DEVELOPMENT TEAM PROJECT – DESIGN DOCUMENT

Secure Systems Architecture October 2025

SUBMITTED BY

Aldana Alsada

Pragadheesh Marimuthu

Precious Olasunkanmi

ir

Ahmed Mohamed Ahmed Talib Alsalam

Contents

1. Introduction

For this project, we chose the case study of Bhattachariya on Blockchain in Cyber-Physical System (CPS) and Internet of Things (IoT). The main focus of the case study is on the data communication, specifically sustaining confidentiality, integrity and availability (CIA). The chosen network is based on System of Systems (SoS) which demonstrates autonomy, diversity, belonging, connectivity, and emergence (Boardman & Sauser,2006).

Every device within the internet of things operates independently but also collaborates with other controllers and hubs within the blockchain to establish and maintain distributed communication securely. The Attack-Defence tree (AD) tree which is developed as part of this report highlights the key vulnerabilities at different levels including client level, hub level and over all system level and it also highlights appropriate mitigations for these vulnerabilities.

2. Identified Vulnerabilities

There are three levels of vulnerabilities identified:

2.1. Client-Level:

Nodes within the IoT face outdated firmware, limited encryption, and weak authentication which makes them vulnerable to MIM (man in the middle) attack or replay attacks (Massad & Alsaify,2020).

2.2. Controller/Hub Level:

At controller & hub level, poor key protection, consensus manipulation, and smart-contract errors are causes of the major vulnerabilities which could affect the ledger for blockain.

2.3. System Level:

At system level, vulnerabilities include DDoS attacks (approximately 51% attacks) (Yu,202). These two can affect CIA and the trust model which can unperin the SoS.

3. Attack-Defence Tree (AD-Tree)

The attack-defence tree below outlines how blockchain-enabled IoT communication can be targeted and protected.

At the root is the threat of system compromise. This branches into three main areas:

3.1. Client Exploitation:

Typical attacks involve stolen credentials, outdated devices, and unauthorised access. Defences include multi-factor authentication, secure firmware updates, and lightweight encryption.

3.2. Hub Manipulation:

Risks stem from consensus hijacking, key theft, and code injection. These are countered by robust key management, auditing smart contracts, and enforcing zero-trust validation.

3.3. System Disruption:

Attacks such as DDoS or majority control are mitigated through redundancy, rate-limiting, and hybrid consensus approaches.

This visual summary clarifies both vulnerability points and the layered defences adopted throughout the system, enhancing trust and security in blockchain-integrated IoT operations.

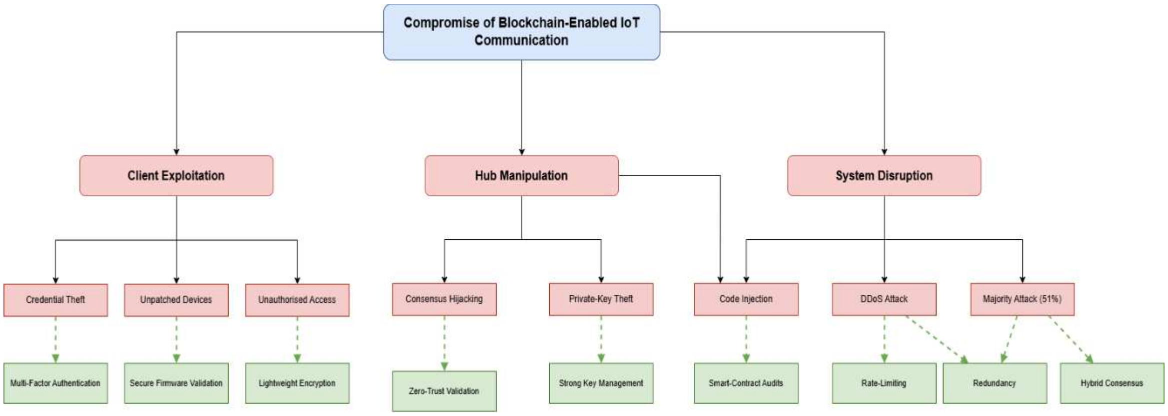

Figure 1: *Attack-Defence Tree illustrating vulnerabilities and mitigations in a blockchain-enabled CPS/IoT System of Systems (Team A)*

4. Quantitative Domain Evaluation

A likelihood–impact domain is employed to quantify risk severity. Attack nodes are allocated a score between 0 and 1 for both likelihood and impact, the product of these values yields an overall risk value. This approach supports the prioritisation of security controls objectively (Planas and Cabot, 2020).

Attack Vector	Likelihood (0-1)	Impact (0-1)	Risk Value
Client Credential Theft	0.6	0.8	**0.48**
Hub Consensus Hijack	0.3	0.9	**0.27**
System DDoS Attack	0.4	0.7	**0.28**

Mitigation effort prioritisation is indicated in nodes with higher scores, suggesting a greater combined probability & consequence

5. Mitigation Strategies

To reinforce resilience across the SoS:

- Implement blockchain-based device identity management for verifiable onboarding

- Apply adaptive encryption optimised for low-power IoT devices
- Introduce automated firmware patching & validation
- Utilise Sybil-resistant consensus algorithms, including Proof-of-Authority
- Introduce network segmentation and redundancy to contain faults

Using these countermeasures within CPS/IoT setups, confidentiality, integrity and availability of information are upheld (Bhattacharjya, 2022).

6. Conclusion

This work showcases how blockchain integration in CPS and IoT could bring significant improvement in security, given that system vulnerabilities are properly modelled and approached. Utilization of AD-Trees has allowed for a multi-layer ability to visualize potential risks, enabling quantitative assessments to support data-driven and prioritized security decisions (Planas & Cabot, 2020). Through investigation of client-to-hub, hub-to-network interactions, and vice-versa, the design team elaborated on scalable and practical countermeasures against attacks that keep the core CIA triad of Confidentiality, Integrity, and Availability within a secure Systems of Systems (SoS) framework. This structured approach has shown the importance of integrating knowledge about distributed systems with model-based engineering to proactively cope with evolving cyber threats within complex, interconnected systems (Yu, 2020).

References

1. Bhattacharjya, A. (2022) ‘A holistic study on the use of blockchain technology in CPS and IoT architectures maintaining the CIA triad in data communication’, International Journal of Applied Mathematics and Computer Science, 32(3), pp. 403–413. (Accessed: 7 November 2025).
2. Boardman, J. and Sauser, B. (2006) ‘Systems of Systems – The Meaning of Of’, IEEE/SMC International Conference on System of Systems Engineering, pp. 118–123. (Accessed: 7 November 2025).
3. Massad, M.A. and Alsaify, B.A. (2020) ‘MQTTSec based on context-aware cryptographic selection algorithm (CASA) for resource-constrained IoT devices’, 11th International Conference on Information and Communication Systems (ICICS), pp. 234–239. (Accessed: 7 November 2025).
4. Planas, E. and Cabot, J. (2020) ‘How are UML class diagrams built in practice? A usability study of two UML tools: MagicDraw and Papyrus’, Computer Standards & Interfaces, 70, pp. 103–113. (Accessed: 7 November 2025).
5. Yu, D. (2020) ‘Why Distributed Systems Are Hard’. (Accessed: 7 November 2025).

Index of comments

3.1 (ADTree) not (AD) tree