SMART INDIA HACKATHON 2024

Problem Statemet ID: SIH1529

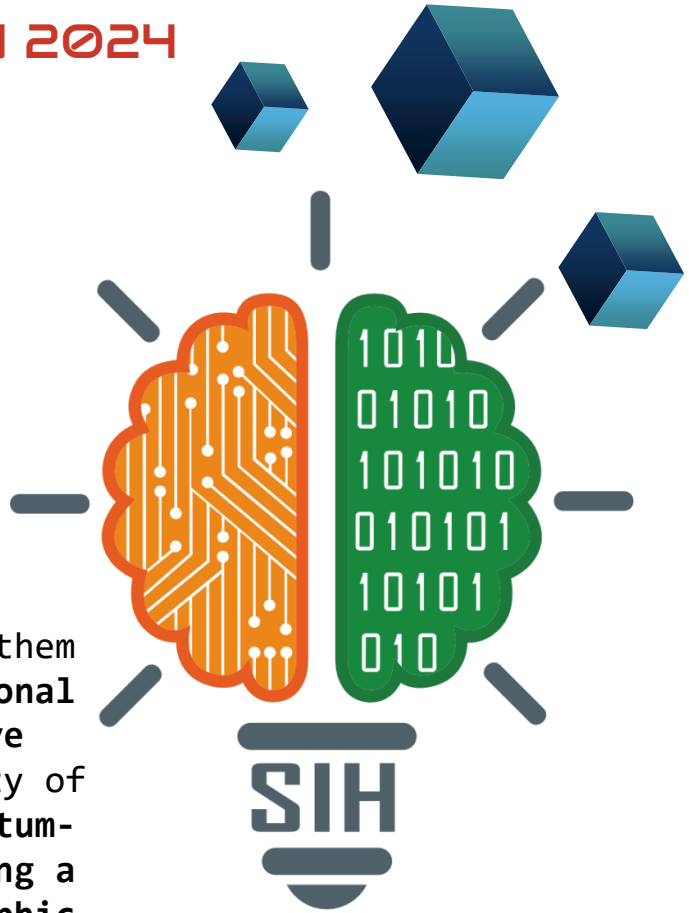
Problem Statement Title: Student Innovation

Theme: Blockchain & Cybersecurity

PS Category: Hardware

Team ID: SVCESIH24HW053

Team Name: IoTEnigma



Problem Statement/Idea

The **increasing adoption of IoT devices** has made them **vulnerable to quantum computing threats. Traditional cryptographic algorithms** may become **ineffective against quantum attacks,** compromising the security of sensitive data and critical infrastructure. **Quantum-Shield** aims to address this challenge by **providing a robust and efficient quantum-resistant cryptographic solution for IoT devices.**

SMART INDIA HACKATHON 2024

Solution Approach

Hybrid Approach:

- Combines Lattice-Based Encryption (LBE) and Code-Based Error Correction (CBEC).

Quantum Resistance:

- Offers enhanced protection against quantum attacks.

Lightweight Design:

- Suitable for resource-constrained IoT devices.

Improved Security:

- Provides stronger cryptographic guarantees compared to traditional methods.

Efficiency:

- Balances security with performance requirements.

Real-World Applicability:

- Can be integrated into existing IoT systems with minimal modifications.

SMART INDIA HACKATHON 2024

Technical Approach

Hybrid Cryptographic Framework

Lattice-Based Encryption (LBE): Quantum-resistant encryption using complex lattice problems for secure key generation and encryption.

Code-Based Error Correction (CBEC): Enhances data integrity with error-correcting codes, ensuring reliable communication.

Evaluation Metrics

Performance: Measures encryption/decryption time, memory, and power usage
Security: Assesses quantum resistance and error correction effectiveness

IoT Device Implementation

Public/Private Key Management: Each IoT device (NodeMCU) uses public/private keys for secure communication; encryption by NodeMCU-1 and decryption by NodeMCU-2.

Resource Optimization: Lightweight algorithms designed to fit IoT device constraints.

Workflow And Technical Stack

Workflow Diagram

SMART INDIA HACKATHON 2024

Sample Message

<Web Request From Server>

NodeMCU With Quantum Resistive Algo Trained

Response

Server

Raises Requests

Web Page GUI

Gets insights & Performs Tasks

End Users

Encrypted ⟷ Decrypted Msg Transfer

Encryption

Algorithm

Decryption

Decrypted Message

Output Display

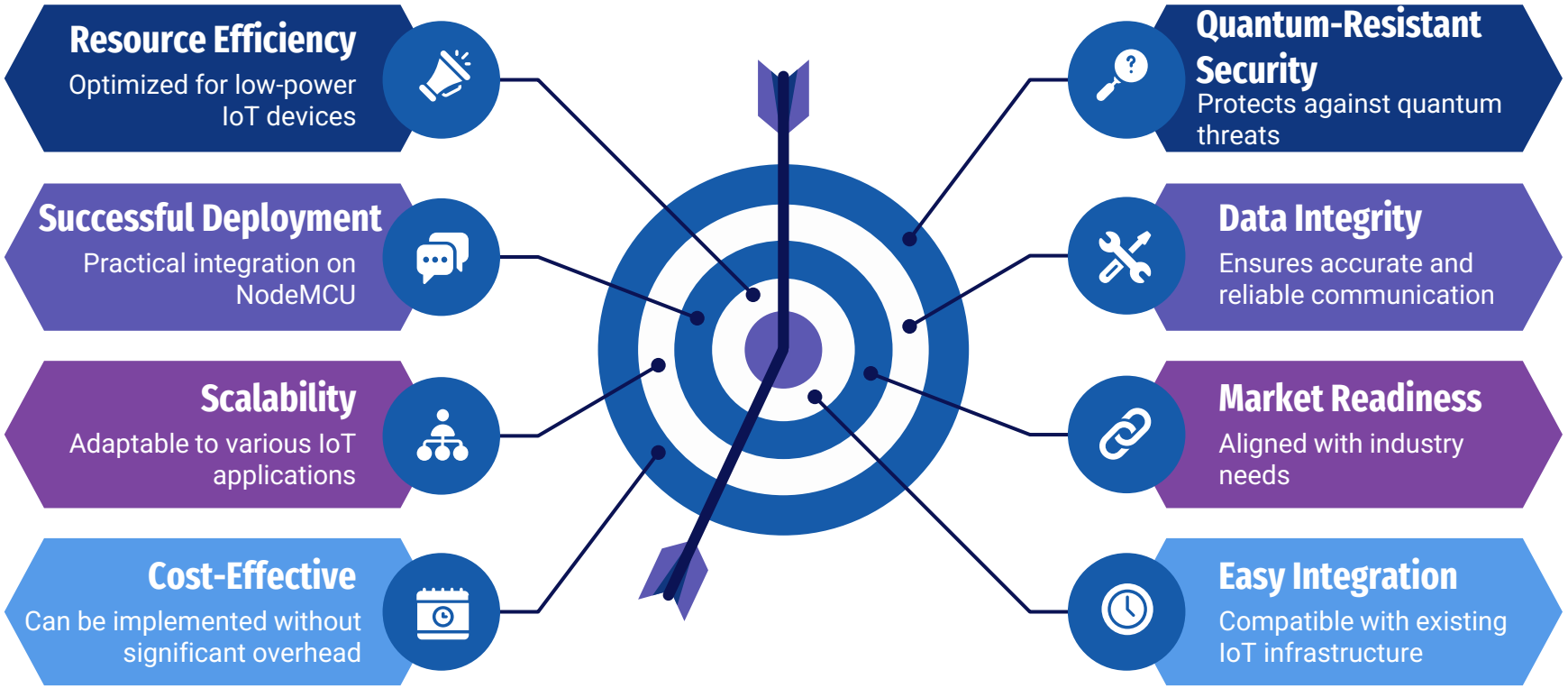
Tech Stacks

ESP NOW

POSTMAN

SMART INDIA HACKATHON 2024

Feasibility and Viability



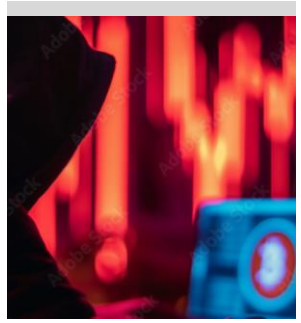
SMART INDIA HACKATHON 2024

IMPACT AND BENEFITS

Enhanced Cybersecurity: Protects critical infrastructure and personal data from quantum-based attacks

Improved Privacy: Safeguards sensitive information, ensuring individuals' privacy rights.

Economic Benefits: Reduces costs associated with data breaches and disruptions, benefiting businesses and consumers.



Technological Advancement: Drives innovation in quantum-resistant cryptography and related fields.

Global Security: Contributes to overall global security by mitigating potential threats from quantum computing.

Trust and Confidence: Builds trust in digital technologies and promotes confidence in online interactions.

Enhanced Security: Protects against quantum threats and improves data privacy.

Efficient Resource Use: Balances security with performance.

Reduced Risk: Minimizes financial losses and reputational damage.

Regulatory Compliance: Reduces legal risks.

Scalability: Easily adaptable to various IoT applications

Quantum-Resistant Encryption: Protects against future quantum attacks.