HYBRID INSIDER THREAT DEFENCE

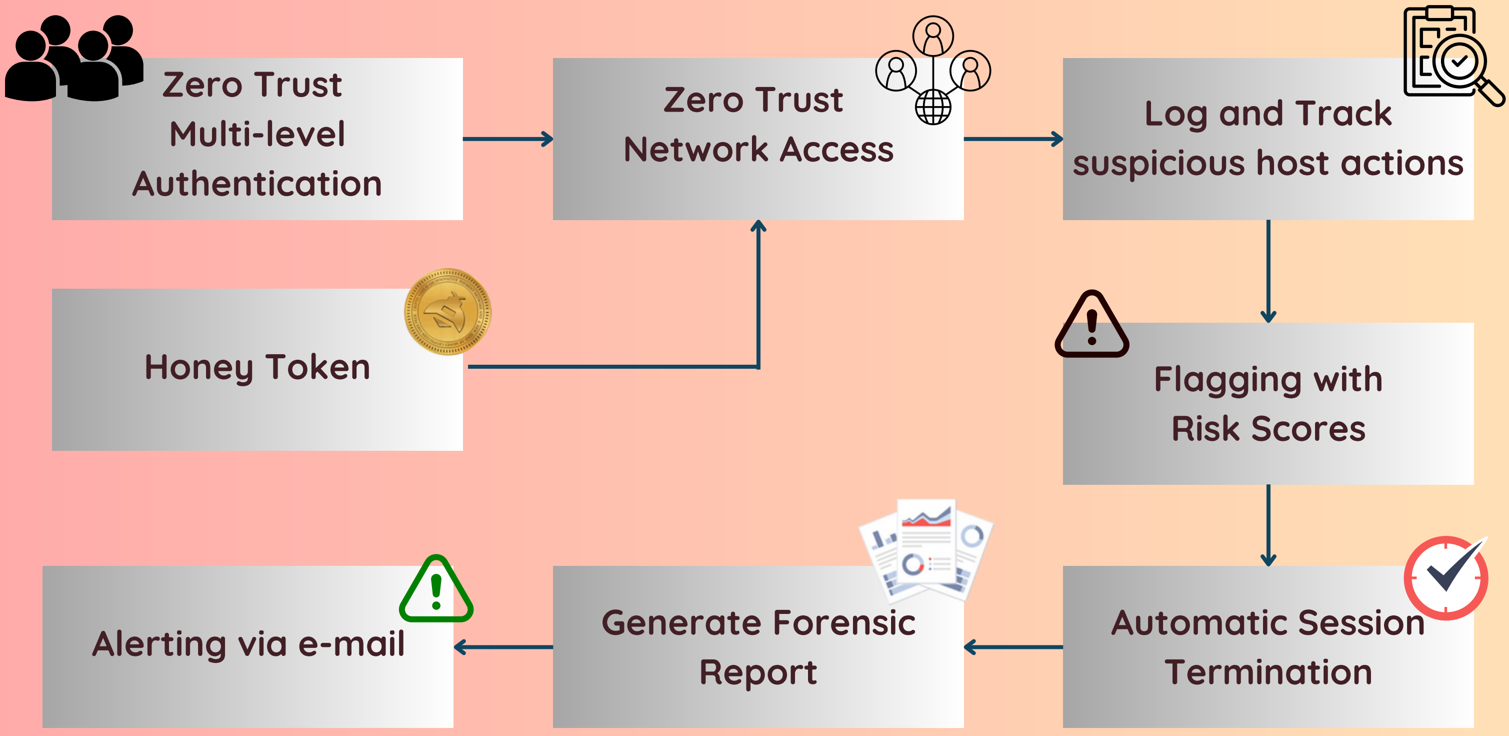
ABSTRACT

This project presents a real-time Insider Threat Detection System designed to identify, log, and respond to suspicious internal user behavior. By streaming user activities via Kafka, the system uses rule-based scoring to detect threats, raise alerts, and block users whose behavior crosses a defined risk threshold. MongoDB stores the logs and risk scores, while a Flask-based admin dashboard provides real-time visualization and control.

PROBLEM STATEMENT

Internal users often bypass traditional security layers, making insider threats one of the most challenging forms of cyberattacks. This project aims to proactively detect such threats by continuously monitoring user activity, identifying anomalies (like honeytoken access), and responding with immediate countermeasures.

SYSTEM DESIGN



Zero Trust Multi-level Authentication

Zero Trust Network Access

Log and Track suspicious host actions

Honey Token

Flagging with Risk Scores

Automatic Session Termination

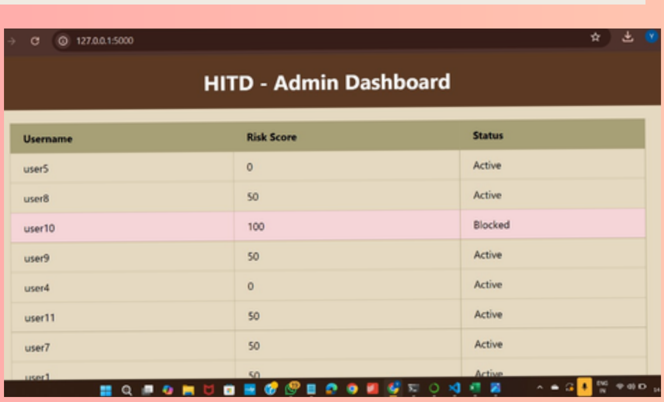
Generate Forensic Report

Alerting via e-mail

KEY FEATURES

- Real-time log processing via Kafka
- Honeytoken trap detection system
- Risk-based user behavior scoring
- Auto-blocking of high-risk users
- Admin dashboard for live tracking
- PDF reports for audit & compliance

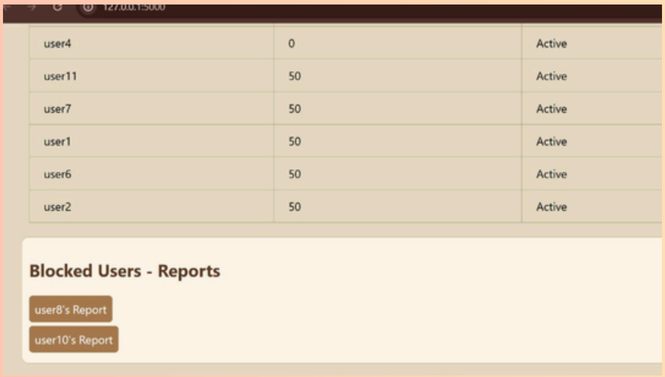
VISUALS



127.0.0.1:5000

HITD - Admin Dashboard

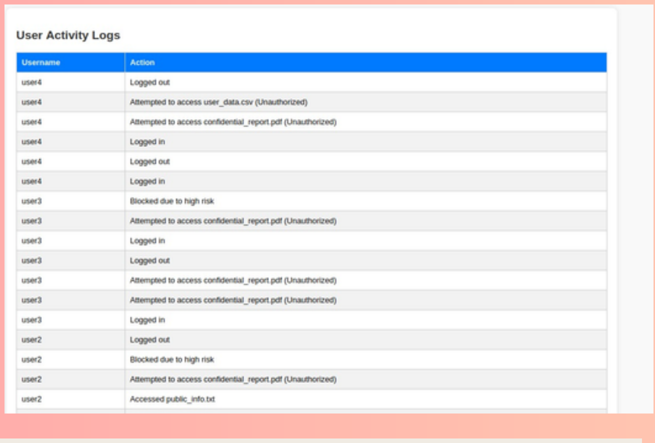
Username	Risk Score	Status
user5	0	Active
user8	50	Active
user10	100	Blocked
user9	50	Active
user4	0	Active
user11	50	Active
user7	50	Active
user1	50	Active



127.0.0.1:5000

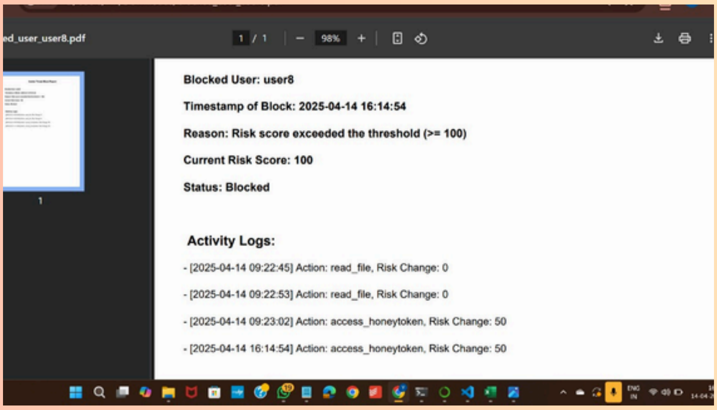
user4	0	Active
user11	50	Active
user7	50	Active
user1	50	Active
user6	50	Active
user2	50	Active

Blocked Users - Reports



User Activity Logs

Username	Action
user4	Logged out
user4	Attempted to access user_data.csv (Unauthorized)
user4	Attempted to access confidential_report.pdf (Unauthorized)
user4	Logged in
user4	Logged out
user4	Logged in
user3	Blocked due to high risk
user3	Attempted to access confidential_report.pdf (Unauthorized)
user3	Logged in
user3	Logged out
user3	Attempted to access confidential_report.pdf (Unauthorized)
user3	Attempted to access confidential_report.pdf (Unauthorized)
user3	Logged in
user2	Logged out
user2	Blocked due to high risk
user2	Attempted to access confidential_report.pdf (Unauthorized)
user2	Accessed public_info.txt



Blocked User: user8

Timestamp of Block: 2025-04-14 16:14:54

Reason: Risk score exceeded the threshold (>= 100)

Current Risk Score: 100

Status: Blocked

Activity Logs:

```
- [2025-04-14 09:22:45] Action: read_file, Risk Change: 0
- [2025-04-14 09:22:53] Action: read_file, Risk Change: 0
- [2025-04-14 09:23:02] Action: access_honeytoken, Risk Change: 50
- [2025-04-14 16:14:54] Action: access_honeytoken, Risk Change: 50
```

RESULTS

- Users triggering honeytoken alerts were blocked within seconds
- Risk scores updated in real-time and visualized instantly
- Logs stored efficiently in MongoDB
- PDF reports auto-generated on blocking events

TEAM

1. **PRASITAA K - 2022115014**
2. **YAAMINI T - 2022115067**
3. **ABINAYA K - 2022115070**