QUANTAM SHIELD QRNG+ E91 QKD + AES-256-GCM

A.Md.Saffan,K Mohan, N.Pallavi, P.Bhavya, Y.Prasanth, P.Vinesh

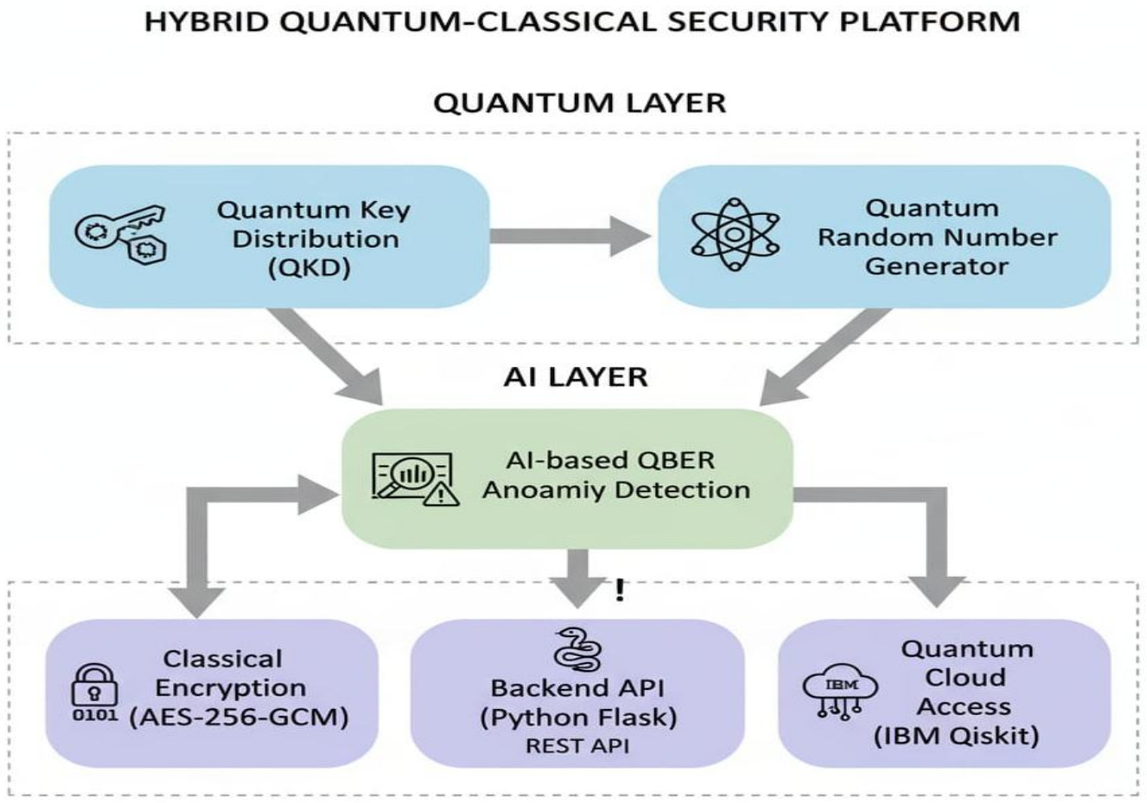
S K U College of Engineering & Technology

Contact mail: hackathonwarriors150@gmail.com

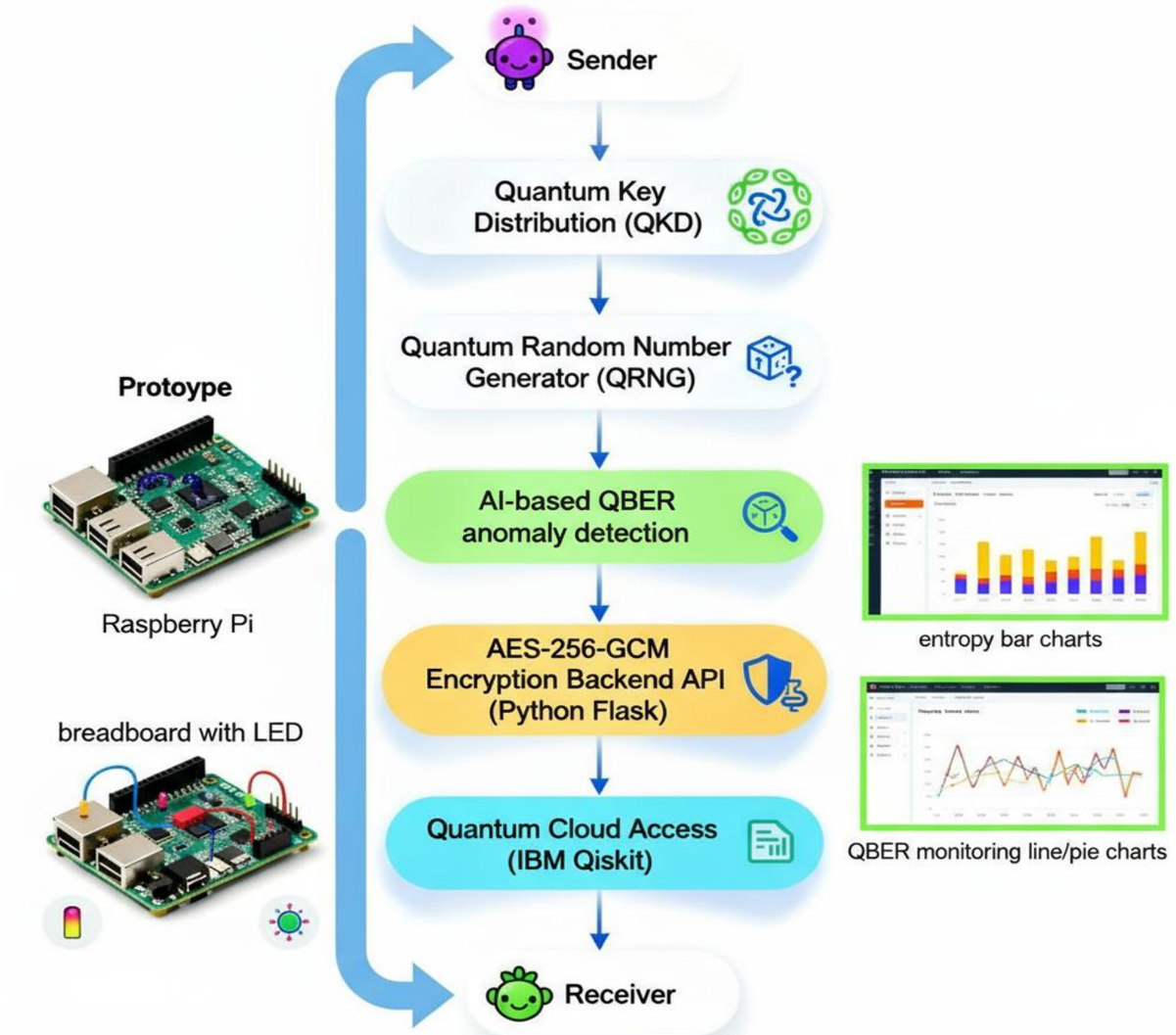
Introduction

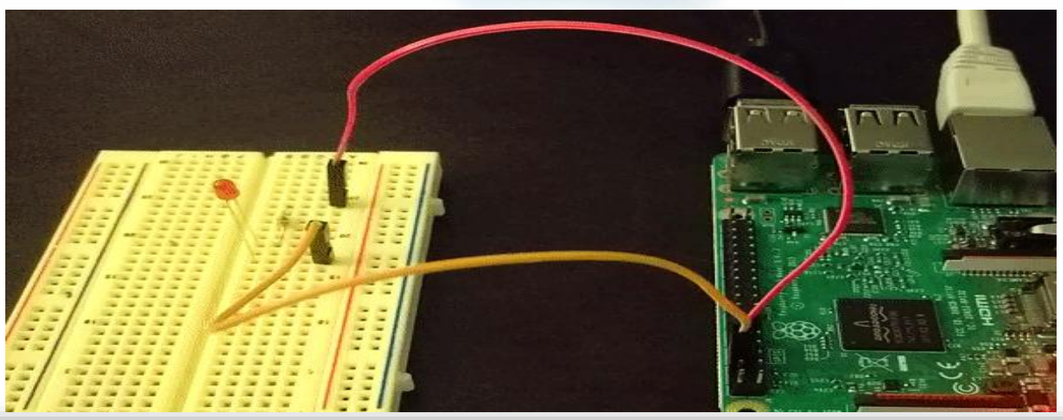
- Classical cryptography is vulnerable to quantum computing threats.
- The project builds a platform using QKD and QRNG for security.
- QRNG ensures truly random keys for strong encryption.
- It focuses on quantum cryptography, communication, and computing..

DESIGN ARCHITECTURE



Implementation

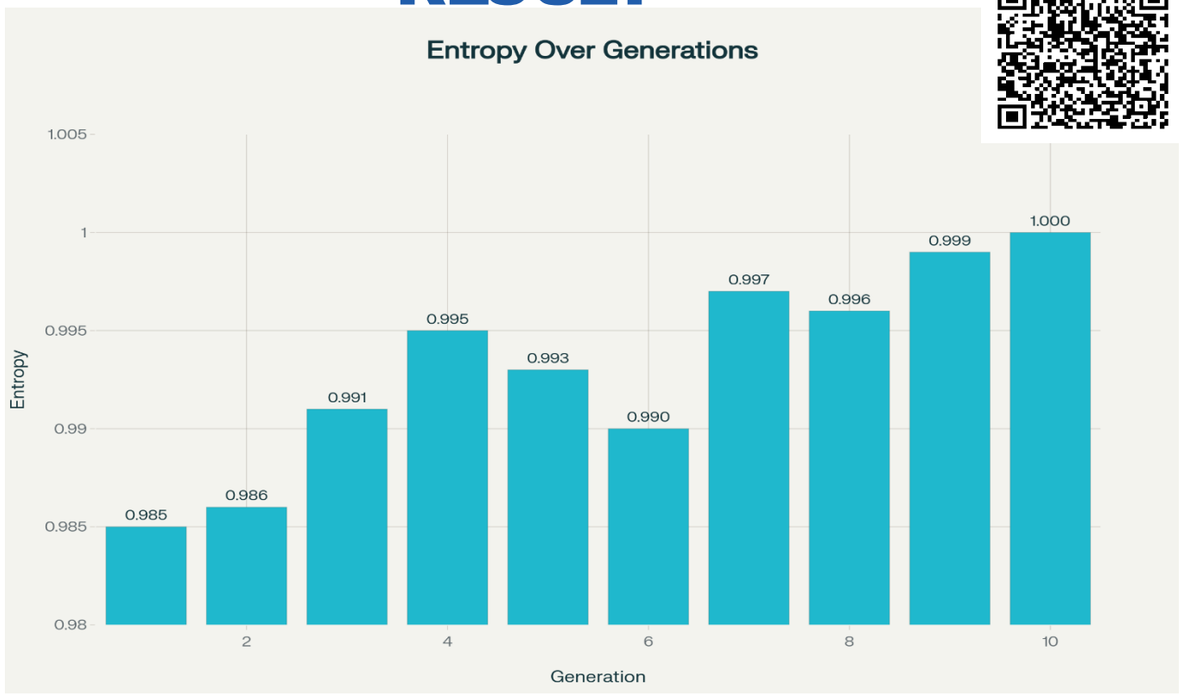




Problem statement:

1. Classical cryptography risks quantum attacks.
2. Users: defense and security agencies.
3. Data breaches threaten national security.
4. Project ensures quantum-proof data safety.

RESULT



NOVELTY

1. Unified quantum-classical security workflow
2. Real-time analytics for entropy and QBER
3. Provisional patent filed: **E-11036192025-CHE.**

OUTCOMES

1. Quantum entropy >0.98 ensures strong keys.
2. Low QBER confirms secure transmission.
3. Quantum-classical encryption validate d for security.

IMPACT

1. Enables quantum security for defense, finance, and telecom
2. Key users: agencies, banks, cloud, infrastructure
3. Secures data and digital transactions from quantum threats Modular APIs integrate with existing systems easily

Future Work & Conclusion

- Upgrade to fiber and satellite QKD for wider deployment.
- Integrate post-quantum cryptography standards.
- Expand system compatibility across industries.
- Aim for scalable, compliant quantum-safe infrastructure.

REFERENCES &ACKNOWLEDGEMENT

- Patent filing: Provisional Patent E-11036192025-CHE (2025)
- Key references: DRDO,IIT Delhi, IDEX.,IBM, Market and research reports (2024–2025) on quantum cryptography trends.

- Heartfelt thanks to mentors**: Dr.C. Chandra Mouli (CEO, AIC-SKU)** , **Prof. D N Kuldeep Shamgar (SPOC AQVH)**
- Grateful to AQVH2025 organizers, sponsors, and supportive team members**.**