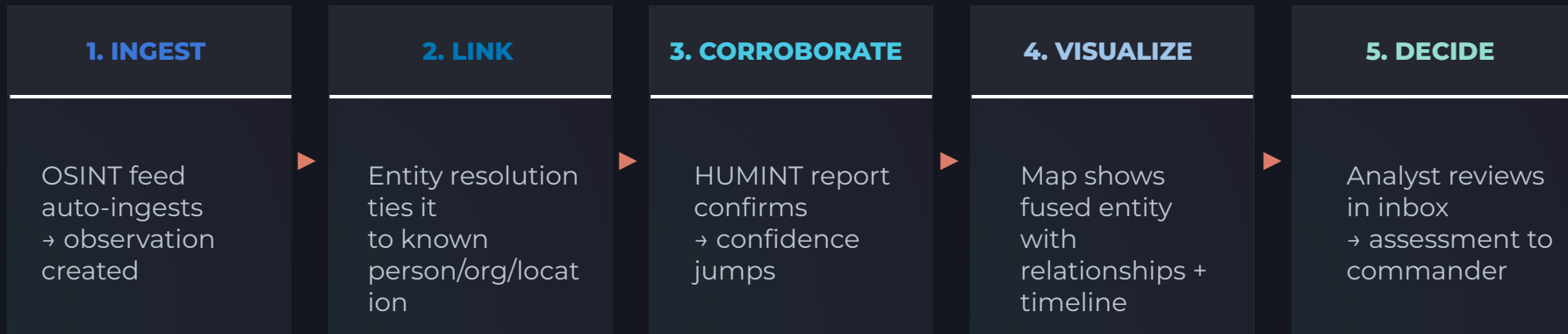
## OSINT + HUMINT + GEOINT + SIGINT + Cyber → **Single Fused Picture**

- ▶ Every source resolves to the same entities — people, orgs, locations, events
- ▶ Confidence and evidence travel with the data — not in a separate report
- ▶ One picture every analyst and commander sees — no reconciliation, no handoff

Five feeds in. One sourced, time-stamped, entity-centric picture out.



# Data to Decision: Minutes, Not Hours



Complete intelligence cycle – from raw signal to commander's decision in minutes



# One platform replacing six tools.

**SOURCE — TIGER-8**

ACTIVE Reliability: C Last contact: 2026-05-25

REAL NAME: Zhang Wei  
CONTACT: wz\_trade@163.com

NOTES:  
Mid-level logistics manager at PLA-linked trading company in Lhasa with business connections to Nathu La border trade. Provides commercial cover intelligence on dual-use goods movement toward LAC sectors. Recruited 2023 via third-country intermediary (Kathmandu). Intelligence corroborated twice on equipment movements. Access is limited — does not have direct military visibility. Handle with care.

ENCOUNTER LOGS + LOG ENCOUNTER

In Person 2026-05-25 Possibly true  
Kathmandu — third-country RV

TIGER-8 reports 40-50 container loads of dual-use electronics (RF components, optical sighting systems) transited Shigatse rail hub 8-10 March bound for Ngari-Gunsa airfield. Packing manifests describe contents as 'agricultural equipment'. Assessed consistent with EW upgrade programme at Ngari forward position.

Threat: S1d001e

**INTEL REPORT — SIGINT — CROSS-BORDER COMMUNICATION, AMRITSAR SECTOR (REF: S1G-2026-0055)**

SIGINT Amritsar drone video punjab constint

COMINT station Ferozpur intercepted 14 encrypted voice transmissions on 483 MHz frequency band — Amritsar sector — 13-14 March 0130-0315 hrs window. Linguistic analysis: Punjabi with Lahori dialect markers, 2 distinct speakers. Content partially decoded: references to "package", "three nights from now", and a grid reference consistent with Amritsar International Airport perimeter. Assess as advance coordination for drone delivery or VBIED prepositioning. QRF and counter-drone protocol activated at Amritsar sector.

LINKED THREATS: 3d3706ac

NOTEBOOK

**NORTHERN ...** 3 (1 online)

Chat Tasks Incidents Annotate

col\_sharma maj\_verma lt\_nair

col\_sharma 19:19  
NORTHERN COMMAND WATCH standing cell activated for daily theatre brief aggregation.

maj\_verma 19:19  
Daily brief 14 Mar: LoC quiet overnight, 2 drone alerts (Amritsar), Shopian cell update pending.

maj\_verma 19:19  
Daily brief 15 Mar: FALCON-1 debrief complete. Infiltration group tracked to Nala Leepa sector.

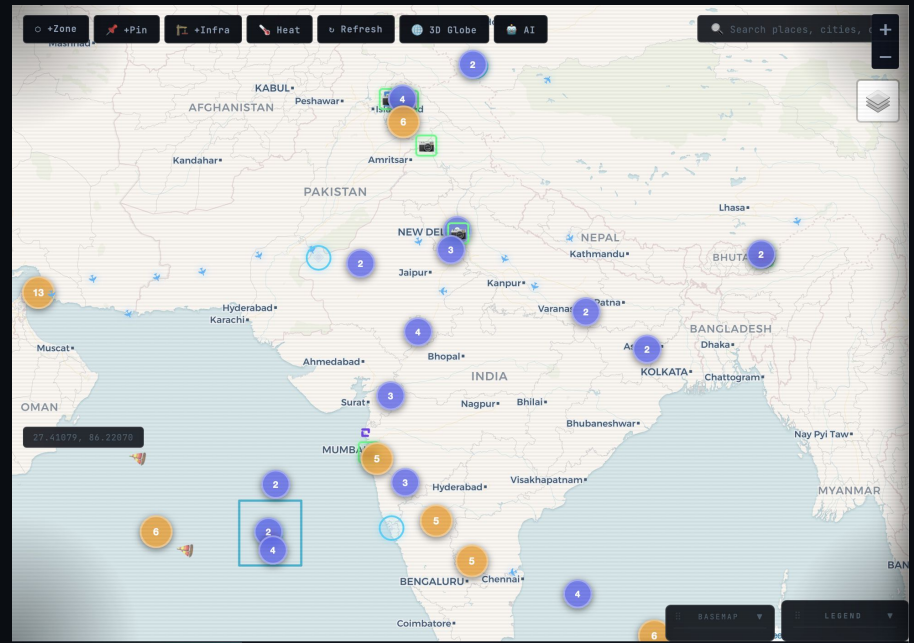
maj\_verma 19:19  
Daily brief 16 Mar: 3 zone breach alerts overnight — all friendly assets. CORDON OP ongoing.

col\_sharma 19:19  
Escalation: Infiltration group not neutralised after 72 hrs. DGM1 briefed. Additional assets authorised.

maj\_verma 19:19  
Daily brief 18 Mar: Maritime intercept ongoing. Tawang MASINT filed. Delhi cyber incident contained.

maj\_verma 19:19  
**LoC Nala Leepa Crossing — Active Sector**  
34.08000°, 73.90000°  
Primary active threat vector. Infiltration group still unaccounted for.  
[Click to open bookmark](#)

maj\_verma 19:19  
**Arabian Sea Grid 7 — Intercept Zone**  
16.20000°, 68.10000°  
Maritime intercept ongoing. MV Ramzan escort to Karwar.





# Before Vs After RavenAI

## BEFORE

6 disconnected tools  
Manual correlation  
Static reports  
Multiple handoffs

HOURS



## AFTER

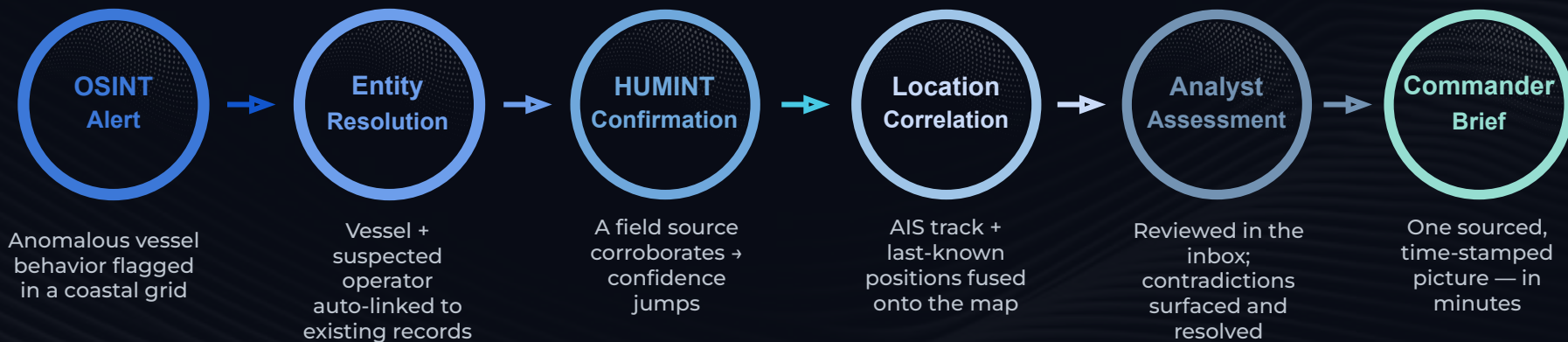
1 unified platform  
Automated fusion  
Live operating picture  
Single workflow

MINUTES

From fragmented tools to one fused operating picture.



# Use Case#1: Coastal Smuggling



**Five sources. One fused entity. Minutes to decision — not a multi-day correlation effort.**



# Use Case#2: Cross-Border Narco-Trafficking & Infiltration

## 1. Social Media Monitoring (OSINT)

Cross-border chatter and narcotics indicators detected.

## 2. Border Surveillance Inputs

Smart fence, UAV, and sensor alerts triggered.

## 3. Entity Resolution

Aliases, devices, vehicles & suspects linked.

## 4. Telecom Correlation

CDRs reveal handler-to-receiver communication patterns.

## 5. HUMINT Confirmation

Field sources confirm infiltration plans & routes.

## 6. Geospatial Correlation

Routes, detections, and incidents fused on map.

## 7. Analyst Assessment

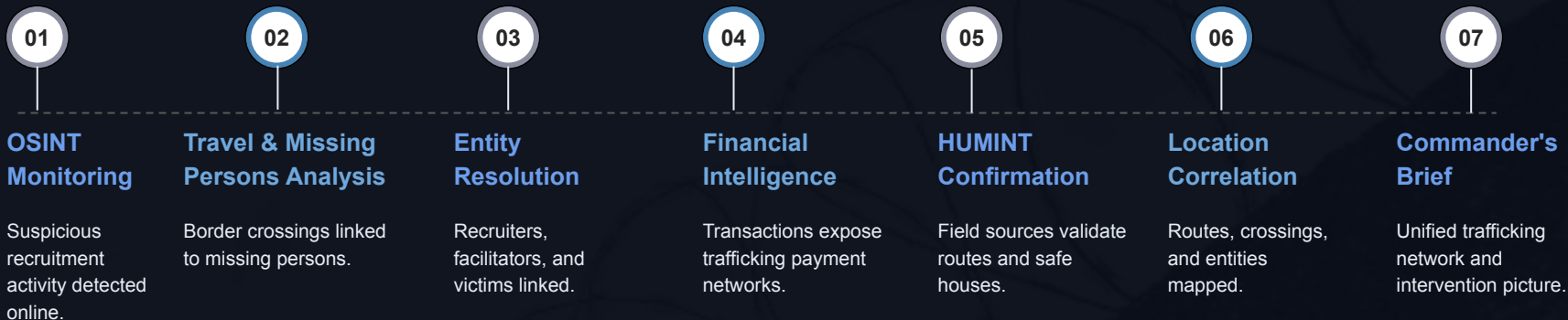
Evidence validated, confidence scored, contradictions resolved.

## 8. Commander's Brief

Unified threat picture with routes & interception points.



# Use Case#3: Human Trafficking Network



From Suspicion to Interception in Minutes.



# What's under the hood ?

## Entity Graph

- 10 entity types
- 16 relationship types
- Auto-linked across sources

## Confidence Engine

- 5-factor scoring
- Evidence chains
- Contradiction detection

## Fusion Map

- 5 semantic layers
- Temporal replay
- Lasso + radial menu

## Analyst Inbox

- Observations, reviews
- Contradictions, field activity
- Single-screen workflow

## OSINT Aggregation

- 7 live feeds
- Auto-classified
- Entity-linked

## HUMINT Encryption

- AES-256-GCM at rest
- RBAC with 7 roles
- Field agent mobile app

## Ops Rooms

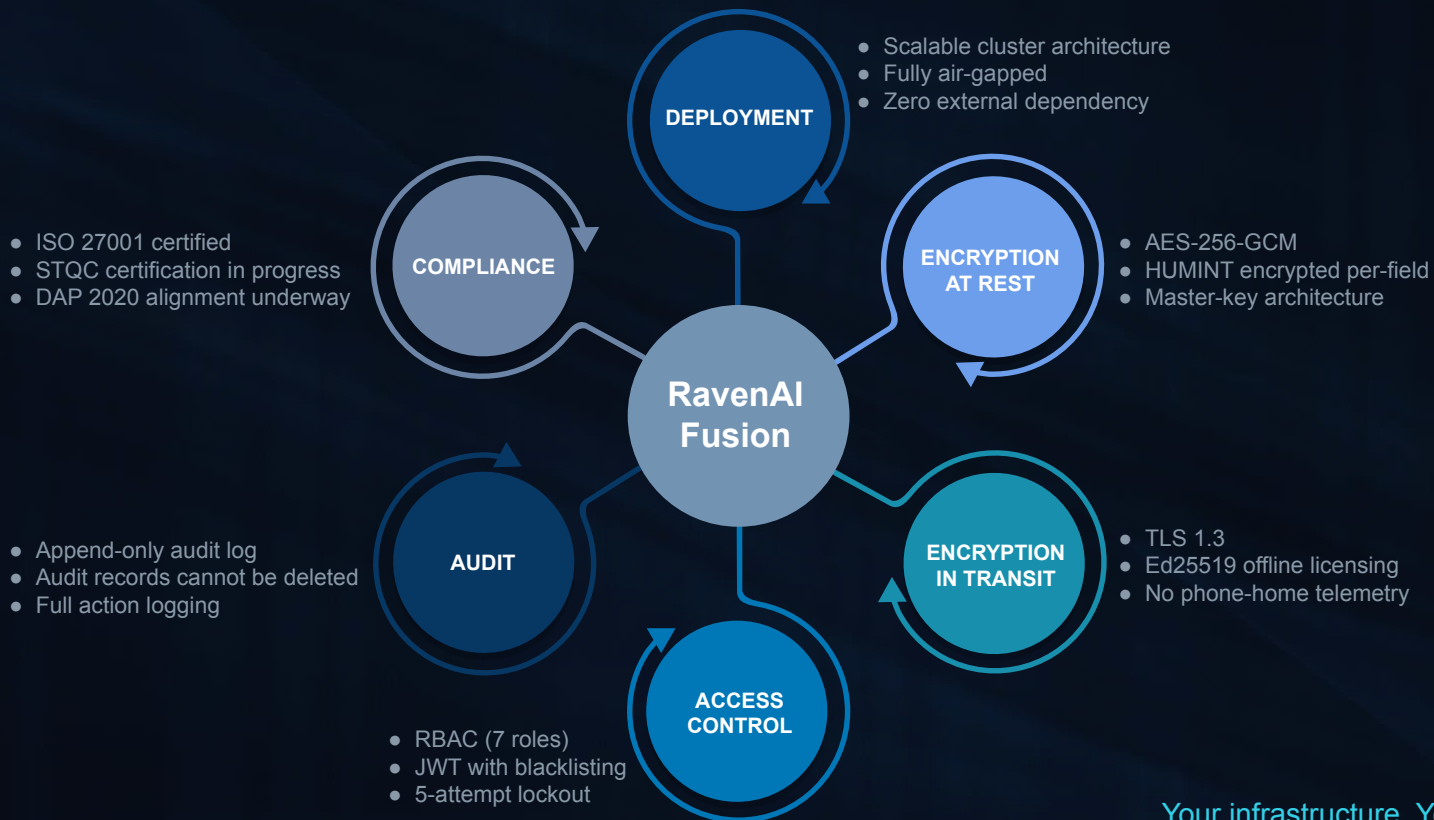
- Real-time chat
- Shared entities + map
- WebRTC + task mgmt

## Mobile App

- React Native
- Offline-capable
- Field agent focused



# Built for Classified Environments



Your infrastructure. Your data. Your control.



# The Real Comparison

	Other platforms	RavenAI Fusion
<b>Data residency</b>	Their cloud, their jurisdiction	<b>Your infrastructure, your control</b>
<b>Air-gapped</b>	Partial / bolt-on afterthought	<b>Native — designed for it from day one</b>
<b>Cost</b>	\$10 - 100M+ per year	<b>A fraction of that</b>
<b>Customization</b>	12–18 month release cycles	<b>Weeks — embedded team model</b>
<b>Built for</b>	Adapted for export	<b>Indian requirements, ground-up</b>

Built ground-up for Indian requirements — not version 10 adapted for export.



# Why Us ?

---

## TEAM

Proven deployments in the Indian defence / security ecosystem. We know your constraints.

## INTELLECTUAL PROPERTY

RavenAI patent granted. Trademark protected.

## CERTIFICATIONS

ISO 27001 certified. STQC certification in progress. DAP 2020 alignment underway.

## ENGINEERING DEPTH

18 development phases · 233+ integration tests · 294 static-analysis checks.

## INTEROPERABILITY

CoT/TAK compatible · OGC compliant · NATO STANAG aligned. [add logos]



# Don't evaluate a slide deck. Evaluate the platform.

## 30-Day Embedded Pilot

### What we bring

- ▶ Platform deployed on your infrastructure
- ▶ Dedicated engineering support team

### What you bring

- ▶ A real problem and a team to test it

**Operationally deployable today. Configurable for your mission requirements.**

If we don't deliver value, you owe us nothing.

[contact@pivotchain.com](mailto:contact@pivotchain.com) | [pivotchain.com](https://pivotchain.com)



# About Us

## Company

**Pivotchain Solutions** is an Pune, India based AI startup delivering security software for homeland, banking and aviation sector. Some of our key engagements include the **Ministry of Defence (India), Maharashtra Home Department (Prisons), Dubai Airport, Kotak Bank, Societe Generale, Maersk Shipping.**

## Product

**RavenAI** is our **patented** AI driven surveillance software that provides **large scale monitoring in a cost efficient manner.** RavenAI is entirely made in Maharashtra, India.

## Recognition

**Prime Minister's Award (National Startup Winner)**

Top 10 Intrusion detection companies globally

Top 5 Computer Vision (AI) startup globally

## Founders

**Deepak Rao, Founder, CEO**

*Ex Goldman Sachs, Morgan Stanley, Lehman Brothers with 20 Years of experience.*

**Yogendra Singh, Co-Founder, COO**

*Ex PwC, IBM, HSBC, Bajaj Finance. 11 years of experience.*



भारत सरकार, भारत सरकार Intellectual Property Office, Government of India, ऑफिस, नवमिहारा, पुणे, महाराष्ट्र, भारत सरकार  
INTELLECTUAL PROPERTY INDIA  
भारत सरकार, भारत सरकार  
कर्म सं/SL No :022153147

पेटेंट कार्यालय, भारत सरकार | The Patent Office, Government Of India

पेटेंट प्रमाण पत्र | Patent Certificate

(पेटेंट नियमावली का नियम 74) | (Rule 74 of The Patents Rules)

पेटेंट सं. / Patent No. : 575688  
आवेदन सं. / Application No. : 202421007157  
फाइल करने की तारीख / Date of Filing : 02/02/2024  
पेटेंटी / Patentee : Pivotchain Solution Technologies Pvt. Ltd

प्रमाणित किया जाता है कि पेटेंटी को, उपरोक्त आवेदन में यथाप्रकटित VIDEO SURVEILLANCE SYSTEM AND A METHOD THEREOF नामक आविष्कार के लिए, पेटेंट अधिनियम, 1970 के उपबन्धों के अनुसार आज तारीख फरवरी 2024 के दूसरे दिन से बीस वर्ष की अवधि के लिए पेटेंट अनुदान किया गया है।

It is hereby certified that a patent has been granted to the patentee for an invention entitled VIDEO SURVEILLANCE SYSTEM AND A METHOD THEREOF as disclosed in the above mentioned application for the term of 20 years from the 2<sup>nd</sup> day of February 2024 in accordance with the provisions of the Patents Act,1970.



अखिलेश कुमार  
अखिलेश कुमार  
Controller of Patents

अवदान की तारीख : 11/12/2025  
नियम - इस पेटेंट के नवीकरण के लिए फीस, यदि इसे बनाए रखा जाना है, फरवरी 2026 के दूसरे दिन को और उसके पश्चात प्रत्येक वर्ष में उसी दिन देना होगा।  
Note - The fees for renewal of this patent, if it is to be maintained, will fall / has fallen due on 2<sup>nd</sup> day of February 2026 and on the same day in every year thereafter.



# Key Engagements

Proven In The Field

Validated by Critical Infrastructure and Institutions





**Let us show you what  
this looks like in action.**

---

[Product Video](#) → [Live Demo](#) → [Q&A](#)

**Thank You!**