# S G INTELLECTUAL

# Invoice

(Subject to Delhi Jurisdiction)

**S G INTELLECTUAL**
4-D (Upper Floor), DDA Pocket-2
Sector-6, Dwarka,
New Delhi-110075, India
**Mob:** +91 9213764385
**E-mail:** info@sgintellectual.com

**Invoice No.: SGI/ANU/START-UP/ AI CPP SYSTEM -PATENT-06/2026**

**Vendor.** A STARTUP: **SRJX RESEARCH AND INNOVATION LAB LLP**
- **Certificate No. DIPP/203406**

THURSDAY, **MARCH 19, 2026**
Our Ref.: **ANU/AI CPP SYSTEM -PATENT-04/2026**

To
**SRJX RESEARCH AND INNOVATION LAB LLP**
PLOT No-3E/474, SECTOR-9, CDA, POST- MARKAT NAGAR,
AVINAB BIDANASI, CUTTACK- 753014

| **Description** | **Fee. (INR)** |
|---|---|
| 1. Professional fee towards providing general advisory on different intellectual property rights to start ups, providing information on protecting and promoting IPR to start ups in other countries, drafting Complete Specification and preparing and filing other documents such as Form-1, Form-2, Form-3, Form-9 and Form 18A, reporting to client the filing of the Patent Application No. **202631033028** dated **18TH MARCH 2026.** | NIL |
| 2. Government Fee for filing the Patent Application. | INR 19,460/- |
| 3. Miscellaneous expenses including charges for typing, phone, Print outs, photocopy, stamp fee, postal charges, conveyance etc. | INR 1000/- |
| Total | **INR 20,460/.00 (excluding taxes)** |
| **Rs. TWENTY THOUSAND AND FOUR HUNDRED SIXY ONLY (excluding taxes)** | |

**Payment Options**: : By Direct Deposit to
A/c Name: **S G Intellectual**
Acct No. **60394529800**
Name of the Bank: Bank of Maharashtra,
Sector-19, Dwarka, New Delhi
IFSC Code: MAHB0001244

**This invoice is computer generated and does not need a signature.**

Welcome ANURADHA GUPTA Sign out

**Controller General of Patents, Designs & Trade Marks**

सत्यमेव जयते

INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS
GEOGRAPHICAL INDICATIONS

**G.A.R.6**
**[See Rule 22(1)]**
**RECEIPT**

**Docket No 7518**

**Date/Time 2026/03/18 21:06:19**

**To**
**ANURADHA GUPTA**

**4-D (UPPER FLOOR), DDA, POCKET - 2,**
**SECTOR -6, DWARKA, NEW DELHI**

**UserId: anuradha4d**

**CBR Detail:**

| Sr. No. | App. Number | Ref. No./Application No. | Amount Paid | C.B.R. No. | Form Name | Remarks |
|---|---|---|---|---|---|---|
| 1 | 202631033028 | TEMP/E-1/35841/2026-KOL | 8960 | 3979 | FORM 1 | ARTIFICIAL SUPER INTELLIGENCE (ASI) BASED CRIME PREDICTION AND PREVENTION SYSTEMS |
| 2 | E-106/1720/2026/KOL | 202631033028 | 0 | ----- | FORM28 | ---- |

| TransactionID | Payment Mode | Challan Identification Number | Amount Paid | Head of A/C No |
|---|---|---|---|---|
| N-0001898994 | Online Bank Transfer | 1803260077993 | 8960.00 | 1475001020000001 |

Total Amount : ₹ 8960.00
Amount in Words: Rupees Eight Thousand Nine Hundred Sixty Only

Received from ANURADHA GUPTA the sum of ₹ 8960.00 on account of Payment of fee for above mentioned Application/Forms.

* This is a computer generated receipt, hence no signature required.

Print

Home About Us Contact Us

Welcome ANURADHA GUPTA Sign out

**Controller General of Patents, Designs & Trade Marks**
CP-2, Sector V, Salt Lake City, Kolkata-700091
Tel No. (091)(033) 23671945-46 Fax No. 033 23671988
E-mail: kolkata-patent@nic.in
Web Site: www.ipindia.gov.in

सत्यमेव जयते

INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS
GEOGRAPHICAL INDICATIONS

**G.A.R.6**
**[See Rule 22(1)]**
**RECEIPT**

**Docket No 7621** **Date/Time 2026/03/19 18:15:27**

**To** **UserId: anuradha4d**
**ANURADHA GUPTA**

**4-D (UPPER FLOOR), DDA, POCKET - 2,**
**SECTOR -6, DWARKA, NEW DELHI**

**CBR Detail:**

| Sr. No. | App. Number | Ref. No./Application No. | Amount Paid | C.B.R. No. | Form Name | Remarks |
|---|---|---|---|---|---|---|
| 1 | E-12/647/2026/KOL | 202631033028 | 2500 | 4034 | FORM 9 | |

| TransactionID | Payment Mode | Challan Identification Number | Amount Paid | Head of A/C No |
|---|---|---|---|---|
| N-0001899816 | Online Bank Transfer | 1903260051874 | 2500.00 | 1475001020000001 |

Total Amount : ₹ 2500.00
Amount in Words: Rupees Two Thousand Five Hundred Only

Received from ANURADHA GUPTA the sum of ₹ 2500.00 on account of Payment of fee for above mentioned Application/Forms.

* This is a computer generated receipt, hence no signature required.

Print

Home About Us Contact Us

Welcome ANURADHA GUPTA Sign out

Controller General of Patents, Designs & Trade Marks
CP-2, Sector V, Salt Lake City, Kolkata-700091
Tel No. (091)(033) 23671945-46 Fax No. 033 23671988
E-mail: kolkata-patent@nic.in
Web Site: www.ipindia.gov.in

सत्यमेव जयते

INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS
GEOGRAPHICAL INDICATIONS

**G.A.R.6**
**[See Rule 22(1)]**
**RECEIPT**

**Docket No 7633**

**Date/Time 2026/03/19 18:50:48**

**To**
**ANURADHA GUPTA**

**4-D (UPPER FLOOR), DDA, POCKET - 2,**
**SECTOR -6, DWARKA, NEW DELHI**

**UserId: anuradha4d**

**CBR Detail:**

| Sr. No. | App. Number | Ref. No./Application No. | Amount Paid | C.B.R. No. | Form Name | Remarks |
|---|---|---|---|---|---|---|
| 1 | E-3/934/2026/KOL | 202631033028 | 0 | ----- | FORM 3 | |
| 2 | E20263019551 | 202631033028 | 8000 | 4039 | FORM 18A | ---- |
| 3 | E-45/752/2026/KOL | 202631033028 | 0 | ----- | FORM 26 | ---- |

| TransactionID | Payment Mode | Challan Identification Number | Amount Paid | Head of A/C No |
|---|---|---|---|---|
| N-0001899864 | Online Bank Transfer | 1903260054786 | 8000.00 | 1475001020000001 |

Total Amount : ₹ 8000.00
Amount in Words: Rupees Eight Thousand Only

Received from ANURADHA GUPTA the sum of ₹ 8000.00 on account of Payment of fee for above mentioned Application/Forms.

* This is a computer generated receipt, hence no signature required.

Print

Home About Us Contact Us

(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :18/03/2026

(21) Application No.202631033028 A

(43) Publication Date : 27/03/2026

(54) Title of the invention : ARTIFICIAL SUPER INTELLIGENCE (ASI) BASED CRIME PREDICTION AND PREVENTION SYSTEMS

| | |
|---|---|
| (51) International classification | :H04L 29/06, G08B 13/196, H04W 4/38, G08B 25/10, H04W 4/02 |
| (31) Priority Document No | :NA |
| (32) Priority Date | :NA |
| (33) Name of priority country | :NA |
| (86) International Application No<br>Filing Date | :<br>:01/01/1900 |
| (87) International Publication No | : NA |
| (61) Patent of Addition to Application Number<br>Filing Date | :NA<br>:NA |
| (62) Divisional to Application Number<br>Filing Date | :NA<br>:NA |

(71)**Name of Applicant :**
**1)SRJX RESEARCH AND INNOVATION LAB LLP**
Address of Applicant :PLOT NO.-3E/474 SECTOR-9, CDA, POST-MARKAT NAGAR, CUTTACK, ODISHA, INDIA CUTTACK Orissa India
(72)**Name of Inventor :**
**1)JENA, Soumya Ranjan**
**2)MENDAGUDLI, Mallappa Gurupadappa**

(57) Abstract :
The present invention discloses an Artificial Superintelligence (ASI) based a real-time crime prediction and prevention system (100) and its method. The system (100) comprises a plurality of field sensing devices (102), edge gateway devices (104), a secure communication network (106), command center server (108), databases (110), operator terminals (112) and patrol mobile communication devices (114). The plurality of field sensing devices (102) is configured to generate structured and unstructured event data streams. The one or more edge gateway devices (104) is operatively coupled to the field sensing devices (102). The secure communication network (106) is configured to provide encrypted and authenticated data transmission. The command center server (108) is communicatively coupled to the secure communication network (106). The databases (110) are operatively coupled to the command center server (108). The operator terminals (112) and patrol mobile communication devices (114) are communicatively coupled to the command center server (108).

No. of Pages : 66 No. of Claims : 15

**FORM 2**

THE PATENTS ACT, 1970

[39 of 1970]

&

THE PATENTS RULES, 2003

**COMPLETE SPECIFICATION**

(Section 10; Rule 13)

# ARTIFICIAL SUPER-INTELLIGENCE (ASI) BASED CRIME PREDICTION AND PREVENTION SYSTEMS

**SRJX RESEARCH AND INNOVATION LAB LLP**

PLOT NO-3E/474, SECTOR-9, CDA, POST- MARKAT NAGAR,

CUTTACK- 753014, ODISHA, INDIA

An Indian Company

The following Specification particularly describes the invention and the manner in which it is to be performed.

## FIELD OF INVENTION

The present invention relates to crime prediction and prevention systems, more particularly relates to an Artificial Super-Intelligence (ASI) based crime prediction and prevention system.

## BACKGROUND

Crime prevention and public safety operations increasingly depend on timely intelligence derived from large volumes of heterogeneous information, including incident reports, emergency calls, CCTV and body-worn camera feeds, social media signals, mobility and crowd density data, weather and event schedules, and socio-economic indicators. Conventional policing methods typically rely on manual analysis, periodic reporting, and human experience to identify hotspots, repeat offenders, and emerging threats. However, urban growth, rapid mobility, and evolving criminal tactics create complex, fast-changing patterns that are difficult to detect early using traditional tools, often resulting in delayed intervention, inefficient resource allocation, and preventable harm to citizens and property.

Existing computer-aided dispatch and analytics platforms provide dashboards, mapping, and statistical summaries, but many remain limited to descriptive reporting (what happened and where) rather than actionable forecasting (what is likely to happen next and how to reduce the risk). Where predictive policing solutions exist, they commonly use historical crime counts and basic spatial-temporal models to produce hotspot maps or risk scores for a given region and time window. These approaches can be constrained by incomplete or delayed data entry, variations in reporting practices across jurisdictions, and a lack of integration between independent databases maintained by police, municipal agencies, private security partners, and emergency responders. As a result, risk forecasts may be coarse, inconsistent, and difficult to operationalize at the moment of decision.

Many current machine learning approaches also face technical and practical shortcomings. Crime events are often "rare" relative to non-events, causing class imbalance and unstable model behavior, particularly for low-frequency but high-severity incidents. Models trained on past patterns may degrade when criminal behavior shifts, when new surveillance infrastructure is deployed, or when policies change, leading to concept drift. Further, several approaches function as "black boxes," offering limited interpretability or traceability for why a location, time, or individual was flagged. In high-stakes public safety contexts, lack of explainability can reduce trust, complicate auditing, and hinder adoption by field personnel who must justify actions and comply with procedural safeguards.

Another recognized limitation involves ethical, legal, and governance risks. Data sources may contain historical bias, under-reporting, or enforcement-driven artifacts that can inadvertently amplify disproportionate targeting of specific communities if used without safeguards. Privacy concerns arise when large-scale surveillance, personal identifiers, or sensitive attributes are combined without strong access controls, minimization, and accountability. Additionally, many solutions emphasize prediction but provide limited guidance on prevention actions that are proportional, policy-compliant, and measurable, such as optimized patrol routing, community outreach triggers, situational alerts, or coordination with non-police services.

Accordingly, there is a need for an improved crime prediction and prevention system that can (i) fuse multi-modal data in near real time, (ii) continuously learn and adapt to changing conditions, (iii) provide explainable and auditable risk assessments, and (iv) recommend prevention interventions under explicit operational constraints and governance rules. There is also a need for human-in-the-loop decision support that integrates with existing law-enforcement workflows, supports escalation and de-escalation protocols, and produces outcome feedback for measuring effectiveness. An Artificial Super-Intelligence (ASI)- based approach, emphasizing advanced reasoning, continual learning, and safety-constrained decisioning, is intended to address these

unmet needs while enabling responsible deployment aligned with public safety objectives and regulatory requirements.

Prior art crime prediction and predictive policing systems are commonly driven by limited and incomplete data, most often relying heavily on historical crime incident logs and basic dispatch records. These sources can be delayed, inconsistently recorded across stations, or under-represent certain incident types due to underreporting. As a result, earlier inventions may generate hotspot outputs that reflect past reporting practices rather than real, evolving risk, which reduces operational usefulness for prevention.

Many earlier solutions focus on descriptive analytics and static hotspot mapping rather than dynamic forecasting. In practice, several systems produce periodic heatmaps (daily/weekly) and generalized risk zones that do not update rapidly as conditions change (crowd formation, sudden events, traffic disruptions, or social unrest). This lack of real-time adaptation can lead to missed early warnings, delayed interventions, and inefficient deployment of patrol resources.

A major technical limitation in prior art is poor handling of rare and high-severity events. Serious incidents such as violent crimes or targeted attacks can be relatively infrequent, creating class imbalance and unstable prediction models. Traditional machine learning systems may either overpredict (creating excessive false alerts) or underpredict (missing true threats). Many legacy approaches also fail to incorporate uncertainty estimation, making it difficult for officers to interpret confidence levels and act proportionately.

Prior inventions often lack robust mechanisms to address concept drift and evolving criminal tactics. When offender behavior changes due to enforcement pressure, new technology, seasonal shifts, or socio-economic changes, models trained on older patterns degrade rapidly. Earlier solutions may require manual retraining cycles and do

not provide automated drift detection, continuous learning, or rapid recalibration, which causes forecasts to become outdated and unreliable.

Another problem in prior art is insufficient multi-modal fusion and contextual reasoning. Many systems do not properly integrate unstructured and real-time inputs such as CCTV analytics, sensor alerts, crowd density signals, social media indicators, weather, festival schedules, or event permits. Without contextual enrichment, earlier systems cannot distinguish a genuine risk buildup from normal anomalies (e.g., a concert crowd vs. a riot situation), leading to either false alarms or missed escalation cues.

A significant operational gap is that many earlier inventions generate predictions but provide limited support for prevention actions. Outputs are frequently presented as risk scores or heatmaps without converting them into executable recommendations such as optimized patrol routing, resource staging, targeted alerts, inter-agency coordination, or escalation/de-escalation workflows. This weak linkage between analytics and field operations reduces adoption and makes it difficult to demonstrate measurable crime reduction.

Prior art systems also face challenges related to explainability and auditability. Black-box models may provide a high-risk label without stating why a location or situation was flagged, which limits trust among decision-makers and frontline officers. In high-stakes public safety deployments, agencies need traceable reasoning, factor attribution, and logs for auditing; earlier inventions often do not provide adequate transparency to support governance, accountability, and legal defensibility.

Ethical and legal risks represent another major weakness in earlier solutions. Many legacy predictive policing tools are criticized for bias amplification, where historical enforcement patterns can disproportionately influence risk outputs for particular

communities. Several older systems lack fairness constraints, bias monitoring, privacy-preserving design, and policy controls to ensure that outputs remain compliant with lawful policing standards. This results in reputational risk, reduced community trust, and potential regulatory or judicial challenges. Earlier inventions may not implement strong data security, access control, and privacy safeguards appropriate for sensitive law-enforcement data. Inadequate encryption, weak authentication, insufficient logging, or uncontrolled sharing across systems can lead to data misuse and breaches. The present invention targets these deficiencies by incorporating secure ingestion, masking/anonymization options, role-based access controls, and continuous audit logging while supporting accountable, policy-governed decision support.

Therefore, there is a need for an Artificial Superintelligence (ASI) based crime prediction and prevention system to overcome the above mentioned drawbacks.

## OBJECTS OF THE INVENTION

According to embodiments of the present invention, the key objectives are given below:

1. To provide Real-time crime risk forecasting by predicting where, when, and what type of crime is likely to occur within defined time windows.
2. Multi-source data fusion by integrating historical crime records with live feeds (CCTV/IoT), emergency calls, GPS/patrol data, weather, events, and public reports.
3. Fine-grained hotspot and micro-zone prediction at street/block/ward level with dynamic updates.
4. Early warning and alert generation for high-risk zones, repeat patterns, and emerging threats.
5. Explainable and auditable outputs showing key contributing factors, confidence score, and reasoning trace for each prediction.
6. Prevention-oriented recommendations including patrol allocation, route optimization, surveillance focus, and coordinated response actions.

7. Human-in-the-loop control allowing authorized officers to review, approve, modify, or reject suggested preventive actions.
8. Continuous learning and drift adaptation to handle changing crime patterns, seasonal effects, and new modus operandi.
9. Bias and fairness monitoring to reduce discriminatory outcomes and ensure responsible decision support.
10. Privacy and security compliance through data minimization, anonymization/masking, access control, and secure logging.
11. Outcome feedback loop capturing real-world results (true/false alerts, intervention impact) to improve accuracy over time.
12. Operational performance improvement by reducing response time, improving resource utilization, and enabling measurable crime prevention impact.

**SUMMARY OF THE INVENTION**

The present invention relates to an Artificial Super-Intelligence (ASI) based Crime Prediction and Prevention System that provides proactive, real-time decision support to public safety agencies. The system is designed to continuously ingest and fuse multi-source, multi-modal data—such as historical crime records, emergency call logs, patrol and GPS traces, weather and event schedules, CCTV/IoT sensor streams, social media and public alerts, and contextual geo-spatial information—to generate dynamic risk forecasts for potential criminal incidents. Unlike conventional hotspot mapping tools that primarily rely on past crime frequency, the invention produces time-sensitive, fine-grained predictions across locations, crime categories, and evolving situational conditions.

In one embodiment, the system includes a data ingestion and normalization layer that securely collects structured and unstructured inputs from multiple authorities and devices, performs de-duplication, anonymization or masking (where required), and converts the inputs into a unified spatio-temporal representation. A feature engineering and context enrichment module then derives predictive indicators including movement

anomalies, crowd density shifts, repeat-pattern signatures, environmental triggers (e.g., rainfall, temperature, holidays), infrastructure context (e.g., transit stations, schools, ATMs), and known incident correlations. This enriched representation is stored within a secure data lake and real-time stream buffer to support both historical learning and live inference.

In another embodiment, the invention comprises an ASI-based intelligence core that combines multiple modeling paradigms, including deep learning, graph-based reasoning, and probabilistic forecasting, to estimate the likelihood, time window, and potential severity of crime occurrences. The intelligence core can learn relationships between entities (locations, incident types, modus operandi patterns, resources, and temporal cycles) and can adapt to shifting trends using continual learning and drift detection. The system further generates explainable outputs, including the main contributing factors, confidence levels, and uncertainty bounds, enabling officers and administrators to understand why a region or situation has been flagged and to audit the decision flow.

In yet another embodiment, the system includes a prevention and response orchestration engine that converts predictions into operational recommendations. Such recommendations can include optimized patrol deployment, dynamic route planning, resource staging, targeted situational alerts to nearby units, coordination with emergency medical services, activation of surveillance focus zones, and community safety advisories. The prevention engine operates under configurable policy constraints—such as jurisdiction boundaries, permissible interventions, priority rules, and fairness thresholds—to ensure that outputs remain compliant with governance standards and departmental procedures. A human-in-the-loop approval workflow may be provided, allowing authorized personnel to review, modify, approve, or reject recommended actions prior to execution.

In a further embodiment, the invention provides an outcome feedback and learning loop that captures post-action results, incident confirmations, false positives, officer notes, and community reports to evaluate effectiveness and continuously improve model

performance. The system can generate performance dashboards (precision, recall, response-time improvement, risk reduction indicators) and can support periodic auditing for bias, privacy compliance, and model drift. Accordingly, the invention delivers an integrated, explainable, and policy-governed ASI-based framework for forecasting crime risk and enabling timely, measurable prevention actions, thereby enhancing public safety preparedness and resource efficiency.

An embodiment of the present invention describes a real-time crime prediction and prevention system (100). The system (100) comprises a plurality of field sensing devices (102) configured to generate structured and unstructured event data streams; one or more edge gateway devices (104) operatively coupled to the field sensing devices (102), each edge gateway device comprising: a first hardware processor (116), and a first memory unit (118) storing executable instructions that, when executed by the first hardware processor (116), cause the edge gateway device to: receive raw event data streams from the field sensing devices (102), perform filtering, compression, anomaly detection, timestamp synchronization, and geo-tag normalization, generate standardized event metadata, and transmit the standardized event metadata over a secure communication network (106); the secure communication network (106) configured to provide encrypted and authenticated data transmission; at least one command center server (108) communicatively coupled to the secure communication network (106), the command center server (108) comprising: a second hardware processor (120), and a second memory unit (122) storing executable instructions that, when executed by the second hardware processor (120), cause the command center server (108) to: ingest the standardized event metadata and additional structured and unstructured data including historical crime records, patrol logs, mobility data, and contextual inputs, perform de-duplication, normalization, timestamp alignment, and geo-spatial indexing, transform the ingested data into geo-gridded time-series tensors and relational entity graphs representing micro-zones, execute a hybrid intelligence processing pipeline stored in the second memory unit to generate a risk forecast

including predicted micro-zone, predicted time window, predicted crime category, probability score, severity index, and uncertainty bound, generate ranked contributing factors and confidence values corresponding to the risk forecast, compute constrained intervention recommendations based on patrol resources, jurisdiction boundaries, response-time thresholds, and governance policies, enforce governance controls including role-based access control and audit logging, and update model parameters using outcome feedback including confirmed incidents and response metrics; one or more databases (110) operatively coupled to the command center server (108); and operator terminals (112) and patrol mobile communication devices (114) communicatively coupled to the command center server (108), wherein the second hardware processor is configured to transmit intervention instructions from the command center server (108) to the patrol mobile communication devices (114) only upon receipt of an approval signal generated through the human-in-the-loop authorization workflow executed at the operator terminals (112).

According an embodiment of the present invention, the first hardware processor of the edge gateway device is configured to transmit only event metadata when no anomaly threshold is exceeded and to transmit corresponding raw media segments when the anomaly threshold is exceeded.

According another embodiment of the present invention, the second hardware processor is configured to assign confidence weights to heterogeneous data sources and resolve conflicting event records using timestamp reconciliation and geo-spatial clustering.

According to yet another embodiment of the present invention, the hybrid intelligence processing pipeline comprises a non-linear pattern extraction component, a relational dependency modeling component, and a probabilistic forecasting component, executed by the second hardware processor.

According to yet another embodiment of the present invention, the second hardware processor is configured to detect statistical distribution shifts in incoming data streams and initiate controlled model recalibration while maintaining versioned model parameters in the databases (110).

According to yet another embodiment of the present invention, the governance controls include masking or tokenization of sensitive identifiers prior to inclusion in model training datasets.

According to yet another embodiment of the present invention, the second hardware processor computes multiple ranked intervention scenarios with corresponding estimated resource costs and predicted impact scores prior to presenting the intervention recommendations at the operator terminals (112).

According to yet another embodiment of the present invention, the geo-gridded time-series tensors represent predefined micro-zones at street-level granularity within the monitored jurisdiction.

According to yet another embodiment of the present invention, the operator terminals (112) are configured to display dynamic risk heatmaps with associated confidence intervals and contributing factor rankings.

According to yet another embodiment of the present invention, the second hardware processor computes performance metrics including precision, recall, and response-time improvement indicators and stores the performance metrics in the databases (110).

Another embodiment of the present invention describes a computer-implemented method for real-time crime prediction and prevention executed by at least one edge gateway device and at least one command center server. The method comprises receiving, by a first hardware processor of the edge gateway device, raw event data

streams from a plurality of field sensing devices; performing, by the first hardware processor, localized preprocessing including filtering, compression, anomaly detection, timestamp synchronization, and geo-tag normalization; generating standardized event metadata corresponding to detected events; and transmitting the standardized event metadata, without transmitting full raw media streams unless a predefined anomaly threshold is exceeded, over a secure communication network to the command center server; receiving, by a second hardware processor of the command center server, the standardized event metadata and additional structured and unstructured data including historical crime records, patrol deployment logs, mobility traces, and contextual environmental inputs; performing de-duplication, schema normalization, timestamp alignment, and geo-spatial indexing to generate a unified dataset; transforming the unified dataset into: geo-gridded time-series tensors representing predefined micro-zones within a monitored jurisdiction; and relational entity graphs representing associations among locations, incident categories, temporal cycles, infrastructure nodes, and mobility patterns; executing, by the second hardware processor, a hybrid intelligence processing pipeline stored in memory unit to generate a risk forecast including predicted micro-zone, predicted time window, predicted crime category, probability score, severity index, and uncertainty bound; generating ranked contributing factors and confidence values corresponding to the risk forecast; computing constrained intervention recommendations based on available patrol resources, jurisdiction boundaries, patrol shift schedules, response-time thresholds, traffic conditions, and governance policies; presenting the risk forecast and intervention recommendations at operator terminals; receiving an approval signal generated through a human-in-the-loop authorization workflow executed at the operator terminals; and transmitting intervention instructions from the command center server to patrol mobile communication devices only upon receipt of the approval signal; updating model parameters based on outcome feedback including confirmed incidents, false alerts, and response metrics.

According to another embodiment of the present invention, the method of performing localized preprocessing further includes selectively transmitting raw media segments only when anomaly scores exceed a predefined threshold.

According to yet another embodiment of the present invention, the method of executing the hybrid intelligence processing pipeline further comprises assigning confidence weights to heterogeneous data sources and resolving conflicting records using geo-spatial clustering.

According to yet another embodiment of the present invention, the method of computing constrained intervention recommendations further comprises generating multiple ranked intervention scenarios with corresponding resource cost estimates prior to presenting the recommendations at the operator terminals.

According to yet another embodiment of the present invention, the method of updating model parameters further comprises detecting statistical divergence between real-time input data and baseline training data and initiating incremental recalibration while maintaining versioned model parameters.

## BRIEF DESCRIPTION OF THE ACCOMPANYING DRAWINGS

This invention is described by way of example with reference to the following drawings. These drawings being referred herein are for the purpose of illustrating preferred embodiments of the invention only, and not for the purpose of limiting the same.

**FIG. 1** illustrates a block diagram of a real-time crime prediction and prevention system, according to an embodiment of the present invention.

**FIG. 2** illustrates an Artificial Superintelligence (ASI) based real-time crime prediction and prevention system, according to an embodiment of the present invention.

**FIG. 3** illustrates an Artificial Superintelligence (ASI) based real-time crime prediction and prevention system, according to an exemplary embodiment of the present invention.

**FIG. 4** illustractes a logic layer architecture of an Artificial Superintelligence (ASI) based real-time crime prediction and prevention system, according to an embodiment of the present invention.

**FIG. 5** illustractes a loop approval workflow for an Artificial Superintelligence (ASI) based real-time crime prediction and prevention system, according to an embodiment of the present invention.

**FIG. 6A and 6B** illustracte a flow-chart illustrating a computer-implemented method for real-time crime prediction and prevention, according to an embodiment of the present invention.

## DETAILED DESCRIPTION OF THE ACCOMPANYING DRAWINGS

The present invention is described hereinafter by various embodiments with reference to the accompanying drawings, wherein reference numerals used in the accompanying drawings correspond to the like elements throughout the description. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, the embodiments are provided so that this disclosure will be thorough and complete and will fully convey the scope of the invention to those skilled in the art.

It will be understood by those skilled in the art that the foregoing general description and the following detailed description are exemplary and explanatory of the invention and are not intended to be restrictive thereof. The terms "comprises", "comprising", or any other variations thereof, are intended to cover a non-exclusive inclusion, Appearances of the phrase "in an embodiment", "in another embodiment" and similar

language throughout this specification may, but not necessarily do, all refer to the same embodiment.

Further, the words "a" or "an" mean "at least one" and the word "plurality" means "one or more" unless otherwise mentioned. Furthermore, the terminology and phraseology used herein is solely used for descriptive purposes and should not be construed as limiting in scope. The systems, methods, and examples provided herein are only illustrative and not intended to be limiting.

The present invention introduces an Artificial Super-Intelligence (ASI) based, policy-governed crime prediction and prevention framework that goes beyond conventional predictive policing by combining continuous reasoning, multi-layer learning, and operational decision support in a single system. Unlike prior approaches that primarily generate static hotspot maps from historical crime logs, the invention provides a dynamic, real-time risk intelligence pipeline that continuously updates forecasts and recommended interventions as new signals arrive from multiple sources.

A first unique aspect is the multi-modal, real-time fusion of heterogeneous inputs into a unified spatio-temporal intelligence representation. The system securely ingests structured data (FIR/incident records, emergency calls, patrol logs, offender history, traffic flows) and unstructured data (CCTV metadata, sensor alerts, citizen tips, open-source signals) and converts them into standardized geo-tagged time-series and event graphs. This enables the invention to detect emerging risk patterns earlier than systems that rely on single-source historical crime counts.

A second unique aspect is the ASI-based hybrid reasoning core that combines (i) statistical forecasting, (ii) deep learning, and (iii) graph-based relational reasoning to model not only where crime might occur, but also why risk is rising and how risk may propagate across locations, time windows, and connected entities. The system can infer

relationships such as repeat-modus-operandi patterns, offender-location associations, trigger events, and infrastructure vulnerabilities (e.g., transit hubs, ATM clusters), producing risk forecasts with structured causal indicators rather than only probability values.

A third unique aspect is the inclusion of continuous learning with automated drift detection and controlled recalibration. The invention monitors changes in data distribution and prediction performance to detect concept drift caused by seasonal effects, policy changes, or evolving criminal tactics. Upon drift detection, the system adapts using a governed learning loop that updates model components without destabilizing field operations, thereby maintaining long-term reliability compared to prior systems that require manual retraining cycles and periodic offline updates.

A further unique aspect is the explainable, auditable risk reasoning layer that generates transparent outputs for each prediction. The system provides confidence scores, uncertainty bounds, and ranked contributing factors (e.g., recent incident clusters, crowd anomalies, weather triggers, temporal cycles, sensor evidence) along with traceable logs that enable review by supervisors, auditors, and authorized oversight bodies. This improves operational trust and defensibility compared to black-box systems that cannot justify their alerts.

Another unique aspect is the prevention orchestration engine, which converts predicted risks into actionable, policy-compliant recommendations. Instead of merely displaying hotspots, the invention generates intervention options such as optimized patrol routing, resource staging, targeted situational alerts, surveillance focus areas, traffic diversion coordination, and community outreach triggers. Each recommendation is produced under explicit constraints such as jurisdiction rules, available manpower, response-time objectives, and proportionality limits, enabling measurable prevention planning rather than passive forecasting.

A further unique aspect is the fairness, privacy, and compliance-by-design governance module embedded into the technical workflow. The invention supports configurable privacy controls (masking/anonymization, minimization, retention limits), role-based access, secure logging, and bias monitoring metrics. It can enforce fairness thresholds and prevent sensitive-attribute misuse, thereby reducing the risk of discriminatory outcomes and supporting responsible deployment, which is often absent or weakly implemented in earlier solutions. The invention introduces a closed-loop outcome learning and effectiveness measurement mechanism. The system captures post-intervention outcomes such as confirmed incidents, false alerts, response effectiveness, and community feedback to continuously improve accuracy and quantify real-world impact. By linking prediction → intervention → measured outcome, the invention enables agencies to evaluate whether actions reduced incidents, improved response times, or optimized resource utilization, thereby providing a complete, adaptive, and accountable crime prevention intelligence system.

**FIG. 1** illustrates a block diagram of a real-time crime prediction and prevention system (100), according to an embodiment of the present invention.

In one embodiment, the present invention provides a real-time crime prediction and prevention system (100) configured to collect situational data from distributed sensing infrastructure, process the collected data through a distributed computing framework, and generate predictive risk assessments together with operational intervention recommendations.

As illustrated in FIG. 1, the system (100) comprises a plurality of field sensing devices (102), one or more edge gateway devices (104), a secure communication network (106), a command center server (108), one or more databases (110), operator terminals (112), and patrol mobile communication devices (114).

The system architecture enables distributed data acquisition, localized preprocessing at edge devices, centralized intelligence processing at the command center server, and controlled deployment of preventive interventions.

**Field Sensing Devices**

In one of embodiment of the present invention, the field sensing devices (102) are deployed across monitored geographic regions such as streets, public spaces, transportation hubs, and critical infrastructure zones. These devices are configured to continuously monitor environmental conditions and generate event data streams indicative of situational activity.

In various embodiments, the field sensing devices may include:

- surveillance cameras
- acoustic sensors
- environmental monitoring sensors
- gunshot detection sensors
- motion detection sensors
- IoT-based situational monitoring devices

Each field sensing device may include an embedded processing unit, a local memory buffer, and a communication interface configured to transmit event signals to the edge gateway devices.

In one embodiment, the event data generated by the field sensing devices may include both structured and unstructured data. The Structured data may include sensor identifier, timestamp, geographic coordinates, detected event category, and signal intensity or confidence score. The Unstructured data may include video frames, audio recordings, image snapshots, and free-text alerts generated by monitoring systems.

**Edge Gateway Devices**

In one embodiment, the edge gateway devices (104) are positioned between the field sensing infrastructure and the centralized command center server. Each edge gateway

device comprises a first hardware processor (116) and a first memory unit (118) configured to execute localized data processing operations.

The edge gateway devices perform preliminary preprocessing of sensor-generated data in order to reduce communication overhead and improve overall system responsiveness.

In one embodiment, the preprocessing operations include:

- filtering redundant or noisy sensor signals
- compressing data streams to reduce bandwidth consumption
- performing preliminary anomaly detection on incoming sensor data
- synchronizing timestamps across heterogeneous sensors
- normalizing geo-location information into standardized geographic coordinate formats

Filtering operations may remove duplicate or corrupted event records generated by overlapping sensors. Compression operations may encode video or metadata streams using standard compression protocols. Timestamp synchronization may be achieved using network time synchronization protocols such as Network Time Protocol (NTP) or Precision Time Protocol (PTP).

Geo-tag normalization may convert sensor-provided coordinates into standardized geographic information system (GIS) formats to enable consistent spatial processing within the command center server.

After preprocessing, the edge gateway devices generate **standardized event metadata** representing summarized event descriptors that can be efficiently transmitted to the centralized processing infrastructure.

**Secure Communication Network**

In one of embodiment, the processed event metadata generated by the edge gateway devices is transmitted through the secure communication network (106) to the command center server.

The secure communication network may include one or more of the following communication infrastructures:

- encrypted internet communication channels
- virtual private networks (VPN)
- private wireless communication networks
- secure 4G/5G communication links
- municipal fiber communication networks

In one embodiment, the communication channels implement encryption protocols such as Transport Layer Security (TLS) or Internet Protocol Security (IPsec) to ensure authenticated and tamper-resistant transmission of operational data.

The network may further employ message queuing or streaming protocols for reliable delivery of event metadata between system components.

**Command Center Server**

In one of embodiment, the command center server (108) forms the central intelligence processing component of the system. The command center server comprises a second hardware processor (120) and a second memory unit (122) configured to execute predictive analytics operations on the received event metadata.

The command center server is communicatively coupled to one or more databases (110) configured to store historical crime records, incident reports, patrol deployment logs, contextual environmental data, and system-generated prediction outputs.

Upon receiving event metadata from the edge gateway devices, the command center server performs a sequence of data processing operations.

First, the server performs data ingestion and normalization operations, including:

- de-duplication of redundant event records
- schema normalization across heterogeneous data sources
- timestamp alignment across multiple event streams
- geo-spatial indexing of event locations

Geo-spatial indexing may involve mapping incoming events to predefined spatial micro-zones within the monitored geographic region.

**Spatio-Temporal Representation**

After ingestion and normalization, the command center server transforms the unified dataset into structured spatio-temporal representations that can be processed by predictive intelligence models.

In one embodiment, the spatial domain of the monitored region is divided into micro-zones, each representing a predefined geographic grid cell. Event occurrences within each micro-zone are aggregated over discrete time intervals to generate geo-gridded time-series tensors.

Each tensor may represent spatial-temporal features such as:

- event frequency within the micro-zone
- temporal patterns of incidents
- sensor anomaly indicators
- contextual environmental variables

In addition to tensor representations, the system may construct relational entity graphs representing relationships between entities such as locations, incidents, infrastructure nodes, and temporal event sequences.

These structured representations enable efficient pattern recognition and predictive modeling.

**Hybrid Intelligence Processing Pipeline**

In one of embodiment, the command center server executes a hybrid intelligence processing pipeline stored in the second memory unit to generate predictive risk assessments.

The hybrid intelligence pipeline may combine multiple analytical techniques, including:

- statistical pattern analysis
- spatio-temporal machine learning models
- relational graph analysis
- probabilistic forecasting models

These models analyze historical incident patterns together with real-time sensor observations to estimate the likelihood of future crime events within specific geographic micro-zones and time windows.

The predictive output generated by the intelligence pipeline may include:

- predicted micro-zone of potential crime occurrence
- predicted time window of potential occurrence
- predicted crime category
- probability score representing likelihood of occurrence
- severity index representing potential impact level
- uncertainty bounds representing prediction confidence.

In one embodiment, the system further generates ranked contributing factors explaining the prediction outcome. These factors may identify key variables influencing the prediction, such as recent incident patterns, environmental conditions, or sensor-detected anomalies.

Based on the generated risk forecasts, the command center server computes constrained intervention recommendations for law-enforcement operations.

The recommendations may consider operational constraints including:

- available patrol resources
- jurisdiction boundaries
- patrol shift schedules
- response time thresholds
- traffic conditions
- predefined governance policies.

The system may generate optimized patrol deployment routes or preventive patrol assignments to mitigate predicted risks.

**Human-in-the-Loop Authorization**

The generated risk forecasts and intervention recommendations are presented at the operator terminals (112) within the command center.

Authorized personnel may review the predictive outputs, analyze contributing factors, and evaluate recommended interventions through interactive visualization interfaces.

In one embodiment, intervention instructions are transmitted to patrol mobile communication devices (114) only after receiving an approval signal generated through a human-in-the-loop authorization workflow executed at the operator terminals.

This approval workflow ensures that automated predictions remain subject to human oversight before operational actions are initiated.

**Outcome Feedback and Model Updating**

Following the deployment of intervention actions, the system collects outcome feedback including confirmed incidents, false alerts, patrol response times, and operational reports generated by field personnel.

The command center server may utilize this feedback to update model parameters and refine predictive accuracy through periodic retraining or incremental model updates.

The architecture described above provides several technical advantages including:

- reduction of network bandwidth usage through edge-level preprocessing
- improved system responsiveness through distributed computing architecture
- enhanced prediction accuracy through integration of multi-source data
- improved operational coordination through human-supervised intervention workflows.

**Hybrid Intelligence Engine**

In one embodiment, the command center server (108) implements a hybrid intelligence processing engine configured to generate predictive crime risk assessments using a combination of spatio-temporal data analysis, relational entity modeling, and probabilistic forecasting mechanisms. The hybrid intelligence processing engine is executed by the second hardware processor (120) using executable instructions stored in the second memory unit (122) and operates on structured representations generated from the event metadata received from the edge gateway devices (104).

The hybrid intelligence engine operates as a multi-stage processing pipeline designed to transform heterogeneous sensor observations and historical incident data into predictive risk forecasts for predefined geographic micro-zones.

**Data Preparation and Feature Construction**

Upon receiving the standardized event metadata, the command center server performs feature preparation operations to construct input variables suitable for predictive analysis.

The system aggregates events within predefined geographic micro-zones and discrete time intervals to generate a spatio-temporal representation of situational activity. Each micro-zone may correspond to a grid cell defined over the monitored geographic region.

For each micro-zone and time interval, the system constructs a feature vector that may include:

- incident frequency within the micro-zone
- temporal occurrence patterns of incidents
- environmental sensor indicators
- crowd density or mobility signals
- anomaly detection scores generated at the edge gateway devices
- contextual environmental variables such as weather or time-of-day indicators.

These features are organized into **geo-gridded time-series tensors** representing spatial and temporal patterns of activity within the monitored region.

In one embodiment, the tensor representation comprises three dimensions:

- spatial micro-zone index
- time window index
- feature vector dimension.

The resulting spatio-temporal tensor provides a structured representation of historical and real-time situational data that can be processed by predictive intelligence models.

**Relational Entity Graph Construction**

In addition to tensor-based representations, the system constructs relational entity graphs representing relationships between relevant entities associated with crime events.

Entities represented within the relational graph may include:

- geographic locations
- incident types
- temporal sequences of events
- infrastructure nodes
- patrol routes
- contextual environmental indicators.

Edges within the relational graph represent relationships such as spatial proximity, temporal adjacency, or similarity in event characteristics.

The relational graph enables the hybrid intelligence engine to analyze dependencies between events and identify correlated patterns across different geographic zones and time periods.

Graph representations may be stored in the databases (110) and accessed by the second hardware processor during predictive analysis.

**Spatio-Temporal Pattern Analysis**

In one embodiment, the hybrid intelligence engine performs pattern extraction operations on the spatio-temporal tensors to identify recurring patterns associated with crime occurrence.

In one embodiment, the second hardware processor executes spatio-temporal analysis models capable of detecting correlations between incident occurrences across neighboring micro-zones and adjacent time windows.

These models may include machine-learning or statistical models configured to learn spatial and temporal dependencies within historical crime data.

The pattern extraction process may identify:

- periodic crime occurrence trends
- spatial clustering of incidents
- correlations between environmental conditions and incident occurrence
- propagation patterns across adjacent micro-zones.

The extracted patterns form the basis for predictive risk estimation.

**Relational Dependency Modeling**

The relational entity graphs are analyzed to identify structural dependencies between entities associated with crime events.

Graph-based processing operations executed by the second hardware processor may evaluate the connectivity structure of the relational graph to determine how events in one location influence potential events in neighboring locations.

For example, the system may identify relationships such as:

- repeated incident sequences along transportation corridors
- correlated activity between adjacent geographic zones
- temporal chains of related incidents.

Graph analysis enables the hybrid intelligence engine to incorporate relational dependencies into predictive forecasting.

**Probabilistic Risk Forecasting**

Using the outputs of the spatio-temporal analysis and relational graph modeling stages, the hybrid intelligence engine performs **probabilistic forecasting** to estimate the likelihood of crime occurrence within each micro-zone.

In one embodiment, the system computes a probability score representing the estimated likelihood of an incident occurring within a specific micro-zone during a defined time window.

The probability score may be derived from predictive models trained using historical crime data combined with real-time sensor observations.

The predictive output generated by the hybrid intelligence engine may include:

- predicted micro-zone
- predicted time window
- predicted crime category
- probability score representing likelihood of occurrence
- severity index representing potential impact level
- uncertainty bounds representing prediction confidence.

The severity index may be derived from a weighted evaluation of crime categories, historical impact levels, and contextual situational indicators.

The uncertainty bounds may be computed based on the confidence distribution of the predictive model outputs.

**Explainability and Feature Attribution**

To improve transparency and operational usability, the hybrid intelligence engine generates explainability outputs that identify the most influential factors contributing to each risk forecast.

The explainability component may compute feature attribution scores representing the contribution of individual input features to the predicted risk score.

These contributing factors may include variables such as:

- recent incident activity within a micro-zone
- abnormal sensor readings detected by field devices
- temporal crime trends
- contextual environmental conditions.

The ranked contributing factors are presented to system operators through the operator terminals (112) to support informed decision-making.

**Intervention Recommendation Integration**

The outputs of the hybrid intelligence engine are provided as input to the intervention recommendation component executed by the command center server.

The intervention recommendation component evaluates the predicted risk forecasts together with operational constraints including:

- available patrol resources
- jurisdiction boundaries
- response-time thresholds
- patrol shift schedules
- traffic conditions.

Based on these constraints, the system generates recommended preventive actions, which may include patrol redeployment suggestions or targeted monitoring of specific micro-zones.

**Hardware Execution Environment**

The hybrid intelligence processing pipeline is executed by the second hardware processor (120) of the command center server using instructions stored in the second memory unit (122).

The command center server may comprise:

- multi-core processors configured for parallel data processing

- high-capacity system memory for storing spatio-temporal tensors and relational graphs
- network interfaces configured for real-time communication with edge gateway devices
- persistent storage systems for maintaining historical incident databases.

The processing operations performed by the hybrid intelligence engine therefore constitute hardware-implemented data processing operations performed on structured data representations rather than abstract algorithmic operations.

The hybrid intelligence engine described above enables the system to transform heterogeneous multi-source sensor data into structured predictive insights through hardware-implemented spatio-temporal and relational data processing.

This architecture provides several technical improvements including:

- efficient processing of large-scale sensor networks through distributed edge preprocessing
- structured transformation of real-time situational data into spatio-temporal tensors and relational graphs
- improved predictive capability through integration of spatial, temporal, and relational data dependencies
- reduced response latency through real-time risk forecasting and decision support.

These technical features enable the system to perform computer-implemented situational analysis and predictive forecasting using specialized data processing architecture, thereby providing a technological solution to real-time crime prediction and prevention.

**Spatio-Temporal Representation Engine**

In one embodiment, the command center server (108) further implements a spatio-temporal representation engine configured to transform heterogeneous event data received from the edge gateway devices (104) into structured data representations suitable for predictive analysis. The spatio-temporal representation engine is executed by the second hardware processor (120) using instructions stored in the second memory unit (122).

The purpose of the spatio-temporal representation engine is to convert incoming event metadata and contextual data streams into structured representations that capture spatial relationships, temporal evolution of events, and correlations among incident variables. These representations enable efficient processing by the hybrid intelligence processing pipeline described above.

**Spatial Micro-Zone Partitioning**

In one embodiment, the monitored geographic region is partitioned into a plurality of spatial micro-zones. Each micro-zone corresponds to a predefined geographic grid cell representing a limited physical area within the monitored environment.

The micro-zones may be defined using geographic coordinate boundaries derived from mapping systems such as geographic information systems (GIS). For example, a city map may be divided into grid cells representing areas such as street segments, blocks, or intersections.

Each incoming event received from the edge gateway devices is mapped to a corresponding micro-zone based on its geo-location coordinates. The mapping operation may involve comparing the latitude and longitude of the event location with the spatial boundaries of predefined grid cells stored in the databases (110).

This spatial partitioning enables the system to associate events with specific geographic regions and facilitates spatial pattern analysis.

**Temporal Windowing**

In addition to spatial partitioning, the spatio-temporal representation engine organizes events into temporal windows representing discrete time intervals.

Each temporal window may correspond to a predefined duration such as several minutes, hours, or other operationally relevant intervals. Events occurring within the same time interval are grouped together for analysis.

Temporal windowing enables the system to capture temporal dynamics of incident occurrences, including recurring patterns that may appear at particular times of day or during specific operational periods.

The combination of spatial micro-zones and temporal windows produces a spatio-temporal grid representing the monitored region across time.

**Geo-Gridded Time-Series Tensor Construction**

After spatial and temporal grouping of events, the spatio-temporal representation engine constructs geo-gridded time-series tensors representing the aggregated activity within each micro-zone over time.

In one embodiment, the tensor representation comprises multiple dimensions including:

- a spatial dimension representing the micro-zone index
- a temporal dimension representing discrete time windows
- a feature dimension representing situational indicators associated with each micro-zone.

The feature dimension may include variables such as:

- incident frequency within the micro-zone
- counts of specific event types
- anomaly indicators generated by edge gateway preprocessing
- environmental sensor measurements
- mobility indicators derived from sensor observations.

Each tensor element therefore represents the state of a particular geographic micro-zone at a specific time interval with respect to multiple situational features.

The tensor representation enables the hybrid intelligence engine to identify patterns across both spatial and temporal dimensions of the monitored region.

**Relational Entity Graph Generation**

In addition to tensor-based representations, the spatio-temporal representation engine generates relational entity graphs representing relationships among entities associated with crime events.

Entities represented in the relational graph may include:

- geographic locations or micro-zones
- incident categories
- infrastructure nodes such as transportation hubs
- temporal event sequences
- contextual environmental conditions.

Edges in the relational graph represent relationships between these entities. Examples of such relationships include:

- spatial proximity between neighboring micro-zones
- temporal adjacency between sequential incidents
- similarity relationships between incident types.

The relational entity graph enables the system to capture dependencies and correlations between events that may not be evident from spatial aggregation alone.

The relational graph structures may be stored in the databases (110) and accessed by the command center server during predictive analysis.

**Data Synchronization and Consistency Management**

The spatio-temporal representation engine further performs data synchronization operations to ensure consistency across heterogeneous data sources.

Events arriving from multiple edge gateway devices may exhibit variations in timestamps or coordinate formats. The engine therefore aligns timestamps across sensor streams and converts location information into a consistent geographic reference system.

These synchronization operations ensure that the spatial and temporal representations accurately reflect real-world event sequences.

**Data Storage and Retrieval**

The generated spatio-temporal tensors and relational entity graphs are stored within the databases (110) associated with the command center server. In one embodiment, the databases may include specialized storage mechanisms such as time-series databases, spatial databases, or graph databases configured to efficiently store and retrieve structured situational data.

These stored representations enable the hybrid intelligence engine to perform predictive analysis using both historical records and real-time event observations.

**Integration with Predictive Intelligence Processing**

In one embodiment, the spatio-temporal representations generated by the representation engine serve as input to the hybrid intelligence processing pipeline executed by the command center server.

By converting heterogeneous sensor data into structured spatial-temporal representations, the representation engine enables the predictive models to efficiently analyze patterns across geographic regions and time intervals.

This structured transformation of raw event data into geo-gridded tensors and relational graphs constitutes a technical data processing operation implemented by the command center server hardware, thereby enabling the predictive functionality of the real-time crime prediction and prevention system.

The spatio-temporal representation engine provides a technical mechanism for organizing large volumes of heterogeneous sensor data into structured representations that support efficient predictive analysis.

This transformation of distributed sensor observations into geo-gridded tensors and relational entity graphs improves the ability of the system to identify spatial and temporal correlations in incident data and enables real-time risk forecasting across monitored regions.

By performing these operations within the command center server hardware, the system achieves efficient processing of multi-source situational data and supports timely operational decision-making for crime prevention activities.

**Spatio-Temporal Representation Engine**

In one embodiment, the command center server (108) further implements a spatio-temporal representation engine configured to transform heterogeneous event data received from the edge gateway devices (104) into structured data representations suitable for predictive analysis. The spatio-temporal representation engine is executed by the second hardware processor (120) using instructions stored in the second memory unit (122).

The purpose of the spatio-temporal representation engine is to convert incoming event metadata and contextual data streams into structured representations that capture spatial relationships, temporal evolution of events, and correlations among incident variables. These representations enable efficient processing by the hybrid intelligence processing pipeline described above.

**Spatial Micro-Zone Partitioning**

In one embodiment, the monitored geographic region is partitioned into a plurality of spatial micro-zones. Each micro-zone corresponds to a predefined geographic grid cell representing a limited physical area within the monitored environment.

The micro-zones may be defined using geographic coordinate boundaries derived from mapping systems such as geographic information systems (GIS). For example, a city map may be divided into grid cells representing areas such as street segments, blocks, or intersections.

Each incoming event received from the edge gateway devices is mapped to a corresponding micro-zone based on its geo-location coordinates. The mapping operation may involve comparing the latitude and longitude of the event location with the spatial boundaries of predefined grid cells stored in the databases (110).

This spatial partitioning enables the system to associate events with specific geographic regions and facilitates spatial pattern analysis.

**Temporal Windowing**

In addition to spatial partitioning, the spatio-temporal representation engine organizes events into temporal windows representing discrete time intervals.

Each temporal window may correspond to a predefined duration such as several minutes, hours, or other operationally relevant intervals. Events occurring within the same time interval are grouped together for analysis.

Temporal windowing enables the system to capture temporal dynamics of incident occurrences, including recurring patterns that may appear at particular times of day or during specific operational periods.

The combination of spatial micro-zones and temporal windows produces a spatio-temporal grid representing the monitored region across time.

**Geo-Gridded Time-Series Tensor Construction**

After spatial and temporal grouping of events, the spatio-temporal representation engine constructs geo-gridded time-series tensors representing the aggregated activity within each micro-zone over time.

In one embodiment, the tensor representation comprises multiple dimensions including:

- a spatial dimension representing the micro-zone index
- a temporal dimension representing discrete time windows
- a feature dimension representing situational indicators associated with each micro-zone.

The feature dimension may include variables such as:

- incident frequency within the micro-zone
- counts of specific event types
- anomaly indicators generated by edge gateway preprocessing
- environmental sensor measurements
- mobility indicators derived from sensor observations.

Each tensor element therefore represents the state of a particular geographic micro-zone at a specific time interval with respect to multiple situational features.

The tensor representation enables the hybrid intelligence engine to identify patterns across both spatial and temporal dimensions of the monitored region.

**Relational Entity Graph Generation**

In addition to tensor-based representations, the spatio-temporal representation engine generates relational entity graphs representing relationships among entities associated with crime events.

Entities represented in the relational graph may include:

- geographic locations or micro-zones
- incident categories
- infrastructure nodes such as transportation hubs
- temporal event sequences
- contextual environmental conditions.

Edges in the relational graph represent relationships between these entities. Examples of such relationships include:

- spatial proximity between neighboring micro-zones

- temporal adjacency between sequential incidents
- similarity relationships between incident types.

The relational entity graph enables the system to capture dependencies and correlations between events that may not be evident from spatial aggregation alone.

The relational graph structures may be stored in the databases (110) and accessed by the command center server during predictive analysis.

**Data Synchronization and Consistency Management**

In one embodiment, the spatio-temporal representation engine further performs data synchronization operations to ensure consistency across heterogeneous data sources.

Events arriving from multiple edge gateway devices may exhibit variations in timestamps or coordinate formats. The engine therefore aligns timestamps across sensor streams and converts location information into a consistent geographic reference system.

These synchronization operations ensure that the spatial and temporal representations accurately reflect real-world event sequences.

**Data Storage and Retrieval**

In one embodiment, the generated spatio-temporal tensors and relational entity graphs are stored within the databases (110) associated with the command center server. In one embodiment, the databases may include specialized storage mechanisms such as time-series databases, spatial databases, or graph databases configured to efficiently store and retrieve structured situational data.

These stored representations enable the hybrid intelligence engine to perform predictive analysis using both historical records and real-time event observations.

**Integration with Predictive Intelligence Processing**

In one embodiment, the spatio-temporal representations generated by the representation engine serve as input to the hybrid intelligence processing pipeline executed by the command center server.

By converting heterogeneous sensor data into structured spatial-temporal representations, the representation engine enables the predictive models to efficiently analyze patterns across geographic regions and time intervals.

This structured transformation of raw event data into geo-gridded tensors and relational graphs constitutes a technical data processing operation implemented by the command center server hardware, thereby enabling the predictive functionality of the real-time crime prediction and prevention system.

The spatio-temporal representation engine provides a technical mechanism for organizing large volumes of heterogeneous sensor data into structured representations that support efficient predictive analysis.

This transformation of distributed sensor observations into geo-gridded tensors and relational entity graphs improves the ability of the system to identify spatial and temporal correlations in incident data and enables real-time risk forecasting across monitored regions.

By performing these operations within the command center server hardware, the system achieves efficient processing of multi-source situational data and supports timely operational decision-making for crime prevention activities.

**Technical Effects and Advantages of the Invention**

The real-time crime prediction and prevention system described herein provides several technical improvements in distributed situational monitoring and predictive decision-support systems used in public safety environments. These improvements arise from the integration of distributed sensing infrastructure, edge-level preprocessing, centralized predictive intelligence processing, and human-supervised intervention orchestration within a unified computing architecture.

**Reduction of Network Bandwidth Utilization**

One technical effect of the present invention arises from the use of edge gateway devices configured to perform localized preprocessing of raw sensor data before transmitting information to the command center server. By filtering redundant data, compressing sensor streams, and generating standardized event metadata, the edge gateway devices reduce the amount of raw multimedia data transmitted over the secure communication network.

This distributed preprocessing architecture significantly reduces network bandwidth requirements compared with conventional surveillance systems that transmit continuous raw video streams to central servers.

**Reduced Latency in Situational Analysis**

Another technical effect of the invention is the reduction of processing latency in real-time situational analysis. By combining edge-level preprocessing with centralized predictive intelligence processing executed by the command center server, the system enables rapid transformation of incoming sensor signals into actionable risk forecasts.

The ability to process event metadata in near real-time allows the system to identify emerging risk conditions within specific geographic micro-zones without requiring delayed batch processing of large historical datasets.

**Improved Spatial Granularity of Risk Forecasting**

In one embodiment, the present invention introduces a spatio-temporal representation mechanism that transforms heterogeneous event data into geo-gridded time-series tensors and relational entity graphs. This structured spatial representation enables the predictive intelligence engine to analyze incident patterns at a finer spatial resolution than conventional hotspot analysis systems.

As a result, the system can generate predictive risk assessments for small geographic micro-zones such as street segments or intersections, thereby enabling more precise identification of emerging risk locations.

**Enhanced Predictive Modeling Through Multi-Source Data Integration**

The present invention improves predictive analysis by integrating multiple heterogeneous data sources including:

- historical crime records
- sensor-generated situational signals
- patrol deployment logs
- environmental and contextual information.

The hybrid intelligence processing pipeline combines spatio-temporal analysis with relational dependency modeling to capture correlations across spatial regions and temporal sequences. This multi-source integration enables the system to detect emerging risk patterns that may not be observable when using a single data source.

**Improved Operational Resource Allocation**

The prevention and response orchestration engine described in the invention enables automated analysis of operational constraints and patrol resource availability when generating intervention recommendations.

By evaluating parameters such as patrol unit availability, jurisdiction boundaries, response-time constraints, and predicted risk severity, the system can recommend optimized patrol deployment strategies for mitigating potential crime events.

This capability improves the efficiency of resource utilization within law-enforcement operations and assists command personnel in prioritizing preventive actions.

**Enhanced Decision Transparency and Accountability**

The invention further provides an explainability layer that generates ranked contributing factors and confidence values corresponding to predictive risk forecasts. These explainability outputs allow command center personnel to understand the underlying factors influencing each prediction.

Providing such transparent reasoning information improves trust in predictive outputs and enables supervisory review and auditing of system decisions.

**Improved Operational Governance and Safety**

The system incorporates a human-in-the-loop authorization workflow that requires supervisory approval before intervention instructions are transmitted to patrol mobile communication devices.

This workflow ensures that predictive intelligence outputs remain subject to human oversight and prevents automated enforcement actions without supervisory verification.

**Continuous System Improvement Through Outcome Feedback**

The system further incorporates an outcome feedback loop that captures operational results including confirmed incidents, false alerts, and patrol response metrics.

These outcome records are used to update predictive models and refine future risk forecasts, thereby enabling continuous improvement of system accuracy over time.

By combining distributed sensor data acquisition, edge-level preprocessing, centralized predictive intelligence processing, and policy-governed intervention orchestration within a unified computing architecture, the present invention provides a technological improvement in real-time situational analysis and decision-support systems used for crime prevention operations.

The invention therefore enables more efficient processing of multi-source situational data, more accurate identification of emerging risk patterns, and improved coordination of preventive operational responses.

In certain embodiments of the present invention, additional operational features may be implemented within the system architecture described above in order to enhance data processing efficiency, predictive accuracy, and operational decision support.

In one embodiment, the edge gateway devices (104) are configured to selectively transmit information to the command center server based on anomaly detection results

generated during localized preprocessing. When the anomaly score associated with incoming sensor data remains below a predefined anomaly threshold, the edge gateway device transmits only compact event metadata representing the detected observation. However, when the anomaly score exceeds the predefined threshold, the edge gateway device additionally transmits corresponding raw media segments, such as video frames or audio samples, to the command center server for further analysis. This conditional transmission mechanism reduces network bandwidth consumption while ensuring that critical situational data is available for centralized intelligence processing.

In another embodiment, the command center server (108) assigns confidence weights to heterogeneous data sources when processing incoming event records. The confidence weights may be determined based on factors including historical reliability of sensors, reporting accuracy, signal quality indicators, or prior error rates associated with particular data sources. When multiple event records corresponding to similar observations are received from different sensors or reporting channels, the command center server performs conflict resolution operations using timestamp reconciliation and geo-spatial clustering techniques to determine whether the records correspond to a single underlying event.

In a further embodiment, the hybrid intelligence processing pipeline executed by the second hardware processor (120) comprises multiple complementary processing components including a non-linear pattern extraction component, a relational dependency modeling component, and a probabilistic forecasting component. The non-linear pattern extraction component analyzes spatio-temporal tensors to detect complex correlations between incident variables, while the relational dependency modeling component analyzes entity graphs representing relationships among locations, incidents, and contextual indicators. The probabilistic forecasting component estimates the likelihood of potential crime events occurring within specific geographic micro-zones and time windows.

In certain embodiments, the command center server continuously monitors statistical characteristics of incoming event data streams to detect distribution shifts or changes

in underlying crime patterns. When significant statistical deviations from baseline data distributions are detected, the system initiates controlled model recalibration procedures to update predictive models using newly observed data. Model parameters associated with each version of the predictive models may be stored within the databases (110), thereby enabling version tracking, auditing, and rollback to previously validated model configurations when necessary.

In another embodiment, the system implements governance controls to protect sensitive information contained in incident records or sensor data. Sensitive identifiers associated with individuals, vehicles, or locations may be protected through masking or tokenization techniques prior to inclusion in model training datasets. Tokenization replaces identifiable attributes with surrogate tokens while preserving relational consistency within the dataset.

In one embodiment, the prevention and response orchestration engine generates multiple candidate intervention scenarios corresponding to different patrol deployment strategies. Each intervention scenario may be evaluated according to estimated operational resource costs including patrol travel distance, personnel allocation, and estimated response time. Additionally, each scenario may be assigned a predicted impact score representing the expected effectiveness of the intervention in reducing crime risk. The intervention scenarios are ranked according to these evaluation metrics before being presented to authorized personnel at the operator terminals (112).

In certain embodiments, the spatio-temporal representation engine partitions the monitored geographic region into spatial micro-zones at street-level granularity, such as road segments, blocks, or intersections. This fine-grained spatial representation enables the predictive intelligence engine to analyze situational patterns at a detailed geographic scale and improves the accuracy of localized risk forecasts.

In another embodiment, the operator terminals (112) provide graphical visualization interfaces configured to display dynamic risk heatmaps representing predicted crime probability across geographic micro-zones. The heatmaps may include visual indicators representing prediction confidence intervals and ranked contributing factors

generated by the predictive intelligence engine. These visualizations assist command personnel in interpreting risk forecasts and evaluating recommended intervention strategies.

In certain embodiments, the system further computes performance metrics associated with predictive forecasting and operational outcomes. Such metrics may include predictive precision, recall, false-positive rates, and response-time improvement indicators derived from comparisons between predicted events and confirmed incident outcomes. These performance metrics may be stored within the databases (110) and used to evaluate system performance and guide model updates.

The present invention, titled “Artificial Super-Intelligence (ASI) Based Crime Prediction and Prevention System”, relates to a computer-implemented, network-enabled public safety intelligence platform that predicts the probability, location, time window, and potential severity of criminal events and further generates prevention and response recommendations under configurable governance constraints. The invention is deployable as a centralized cloud system, an on-premises command-and-control system, or a hybrid configuration. It interfaces with law-enforcement information systems, emergency response systems, surveillance infrastructure, IoT devices, and authorized third-party data sources to provide near real-time operational support.

In one embodiment, the invention comprises a Data Ingestion and Integration Layer configured to receive multi-source inputs including, but not limited to, historical crime records, FIR/case metadata, emergency call/dispatch logs, patrol beat logs, GPS traces of response units, traffic data, public event schedules, weather feeds, CCTV metadata, sensor alerts, and citizen-generated tips. The ingestion layer includes connectors, APIs, streaming brokers, and batch pipelines to collect data at different velocities. The ingestion layer further performs validation, timestamp alignment, geo-tag normalization, de-duplication, and standardization into a unified schema so that

heterogeneous data becomes comparable and processable in a single analytics workflow.

In another embodiment, the invention includes a Privacy, Security, and Governance Module coupled to the ingestion pipeline. This module enforces role-based access control, encryption for data in transit and at rest, secure key management, audit logging, and configurable data retention. Where legally required, the module applies data minimization, masking, tokenization, or anonymization to sensitive identifiers before they are used for model training or inference. The governance module can enforce policy rules such as restricting the use of protected attributes, limiting individualized scoring, and allowing only aggregated risk outputs depending on jurisdictional regulations and departmental standard operating procedures.

In another embodiment, the invention provides a Unified Spatio-Temporal Knowledge Representation Engine that converts ingested data into structured representations suitable for ASI-based reasoning. This engine generates (i) geo-gridded time-series tensors for hotspot and trend learning, (ii) event sequences for temporal forecasting, and (iii) a relational graph connecting entities such as locations, incident types, modus operandi patterns, time windows, infrastructure points (e.g., transit hubs, schools, ATMs), and known risk indicators. The representation engine may assign confidence weights to different sources, resolve conflicts between sources, and create a continuously updated "situational context state" for each micro-region within the monitored jurisdiction.

In a further embodiment, the invention comprises an ASI-based Hybrid Intelligence Core configured to perform forecasting and reasoning using multiple complementary model families. The intelligence core can include ensemble learning models for structured data, deep neural networks for complex non-linear interactions, and graph-based reasoning models to learn relational dependencies across connected entities. The intelligence core outputs one or more risk forecasts including: predicted crime category, probability score, predicted time window, predicted spatial unit (micro-zone), severity index, and uncertainty bounds. The system can optionally generate multiple

scenario forecasts (best-case, expected, worst-case) to support planning under uncertainty.

In another embodiment, the invention includes an Adaptive Learning and Drift Management Module. This module monitors prediction performance, data distribution shifts, and operational feedback to detect model drift. Upon detecting drift, the module initiates controlled recalibration using incremental learning, scheduled retraining, or selective model replacement while preserving stability for field operations. The module maintains versioning of models, records training datasets and parameters, and supports rollback to earlier versions if required by governance policy. This ensures the system remains reliable over time despite changes in crime patterns, reporting behavior, or environmental conditions.

In another embodiment, the invention further includes an Explainability and Auditability Layer that generates interpretable outputs for decision-makers. For each risk forecast, the layer provides ranked contributing factors such as recent incident clustering, anomalous mobility signatures, event crowd indicators, weather triggers, repeated modus operandi patterns, or sensor corroborations. It generates confidence values and uncertainty measures and logs the reasoning trace, input data references (as permitted), and model version used. This enables supervisors and auditors to review why a forecast was produced, supports accountability, and improves adoption by frontline personnel.

In a further embodiment, the invention provides a Prevention and Response Orchestration Engine that transforms forecasts into actionable recommendations. The orchestration engine may generate optimized patrol deployment plans, route suggestions, dynamic staging points, targeted alerts to nearby units, surveillance focus region activation, coordination prompts to traffic control or emergency medical teams, and community advisory triggers. Recommendations are computed under constraints including available manpower, response time objectives, patrol shift schedules, jurisdiction boundaries, priority rules, and proportionality limits. The engine can output

multiple ranked intervention options, each with expected effectiveness and resource cost estimates.

In another embodiment, the invention includes a Human-in-the-Loop Command Workflow integrated with a dashboard or command center interface. The workflow allows authorized personnel to review forecasts, examine contributing factors, adjust parameters (risk thresholds, time windows, crime categories), approve or reject recommended interventions, and generate operational tasks. The system can support escalation protocols whereby high-severity risk forecasts trigger supervisor approval requirements, multi-agency notification, or additional corroboration checks before any action is initiated. This ensures the invention functions as decision support rather than uncontrolled automation.

In a further embodiment, the invention comprises an Outcome Feedback and Effectiveness Measurement Loop that collects post-action results including confirmed incidents, false positives, false negatives, response times, patrol coverage data, officer annotations, and community feedback. The system computes performance metrics such as precision, recall, lead-time gained, incident reduction indicators, and resource utilization improvement. These measured outcomes are fed back into the learning pipeline to improve future forecasting accuracy and to quantify operational impact. The feedback loop enables continuous improvement while preserving governance controls and traceability.

Finally, the invention supports scalable deployment and interoperability through modular microservices, standardized APIs, and configurable data connectors. It can be adapted to different city sizes, rural deployments, and infrastructure conditions by adjusting spatial granularity, model complexity, and available input sources. The system can operate with partial data availability by applying confidence weighting and uncertainty reporting, thereby ensuring it remains useful even when some sensors or feeds are unavailable. Accordingly, the present invention provides an integrated, adaptive, explainable, and policy-governed ASI-based framework that improves crime

prediction accuracy and enables measurable crime prevention and response effectiveness.

**FIG. 2** illustrates an Artificial Superintelligence (ASI) based real-time crime prediction and prevention system, according to an embodiment of the present invention.

The figure shows the end-to-end working of an Artificial Super-Intelligence (ASI) Based Crime Prediction and Prevention System, starting from multi-source data collection and ending in field-level preventive actions, with governance and continuous learning built in as feedback loops. On the left, the Data Sources block represents all incoming inputs used to understand the public-safety situation. These include Crime Records (historical incidents/FIR summaries), Emergency Calls (112/911 call logs and dispatch tickets), CCTV/IoT Feeds (camera analytics, intrusion sensors, gunshot sensors, etc.), GPS/Patrol Data (vehicle/beat tracking and patrol coverage), Social Media (public alerts, crowd reports, open-source intelligence signals), and Weather & Events (festival calendars, large gatherings, rainfall/temperature, etc.). These diverse signals help the system detect patterns that are not visible in historical crime logs alone.

All incoming signals flow into the Data Ingestion & Integration Layer, which acts as the central "collection and standardization" stage. Here, data is cleaned, de-duplicated, time-synchronized, geo-tagged, and converted into a common format so that different sources can be analyzed together. This layer may also create real-time streams and structured datasets suitable for forecasting and decision-making. The Privacy & Security Module supports the ingestion pipeline by enforcing protection controls such as encryption, access permissions, masking/tokenization of sensitive identifiers (when required), and secure audit logging. In the diagram, this module connects into the pipeline so that only authorized, policy-compliant data is allowed to move forward for intelligence processing.

At the base, the Governance & Compliance Module provides system-wide rules that constrain how data and outputs are handled. It defines permissible use policies, retention rules, fairness/bias checks (if configured), and operational constraints such as jurisdiction boundaries and escalation procedures. In the diagram, it connects across the architecture to ensure every stage (ingestion, intelligence, recommendations, and learning updates) follows configured governance requirements. The core of the system is the ASI Hybrid Intelligence Core. This is where the system performs multi-model forecasting (combining more than one predictive model), graph & deep learning (learning relationships among places, events, and entities), and drift detection & adaptation (detecting when crime patterns change over time and updating models safely). The output from this core is a risk forecast: likely location/micro-zone, time window, crime category (if applicable), risk score, and confidence/uncertainty.

The forecast then passes through the Explainability & Audit Layer, which converts model outputs into human-understandable reasoning. This layer produces the "why" behind each alert—such as major contributing factors, confidence scores, and traceable logs of model version and input evidence categories. This supports trust, supervision review, and auditability for compliance and accountability.

Next, the Prevention & Response Orchestration Engine converts intelligence into action options. According to the diagram, it supports patrol optimization, alert generation, resource allocation, and action recommendations. Practically, it can propose where to deploy units, which routes to follow, which hotspots need surveillance focus, and what coordination is required with emergency services or control rooms—while obeying the governance constraints. The Human-In-The-Loop Interface is the operational control point for officers/supervisors. Instead of fully automatic enforcement, this interface enables authorized users to review predictions, verify explanations, approve or modify recommended actions, and initiate operational tasks. This reduces inappropriate automation and ensures decisions remain accountable to the command structure and standard procedures.

Finally, the Outcome Feedback & Learning Loop captures real-world results such as incident confirmations, false alerts, response effectiveness, and performance metrics. These outcomes are used to generate model updates and operational tuning, which then feed back (through governance control) into the intelligence core and system configuration. This closes the loop so the system improves over time based on measurable field outcomes rather than remaining a static prediction tool.

**FIG. 3** illustrates an Artificial Superintelligence (ASI) based real-time crime prediction and prevention system, according to an exemplary embodiment of the present invention. The hardware block diagram presents the physical/deployment view of the ASI-based crime prediction and prevention system, showing how field devices, communication networks, and command-center infrastructure connect to deliver real-time alerts and operational intelligence. At the left side, the CCTV / IoT Sensors block represents the on-ground sensing infrastructure deployed across streets, public buildings, markets, transport hubs, and sensitive zones. This includes CCTV cameras and multiple IoT sensors such as gunshot detectors and environmental sensors (which may detect smoke, unusual sound patterns, temperature anomalies, or other contextual triggers). These devices continuously capture situational signals that can indicate abnormal events, suspicious activity, or risk escalation.

Below the sensors, the Edge Gateways are shown as intermediary hardware units. Their purpose is to collect data from nearby sensors and cameras, perform basic processing (such as filtering, compression, time-stamping, formatting), and securely transmit the relevant data onward. Edge gateways also reduce bandwidth load by forwarding only necessary event metadata or prioritized streams, and they help maintain local connectivity when sensors use different communication protocols.

At the center of the diagram, the Secure Communication Network is the backbone that connects edge gateways, command center servers, databases, and field devices. It typically includes secured internet/VPN links, leased lines, private LTE/5G networks, or encrypted radio/IP communication. The padlock icons in the diagram indicate protected transmission using encryption and access control so that sensitive law-enforcement information is not intercepted or tampered with.

The Command Center Server is the central computing infrastructure (on-premises server rack or cloud-hosted system) where the main analytics, ASI intelligence processing, alert generation, and coordination logic run. It receives fused data from sensors and edge gateways via the secure network, executes crime risk prediction and prevention logic, and then distributes outputs (alerts, risk maps, recommendations) to operator terminals and patrol units. This server also coordinates the overall workflow such as logging, model updates, and integration with other police IT systems.

Connected to the secure network are the Databases, which store both historical and real-time records. This includes crime history, incident tickets, dispatch logs, geo-maps, sensor event logs, and model outputs. These databases support training and refinement of prediction models, enable retrieval of past patterns for comparison, and maintain audit trails for compliance and accountability. On the right side, the Operator Terminals represent the control room interface used by analysts and supervising officers. These terminals display live maps, threat alerts, predicted hotspots, resource availability, and recommended actions. Operators can validate alerts, monitor multiple zones simultaneously, coordinate dispatch, and initiate escalation when required. This is the main human decision and monitoring point in the physical deployment.

At the bottom right, the Patrol Vehicle block represents police vehicles equipped with onboard terminals or rugged tablets that receive real-time alerts and navigation guidance. These devices can show hotspot routes, target locations, and incident details,

helping patrol teams respond faster and position themselves strategically to prevent crimes rather than only reacting after incidents occur.

Finally, the Patrol Mobile Devices block represents handheld devices used by field officers (smartphones, tablets, radios with data capability). These devices receive alerts, task assignments, and location-based instructions from the command center through the secure network. Officers can also send feedback, confirmations, photos, and incident updates back to the command center, supporting continuous situational awareness and closing the operational loop.

Overall, the diagram demonstrates a complete physical deployment architecture where field sensors and gateways feed secure data to a command center server and databases, and then intelligence outputs are delivered to operator terminals and patrol teams in real time for prevention and rapid response.

**FIG. 4** illustractes a logic layer architecture of an Artificial Superintelligence (ASI) based real-time crime prediction and prevention system, according to an embodiment of the present invention.

**FIG. 5** illustractes a loop approval workflow for an Artificial Superintelligence (ASI) based real-time crime prediction and prevention system, according to an embodiment of the present invention.

**FIG. 6A and 6B** illustractes computer-implemented method for real-time crime prediction and prevention executed by at least one edge gateway device and at least one command center server, according to an embodiment of the present invention. At step 602, the method comprises receiving, by a first hardware processor of the edge gateway device, raw event data streams from a plurality of field sensing devices.

At step 604, the method comprises performing, by the first hardware processor, localized preprocessing including filtering, compression, anomaly detection, timestamp synchronization, and geo-tag normalization.

At step 606, the method comprises generating standardized event metadata corresponding to detected events.

At step 608, the method comprises transmitting the standardized event metadata, without transmitting full raw media streams unless a predefined anomaly threshold is exceeded, over a secure communication network to the command center server.

At step 610, the method comprises receiving, by a second hardware processor of the command center server, the standardized event metadata and additional structured and unstructured data including historical crime records, patrol deployment logs, mobility traces, and contextual environmental inputs.

At step 612, the method comprises performing de-duplication, schema normalization, timestamp alignment, and geo-spatial indexing to generate a unified dataset.

At step 614, the method comprises transforming the unified dataset into: geo-gridded time-series tensors representing predefined micro-zones within a monitored jurisdiction; and relational entity graphs representing associations among locations, incident categories, temporal cycles, infrastructure nodes, and mobility patterns;

At step 616, the method comprises executing, by the second hardware processor, a hybrid intelligence processing pipeline stored in memory unit to generate a risk forecast including predicted micro-zone, predicted time window, predicted crime category, probability score, severity index, and uncertainty bound.

At step 618, the method comprises generating ranked contributing factors and confidence values corresponding to the risk forecast.

At step 620, the method comprises computing constrained intervention recommendations based on available patrol resources, jurisdiction boundaries, patrol shift schedules, response-time thresholds, traffic conditions, and governance policies.

At step 622, the method comprises presenting the risk forecast and intervention recommendations at operator terminals.

At step 624, the method comprises receiving an approval signal generated through a human-in-the-loop authorization workflow executed at the operator terminals.

At step 626, the method comprises transmitting intervention instructions from the command center server to patrol mobile communication devices only upon receipt of the approval signal.

At step 628, the method comprises updating model parameters based on outcome feedback including confirmed incidents, false alerts, and response metrics.

The present invention provides following advantages:

1. Proactive prevention (not just reporting): Predicts likely crime risks in advance so authorities can act before incidents occur.
2. Real-time intelligence: Updates risk levels continuously using live data streams (calls, CCTV/IoT, patrol GPS, etc.).
3. Higher prediction accuracy: Uses multi-source fusion and advanced learning to reduce false alarms compared to single-data models.
4. Fine-grained hotspot detection: Produces micro-zone (street/block/ward) risk maps instead of broad area-level forecasts.
5. Explainable decisions: Provides reasons, key contributing factors, and confidence scores to support trust and auditing.
6. Optimized resource deployment: Suggests best patrol allocation, routing, and resource staging to reduce manpower wastage.
7. Faster response time: Generates early alerts and situational recommendations, helping units respond quickly.
8. Adaptive to changing crime patterns: Detects trend shifts (concept drift) and self-updates models to stay effective over time.
9. Supports coordinated multi-agency action: Enables collaboration among police, emergency response, traffic, municipal services, and security teams.
10. Built-in bias/fairness monitoring: Helps reduce discriminatory outcomes through fairness constraints and periodic audits.

11. Privacy and security protection: Supports anonymization/masking, strong access control, encryption, and complete logging.
12. Measurable impact tracking: Captures outcomes and produces dashboards (precision, recall, reduction in incidents, response improvement).
13. Scalable and modular design: Can be deployed city-wise, state-wise, or nationwide with plug-and-play data connectors.
14. Supports both urban and rural policing: Learns local patterns and can adapt to different population densities and infrastructures.

The foregoing description describes embodiments of the present invention. It should be appreciated that these embodiments are described for the purpose of illustration only, and that numerous alterations and modifications may be practiced by those skilled in the art without departing from the scope of the invention. It is intended that all such modifications and alterations be included in so far as they come within the scope of the invention as claimed or the equivalents thereof.

**We claim:**

1. A real-time crime prediction and prevention system (100), comprising:

a plurality of field sensing devices (102) configured to generate structured and unstructured event data streams;

one or more edge gateway devices (104) operatively coupled to the field sensing devices (102), each edge gateway device comprising:

a first hardware processor (116), and

a first memory unit (118) storing executable instructions that, when executed by the first hardware processor (116), cause the edge gateway device to:

receive raw event data streams from the field sensing devices (102),

perform filtering, compression, anomaly detection, timestamp synchronization, and geo-tag normalization,

generate standardized event metadata, and

transmit the standardized event metadata over a secure communication network (106);

the secure communication network (106) configured to provide encrypted and authenticated data transmission;

at least one command center server (108) communicatively coupled to the secure communication network (106), the command center server (108) comprising:

a second hardware processor (120), and

a second memory unit (122) storing executable instructions that, when executed by the second hardware processor (120), cause the command center server (108) to:

ingest the standardized event metadata and additional structured and unstructured data including historical crime records, patrol logs, mobility data, and contextual inputs,

perform de-duplication, normalization, timestamp alignment, and geo-spatial indexing,

transform the ingested data into geo-gridded time-series tensors and relational entity graphs representing micro-zones,

execute a hybrid intelligence processing pipeline stored in the second memory unit to generate a risk forecast including predicted micro-zone, predicted time window, predicted crime category, probability score, severity index, and uncertainty bound,

generate ranked contributing factors and confidence values corresponding to the risk forecast,

compute constrained intervention recommendations based on patrol resources, jurisdiction boundaries, response-time thresholds, and governance policies,

enforce governance controls including role-based access control and audit logging, and

update model parameters using outcome feedback including confirmed incidents and response metrics;

one or more databases (110) operatively coupled to the command center server (108); and

operator terminals (112) and patrol mobile communication devices (114) communicatively coupled to the command center server (108),

wherein the second hardware processor is configured to transmit intervention instructions from the command center server (108) to the patrol mobile communication devices (114) only upon receipt of an approval signal generated through the human-in-the-loop authorization workflow executed at the operator terminals (112).

2. The system as claimed in claim 1, wherein the first hardware processor of the edge gateway device is configured to transmit only event metadata when no anomaly threshold is exceeded and to transmit corresponding raw media segments when the anomaly threshold is exceeded.

3. The system as claimed in claim 1, wherein the second hardware processor is configured to assign confidence weights to heterogeneous data sources and resolve conflicting event records using timestamp reconciliation and geo-spatial clustering.
4. The system as claimed in claim 1, wherein the hybrid intelligence processing pipeline comprises a non-linear pattern extraction component, a relational dependency modeling component, and a probabilistic forecasting component, executed by the second hardware processor.
5. The system as claimed in claim 1, wherein the second hardware processor is configured to detect statistical distribution shifts in incoming data streams and initiate controlled model recalibration while maintaining versioned model parameters in the databases (110).
6. The system as claimed in claim 1, wherein the governance controls include masking or tokenization of sensitive identifiers prior to inclusion in model training datasets.
7. The system as claimed in claim 1, wherein the second hardware processor computes multiple ranked intervention scenarios with corresponding estimated resource costs and predicted impact scores prior to presenting the intervention recommendations at the operator terminals (112).
8. The system as claimed in claim 1, wherein the geo-gridded time-series tensors represent predefined micro-zones at street-level granularity within the monitored jurisdiction.
9. The system as claimed in claim 1, wherein the operator terminals (112) are configured to display dynamic risk heatmaps with associated confidence intervals and contributing factor rankings.
10. The system as claimed in claim 1, wherein the second hardware processor computes performance metrics including precision, recall, and response-time improvement indicators and stores the performance metrics in the databases (110).
11. A computer-implemented method for real-time crime prediction and prevention executed by at least one edge gateway device and at least one command center server, the method comprising:

receiving, by a first hardware processor of the edge gateway device, raw event data streams from a plurality of field sensing devices;

performing, by the first hardware processor, localized preprocessing including filtering, compression, anomaly detection, timestamp synchronization, and geo-tag normalization;

generating standardized event metadata corresponding to detected events; and

transmitting the standardized event metadata, without transmitting full raw media streams unless a predefined anomaly threshold is exceeded, over a secure communication network to the command center server;

receiving, by a second hardware processor of the command center server, the standardized event metadata and additional structured and unstructured data including historical crime records, patrol deployment logs, mobility traces, and contextual environmental inputs;

performing de-duplication, schema normalization, timestamp alignment, and geo-spatial indexing to generate a unified dataset;

transforming the unified dataset into:

geo-gridded time-series tensors representing predefined micro-zones within a monitored jurisdiction; and

relational entity graphs representing associations among locations, incident categories, temporal cycles, infrastructure nodes, and mobility patterns;

executing, by the second hardware processor, a hybrid intelligence processing pipeline stored in memory unit to generate a risk forecast including predicted micro-zone, predicted time window, predicted crime category, probability score, severity index, and uncertainty bound;

generating ranked contributing factors and confidence values corresponding to the risk forecast;

computing constrained intervention recommendations based on available patrol resources, jurisdiction boundaries, patrol shift schedules, response-time thresholds, traffic conditions, and governance policies;

presenting the risk forecast and intervention recommendations at operator terminals;

receiving an approval signal generated through a human-in-the-loop authorization workflow executed at the operator terminals; and

transmitting intervention instructions from the command center server to patrol mobile communication devices only upon receipt of the approval signal;

updating model parameters based on outcome feedback including confirmed incidents, false alerts, and response metrics.

12. The method as claimed in claim 11, wherein performing localized preprocessing further includes selectively transmitting raw media segments only when anomaly scores exceed a predefined threshold.

13. The method as claimed in claim 11, wherein executing the hybrid intelligence processing pipeline further comprises assigning confidence weights to heterogeneous data sources and resolving conflicting records using geo-spatial clustering.

14. The method as claimed in claim 11, wherein computing constrained intervention recommendations further comprises generating multiple ranked intervention scenarios with corresponding resource cost estimates prior to presenting the recommendations at the operator terminals.

15. The method as claimed in claim 11, wherein updating model parameters further comprises detecting statistical divergence between real-time input data and baseline training data and initiating incremental recalibration while maintaining versioned model parameters.

Dated this 18th day of March 2026

Signature

-Digitally Signed-
Anuradha Gupta
Patent Agent (IN/PA-1514)
Agent for the Applicant

## ABSTRACT

### ARTIFICIAL SUPER-INTELLIGENCE (ASI) BASED CRIME PREDICTION AND PREVENTION SYSTEMS

The present invention discloses an Artificial Superintelligence (ASI) based a real-time crime prediction and prevention system (100) and its method. The system (100) comprises a plurality of field sensing devices (102), edge gateway devices (104), a secure communication network (106), command center server (108), databases (110), operator terminals (112) and patrol mobile communication devices (114). The plurality of field sensing devices (102) is configured to generate structured and unstructured event data streams. The one or more edge gateway devices (104) is operatively coupled to the field sensing devices (102). The secure communication network (106) is configured to provide encrypted and authenticated data transmission. The command center server (108) is communicatively coupled to the secure communication network (106). The databases (110) are operatively coupled to the command center server (108). The operator terminals (112) and patrol mobile communication devices (114) are communicatively coupled to the command center server (108).

**FIG. 1**

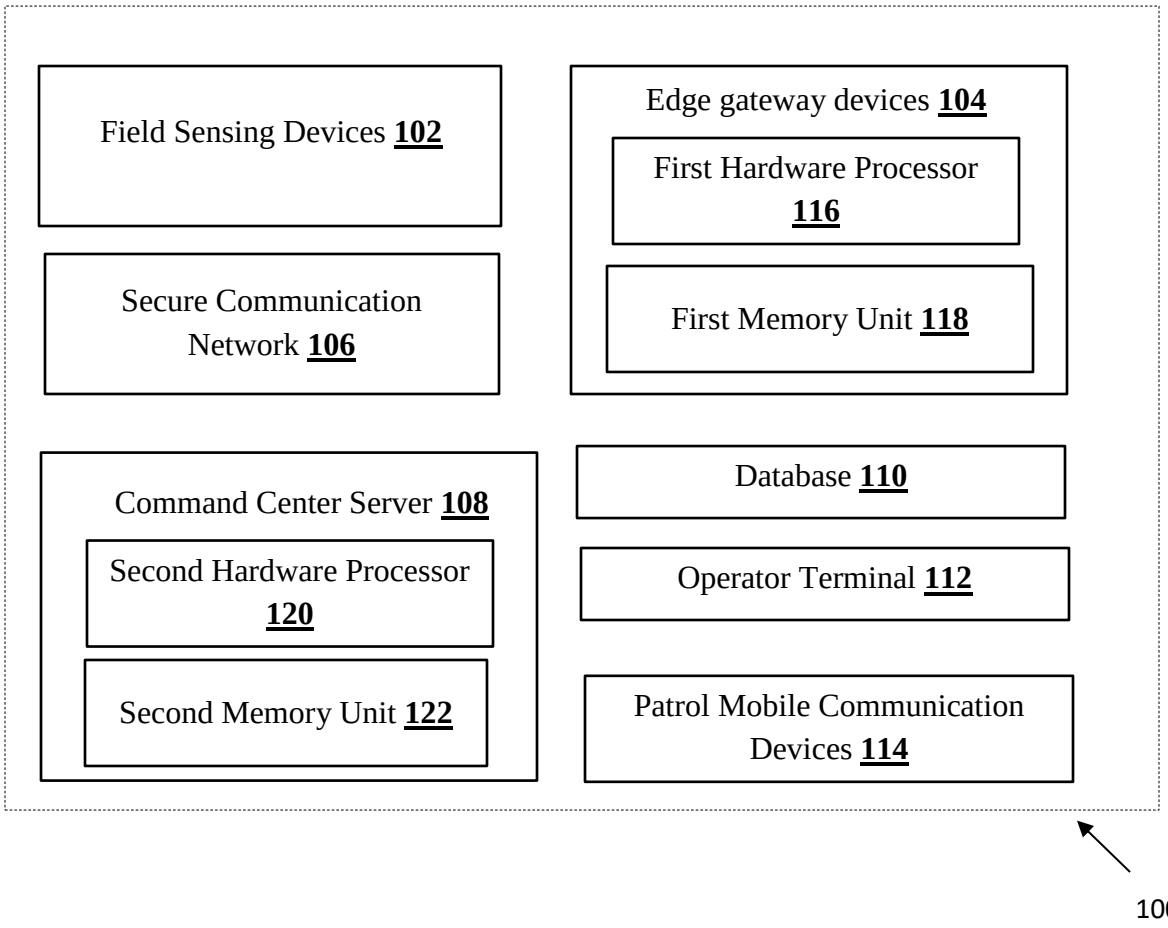


**FIG. 1**

-Digitally Signed-
ANURADHA GUPTA
Patent Agent (IN/PA-1514)
Agent for the applicant


**FIG. 2**

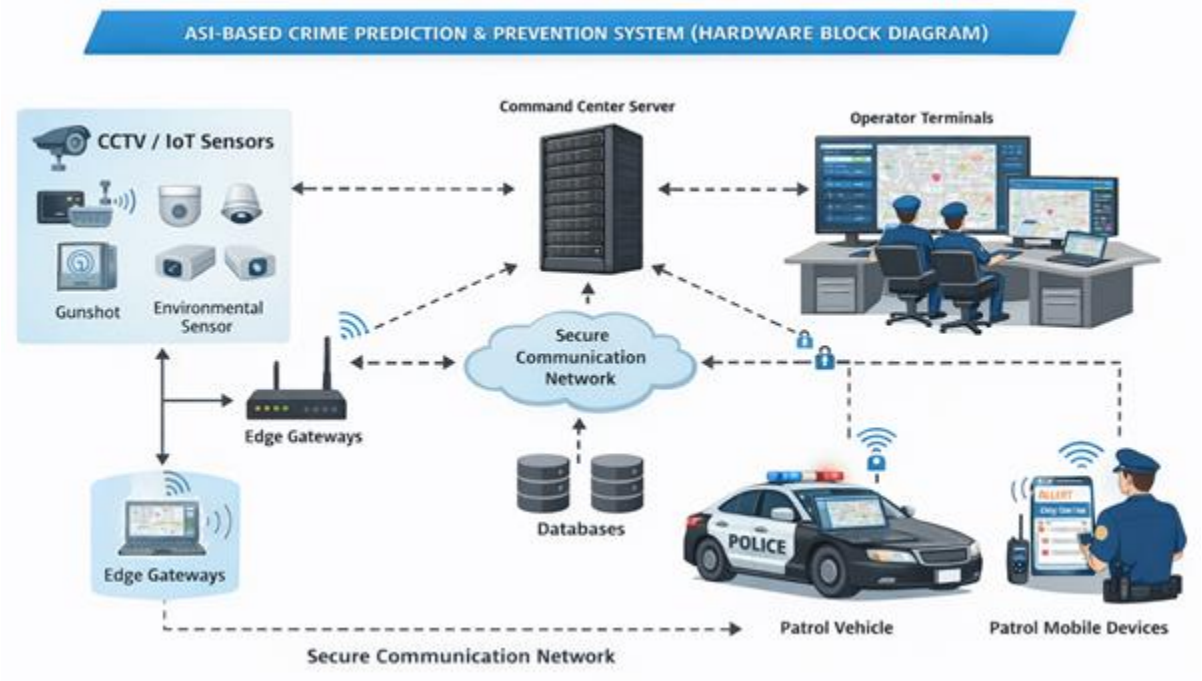


**FIG. 3**

-Digitally Signed-
ANURADHA GUPTA
Patent Agent (IN/PA-1514)
Agent for the applicant

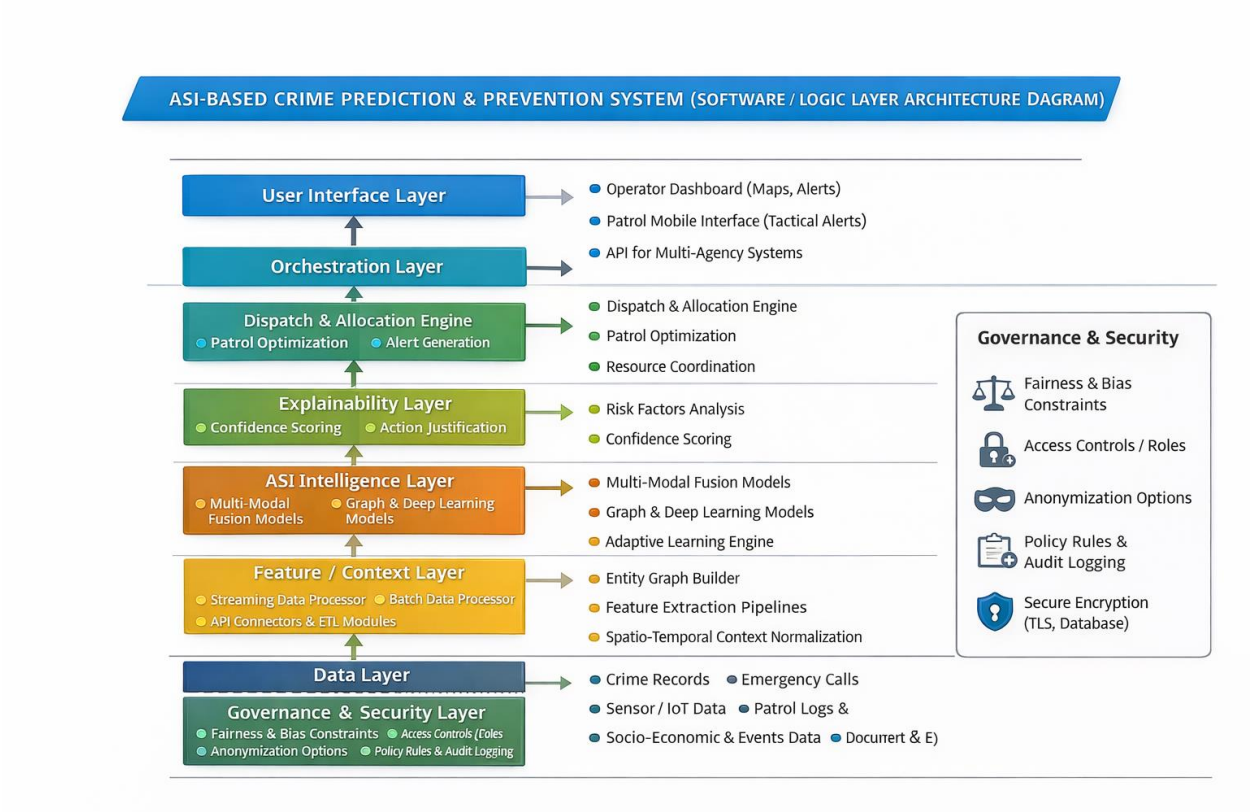


**FIG. 4**

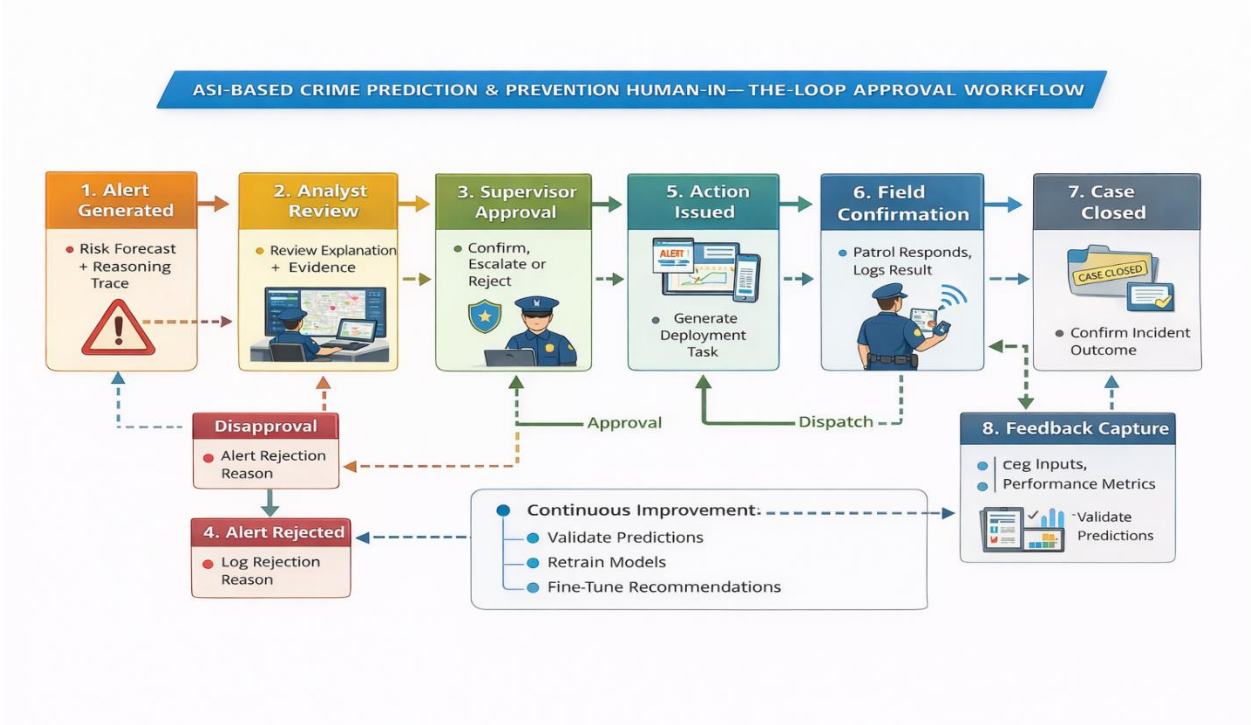


**FIG. 5**

-Digitally Signed-
ANURADHA GUPTA
Patent Agent (IN/PA-1514)
Agent for the applicant

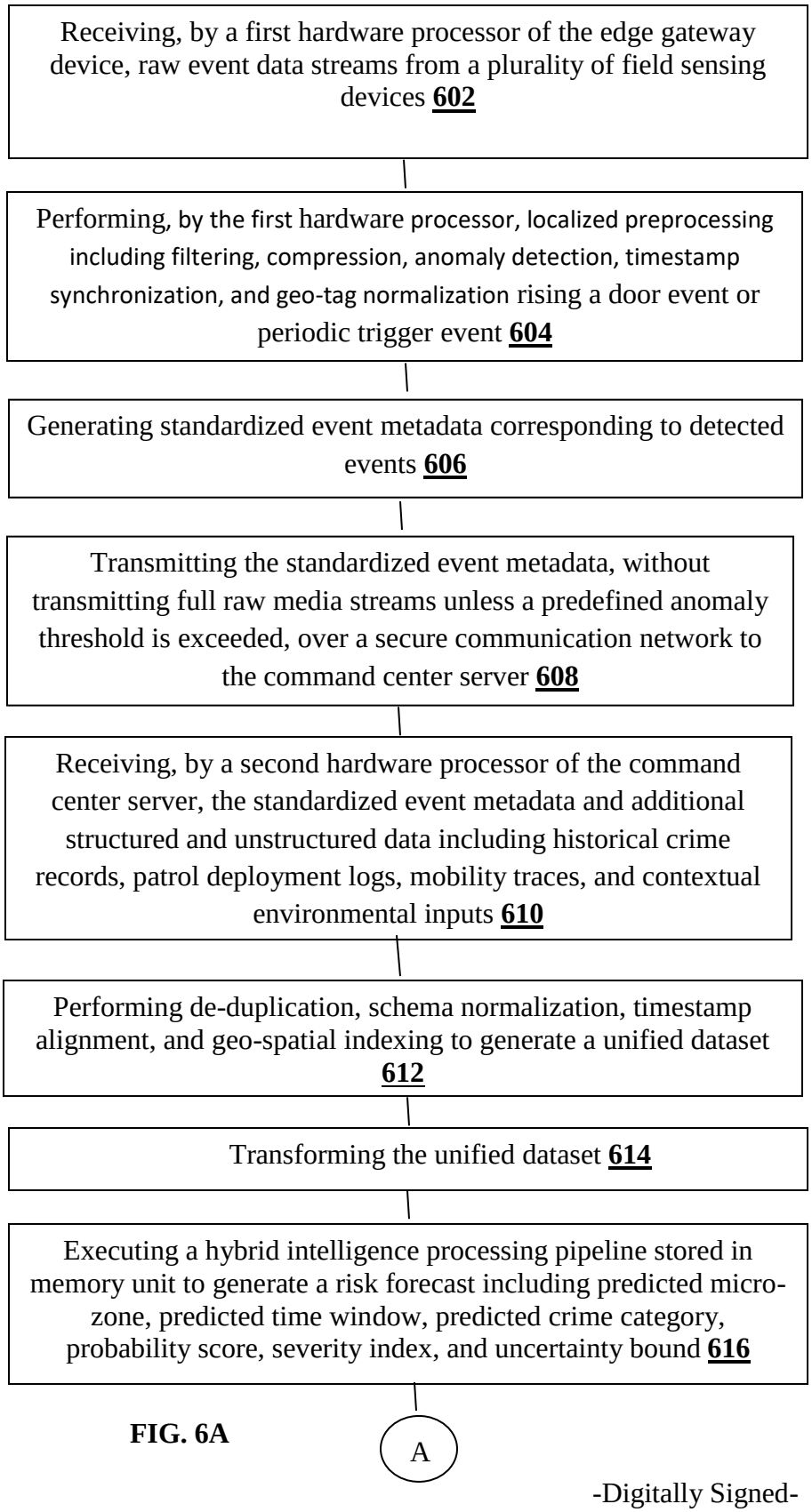


**FIG. 6A**

-Digitally Signed-
ANURADHA GUPTA
Patent Agent (IN/PA-1514)
Agent for the applicant

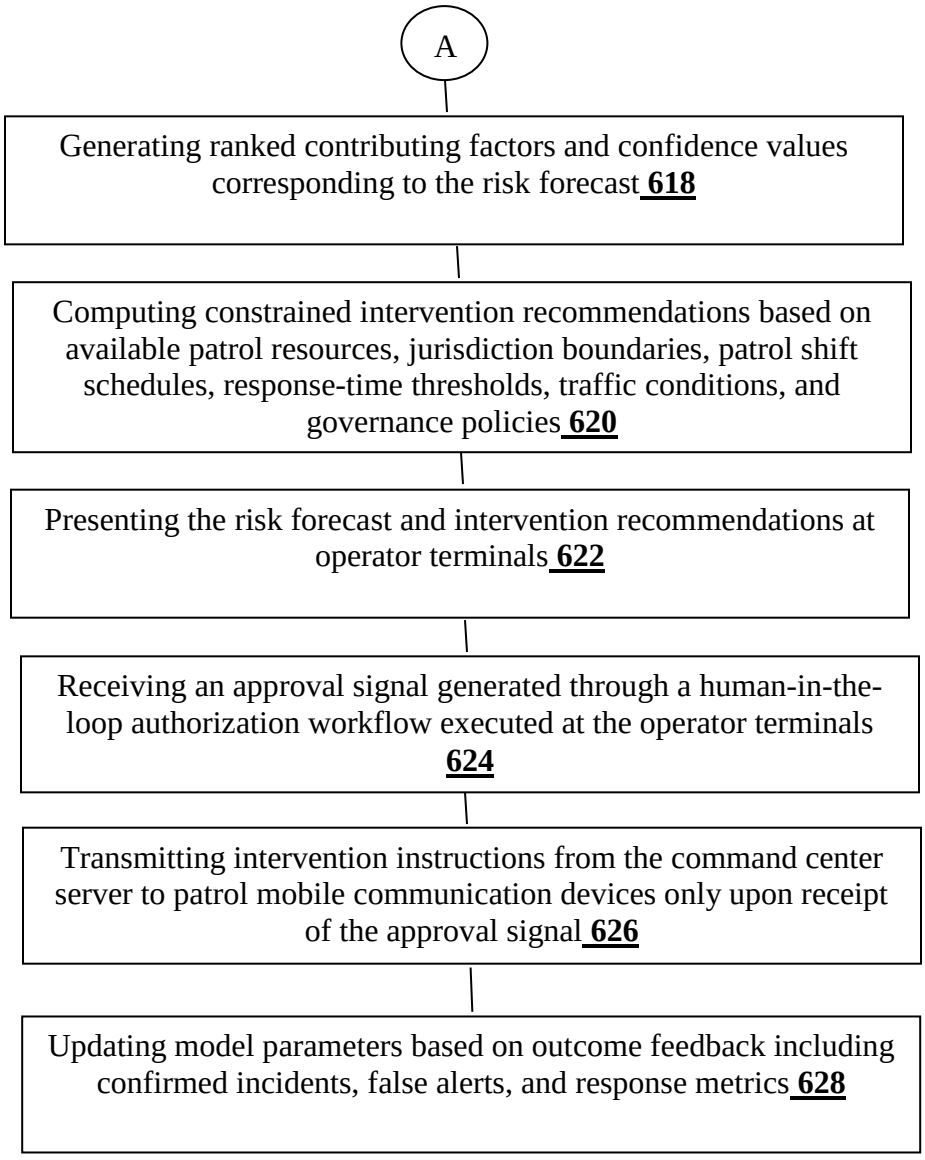


**FIG. 6B**

-Digitally Signed-
ANURADHA GUPTA
Patent Agent (IN/PA-1514)
Agent for the applicant

Digitally Signed By:
ANURADHA GUPTA
Date: 18-03-2026 19:38:48

| "FORM 1<br>THE PATENTS ACT 1970 (39 of 1970) and<br>THE PATENTS RULES, 2003<br>APPLICATION FOR GRANT OF PATENT<br>(See section 7, 54 and 135 and sub-rule (1) of rule 20) | (FOR OFFICE USE ONLY) |
|---|---|

| | | |
|---|---|---|
| | Application No. | |
| | Filing date: | |
| | Amount of Fee paid: | |
| | CBR No: | |
| | Signature: | |
| 1. APPLICANT'S REFERENCE / IDENTIFICATION NO. (AS ALLOTTED BY OFFICE) | | |

2. TYPE OF APPLICATION *Please tick (✓ ) at the appropriate category+

| Ordinary (✓) | | Convention ( ) | | PCT-NP ( ) | |
|---|---|---|---|---|---|
| Divisional ( ) | Patent of Addition ( ) | Divisional ( ) | Patent of Addition ( ) | Divisional ( ) | Patent of Addition ( ) |

3A. APPLICANT(S)

| Name in Full | Nationality | Country of Residence | Address of the Applicant | |
|---|---|---|---|---|
| **SRJX RESEARCH AND INNOVATION LAB LLP** | **Indian Company** | **INDIA** | House No. | **PLOT NO.-3E/474 SECTOR-9, CDA** |
| | | | Street | **POST- MARKAT NAGAR,** |
| | | | City | **CUTTACK** |
| | | | State | **ODISHA** |
| | | | Country | **INDIA** |
| | | | Pin code | **753014** |

3B. CATEGORY OF APPLICANT *Please tick (✓) at the appropriate category+

| Natural Person () | Other than Natural Person (✓) | | |
|---|---|---|---|
| | Small Entity ( ) | Startup (✓ ) | Others () |

4. INVENTOR(S) *Please tick (✓) at the appropriate category+

| | | |
|---|---|---|
| Are all the inventor(s) same as the applicant(s) Named above? | Yes () | No (✓) |

If "No", furnish the details of the inventor(s)

| Name in Full | Nationality | Country of Residence | Address of the Inventor | |
|---|---|---|---|---|
| **JENA, Soumya Ranjan** | **INDIAN** | **INDIA** | House No. | **PLOT NO.-3E/474 SECTOR-9, CDA** |
| | | | Street | **POST- MARKAT NAGAR** |
| | | | City | **CUTTACK** |
| | | | State | **ODISHA** |
| | | | Country | **INDIA** |
| | | | Pin code | **753014** |
| **MENDAGUDLI, Mallappa Gurupadappa** | **INDIAN** | **INDIA** | House No. | **PLOT NO. - 26 VISHWESHWARAYYA NAGAR, NEAR MALLIKARJUN ASHRAM, DISTRICT: VIJAYAPURA, KARNATAKA- 586103, INDIA** |

5. TITLE OF THE INVENTION: **ARTIFICIAL SUPER-INTELLIGENCE (ASI) BASED CRIME PREDICTION AND PREVENTION SYSTEMS**

| | | |
|---|---|---|
| 6. AUTHORISED REGISTERED PATENT AGENT(S) | Patent Agent No. | **1514** |
| | Name | **ANURADHA GUPTA** |
| | Mobile No. | **9213764385** |
| 7. ADDRESS FOR SERVICE OF APPLICANT IN INDIA | Name | **S G INTELLECTUAL** |
| | Postal Address | **4-D (UPPER FLOOR), DDA POCKET-2 SECTOR-6, DWARKA, NEW DELHI-110075, DELHI** |
| | Telephone No. | **011 35586108** |
| | Mobile No. | **9213764385** |
| | E-mail ID | **sav@sgintellectual.com** |

8. IN CASE OF APPLICATION CLAIMING PRIORITY OF APPLICATION FILED IN CONVENTION COUNTRY, PARTICULARS OF CONVENTION APPLICATION

| Country | Application Number | Filing date | Name of the applicant | Title of the Invention |
|---|---|---|---|---|
| --- | --- | --- | --- | --- |

| 9. IN CASE OF PCT NATIONAL PHASE APPLICATION, PARTICULARS OF INTERNATIONAL APPLICATION FILED UNDER PATENT CO-OPERATION TREATY (PCT) | |
|---|---|
| International application number | International filing date |
| ---------- | ---------- |
| 10. IN CASE OF DIVISIONAL APPLICATION FILED UNDER SECTION 16, PARTICULARS OF ORIGINAL (FIRST) APPLICATION-NA | |
| Original (first) application No | Date of filing of original (first) application |
| ---------- | ---------- |
| 11. IN CASE OF PATENT OF ADDITION FILED UNDER SECTION 54, PARTICULARS OF MAIN APPLICATION OR PATENT-NA | |
| Main application/patent No.---------- | Date of filing of main application ---------- |

12. DECLARATIONS

(i) Declaration by the inventor(s)-
(In case the applicant is an assignee: the inventor(s) may sign herein below or the applicant may upload the assignment or enclose the assignment with this application for patent or send the assignment by post/electronic transmission duly authenticated within the prescribed period).

We, the above named inventors are the true & first inventors for this Invention and declare that the applicant herein is our assignee ~~or legal representative~~.

i) (a) Date: 18-MAR-2026

(b) Signature: Soumya Ranjan Jena

(c) Name : **JENA, Soumya Ranjan**

ii) (a) Date: 18-MAR-2026

(b) Signature:

(c) Name : **MENDAGUDLI, Mallappa Gurupadappa**

ii) Declaration by the applicant(s) in the convention country ---N/A

~~(In case the applicant in India is different than the applicant in the convention country: the applicant in the convention country may sign herein below or applicant in India may upload the assignment from the applicant in the convention country or enclose the said assignment with this application for patent or send the assignment by post/electronic transmission duly authenticated within the prescribed period)~~

~~I/We, the applicant(s) in the convention country declare that the applicant(s) herein is/are my/our assignee or legal representative.~~

~~(a) Date~~

~~(b) Signature(s)~~

~~(c) Name(s)~~

(iii) Declaration by the applicant(s)

- ~~I~~/We the applicant(s) hereby declare(s) that: -
- ~~I am~~/We-are in possession of the above-mentioned invention.
- The Complete Specification relating to the invention is filed with this Application.
- ~~The invention as disclosed in the specification uses the biological material from India and the necessary permission from the competent authority shall be submitted by me/us before the grant of patent to me/us.~~
- There is no lawful ground of objection(s) to the grant of the Patent to me/us.
- ~~I am/we are the true & first inventor(s).~~
- ~~I am~~/we are the assignee or legal representative of true & first inventor(s).
- ~~The application or each of the applications, particulars of which are given in Paragraph-8, was the first application in convention country/countries in respect of my/our invention(s).~~
- ~~I/We claim the priority from the above-mentioned application(s) filed in convention country/countries and state that no application for protection in respect of the invention had been made in a convention country before that date by me/us or by any person from which I/We derive the title.~~
- ~~My/our application in India is based on international application under Patent Cooperation Treaty (PCT) as mentioned in Paragraph-9.~~
- ~~The application is divided out of my /our application particulars of which is given in Paragraph-10 and pray that this application may be treated as deemed to have been filed on DD/MM/YYYY under section 16 of the Act.~~

13. FOLLOWING ARE THE ATTACHMENTS WITH THE APPLICATION

(a) Form 1

| Item | Details | Fee | Remarks |
|---|---|---|---|
| Complete specification | No. of Pages - 55 | Rs. 8960/- | |
| Claim(s) | No. of Claims - 15<br>No. of Pages - 5 | ---------- | ---------- |
| Abstract | No. of Pages - 1 | | |
| Drawing(s)- | No. of Drawings - 6<br>No. of Pages - 5 | | |

(b) Complete Specification
(d) Drawings
(c) Abstract
(d) Application Form-1
(e) DIPP Certificate.
(f) Form-28
.....

We hereby declare that to the best of our knowledge, information and belief, the fact and matters stated herein are correct and We request that a patent may be granted to us for the said invention.

Dated this 18th day of March 2026

Signature: Soumya Ranjan Jena

**(Dr. Soumya Ranjan Jena)**
**DIRECTOR**
Name of Applicant: **SRJX RESEARCH AND INNOVATION LAB LLP**

SRJX Research and Innovation Lab LLP
LLPIN: ACO-1435

To
The Controller of Patents
The Patent Office, KOLKATA

Digitally Signed By:
ANURADHA GUPTA
Date: 19-03-2026 19:12:14

FORMS 28
THE PATENTS ACT, 1970
(39 of 1970)
AND
THE PATENTS RULES, 2003
TO BE SUBMITTED BY A SMALL ENTITY / STARTUP
[See rules 2 (fa), 2(fb) and 7]

| | | |
|---|---|---|
| 1. | Insert name, address and nationality | We, **SRJX RESEARCH AND INNOVATION LAB LLP**, a company registered in India, having office at PLOT NO.-3E/474, SECTOR-9, CDA, POST- MARKAT NAGAR, CUTTACK-753014, ODISHA, INDIA<br>Applicant in respect of the patent application No. 202631033028.<br><br>Hereby declare that we are a startup in accordance with rule 2(fb) and submit the following documents(s) as proof: |
| 2. | Documents to be submitted | |
| | ii. For claiming the status of a startup | |
| | A. For an Indian applicant: Any document as evidence of eligibility, as defined in rule 2(fb). | |
| | **Certificate of Recognition issued by DIPP: Certificate No. DIPP203406** | |
| 3. | To be signed by the applicant(s) / patentee(s) / authorized registered patent agent. | The information provided herein is correct to the best of our knowledge and belief.<br><br>Dated this 19th day of March 2026. |
| 4. | Name of the natural person who has signed. Designation and official seal, if any, of the person who has signed. | Signature :<br><br>-Digitally Signed-<br>(Anuradha Gupta)<br>Patent Agent (IN/PA-1514)<br>Agent for the Applicant<br><br>To<br>The Controller of Patents,<br>The Patent Office,<br>At Kolkata. |

Digitally Signed By:
ANURADHA GUPTA
Date: 19-03-2026 18:46:07

**FORM 9**
**THE PATENTS ACT, 1970**
**(39 of 1970)**
**&**
**The Patents Rules, 2003**
**REQUEST FOR PUBLICATION**
**[See section 11A (2); Rule 24A]**

| | |
|---|---|
| 1. Name, address and nationality of Applicant(s) | We, **SRJX RESEARCH AND INNOVATION LAB LLP** a Company registered in India, having office at PLOT No.-3E/474, SECTOR-9, CDA, POST- MARKAT NAGAR, CUTTACK- 753014, ODISHA, India, |
| 2. To be signed by the applicant or his authorized registered patent agent | hereby request for early publication of our Patent Application No. **202631033028 dated 18th March 2026** under Section 11A (2) of the Patent Act. |

.

Dated this 19th day of March 2026

| | |
|---|---|
| 3. Name of the natural person who has signed. | -Digitally Signed-<br>(Anuradha Gupta)<br>Patent Agent (IN/PA-1514)<br>Agent for the Applicant |

To
The Controller of Patents,
The Patent Office,
At KOLKATA

Digitally Signed By:
ANURADHA GUPTA
Date: 19-03-2026 18:10:14

**FORM 5**
**THE PATENTS ACT, 1970**
**(39 of 1970)**
**&**
**The Patents Rules, 2003**
**DECLARATION AS TO INVENTORSHIP**
**[See section 10(6) and Rule 13 (6)]**

1. **NAME OF THE APPLICANTS: SRJX RESEARCH AND INNOVATION LAB LLP** established at PLOT No-3E/474, SECTOR-9, CDA, POST- MARKAT NAGAR, CUTTACK-753014, ODISHA, INDIA,

hereby declare that the true and first inventor(s) of the invention disclosed in the Complete specification filed in pursuance of our application Numbered 202631033028 dated 18th March 2026 are:

**2. INVENTORS:**

**( i) (a) NAME : JENA, Soumya Ranjan**
**(b) NATIONALITY: INDIAN**
**(c) ADDRESS :** PLOT NO-3E/474, SECTOR-9, CDA, POST- MARKAT NAGAR, CUTTACK- 753014, ODISHA, INDIA

**(ii) (a) NAME : MENDAGUDLI, Mallappa Gurupadappa**
**(b) NATIONALITY: INDIAN**
**(c) Address :** PLOT NO. - 26 VISHWESHWARAYYA NAGAR, NEAR MALLIKARJUN ASHRAM, DISTRICT: VIJAYAPURA, KARNATAKA- 586103, INDIA

**3. DECLARATION TO BE GIVEN WHEN THE APPLICATION IN INDIA IS FILED BY THE APPLICANT(S) IN THE CONVENTION COUNTRY :- N/A**

~~We the applicant in the convention country hereby declares that our right to apply for a Patent in India is by way of assignment from the true and first inventors.~~

Dated this 19th day of March 2026 Name of the signatory **Anuradha Gupta**
**Patent agent - IN/PA-1514**

**4. STATEMENT** (to be signed by the additional inventor(s) not mentioned in the application **F**orm : **N/A**

~~/We assent to the invention referred to in the above declaration, being included in the Complete specification filed in pursuance of the stated application.~~

Dated this day of 20……..

Signature of the additional inventor(s):

Name----------

To
The Controller of Patent
The Patent Office Branch
At KOLKATA

Digitally Signed By:
ANURADHA GUPTA
Date: 19-03-2026 19:12:50

**FORM 3**

THE PATENT ACT, 1970

(39 of 1970)

and

THE PATENTS RULES, 2003

**STATEMENT AND UNDERTAKING UNDER SECTION 3**

(See Section 8; Rule 12)

| | |
|---|---|
| 1. Name of Applicant | I/We, **SRJX RESEARCH AND INNOVATION LAB LLP** established at PLOT No-3E/474, SECTOR-9, CDA, POST- MARKAT NAGAR, CUTTACK- 753014, ODISHA, INDIA,<br>Hereby Declare: |
| | (i) That I/We who have made the application for Patent number 202631033028 in India, dated 18th March 2026 alone<br>(ii) that I/We have not made any application for the same/substantially the same invention outside India<br>Or<br>(ii) ~~that I/We have made for the same/substantially same invention, application(s) for patent in the other countries, the particular of which are given below:~~ |

| **Name of the Country** | **Date of application** | **Application No.** | **Status of the application** | **Date of publication** | **Date of grant** |
|---|---|---|---|---|---|
| --- | --- | NIL | --- | --- | --- |

| | |
|---|---|
| 2. Name and address of the assignee | ~~(i) that the rights in the application(s) filed in India has/have been assigned to……~~<br>(ii) that I/We undertake that upto the date of grant of the patent by the Controller, I/We would keep him informed in writing regarding the details of corresponding applications for patents filed outside India in accordance with the provisions contained in section 8 and rule 12.<br><br>Dated this 19th day of March 2026. |
| 3. To be signed by the applicant or his authorized registered patent agent | Signature |
| 4. Name of the Natural person who has signed | (**Anuradha Gupta)**<br>Patent Agent (IN/PA-1514)<br>Agent for the Applicant |
| | To<br>The Controller of Patents,<br>The Patent Office<br>At Kolkata |

Digitally Signed By:
ANURADHA GUPTA
Date: 19-03-2026 18:44:50

| **FORM 18 A**<br>**THE PATENTS ACT,1970**<br>**and THE PATENT RULES,2003**<br>**REQUEST FOR EXPEDITED EXAMINATION OF APPLICATION FOR PATENT**<br>**[See section 11B and Rule 24C]** | (FOR OFFICE USE ONLY)<br><br>RQ. No.:<br>Filing Date:<br>Amount of fee Paid:<br>CBR no:<br>Signature: |
|---|---|

**1. APPLICANT:**

**(A) NAME**: **SRJX RESEARCH AND INNOVATION LAB LLP**

**(B) NATIONALITY**: **Indian Company**

**(C) ADDRESS**: **PLOT No.-3E/474, SECTOR-9, CDA, POST- MARKAT NAGAR, CUTTACK- 753014, ODISHA, INDIA**

2. We, **SRJX RESEARCH AND INNOVATION LAB LLP** established at PLOT No-3E/474, SECTOR-9, CDA, POST- MARKAT NAGAR, CUTTACK- 753014, ODISHA, INDIA, hereby request that our Application Patent No. **202631033028** filed on 18th March 2026 for invention Titled "**ARTIFICIAL SUPER-INTELLIGENCE (ASI) BASED CRIME PREDICTION AND PREVENTION SYSTEMS"** shall be examined under sections 12 and 13 of the Act.

~~or~~

~~I/We ---------- hereby request that my/our application for patent no. ---------- filed on ---------- for ---------- the ---------- invention titled ---------- based on Patent Cooperation Treaty (PCT) application no……..…. dated…….. made in country …….. shall be examined under sections 12 and 13 of the Act, immediately without waiting for the expiry of 31 months as specified in rule 20(4)(ii). or~~

~~I/We hereby request that my/our request for examination bearing no. ---------- for application for patent no. ---------- filed on ---------- for ---------- the ---------- invention titled ---------- may be converted to a request for expedited examination of patent application under rule 24C and the application shall be examined under sections 12 and 13 of the Act.~~

3. The applicant(s) to indicate (by ticking the appropriate box) any of the grounds applicable for request for expedited examination:

() that India has been indicated as the competent International Searching Authority or elected as an International Preliminary Examining Authority in the corresponding international application; or

(✓) that the applicant is a startup; or

( ) that the applicant is a small entity; or

( ) that the applicant is a natural person or in the case of joint applicants, all the applicants are natural persons, then applicant or at least one of the applicants is a female; or

( ) that the applicant is a department of the Government; or

( ) that the applicant is an institution established by a Central, Provincial or state Act, which is owned or controlled by the Government; or

( ) that the applicant is a Government company as defined in clause (45) of section 2 of the Companies Act, 2013 (18 of 2013); or

( ) that the applicant is an institution wholly or substantially financed by the Government; or

( ) that the application pertains to a sector which has been notified by the Central Government, on the basis of a request from the head of department of the Central Government; or

( ) that the applicant is eligible under an arrangement for processing a patent applicant pursuant to an agreement between Indian Patent Office and a foreign Patent Office.

**ADDRESS FOR SERVICE IN INDIA:**

ANURADHA GUPTA
4-D (UPPER FLOOR), DDA Pocket-2, Sector-6, Dwarka, New Delhi-110075, India
Mobile No. +91 9213764385
Email: sav@sgintellectual.com; anuradha@sgintellectual.com

Dated this 19th day of March, 2026

Signature

-Digitally Signed-

Name of the signatory: **Anuradha Gupta**

**Agent for the Applicant**

**IN/PA-1514**

To
The Controller of Patent
The Patent Office, at Kolkata

सत्यमेव जयते

# INDIA NON JUDICIAL

## Government of National Capital Territory of Delhi

₹100

**e-Stamp**

₹100₹100₹100₹100

| | | |
|---|---|---|
| Certificate No. | : | IN-DL49794072924674Y |
| Certificate Issued Date | : | 07-Feb-2026 06:44 PM |
| Account Reference | : | SELFPRINT (PU)/ dl-self/ NEHRU/ DL-DLH |
| Unique Doc. Reference | : | SUBIN-DLDL-SELF21149788829774Y |
| Purchased by | : | SATYA NARAYAN SAV |
| Description of Document | : | Article 48(c) Power of attorney - GPA |
| Property Description | : | GPA FOR FILING PATENT APPLICATIONS |
| Consideration Price (Rs.) | : | 0<br>(Zero) |
| First Party | : | SRJX RESEARCH AND INNOVATION LAB LLP |
| Second Party | : | SATYA NARAYAN SAV AND ANURADHA GUPTA |
| Stamp Duty Paid By | : | SRJX RESEARCH AND INNOVATION LAB LLP |
| Stamp Duty Amount(Rs.) | : | 100<br>(One Hundred only) |

₹100

SELF PRINTED CERTIFICATE TO BE VERIFIED BY THE RECIPIENT AT WWW.SHCILESTAMP.COM

IN-DL49794072924674Y

Please write or type below this line

**FORM 26**

**THE PATENTS ACT, 1970**

(39 of 1970)

**&**

**THE PATENTS RULES, 2003**

**Form of authorization of a patent agent/or any person in a matter or proceeding under the Act**

(See sections 127 and 132 and rule 135)

We,

**SRJX RESEARCH AND INNOVATION LAB LLP**, a company registered in India, having office at **PLOT NO.-3E/474, SECTOR-9, CDA, POST-MARKAT NAGAR, CUTTACK- 753014, ODISHA, INDIA**

do hereby authorize **S. N. Sav and Anuradha Gupta**, Patent Agent of **S G Intellectual**, 4-D (UPPER FLOOR) DDA Pocket-2, Sector-6, Dwarka, New Delhi--110075, **Delhi** , and also at A-108, Block -A, MBR Shangri La, Mysore Road, Kengeri, **Bangalore**-560059, India and/or all or any Associates/ Partners of the firm, to act on our behalf in connection with filing any and all Patent Application for any and all the inventions with the Controller of Patents, appearing on our behalf before the Controller, processing our application in respect of the same, filing provisional and/or complete specifications, and other necessary request and documents in connection with the grant of Patent for the patent application, obtaining certified copies/extracts from the Patent Office, Certificate/s of Registration, filing request for renewal of the Patent and generally to do all acts, deeds and things that may be necessary in connection with the above application, including appointment of any substitute or substitutes.

We request that all notices, requisitions and communication relating thereto may be sent to such person at the above address unless otherwise specified.

We hereby revoke all our previous authorization, if any made, in respect of same matter or proceeding.

We hereby assent to the action already taken by the above said person in the matter.

Dated this 7th day of **February 2026**

Soumya Ranjan Jena

**(Dr. Soumya Ranjan Jena)**
**Designation: Director**
**SRJX RESEARCH AND INNOVATION LAB LLP**

To,
The Controller of Patents
Patent Office, Kolkata

SRJX Research and Innovation Lab LLP
LLPIN: ACO-1435

Digitally Signed By:
ANURADHA GUPTA
Date: 19-03-2026 18:45:28

**CERTIFICATE NO:**
*DIPP203406*

सत्यमेव जयते

Government of India
Ministry of Commerce & Industry
Department for Promotion of Industry and Internal Trade

#startupindia

# CERTIFICATE OF RECOGNITION

*This is to certify that* ***SRJX RESEARCH AND INNOVATION LAB LLP*** *incorporated as a* ***Limited Liability Partnership*** *on* ***05-05-2025****, is recognized as a startup by the Department for Promotion of Industry and Internal Trade. The startup is working in 'Professional & Commercial Services' Industry and 'Professional Information Services' sector as self-certified by them.*

This certificate shall only be valid for the Entity up to **Ten** years from the date of its incorporation only if its turnover for any of the financial years has not extended **₹ 100 Cr.**

14-05-2025
**DATE OF ISSUE**

Scan to Verify

04-05-2035
**VALID UPTO**

Digitally Signed By:
ANURADHA GUPTA
Date: 18-03-2026 19:38:49