Defensive Publication (Prior Art Record)

Novel Authentication Method Prevents AI Voice Cloning Through Neural–Acoustic Correlation

Document Metadata

Document ID: GABEY-DP-2026-02-06-MULTIMODAL-VOICE-VERIFICATION-v1.0
Version: v1.0
Development Commenced (claimed): February 3, 2026 (Australia/Melbourne, AEDT, UTC+11)
Architecture Specification Completed: February 5, 2026 (Australia/Melbourne, AEDT, UTC+11)
Public Disclosure Published (verifiable): February 6, 2026 10:55 PM (Australia/Melbourne, AEDT, UTC+11)

Primary Inventor: W. Prasanna Abeysekera
Organization: GABEY Consulting Pty. Ltd.
Contact: pabey642@gmail.com
Related Implementation: DSH-DSK-M7-Q4 (Speech Processing / Voice Interface Security Module)

Integrity Hashes: Published separately in GABEY-DP-2026-02-06-MULTIMODAL-VOICE-VERIFICATION-v1.0.HASHES.txt

Document Hashes:

- SHA-256 (PDF): `[To be calculated after PDF generation]`
- SHA-256 (MD): `[To be calculated after finalization]`

Legal Notice

DEFENSIVE PUBLICATION NOTICE

This document is published as a defensive publication to establish prior art as of February 6, 2026. This is **NOT** a patent application. By publishing this disclosure, the inventor establishes documented evidence of conception and technical details as of this date.

Purpose: To create public prior art that may be cited against future patent applications claiming similar inventions by third parties.

Rights Reserved: The inventor reserves all rights to file patent applications claiming specific implementations, algorithms, and embodiments of the concepts disclosed herein. This

Disclaimer: This disclosure is provided "as is" without warranties of any kind. The inventor assumes no liability for any use or reliance on this information.

Abstract

This publication discloses a multi-modal biometric authentication system that defeats AI-generated voice cloning and deepfake attacks by verifying the temporal correlation between brain activity and speech production. While conventional voice biometric systems authenticate based solely on acoustic characteristics, making them vulnerable to sophisticated AI synthesis, replay attacks, and voice conversion, the disclosed method introduces a physiological verification layer that confirms the speaker's physical presence and cognitive intent. By measuring electroencephalographic (EEG) signals during speech and establishing that neural activity naturally precedes and correlates with corresponding phoneme production, the system creates a composite biometric signature that is physiologically difficult to replicate through artificial speech generation, recorded playback, or unauthorised voice sample usage. This innovation enables voice authentication in high-security applications, including medical documentation, financial transactions, and legal proceedings, where existing voice-only systems are inadequate due to cloning vulnerabilities.

1. Problem Statement

Current Vulnerabilities in Voice Authentication

Voice-based authentication systems face increasing threats from:

- **AI Voice Cloning:** Text-to-speech (TTS) and voice conversion (VC) systems can generate highly convincing synthetic speech from small audio samples
- **Replay Attacks:** Recorded authentic speech can be played back to defeat authentication systems
- **Deepfake Conversational Agents:** Prompt-driven AI agents can engage in real-time conversation while impersonating target speakers
- **Compromised Enrolment:** Reference voiceprints may themselves be synthetic or tampered, undermining the entire authentication chain

Critical Gap

Existing systems authenticate "the voice" but not "the person actively speaking."

These attacks succeed because current voice biometric systems depend solely on acoustic similarity matching, with no verification of:

- Physical presence of the speaker
- Cognitive intent and consciousness

- Active speech production (vs. playback)
- Physiological characteristics unique to human speech generation

---

2. Summary of the Invention

Core Innovation

The disclosed invention adds a **physiological "liveness + intent" verification layer** by coupling two concurrent data streams:

1. **Acoustic Stream:** Microphone-captured speech signal containing phonemes, prosody, and timing information
2. **Neural Stream:** Electroencephalographic (EEG) signals recorded during speech production

Authentication Mechanism

Authentication is granted **only if** the system confirms a consistent temporal and statistical correlation between:

- **EEG-derived features:** Event-related potentials (ERPs), motor planning signatures, speech-specific neural activity patterns, and frequency bandpower dynamics
- **Speech features:** Phoneme onset timing, syllable structure, articulatory proxies, and prosodic contours

Key Principle

This neural-acoustic correlation is **physiologically intrinsic** to human speech production:

- Neural activity in motor cortex and speech-planning regions **precedes** articulation by measurable intervals (~50-200ms)
- This temporal relationship is causally linked to speech production
- The correlation cannot be authentically reproduced using synthetic audio alone
- Absence or anomaly in this correlation indicates spoofing, playback, or synthesis

---

3. Key Novelty

Novel Technical Elements

3.1 Neural–Acoustic Correlation Gate

A verification mechanism that confirms the speaker's brain activity temporally aligns with speech waveform timing and phoneme structure. This creates a physiological "proof of speech production" that cannot be faked with audio alone.

3.2 Presence + Cognitive Intent Verification

The system distinguishes authentic speech production (requiring conscious neural activity) from:

- Pre-recorded playback (no neural activity)
- AI-synthesised speech (no biological neural patterns)
- Coerced or unconscious vocalisation (abnormal neural signatures)

3.3 Composite Biometric Signature

The paired EEG+speech signature creates a multi-modal biometric that is:

- Significantly harder to spoof than voice-only embeddings
- Temporally bound (cannot be separated and recombined)
- Physiologically unique to each individual
- Revocable (can re-enrol if compromised)

3.4 Differentiation from Prior Art

Vs. Voice-Only Biometrics:

- Prior art relies solely on acoustic features (vulnerable to AI synthesis)
- This invention adds a physiological verification layer (defeats synthesis)

Vs. EEG-Only Authentication:

- Prior art uses EEG for general access control (not speech-specific)
- This invention uses speech-production-specific neural signatures correlated with acoustic output.

Vs. Multi-Modal Biometrics (e.g., face + voice):

- Prior art combines independent biometric factors
- This invention creates **a temporal correlation** between dependent physiological processes

Novel Contribution: No known prior art correlates speech-production neural activity with acoustic output for the specific purpose of detecting voice cloning and synthesis attacks.

---

4. High-Level Method (Illustrative)

System Workflow

Step 1: Concurrent Signal Capture

- **EEG Acquisition:** Multi-channel EEG headset records brain activity (focusing on motor cortex, Broca's area, and speech-planning regions)

- **Audio Acquisition:** The microphone captures the speech signal
- **Synchronisation:** Both signals are time-stamped with a common time reference

Step 2: Signal Pre-Processing

EEG Stream:

- Bandpass filtering (remove DC drift, high-frequency noise)
- Artifact removal (eye blinks, muscle activity, electrical interference)
- Temporal segmentation aligned with speech events

Audio Stream:

- Voice Activity Detection (VAD)
- Phoneme segmentation and feature extraction
- Speech quality assessment

Step 3: Feature Extraction

EEG Features:

- Time-frequency decomposition (wavelet or STFT)
- Event-Related Potentials (ERPs) aligned to phoneme onsets
- Frequency band power dynamics (alpha, beta, gamma bands)
- Speech-motor planning signatures

Audio Features:

- Phoneme timing and onset detection
- Mel-Frequency Cepstral Coefficients (MFCCs) or learned embeddings
- Prosodic contours (pitch, energy, duration)
- Speaker-specific acoustic characteristics

Step 4: Temporal Alignment + Correlation Analysis

Correlation Computation:

- Estimate expected EEG→phoneme lag windows (typically 50-200ms before phoneme onset)
- Compute correlation/coherence/mutual information across sliding time windows
- Apply machine learning alignment scoring (e.g., cross-correlation, dynamic time warping, or learned correlation model)
- Generate composite correlation score

Expected Pattern (Authentic Speech):

```
Timeline:
  t=0ms:    Motor planning EEG signature detected
  t=100ms:  Pre-motor cortex activation
  t=150ms:  Articulatory motor commands
  t=200ms:  Phoneme produced (acoustic signal)

Correlation: HIGH (EEG precedes and correlates with speech)
```

Pattern Indicating Spoofing:

```
Timeline:
  t=0ms:    No relevant EEG activity
  t=200ms:  Phoneme in acoustic signal (playback)

Correlation: LOW or ABSENT (no neural-acoustic binding)
```

Step 5: Authentication Decision

Decision Logic:

```
IF (voice_biometric_match >= voice_threshold)
   AND (neural_acoustic_correlation >= correlation_threshold)
   AND (liveness_indicators == PASS)
THEN
   AUTHENTICATE (grant access)
ELSE
   REJECT (potential spoofing attack)
```

Multi-Factor Scoring:

- Voice match confidence: 0.0-1.0
- Neural-acoustic correlation: 0.0-1.0
- Liveness score: 0.0-1.0
- Composite authentication score: weighted combination
- Risk-based threshold adjustment based on application sensitivity

---

5. Threat Model and Defences

Attacks Defended Against

5.1 AI-Generated Speech (TTS/Voice Conversion)

- **Attack:** Synthesise voice using neural TTS or voice conversion
- **Defence:** No corresponding EEG signals; correlation test fails
- **Result:** System rejects due to the absence of neural-acoustic binding

5.2 Replay Attacks

- **Attack:** Playback of previously recorded authentic speech
- **Defence:** Recording contains no EEG data; no live neural activity
- **Result:** System rejects due to a missing neural stream

5.3 Voice Cloning with Small Samples

- **Attack:** Train a voice cloning model on leaked audio samples
- **Defence:** Cloned voice lacks synchronised brain activity
- **Result:** System rejects due to correlation failure

5.4 Stolen Audio Samples

- **Attack:** Use authentic recordings for impersonation
- **Defence:** Audio alone insufficient; requires concurrent EEG
- **Result:** System rejects (no EEG correlation)

5.5 Real-Time Voice Conversion

- **Attack:** Convert the attacker's voice to the target speaker in real-time
- **Defence:** Attacker's EEG patterns won't match the target speaker's template
- **Result:** System rejects due to biometric mismatch

Additional Security Considerations

Attacks Requiring Additional Controls

5.6 EEG Signal Injection/Manipulation:

- **Attack:** Compromise the EEG device or data channel to inject synthetic neural signals
- **Defence Requirements:**
  - Device authentication and attestation
  - Encrypted EEG data transmission
  - Tamper-evident hardware
  - Challenge-response liveness protocols

5.7 Endpoint Malware:

- **Attack:** Malware on the client device captures or manipulates signals
- **Defence Requirements:**
  - Secure boot and trusted execution environment
  - Runtime integrity monitoring
  - Anti-malware controls

5.8 Coercion Scenarios:

- **Attack:** Force a legitimate user to authenticate under duress
- **Defence Requirements:**
  - Policy-level controls (transaction limits, multi-party authorisation)
  - Behavioural analysis for stress indicators
  - Out-of-band verification for high-value operations

6. Example Use Cases

6.1 Medical Transcription and Clinical Documentation

Problem: Prevent cloned physician voice from authorising fraudulent medical orders or prescriptions

Solution: Physician dictates notes while wearing an EEG device; the system verifies both voice match and neural-acoustic correlation before accepting the transcription as authenticated

Benefit: HIPAA-compliant verified identity for medical documentation

---

6.2 Financial Voice Authorisation

Problem: Voice-based banking is vulnerable to deepfake attacks authorising fraudulent transactions

Solution: Customer wears consumer-grade EEG headset during high-value transaction authorisation; system confirms both voiceprint and brain activity correlation

Benefit: Defeats AI voice cloning attacks that bypass voice-only authentication

---

6.3 Legal Attestations and Testimony

Problem: Recorded statements and depositions could be fabricated using AI voice cloning

Solution: Speaker wears an EEG device during statement recording; correlation data provides cryptographic proof of authentic speech production

Benefit: Verifiable evidence that testimony came from a physically present, conscious individual

---

6.4 Secure Government/Military Communications

Problem: Impersonation attacks in voice-based command and control systems

Solution: Personnel authenticate using voice+EEG correlation before issuing commands or accessing classified information

Benefit: Additional assurance layer beyond voice-only authentication

---

6.5 Enterprise Remote Access

Problem: Work-from-home scenarios are vulnerable to voice-based social engineering

Solution: Employees authenticate to VPN or sensitive systems using voice+EEG verification

Benefit: Prevents unauthorised access using stolen or synthesised voice samples

---

7. Implementation Considerations

7.1 Hardware Requirements

EEG Acquisition:

- Consumer-grade devices: Dry electrode systems (e.g., Muse, Emotiv) - suitable for moderate security applications
- Medical-grade devices: Wet electrode systems with higher channel counts - suitable for high-security medical/financial applications
- Minimum viable: Single-channel forehead sensor focusing on frontal motor regions
- Optimal: Multi-channel system covering the motor cortex and Broca's area

Data Transmission:

- Wireless (Bluetooth) or wired connection
- Encrypted transmission to prevent eavesdropping
- Device authentication to prevent spoofing

7.2 Software Architecture

Local Processing (Privacy-Preserving):

- All EEG and voice processing can occur on a local device
- No cloud transmission of biometric data required
- Supports offline authentication in secure environments

Cloud-Based Processing (Scalable):

- Encrypted upload of features (not raw biometrics)
- Centralised template management
- Suitable for enterprise deployments

7.3 Database Architecture

Biometric Template Storage:

- Encrypted EEG feature templates (irreversible transformation)
- Voice biometric templates

- Temporal correlation parameters
- Template versioning for adaptation over time

Audit Logging:

- Minimum required fields:
  - Timestamp (ISO 8601 format)
  - User identifier (hashed for privacy)
  - Device ID and model
  - Authentication decision (accept/reject)
  - Confidence scores (voice, EEG, correlation)
  - Software/model versions used
  - Policy threshold applied

Compliance Requirements:

- HIPAA compliance: No PHI in logs, 7-year retention, encryption at rest
- GDPR compliance: Right to erasure (revocable biometric templates)
- PCI DSS: Secure storage of authentication credentials

7.4 Performance Considerations

Latency Targets:

- EEG acquisition: Real-time streaming (<100ms latency)
- Feature extraction: <500ms
- Correlation analysis: <200ms
- Total authentication time: <2 seconds

Accuracy Targets:

- False Accept Rate (FAR): <0.1% (1 in 1000 attack attempts)
- False Reject Rate (FRR): <5% (acceptable user experience)
- Equal Error Rate (EER): <2% (balanced security/usability)

7.5 User Experience

Enrolment Process:

- User speaks 3-5 enrolment phrases while wearing the EEG device
- System captures voice+EEG correlation baseline
- Takes 2-3 minutes
- Can be performed remotely

Authentication Process:

- User speaks authentication phrase (text-dependent or independent)
- The EEG device must be worn

- Authentication completes in <2 seconds
- Transparent to the user (no additional actions required)

Device Wearability:

- Consumer EEG headsets: Comfortable for 30–60-minute sessions
- Medical-grade: May require gel application (5-minute setup)
- Ideal: Dry-electrode headband or earpiece form factor

---

8. Technical Advantages Summary

Security Advantages

✅ **Defeats AI voice cloning** - Synthesised speech lacks correlated neural activity
✅ **Prevents replay attacks** - Recordings have no live EEG signals
✅ **Verifies liveness** - Confirms conscious, intentional speech production
✅ **Multi-modal binding** - Temporal correlation creates an unforgeable signature
✅ **Revocable credentials** - User can re-enrol if the template is compromised

Privacy Advantages

✅ **Local processing** - No cloud transmission of biometric data required
✅ **Irreversible templates** - Cannot reconstruct raw EEG from stored features
✅ **Minimal data retention** - Only feature vectors stored, not raw signals
✅ **User control** - Biometric data remains on the user's device

Deployment Advantages

✅ **Scalable** - Works with consumer-grade EEG devices (~$200)
✅ **Offline capable** - Suitable for air-gapped secure environments
✅ **Cross-platform** - Compatible with Windows, Linux, macOS, mobile
✅ **Standards-based** - Uses existing EEG and audio formats

---

9. Related Work and Prior Art Differentiation

Voice Biometric Authentication (Existing)

Examples: Nuance, Pindrop, Google Voice Match
Limitation: Vulnerable to AI synthesis and voice cloning
This Invention's Advancement: Adds a physiological verification layer

EEG-Based Authentication (Existing)

Examples: Various research papers on brainwave-based login
Limitation: General-purpose authentication, not speech-specific
This Invention's Advancement: Correlates the EEG specifically with speech production

Multi-Modal Biometrics (Existing)

Examples: Face + voice, fingerprint + voice
Limitation: Independent factors, no temporal binding
This Invention's Advancement: Creates a time-locked correlation between dependent physiological signals

Liveness Detection (Existing)

Examples: Face anti-spoofing, pulse detection
Limitation: Not integrated with voice authentication
This Invention's Advancement: Speech-specific liveness through neural activity

Anti-Spoofing Research (Existing)

Examples: Acoustic anti-spoofing features, replay detection
Limitation: Analyse audio signals only
This Invention's Advancement: Uses out-of-band physiological signal for verification

Conclusion: No known prior art combines speech-production neural activity measurement with acoustic analysis for the specific purpose of defeating voice cloning attacks through temporal correlation verification.

---

10. Disclosure Scope

Disclosed for Prior Art Purposes

The following concepts are disclosed to establish prior art as of February 6, 2026:

✅ Multi-modal authentication combining voice and EEG signals
✅ Temporal correlation between neural activity and speech production
✅ Using EEG-speech correlation to detect voice cloning/synthesis
✅ Liveness detection via speech-production neural signatures
✅ Database architecture for storing voice-EEG binding records
✅ Continuous authentication through periodic neural verification

✅ Composite confidence scoring from voice+EEG+correlation
✅ Irreversible biometric template generation from EEG
✅ Revocable biometric credentials through re-enrolment

Implementation Details Reserved

The following specific implementations remain proprietary and are **NOT disclosed** in this publication:

🔒 Specific signal processing algorithms and filter designs
🔒 Exact feature extraction methods and dimensionality
🔒 Template generation of mathematical formulas
🔒 Correlation calculation algorithms and weighting schemes
🔒 Machine learning model architectures and training procedures
🔒 Security protocols for device authentication
🔒 Database encryption and key management schemes
🔒 Specific threshold values and decision logic
🔒 Performance optimisation techniques
🔒 Integration APIs and system interfaces

These implementation details may be protected through:

- Trade secret protection
- Patent applications (provisional or full utility patents)
- Proprietary software licensing

---

11. Patent Rights and Licensing

Rights Reserved

The inventor expressly **reserves all rights** to file patent applications claiming:

- Specific implementations of the disclosed concepts
- Detailed algorithms and methods
- System architectures and apparatus designs
- Software and hardware embodiments

Future Patent Filings

This defensive publication does **NOT** preclude the inventor from filing patent applications on:

- Specific correlation algorithms
- Novel EEG feature extraction methods
- Optimised temporal alignment techniques

- Hardware implementations and device designs
- Database schema and security architectures

Licensing Availability

Implementation licenses may be available for:

- Commercial software vendors
- Medical device manufacturers
- Financial services companies
- Government agencies

Contact for licensing inquiries: pabey642@gmail.com

---

12. Publication Metadata and Verification

Publication Platforms

This defensive publication is being disseminated through:

- ✅ Personal/Professional Website: https://nomateq.com.au/resources/
- ✅ LinkedIn Article: [URL to be added]
- ✅ GitHub Repository: [URL to be added]
- ✅ ResearchGate: [URL to be added]
- ✅ Internet Archive: [archive.org URL to be added]
- ✅ Blockchain Timestamp: [Transaction ID to be added]

Timestamp Verification

Publication Timestamp: February 6, 2026 [10:55 PM]
Timezone: Australia/Melbourne (AEDT, UTC+11)
Blockchain Timestamp: [To be completed after publication]
Internet Archive Snapshot: [To be completed after archival]

Document Integrity

SHA-256 Hash (Markdown): [To be calculated]
SHA-256 Hash (PDF): [To be calculated after PDF generation]

To verify document authenticity, recalculate the hash and compare it with the published values.

13. Citation Information

Recommended Citation (Academic)

```
Abeysekera, W.P. (2026). Novel Authentication Method Prevents AI Voice
Cloning Through Neural-Acoustic Correlation. Defensive Publication.
GABEY Consulting Pty. Ltd. Document ID: GABEY-DP-2026-02-06-MULTIMODAL-
VOICE-VERIFICATION-v1.0. Published: February 6, 2026.
Available at: https://nomateq.com.au/resources/defensive-
publications/GABEY-DP-2026-02-06-MULTIMODAL-VOICE-VERIFICATION-v1.0.pdf
```

Recommended Citation (Patent)

```
Abeysekera, W.P., "Multi-modal biometric authentication using neural-
acoustic
correlation," Defensive Publication GABEY-DP-2026-02-06, February 6, 2026.
```

Bibliographic Data

Author: W. Prasanna Abeysekera
Title: Novel Authentication Method Prevents AI Voice Cloning Through Neural-Acoustic Correlation
Publication Type: Defensive Publication / Technical Disclosure
Publisher: GABEY Consulting Pty. Ltd.
Date: February 6, 2026
Language: English
Subject Matter: Biometric authentication, voice security, EEG, anti-spoofing

14. Contact Information

For Patent-Related Inquiries

Patent Counsel Contact Only
Please direct all patent licensing, infringement, or legal inquiries to qualified patent counsel.

Do NOT contact the inventor directly regarding:

- Implementation specifics prior to the licensing agreement
- Patent application status or claims

- Confidential technical details

For Research Collaboration

Email: pabey642@gmail.com
Subject Line: Research Collaboration - Neural-Acoustic Authentication

Appropriate topics:

- Academic research partnerships
- Non-commercial research use
- Conference presentations or publications referencing this work

For General Information

Organisation: GABEY Consulting Pty. Ltd.
Website: https://www.gabey.com.au/, https://nomateq.com.au/

---

15. Disclaimer and Legal Notices

No Warranties

This disclosure is provided **"AS IS"** without warranties of any kind, either express or implied, including but not limited to:

- Merchantability
- Fitness for a particular purpose
- Non-infringement
- Accuracy or completeness

Limitation of Liability

The inventor and GABEY Consulting Pty. Ltd. shall not be liable for:

- Any use or reliance on this information
- Any implementation attempts based on this disclosure
- Any damages arising from the use of disclosed concepts
- Patent infringement claims by third parties

Export Control

Implementation of the disclosed technology may be subject to:

- Australian export control regulations
- US ITAR or EAR restrictions (if applicable)
- EU dual-use regulations
- Other applicable export control laws

Implementers are responsible for ensuring compliance with all applicable regulations.

Medical Device Regulations

Applications in medical contexts may require:

- Australian TGA approval
- US FDA clearance or approval
- EU Medical Device Regulation (MDR) compliance
- Other regional regulatory authorisations

This disclosure does not constitute regulatory approval for any medical application.

Data Protection and Privacy

Implementations must comply with:

- Australian Privacy Act 1988
- GDPR (for EU users)
- HIPAA (for US healthcare)
- Other applicable privacy regulations

Biometric data handling requires specific legal compliance.

---

16. Document Version History

Version 1.0 (February 6, 2026)

- Initial public disclosure
- Established prior art for neural-acoustic correlation authentication
- Published across multiple platforms with timestamp verification
- SHA-256 hashes calculated for document integrity

Future Amendments

Any substantive amendments will be published as new versions with:

- Incremented version number
- Change description
- New timestamp and hash values
- Cross-reference to previous versions

Minor corrections (spelling, formatting) will not trigger version updates.

---

17. Acknowledgments

Related Technical Work:

- DSH-DSK-M7-Q4 Speech Processing Architecture (February 3-5, 2026)
- Multi-Language Speech Engine Database Architecture (February 5, 2026)
- System Architecture Specification (February 3, 2026)

Technology Context: This disclosure emerged from work on secure multi-language speech recognition systems with medical-grade compliance requirements.

---

18. Keywords and Classification

Keywords

voice authentication, biometric security, EEG, electroencephalography, anti-spoofing, liveness detection, deepfake detection, voice cloning prevention, multi-modal biometrics, neural signals, brain-computer interface, speech production, temporal correlation, medical transcription security, financial authentication

Technical Classification (CPC)

Primary:

- G10L17/00 - Speaker identification or verification
- G06F21/32 - User authentication using biometric data
- A61B5/0476 - Electroencephalography [EEG]

Secondary:

- G10L15/00 - Speech recognition
- G06F21/55 - Detecting local intrusion or implementing counter-measures
- H04L9/32 - Including means for verifying the identity or authority of a user

Application Domains

- Medical documentation systems
- Financial services authentication
- Legal and judicial systems
- Government and Defence communications
- Enterprise security
- Consumer privacy protection

END OF DEFENSIVE PUBLICATION

Document Status: Published for Prior Art Establishment
Effective Date: February 6, 2026
Next Review: No events scheduled - static disclosure. Corrections or additions will be issued as a new version; previous versions remain available.

Archival Status: Public record (intended permanent); superseded versions retained.

CERTIFICATION

I, W. Prasanna Abeysekera, hereby certify that:

1. I am the inventor of the subject matter disclosed in this document
2. The invention was conceived on or before February 3, 2026
3. This disclosure accurately represents my invention as of February 6, 2026
4. This publication is made voluntarily to establish prior art
5. I understand this publication may affect my patent rights

Signed: W. Prasanna Abeysekera

Prasanna_18-10-2025

Digitally signed by Prasanna_18-10-2025
DN: OU=NOMATEQ Innovation, O=GABEY Consulting Pty. Ltd., CN=Prasanna_18-10-2025, E=gabeyinfo@gmail.com
Reason: I am the author of this document
Location: Melbourne, Australia
Date: 2026.02.06 22:57:56+11'00'
Foxit PDF Reader Version: 2025.2.0

Date: February 6, 2026

Location: Melbourne, Australia
