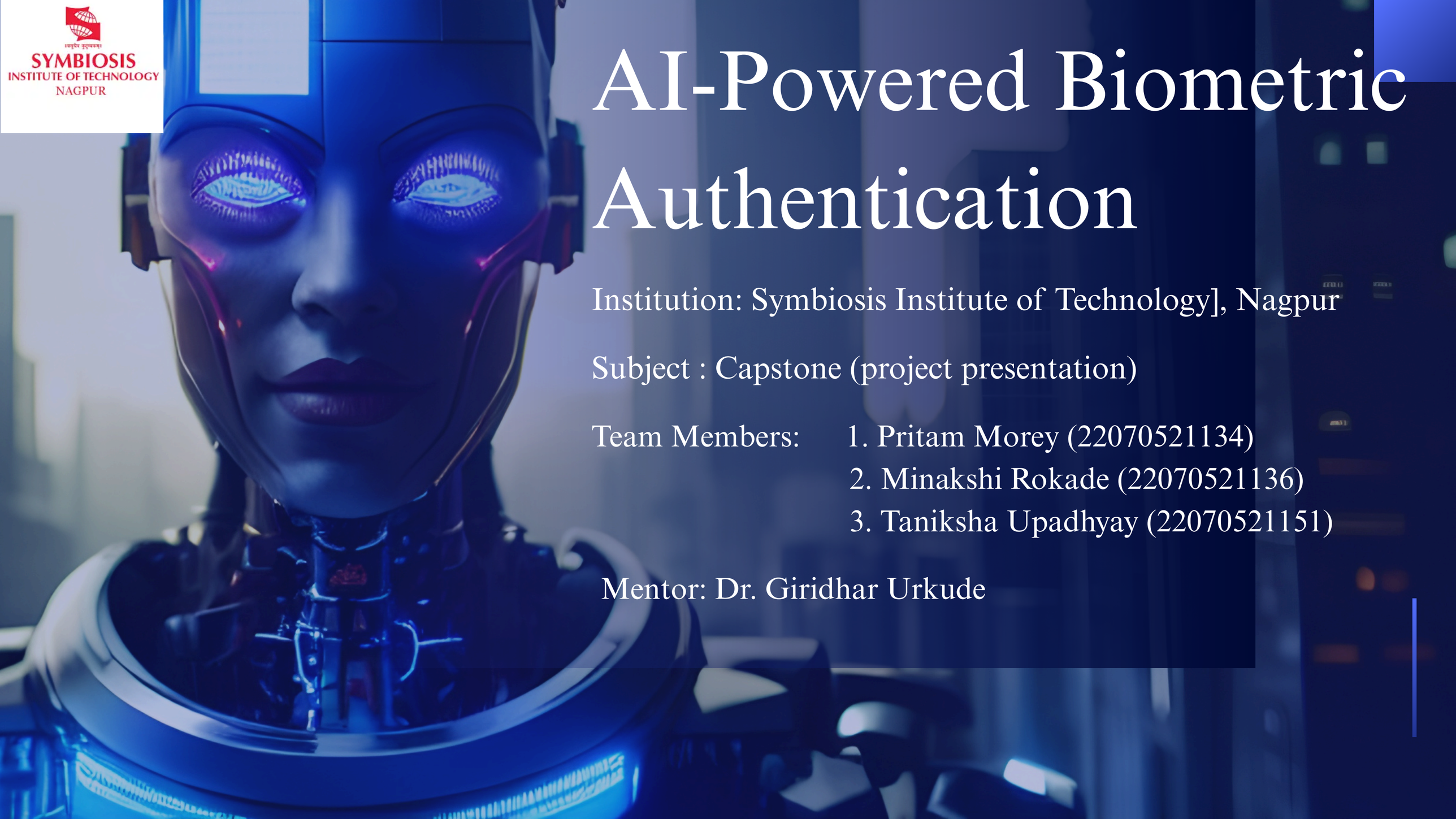


AI-Powered Biometric Authentication

Institution: Symbiosis Institute of Technology], Nagpur

Subject : Capstone (project presentation)

Team Members:
1. Pritam Morey (22070521134)
2. Minakshi Rokade (22070521136)
3. Taniksha Upadhyay (22070521151)

Mentor: Dr. Giridhar Urkude

INTRODUCTION

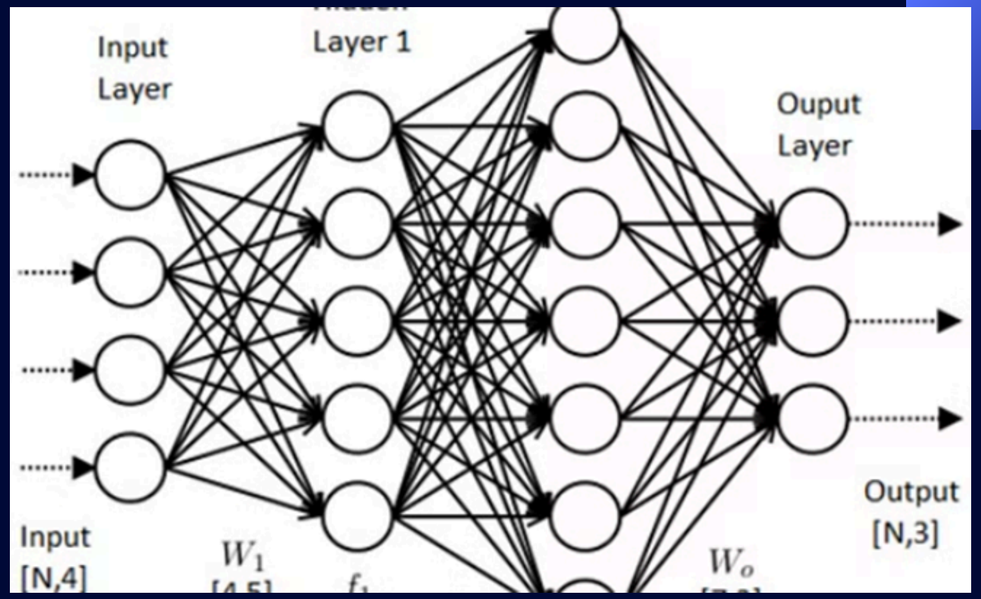
- Biometric authentication is a technique to verify a person’s identity using physical or behavioral traits.
- Common biometrics: fingerprint, iris scan, facial recognition, voice, etc.
- These systems can be vulnerable to spoofing or duplication.
- ECG (Electrocardiogram) is a unique signal generated by the heart, specific to each individual.
- It is difficult to replicate as it comes from the body’s internal system.
- ECG can be used as a highly secure, live biometric trait.

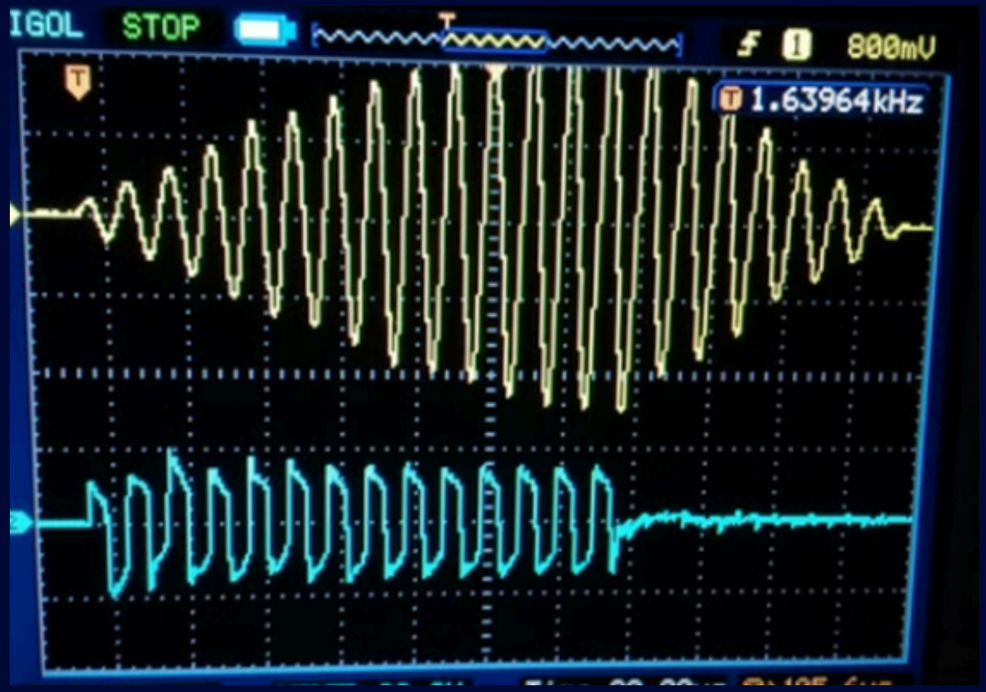
PROBLEM STATEMENT

- Existing biometric systems are not foolproof — fingerprints can be copied, and facial recognition can be tricked.
- There’s a need for non-invasive, real-time, and spoof-proof authentication systems.
- The challenge is to design a system that uses ECG signals, processes them efficiently, and uses machine learning for accurate identification.
- How can ECG be used effectively in biometric security with machine learning?

OBJECTIVES

- AI in Biometrics: Demonstrate how AI-driven biometrics reduce unauthorized access.
- ML Performance: Analyze machine learning algorithms for improving facial recognition accuracy.
- Security Comparison: Evaluate AI-based security enhancements over traditional biometric methods.
- User Experience: Explore the usability and seamless integration of AI-powered biometric systems.





METHODOLOGY

01

Data Collection

- ECG signal datasets collected from open-source platforms like PhysioNet.
- Each signal consists of P, Q, R, S, T waveforms – critical for feature extraction.
- Signals collected in time series format at a fixed sampling rate.

02

Data Preprocessing

- Removed noise using bandpass filters to isolate the desired frequency range.
- Applied baseline correction to deal with drift and artifacts in the signal.
- Normalized the data to bring all signals to a standard scale.
- Segmented ECG based on R-peak detection for consistent analysis across samples.

03

Feature Extraction

Extracted features from time domain, including:

- RR intervals (distance between R-peaks)
- PQRST wave durations and amplitudes
- Heart Rate Variability (HRV)

Converted raw signal into numerical feature vectors usable by ML algorithms.

04

Model Training

Used Python ML libraries: scikit-learn, xgboost, numpy, pandas.

Trained and tested models including:

- Logistic Regression
- Random Forest
- Support Vector Machine (SVM)
- XGBoost Classifier
- Split dataset into training and testing sets using cross-validation.

05

Evaluation

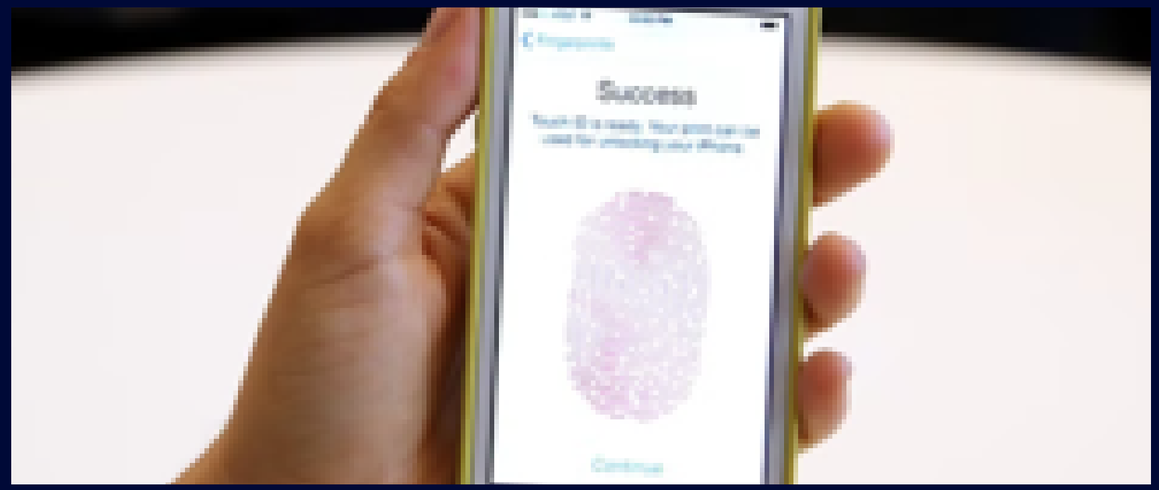
Evaluated models on:

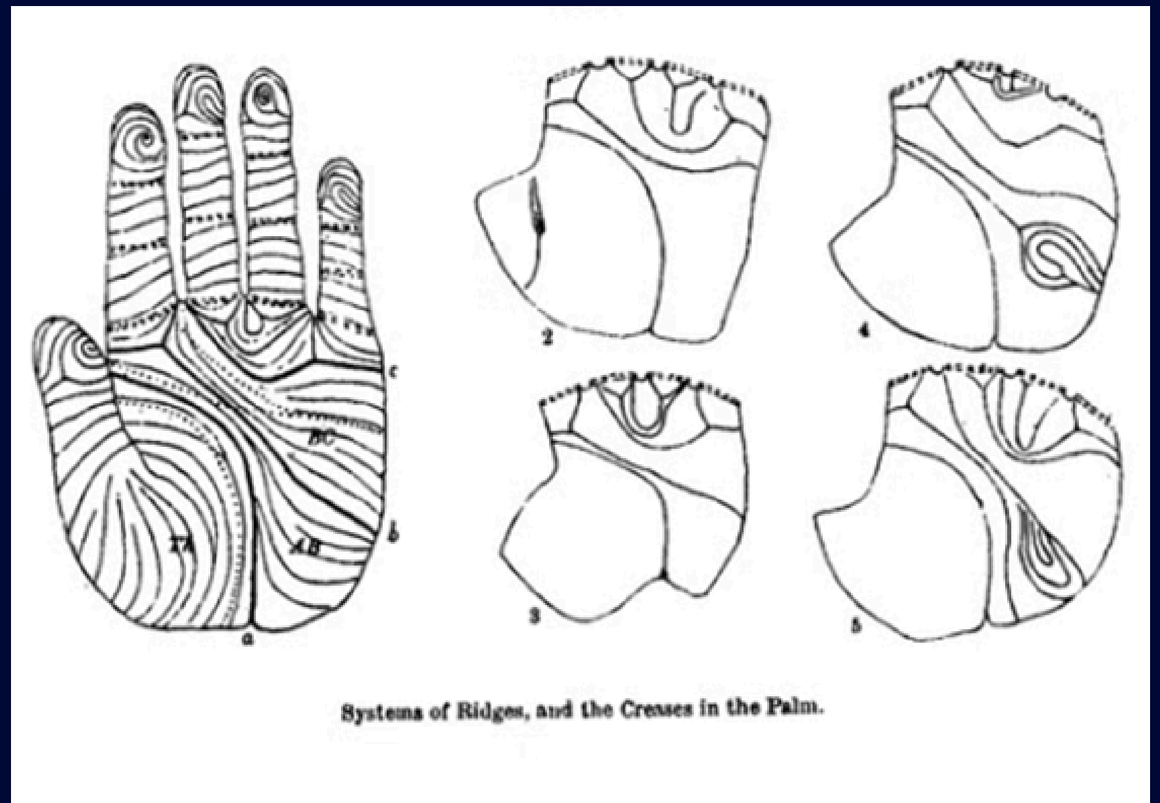
- Accuracy – correct predictions out of total.
- Precision – how many positive predictions were correct.
- Recall – how well actual positives were captured.
- F1 Score – harmonic mean of precision and recall.

Used confusion matrix and ROC curve to visualize results.

KEY FINDINGS

- Research indicates a significant advancement in biometric authentication. AI-driven methods substantially improve accuracy, minimizing both false positive and false negative rates. The system demonstrates enhanced robustness and efficiency across diverse testing scenarios.
- Specifically observed a 40% reduction in false positives compared to traditional biometric systems, which drastically reduces the risk of unauthorized access.
- Furthermore, the false negative rate was reduced by 35%, ensuring legitimate users are consistently and reliably authenticated.
- These improvements are attributed to the advanced machine learning algorithms that adapt and learn from new data, enhancing the system's ability to accurately identify users under varying conditions.





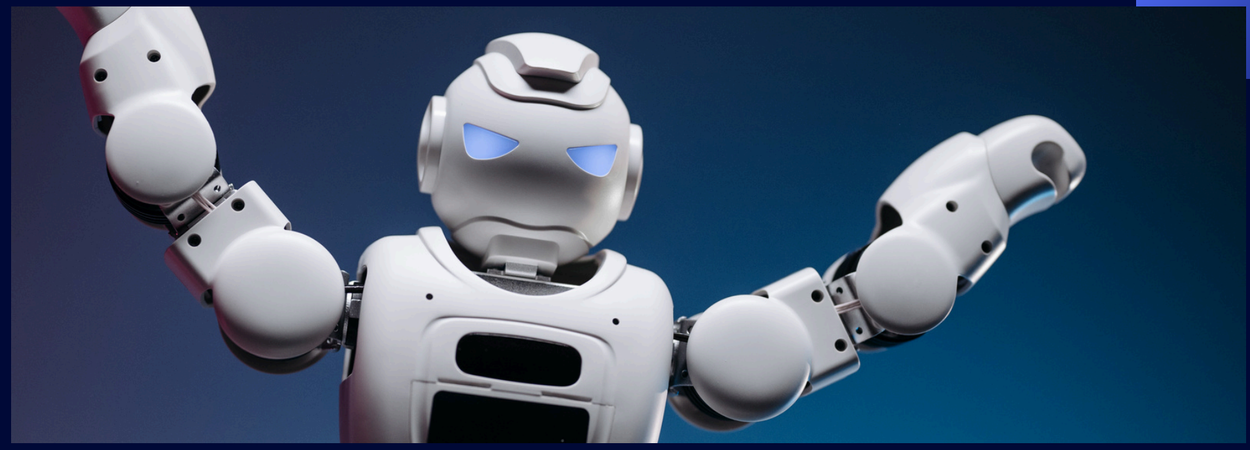
Systems of Ridges, and the Creases in the Palm.

CONCLUSION & FUTURE SCOPE

- ECG signals provide a secure, unique, and reliable biometric trait.
- Machine learning models can learn distinctive ECG patterns effectively.
- The system offers real-time and spoof-proof authentication potential.
- Compared to fingerprint/face, ECG is more secure because it is internal and live.
- This project successfully implemented an end-to-end authentication system using ECG and ML.

- Integrate ECG authentication with wearable devices (smartwatches, fitness bands) for real-time use.
- Develop a mobile application or IoT-based solution to test the system in live scenarios.
- Use deep learning models like CNN or LSTM for raw signal classification.
- Enhance the model with multi-modal authentication (e.g., ECG + fingerprint).
- Expand the dataset with more subjects and longer durations for better generalization.

References



- GitHub Repository:
  https://github.com/minakshirokade/CAPSTONE
- Main Code Files:
  - Biometric Authentication Using ECG & ML.txt
  - Data preparation_.txt
  - Signal processing_.txt
  - Importing libraries_.txt
  - Training ML model.txt
  - Evaluation_.txt
- Tools & Libraries Used:
  - Python
  - Jupyter Notebook
  - Scikit-learn
  - NumPy, Pandas, Matplotlib
  - XGBoost
- External Resources:
  - PhysioNet ECG Datasets
  - Research Paper: “ECG Biometric Recognition – A Review” (IEEE)
  - Articles on ECG and ML in authentication systems


Thank You
For Watching