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 EE COMPUTING DEVICE -PATENT-10/2026

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

WEDNESDAY, **APRIL 22, 2026**

Our Ref.: **ANU/AI EE COMPUTING DEVICE -PATENT-06/2026**

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. **202631050972** dated **21ST APRIL 2026.**	NIL
2. Government Fee for filing the Patent Application.	INR 22,020/--
3. Miscellaneous expenses including charges for typing, phone, Print outs, photocopy, stamp fee, postal charges, conveyance etc.	INR 1000/-
Total	**INR 23,020/- (excluding taxes)**
INR. TWENTY THREE THOUSAND AND TWENTY 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
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 11232 **Date/Time 2026/04/21 19:40:00**

ANURADHA GUPTA 4-D (UPPER FLOOR), DDA, POCKET - 2, SECTOR -6, DWARKA, NEW DELHI Email: anuradha_sgi@yahoo.in

Sr. No.	App. Number	Ref. No./Application No.	Amount Paid	C.B.R. No.	Form Name	Fee Payment	Remarks
1	E-106/2275/2026/KOL	202631050972	0	-1	FORM28	Full	
2	202631050972	TEMP/E-1/55575/2026-KOL	11520	5918	FORM 1	Full	AN EXAM-SAFE OFFLINE ARTIFICIAL INTELLIGENCE (AI)-ENABLED ELECTRONIC COMPUTING DEVICE AND METHOD THEREOF

TransactionID	Payment Mode	Challan Identification Number	Amount Paid	Head of A/C No
N-0001931449	Online Bank Transfer	2104260068429	11520.00	1475001020000001

Total Amount : ₹ 11520.00
Amount in Words: Rupees Eleven Thousand Five Hundred Twenty Only

Received from ANURADHA GUPTA the sum of ₹ 11520.00 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

सत्यमेव जयते

INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS
GEOGRAPHICAL INDICATIONS

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

Docket No 11303

Date/Time 2026/04/22 14:19:29

To
ANURADHA GUPTA

UserId: anuradha4d

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	E20263027794	202631050972	8000	5953	FORM 18A	

TransactionID	Payment Mode	Challan Identification Number	Amount Paid	Head of A/C No
N-0001932081	Online Bank Transfer	2204260035637	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

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 11291 **Date/Time 2026/04/22 13:11:00**

ANURADHA GUPTA 4-D (UPPER FLOOR), DDA, POCKET - 2, SECTOR -6, DWARKA, NEW DELHI Email: anuradha_sgi@yahoo.in

Sr. No.	App. Number	Ref. No./Application No.	Amount Paid	C.B.R. No.	Form Name	Fee Payment	Remarks
1	E-12/1400/2026/KOL	202631050972	2500	5946	FORM 9	Full	

TransactionID	Payment Mode	Challan Identification Number	Amount Paid	Head of A/C No
N-0001931987	Online Bank Transfer	2204260029308	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

(10) Publication No: **IN202631050972 A1**
(22) Date of Filing: 21-04-2026

(43) Publication Date: 01-05-2026
Journal No: 18/2026

(19) Intellectual Property Office, India

(12) INDIAN PATENT APPLICATION

(54) Title: **An exam-safe offline artificial intelligence (ai)-enabled electronic computing device and method thereof**

(51) International Classification:
G06N 5/04, G06N 20/00, G06N 3/08, G06N 3/04 G09B 7/02

(21) Application No: **202631050972**

(31) Priority Document No: **--**

(32) Priority Date: **--**

(86) International Application No: **--**
Filing Date: **--**

(87) International Publication No: **--**

(61) Patent of Addition to Application No: **--**
Filing Date: **--**

(62) Divisional to Application No: **--**
Filing Date: **--**

(71) Name of Applicant(s):
Srjx Research And Innovation Lab Llp,

(72) Name of Inventor(s):
1. Mohanachandran, Dileep Kumar
2. Rao, Lella Sridhara
3. Jena, Soumya Ranjan

(57) Abstract:

The present invention discloses an exam-safe offline artificial intelligence (AI)-enabled electronic computing device configured as a handheld scientific computation device and its method. The computing device (100) comprises a processing unit (102), a memory unit (104), a keypad input interface (106), a display module (108), a mathematical computation module (110), an offline artificial intelligence (AI) inference module (112), a security control circuitry (114), a mode control interface (116), and a power management circuitry (118). The mathematical computation module (110) performs deterministic scientific computations based on the structured mathematical expressions. The offline AI inference module comprises an artificial intelligence model (120), and an inference module (122). The security control circuitry comprises a secure boot module (124), a tamper detection module (126), and an exam-safe mode control module (128). The mode control interface (116) is configured to selectively switch the computing device between a standard computation mode and an exam-safe restricted mode.

FORM 2

THE PATENTS ACT, 1970

[39 of 1970]

&

THE PATENTS RULES, 2003

COMPLETE SPECIFICATION

(Section 10; Rule 13)

AN EXAM-SAFE OFFLINE ARTIFICIAL INTELLIGENCE (AI)-ENABLED ELECTRONIC COMPUTING DEVICE AND METHOD THEREOF

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 generally to the field of computation device. More particularly relates to an exam-safe offline artificial intelligence (AI)-enabled electronic computing device configured as a handheld scientific computation device.

BACKGROUND

Scientific calculators have long been essential tools in school education, higher studies, engineering practice, laboratory work, and professional problem-solving. In academic examinations, particularly in mathematics, physics, chemistry, statistics, engineering, and technical entrance tests, scientific calculators are often permitted because they help users perform complex numerical operations accurately and quickly. Conventional scientific calculators are designed to execute predefined mathematical functions such as trigonometric operations, logarithms, exponential calculations, fractions, permutations, combinations, and statistical computations. However, these devices are fundamentally limited to direct input-output computation and do not provide intelligent guidance, contextual assistance, symbolic interpretation, or adaptive support for more advanced problem-solving needs. With the rapid growth of artificial intelligence, modern software tools and internet-based applications now provide advanced mathematical assistance far beyond the capabilities of traditional calculators. AI powered systems can interpret equations, recognize handwritten expressions, generate step-by-step solutions, explain concepts, and even respond to natural-language queries. Such systems are widely available in smartphones, tablets, computers, and cloud-based educational platforms. While these tools have significantly improved learning and accessibility, they are generally dependent on internet connectivity, large computing resources, and unrestricted digital environments. As a result, they are unsuitable for use in controlled examination settings, where fairness, security, and prevention of unauthorized assistance are critical requirements. A major challenge in present examination systems is that existing AI-enabled devices are not exam-safe. Smartphones, smartwatches, tablets, and internet-connected calculators can access online content, communicate externally, store unauthorized study materials, or run unrestricted software applications. Because of these risks, examination authorities either ban such devices entirely or impose strict usage limitations. Consequently, students and candidates are forced to rely on conventional calculators that are computationally useful but not intelligent. This creates a gap between the capabilities available during normal study and those permitted during examinations. There is therefore a need for a secure technological solution that combines the benefits of artificial intelligence with the reliability and regulatory acceptability of a dedicated scientific calculator. Another limitation of existing AI tools is their heavy reliance on cloud processing and remote servers. Such systems require constant connectivity for model inference, data retrieval, updates, and computational support. This dependency introduces problems relating to network unavailability, latency, privacy, cybersecurity, and non-compliance with exam regulations. In many educational institutions and examination centers, internet access is either restricted or completely prohibited. A device intended for legitimate examination use must therefore be capable of operating independently, with offline intelligence embedded directly into the hardware or firmware of the calculator itself, without requiring access to external networks, cloud services, or third-party applications. Conventional calculators also lack a secure architecture for controlled AI assistance. Even where programmable or graphing calculators are allowed, they may include memory storage, scripting capability, or communication interfaces that can be misused. Existing devices generally do not provide a dedicated "exam-safe mode" that restricts non-permitted operations while still allowing useful offline intelligent computational support. There is no widely adopted low-cost hardware platform specifically designed to offer embedded AI assistance under strict operational boundaries suitable for regulated examinations. This absence has limited the practical deployment of intelligent calculators in formal assessment environments. Accordingly, there exists a need for an exam-safe offline artificial intelligence scientific calculator system that integrates dedicated hardware, secure firmware, restricted operating modes, and embedded AI computation within a portable calculator form factor. Such a system should preserve the trusted functionality of a standard scientific calculator while adding controlled intelligent capabilities such as equation interpretation, limited offline guidance, error reduction, and enhanced usability, all without violating examination security requirements. The present invention is directed toward overcoming these deficiencies in the prior art by providing a technically secure, affordable, and examination-compliant AI scientific calculator implemented as a hardware invention rather than mere software.

Therefore, there is a need for an exam-safe offline artificial intelligence (AI)-enabled electronic computing device 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 an exam-safe scientific electronic computing device integrated with offline artificial intelligence capabilities.
2. To develop a dedicated hardware-based scientific electronic computing device that operates independently without reliance on cloud servers or internet connectivity.
3. To combine the functions of a traditional scientific computing device with controlled AI-assisted computational support in a single portable unit.
4. To ensure that the calculator remains secure and compliant for examination environments by restricting unauthorized communication, data sharing, and external access.
5. To provide an offline AI inference engine capable of assisting with mathematical interpretation, structured input handling, and error reduction.
6. To enable accurate scientific, engineering, and academic computing with improved usability over conventional calculators.
7. To minimize user mistakes by incorporating syntax checking, expression verification, and bounded intelligent correction mechanisms.

8. To provide a restricted operating mode in which only approved and predefined AI-supported functions are available during examinations.
9. To prevent misuse by disabling or controlling wireless communication, external storage access, programmable abuse, and unrestricted software execution.
10. To create a computing architecture that supports secure firmware control, locked execution pathways, and protected system integrity.
11. To offer a dual-purpose device that can function in both standard computing mode and controlled AI-assisted mode depending on institutional or user settings.
12. To provide a system that improves fairness, transparency, and trust in academic and technical examination settings.
13. To design a low-power and low-cost embedded hardware platform suitable for students, institutions, and large-scale educational deployment.
14. To provide a practical alternative to smartphones, tablets, and internet-based AI tools that are generally not permitted in regulated examinations.
15. To enhance accessibility and computational convenience while preserving the core reliability of a scientific calculator.
16. To create a novel technical solution that can be framed as a hardware invention with tangible technical effect, rather than as mere software.
17. To enable secure and efficient use of artificial intelligence in education, testing, engineering, and professional problem-solving environments.
18. To bridge the technological gap between conventional calculators and modern intelligent computational systems in a safe and controlled manner.

SUMMARY OF THE INVENTION

The present invention relates to an exam-safe offline artificial intelligence (AI)-enabled electronic computing device configured as a dedicated hardware device for secure mathematical computation and controlled intelligent assistance in examination and academic environments. The invention combines the trusted functionality of a conventional scientific calculator with embedded offline artificial intelligence features, while ensuring that the device remains compliant with examination safety requirements. In particular, the invention is designed to operate without internet connectivity, cloud dependence, external communication, or unrestricted software execution, thereby making it suitable for regulated testing conditions where fairness, transparency, and operational control are essential.

In one aspect, the invention provides a portable scientific computing device comprising a processing unit, memory unit, display unit, keypad interface, power management circuitry, and an embedded artificial intelligence module stored locally within the device. The embedded AI module is configured to assist in mathematical interpretation, structured equation handling, input correction, and limited context-aware computational support, all within pre-authorized examination boundaries. Unlike general-purpose AI applications running on smartphones or computers, the present device functions as a self-contained hardware computing device with restricted capabilities specifically tailored for secure academic and technical usage.

In another aspect, the invention introduces an exam-safe operating architecture in which the intelligent features of the calculator are governed by a secure control framework. This framework may include firmware-based restrictions, locked execution pathways, secure boot validation, non-programmable examination mode, restricted memory access, and disabled communication interfaces. The device is configured such that during examination operation it cannot access wireless networks, external databases, remote servers, messaging systems, or stored unauthorized educational content. The invention thereby ensures that the artificial intelligence functionality remains bounded to approved offline computational assistance rather than open-ended generative or communicative behavior.

In a further aspect, the invention provides an offline AI inference engine optimized for low-power embedded hardware. This engine may include a compressed or lightweight machine learning model trained to recognize mathematical patterns, detect syntax errors in expressions, interpret multi-step input structures, and provide controlled assistance for scientific operations such as algebraic arrangement, trigonometric evaluation, logarithmic computation, statistics handling, and unit-aware calculations. The offline nature of the inference engine eliminates dependence on external servers and reduces concerns relating to privacy, latency, and exam rule violations. At the same time, it allows the calculator to deliver a more intelligent and user-friendly computational experience than traditional scientific calculators.

In another aspect, the invention provides a restricted assistance mechanism that differs fundamentally from unrestricted AI tutoring systems. The computing device does not act as a general chat device or open-domain question-answering platform. Instead, it is configured to support only predefined categories of mathematical and scientific assistance permitted by device policy or examination settings. Such assistance may include expression verification, syntax-level correction, formula selection from approved internal libraries, numerical checking, step-limited guidance, and symbolic interpretation within strictly bounded rules. This selective intelligence improves usability and reduces user error while preserving compliance with controlled examination standards.

In one embodiment, the invention may further include a secure display management system and interaction logic through which the user can switch between standard calculator mode and controlled AI-assisted mode, subject to administrative permissions or preset institutional policies. In some implementations, the examination mode may automatically disable advanced assistance beyond a permitted threshold, while in practice or learning mode the same hardware may provide broader offline AI support. Such dual-mode architecture enables the device to be useful both inside and outside examination environments without compromising security during regulated use. The transition between modes may be controlled through password protection, authenticated firmware settings, hardware switches, or invigilator-configured access control.

In another embodiment, the invention may include additional technical safeguards such as tamper detection, audit logging, secure firmware hash verification, disabled USB data transfer during restricted mode, restricted storage partitions, and hardware-level isolation of the AI processing block. These features strengthen the technical character of the invention and distinguish it from mere software implementation. The invention therefore resides not only in the abstract concept of AI-based calculation, but in the specific combination of hardware architecture, embedded offline intelligence, examination-safe control logic, and secure execution environment integrated into a scientific calculator platform.

A further advantage of the invention is its suitability as a low-cost and scalable device for educational institutions, examination boards, students, engineers, and technical professionals. By using optimized local models and embedded electronics, the system can be manufactured at relatively low cost compared with laptops, tablets, or advanced connected devices. It may therefore serve as a practical bridge between conventional calculators and modern intelligent tools, enabling users to benefit from AI-assisted accuracy and usability without introducing the risks associated with internet-enabled devices.

Accordingly, the invention provides a novel hardware-based scientific computing device/system that integrates offline artificial intelligence with examination-safe restrictions in a compact portable device. The invention addresses the longstanding gap between traditional calculators and unrestricted AI tools by delivering secure, bounded, and technically controlled intelligent computation. It thereby offers an improved solution for modern academic and technical environments where both computational efficiency and examination integrity are of critical importance.

An embodiment of the present invention describes an exam-safe offline artificial intelligence (AI)-enabled electronic computing device (100) configured as a handheld scientific computation device. The computing device comprises a processing unit (102) configured to control operation of the computing device and execute stored instructions, a memory unit (104) operatively coupled to the processing unit, the memory unit comprising: a firmware storage storing authenticated executable firmware, and a data storage storing predefined mathematical function libraries and a locally stored artificial intelligence model, a keypad input interface (106) comprising a plurality of physical keys configured to receive structured mathematical expressions, a display module (108) operatively coupled to the processing unit and configured to display at least one of the structured mathematical expressions, computational outputs, and restricted assistance prompts, a mathematical computation module (110) executed by the processing unit and configured to perform deterministic scientific computations including arithmetic, trigonometric, logarithmic, algebraic, and statistical operations based on the structured mathematical expressions, an offline artificial intelligence (AI) inference module (112) stored in the memory unit and executable by the processing unit, the offline AI inference module comprising: an artificial intelligence model (120), and an inference module (122) configured to process the structured mathematical expressions to perform at least one of: syntax validation, operator placement verification, expression structure interpretation, and bounded input correction, a security control circuitry (114) operatively coupled to the processing unit, the security control circuitry (114) comprising: a secure boot module (124) configured to authenticate the firmware prior to execution, a tamper detection module (126) configured to detect unauthorized modification of the computing device, and an exam-safe mode control module (128), a mode control interface (116) configured to selectively switch the computing device between a standard computation mode and an exam-safe restricted mode; and a power management circuitry (118) configured to supply regulated power to the processing unit and one or more associated components, wherein, when the computing device (100) operates in the exam-safe restricted mode:

the exam-safe mode control module disables or restricts external communication interfaces and external data access pathways. The offline AI inference module is constrained to execute only a predefined set of permitted assistance functions stored in the memory unit. The mathematical computation module executes only validated structured mathematical expressions to generate deterministic computational outputs. The computing device provides restricted artificial intelligence assistance limited to predefined permissible categories without enabling unrestricted tutoring, external information retrieval, or non-deterministic interaction, thereby enabling a controlled and restricted offline intelligent computational environment that reduces input errors and enhances computational reliability while maintaining compliance with controlled examination conditions.

According an embodiment of the present invention, the tamper detection module is configured to detect at least one of enclosure opening, firmware alteration, or unauthorized hardware access, and in response, trigger a restricted operational state. The restricted operational state comprises at least one of: disabling the offline artificial intelligence inference module, restricting access to stored data, and preventing normal computational operation.

According another embodiment of the present invention, the memory unit comprises segmented memory partitions including: a firmware storage partition, a restricted data storage partition, and a volatile working memory partition, and wherein access to the restricted data partition is controlled by the security control circuitry, wherein the volatile working memory partition is configured to automatically erase stored data upon power-off when the computing device operates in the exam-safe restricted mode.

According to yet another embodiment of the present invention, the artificial intelligence model is a compressed model optimized for embedded execution, comprising at least one of: quantized parameters, reduced precision representations, and pruned model architecture. The artificial intelligence model (120) is configured to receive a structured mathematical expression comprising tokenized elements arranged as an expression tree or a precedence-based token sequence, perform feature extraction by identifying syntactic and structural attributes including operator sequences, operand relationships, bracket structures, and function-argument mappings, and generate model outputs comprising classification scores, pattern recognition results, or error likelihood indicators associated with the structured mathematical expression, The inference module (122) is configured to utilize outputs of the artificial intelligence model (120) to perform syntax validation, operator placement verification, expression structure interpretation, and bounded input correction. The inference module is configured to execute the compressed artificial intelligence model with bounded computational complexity to maintain deterministic response time and low power consumption.

According to yet another embodiment of the present invention, the mode control interface comprises at least one of: a password-based access mechanism, an administrator-controlled configuration, and a hardware-based switching element, for enforcing transition between the standard computation mode and the exam-safe restricted mode, wherein the exam-safe restricted mode is configured to be automatically re-enabled upon device restart or after a predefined session interval.

According to yet another embodiment of the present invention, the security control circuitry is configured to disable or isolate communication hardware interfaces including at least one of wireless communication modules, data ports, and external connectivity channels during the exam-safe restricted mode.

According to yet another embodiment of the present invention, the offline AI inference module is governed by a policy control mechanism stored in the memory unit, the policy control mechanism defining a set of permissible assistance functions executable in the exam-safe restricted mode, wherein the permissible assistance functions comprise at least one of: expression validation, syntax error indication, operator correction prompts, or structured input guidance, while preventing generation of step-by-step derivations or unrestricted explanatory outputs.

According to yet another embodiment of the present invention, the computing device further comprising a secure boot verification mechanism configured to compare firmware integrity values with stored reference values prior to system initialization, and to inhibit normal operation upon detection of mismatch.

Another embodiment of the present invention describes a computer-implemented method for providing controlled offline scientific computation using an exam-safe offline artificial intelligence (AI)-enabled electronic computing device, the method comprising: initializing, by a processing unit, the computing device through execution of a secure boot process, including verifying integrity of firmware stored in a memory unit, accessing, by the **processing** unit, predefined mathematical function libraries and a locally stored artificial intelligence model from the memory unit, receiving, by a keypad input interface, a structured mathematical expression, selecting, by a mode control interface, an operational mode including one of a standard computation mode and an exam-safe restricted mode, processing, by the processing unit, the structured mathematical expression using a mathematical computation module, evaluating, by an offline artificial intelligence (AI) inference module executed by the processing unit, the structured mathematical expression to perform at least one of: syntax validation, operator placement verification, expression structure interpretation, and bounded input correction, restricting, by a security control circuitry, execution of non-permitted functions and external communication pathways when the computing device operates in the exam-safe restricted mode, generating, by the mathematical computation module, a deterministic computational result based on a validated structured mathematical expression, and displaying, by a display module, the deterministic computational result along with any permitted restricted assistance output, wherein, the offline AI inference module operates exclusively on locally stored data and is constrained to predefined permissible assistance functions in the exam-safe restricted mode, thereby enabling a controlled and restricted offline computation process compliant with examination conditions.

According to another embodiment of the present invention, the secure boot process further comprises comparing firmware integrity values with stored reference values and inhibiting system initialization upon detection of mismatch.

According to yet another embodiment of the present invention, the method further comprises detecting, by a tamper detection module, at least one of physical intrusion, firmware modification, and unauthorized access, and transitioning the computing device into a restricted operational state, wherein the restricted operational state comprises at least one of: disabling the offline AI inference module, restricting access to stored data, and preventing execution of computational functions.

According to yet another embodiment of the present invention, the method further comprises partitioning, by the memory unit, stored data into secure partitions including firmware storage partition, restricted data storage partition, and volatile working memory partition.

According to yet another embodiment of the present invention, the method further comprises erasing, by the processing unit, data stored in the volatile working memory upon power-off when operating in the exam-safe restricted mode.

According to yet another embodiment of the present invention, the method of evaluating the structured mathematical expression by the offline artificial intelligence inference module comprises executing a compressed artificial intelligence model having reduced computational complexity, wherein the compressed artificial intelligence model comprises at least one of quantized parameters, reduced precision data representation, and pruned model architecture.

According to yet another embodiment of the present invention, the method further comprising enforcing, by the security control circuitry, disabling or isolation of external communication interfaces during the exam-safe restricted mode.

According to yet another embodiment of the present invention, the method further comprises controlling, by a policy module, execution of the offline artificial intelligence inference module to allow only predefined assistance functions, wherein the predefined assistance functions comprise at least one of: expression validation, syntax error indication, operator correction prompting, and structured input guidance, while preventing generation of unrestricted explanatory outputs.

According to yet another embodiment of the present invention, the method further comprises automatically re-enabling the exam-safe restricted mode upon system restart or after a predefined time interval.

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 an exam-safe offline artificial intelligence (AI)-enabled electronic computing device configured as a handheld scientific computation device, according to an embodiment of the present invention.

FIG. 2 illustrates a flow chart of a computer-implemented method for providing controlled offline scientific computation using an exam-safe offline artificial intelligence (AI)-enabled electronic computing device, according to an embodiment of the present invention.

FIG. 3 illustrates an exam-safe offline artificial intelligence (AI)-enabled electronic computing device configured as a handheld scientific computation device, according to an embodiment of the present invention.

FIG. 4 illustractes a logic layer architecture an exam-safe offline artificial intelligence (AI)-enabled electronic computing device, according to an embodiment of the present invention.

FIG. 5 illustrates an external device view of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device, according to an embodiment of the present invention.

FIG. 6 illustractes an Offline AI Processing Flow Diagram of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device, according to an embodiment of the present invention.

FIG. 7 illustractes Secure Boot and Integrity Verification Flow Diagram of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device, according to an embodiment of the present invention.

FIG. 8 illustractes a flow chart of a computer-implemented method for providing controlled offline scientific computation using an exam-safe offline artificial intelligence (AI)-enabled electronic computing device, 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. In one embodiment, an exam-safe offline artificial intelligence (AI)-enabled electronic computing device is also referred as an exam-safe offline artificial intelligence (AI)-based electronic computing device.

The present invention provides a dedicated, exam-safe scientific computing/calculator hardware device that incorporates offline artificial intelligence within a controlled and restricted operating environment. Unlike conventional scientific calculators that only execute predefined functions, and unlike smartphone-based AI math solvers that rely on open operating systems and internet services, the invention uniquely merges the reliability of an examination-permitted calculator with embedded intelligence designed specifically for regulated settings. The uniqueness lies not merely in “using AI,” but in the technical integration of AI computation into a calculator appliance with enforceable boundaries suitable for examinations. In one embodiment, an exam-safe offline artificial intelligence (AI)-enabled electronic computing device is a scientific calculator that incorporates offline artificial intelligence within a controlled and restricted operating environment.

A key unique aspect is the invention's Offline AI Inference Engine implemented on embedded hardware, allowing the computing device to perform intelligent operations without any dependence on cloud connectivity. Existing AI calculators and apps commonly depend on online servers or internet-based models for recognition and explanation. In contrast, the present invention stores compressed, optimized AI models locally in secure memory and executes inference through the device processing unit (or an optional low-cost AI accelerator). This enables features such as expression understanding, syntax-aware validation, structured equation parsing, and context-limited assistance entirely offline. The offline execution ensures privacy, low latency, and compliance with exam rules that prohibit network access.

Another unique aspect is the Exam-Safe Restricted Mode Architecture that technically enforces permissible behavior. In one embodiment, the computing device includes secure firmware control that disables or permanently omits external communication channels (Wi-Fi, Bluetooth, cellular, messaging) and restricts any functionality that could provide unfair advantage. This includes restricted access to stored content, prevention of file browsing, and elimination of general-purpose app installation. The invention thus introduces a "policy-governed computing device" in hardware form, where the AI operates only within an allowed feature set. The device can be configured to function as a normal scientific computing device while the AI module operates under strict rules, ensuring that the intelligence cannot become an open tutoring platform during examinations.

A further unique aspect is the invention's Controlled Assistance Model, which intentionally provides bounded intelligence rather than unrestricted step-by-step tutoring. The AI module is configured to assist only in exam-permitted ways, such as verifying expression correctness, highlighting input errors, suggesting valid operator placement, confirming unit consistency (where enabled), or offering limited structured hints without revealing full derivations if such derivations are not permitted. This design is unique because most existing AI math systems are designed for maximum help and explanation, whereas the invention is designed for compliance-first intelligence—a fundamentally different technical objective and constraint set.

The invention is also unique in its Secure Execution and Integrity Framework tailored to examination use. In one embodiment, the device uses secure boot, signed firmware, and checksum verification so that only authentic system software can run. Optional tamper-resistance mechanisms may detect attempts to open the device, alter the firmware, or inject unauthorized code, thereby triggering restricted operation, logging, or lockout. This ensures the computing device remains trustworthy in examination halls and prevents modification into a cheating device. Such an integrity framework distinguishes the invention from general consumer gadgets and from modified calculators that simply add network-based AI access.

Another unique aspect is the invention's Dual-Mode Functional Partitioning: a standard computing mode and a controlled AI-assisted mode, with mode transitions governed by secure methods such as an invigilator key sequence, password, device administrator configuration, or hardware switch. In learning/practice settings, expanded offline AI features may be enabled; in exam settings, the device automatically enforces strict limits. This dual-mode partitioning is unique because it allows one low-cost hardware product to serve both everyday learning and regulated assessment while preserving exam security through technical restriction rather than reliance on user discipline.

The invention further includes uniqueness in Low-Cost Embedded Optimization for AI Mathematics, where the AI models and math-processing pipeline are engineered for limited memory, low power consumption, and fast response. In one embodiment, the system uses lightweight symbolic computation combined with compact machine learning models (for recognition, validation, and guidance) so that the device remains affordable and battery-efficient. The architecture may allocate fixed memory partitions for AI models, fixed libraries for permitted functions, and a deterministic computation path that avoids unpredictable outputs. This creates a technical effect: improved usability and reduced user error in scientific computation, without requiring expensive smartphone hardware.

Additionally, the invention is unique in its Exam-Compliance Interface Design, where the user interaction is intentionally computing device-like (keypad-driven, limited text entry, deterministic menu navigation) rather than chat-like. This prevents misuse and reduces ambiguity. The invention may also include a visible exam indicator (LED/icon) showing that restricted mode is active, providing transparency to invigilators. This interface-level compliance is an important novel aspect because it transforms AI assistance into a controlled calculator feature set rather than turning the device into a general AI terminal.

Accordingly, the present invention is unique due to its unique combination of (i) offline embedded AI, (ii) hardware-enforced exam-safe restrictions, (iii) controlled, bounded assistance, (iv) secure integrity and anti-tamper architecture, and (v) low-cost embedded optimization, all implemented in a dedicated scientific computing device. These aspects collectively create a new technical solution that bridges the gap between traditional exam-permitted calculators and modern AI tools, while maintaining fairness, security, and regulatory suitability.

FIG. 1 illustrates a block diagram of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device configured as a handheld scientific computation device, according to an embodiment of the present invention. The computing device (100) comprises a processing unit (102), a memory unit (104), a keypad input interface (106), a display module (108), a mathematical computation module (110), an offline artificial intelligence (AI) inference module (112), a security control circuitry (114), a mode control interface (116), and a power management circuitry (118).

The processing unit (102) is configured to control operation of the computing device and execute stored instructions. In one embodiment, the processing unit (102) may comprise a microcontroller, microprocessor, or system-on-chip (SoC) configured to execute firmware instructions stored in the memory unit (104). The processing unit (102) coordinates deterministic computation, input parsing, AI inference execution, and enforcement of security policies through direct communication with each subsystem via internal buses.

The memory unit (104) is operatively coupled to the processing unit. The memory unit comprises a firmware storage storing authenticated executable firmware, and a data storage storing predefined mathematical function libraries and a locally stored artificial intelligence (AI) model (120). The firmware storage is configured as non-volatile secure memory, while the data storage may include flash memory and volatile RAM.

The keypad input interface (106) comprises a plurality of physical keys configured to receive structured mathematical expressions. In one embodiment, the keypad input interface (106) comprises a matrix of physical keys mapped to numerical inputs, operators, and predefined scientific functions, wherein the keypad input interface is configured to generate structured input signals representing mathematical expressions entered by a user. Upon receiving input through the keypad input interface (106), the processing unit (102) is configured to convert sequences of keypresses into a structured representation, including a tokenized expression tree or an equivalent parsed format. The structured expression is then forwarded to the mathematical computation module (110), which is executed by the processing unit (102) and configured to perform deterministic evaluation of the expression using predefined mathematical libraries. The computation module applies fixed and reproducible algorithms to generate a corresponding computational result based on the structured input.

The display module (108) is operatively coupled to the processing unit and configured to display at least one of the structured mathematical expressions, computational outputs, and restricted assistance prompts.

The mathematical computation module (110) is executed by the processing unit and configured to perform deterministic scientific computations including arithmetic, trigonometric, logarithmic, algebraic, and statistical operations based on the structured mathematical expressions. In one embodiment, the mathematical computation module (110) is configured to perform deterministic evaluation of mathematical expressions using predefined computational routines. The computation module (110) executes arithmetic operations using fixed-point or floating-point arithmetic, depending on implementation requirements. The module is further configured to perform trigonometric calculations using lookup tables, series approximations, or equivalent numerical methods, and to evaluate logarithmic and exponential functions using iterative computation techniques or table-based approaches. Additionally, the computation module (110) is configured to perform algebraic and statistical operations using predefined deterministic routines stored in the memory unit. Such implementation ensures accurate, repeatable, and efficient computation of a wide range of scientific functions within the computing device.

The output is generated as a **deterministic computational result**, ensuring reproducibility for identical inputs.

The offline artificial intelligence (AI) inference module (112) is stored in the memory unit and executable by the processing unit. The offline AI inference module (112) operates as a bounded pre-processing and validation engine integrated into the computational pipeline.

The offline AI inference module (112) includes an artificial intelligence model (120), and an inference module (122) executing controlled evaluation logic.

In one embodiment, the artificial intelligence model (120) forms part of the offline artificial intelligence inference module (112) and is configured as a computational model for evaluating structured mathematical expressions. The artificial intelligence model (120) is implemented as a compressed embedded model stored in the memory unit (104) and executable by the processing unit (102), and operates exclusively on locally available data without requiring external communication or cloud-based processing. The artificial intelligence model (120) is configured to receive, as input, a structured representation of a mathematical expression comprising tokenized elements arranged as an expression tree or a precedence-based token sequence.

Upon receiving the structured input, the artificial intelligence model (120) is configured to perform feature extraction by identifying syntactic and structural attributes of the expression, including operator sequences, operand relationships, bracket structures, and function-argument mappings. The model processes the extracted features using a trained inference pipeline comprising pattern recognition logic, rule-based constraints, and machine learning-based classification layers to generate evaluation outputs indicative of structural validity, error likelihood, and correction candidates.

In one embodiment, the artificial intelligence model (120) is optimized for embedded execution through model compression techniques including parameter quantization, reduced precision data representation, and architectural pruning, thereby reducing computational complexity and memory requirements. The model is configured to execute with deterministic inference latency and bounded resource utilization, enabling real-time processing within the computing device. The outputs generated by the artificial intelligence model (120) comprise classification results, validation indicators, or correction suggestions, which are provided to the inference module (122) for further processing.

Accordingly, the artificial intelligence model (120) operates as a computational engine for pattern recognition and structured evaluation, without independently enforcing execution control or system-level constraints.

In one embodiment, the inference module (122) is configured to control evaluation of structured mathematical expressions using outputs generated by the artificial intelligence model (120). Upon receiving the structured mathematical expression, the inference module (122) is configured to parse the expression into syntactic components and coordinate execution of validation and correction processes. The inference module (122) includes a validation engine configured to perform grammar checking based on operator placement rules, validation of bracket matching, and verification of function-argument consistency using both deterministic rules and outputs provided by the artificial intelligence model (120).

The inference module (122) further includes a bounded correction engine configured to detect incomplete or malformed expressions and to generate constrained correction prompts based on model-derived suggestions and predefined rule sets. The inference module (122) is configured to filter and constrain such outputs in accordance with a policy control mechanism stored in the memory unit (104), thereby ensuring that only permitted assistance functions are executed.

The inference module (122) is further configured to control output generation by selecting and formatting permissible assistance outputs, including validation indicators, syntax error notifications, and structured input guidance, while preventing generation of unrestricted explanatory content, step-by-step derivations, or open-ended responses. Accordingly, the inference module (122) operates as an execution and control layer that integrates deterministic validation logic with model-based evaluation outputs to provide bounded and policy-compliant assistance within the computing device.

The security control circuitry (114) is operatively coupled to the processing unit. The security control circuitry (114) comprises a secure boot module (124) configured to authenticate the firmware prior to execution, a tamper detection module (126) configured to detect unauthorized modification of the computing device, and an exam-safe mode control module (128). In one embodiment, the secure boot module (124) is configured to authenticate firmware integrity during device initialization. Upon power-on or system reset, the secure boot module (124) computes a firmware integrity value by applying a cryptographic hashing function, including but not limited to a Secure Hash Algorithm (SHA)-based technique, to executable firmware stored in the memory unit. The computed integrity value is then compared with a corresponding reference value stored in a secure memory region. In response to determining that the computed integrity value matches the reference value, the processing unit proceeds with normal system initialization. Conversely, in response to detecting a mismatch between the computed integrity value and the stored reference value, the secure boot module (124) is configured to inhibit normal execution by halting system initialization or transitioning the computing device into a restricted safe mode, thereby preventing execution of unauthorized or modified firmware.

In one embodiment, the tamper detection module (126) is configured to monitor integrity of the computing device through multiple detection mechanisms. The tamper detection module (126) may detect enclosure integrity using mechanical switches, conductive traces, or equivalent physical intrusion sensing arrangements. The module may further verify firmware integrity through checksum validation or hash-based verification techniques, and monitor hardware access by detecting anomalies in internal communication buses. Upon detection of any unauthorized modification, intrusion, or integrity violation, the tamper detection module (126) is configured to trigger a restricted operational state, wherein the offline artificial intelligence inference module is disabled, access to stored data is restricted, and execution of computational operations is halted or limited.

In one embodiment, the security control circuitry (114) is configured to enforce communication isolation when the computing device operates in the exam-safe restricted mode. During such operation, one or more communication interfaces, where present, are selectively disabled or isolated to prevent external data exchange. The isolation is implemented by electrically disabling the communication hardware or by logically isolating the interfaces through firmware-controlled gating mechanisms. The communication interfaces subjected to such restriction include, but are not limited to, wireless communication modules, data ports, and external connectivity channels. By disabling or isolating these interfaces, the system prevents access to external networks, devices, or data sources, thereby ensuring controlled and secure operation in compliance with examination conditions.

In one embodiment, the exam-safe mode control module (128) is configured to enforce a restricted operational state of the computing device during controlled usage conditions. The exam-safe mode is activated via the mode control interface (116), which comprises one or more mechanisms including password-based authentication, administrator-controlled configuration, or a hardware-based switching element. Upon activation of the exam-safe restricted mode, the exam-safe mode control module (128), in coordination with the security control circuitry (114), restricts system operation such that only pre-approved functions are accessible for execution. Further, the offline artificial intelligence inference module is governed by a policy-controlled execution framework, external communication pathways are disabled or isolated, and access to restricted memory partitions is blocked. In one embodiment, the system is configured to automatically enforce the exam-safe restricted mode upon device restart or after expiration of a predefined session interval, thereby ensuring continued compliance with controlled operational requirements.

In one embodiment, the offline artificial intelligence inference module (112) is governed by a policy control mechanism stored in the memory unit (104), the policy control mechanism being configured to define and enforce a set of permissible artificial intelligence functions during operation of the computing device. The policy control mechanism enables execution of limited assistance operations including syntax validation of structured mathematical expressions, generation of operator correction prompts, and provision of structured input guidance. Concurrently, the policy control mechanism restricts execution of non-permitted functions, including generation of step-by-step derivations, explanatory tutoring outputs, and open-ended or unrestricted responses. By enforcing such controlled execution, the system ensures that the artificial intelligence inference module operates within predefined boundaries, thereby providing bounded computational assistance with predictable execution behavior while maintaining compliance with examination constraints.

In one embodiment, the memory unit (104) is organized into a segmented architecture comprising a firmware partition, a restricted data partition, and a volatile working memory partition. The firmware partition is configured as a secure, read-only memory region storing authenticated executable firmware, while the restricted data partition is configured to store controlled data accessible under policy-defined conditions. The volatile working memory partition is configured to temporarily store runtime data generated during operation of the computing device. Access to the restricted data partition is controlled by the security control circuitry (114), thereby preventing unauthorized retrieval or modification of stored data. Further, when the computing device operates in the exam-safe restricted mode, the volatile working memory partition is automatically cleared upon power-off, ensuring that no residual data persists beyond a session. This segmented memory architecture prevents unauthorized storage usage and eliminates persistence of sensitive data, thereby enhancing system security and compliance with controlled operational requirements.

In one embodiment, the power management circuitry (118) is configured to regulate and distribute electrical power to the processing unit and associated components of the computing device. The power management circuitry (118) controls voltage levels supplied to various modules to ensure stable and reliable operation under varying load conditions. The circuitry is further configured to selectively activate or deactivate the offline artificial intelligence inference module (112) based on operational requirements, thereby optimizing power utilization during computation. Additionally, the power management circuitry (118) maintains low-power operation during idle or standby states by reducing power consumption of non-essential components while preserving system readiness. Such controlled power management enhances energy efficiency, prolongs battery life, and ensures consistent performance of the computing device.

The mode control interface (116) is configured to selectively switch the computing device between a standard computation mode and an exam-safe restricted mode. The power management circuitry (118) is configured to supply regulated power to the processing unit and one or more associated components. When the computing device (100) operates in the exam-safe restricted mode, the following steps follows: Firstly, the exam-safe mode control module disables or restricts external communication interfaces and external data access pathways. Secondly, the offline AI inference module is constrained to execute only a predefined set of permitted assistance functions stored in the memory unit. Thirdly, the mathematical computation module executes only validated structured mathematical expressions to generate deterministic computational outputs. Fourthly, the computing device provides restricted artificial intelligence assistance limited to predefined permissible categories without enabling unrestricted tutoring, external information retrieval, or non-deterministic interaction. Thereby enabling a controlled and restricted offline intelligent computational environment that reduces input errors and enhances computational reliability while maintaining compliance with controlled examination conditions.

The present invention relates to an Exam-Safe Offline Artificial Intelligence Scientific computing device/ System configured as a dedicated electronic hardware device for performing scientific computation with controlled artificial intelligence assistance in secure academic, examination, engineering, and professional environments. The invention is designed to combine the conventional functionality of a scientific calculator with embedded offline intelligence, while preventing unauthorized communication, unrestricted tutoring, external data access, or software misuse. The invention is therefore implemented as a technical hardware computing device having defined electronic architecture, secure firmware behavior, and bounded AI-assisted computational operation.

In one embodiment, the invention comprises a main computing device housing a processing unit, memory unit, display module, keypad input interface, power supply circuitry, AI inference module, and security control circuitry. The processing unit may be a low-power microcontroller, microprocessor, or system-on-chip configured to execute calculator logic, interface control, mathematical function processing, and offline AI routines. The memory unit may include read-only memory, flash memory, secure firmware storage, volatile working memory, and protected non-volatile data partitions. The display module may be an LCD, e-paper, OLED, or similar low-power visual display configured to present numerical outputs, expressions, function menus, restricted prompts, and controlled AI-generated responses.

The keypad input interface may include dedicated numeric keys, arithmetic operators, trigonometric function keys, logarithmic keys, statistical keys, algebraic function keys, navigation keys, confirmation keys, and one or more restricted-purpose intelligent-assistance keys. In one embodiment, the keypad is arranged in a familiar scientific-calculator format to maintain ease of use and compliance with exam expectations. The user enters an expression through the keypad, and the entered data are interpreted by the calculator control logic. In a standard mode, the expression is processed purely as a conventional calculator instruction. In an AI-assisted mode, the same expression may additionally be passed through a local interpretation engine for syntax validation, ambiguity reduction, and bounded assistance.

The processing unit is operatively connected to a mathematical computation engine configured to execute standard scientific functions including addition, subtraction, multiplication, division, fractions, roots, exponents, logarithms, trigonometric functions, inverse trigonometric functions, hyperbolic functions, permutations, combinations, matrix support where permitted, statistical calculations, and similar functions commonly found in a scientific calculator. The mathematical computation engine may be implemented using deterministic firmware routines, fixed libraries, pre-validated algorithms, and protected mathematical tables. In one embodiment, the results of the mathematical computation engine are always reproducible and deterministic under the same input conditions.

A significant aspect of the invention is the inclusion of an offline artificial intelligence inference module embedded within the hardware device. The offline AI inference module may comprise a compressed machine learning model, symbolic-processing model, pattern-recognition model, rules-based inference engine, or hybrid lightweight intelligence framework stored locally in device memory. The AI inference module is configured to execute only within device-authorized limits and does not require internet connectivity, remote cloud servers, or external applications. In one embodiment, the AI inference module is optimized for low-memory and low-power embedded execution so that the calculator remains portable, affordable, and suitable for long-duration use.

The offline AI inference module may perform one or more restricted intelligent functions including expression syntax checking, operator placement validation, parenthesis matching, formula pattern recognition, structured equation interpretation, limited algebraic expression understanding, symbol normalization, unit consistency checks where permitted, and bounded mathematical guidance. For example, if a user enters an incomplete or malformed expression, the AI module may detect the structural issue and prompt a correction message such as "check bracket closure" or "missing operator," rather than merely returning a generic error. In another embodiment, the AI module may identify that the entered function appears to require angle mode alignment or statistical mode selection and provide a restricted device prompt accordingly.

In one embodiment, the invention includes a restricted assistance policy engine that governs how the AI module behaves. This policy engine may be implemented in firmware and may define a set of approved assistance categories. Such categories may include expression verification, basic interpretation aid, allowed formula recall, permitted input correction, and limited structured hints. The policy engine prevents the AI module from operating as a general-purpose tutor, open-domain chatbot, internet search interface, unrestricted derivation generator, or communication terminal. Thus, the AI support is intentionally bounded to calculator-relevant assistance rather than educational overreach during examination use.

The invention further includes an exam-safe operating mode. In one embodiment, when exam-safe mode is activated, the device disables, omits, or logically isolates all external communication pathways. This may include Wi-Fi, Bluetooth, NFC, cellular communication, infrared communication, USB data exchange, wireless synchronization, audio transmission, file transfer, and similar interfaces. In some embodiments, such communication hardware may be physically absent. In other embodiments, where communication hardware is present for maintenance or institutional provisioning, it may be disabled through secure firmware lockout during exam mode. Thus, the device is rendered incapable of accessing remote data sources, online AI services, unauthorized stored notes, or peer devices while in restricted use.

In one embodiment, the invention includes a secure firmware architecture. The firmware may be digitally signed and verified at startup through a secure boot process. The processing unit may compare boot code or firmware hash values with protected reference values stored in secure memory. If tampering, corruption, or unauthorized firmware replacement is detected, the device may enter a lock state, restricted safe mode, or administrator-service-only state. This ensures that the computing device cannot be easily modified into an unauthorized communication or cheating device. In another embodiment, write access to firmware partitions is blocked during ordinary operation and may require authenticated service procedures.

The invention may also include tamper-evidence or tamper-detection features. For example, the housing may include seal-based detection, switch-based enclosure detection, conductive trace interruption sensing, or sensor-based physical intrusion detection. If unauthorized opening or hardware alteration is detected, the device may erase sensitive configuration data, disable AI-assisted mode, or permanently record a tamper flag in protected memory. Such measures increase trustworthiness for institutional or examination use and distinguish the invention from modified consumer devices.

In one embodiment, the device may provide dual-mode functionality, namely a standard calculator mode and a controlled AI-assisted mode. The standard calculator mode may be intended for strict examination environments and may expose only approved assistance levels. The controlled AI-assisted mode may be used during practice, self-learning, or institutional instruction while still remaining offline. Switching between modes may be achieved through password-based authorization, administrator menu selection, invigilator-issued access code, hardware slide switch, magnetic key, or firmware policy assignment. In another embodiment, the device may automatically revert to exam-safe restrictions after power cycle or after a time-limited session expires.

The display control subsystem may present outputs in a manner consistent with exam-safe design. In one embodiment, the display shows entered expressions, numerical answers, restricted prompts, and status indicators. The computing device may include a visible exam-safe indicator, such as a lock icon, LED, dedicated label, or persistent on-screen marker, showing that the device is operating under restricted examination conditions. This feature assists invigilators and institutions in visually verifying device state. In another embodiment, menu structures are deliberately limited, shallow, and deterministic to prevent hidden functionality or concealed data browsing.

The invention may optionally include a local expression history buffer for recent calculations. In one embodiment, the history buffer stores only a limited number of recent expressions and results, sufficient for normal calculator use but not sufficient to store notes, formulas, or textual study material. The history may be volatile and erased upon power-off in exam-safe mode. In another embodiment, persistent storage is segmented so that restricted-mode operation cannot access non-permitted data partitions, thereby preventing use of the device as a memory-based cheating aid.

In another embodiment, the invention may include a formula library under policy control. This library may store approved mathematical relations, constants, unit conversions, or examination-permitted formulas in a protected internal database. The policy engine determines whether such formulas can be shown in a given operational mode. For example, in a practice mode, the AI module may assist the user in selecting an appropriate formula from the permitted library; in a strict exam mode, only device-allowed constants and direct computation support may be available. This controlled architecture allows institutional customization without compromising security.

The power subsystem may include one or more batteries, rechargeable cells, or solar-assisted supply modules, together with voltage regulation and low-power management circuitry. Since the offline AI module is optimized for embedded execution, power consumption remains significantly lower than that of smartphones or general-purpose computing devices. In one embodiment, the processing unit selectively activates the AI inference block only when assistance is requested, thereby conserving power during ordinary calculator use. The device may further enter sleep or low-power standby states while preserving session continuity.

In one embodiment, the invention may optionally include a limited optical input module such as a low-resolution camera, scanner strip, or symbol capture sensor, provided such inclusion remains compatible with exam policy. Where enabled, the optical input module may be restricted to local symbol recognition or equation capture and may not be capable of general photography, communication, or unrestricted image storage. Recognized symbols may be passed through the local AI module for mathematical normalization and validation. In stricter embodiments intended for broader exam acceptance, the device may omit optical capture entirely and rely solely on keypad entry while retaining offline AI assistance for interpretation and error reduction.

The present invention may be manufactured as a compact handheld unit resembling a standard scientific calculator in size, ergonomics, and portability. The housing may be fabricated using molded polymer, reinforced composite, or equivalent lightweight materials. Internally, the processing board, memory components, display, keypad matrix, and power circuit are arranged to minimize size and cost. In one embodiment, the device is specifically optimized for affordability so that students, institutions, and examination boards can deploy it at scale.

In operation, a user powers on the computing device, enters a mathematical expression through the keypad, and selects the desired function. The processing unit interprets the input and sends it to the mathematical computation engine. If AI assistance is enabled within policy limits, the same input may additionally be evaluated by the offline AI inference module for expression integrity, operator correctness, and allowed contextual support. The resulting output is displayed to the user as a numerical answer, symbolic result, restricted prompt, or permitted guidance message. Throughout operation, the policy engine ensures that all behavior remains within approved exam-safe boundaries. Accordingly, the invention provides a hardware-integrated, secure, offline, AI-assisted scientific calculator that addresses the limitations of conventional calculators and unrestricted AI tools. Its uniqueness resides in the combination of scientific computation, embedded offline intelligence, secure exam-safe restrictions, limited assistance policy, and technical hardware enforcement within a dedicated handheld computing device suitable for academic and regulated use.

FIG. 2 illustrates a flow chart of a computer-implemented method for providing controlled offline scientific computation using an exam-safe offline artificial intelligence (AI)-enabled electronic computing device, according to an embodiment of the present invention. At the beginning, the process starts with Start / Power ON. Once the computing device is powered on, the system shows a boot screen and immediately performs a Secure Boot & Integrity Check. This stage is important because it verifies whether the firmware and internal system files are authentic and unmodified. If the integrity check fails, the calculator does not proceed normally; instead, it enters an Access Denied / Restricted Mode condition to prevent unsafe or unauthorized operation. If the verification is successful, the system proceeds to authenticated initialization.

After successful verification, the computing device enters the Power-ON and Initialization stage. In this stage, the device loads the firmware, initializes the required hardware components, and loads the approved internal resources needed for operation. These approved resources include the math libraries, the offline AI model, and the security rules. The math libraries support ordinary scientific calculation, the AI model enables restricted offline assistance, and the security rules define what is allowed and what is blocked in different usage modes. Once these internal modules are loaded, the computing device displays the home screen, indicating that the device is ready for controlled use.

The next phase is the Mode Selection stage. Here, the user or system selects the desired operating mode. The flowchart shows three logical possibilities in the electronic computing device: a normal calculator mode, an exam-safe restricted mode, and an offline AI practice mode. In practice, the most important distinction is whether the device is in a restricted examination condition or a broader offline assistance condition. In the exam-safe mode, wireless access, external connectivity, and unrestricted AI behavior are blocked, and only limited assistance is allowed. In the offline AI practice mode, the system may allow somewhat broader help, but it still remains offline and does not depend on the internet. After mode selection, the system enters the Ready for Input state.

In the User Stage, the user enters a mathematical expression through the keypad input. The entered data are captured and parsed by the internal system. This means the calculator or computing device does not immediately compute the answer blindly; instead, it first interprets the structure of the entered symbols, numbers, and operators. The parsed expression is then sent to the processing unit, which decides how the input should be handled according to the active operational mode and security rules.

The next phase is the Processing Stage, which forms the core of the working flow. First, the system checks whether Exam-Safe Mode is Active. If exam-safe mode is active, the system then determines whether AI assistance is allowed under the applicable restrictions. If limited AI support is permitted, the computing device applies restricted assistance rules. These rules ensure that the AI can only operate within safe boundaries.

At this stage, the system may perform tasks such as syntax checking, error or pattern detection, and the generation of a bounded hint or alert. These bounded outputs are restricted in nature and are not intended to provide unrestricted tutoring or full derivations. The processed input is then passed to the Math Computation Engine, which performs the actual calculation.

If exam-safe mode is not active, or if the device is in a non-restricted practice mode, the system can invoke the Offline AI Inference stage more flexibly. In that case, the AI may help validate the structure of the expression, identify possible user mistakes, or support interpretation before the result is computed. However, even in this broader mode, the AI still functions offline and within the internal device environment. After AI-supported validation or assistance, the expression is passed to the Math Computation Engine, where the final calculation is carried out using deterministic mathematical logic.

Once the computation is complete, the process moves to the Output Stage. Here, the result is transferred to the Result Display Control block, which formats and shows the output to the user. If needed, the system may also generate a voice or visual alert, such as a warning, correction prompt, or approved status message. Finally, the calculator displays the final output, which may include the answer and any permitted information allowed under the active policy. In exam-safe conditions, the displayed assistance remains strictly limited to approved output only.

After the result is shown, the flowchart enters the Post-Action Stage. At this point, the system checks whether the result should be saved to history, if such storage is allowed under the active rules. If allowed, the result is stored only in temporary limited storage rather than unrestricted memory. This is followed by an additional security check and UI update so that the device remains in a safe and synchronized operating state. If storage is not allowed, the process simply skips that step and continues securely.

Finally, the flowchart reaches the Shutdown Stage. Before the device powers off, the system checks whether session-related information should be cleared, especially in exam mode, where privacy and anti-misuse requirements are stricter. Once the appropriate cleanup is completed, the calculator proceeds to Power OFF. This ensures that the device shuts down in a secure manner without leaving behind unauthorized usable data for later misuse.

Overall, the flowchart shows that the invention works through a secure startup process, approved resource loading, controlled mode selection, structured user input capture, restricted or unrestricted offline AI-assisted processing depending on mode, deterministic mathematical computation, controlled result display, limited post-processing storage, and secure shutdown. The design ensures that the computing device remains intelligent, offline, secure, and suitable for examination-oriented use.

FIG. 3 illustrates an exam-safe offline artificial intelligence (AI)-enabled electronic computing device configured as a handheld scientific computation device, according to an embodiment of the present invention.

1. Scientific Computing Device

The Scientific Computing/Calculator Device is the main physical unit handled by the user. It serves as the outer hardware platform that houses the internal computational, memory, AI, security, and interface subsystems. In practical use, the computing device behaves like a conventional scientific calculator so that it remains familiar, portable, and suitable for academic and examination environments. Its overall function is to provide a compact and secure appliance through which the user can enter expressions, invoke scientific operations, obtain results, and access only bounded AI-supported assistance under controlled conditions.

2. Computing Device Display Section

The display section of the computing device presents the entered mathematical expression, intermediate prompts, operating mode information, and final computational result. In the illustrated figure, the display shows a sample equation, indicating that the device can visually render expressions before evaluation. Functionally, the display acts as the main feedback surface between the machine and the user. It allows the user to verify whether the entered symbols, numbers, and operators are correct before execution. In AI-assisted operation, it may also show restricted prompts such as input correction notices, structural warnings, or approved guidance messages, while in standard mode it behaves as a conventional calculator display.

3. Keypad Section

The keypad section is the physical input area through which the user enters digits, operators, functions, and execution commands. It includes the numerical keys and function keys required for scientific computation. The keypad is significant because it preserves the conventional usability of a scientific calculator while routing all user actions into the secure internal processing chain. Instead of acting like a free-form computer keyboard, it limits user interaction to calculator-relevant inputs, thereby helping maintain exam safety and preventing misuse as a general-purpose computing device.

4. Mode Control Button

The Mode Control Button allows the user, institution, or authorized controller to switch the device between predefined operational states, such as standard calculator mode and restricted AI-assisted mode. Its function is not merely cosmetic; it is tied to internal mode logic that determines which features are active and which restrictions are enforced. For example, in a strict examination state, this control may ensure that only permitted calculation and limited assistance functions are available, while broader offline support may be enabled in a learning or practice mode. Thus, the mode control mechanism is central to balancing usability with security.

5. Processing Unit

The Processing Unit is the primary control and execution core of the system. It manages instruction flow, supervises interaction between all modules, executes calculator firmware, coordinates memory access, and controls how user input is processed. When a user enters an expression, the processing unit determines whether the input should be sent only to the standard math engine or also to the offline AI inference subsystem under policy limits. It therefore acts as the central decision-making hardware that integrates standard scientific calculation with secure AI-enabled behavior.

6. Memory Unit

The Memory Unit stores the firmware, operational data, configuration settings, permitted model assets, and temporary processing information. It supports both persistent and runtime storage. Functionally, it ensures that the device has access to its operating instructions and the data needed for stable operation. It also provides the storage foundation for secure mode management, historical temporary calculations if allowed, and internal rule sets governing exam-safe behavior. The memory unit is especially important because it enables offline operation; the device does not need to fetch remote resources to function.

7. Firmware Storage

Firmware Storage holds the core embedded software that defines the calculator's behavior. This includes the startup logic, scientific calculation routines, user interface handling, security enforcement instructions, and the rules controlling AI assistance. Firmware storage is critical because it transforms the hardware into a purpose-specific calculator rather than a general programmable computer. In a secure design, this storage is protected against unauthorized alteration so that the device cannot easily be modified into a cheating tool or a network-enabled assistant.

8. Data Storage

Data Storage stores operational data used by the system during functioning. This may include approved constants, allowed formula resources, restricted configuration tables, local settings, temporary logs, and bounded session data. Its role is to support the machine's working environment without becoming an open notebook or unrestricted memory bank. In an exam-safe architecture, the data storage is controlled so that it cannot be used to keep unauthorized study material, communication content, or hidden applications.

9. Offline AI Inference Module

The Offline AI Inference Module is the intelligent subsystem that provides bounded artificial intelligence support without internet access. Its function is to analyze the user's mathematical input locally and assist in restricted ways, such as checking expression structure, identifying certain syntax issues, recognizing mathematical patterns, or giving approved computational guidance. The major importance of this module lies in the fact that it performs intelligent processing entirely on-device. This avoids dependence on cloud servers, reduces security risk, preserves privacy, and keeps the system suitable for offline and controlled examination use.

10. AI Model

The AI Model is the stored mathematical intelligence component inside the inference module. It represents the trained or configured internal logic used to detect patterns, interpret structured mathematical inputs, and support limited reasoning tasks. Functionally, the AI model may help identify whether an entered expression appears incomplete, structurally inconsistent, or unsuitable for the selected computational mode. It may also support recognized categories of assistance that are pre-approved by the device policy. The AI model is therefore the knowledge-bearing part of the offline intelligence subsystem.

11. Inference Engine

The Inference Engine is the execution layer that runs the AI model on live user input. While the AI model contains learned or encoded intelligence, the inference engine performs the actual computation that applies that intelligence to a present problem. In other words, when the user enters an equation, the inference engine processes that input through the model and produces a bounded output such as validation, pattern recognition, or a restricted suggestion. It is optimized for local embedded use so that intelligent processing can occur quickly and efficiently on low-power calculator hardware.

12. Math Computation Engine

The Math Computation Engine is the standard deterministic calculation block responsible for performing actual mathematical operations. It handles arithmetic, trigonometric, logarithmic, exponential, statistical, and other scientific functions supported by the calculator. This engine is the heart of the calculator's traditional computing capability. Even if AI assistance is disabled, the device can still work through this engine exactly as a scientific calculator. When AI is enabled, the AI subsystem may help validate or interpret the input, but the final execution of numerical or symbolic calculation is still governed by this controlled computation engine.

13. Exam-Safe Mode Control

The Exam-Safe Mode Control block governs whether the calculator is operating under restricted examination conditions. Its function is to enforce behavioral limitations appropriate for secure test environments. When active, it may restrict advanced assistance, disable non-permitted data access paths, reduce visible functionality to approved features, and ensure that the device behaves only within allowable boundaries. This component is essential because it gives the invention its exam-safe identity; it converts a powerful calculator into a compliant examination instrument.

14. Tamper Detection

Tamper Detection is responsible for identifying unauthorized physical or logical interference with the device. Its function may include sensing enclosure opening, firmware modification attempts, suspicious mode switching, or unauthorized internal access. If tampering is detected, the system may disable sensitive functions, record an alert state, or force the device into a safe restricted condition. This protects the integrity of the calculator and assures examination authorities that the unit has not been altered to enable cheating or hidden communication.

15. Secure Boot & Integrity Check

The Secure Boot & Integrity Check component verifies at startup that the firmware and critical system elements are authentic and unmodified. It establishes trust before the computing device / calculator becomes operational. Functionally, it may compare the installed firmware and critical resources against expected secure values. If mismatches are found, the device can prevent normal operation or enter a restricted fault state. This ensures that the calculator always runs approved embedded logic and not unauthorized software injected after manufacture or distribution.

16. Security Control Circuitry

The Security Control Circuitry is the overall protective management block that supervises security-sensitive behavior throughout the device. It integrates exam-safe mode control, tamper detection, and secure integrity verification into one coordinated framework. Its purpose is to ensure that all other subsystems operate inside approved boundaries. This circuitry is what distinguishes the invention from a normal smart gadget: it is built not only to compute, but also to enforce trust, compliance, and controlled use.

17. Power Management

The Power Management block handles the supply, regulation, and efficient use of electrical power throughout the computing device / calculator. It distributes energy to the processing unit, memory, display, AI subsystem, and security circuitry in a stable and optimized manner. Because the invention is intended to remain portable and low cost, effective power management is important. It ensures long battery life, stable operation during exams, and efficient use of power even when AI assistance is invoked.

18. Battery Unit

The Battery Unit is the energy source of the computing device / calculator. Its purpose is to provide portable, self-contained operation without dependence on external power. In an examination setting, this is especially important because the device must function reliably in different rooms and usage conditions. The battery supports all normal calculator operations as well as local AI processing, while remaining compact enough to preserve handheld portability.

19. Power Regulation

Power Regulation conditions and stabilizes the electrical supply before it is delivered to the internal modules. Different components may require different voltage levels or protection against fluctuations. The function of this block is to prevent unstable performance, computational errors, display issues, or security malfunctions caused by improper power flow. It therefore improves reliability and helps protect sensitive circuits such as the processor, memory, and security modules.

20. User Interface Control

The User Interface Control block governs the visible and physical interaction between the user and the computing device. It coordinates how keypad inputs are interpreted and how display outputs are shown. This block ensures that the machine responds consistently and predictably to user actions. In a secure computing device / calculator design, it also helps prevent ambiguous interaction styles by maintaining a calculator-like operating experience rather than a free-form computer-style interface.

21. Display Control

Display Control manages what appears on the screen and how it appears. It determines formatting, output visibility, expression rendering, prompts, warnings, and status signals. In restricted mode, display control can help ensure that only approved information is shown. For example, it can allow direct results and permitted notices while preventing unrestricted explanatory content if such content is not allowed in an exam environment.

22. Keypad Logic

Keypad Logic translates physical key presses into digital instructions usable by the processing unit and computation engine. It handles interpretation of numeric keys, function keys, execution commands, and control keys. This block ensures accurate entry handling and can also support debouncing, key sequence recognition, and mode-sensitive input interpretation. Its role is important because the correctness of all subsequent computation depends on faithful translation of user input.

23. Restricted I/O Interfaces

The Restricted I/O Interfaces block represents the system's deliberately limited external input/output capability. Its role is to ensure that the device does not operate as a communication terminal or programmable computer. Instead of offering broad connectivity, these interfaces are constrained so that the calculator remains a dedicated secure appliance. This restriction is one of the major technical features supporting exam-safe usage.

24. No Wireless Comms

The No Wireless Comms condition means the device is designed so that wireless communication is unavailable, disabled, or blocked in restricted use. This prevents internet access, remote assistance, peer-device messaging, and unauthorized data exchange. Functionally, it protects examination integrity by ensuring the calculator cannot connect to online AI systems, websites, cloud databases, or other users during operation.

25. No External Data Access

The No External Data Access condition ensures that the device cannot fetch outside files, notes, formula banks, or other unauthorized materials from removable media or connected systems during restricted use. This prevents the calculator from becoming a hidden storage or retrieval platform. It reinforces the principle that all available functionality must be internally controlled and pre-approved.

26. No Programming

The No Programming condition means that the device cannot be freely reprogrammed by the end user in examination mode. This prevents custom scripts, hidden apps, stored procedures, or user-defined exploit logic from being introduced into the calculator. Its function is to keep the machine deterministic, predictable, and trustworthy, which is crucial for regulatory acceptance in examinations.

27. Functional Arrows / Interconnections

The arrows between the components indicate the direction of operational communication and control flow. For example, user input enters through the calculator and keypad pathway, is processed by the computation and AI-related blocks, checked by the security architecture, and then returned to the display under controlled conditions. These interconnections show that the invention is not a set of isolated modules; rather, it is an integrated hardware system in which each block supports the others to achieve secure, offline, intelligent scientific computation.

Taken together, the diagram describes a hardware-based secure scientific calculator that combines standard mathematical computation with restricted offline AI assistance, all under strong security and examination-control mechanisms. The calculator receives input from the user, processes it through deterministic math logic, optionally supplements it with bounded local AI reasoning, checks integrity and operating restrictions through the security circuitry, powers everything through controlled power management, and returns the result through a managed user interface. The overall objective is to provide a more intelligent scientific calculator without sacrificing examination safety, device integrity, or offline independence.

FIG. 4 illustractes a logic layer architecture of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device, according to an embodiment of the present invention.

The Logic Layer Diagram represents the internal logical organization of the Exam-Safe Offline AI Scientific computing/calculator device. It shows how the software-controlled functions of the invention are arranged in multiple layers over a dedicated processor and embedded system foundation. This layered structure is important because it separates user interaction, mathematical computation, artificial intelligence processing, security control, and hardware-level firmware functions into clearly defined operational domains. Such separation improves reliability, maintainability, security, and examination compliance by ensuring that each logical layer performs a specific role while remaining coordinated with the others.

At the top of the architecture is the User Interface Layer. This layer is responsible for all visible and direct interaction between the user and the calculator/computing device. It includes display management and keypad input handling. Its primary function is to receive user-entered mathematical expressions, commands, and control selections through the keypad, and to present outputs, prompts, warnings, and status information through the display. This layer ensures that the device behaves like a conventional calculator from the user’s perspective, while still acting as the entry and exit point for the deeper processing layers below. It provides a structured and controlled interface rather than an open computing interface, thereby supporting the exam-safe nature of the invention.

Below the user interface layer is the Calculator Engine Layer. This layer performs the core scientific calculator operations. It includes the Math Computation Engine and Expression Parsing / Validation functions. The math computation engine executes deterministic mathematical functions such as arithmetic, trigonometric operations, logarithms, exponents, roots, and statistical calculations. The expression parsing and validation function checks whether the user's input is syntactically correct and mathematically processable before the actual computation takes place. In practical terms, this layer ensures that the invention can always operate as a proper scientific calculator even when advanced AI-assisted features are not being invoked. It acts as the conventional computational backbone of the system.

The next layer is the Offline AI Inference Layer, which provides the invention's embedded artificial intelligence capability. This layer contains the Mathematical AI Model and the Inference Logic & Validation function. The mathematical AI model stores the locally embedded intelligence used for bounded mathematical assistance. The inference logic applies that intelligence to live user input in order to recognize structural patterns, identify possible input mistakes, and support limited reasoning tasks. Because this layer operates entirely offline, it does not depend on internet access, remote servers, or cloud inference. Its purpose is to enhance the calculator's usability and intelligence while keeping the device secure, private, and suitable for examination conditions.

Beneath the AI layer is the Security Policy Layer, which is one of the most important layers in the invention. It includes Exam-Safe Operation Rules, Tamper / Integrity Checks, and Exam-Safe Restrictions. The function of this layer is to define and enforce the behavioral boundaries within which all other layers must operate. For example, it determines whether AI assistance is permitted in the current mode, what type of prompts may be shown, whether certain data can be stored, and whether restricted exam-safe settings are active. It also monitors integrity-related aspects such as tamper detection and rule compliance. This layer ensures that the calculator remains trustworthy and that intelligent assistance never exceeds the limits intended for examination or regulated use.

At the bottom of the logical stack is the Firmware Layer. This layer includes the OS Kernel & Core Logic and Hardware Control Drivers. In the context of this invention, the firmware layer serves as the foundational software that directly controls the embedded hardware. The kernel and core logic establish the basic operating behavior of the device, while the hardware control drivers manage low-level interaction with the display, keypad, processor, memory, power system, and security circuitry. This layer is essential because it translates the higher-layer logical functions into actual hardware operations. It also supports secure startup behavior, reliable device control, and the predictable operation required for examination-safe hardware products.

All of these logical layers operate on top of the Dedicated Processor, Embedded System base shown at the bottom of the diagram. This means that the invention is not intended to run as a general-purpose software application on a smartphone, computer, or unrestricted smart device. Instead, the entire layered architecture is implemented on purpose-built embedded hardware. This dedicated hardware foundation is a major technical feature because it supports low-power operation, stronger security, fixed-function reliability, and improved patent positioning as a technical hardware invention rather than mere software.

From a functional perspective, the layered arrangement works in a top-down and bottom-up manner. When the user enters an expression, the User Interface Layer captures it and passes it downward. The Calculator Engine Layer parses and validates the expression and prepares it for scientific computation. If bounded AI support is permitted, the Offline AI Inference Layer analyzes the input and may provide validation or limited reasoning assistance. At the same time, the Security Policy Layer supervises whether the requested assistance or operation is allowed under current rules. All of this is executed through the underlying Firmware Layer, which coordinates the actual hardware behavior through the embedded processor and control drivers.

Finally, the result or permitted output is returned upward to the user interface for display.

An important advantage of this layered logic design is that it provides modularity and controlled isolation between functions. The user interface does not directly control the AI in an unrestricted way; instead, the AI works through controlled inference logic. Similarly, the AI does not directly override security rules; it remains subordinate to the security policy layer. The calculator engine also remains a distinct deterministic computation layer, ensuring that the invention preserves the reliability of a normal scientific calculator. This modularity increases safety, simplifies validation, and makes the system easier to audit for patent, manufacturing, and institutional approval purposes.

The software and logic layer diagram therefore demonstrates that the invention is not simply an AI calculator app, but a structured embedded architecture in which each function is layered with a clear technical purpose. The user interface manages interaction, the calculator engine performs scientific computation, the offline AI layer adds bounded intelligence, the security policy layer enforces exam-safe restrictions, and the firmware layer provides hardware-level control. Together, these layers create a secure, reliable, intelligent, and examination-compliant scientific calculator platform.

FIG. 5 illustrates an external device view of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device configured as a handheld scientific computation device, according to an embodiment of the present invention.

FIG. 6 illustractes an Offline AI Processing Flow Diagram of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device, according to an embodiment of the present invention. The Offline AI Processing Flow Diagram illustrates how user input is intelligently processed in a controlled and secure manner. The process begins when the user enters a mathematical expression using the device keypad. This input is then forwarded to the Parse Input stage, where the system interprets the structure of the expression, identifies operators, variables, and functions, and prepares it for further processing. This step ensures that the input is in a usable format before any computation or analysis takes place.

After parsing, the expression is passed to the Offline AI Model Validation and Assistance stage. Here, the embedded AI system analyzes the expression locally without any internet access. The AI checks for structural correctness, recognizes patterns, and evaluates whether the input contains any syntax errors or inconsistencies. This intelligent validation enhances accuracy and reduces user mistakes.

The process then reaches a decision point: Detect Error or Pattern. If an issue is detected, the device provides Syntax Checks or Hint Alerts, helping the user correct the input. If no error is found, the expression is sent to the Mathematical Computation module/Engine, where the actual calculation is performed. Finally, the system proceeds to Result Generation and Display, presenting the correct output along with any permitted guidance.

FIG. 7 illustractes Secure Boot and Integrity Verification Flow Diagram of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device, according to an embodiment of the present invention. The Secure Boot and Integrity Verification process of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device ensures that the device operates only with authentic and unmodified firmware. The process begins with Power ON, after which the system initiates the Perform Secure Boot stage. During this stage, the device loads a trusted bootloader and prepares the system for verification. This step establishes a secure foundation before any operational software is executed.

Next, the system proceeds to Verify Firmware Integrity, which is a critical decision point. Here, the device checks whether the firmware stored in memory matches its original, trusted version using techniques such as hash comparison or digital signature verification. If the firmware is found to be altered or corrupted, the process follows the Integrity Check Failed path. In this case, the device enters a Safe or Locked Mode, restricting normal functionality to prevent misuse, unauthorized access, or potential cheating in exam conditions.

If the firmware passes verification, the system proceeds with Integrity Check Succeeded, allowing the device to Load Secure Firmware, AI Model, and Data. Only verified and approved components are loaded into the system. Finally, the device enters Normal Operation, where it performs standard calculations with controlled offline AI assistance. This ensures both security and reliability in all operating conditions.

FIG. 8 illustractes a flow chart of a computer-implemented method for providing controlled offline scientific computation using an exam-safe offline artificial intelligence (AI)-enabled electronic computing device, according to an embodiment of the present invention. In one embodiment, a computer-implemented method for providing controlled offline scientific computation is executed by the processing unit (102) of the electronic computing device (100), wherein the method comprises a sequence of hardware-controlled and firmware-executed operations enabling deterministic computation with bounded artificial intelligence assistance. The method is executed through coordinated interaction between the processing unit, memory unit, keypad input interface, mathematical computation module, offline AI inference module, security control circuitry, and display module, as illustrated in the operational flow of Fig. 6. The implementation of each step is described in detail below.

At step 802, the method comprises initializing, by a processing unit, the computing device through execution of a secure boot process, including verifying integrity of firmware stored in a memory unit. In one embodiment, upon power-on or system reset, the processing unit (102) is configured to initiate a secure initialization process including a secure boot procedure for verifying firmware integrity. The secure boot process comprises retrieving firmware integrity data stored in a secure memory region and computing a hash value of the executable firmware using a cryptographic hashing function. The computed hash value is then compared with a corresponding reference value stored in the secure memory. In response to determining that the computed hash value matches the reference value, the processing unit proceeds with normal system initialization. Conversely, in response to detecting a mismatch between the computed hash value and the stored reference value, the system inhibits initialization and transitions the computing device into a restricted operational state. This secure initialization mechanism ensures that only authenticated firmware is executed, thereby preventing unauthorized modification and ensuring deterministic and reliable system behavior.

At step 804, the method comprises accessing, by the **processing** unit, predefined mathematical function libraries and a locally stored artificial intelligence model from the memory unit. In one embodiment, following successful verification of firmware integrity, the processing unit (102) is configured to perform resource loading and system initialization operations. The processing unit loads predefined mathematical function libraries from the memory unit (104) and further loads a locally stored artificial intelligence model (120) into accessible execution memory for use by the offline artificial intelligence inference module (112). The processing unit is further configured to initialize system modules including a keypad input interface controller associated with the keypad input interface (106), a display controller associated with the display module (108), the security control circuitry (114), and the offline artificial intelligence inference module (112). Upon completion of initialization, the computing device transitions into a ready state configured to receive user input and perform controlled computational operations.

At step 806, the method comprises receiving, via. a keypad input interface, a structured mathematical expression entered by a user. Upon receiving the input, the processing unit (102) is configured to convert each keypress into a corresponding symbolic token representing numerical values, operators, or functions. The processing unit is further configured to organize the generated tokens into a structured representation, including an expression tree or a sequential token stream arranged according to operator precedence rules. The structured representation is temporarily stored in a working memory associated with the memory unit (104) for subsequent processing. Such structured representation facilitates deterministic evaluation by the mathematical computation module (110) and enables accurate syntax validation and interpretation by the offline artificial intelligence inference module (112).

At step 808, the method comprises selecting, by a mode control interface, an operational mode including one of a standard computation mode and an exam-safe restricted mode. In one embodiment, the method includes selecting an operational mode using the mode control interface (116). Upon activation of the exam-safe restricted mode, the security control circuitry (114) is configured to enforce controlled operation of the computing device by disabling or isolating communication interfaces, restricting access to non-permitted functions, and governing execution of the offline artificial intelligence inference module (112) through a policy control mechanism. The policy control mechanism ensures that only predefined permissible assistance functions are executed while preventing unrestricted operations. Further, the method includes automatically enforcing the exam-safe restricted mode upon system restart or after expiration of a predefined time interval, thereby maintaining consistent compliance with controlled operational requirements.

At step 810, the method comprises processing, by the processing unit, the structured mathematical expression using a mathematical computation module. In one embodiment, the processing unit (102) is configured to execute the mathematical computation module (110) to process the structured mathematical expression. The structured expression is evaluated using deterministic algorithms to ensure consistent and reproducible computation. The mathematical computation module (110) performs required operations using predefined function libraries, lookup tables, and numerical evaluation routines stored in the memory unit (104). During execution, intermediate values generated in the course of computation are temporarily stored in a working memory associated with the memory unit. Upon completion of evaluation, the computation module generates a deterministic result corresponding to the structured mathematical expression, wherein the result is reproducible for identical inputs under the same operational conditions.

At step 812, the method comprises evaluating, by an offline artificial intelligence (AI) inference module executed by the processing unit, the structured mathematical expression to perform at least one of: syntax validation, operator placement verification, expression structure interpretation, and bounded input correction. In one embodiment, the inference module (122) is configured to parse the structured expression into syntactic components and to perform analytical operations including syntax validation based on operator placement rules, structural verification such as bracket matching, and expression interpretation. The inference module is further configured to perform bounded input correction to identify and rectify incomplete or malformed expressions within predefined constraints. The evaluation is performed using a compressed artificial intelligence model (120) stored in the memory unit (104), wherein the model comprises quantized parameters, reduced precision data representations, and a pruned architecture optimized for embedded execution. Such implementation ensures bounded computational complexity, predictable inference time, and low power consumption during operation of the computing device.

At step 814, the method comprises restricting, by a security control circuitry, execution of non-permitted functions and external communication pathways when the computing device operates in the exam-safe restricted mode. In one embodiment, during operation of the computing device, the security control circuitry (114) is configured to continuously monitor system integrity. The method includes detecting one or more security events including physical intrusion, firmware modification, or unauthorized access to hardware or system resources. In response to detection of any such event, the system is configured to transition into a restricted operational state, wherein the offline artificial intelligence inference module (112) is disabled, access to stored data in the memory unit (104) is restricted, and execution of computational functions is prevented or limited. Further, when the computing device operates in the exam-safe restricted mode, the security control circuitry (114) is configured to disable or isolate external communication interfaces to prevent any data exchange with external devices or networks. Such continuous monitoring and responsive control ensure secure operation of the computing device and maintain compliance with controlled usage conditions.

At step 816, the method comprises generating, by the mathematical computation module, a deterministic computational result based on a validated structured mathematical expression.

At step 818, the method processes displaying, by a display module, the deterministic computational result along with any permitted restricted assistance output. The offline AI inference module operates exclusively on locally stored data and is constrained to predefined permissible assistance functions in the exam-safe restricted mode, thereby enabling a controlled and restricted offline computation process compliant with examination conditions. In one embodiment, following computation and validation of the structured mathematical expression, the mathematical computation module (110) generates a deterministic computational result. The generated result is transmitted by the processing unit (102) to the display module (108) for presentation to the user. The display module (108) is configured to present the computed result along with any permitted restricted assistance output generated by the offline artificial intelligence inference module (112). The assistance output is limited to predefined permissible categories, including validation prompts or structured guidance, and excludes generation of unrestricted explanatory content or open-ended responses. Such controlled output presentation ensures clarity of results while maintaining compliance with restricted operational conditions.

In one embodiment, the secure boot process further comprises comparing firmware integrity values with stored reference values and inhibiting system initialization upon detection of mismatch.

In one embodiment, the method further comprises detecting, by a tamper detection module, at least one of physical intrusion, firmware modification, and unauthorized access, and transitioning the computing device into a restricted operational state, wherein the restricted operational state comprises at least one of: disabling the offline AI inference module, restricting access to stored data, and preventing execution of computational functions.

The method further comprises partitioning, by the memory unit, stored data into secure partitions including firmware storage partition, restricted data storage partition, and volatile working memory partition. In one embodiment, the firmware storage partition is configured to store authenticated executable firmware, while the restricted data storage partition is configured to store controlled data accessible only under authorized conditions enforced by the security control circuitry (114). The volatile working memory partition is configured to temporarily store runtime data generated during operation of the computing device. Access to the restricted data storage partition is permitted only upon satisfaction of predefined authorization conditions, thereby preventing unauthorized data access or modification. Further, when the computing device operates in the exam-safe restricted mode, the processing unit (102) is configured to automatically erase data stored in the volatile working memory upon power-off. Such memory management ensures that sensitive data does not persist beyond an operational session and prevents misuse of stored information.

In one embodiment, the method further comprises erasing, by the processing unit, data stored in the volatile working memory upon power-off when operating in the exam-safe restricted mode.

In one embodiment, the method further comprises evaluating the structured mathematical expression by the offline artificial intelligence inference module comprises executing a compressed artificial intelligence model having reduced computational complexity. The compressed artificial intelligence model comprises at least one of quantized parameters, reduced precision data representation, and pruned model architecture.

In one embodiment, the method further comprising enforcing, by the security control circuitry, disabling or isolation of external communication interfaces during the exam-safe restricted mode. The method includes controlling execution of the offline artificial intelligence inference module (112) using a policy control mechanism stored in the memory unit (104). The policy control mechanism is configured to define and enforce permissible operations of the inference module during execution. In accordance with the defined policy, the inference module is permitted to perform limited assistance operations including expression validation, syntax error indication, operator correction prompting, and provision of structured input guidance. Concurrently, the policy control mechanism restricts execution of non-permitted functions, including generation of step-by-step derivations, unrestricted explanatory outputs, and open-ended interaction. By enforcing such controlled execution, the policy control mechanism ensures that the artificial intelligence inference module operates within predefined boundaries, thereby maintaining bounded assistance behavior and ensuring compliance with controlled usage conditions.

In one embodiment, the method further comprises automatically re-enabling the exam-safe restricted mode upon system restart or after a predefined time interval.

Some exemplary embodiments illustrating applications of the present invention are described below:

The present invention offers a significant advancement over both conventional scientific calculators and unrestricted artificial-intelligence-based mathematical tools by combining the benefits of secure scientific computation, embedded offline intelligence, and examination-safe architecture within a single dedicated hardware platform. One of the primary advantages of the invention is that it enables users to access intelligent computational support without requiring internet connectivity. This makes the device highly reliable in environments where communication networks are unavailable, prohibited, unstable, or undesirable. Unlike smartphone applications and cloud-based math solvers, the invention performs its approved intelligent functions locally, thereby reducing latency, improving privacy, and ensuring uninterrupted operation in controlled examination conditions.

Another major advantage of the invention is its exam-safe operating design. Existing AI-based mathematical assistance tools are generally considered unsuitable for regulated examinations because they may connect to the internet, communicate externally, store unauthorized content, or provide unrestricted tutoring assistance. The present invention overcomes this problem by implementing a dedicated secure hardware architecture in which communication pathways, external access channels, and unauthorized programmability are disabled, restricted, or omitted. As a result, the device can be positioned as a legitimate examination-oriented tool rather than a general smart device. This improves trust among institutions, exam boards, invigilators, and regulatory authorities.

A further advantage lies in the invention's ability to provide controlled artificial intelligence assistance rather than unrestricted generative output. Conventional calculators merely execute numerical commands and return results, offering no meaningful support when the user enters an incomplete expression, misplaced operator, invalid structure, or mode mismatch. In contrast, the present invention can intelligently identify syntax-level issues, check the structural validity of expressions, recognize certain types of user input errors, and provide bounded prompts or approved guidance. This reduces user frustration, lowers calculation mistakes, and improves operational efficiency while still remaining within controlled limits. The invention therefore enhances usability without crossing into impermissible tutoring behavior.

The invention also offers the advantage of dual utility, meaning it can function both as a traditional scientific calculator and as a controlled offline AI-assisted calculator depending on the selected operating mode or institutional policy. This makes the device highly versatile. In examination mode, it can behave as a secure and restricted calculator with only approved assistance enabled. In learning, training, or practice environments, broader but still offline intelligent support may be made available. This dual-purpose design allows students and professionals to become familiar with a single device that can adapt to both study and formal evaluation contexts, reducing the need to purchase and learn multiple separate tools.

An important technical advantage of the invention is its hardware-integrated security and integrity framework. By incorporating secure boot mechanisms, firmware validation, tamper detection, and controlled memory access, the device provides a higher level of trustworthiness than standard programmable or technically advanced computing device / calculators. This reduces the risk of unauthorized firmware replacement, hidden software injection, illicit stored content, or hardware modification. For institutions, this means the computing device / calculator can be verified and trusted as a standardized examination appliance. For users, it means stable and predictable performance. For manufacturers and patentability purposes, it demonstrates a concrete technical effect beyond software alone.

The present invention further offers the advantage of low-power operation with intelligent functionality. Unlike smartphones, tablets, or laptops that consume substantial energy and rely on complex operating systems, the invention is built on an optimized embedded architecture. The offline AI inference module can be selectively activated when needed, while ordinary scientific calculations continue through efficient deterministic processing. This results in improved battery life, reduced thermal issues, and a practical portable form factor. Such power efficiency is particularly beneficial in long examination sessions, classroom use, field calculations, and professional work settings where charging access may be limited.

Another advantage is the invention’s affordability and scalability. Since it is designed as a compact embedded hardware system using optimized local models rather than heavy cloud infrastructure, the device can be manufactured at lower cost than general-purpose smart devices. This makes it more accessible to students, schools, colleges, examination boards, training centers, and technical institutions. The invention therefore has strong practical value not only as a premium specialized device, but also as a scalable educational technology solution suitable for large deployment in academic systems.

The invention also improves data privacy and user confidentiality. Because the computational intelligence operates locally and does not require uploading expressions, questions, or usage patterns to remote servers, the risk of data leakage, user profiling, cloud dependency, or external monitoring is significantly reduced. This is especially relevant in educational and examination contexts, where problem statements, user performance, and institutional procedures may need to remain confidential. Offline functionality ensures that sensitive data stay within the device and do not leave the user's immediate control.

A further advantage is that the invention preserves the familiar ergonomics and discipline of a scientific calculator. Users interact through a structured keypad and a controlled display rather than through a distracting open-ended interface. This reduces cognitive overload, discourages misuse, and ensures that the device remains focused on mathematical work. The calculator-like form also makes the invention easier to accept in traditional academic environments, as it does not appear or function like a general communication device. This balance of familiarity and innovation is a significant practical strength.

The invention additionally offers an advantage in terms of reduced human error and improved computational confidence. Many mistakes in scientific calculation arise not because the user lacks mathematical understanding, but because of keypad entry mistakes, bracket mismatches, operator omissions, or confusion regarding modes and expression formatting. The bounded AI support of the invention helps identify such issues before the final computation is executed. This leads to greater accuracy, better user confidence, and fewer avoidable errors in both educational and professional tasks. From a broader technological perspective, the invention provides an important advantage by bridging the gap between traditional calculators and modern AI tools. Conventional calculators are secure but unintelligent. AI apps are intelligent but insecure for examination use. The present invention creates a middle path: a calculator that is both intelligent and controlled. This fills a longstanding unmet need in education and technical practice, where users increasingly expect smart assistance but institutions still demand fairness, reliability, and strong operational boundaries.

Finally, the invention is framed as a technical hardware solution rather than a mere mathematical or software concept. Its value lies in the integrated combination of embedded offline AI, secure system architecture, restricted assistance policy, and exam-safe mode enforcement. This makes the invention suitable not only for patent protection but also for product differentiation in a growing market where institutions and learners seek trustworthy intelligent devices. The invention therefore stands out as a practical, secure, innovative, and commercially meaningful advancement in scientific calculator technology.

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. An exam-safe offline artificial intelligence (AI)-enabled electronic computing device (100), comprising:

a processing unit (102) configured to control operation of the computing device and execute stored instructions;

a memory unit (104) operatively coupled to the processing unit, the memory unit comprising:

a firmware storage storing authenticated executable firmware, and

a data storage storing predefined mathematical function libraries and a locally stored artificial intelligence model;

a keypad input interface (106) comprising a plurality of physical keys configured to receive structured mathematical expressions;

a display module (108) operatively coupled to the processing unit and configured to display at least one of the structured mathematical expressions, computational outputs, and restricted assistance prompts;

a mathematical computation module (110) executed by the processing unit and configured to perform deterministic scientific computations including arithmetic, trigonometric, logarithmic, algebraic, and statistical operations based on the structured mathematical expressions;

an offline artificial intelligence (AI) inference module (112) stored in the memory unit and executable by the processing unit, the offline AI inference module (112) comprising:

an artificial intelligence model (120), and

an inference module (122) configured to process the structured mathematical expressions to perform at least one of:

- syntax validation,
- operator placement verification,
- expression structure interpretation, and
- bounded input correction;

a security control circuitry (114) operatively coupled to the processing unit, the security control circuitry (114) comprising:

a secure boot module (124) configured to authenticate the firmware prior to execution,

a tamper detection module (126) configured to detect unauthorized modification of the computing device, and

an exam-safe mode control module (128);

a mode control interface (116) configured to selectively switch the computing device between a standard computation mode and an exam-safe restricted mode; and

a power management circuitry (118) configured to supply regulated power to the processing unit and one or more associated components;

wherein, when the computing device (100) operates in the exam-safe restricted mode:

the exam-safe mode control module disables or restricts external communication interfaces and external data access pathways;

the offline AI inference module is constrained to execute only a predefined set of permitted assistance functions stored in the memory unit;

the mathematical computation module executes only validated structured mathematical expressions to generate deterministic computational outputs; and

the computing device provides restricted artificial intelligence assistance limited to predefined permissible categories without enabling unrestricted tutoring, external information retrieval, or non-deterministic interaction;

thereby enabling a controlled and restricted offline intelligent computational environment that reduces input errors and enhances computational reliability while maintaining compliance with controlled examination conditions.

2. The computing device as claimed in claim 1, wherein the tamper detection module (126) is configured to detect at least one of enclosure opening, firmware alteration, or unauthorized hardware access, and in response, trigger a restricted operational state.

wherein the restricted operational state comprises at least one of:

- disabling the offline artificial intelligence inference module,
- restricting access to stored data, and
- preventing normal computational operation.

3. The computing device as claimed in claim 1, wherein the memory unit (104) comprises segmented memory partitions including:

- a firmware storage partition,
- a restricted data storage partition, and
- a volatile working memory partition,

and wherein access to the restricted data partition is controlled by the security control circuitry,

wherein the volatile working memory partition is configured to automatically erase stored data upon power-off when the computing device operates in the exam-safe restricted mode.

4. The computing device as claimed in claim 1, wherein the artificial intelligence model (120) is a compressed model optimized for embedded execution, comprising at least one of:

- quantized parameters,
- reduced precision representations, and
- pruned model architecture.

wherein the artificial intelligence model (120) is configured to

receive a structured mathematical expression comprising tokenized elements arranged as an expression tree or a precedence-based token sequence,

perform feature extraction by identifying syntactic and structural attributes including operator sequences, operand relationships, bracket structures, and function-argument mappings, and generate model outputs comprising classification scores, pattern recognition results, or error likelihood indicators associated with the structured mathematical expression,

wherein the inference module (122) is configured to utilize outputs of the artificial intelligence model (120) to perform syntax validation, operator placement verification, expression structure interpretation, and bounded input correction.

5. The computing device as claimed in claim 1, wherein the mode control interface (116) comprises at least one of:

- a password-based access mechanism,
- an administrator-controlled configuration, and
- a hardware-based switching element,

for enforcing transition between the standard computation mode and the exam-safe restricted mode,

wherein the exam-safe restricted mode is configured to be automatically re-enabled upon device restart or after a predefined session interval.

6. The computing device as claimed in claim 1, wherein the security control circuitry (114) is configured to disable or isolate communication hardware interfaces including at least one of wireless communication modules, data ports, and external connectivity channels during the exam-safe restricted mode.

7. The computing device as claimed in claim 1, wherein the offline AI inference module (112) is governed by a policy control mechanism stored in the memory unit, the policy control mechanism defining a set of permissible assistance functions executable in the exam-safe restricted mode.

wherein the permissible assistance functions comprise at least one of:

- expression validation,
- syntax error indication,
- operator correction prompts, or
- structured input guidance,

while preventing generation of step-by-step derivations or unrestricted explanatory outputs.

8. The computing device as claimed in claim 1, further comprising a secure boot verification mechanism configured to compare firmware integrity values with stored reference values prior to system initialization, and to inhibit normal operation upon detection of mismatch.

9. A computer-implemented method for providing controlled offline scientific computation using an exam-safe offline artificial intelligence (AI)-enabled electronic computing device, the method comprising:

initializing, by a processing unit, the computing device through execution of a secure boot process, including verifying integrity of firmware stored in a memory unit;

accessing, by the **processing** unit, predefined mathematical function libraries and a locally stored artificial intelligence model from the memory unit;

receiving, by a keypad input interface, a structured mathematical expression;

selecting, by a mode control interface, an operational mode including one of a standard computation mode and an exam-safe restricted mode;

processing, by the processing unit, the structured mathematical expression using a mathematical computation module;

evaluating, by an offline artificial intelligence (AI) inference module executed by the processing unit, the structured mathematical expression to perform at least one of:

- syntax validation,
- operator placement verification,
- expression structure interpretation, and
- bounded input correction;

restricting, by a security control circuitry, execution of non-permitted functions and external communication pathways when the computing device operates in the exam-safe restricted mode;

generating, by the mathematical computation module, a deterministic computational result based on a validated structured mathematical expression; and

displaying, by a display module, the deterministic computational result along with any permitted restricted assistance output,

wherein, the offline AI inference module operates exclusively on locally stored data and is constrained to predefined permissible assistance functions in the exam-safe restricted mode, thereby enabling a controlled and restricted offline computation process compliant with examination conditions.

10. The method as claimed in claim 9, wherein the secure boot process further comprises comparing firmware integrity values with stored reference values and inhibiting system initialization upon detection of mismatch.

11. The method as claimed in claim 9, further comprising detecting, by a tamper detection module, at least one of physical intrusion, firmware modification, and unauthorized access, and transitioning the computing device into a restricted operational state,

wherein the restricted operational state comprises at least one of:

- disabling the offline AI inference module ,
- restricting access to stored data, and
- preventing execution of computational functions.

12. The method as claimed in claim 9, further comprising partitioning, by the memory unit, stored data into secure partitions including firmware storage partition, restricted data storage partition, and volatile working memory partition.

13. The method as claimed in claim 12, further comprising erasing, by the processing unit, data stored in the volatile working memory upon power-off when operating in the exam-safe restricted mode.

14. The method as claimed in claim 9, wherein evaluating the structured mathematical expression by the offline artificial intelligence inference module comprises executing a compressed artificial intelligence model having reduced computational complexity.

wherein the compressed artificial intelligence model comprises at least one of quantized parameters, reduced precision data representation, and pruned model architecture.

15. The method as claimed in claim 9, further comprising enforcing, by the security control circuitry, disabling or isolation of external communication interfaces during the exam-safe restricted mode.

16. The method as claimed in claim 9, further comprising controlling, by a policy module, execution of the offline artificial intelligence inference module to allow only predefined assistance functions,

wherein the predefined assistance functions comprise at least one of:

- expression validation,
- syntax error indication,
- operator correction prompting, and
- structured input guidance,

while preventing generation of unrestricted explanatory outputs.

17. The method as claimed in claim 9, further comprising automatically re-enabling the exam-safe restricted mode upon system restart or after a predefined time interval.

Dated this 21st day of April 2026

Signature

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

ABSTRACT

AN EXAM-SAFE OFFLINE ARTIFICIAL INTELLIGENCE (AI)-ENABLED ELECTRONIC COMPUTING DEVICE AND METHOD THEREOF

The present invention discloses an exam-safe offline artificial intelligence (AI)-enabled electronic computing device configured as a handheld scientific computation device and its method. The computing device (100) comprises a processing unit (102), a memory unit (104), a keypad input interface (106), a display module (108), a mathematical computation module (110), an offline artificial intelligence (AI) inference module (112), a security control circuitry (114), a mode control interface (116), and a power management circuitry (118). The mathematical computation module (110) performs deterministic scientific computations based on the structured mathematical expressions. The offline AI inference module comprises an artificial intelligence model (120), and an inference module (122). The security control circuitry comprises a secure boot module (124), a tamper detection module (126), and an exam-safe mode control module (128). The mode control interface (116) is configured to selectively switch the computing device between a standard computation mode and an exam-safe restricted mode.

FIG. 1

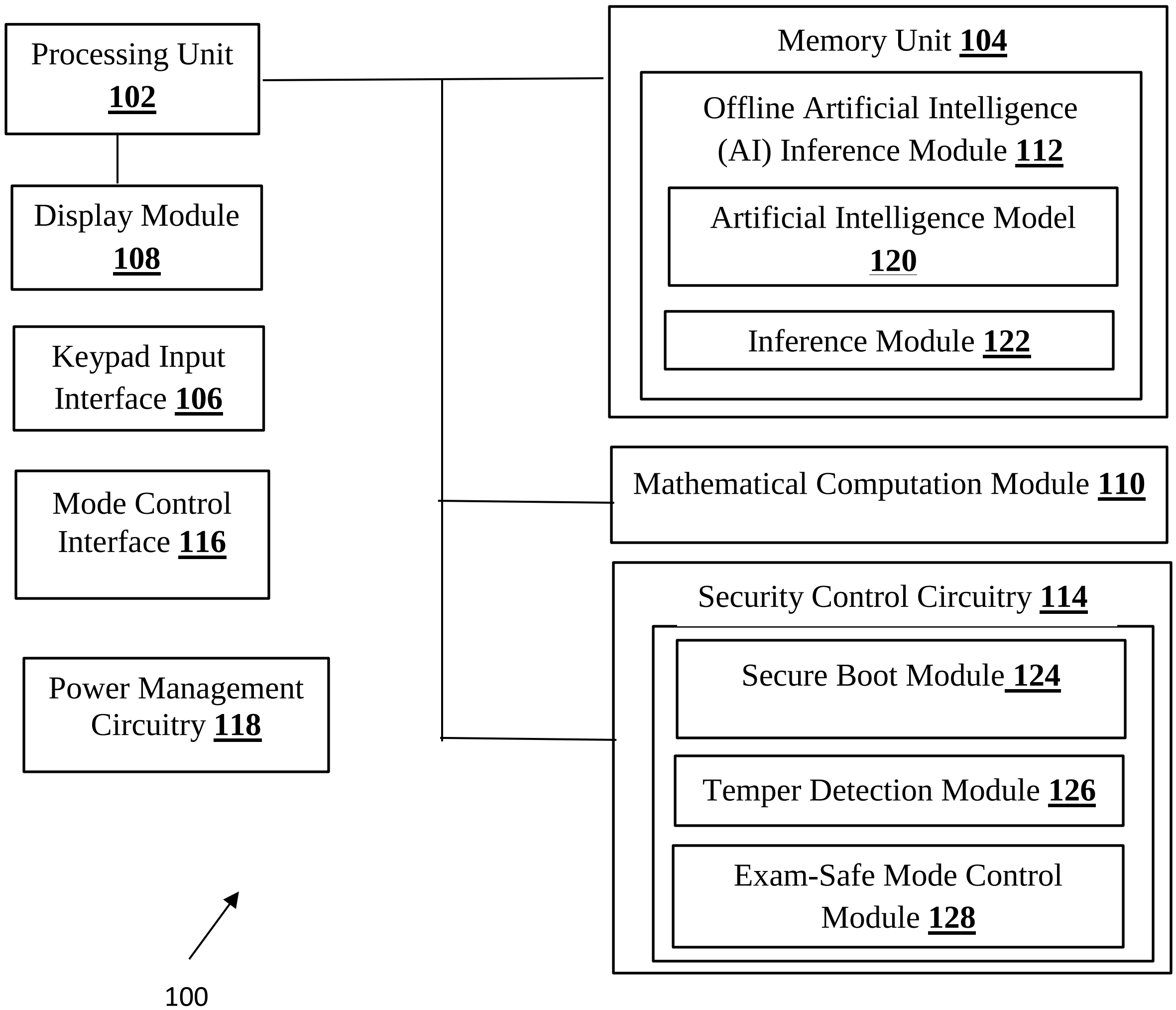

FIG. 1

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

Flowchart of Working of an Exam-safe offline artificial intelligence (AI)-enabled electronic computing device

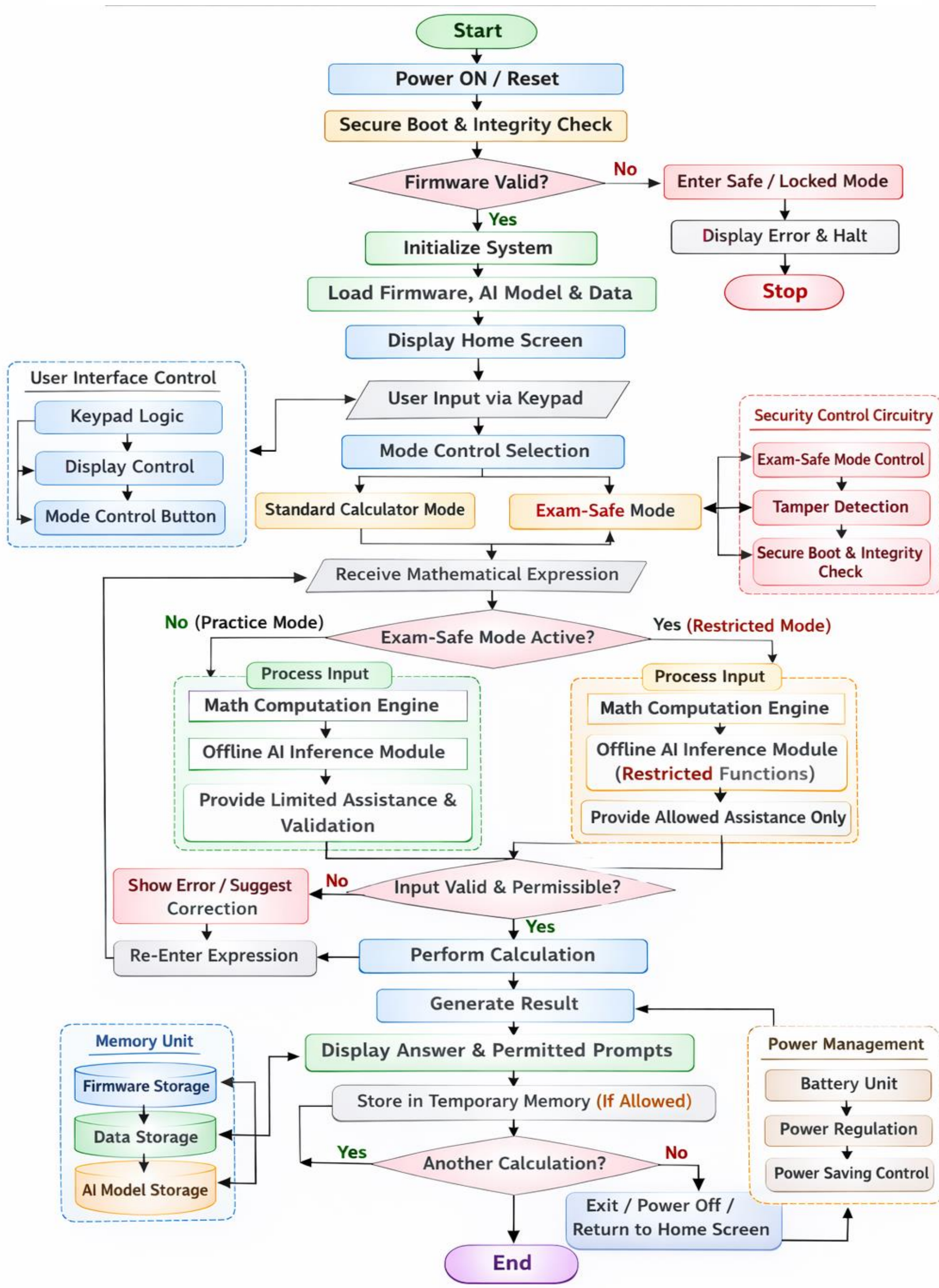

FIG. 2

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

Exam-safe offline artificial intelligence (AI)-enabled electronic computing device

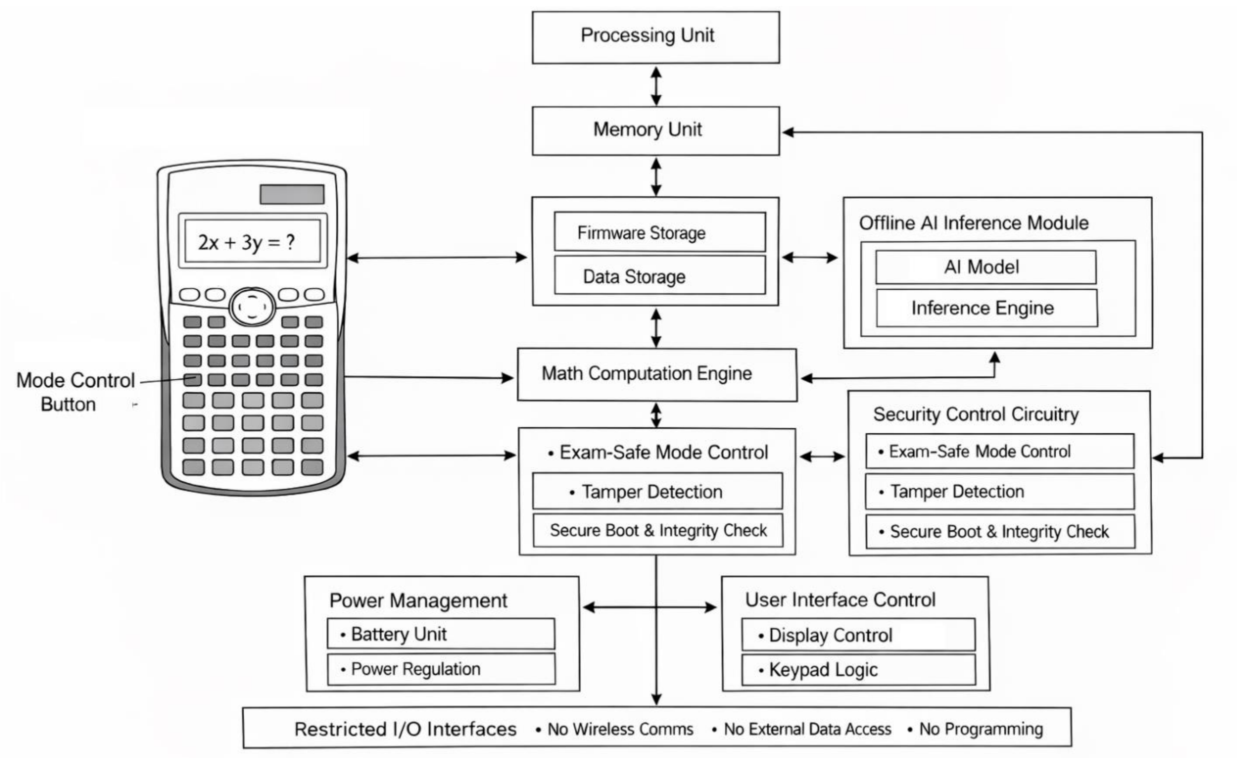

FIG. 3

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

Logic Layer Architecture of Exam-safe offline artificial intelligence (AI)-enabled electronic computing device

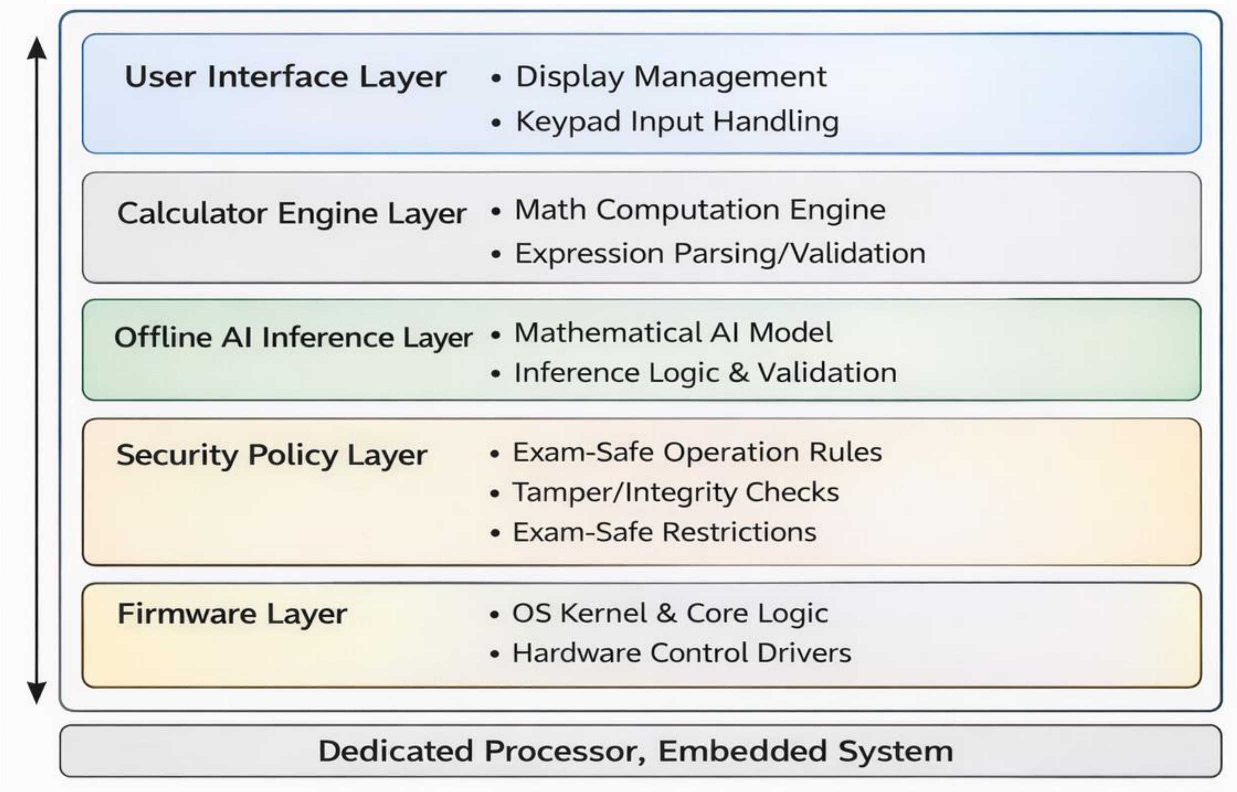

FIG. 4

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

External Device View of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device

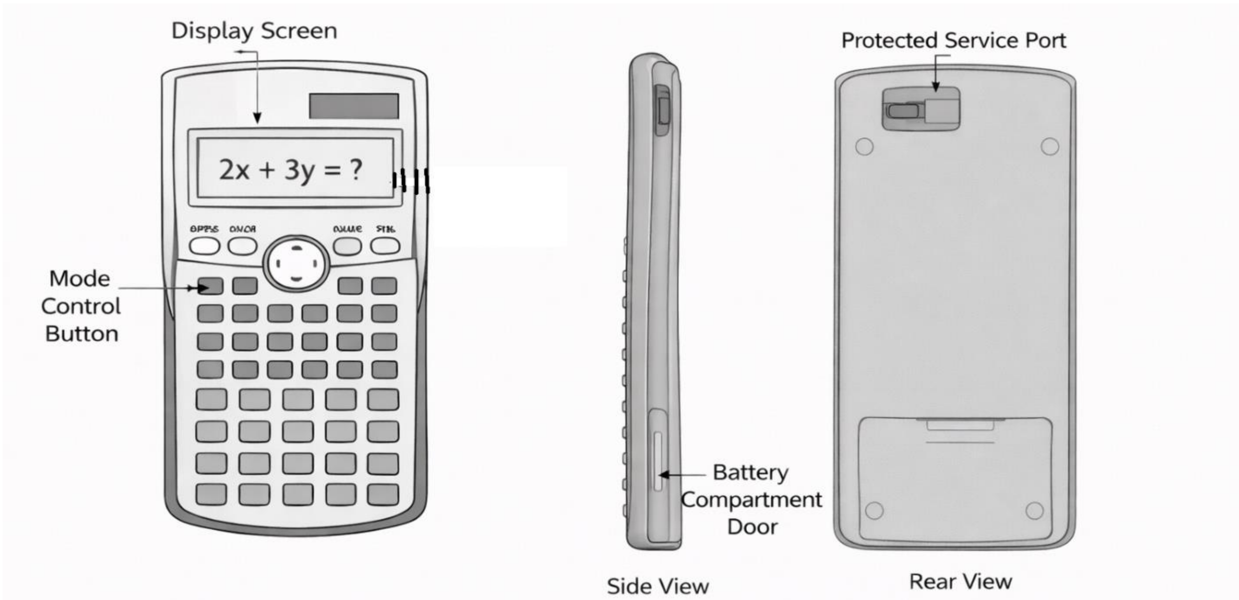

FIG. 5

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

Offline AI Processing Flow Diagram of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device

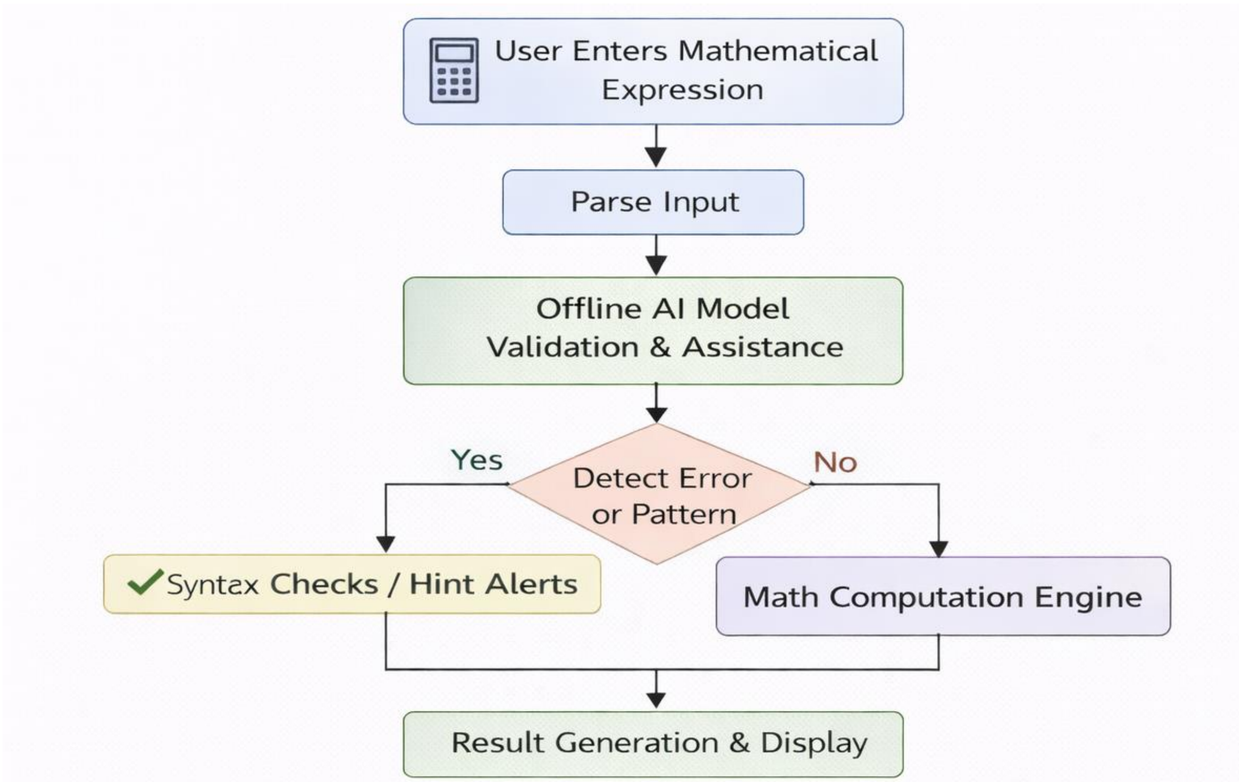

FIG. 6

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

Secure Boot and Integrity Verification Flow Diagram of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device

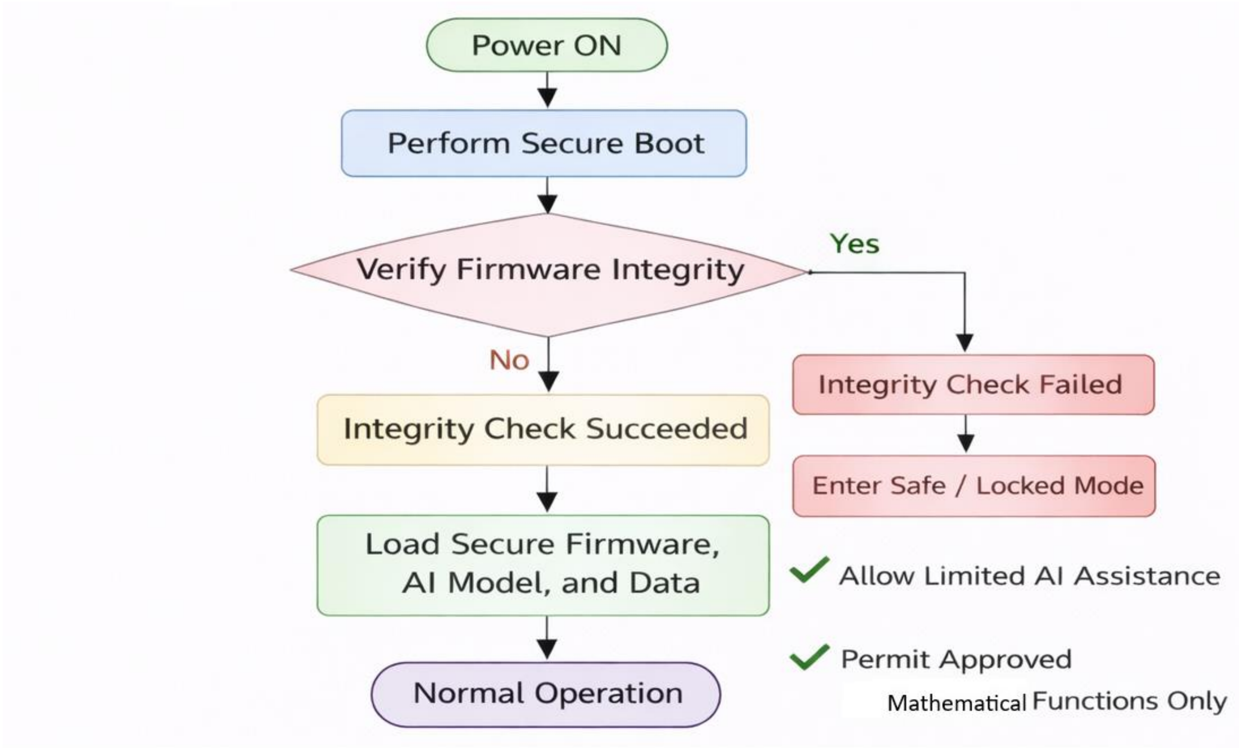

FIG. 7

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

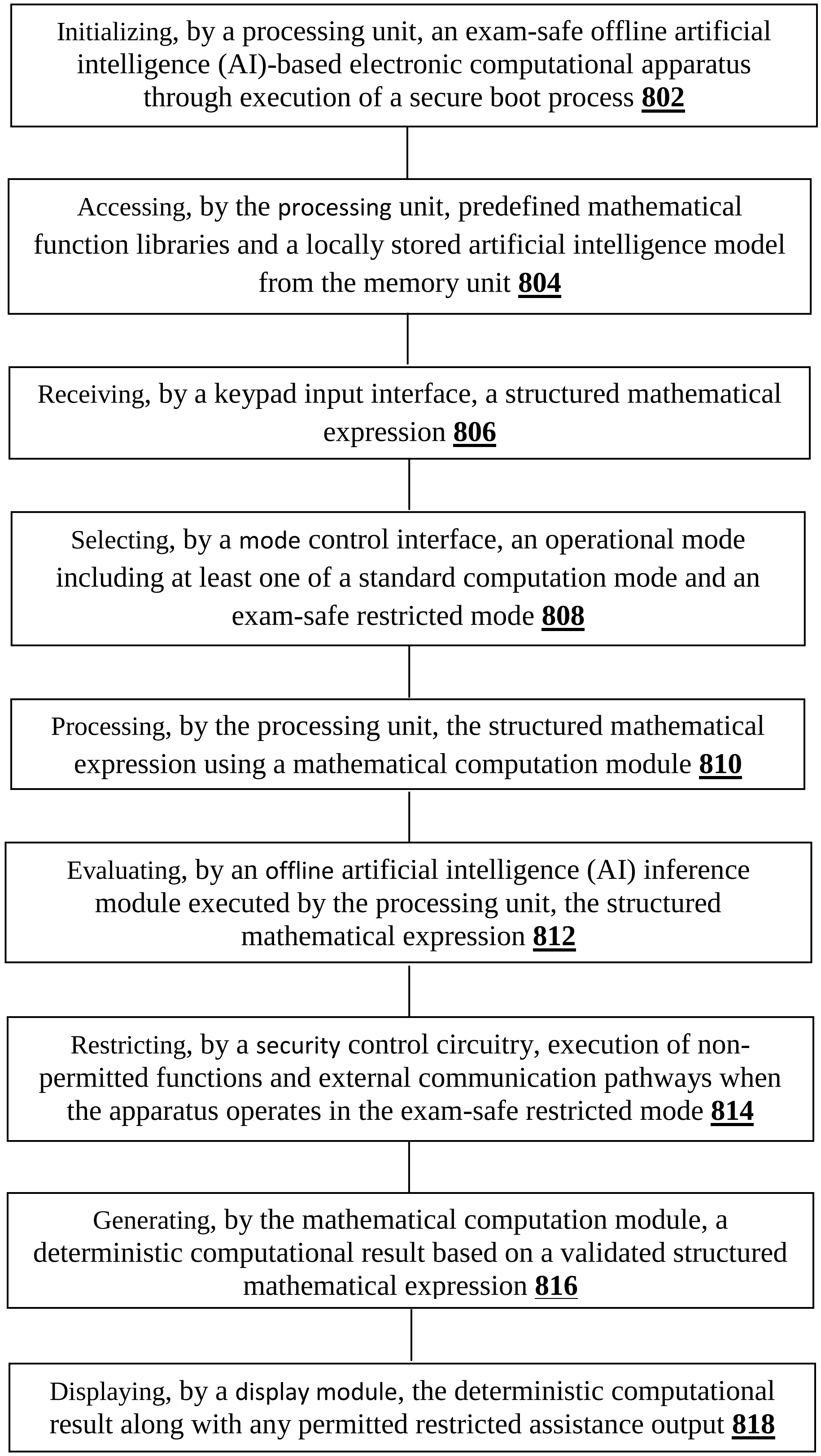

FIG. 8

-Digitally Signed-
Anuradha Gupta
Patent Agent (IN/PA-1314)
Agent for the applicant

Digitally Signed By:
ANURADHA GUPTA
Date: 21-04-2026 19:35:55

FORM 18 A **THE PATENTS ACT,1970** **and THE PATENT RULES,2003** **REQUEST FOR EXPEDITED EXAMINATION OF APPLICATION FOR PATENT** **[See section 11B and Rule 24C]**	(FOR OFFICE USE ONLY) RQ. No.: Filing Date: Amount of fee Paid: CBR no: 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. 202631050972 filed on 21st April 2026 for invention Titled "**AN EXAM-SAFE OFFLINE ARTIFICIAL INTELLIGENCE (AI)-ENABLED ELECTRONIC COMPUTING DEVICE AND METHOD THEREOF"** 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 22nd day of April, 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

Digitally Signed By:
ANURADHA GUPTA
Date: 22-04-2026 14:14:10

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, Hereby Declare:
	(i) That I/We who have made the application for Patent number 202631050972 in India, dated 21st April 2026 alone (ii) that I/We have not made any application for the same/substantially the same invention outside India Or (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……………………..~~ (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. Dated this 22nd day of April 2026.
3. To be signed by the applicant or his authorized registered patent agent	-Digitally Signed- Signature
4. Name of the Natural person who has signed	(**Anuradha Gupta)** Patent Agent (IN/PA-1514) Agent for the Applicant
	To The Controller of Patents, The Patent Office At Kolkata

Digitally Signed By:
ANURADHA GUPTA
Date: 22-04-2026 11:51:34

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 (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 (One Hundred only)

सत्यमेव जयते

₹100

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

IN-DL49794072924674Y

Please write or type below this line

Statutory Alert:

1. The authenticity of this Stamp certificate should be verified at 'www.shcilestamp.com' or using e-Stamp Mobile App of Stock Holding. Any discrepancy in the details on this Certificate and as available on the website / Mobile App renders it invalid.
2. The onus of checking the legitimacy is on the users of the certificate.
3. In case of any discrepancy please inform the Competent Authority.

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: 22-04-2026 12:05:05

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 202631050972 dated 21st April 2026 are:

2. INVENTORS:

(i) (a) NAME : MOHANACHANDRAN, Dileep Kumar
(b) NATIONALITY : INDIAN
(c) ADDRESS : E-305, VAISHNAVI RATNAM APARTMENT, JALAHALLI CROSS, BANGALORE – 560057, KARNATAKA, INDIA

(ii) (a) NAME : RAO, Lella Sridhara
(b) NATIONALITY: INDIAN
(c) Address : 2-352, KAVURU LAKSHNAMA RAO STREET, NEAR PHC, DOSAPADU, KRISHNA, ANDHRA PRADESH-521321, INDIA

(iii) (a) NAME : JENA, Soumya Ranjan
(b) NATIONALITY: INDIAN
(c) Address : PLOT NO-3E/474, SECTOR-9, CDA, POST- MARKAT NAGAR, CUTTACK- 753014, ODISHA, 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.~~

-Digitally Signed-

Dated this 22nd day of April 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: 22-04-2026 12:06:02

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. 202631050972 dated 21st April 2026 under Section 11A (2) of the Patent Act.

.

Dated this 22nd day of April 2026

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

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

Digitally Signed By:
ANURADHA GUPTA
Date: 22-04-2026 10:39:47

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 Applicant in respect of the patent application No. 202631050972. 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. Dated this 22nd day of April 2026. Signature : -Digitally Signed- (Anuradha Gupta) Patent Agent (IN/PA-1514) Agent for the Applicant To The Controller of Patents, The Patent Office, At Kolkata.
4.	Name of the natural person who has signed. Designation and official seal, if any, of the person who has signed.	

Digitally Signed By:
ANURADHA GUPTA
Date: 22-04-2026 14:14:10

FORM 1 THE PATENTS ACT 1970 (39 of 1970) and THE PATENTS RULES, 2003 APPLICATION FOR GRANT OF PATENT (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	
MOHANACHANDRAN, Dileep Kumar	**INDIAN**	**INDIA**	House No.	**E-305, VAISHNAVI RATNAM APARTMENT**
			Street	**JALAHALLI CROSS**
			City	**BANGALORE**
			State	**KARNATAKA**
			Country	**INDIA**
			Pin code	**560057**
RAO, Lella Sridhara	**INDIAN**	**INDIA**	**House No.**	**2-352, KAVURU LAKSHNAMA RAO STREET**
			Street	**NEAR PHC, DOSAPADU**
			District	**KRISHNA**
			State	**ANDHRA PRADESH**
			Country	**INDIA**
			Pin No.	**521321**
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**

5. TITLE OF INVENTION-	**AN EXAM-SAFE OFFLINE ARTIFICIAL INTELLIGENCE (AI) -ENABLED ELECTRONIC COMPUTING DEVICE AND METHOD THEREOF**

6. AUTHORISED REGISTERED PATENT AGENT(S)	Name	**ANURADHA GUPTA**
	Mobile No.	**9213764385**
	Name	**S G INTELLECTUAL**
7. ADDRESS FOR SERVICE OF APPLICANT IN INDIA	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: 21-04-2026 (b) Signature: Dileep Kumar (c) Name : **MOHANACHANDRAN, Dileep Kumar** ii) (a) Date: 21-04-2026 (b) Signature: L. S. Rao (c) Name: **RAO, Lella Sridhara** iii) (a) Date: 21-04-2026 (b) Signature: Soumya Ranjan Jena (c) Name: **JENA, Soumya Ranjan**
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 - 62	Rs. 11520/-	
Claim(s)	No. of Claims - 17 No. of Pages - 7	--------------- --	------------------
Abstract	No. of Pages - 1		
Drawing(s)-	No. of Drawings - 8 No. of Pages - 8		

(b) Complete Specification
(d) Drawings
(c) Abstract
(d) Application Form-1
(e) Power of Attorney
(f) DIPP Certificate.
(g) 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 21st day of April 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: 22-04-2026 18:02:34

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: 22-04-2026 14:14:10

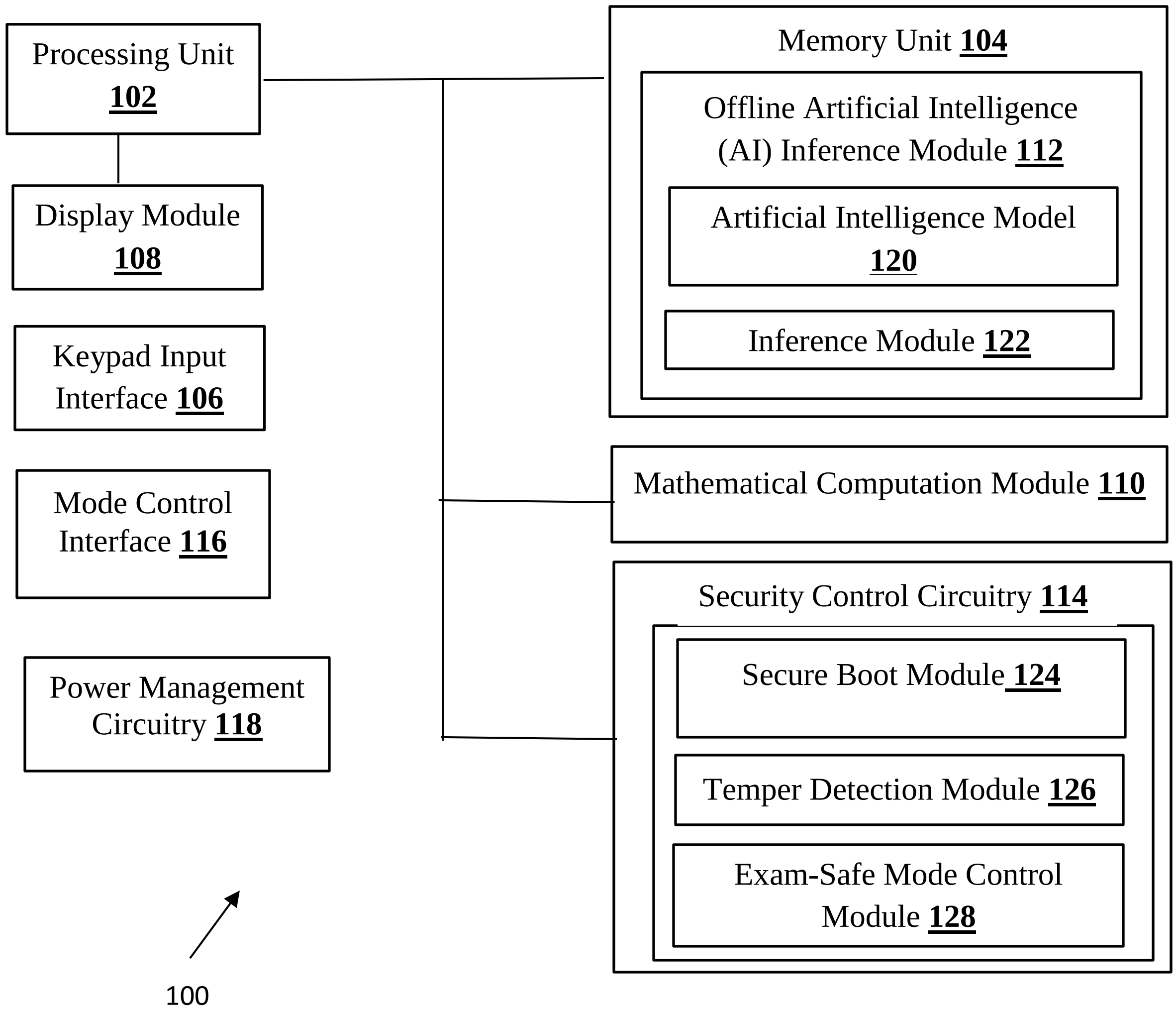

FIG. 1

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

Flowchart of Working of an Exam-safe offline artificial intelligence (AI)-enabled electronic computing device

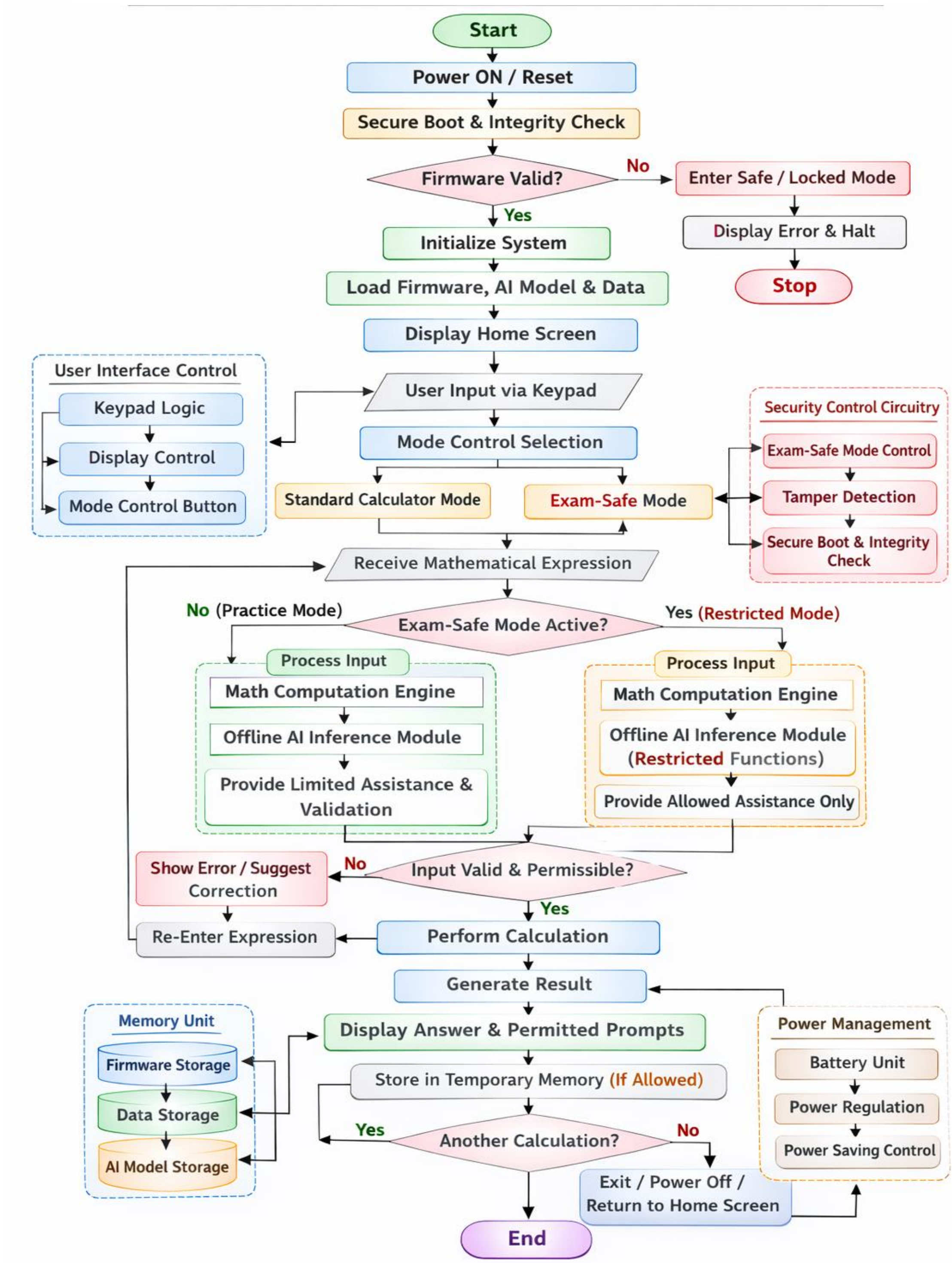

FIG. 2

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

Exam-safe offline artificial intelligence (AI)-enabled electronic computing device

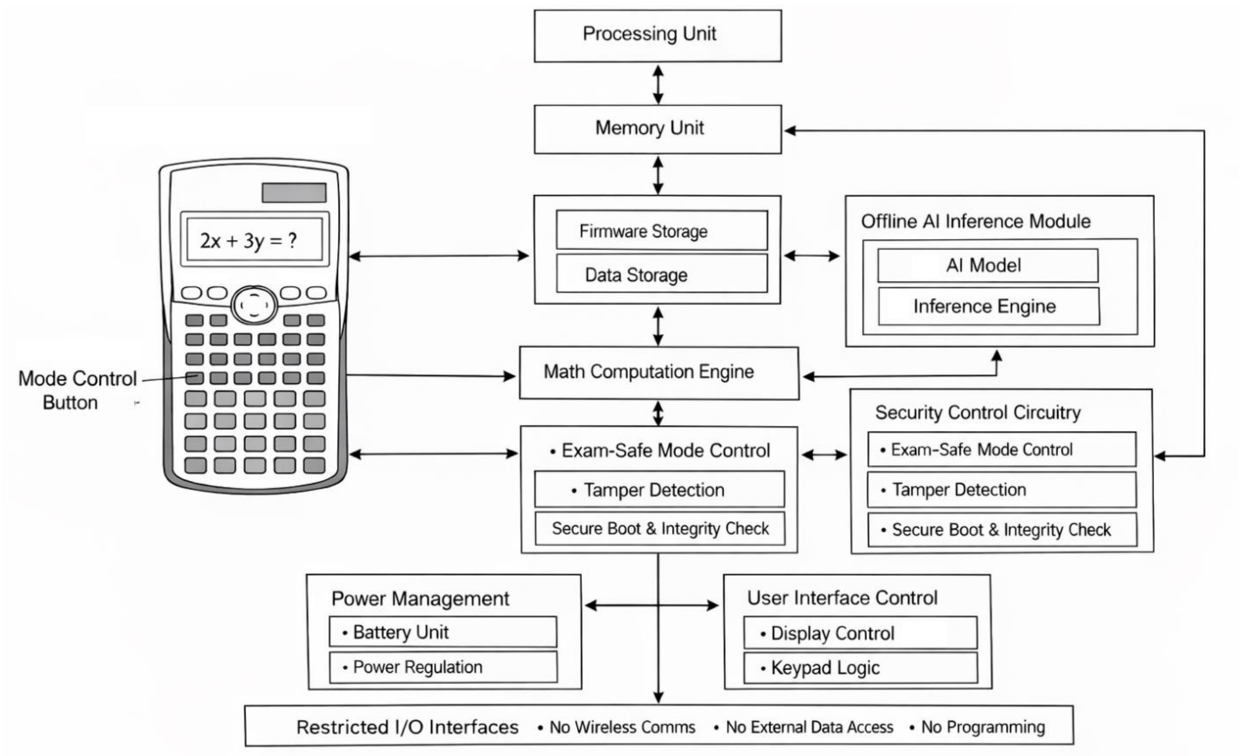

FIG. 3

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

Logic Layer Architecture of Exam-safe offline artificial intelligence (AI)-enabled electronic computing device

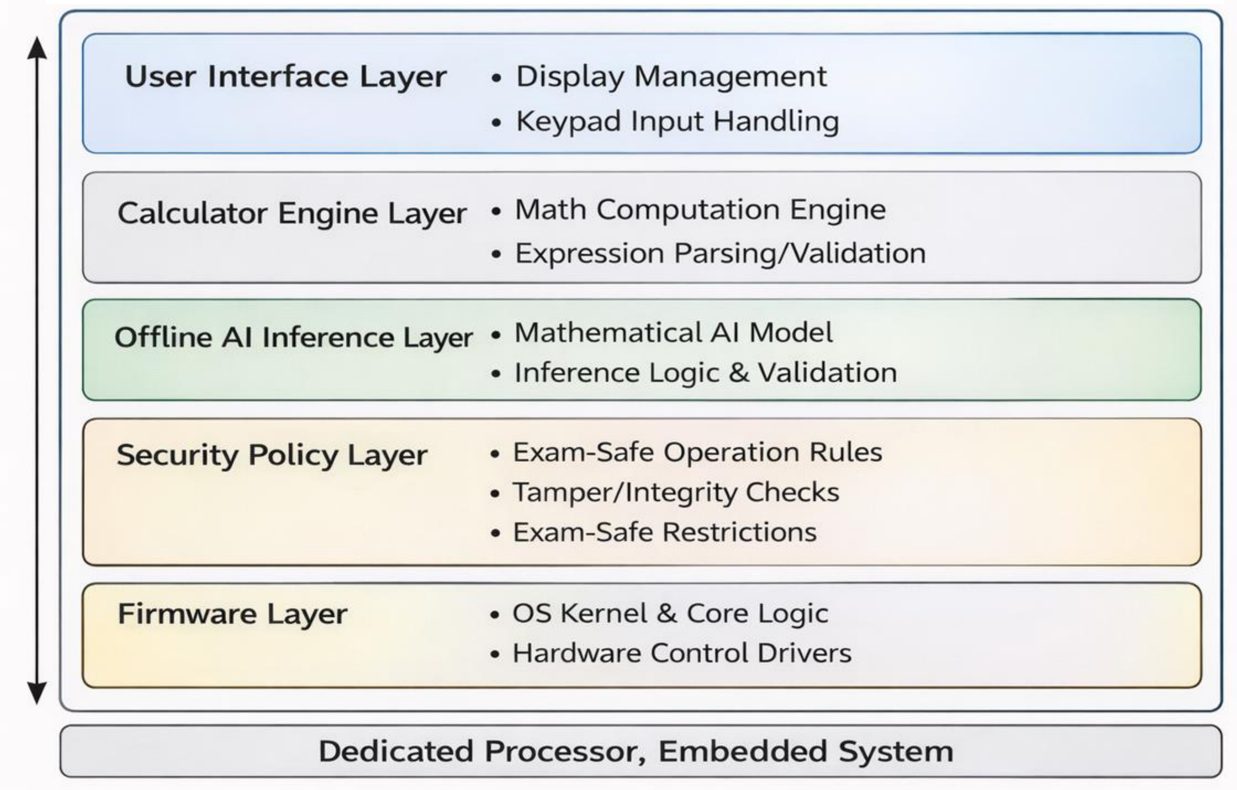

FIG. 4

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

External Device View of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device

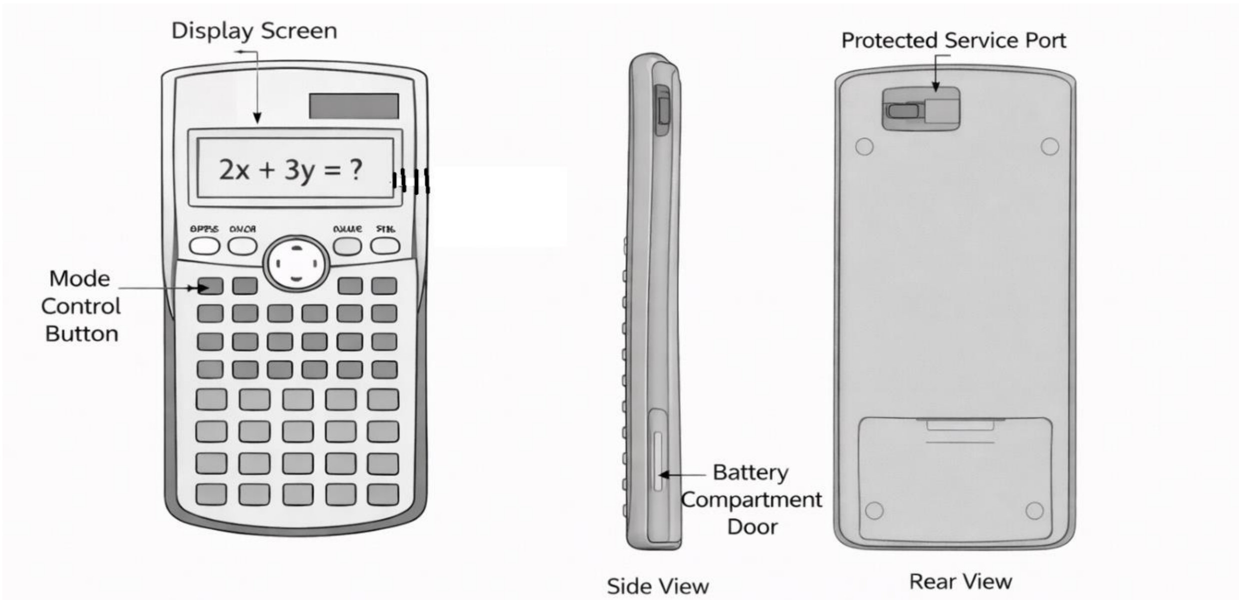

FIG. 5

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

Offline AI Processing Flow Diagram of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device

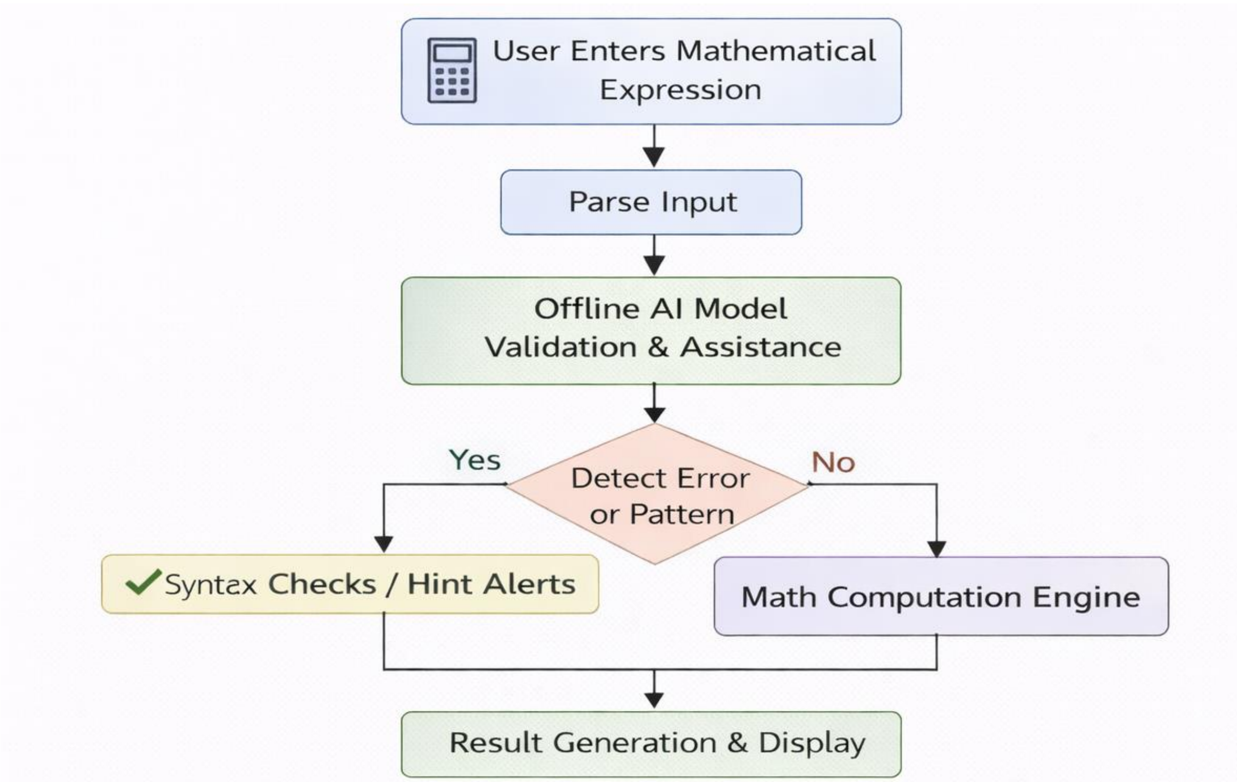

FIG. 6

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

Secure Boot and Integrity Verification Flow Diagram of an exam-safe offline artificial intelligence (AI)-enabled electronic computing device

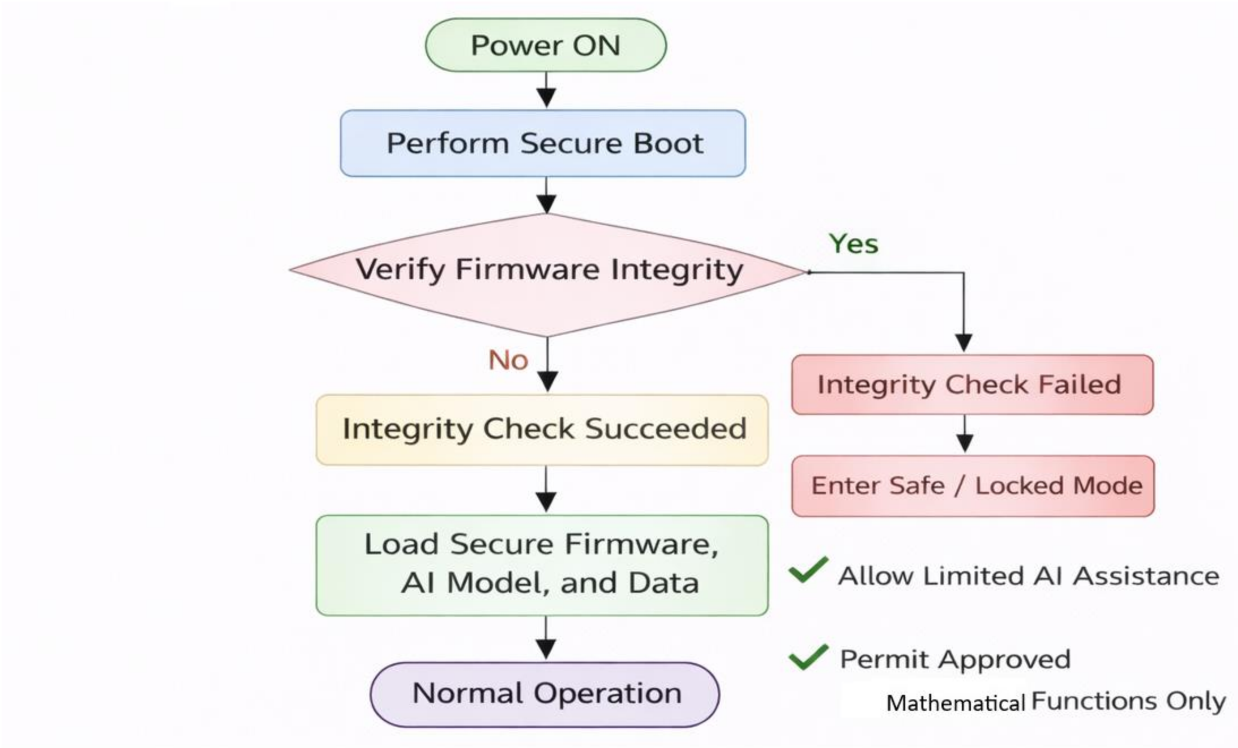

FIG. 7

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

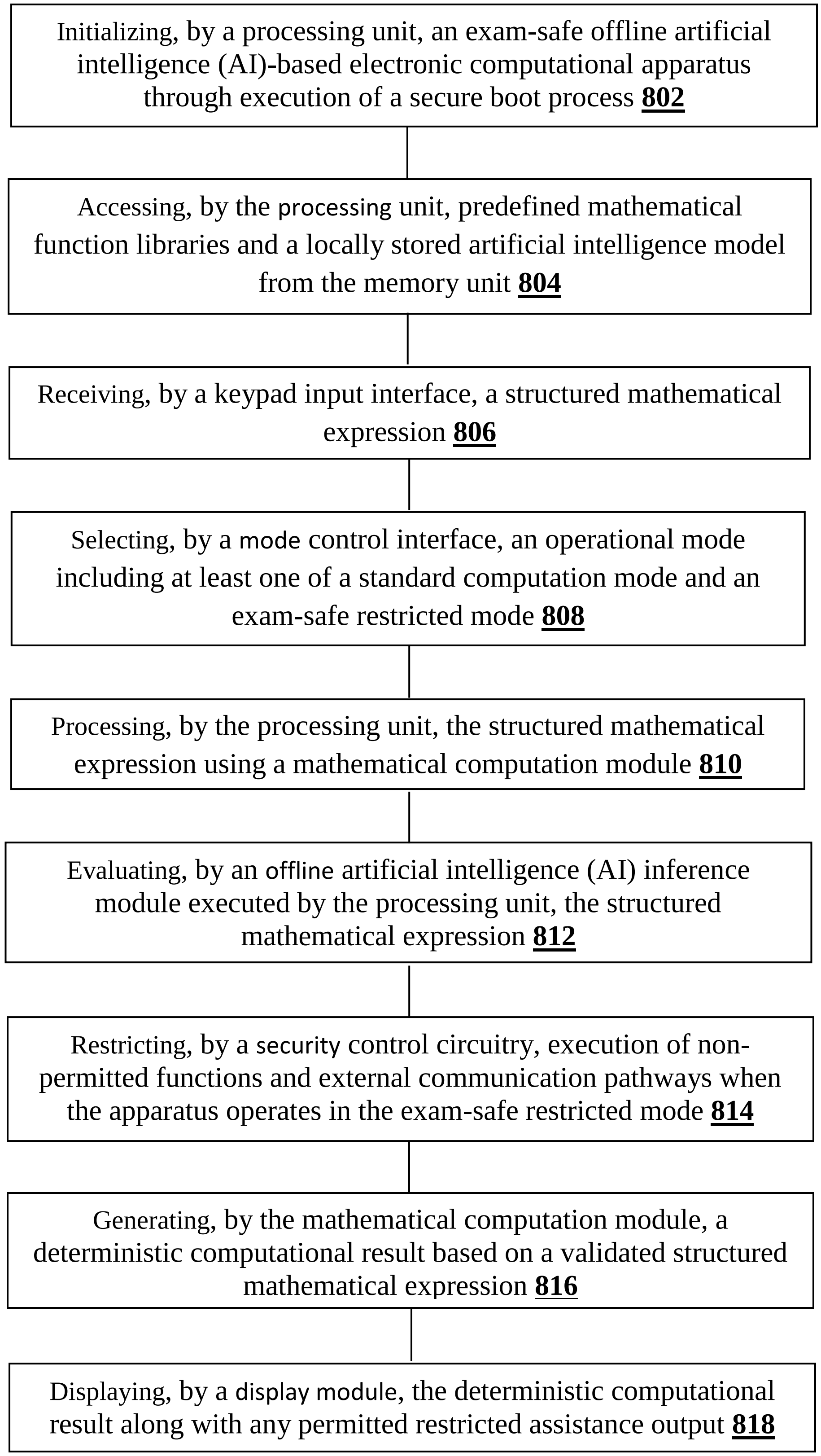

FIG. 8

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

Digitally Signed By:
ANURADHA GUPTA
Date: 21-04-2026 19:35:55

FORM 1 THE PATENTS ACT 1970 (39 of 1970) and THE PATENTS RULES, 2003 APPLICATION FOR GRANT OF PATENT (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	
MOHANACHANDRAN, Dileep Kumar	**INDIAN**	**INDIA**	House No.	**E-305, VAISHNAVI RATNAM APARTMENT**
			Street	**JALAHALLI CROSS**
			City	**BANGALORE**
			State	**KARNATAKA**
			Country	**INDIA**
			Pin code	**560057**
RAO, Lella Sridhara	**INDIAN**	**INDIA**	**House No.**	**2-352, KAVURU LAKSHNAMA RAO STREET**
			Street	**NEAR PHC, DOSAPADU**
			District	**KRISHNA**
			State	**ANDHRA PRADESH**
			Country	**INDIA**
			Pin No.	**521321**
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**

<table>
<tr><td colspan="3">5. TITLE OF INVENTION- AN EXAM-SAFE OFFLINE ARTIFICIAL INTELLIGENCE (AI) -ENABLED ELECTRONIC COMPUTING DEVICE AND METHOD THEREOF</td></tr>
<tr><td rowspan="2">6. AUTHORISED REGISTERED PATENT AGENT(S)</td><td>Name</td><td>ANURADHA GUPTA</td></tr>
<tr><td>Mobile No.</td><td>9213764385</td></tr>
<tr><td rowspan="6">7. ADDRESS FOR SERVICE OF APPLICANT IN INDIA</td><td>Name</td><td>S G INTELLECTUAL</td></tr>
<tr><td>Postal Address</td><td>4-D (UPPER FLOOR), DDA POCKET-2 SECTOR-6, DWARKA, NEW DELHI-110075, DELHI</td></tr>
<tr><td>Telephone No.</td><td>011 35586108</td></tr>
<tr><td>Mobile No.</td><td>9213764385</td></tr>
<tr><td>E-mail ID</td><td>sav@sgintellectual.com</td></tr>
</table>

<table>
<tr><td colspan="5">8. IN CASE OF APPLICATION CLAIMING PRIORITY OF APPLICATION FILED IN CONVENTION COUNTRY, PARTICULARS OF CONVENTION APPLICATION</td></tr>
<tr><td>Country</td><td>Application Number</td><td>Filing date</td><td>Name of the applicant</td><td>Title of the Invention</td></tr>
<tr><td>----------</td><td>---------</td><td>----------------------</td><td>----------------</td><td>___________________________</td></tr>
</table>

<table>
<tr><td colspan="2">9. IN CASE OF PCT NATIONAL PHASE APPLICATION, PARTICULARS OF INTERNATIONAL APPLICATION FILED UNDER PATENT CO-OPERATION TREATY (PCT)</td></tr>
<tr><td>International application number</td><td>International filing date</td></tr>
<tr><td>---</td><td>____</td></tr>
<tr><td colspan="2">10. IN CASE OF DIVISIONAL APPLICATION FILED UNDER SECTION 16, PARTICULARS OF ORIGINAL (FIRST) APPLICATION-NA</td></tr>
<tr><td>Original (first) application No</td><td>Date of filing of original (first) application</td></tr>
<tr><td>---------------------------------------</td><td>-------------------------------</td></tr>
<tr><td colspan="2">11. IN CASE OF PATENT OF ADDITION FILED UNDER SECTION 54, PARTICULARS OF MAIN APPLICATION OR PATENT-NA</td></tr>
<tr><td>Main application/patent No.---------------</td><td>Date of filing of main application -----------------</td></tr>
</table>

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:

(b) Signature:
(c) Name : **MOHANACHANDRAN, Dileep Kumar**

ii) (a) Date:

(b) Signature:
(c) Name: **RAO, Lella Sridhara**

iii) (a) Date:

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

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 - 62	Rs. 11520/-	
Claim(s)	No. of Claims - 17 No. of Pages - 7	-----------------	-------------------
Abstract	No. of Pages - 1		
Drawing(s)-	No. of Drawings - 8 No. of Pages - 8		

(b) Complete Specification
(d) Drawings
(c) Abstract
(d) Application Form-1
(e) Power of Attorney
(f) DIPP Certificate.
(g) 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 21st day of April 2026

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

To
The Controller of Patents
The Patent Office, KOLKATA

Digitally Signed By:
ANURADHA GUPTA
Date: 21-04-2026 19:35:55

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 Applicant in respect of the patent application No……... 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. Dated this 21st day of April 2026.
4.	Name of the natural person who has signed. Designation and official seal, if any, of the person who has signed.	Signature : -Digitally Signed- (Anuradha Gupta) Patent Agent (IN/PA-1514) Agent for the Applicant To The Controller of Patents, The Patent Office, At Kolkata.

Digitally Signed By:
ANURADHA GUPTA
Date: 21-04-2026 19:35:55

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 Applicant in respect of the patent application No……... 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. Dated this 21st day of April 2026. Signature : -Digitally Signed- (Anuradha Gupta) Patent Agent (IN/PA-1514) Agent for the Applicant To The Controller of Patents, The Patent Office, At Kolkata.
4.	Name of the natural person who has signed. Designation and official seal, if any, of the person who has signed.	

Digitally Signed By:
ANURADHA GUPTA
Date: 21-04-2026 19:35:09