UE22CS320A - Capstone Project Approval

Project Title:	Quantum Resilient Cybersecurity for Avionics Networks: A Cloud Native, API Driven Solution Integrating Big data and Blockchain.	
Project ID:	89	
Project Guide:	Animesh Giri	
Project Team:	Akhmal Mohammed	PES2UG22CS047
	Rohit Maddaly	PES2UG22CS459
	Saahil Sudhir Pakhare	PES2UG22CS475
	Shreya Hegde	PES2UG22CS532

Outline

- Problem Statement
- Scope and Feasibility study
- Applications/Use cases
- Expected Deliverables
- Capstone (Phase-I Phase-II, Phase-III) Project Timeline
- Any other information

Problem Statement

- The avionics industry, a critical component of global transportation, increasingly relies on complex digital networks and communication protocols to manage aircraft operations, navigation, and communications.[1]

- These systems often depend on legacy and unencrypted protocols such as ACARS and ADS-B, making them vulnerable to cyber threats.

- The rise of quantum computing poses an even greater risk by rendering current cryptographic measures obsolete, thereby exposing avionics networks to potential disruptions, data breaches, and malicious attacks.[2]

Problem Statement

- With the avionics industry being one with the highest cost of failure (think 100s of lives of passengers and crew), we can not simply wait around for a large scale attack to occur.

- This project aims to develop a quantum-resilient cybersecurity solution for avionics networks by leveraging a cloud-native, API-driven architecture.

- Big data analytics will be used to provide actionable insights into potential threats.

Scope

Case Study:

- Ruben Santamarta, a cybersecurity researcher, conducted a detailed investigation into the vulnerabilities of aircraft communication systems, particularly focusing on Aircraft Communications Addressing and Reporting System (ACARS)[3].

- His work revealed that many avionics communication systems, including in-flight Wi-Fi, entertainment systems, and satellite communication (SATCOM) links, are susceptible to cyber attacks.

- Santamarta discovered that in-flight Wi-Fi and entertainment systems could be used as entry points for attackers to access sensitive avionics systems. By exploiting these vulnerabilities, malicious actors could potentially interfere with flight operations or passenger data.

- ACARS could be intercepted due to the lack of encryption, revealing sensitive operational data such as flight plans, weather updates, and even crew communications.

- He discovered the vulnerabilities by "reverse engineering"[4] - or decoding - highly specialized software known as firmware, used to operate communications equipment made by Cobham Plc, Harris Corp, EchoStar Corp's Hughes Network Systems, Iridium Communications Inc and Japan Radio Co Ltd.

Feasibility

- **Technical Feasibility:** Development and standardization of Post Quantum Cryptographic algorithms and blockchain platforms makes the implementation feasible. Major cloud service providers offer secure APIs for encryption key management, real-time data exchange, and scalable communication infrastructure.

- **Legal and Regulatory Feasibility:** The project will align with the evolving cybersecurity guidelines from regulatory bodies, ensuring adherence to aviation safety and data privacy standards.

- **Operational Feasibility:** Deployment of the new technology onto legacy subsystems, while ensuring the appropriate changes in protocols, hardware and software systems are made. Extensive compatibility testing is conducted to eliminate points of failure in critical subsystems.

- **Business Feasibility:** The advent of quantum computers have spawned novel cybersecurity threats, as these systems can circumvent traditional cryptographic techniques,compelling developments in quantum resilient cryptographic techniques. The application of wireless transmission media eliminates the cost and space overhead from wired avionics communication systems.

Shortcomings

- **Lack of Encryption:** Existing legacy software uses outdated protocols leaving systems vulnerable to eavesdropping, tampering and spoofing.

- **Vulnerable to Quantum attacks:** The current cryptography can be broken by quantum computers making the systems vulnerable to security risks.

- **Limited cloud integration:** Slow integration of cloud-native technologies hampers real-time updates and scalable security solutions.

- Performance overhead and the increased cost of applying quantum-resilient cryptographic techniques.

- **Securing wireless transmissions:** Since the effectiveness of wireless transmission media is enhanced by the openness of the network, securing the transmission from being tapped or intercepted poses a major challenge

- Not securing the Cloud Services, Blockchain nodes and the API’s connecting avionics systems might result in them being the weak points of the cybersecurity network

Challenges

- No quantum resistance: Current cryptography can be broken by future quantum computers, posing a major security risk.

- Limited cloud integration: Slow integration of cloud-native technologies hampers real-time updates and scalable security solutions.

- Performance overhead and the increased cost of applying quantum-resilient cryptographic techniques.

- Securing wireless transmissions: Since the effectiveness of wireless transmission media is enhanced by the openness of the network, securing the transmission from being tapped or intercepted poses a major challenge.

- Many avionics systems are built on old hardware and software platforms, which may not be compatible with advanced cloud-native, quantum-resilient cryptography, and blockchain solutions.

- The aviation industry is heavily regulated. Integrating new cybersecurity solutions, especially involving blockchain and cloud technologies, would require rigorous testing, certification, and compliance with global aviation standards.

Challenges

- Many avionics systems are built on older hardware and software platforms, which may not be compatible with advanced cloud-native, quantum-resilient cryptography, and blockchain solutions.

- The aviation industry is heavily regulated. Integrating new cybersecurity solutions, especially involving blockchain and cloud technologies, would require rigorous testing, certification, and compliance with global aviation standards.

- Not securing the Cloud Services, Blockchain nodes and the API’s connecting avionics systems might result in them being the weak points of the cybersecurity network

Applications

- Secure Air-to-Ground Communication:

  - **Post-Quantum Cryptography (PQC)** algorithms ensure that future quantum computers cannot break the encryption protecting communication between aircraft and ground control.

  - **Blockchain's** immutable ledger can track all communication exchanges between the aircraft and ground stations. This creates a verifiable history of messages, ensuring that if any tampering occurs, it can be detected quickly and reliably.

  - The **Cloud-Native API driven** approach ensures scalable, real-time protection for air-to-ground communication. With **microservices** and **API-driven security protocols**, it allows for quick updates and patches without disrupting operations. **Real-time threat detection** and **resilience** are built in, ensuring continuous monitoring and fault tolerance.

Applications/Use cases

- Securing Inter-Avionic System Communication:
  - Quantum resilient techniques are used for ensuring security and integrity in intercommunication between aircrafts.
  - Big data analytics are used for real time troubleshooting in flight path management between multiple aircrafts and landing scheduling.
  - Cloud-based API provide a dynamically modifiable interface with rapid updates, which is crucial in emergency updates between multiple aircrafts.

Applications/Use cases

- Resilient Fleet Management:
    - PQC can be used to create secure system access policies.
    - Cloud native nature of the solution allows for improved scalability and cost efficiency
    - Blockchain technology is used to create a tamper-proof record of maintenance activities, operational logs, and other critical data.

Applications/Use cases

- Electronic Flight Bag (EFB):
  - An **Electronic Flight Bag (EFB)** is a portable electronic device used by pilots to access digital flight plans, navigation charts, weather data, and operational manuals, replacing traditional paper-based tools. Quantum-resilient techniques can be applied to secure communication between EFBs and aircraft systems, protecting sensitive data from future quantum-based cyber threats, ensuring long-term data integrity and privacy.

Expected Deliverables

- Capstone-I deliverables
- Capstone-II deliverables
- Capstone-III deliverables

Capstone (Phase-I & Phase-II) Project Timeline

Provide

- The timelines for execution of the project through Gantt chart.
- The plan in terms of efforts by individuals in the team.
- Mention the tasks involved in different stages.

Capstone (Phase-I & Phase-II) Project Timeline

Provide

- The timelines for execution of the project through Gantt chart.
- The plan in terms of efforts by individuals in the team.
- Mention the tasks involved in different stages.

References

- [1] Ukwandu, E.; Ben-Farah, M.A.; Hindy, H.; Bures, M.; Atkinson, R.; Tachtatzis, C.; Andonovic, I.; Bellekens, X. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information* **2022**, *13*, 146. https://doi.org/10.3390/info13030146

- [2] **Mashatan, A., Barker, E., Akter, M., Kumar, P., and Garhwal, A.** *Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure*. arXiv preprint.
- [3]https://www.darkreading.com/vulnerabilities-threats/researcher-successfully-hacked-in-flight-airplanes---from-the-ground

- [4]https://www.reuters.com/article/technology/hacker-says-to-show-passenger-jets-at-risk-of-cyber-attack-idUSKBN0G40WQ/

Thank You