

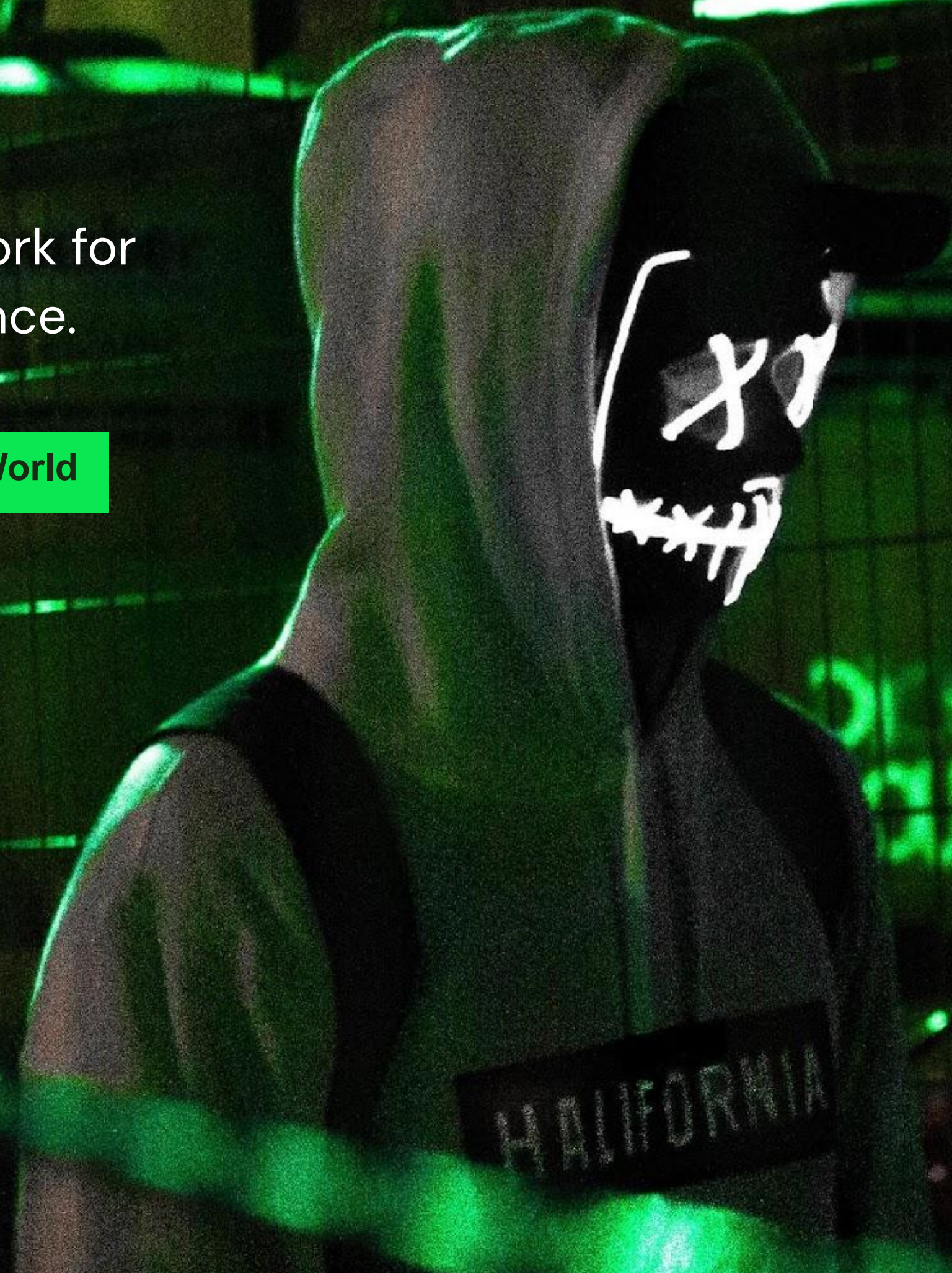


Zero-Trust Privacy-Preserving Framework for Decentralized Cyber Threat Intelligence.

Protecting Data, People, and Progress in a Connected World

Presented By: Md Eyamin Molla

Research Domain: Cybersecurity and AI





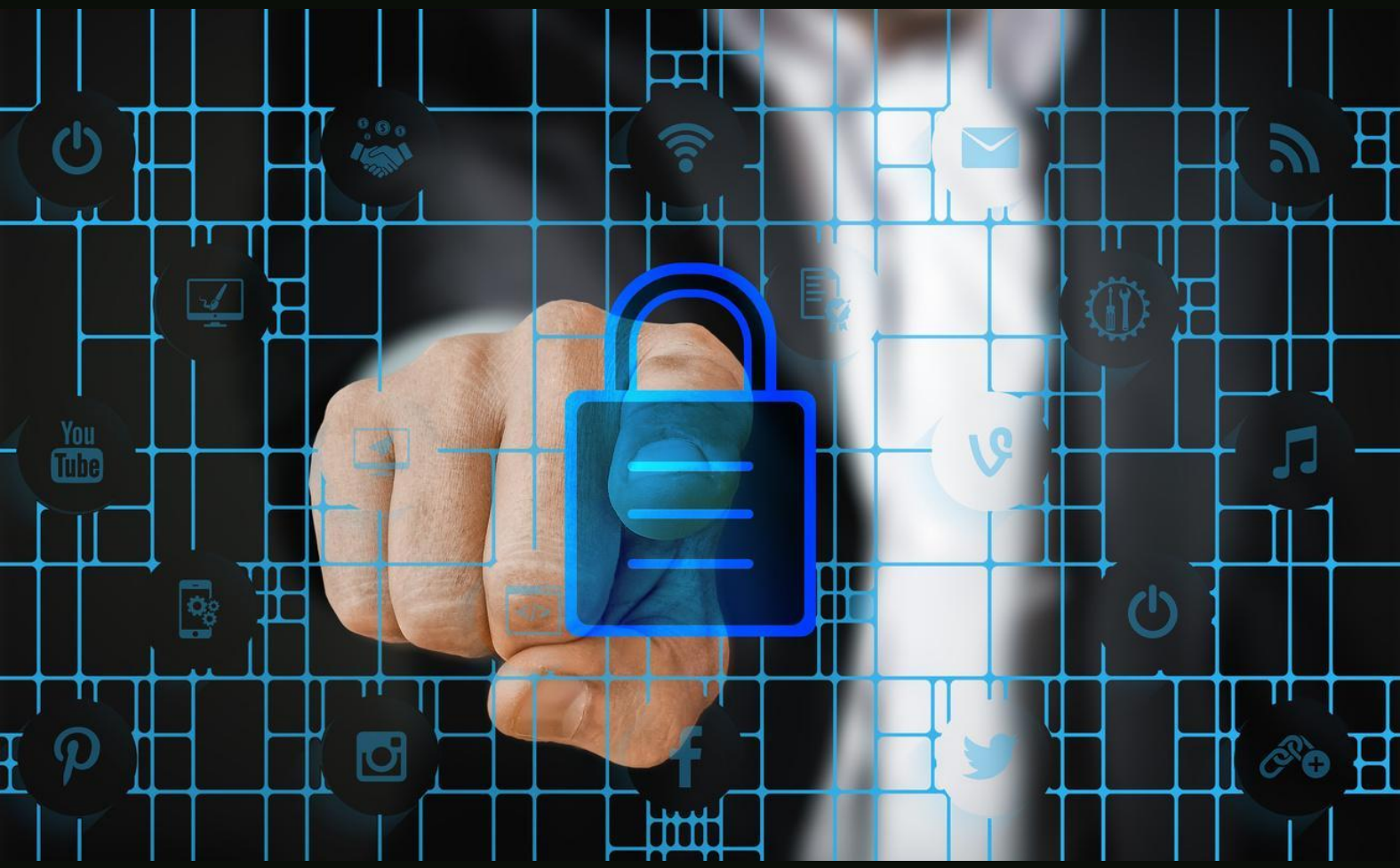
BACKGROUND



- **Current Development:** The rise of AI-driven threats (Ransomware, Botnets) requires massive cross-organizational data sharing.
- **Literature Support:** Recent studies show that centralized data lakes are "honeypots" for hackers, leading to catastrophic data breaches.
- **The Conflict:** Organizations cannot share raw logs due to strict privacy regulations like GDPR.

PROBLEM STATEMENT

- **Identified Gap:** Existing IDS models rely on centralized data, creating a single point of failure.
- **Privacy Leakage:** Standard model sharing is vulnerable to Gradient Inversion Attacks, allowing hackers to reconstruct raw private logs.
- **Literature Support:** Research by Zhu et al. (2024) highlights that model updates (gradients) can leak up to 90% of original training data.

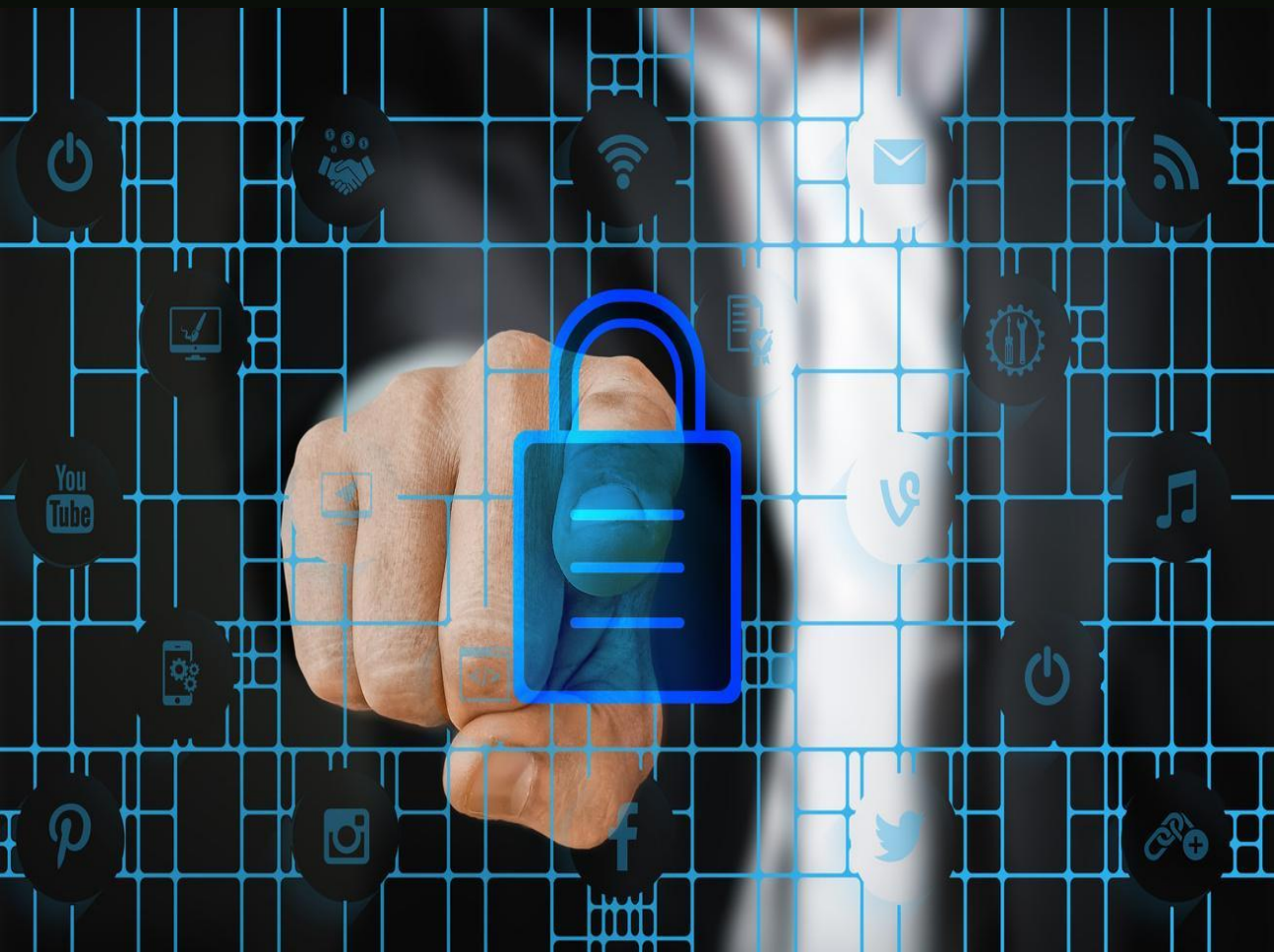


RESEARCH AIM AND OBJECTIVES

Aim: To develop a Zero-Trust intelligence framework that enables collaborative threat detection while maintaining absolute data privacy.

Objectives :

- Design a decentralized Federated Learning protocol for cyber analytics.
- Implement Adaptive Differential Privacy to mathematically mask individual network signatures.
- Evaluate the system's resilience against Model Poisoning attacks using Byzantine-robust aggregation.



Brief Literature Review & Summary

- **Federated Learning (FL):** Decentralized AI training without moving raw data (McMahan et al.).
- **Differential Privacy (DP):** Adding mathematical noise to hide individual records (Dwork et al.).
- Current research on decentralised FL, Federated Learning security, differential privacy, and Zero Trust Architecture, emphasising that earlier studies tackled privacy and access control independently but not in an integrated way (Al Amin Hossain et al.).
- Federated Learning, Zero Trust, and AI security, emphasising adversarial hazards and data leaking. It identifies a weakness in the integrated framework's large-scale adversarial validation in the actual world. (Ramin Ranjbarzadeh et al.).
- Zero Trust and federated learning improve cloud security and privacy, but are mostly studied separately. Integrated zero-trust with privacy-preserving AI for real-time cloud security is still

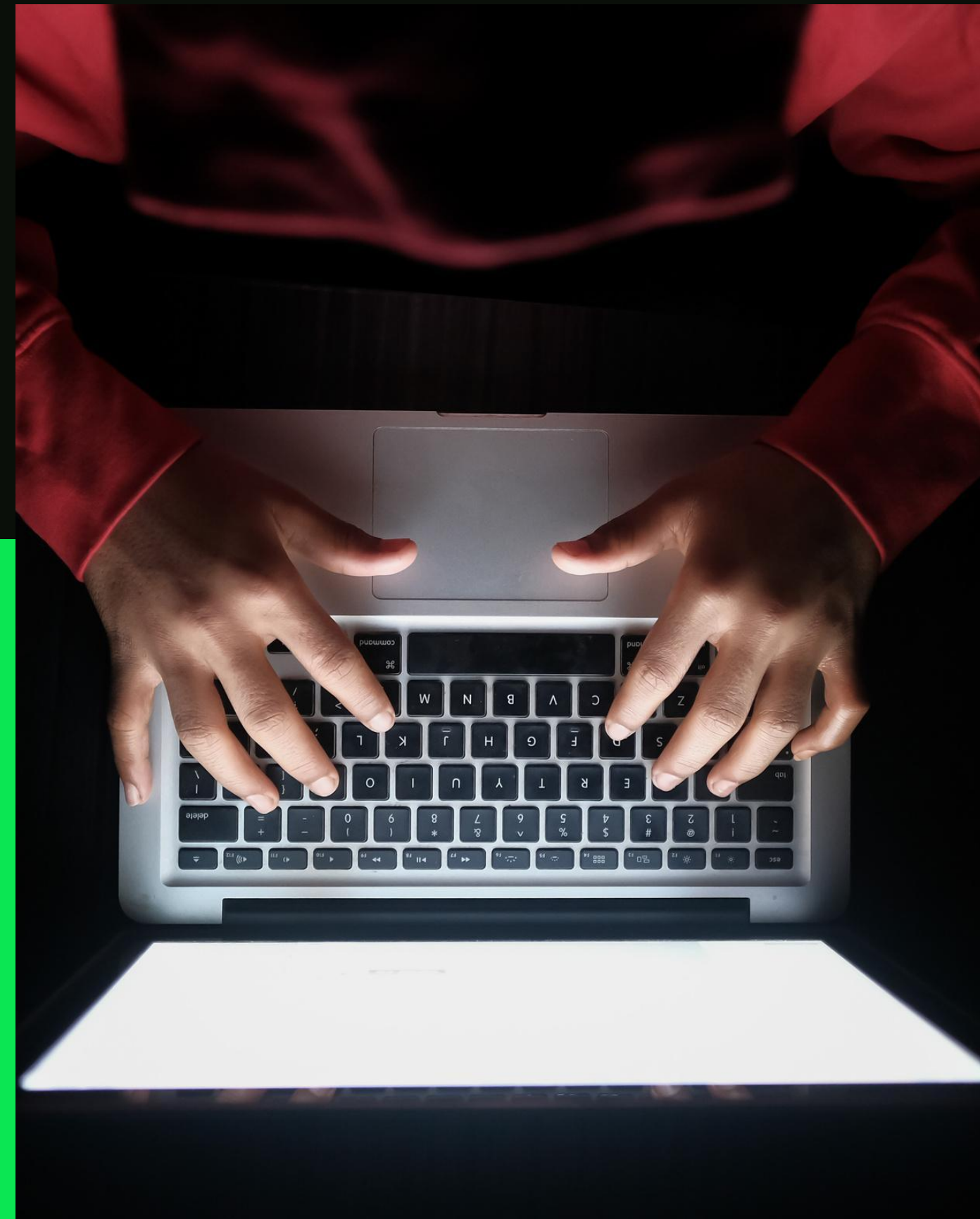
Research Methodology

- **Method:** Hybrid Federated Learning + Adaptive Differential Privacy.
- **Justification:** FL ensures Data Residency, while Adaptive DP provides a tunable Privacy Budget (ϵ), allowing the system to maintain detection accuracy for Zero-day threats.
- **Red Teaming Approach:** Using adversarial testing to validate the privacy layer.



Details of Data Collection

- **Primary Dataset:** CIC-IDS2024 (The latest benchmark for modern cyber-attacks).
- **Data Sources:** Simulated local nodes representing isolated enterprise networks.
- **Traffic Types:** DDoS, Brute Force, API Injection, and Infiltration logs.



Research Methodology

Model Utility: Measuring Accuracy, Precision, and Recall under various privacy levels.

Privacy Strength: Using Membership Inference Attacks (MIA) to test if the model "leaks" user info.

Resilience: Testing the model against 20% compromised (poisoned) nodes



Project Planning

Month 1-2: Literature gap identification and environment setup.

Month 3: Model architecture and decentralized training simulation.

Month 4: Privacy layer (DP) integration and adversarial testing.

Month 5: Results analysis, documentation, and final thesis submission



Resource Management



Software: Python 3.10, PyTorch, Meta's Opacus (DP), PySyft (FL).

Hardware: High-compute GPU environment (Google Colab/Local workstation).

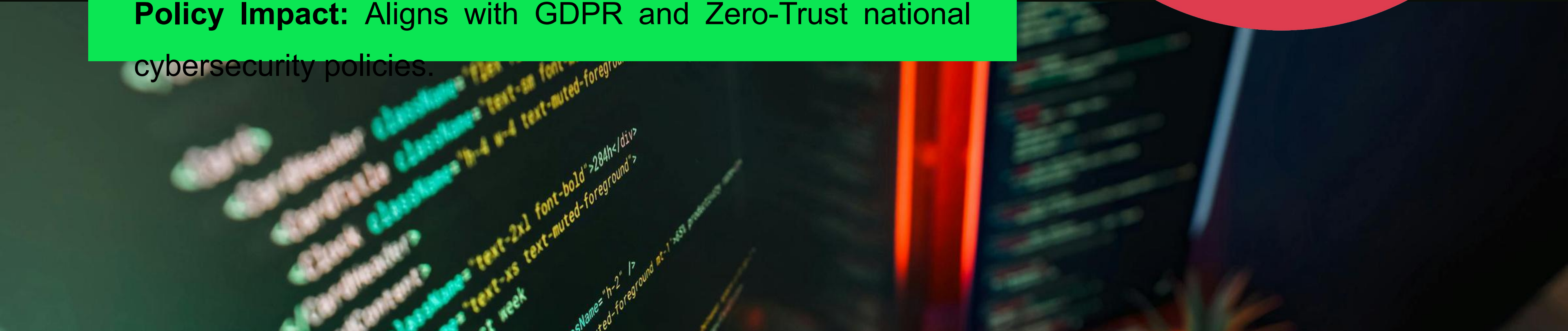
Human Capital: Guidance from the supervisor and peer review for security auditing.

PROJECT IMPACT

Societal Impact: Enhances trust in AI systems by guaranteeing the right to privacy.

Industrial Impact: Allows banks and healthcare providers to collaborate on security without risking sensitive client data.

Policy Impact: Aligns with GDPR and Zero-Trust national cybersecurity policies.



Project Limitations

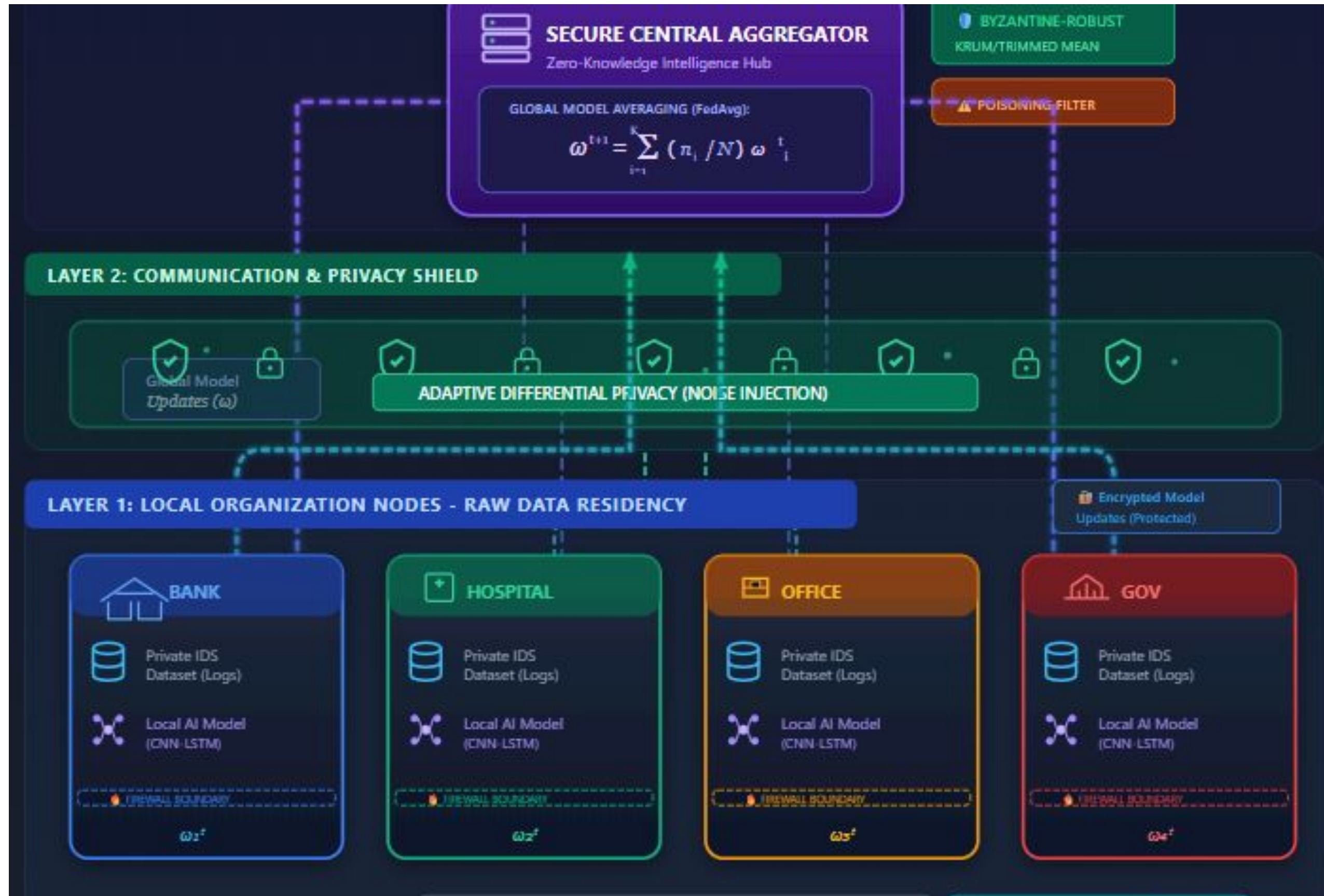
Computational Overhead: Encryption and noise injection can increase processing time.

Utility-Privacy Trade-off: High privacy levels may slightly reduce the detection rate of very subtle anomalies.

Scalability: Managing model aggregation in networks with thousands of nodes requires further optimization.



Federated Learning (FL) Architecture



RELEVANT REFERENCES

- Zhu, T., et al. (2024). Privacy Leakage in Federated Learning. Nature Communications.
- Wang, J., & Miller, S. (2025). Adaptive DP in Cyber Analytics. ACM CCS.
- Chen, L., & Gupta, R. (2026). Byzantine-Robust Security Analytics. IEEE.
- Al Amin Hossain et al.(2025). Architecture for Federated Machine Learning
- Li, X., et al. (2024). Mitigating Membership Inference





CONCLUSION

For decentralised threat intelligence, this architecture integrates privacy-preserving techniques with zero-trust. It ensures secure collaboration while protecting sensitive data. **Defense is the future, but it must be built on a Zero-Trust privacy foundation.**

Thank You