Introduction of Prototype

Traditional access control systems rely on static credentials and perimeter-based security, which are ineffective against modern threats. Our prototype addresses this by using AI to evaluate real-time behavioral and contextual factors, enforcing Zero Trust principles for secure, dynamic access control.

Tools Used

Python , Scikit-learn (Random Forest Classifier)
Pandas & NumPy (data handling)
Matplotlib & Seaborn (visualization)
CLI Interface (for session simulation)

Model Training Mechanism

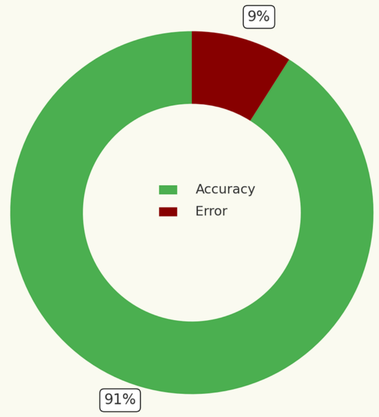
We used Random Forest Classifier for our Model, why ?

It handles both behavioral and contextual data , provides high accuracy and delivers interpretable decisions

OBJECTIVES

- Implement Zero Trust Architecture for modern access control.
- Score each session across five trust vectors.
- Train an AI model using labeled session data
- Make real-time access decisions for end-users and admins.
- Enforce strict admin access via perfect scoring

Model Accuracy



METHODOLOGY

25000 session logs with realistic scenario were extracted

- **Device Trust Score** (MAC recognition)
- **IP Trust Score** (Network recognition, VPN detection)
- **Location Trust Score** (realistic login time and travel feasibility)
- **Access Mechanism** (OS and Browser version detection)
- **User Behavior Score** (user behavior pattern detection)

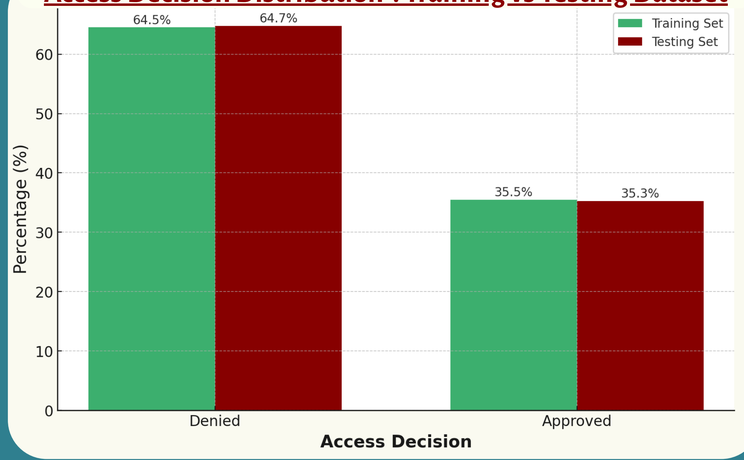
ZTA Compliance Mapping

Never Trust:	No implicit trust for any device or user
Always Verify:	Evaluate all sessions in real-time
Context-Aware:	Access decision based on user context
Least Privilege:	Strict enforcement for Admins
Dynamic Decision:	Approve/Deny based on score thresholds

Scope

- Applies to enterprise login environments (e.g., universities).
- Focus on desktop/laptop logins in Australian cities.
- Includes 7 user roles from Admin to Student.
- Designed as a modular proof-of-concept model.

Access Decision Distribution : Training vs Testing Dataset



AI-Driven Access Control: System Workflow

1. Log Collection
2. Data Cleaning & Preprocessing
3. Score Assignment (5 Mechanisms)
4. Random Forest Model Training
5. CLI-Based Access Testing
6. Visual Analysis & Reporting
7. Zero Trust Alignment Verification

Real imitation of our Access Control System Logic Flow

MAC Address: 28:EE:52:CD:91:7A Device Trust Score: 20 (companyOwned) IP Trust Score: 15 (External, VPN Detected)OS/Browser Score: 20 (macOS Ventura, Chrome ver129) Key Dynamic Score: 20 (Full Match) Location-Time Score: 20 (Valid time + feasible city transition) Final Score: 95 / 100

→ ACCESS GRANTED

Limitations

- No mobile or IoT simulation.
- Scoring uses fixed thresholds.
- Dataset is synthetic (no adversarial attacks).
- No biometric or MFA support.

Key Features

- Role-sensitive scoring logic.
- Strict Admin enforcement.
- CLI testing interface.
- Real-time contextual scoring.
- Fully interpretable model decisions.

Access Decision Logic

- Each login scored out of 100 (20 points per mechanism).
- Access Approved: Total score ≥ 75.
- Admins require a perfect 100.
- Any risky attribute lowers the trust score.

References

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture (SP 800-207)," NIST, 2020.

[2] M. Ali, R. Islam, and M. Faheem, "Revolutionizing Identity and Access Management with AI: A Zero Trust Approach Using User Behavior Analytics," Int. J. Artif. Intell. Mach. Learn., vol. 2, no. 1, pp. 35–49, 2022.

[3] A. Rizzardi, A. Pavani, and N. Capuano, "Harnessing AI-Powered Zero Trust Architectures for Proactive Cyber Defense," in Proc. Int. Conf. Computer and Cyber Security, 2023.

[4] I. A. Khan, M. Mustafa, and A. Yousaf, "AI-Powered Identity and Access Management in Zero Trust Architectures," J. Netw. Secur. Anal., vol. 14, no. 3, pp. 245–262, 2021.

[5] J. R. C. Nurse, S. Li, and S. Creese, "Behavioral Biometrics in Access Control: Opportunities and Risks," IEEE Secur. Privacy, vol. 20, no. 2, pp. 24–31, 2022.

AI DRIVEN ACCESS CONTROL WITH ZERO TRUST ARCHITECTURE

CHARLES DARWIN UNIVERSITY AUSTRALIA

Designed by: Krish Neupane(S375639), Pranjal Ghimire(S376779), Prashiddhika Shrestha(S376554), Rijip Prasain (S378021),