Hybrid Insider Threat Defence

Zero Trust Access with Dynamic Honeytokens

TEAM

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

INTRODUCTION

As organizations increasingly rely on digital infrastructure, the complexity and volume of security threats continue to grow. Among these, insider threats represent a particularly serious challenge—arising from individuals within the organization who misuse their access to steal, leak, or sabotage sensitive information. Traditional perimeter-based security models are no longer sufficient, as insiders often bypass external defenses. This project addresses the urgent need for advanced threat mitigation by integrating Zero Trust Network Access (ZTNA) with a Honeytoken-based detection system. By continuously validating user identities and monitoring for unauthorized access, this solution enhances security posture, ensuring early detection and effective response to potential insider attacks.

PROBLEM STATEMENT

Insider threats present a critical challenge to modern cybersecurity, as internal users with authorized access can intentionally or unintentionally compromise sensitive data and systems. Traditional security approaches often fall short in detecting and mitigating these risks in real-time. This project proposes a dual-layer defense system by integrating Zero Trust Network Access (ZTNA) with a Honeytoken-based detection mechanism. Through strict access validation and the deployment of deceptive honeytokens, the system identifies and reports suspicious activity. Leveraging Docker for containerized environments and Kafka for real-time data streaming, this solution ensures proactive monitoring and rapid detection of potential insider threats.

SOCIAL RELEVANCY

Preventing Cybercrime

Helps organizations detect and stop insider attacks before they lead to data breaches, protecting society from financial and informational harm.

Securing Healthcare Systems:

Prevents unauthorized access to patient medical records and personal health data. Ensures hospitals and clinics comply with HIPAA and data privacy regulations.

Combats Misinformation:

Prevents the unauthorized leak of sensitive news, journalist sources, and confidential reports.
Helps protect whistleblowers and investigative journalists from being compromised.

National Security:

Mitigates insider threats in critical sectors like healthcare, finance, and government, ensuring the safety of public infrastructure and national data.

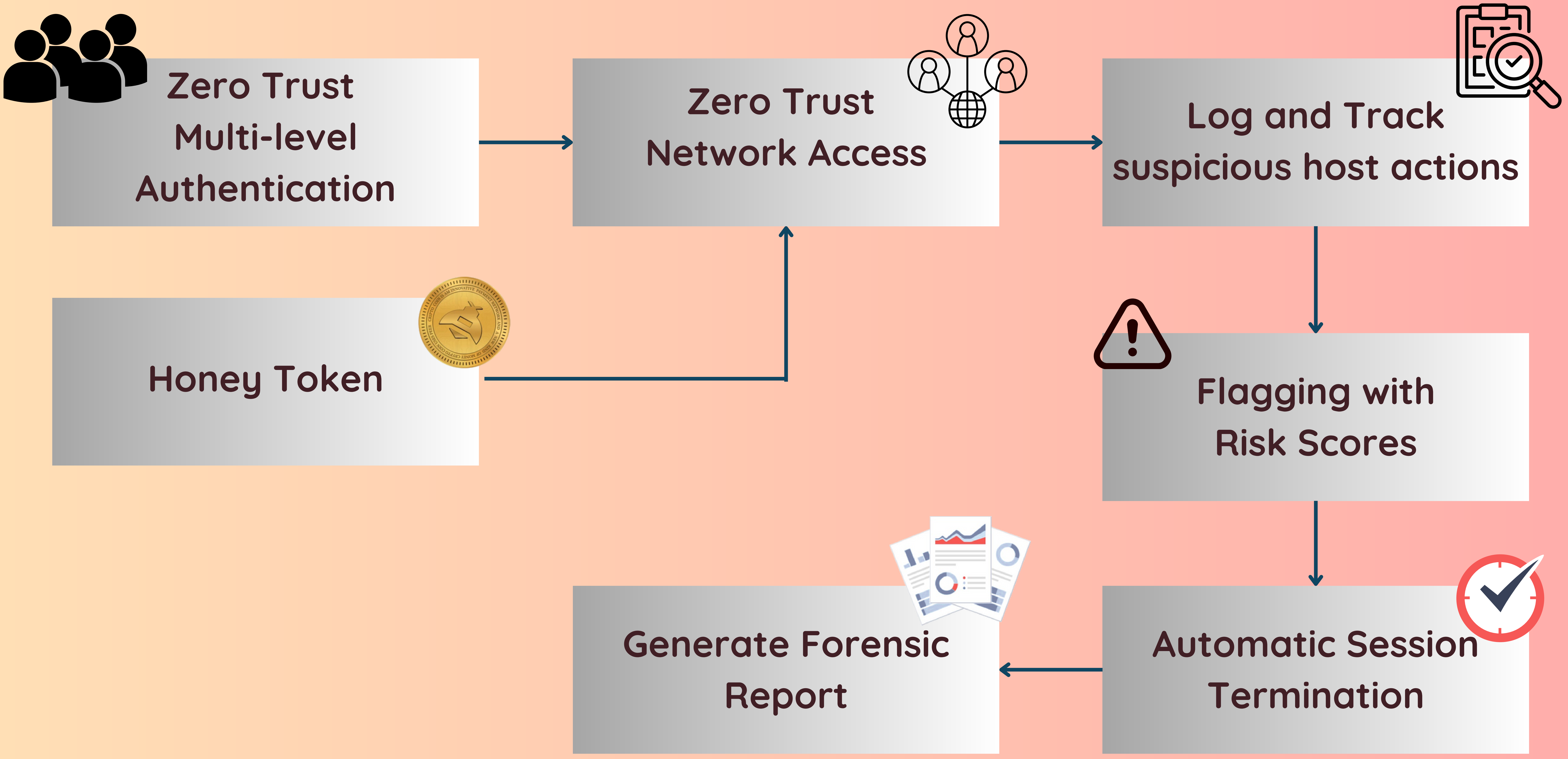
Protecting Human Rights:

Helps safeguard NGOs, human rights organizations, and political activists from data leaks.
Prevents internal sabotage in humanitarian projects that rely on digital security.

Preventing Corporate Epsionage:

Ensures a safe digital workspace by preventing manipulation of financial records.

SYSTEM ARCHITECTURE



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

DETAILED DESIGN:

USER AUTHENTICATION MODULE (ZTNA):

Purpose: Verify user identity and enforce least-privilege access.

Design:

- Implement multi-factor authentication (MFA) for every user.
- Use identity-based policies (e.g., specific access rights for each user role).

HONEYTOKEN GENERATOR:

Purpose: Create fake but realistic decoy data to detect unauthorized access.

Design:

- Auto-generate honeytokens (e.g., fake credentials, database entries).
- Deploy honeytokens in sensitive areas (e.g., financial records, admin files).
- Use Docker to isolate and deliver honeytokens securely.

EVENT STREAMING AND LOGGING:

Purpose: Track and capture all access attempts and honeytoken interactions.

Design:

- Set up Kafka to collect logs from the authentication and honeytoken layers.
- Create Kafka topics for each event type: "Access Logs," "Honeytoken Triggers," etc.
- Use Docker containers to deploy Kafka brokers for real-time data flow.

Anomaly Detection & Alert System

Purpose: Identify suspicious access patterns and trigger alerts.
Design:

- Monitor unusual behaviors (e.g., accessing honeytokens or odd login hours).
- Use a machine-learning model (e.g., Isolation Forest or Logistic Regression) to flag anomalies.
- Dockerize the ML model and connect it to the Kafka pipeline for continuous monitoring. Incident Response Module

Incident Response Module

Purpose: React to detected threats and enforce mitigation strategies.
Design:

- Lockdown user access upon honeytoken triggers.
- Notify administrators via automated alerts (e.g., email, Slack).
- Generate detailed audit logs for investigation.

TOOLS AND TECHNOLOGIES

- **Python (Core Logic):** Handles authentication and the honeytoken system.
- **Apache Kafka (Event Streaming):** Captures and monitors real-time user activities.
- **Streamlit (Admin Dashboard + Visualization):** Displays alerts, logs, and analytics from Kafka and the database.
- **Docker (Sandboxing + Deployment):** Simulates a corporate network environment for security testing.
- **SQLite / MongoDB (Database for Logs & Honeytoken Interactions):**
  - ➢ Stores user activity logs, flagged events, and honeytoken usage.
  - ➢ Acts as the backend data store for Streamlit’s dashboard.
  - ➢ Collects and processes security insights from Kafka streams.

WORKLOAD/MODULE SPLIT:

1 .User Authentication (Python) – Secure login, RBAC, honeytokens for tracking unauthorized access.

2. Real-Time Activity Streaming (Kafka) – Streams user actions for live monitoring & analysis.

3. Threat Detection (Python + Kafka) – Identifies abnormal behavior, detects insider threats.

4. Logging & Storage (Kafka + SQLite/MongoDB) – Stores activity logs for auditing & investigation.

5. Alerts & Notifications (Kafka + Python) – Sends real-time security alerts via email, SMS, or dashboard.

6. Admin Dashboard (Streamlit) – Interactive UI for monitoring logs, alerts & analytics.

7. Deployment & Simulation (Docker) – Containerized setup, simulates a corporate network.

REFERENCES

1. Ward, R. and Beyer, B., 2014. Beyondcorp: A new approach to enterprise security. ; login:: the magazine of USENIX & SAGE, 39(6), pp.6-11.
2. Rose, Scott, Oliver Borchert, Stu Mitchell, and Sean Connelly. "Zero Trust Architecture NIST Special Publication 800-207 (Final). August 2020." f https://doi. org/10.6028/NIST. SP: 800-207.
3. Kindervag, J. and Balaouras, S., 2010. No more chewy centers: Introducing the zero trust model of information security. Forrester Research, 3(1), pp.1-16.
4. Rais, Razi, Christina Morillo, Evan Gilman, and Doug Barth. Zero Trust Networks: Building Secure Systems in Untrusted Networks. " O'Reilly Media, Inc.", 2024.
5. Gupta, Pankaj. "Mutual TLS: Securing Microservices in Service Mesh." TheNewStack (2021).

Thank you