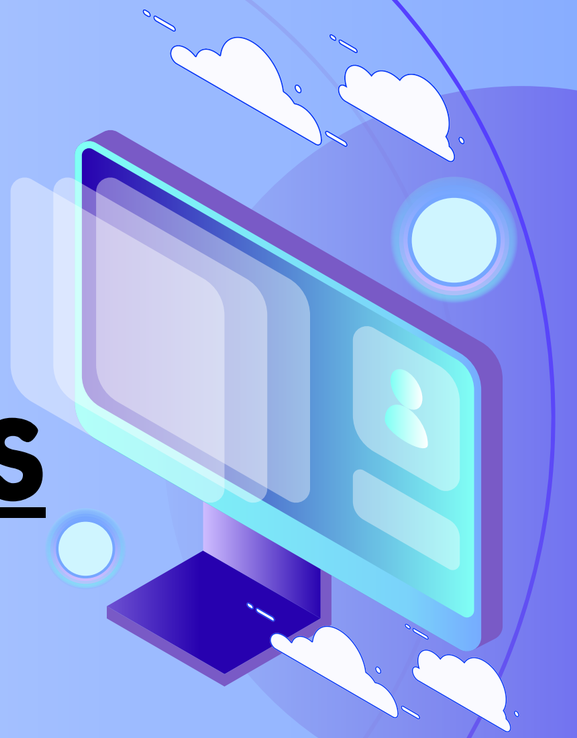
BMS COLLEGE OF ENGINEERING
DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING
PROJECT PHASE -2

# BIOMETRICS BASED KEY GENERATION USING ELECTROENCEPHALOGRAMS

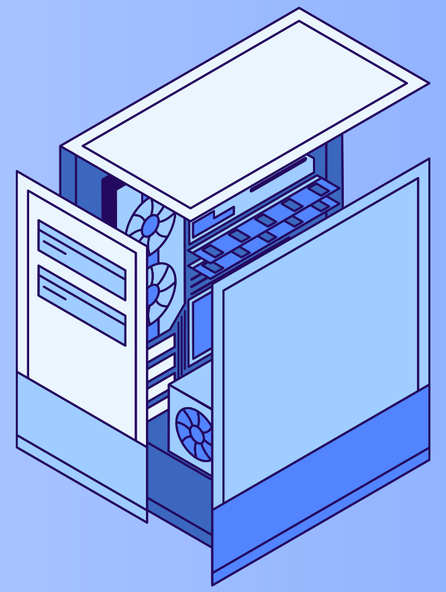


BATCH NO:24
TEAM MEMBERS:
1.Charoo K C - 1BM21IS047
2.Nitisha Bhatta - 1BM21IS108
3.Prathima A - 1BM21IS118

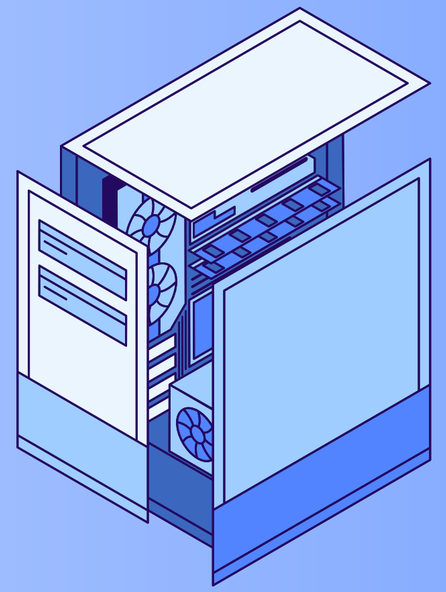
UNDER THE GUIDANCE OF
Dr.K.R.Mamatha
ASSISTANT PROFESSOR
DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

# AGENDA

- Introduction
- Objective
- Problem Statement
- SRS
- System Design
- Detailed Design
- Methodology
- Technology Stack
- Implementation
- Testing
- Results
- Conclusion
- Future Enhancement
- Project Outcome
- References



# INTRODUCTION



- Traditional biometric systems (fingerprints, iris scans, facial recognition) are vulnerable to compromise, leaving individuals at risk of identity theft.
- EEG-based biometrics enhance security but raise privacy concerns due to the sensitive nature of brain data, including cognitive and emotional information.
- A proposed privacy-preserving, cancelable EEG biometric system can safeguard user data while enabling revocation and replacement of compromised templates.

# EXISTING SYSTEM

The existing system, NeuroShield, leverages brain waves or EEG signals to generate unique cryptographic keys, offering a new paradigm of cancelable biometrics. The process relies on cognitive activities to produce biometric-based keys that are secure, unique, and difficult to forge.

**Merits:**

- **High Security:** EEG signals are unique to individuals and nearly impossible to forge due to the unique neuronal wiring of each person.
- **Cancelable:** The system allows the biometric key to be changed by altering the cognitive task, enhancing adaptability in case of compromise.
- **Resilience to Coercion Attacks:** EEG signals change under stress, reducing the risk of unauthorized access .
- **Entropy and Randomness:** The high entropy in EEG biometrics ensures stronger cryptographic keys resistant to cryptanalysis.

## Demerits:

- **False Rejection Rate (FRR):** The system has a relatively high FRR, which may inconvenience users by denying legitimate access.
- **Dependence on Equipment:** The need for EEG recording devices and electrodes may limit widespread adoption.
- **Environmental Sensitivity:** Variations in data acquisition environments can impact the performance and repeatability of the system.

# PROBLEM STATEMENT

- Traditional biometric systems (e.g., fingerprint, facial recognition) are static and non-revocable.
- Once compromised, biometric data cannot be altered, leaving users permanently vulnerable to identity theft.
- Storing raw biometric templates increases privacy risks.

# SYSTEM ARCHITECTURE AND METHODOLOGY

## Enrollment

The system records EEG signals while users think of and perform specific cognitive tasks (e.g., Math, Reading, Relaxation), processes the signals using Fast Fourier Transform (FFT)

## AUTHENTICATION

The system authenticates the user by analyzing the incoming EEG data and comparing it against the stored template. Support Vector Machines (SVM) is utilized to classify and verify the user's identity based on the extracted feature vectors.

## KEY GENERATION

During login, the system validates the user by generating a cryptographic key derived from EEG features and comparing it with the stored key Maps the features to binary vectors through a segmentation and quantization process

# SYSTEM DESIGN

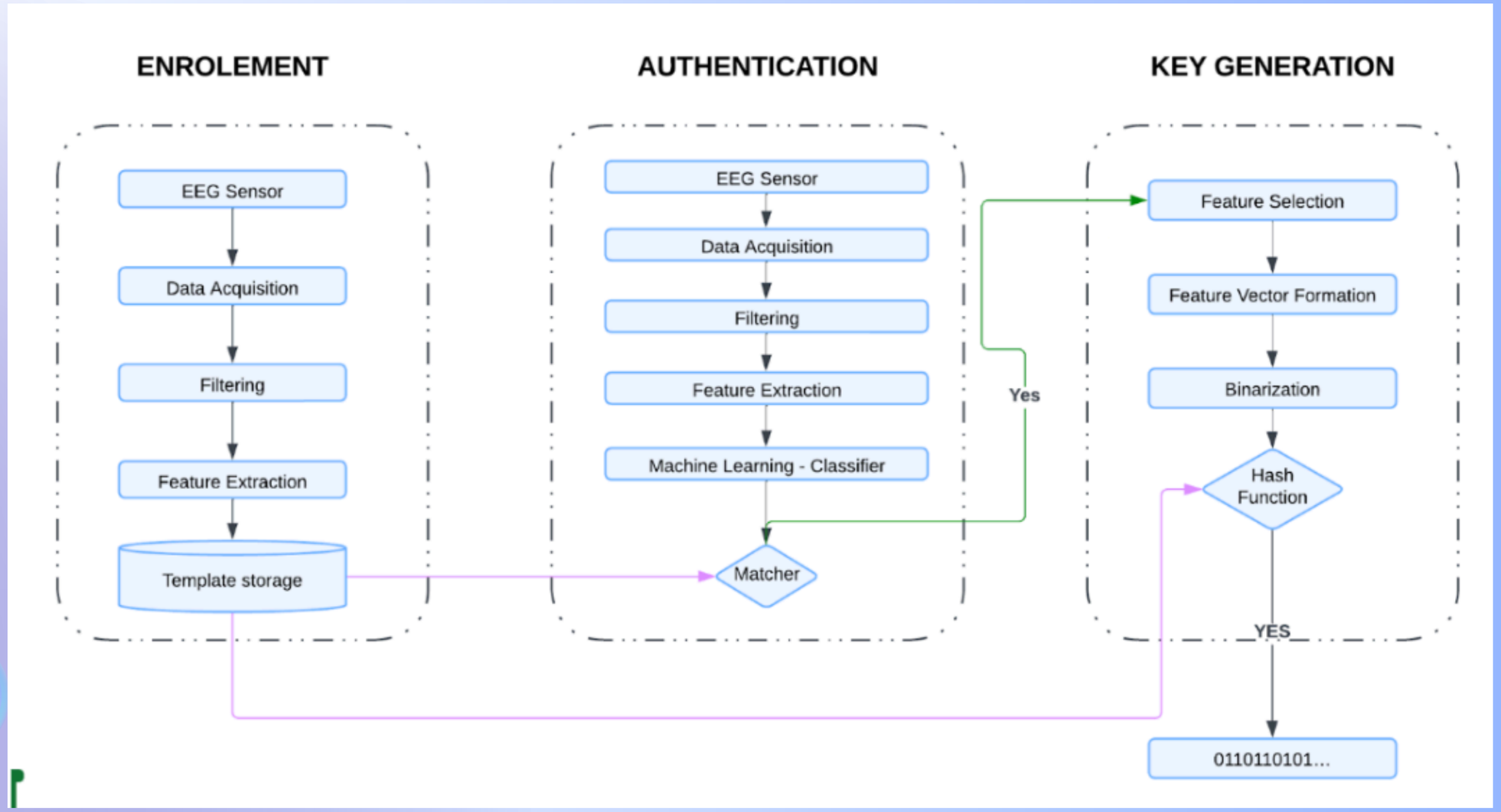



FIG 1 : SYSTEM DESIGN

# METHODOLOGY

**1. Data Collection & Simulation:**

o Simulate EEG signals for multiple users (1500 data rows -Wriring, Imagination ,Reading).

o Users will think of and perform specific tasks while EEG data is recorded.

o Generate and store the EEG dataset in CSV format.

| | Unnamed: 0 | trial number | sensor position | sample num | sensor value | \ |
|---|---|---|---|---|---|---|
| 0 | 5 | 0 | FP1 | 0 | -8.921 | |
| 1 | 6 | 0 | FP1 | 1 | -8.433 | |
| 2 | 7 | 0 | FP1 | 2 | -2.574 | |
| 3 | 8 | 0 | FP1 | 3 | 5.239 | |
| 4 | 9 | 0 | FP1 | 4 | 11.587 | |

| | subject identifier | matching condition | channel | name | time | |
|---|---|---|---|---|---|---|
| 0 | a | S1 obj | 0 | co2a0000364 | 0.000000 | |
| 1 | a | S1 obj | 0 | co2a0000364 | 0.003906 | |
| 2 | a | S1 obj | 0 | co2a0000364 | 0.007812 | |
| 3 | a | S1 obj | 0 | co2a0000364 | 0.011719 | |
| 4 | a | S1 obj | 0 | co2a0000364 | 0.015625 | ) |

# METHODOLOGY

**2. Feature Extraction:**

o Apply FFT to extract frequency-domain features from EEG signals.

o Normalize extracted features for improved classification.

o The EEG signals are processed using Fast Fourier Transform (FFT)

o Statistical measures such as mean, power, and standard deviation are calculated for each frequency band (Delta, Theta, Alpha, Beta, and Gamma).

o These features are then combined to form robust vectors for authentication and key generation.

```
def extract_fft_features(signal_row):
    fft_values = fft(signal_row)
    fft_features = np.abs(fft_values)[:len(fft_values)//2]
    return fft_features
```

```
eeg_signals = df.iloc[:, 2:].values
fft_features = np.array([extract_fft_features(sig) for sig in eeg_signals])
print("FFT Features Shape:", fft_features.shape)
```

# METHODOLOGY

**3. Model Training:**

o Train an SVM, on the extracted features to classify users based on EEG signals.

o Save the trained models for future predictions.

**4. Authentication Mechanism:**

o During login, users will think of the same task performed during enrollment.

o Record new EEG signals for the given task.

o Extract features and pass them through the trained models and compare it with the stored key.

o Grant or deny access based on key match.

**5. Deployment:**

o Build a Flask-based backend for processing and authentication.

o Design a simple HTML frontend for user interaction.

o Store user credentials and cryptographic keys in an PostgreSQL database.

# EXPECTED OUTCOMES

- Provide a reliable, non-replicable means of user authentication. Generate robust cryptographic keys that are resistant to conventional attacks.
- Offer a flexible, cancelable solution for biometric security, reducing risks associated with data breaches.
- Advance privacy-preserving biometric research by demonstrating EEG’s potential as a viable alternative to conventional biometrics like fingerprints or facial recognition.

# SYSTEM REQUIREMENT SPECIFICATION

## Functional Requirements:

1. **EEG Signal Acquisition:** The system should be able to capture EEG signals accurately using suitable sensors.
2. **Data Preprocessing:** The system must handle signal preprocessing, including noise removal and artifact rejection, to enhance the quality of the EEG data.
3. **Feature Extraction**: Extract relevant features from the EEG signal to be used for biometric identification.
4. **Cancelable Template Generation:** The system must generate cancelable EEG templates that can be updated or revoked based on user needs.
5. **Authentication Process**: A mechanism to match the processed EEG data with stored templates for user authentication.
6. **Privacy Preservation:** Ensure raw EEG data is not stored or exposed to prevent privacy violations.

## Non-functional Requirements:

1. **Security:** The system ensures robust security to protect biometric data and prevent unauthorized access.
2. **Scalability**: The system will be scalable to accommodate a large number of users and EEG templates.
3. **Efficiency:** Processing time for data collection, preprocessing, and authentication should be minimal to provide quick responses.
4. **Usability:** The system should be easy to use, with minimal user intervention required during the biometric authentication process.
5. **Flexibility:** Ability to adapt to various EEG devices and protocols used for data collection

# SYSTEM REQUIREMENT SPECIFICATION

## Hardware Requirements:

1. **Processing Unit**: A CPU or GPU capable of handling real-time signal processing and template generation.
2. **Storage**: Sufficient storage for maintaining user templates and processed data (though not raw EEG data).
3. **User Interface**: Hardware for displaying results and enabling user interaction (e.g., monitors or devices for feedback).

## Software Requirements:

1. **Template Generation & Storage System:** Software to generate and manage cancelable biometric templates securely.
2. **Authentication System:** Software for matching EEG-based templates with stored ones during the authentication process.
3. **Privacy Protection Tools:** Software to ensure no raw EEG data is stored in an accessible way, protecting user privacy.
4. **User Interface:** Software to interact with users and provide authentication results.

# DETAILED DESIGN

## CLASS DIAGRAM

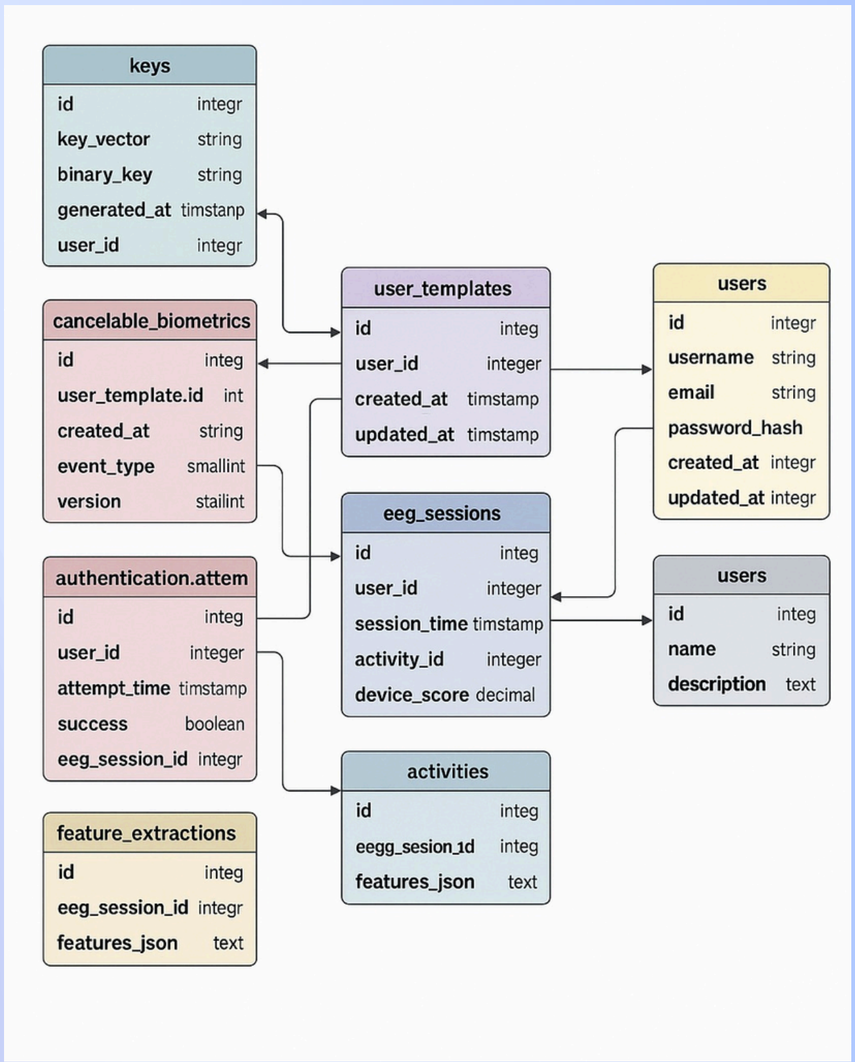



FIG 2 : CLASS DIAGRAM

# DETAILED DESIGN

## ACTIVITY DIAGRAM

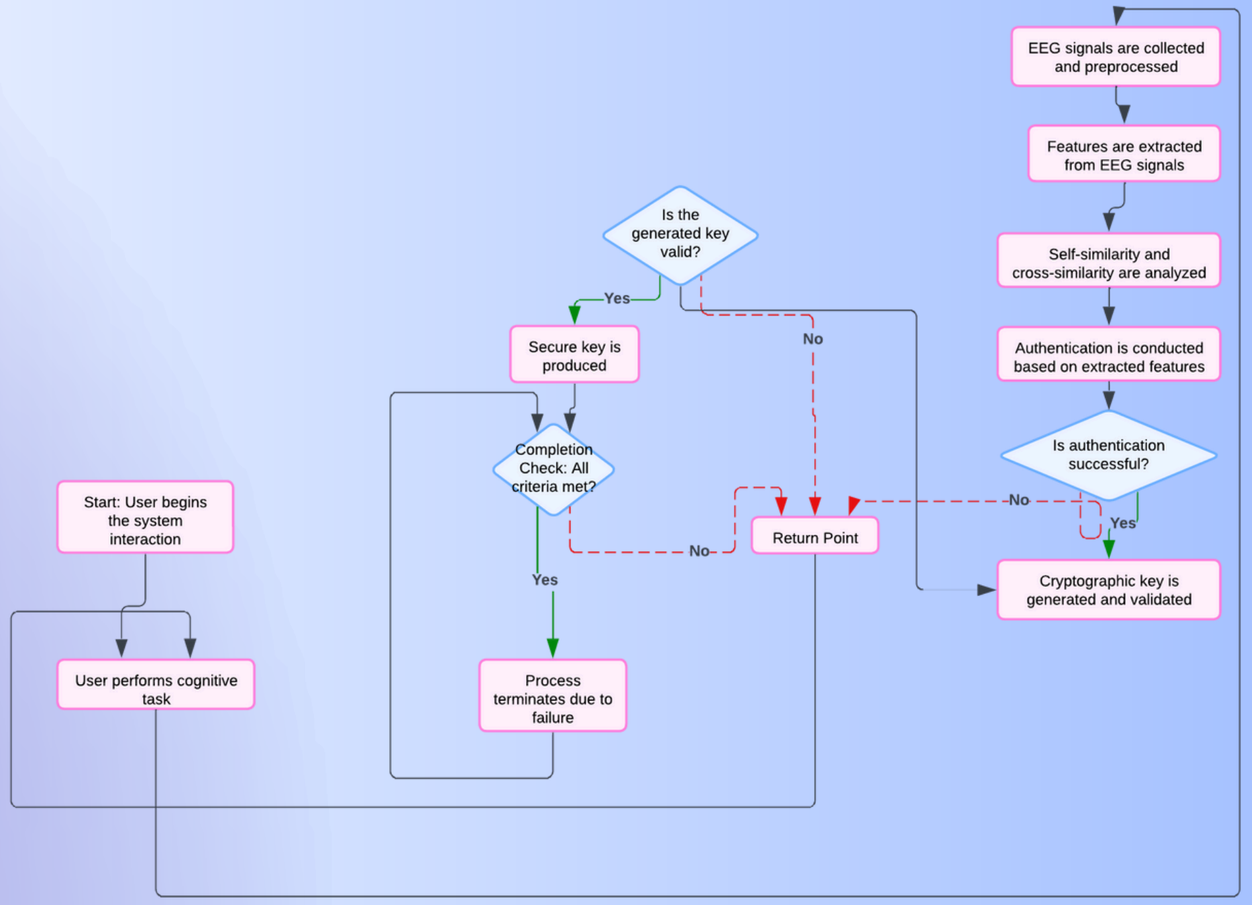



FIG 3: ACTIVITY DIAGRAM

# DETAILED DESIGN

## USE CASE DIAGRAM

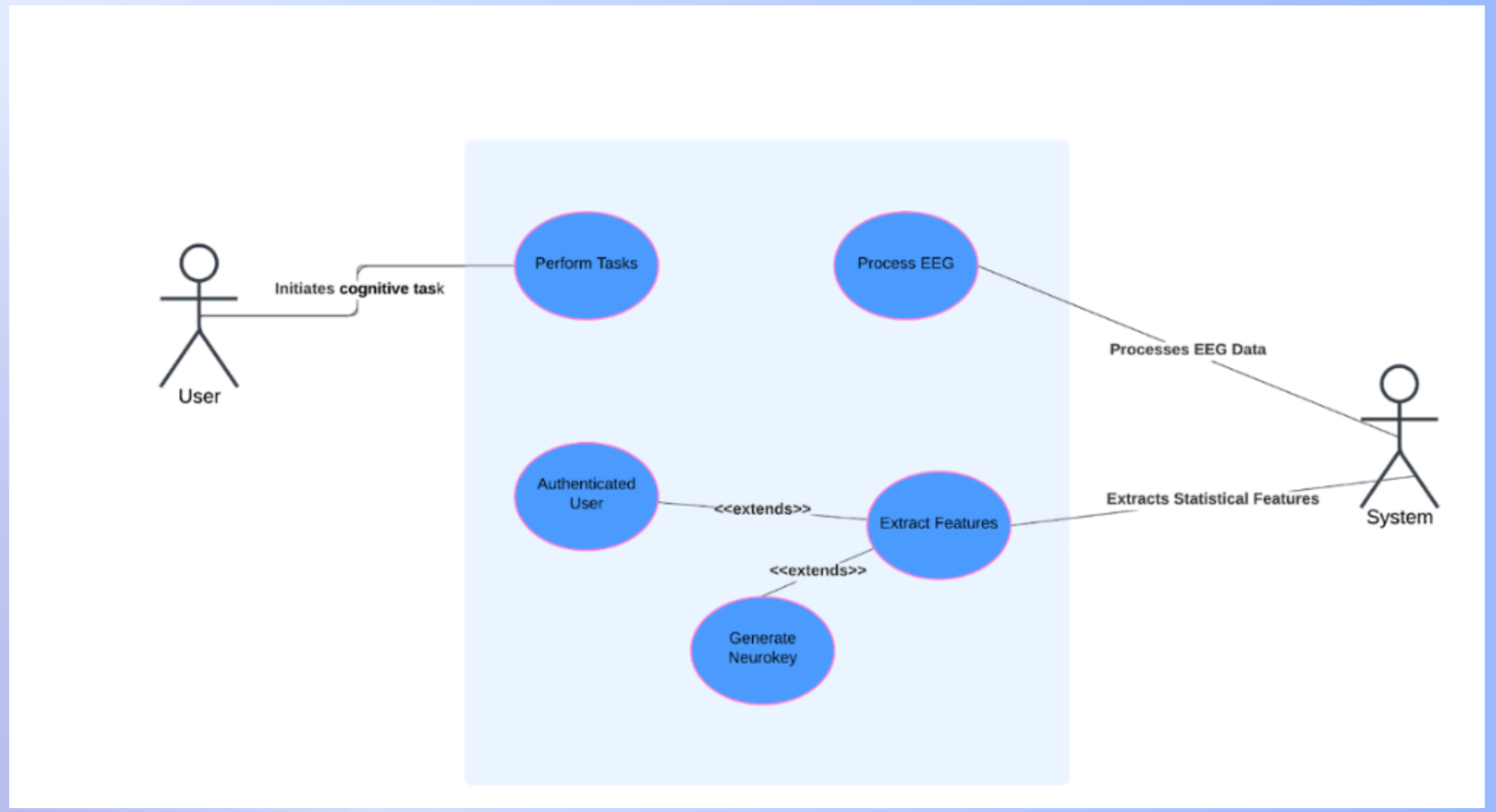



FIG 4: USE CASE DIAGRAM

# IMPLEMENTATION

## 1. Algorithm Steps

1. Enrollment Phase:
    - User enters a unique ID and selects a mental task.
    - Simulated EEG data is generated and stored.
    - Features are extracted and saved for future authentication.

# IMPLEMENTATION

2. Authentication Phase:
    - The user re-performs the same mental task.
    - The system compares the new features with the stored data using an SVM classifier.
    - If successful, the user proceeds to key generation.
3. Key Generation Phase:
    - Extracts top-K features using variance-based selection.
    - Binarizes the features and generates a SHA-256 hash.
    - Stores the neurokey, user ID, and task in PostgreSQL.

# IMPLEMENTATION

4. Login System:
   - Authenticates the user via EEG task.
   - Regenerates the key and compares with the stored key in PostgreSQL.
   - Grants access on match.

5. Cancelable Biometrics:
   - Provides an option for users who forgot their task.
   - Allows generation of a new neurokey using a different task.
   - Updates the PostgreSQL record for seamless future logins.

# IMPLEMENTATION

**Data Structures Used:**

- Feature Vectors:
- Derived from EEG signals using Fast Fourier Transform (FFT) .
- Classification Models:
- SVM for authentication.
- Segmented Feature Regions:
- Used to define bins for key generation.
- Binary Feature Quantization:
- Converts extracted EEG features into cryptographic keys.

# TECHNOLOGY STACK - TOOLS USED

- **Programming Language** : Python
- **Machine Learning** : Numpy, Scikit-learn (SVM)
- **Signal Processing** : FFT
- **Backend** : Flask
- **Database** : PostgreSQL
- **Frontend** : HTML, CSS

# TESTING

| FEATURE | TEST CASE | EXPECTED RESULT | STATUS |
|---|---|---|---|
| Enrollment Form | Input name and activity, then submit | EEG signal is captured, hash is generated and stored | SUCCESSFUL |
| Authentication Form | Input name and activity, then submit | EEG signal is captured, hash is generated and matched | SUCCESSFUL |
| Hash Generation | Triggered after signal capture | Unique deterministic hash is shown in output | SUCCESSFUL |
| Mismatch Handling | Authenticate with a different activity | System should deny access or show mismatch error | SUCCESSFUL |

# RESULTS

**The model trained on Support Vector Machine (SVM) offers  an accuracy of 91.6% in user authentication using EEG signals**

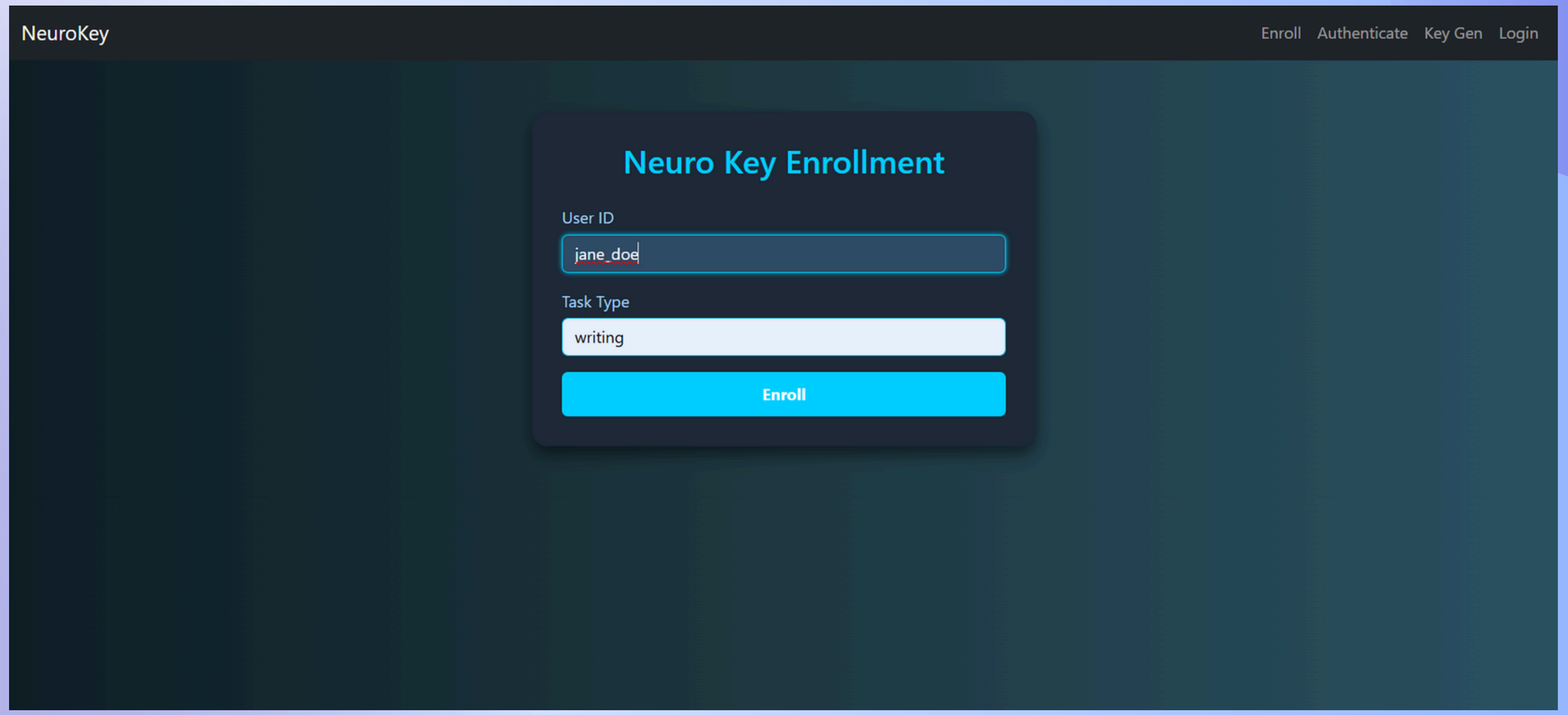



**Fig 1 : Enrollment**

# RESULTS

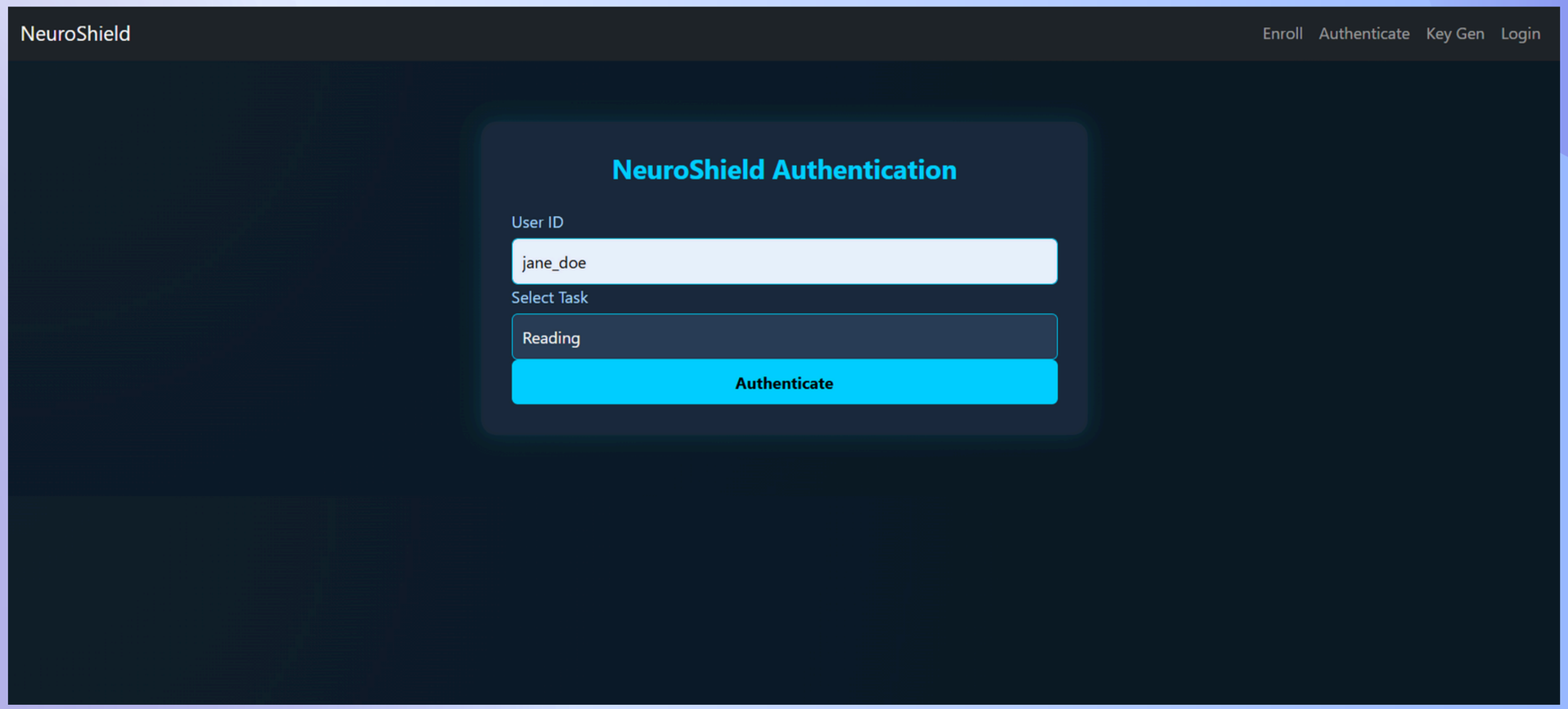



**Fig 2 : Authentication**

# RESULTS

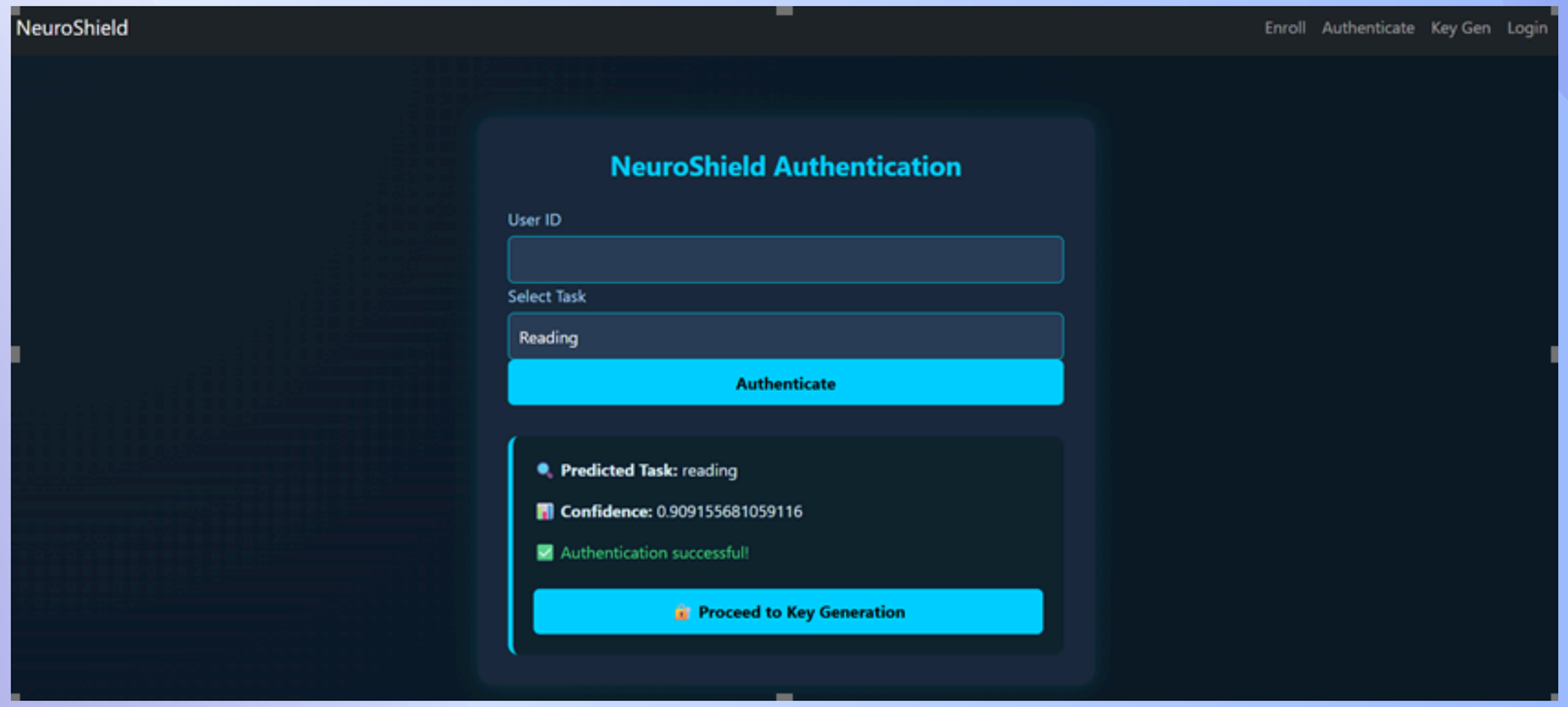



**Fig 3 : Neuro Key Authentication**

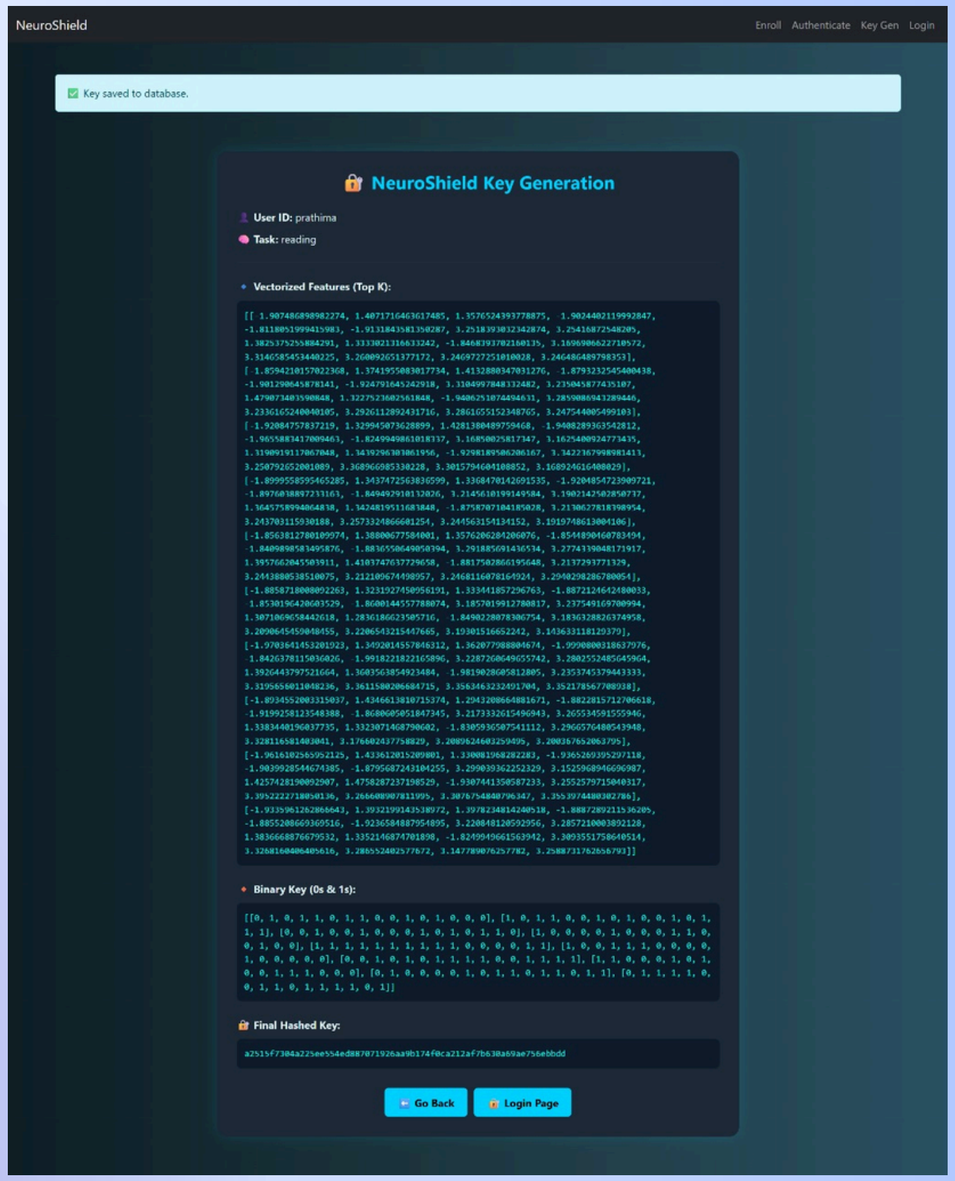
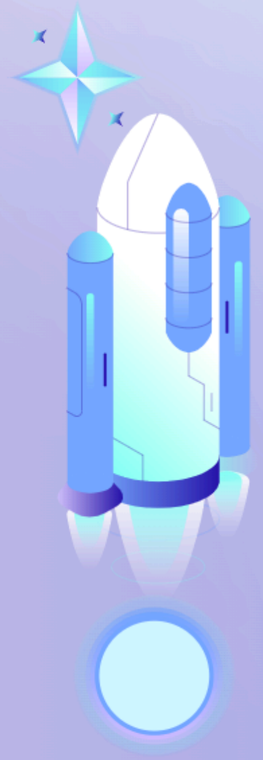



**Fig : Post-authentication interface leading to key generation**

# CONCLUSION

- Neuro Shield introduces a new era of authentication by transforming brainwave patterns into secure, revocable cryptographic keys. Unlike traditional biometrics, it empowers users with privacy and control, ensuring security that adapts with time and threat.
- Through simulation and prototyping, the system has shown high accuracy, consistency, and spoof resistance. Its integration with a web-based interface and secure backend highlights practical viability in real-world use cases.
- As brain–computer interfaces evolve, Neuro Shield opens the door to secure access across healthcare, IoT, and immersive environments. It lays a strong foundation for future-ready, mind-driven authentication systems.

# FUTURE TRENDS



**Neuroadaptive Security Systems:**
Future EEG systems will dynamically adjust security protocols based on real-time brainwave patterns, such as stress or focus levels, offering personalized and adaptive authentication.

**Brainwave-Driven Multi-Factor Authentication:**
EEG patterns could be combined with other biometric data (e.g., fingerprint or facial recognition) for highly secure, multi-layered authentication, ensuring that access is granted only to the rightful user.

**Cognitive Task-Triggered Security:**
Users could change security settings or access permissions by simply engaging in specific mental tasks or thought patterns, offering a completely hands-free way to control access.

**Emotional State Detection for Security Flexibility:**
EEG systems will evolve to detect emotional states, allowing systems to adapt security measures based on whether the user is stressed, relaxed, or under pressure, ensuring more context-aware and resilient authentication.

# PROJECT OUTCOMES

- **Enhanced Security:**
- Introduced EEG-based biometric authentication, eliminating reliance on traditional passwords or tokens vulnerable to theft and misuse.
- **Cancelable Biometrics:**
- Enabled users to regenerate a new neurokey via alternate mental tasks, ensuring both flexibility and security.
- **Simulated EEG Data Utilization:**
- Successfully simulated EEG signals tied to unique mental states, showcasing the feasibility of mental-task-based authentication.
- **Robust Storage and Management:**
- Secure neurokeys stored in a PostgreSQL database using SHA-256 hashing, ensuring high-level cryptographic integrity.
- **Efficient Feature Processing:**
- Applied variance-based feature selection and SVM classifiers to accurately identify and authenticate users based on EEG patterns.
- **Forgotten Task Recovery:**
- Implemented a seamless regeneration mechanism allowing users to securely recover access without system compromise.

# REFERENCES


[1] G. Bajwa and R. Dantu, “Neurokey: Towards a new paradigm of cancelable biometrics-based key generation using electroencephalograms,”Comput. Secur., vol. 62, pp. 95–113, 2016.

[2] D. Nguyen, D. Tran, D. Sharma, and W. Ma, “On the study of EEG-based cryptographic key generation,” Procedia Comput. Sci., vol. 112,pp. 242–249, 2017.

[3] L. Hern´andez- ´Alvarez, J. S. G´omez-Barrero, A. Morales, and J. Fierrez, “KeyEncoder: A secure and usable EEG-based cryptographic key generation mechanism,” Pattern Recognit. Lett., vol. 168, pp. 148–157, 2023.

[4] M. Wang, S. Wang, and J. Hu, “PolyCosGraph: A privacy-preserving cancelable EEG biometric system,” IEEE Trans. Dependable Secure Comput., vol. 19, no. 5, pp. 3938–3952, 2022.

[5] M. Wang, S. Wang, and J. Hu, “Cancellable template design for privacy-preserving EEG biometric authentication systems,” IEEE Trans. Inf. Forensics Security, vol. 17, no. 9, pp. 2541–2554, 2022.

[6] M. Wang, X. Yin, and J. Hu, “Cancellable deep learning framework for EEG biometrics,” IEEE Trans. Inf. Forensics Security, vol. 19, pp.1100–1113, 2024.

[7] M. Khan, S. H. Khan, and F. Khalid, “A comprehensive review of EEG-based biometric cryptosystems and authentication,” PLoS One, vol. 18,no. 1, e0280161, 2023.

[8] A. Sharma and R. K. Sharma, “Cancelable biometric systems depend on ntentionally altering biometric data using techniques like biometric salting or non-invertible transforms,” PLoS One, vol. 19, no. 4, e0291234, 2024.


.

# REFERENCES

[9] S. Ahmed, M. Iqbal, and T. A. Gull, “Cancelable biometric key generation and template protection using Double Random Phase Encozding DRPE),” J. Adv. Res., vol. 44, pp. 121–134, 2024.
[10] M. A. Islam, S. S. Islam, and F. A. Khan, “EEG-based multi-subject and multi-task biometric authentication system for military applications,” Int. J. Commun. Syst., vol. 36, no. 5, e5123, 2023.
[11] C. Hernandez and M. Husain, “Investigating data protection mechanisms or EEG biometric authentication,” in Proc. IEEE Int. Conf. Big Data(BigData), Dec. 2024, pp. 1234–1241.
[12] R. V. Yadav and G. Bajwa, “Emotional influences on cryptographic key generation systems using EEG signals,” ResearchGate, Sep. 2018.
[13] F. M. Alhussein and M. Mahdi, “Multimodal cancelable biometric authentication system based on EEG signal for IoT applications,” ResearchGate, Aug. 2023.
[14] G. Bajwa and R. Dantu, “A study on the stability of EEG signals for user authentication,” ResearchGate, Oct. 2015.
[15] S. Wang and J. Hu, “Do EEG-biometric templates threaten user privacy?,” ResearchGate, Jul. 2018.
[16] F. Liu, M. Wang, and S. Wang, “EEG-based biometric template protection with deep learning and h

# THANK YOU!

# TECHNOLOGY STACK - TOOLS USED

**A. Programming Language: Python**

- **Purpose:** Core language for developing backend logic, ML models, and signal processing.
- **Libraries Used:** NumPy, Pandas, SciPy, Scikit-learn.
- **Application in Neuro shield:**
  - Data loading, preprocessing, and cleaning.
  - Signal transformation and feature extraction.
  - Building and training machine learning models.

# TECHNOLOGY STACK - TOOLS USED

**B. Machine Learning: Scikit-learn**

- **Purpose:** Implements ML algorithms for classification and authentication**.**
- **Models Used:**
  - Support Vector Machine (SVM)
- **Application in Neuro shield:**
  - Trains models on EEG features.
  - Classifies users based on brainwave patterns.
  - Evaluates model performance using accuracy and precision metrics.

# TECHNOLOGY STACK - TOOLS USED

**C. Signal Processing: SciPy (FFT)**

- **Purpose:** Extracts frequency-domain features from EEG signals using FFT.
- **Method Used:** Fast Fourier Transform (FFT) – efficient implementation of DFT.
- **Application in Neurokey:**
  - Transforms EEG from time domain to frequency domain.
  - Extracts Delta, Theta, Alpha, Beta, and Gamma band features.
  - Features used for authentication and cryptographic key generation.

# TECHNOLOGY STACK - TOOLS USED

**D. Backend: Flask**

- **Purpose:** Web framework for handling server-side logic and API routing.
- **Application in Neuro shield:**
  - Hosts the model and handles feature input/output.
  - Connects frontend requests to backend processing.
  - Sends back classification and key generation results.

# TECHNOLOGY STACK - TOOLS USED

**E. Database: PostgreSQL**

- **Purpose:** Lightweight local database for storing authentication data.
- **Application in Neuro shield:**
  - Stores user credentials, EEG logs, and generated keys.
  - Maintains history of successful/failed authentications.
  - Ensures local storage without external dependencies.

**F. Frontend: HTML, CSS**

- **Purpose:** Builds the user interface for interaction and visualization.
- **Application in Neuro shield:**
  - User uploads EEG data and receives authentication result.
  - Displays classification status, key generation output.
  - Ensures responsive and interactive experience.