

Microprocessor-based intelligent cyber defense and high-speed LEO data encryption

Alzhan Tilenbayev [‡]

Department of Information Security

L. N. Gumilyov Eurasian National University

Astana 010000

Kazakhstan

L. La Spada [†]

N. Zeeshan [§]

School of Computing, Engineering and Built Environment

Edinburgh Napier University

10 Colinton Road

Edinburgh EH10 5DT

United Kingdom

M. Bakyt ^{*}

Department of Information Security

L. N. Gumilyov Eurasian National University

Astana 010000

Kazakhstan

Sabyrzhan Atanov [@]

Department of Computer and Software Engineering

L. N. Gumilyov Eurasian National University

Astana 010000

Kazakhstan

[‡] ORCID-ID: 0009-0009-9393-9861

[†] ORCID-ID: 0000-0003-4923-1320

[§] ORCID-ID: 0009-0009-2544-9991

^{*} ORCID-ID: 0000-0002-1246-9696

[@] ORCID-ID: 0000-0003-2115-7130

[‡] E-mail: mr.alzhan01@mail.ru

[†] E-mail: l.laspada@napier.ac.uk

[§] E-mail: nida.zeeshan@napier.ac.uk

^{*} E-mail: bakyt.makhabbat@gmail.com (Corresponding Author)

[@] E-mail: atanov5@mail.ru

Huseyin Canbolat [#]

*Department of Electrical and Electronics Engineering
Ankara Yildirim Beyazit University
Ankara 6000
Turkey*

Shattyk Zh. Kanbayeva ^{\$}

*Department of Information Technology
State Technical Service Company
Astana 010000
Kazakhstan*

B. Prmantayeva ^α

*Department of Space Engineering and Technology
L. N. Gumilyov Eurasian National University
Astana 010000
Kazakhstan*

Sh. Kadirkulov ^β

*Department of the Educational and Methodological Directorate
Sagadat Nurmagambetov Military Institute of the Ground Forces
Colonel
Astana 010000
Kazakhstan*

Kh. Moldamurat [^]

*Department of Space Engineering and Technologies
L. N. Gumilyov Eurasian National University
Astana 010000
Kazakhstan*

Abstract

This paper explores the synergistic integration of microprocessor-based intelligent cyber defence mechanisms with high-speed data encryption techniques for Low Earth

[#] ORCID-ID: 0000-0002-2577-0517

^{\$} ORCID-ID: 0009-0002-5140-3427

^α ORCID-ID: 0009-0009-1979-4895

^β ORCID-ID: 0009-0000-8215-5687

[^] ORCID-ID: 0000-0002-3691-6948

[#] E-mail: huseyin.canbolat@gmail.com

^{\$} E-mail: shattyk.98.05@mail.ru

^α E-mail: prmantayeva_ba@enu.kz

^β E-mail: shihgis070@gmail.com

[^] E-mail: moldamurat@yandex.kz

Orbit (LEO) spacecraft. As LEO constellations become critical infrastructure, ensuring their cybersecurity and the confidentiality of transmitted data is paramount. We investigate novel microprocessor architectures and intelligent algorithms for real-time threat detection, intrusion prevention, and autonomous response tailored to the resource-constrained environment of LEO satellites. Furthermore, we delve into advanced cryptographic methods optimized for high-throughput data streams and the unique challenges of space-based communication, including latency and intermittent connectivity. The paper proposes a layered security framework that leverages on-board intelligent processing for proactive cyber defence and robust encryption to safeguard sensitive data transmitted to and from LEO assets. The potential benefits of this integrated approach include enhanced resilience against cyber threats, improved data security, and increased operational efficiency for future LEO missions.

Subject Classification: 68P25.

Keywords: *Cyber defence, Intelligent systems, Microprocessor, Encryption, High-speed data, LEO satellites, Spacecraft security.*

1. Introduction

Low Earth Orbit (LEO) satellite constellations are rapidly expanding and play a crucial role in global communications, Earth observation, navigation and scientific missions. These systems generate and transmit large volumes of sensitive data, often under stringent real-time constraints and limited on-board resources. At the same time, their increasing connectivity and reliance on software-defined functions expose them to a growing spectrum of cyber threats, including eavesdropping, jamming, spoofing, command injection and denial-of-service attacks. Recent studies on cyber security for space and cyber-physical systems highlight that traditional terrestrial defense mechanisms and perimeter-based security models are not sufficient for space infrastructures [1]-[5]. Many existing solutions assume stable network connectivity, abundant computing resources and the possibility of frequent human intervention, assumptions that seldom hold for LEO spacecraft. Spaceborne platforms must operate autonomously for long periods, under intermittent contact with ground stations and in harsh environmental conditions, which significantly constrains the design and deployment of security mechanisms.

High-speed space communication links further exacerbate these challenges. Conventional encryption schemes, when implemented without careful optimization, can introduce latency and processing overhead that limit achievable throughput on resource-constrained on-board processors. To address this, several works investigate hybrid and optimized cryptographic schemes. For example, new key-management scenarios that combine Feistel structures with the Advanced Encryption Standard (AES)

are proposed to strengthen resistance against brute-force and side-channel attacks [6]-[10]. Other research explores hybrid block-cipher constructions and multi-round authentication methods, such as combinations of AES and Blowfish, to improve both performance and robustness in high-speed data environments [11]-[12]. Lightweight cryptographic primitives and intrusion detection mechanisms have also been considered for satellite and space communication networks, particularly in connection with emerging applications such as secure Internet-of-Things (IoT) and cyber-physical systems [13]-[16].

Despite these advances, there is still no comprehensive and integrated framework that jointly addresses intelligent cyber defense and high-speed data encryption at the microprocessor level for LEO spacecraft. Most existing approaches focus either on link-level encryption without explicit consideration of on-board intelligent defense, or on intrusion detection and response without deeply integrating high-throughput encryption into the embedded architecture. As a result, current solutions may leave blind spots to sophisticated, multi-stage attacks or become bottlenecks when confronted with the high data rates typical of modern LEO missions. This paper proposes a microprocessor-based intelligent cyber defense and high-speed encryption framework tailored to the constraints and requirements of LEO spacecraft. The primary goal is to design and evaluate an integrated, layered security architecture that combines on-board intelligent threat detection and response with efficient, high-throughput data protection [17]-[19]. To achieve the goal of securing Low Earth Orbit (LEO) satellites, this paper pursues the following objectives: (1) analyzing primary cyber threats and vulnerabilities specific to LEO satellites; (2) evaluating candidate space-qualified microprocessor architectures for supporting intelligent cyber defense and high-speed encryption within resource constraints; (3) developing lightweight intelligent cyber defense algorithms for on-board anomaly detection, intrusion prevention, and autonomous response; (4) assessing and adapting high-speed encryption techniques for LEO communications with emphasis on throughput and security; and finally, (5) proposing and evaluating an integrated, layered security framework that combines intelligent cyber defense and high-speed encryption at the microprocessor level, quantifying its effectiveness under representative LEO scenarios.

The proposed framework is particularly relevant for applications that require both high data rates and strong security guarantees, such as satellite-based broadband Internet, high-resolution Earth observation, secure command and control, and distributed satellite missions. By tightly coupling onboard intelligent cyber defense with high-speed encryption, the framework aims to provide proactive detection and mitigation of cyber threats while preserving the confidentiality and integrity of mission data

without introducing prohibitive overhead. The remainder of this paper is organized as follows. Section 2 describes the threat modelling activities, microprocessor evaluation and the design of intelligent cyber defense and high-speed encryption components. Section 3 presents the integrated security framework and discusses simulation results and performance evaluation. Section 4 concludes the paper and outlines directions for future research.

2. Methods

This study adopts a multi-faceted methodological approach that combines threat modelling and vulnerability analysis, comparative evaluation of space-qualified microprocessor architectures, development of on-board intelligent cyber defense algorithms, assessment of high-speed encryption techniques and design of an integrated security framework for LEO spacecraft. Simulation-based evaluation is used to quantify the performance, resource utilization and security effectiveness of the proposed architecture, and potential hardware–software co-design options are considered where relevant.

2.1 *Threat Modelling and Vulnerability Analysis*

We conduct a comprehensive analysis of potential cyber threats targeting LEO satellite systems. The threat-modeling process systematically generates a catalogue of plausible attack scenarios and associated vulnerabilities by performing three main activities: (i) a literature review of existing reports and incident databases to identify common attack vectors affecting space systems; (ii) attack-tree construction to systematically map potential attack paths, preconditions, and attacker capabilities against key LEO satellite components (microprocessors, links, sensors, etc.); and (iii) a vulnerability assessment focusing on common hardware and software flaws in space-qualified embedded systems, particularly examining firmware updates, protocols, memory protection, and subsystem interfaces.

2.2 *Microprocessor Architecture Evaluation*

We perform a comparative study of several microprocessor architectures suitable for deployment in LEO spacecraft (Table 1). The analysis focuses on representative space-grade or space-oriented designs, labelled Processor A, Processor B and Processor C, based respectively on a RISC-V core, an ARM Cortex-R core and a LEON3 core. For each candidate,

we examine key architectural and implementation features that influence the feasibility and efficiency of implementing intelligent cyber defence mechanisms and high-speed encryption on-board. Table 1 summarises the main characteristics considered in the comparison, including architecture type, clock frequency range, power consumption, radiation hardness, availability of cryptographic acceleration units and on-chip memory size. These parameters are interpreted with respect to their impact on security-related workloads, for example the effect of clock speed on the throughput of encryption algorithms or the influence of on-chip memory on the deployment of anomaly-detection models.

Table 1
Comparative Analysis of Potential Microprocessor Architectures for LEO
Spacecraft

Feature	Processor A (Example)	Processor B (Example)	Processor C (Example)	Evaluation
Architecture	RISC-V	ARM Cortex-R	LEON3	Suitability for real-time, power efficiency, and radiation tolerance
Clock Speed (MHz)	100-500	200-800	50-200	Impact on processing speed for security algorithms and data encryption
Power Consumption (W)	0.1-1.0	0.2-1.5	0.5-2.0	Crucial for LEO power budgets
Radiation Hardness (kRad)	>100	50-150	>150	Essential for long- duration space missions
Crypto Acceleration	Optional	Optional	Optional	Potential for hardware- accelerated encryption and decryption
On-Chip Memory (KB)	64-512	128-1024	32-256	Influence on the feasibility of on-board intelligent algorithm deployment

To guide the selection of a suitable microprocessor for further study, the architectures are evaluated according to the following criteria: Performance: processing capability (e.g. MIPS/DMIPS) and suitability for real-time execution of cyber defence and encryption algorithms alongside mission tasks. Power efficiency: power consumption in Watts, ensuring compatibility with the limited power budgets and thermal constraints of

LEO satellites. Radiation hardness: tolerance to total ionising dose and single-event effects typical of the space environment, which is essential for long-duration missions. Resource availability: amount of on-chip memory (SRAM, ROM/Flash) and presence of hardware acceleration units for cryptographic operations or signal processing. Cost and availability: cost-effectiveness and availability of space-qualified variants or radiation-tolerant versions of the architectures.

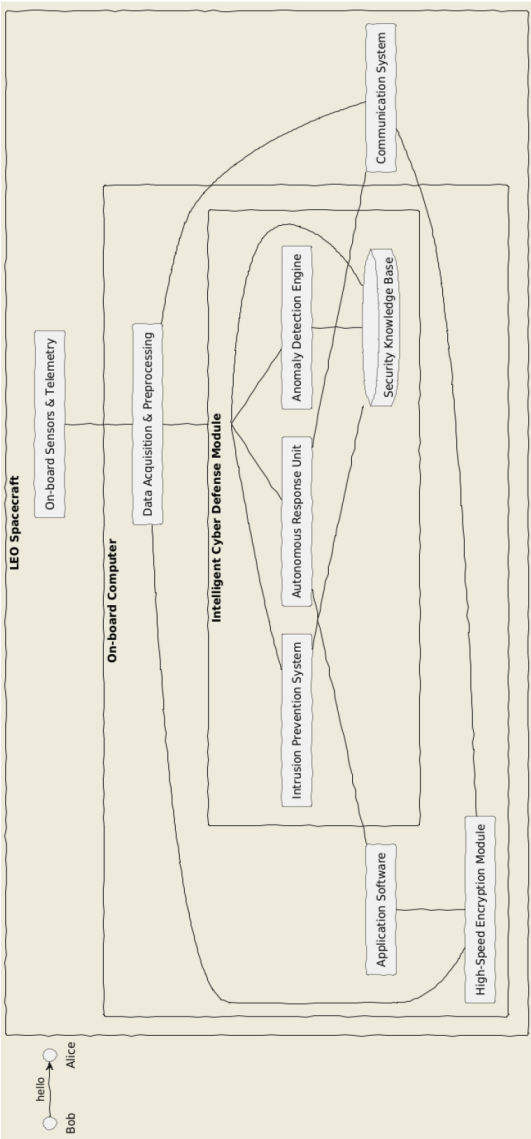


Figure 1
Conceptual Architecture of the Intelligent Cyber Defence System

2.3. *Development of Intelligent Cyber Defence Algorithms*

Based on the identified threats and processor capabilities, we design intelligent on-board cyber defence mechanisms organised according to the conceptual architecture shown in Figure 1.

The proposed intelligent cyber defence system comprises three tightly coupled functional blocks: *Anomaly detection*. Algorithms are developed to identify deviations from nominal system behaviour that may indicate malicious activity. The anomaly detectors operate on telemetry data, communication patterns and resource-usage metrics collected from the on-board computer and communication subsystems. Lightweight statistical and machine-learning models suitable for implementation on space-grade microprocessors are considered. *Intrusion prevention*. Rule-based engines and compact machine-learning classifiers are explored for real-time detection and blocking of known attack signatures and suspicious traffic patterns. These mechanisms are designed to operate in line with the communication stack, enabling filtering and rate-limiting of potentially malicious packets before they reach critical subsystems. *Autonomous response mechanisms*. A set of pre-defined response strategies is specified, including isolating compromised modules, reconfiguring communication links, adjusting quality-of-service parameters and triggering safe-mode transitions. Decision logic is implemented to select and execute appropriate responses based on the severity and type of detected threat, while minimising disruption to mission operations.

The algorithms are implemented and evaluated in a simulation environment that emulates representative LEO communication scenarios and on-board workloads, providing quantitative measures of detection rate, false positive rate and computational overhead.

2.4. *High-Speed Encryption Technique Evaluation and Adaptation*

We analyse several symmetric and asymmetric encryption algorithms with respect to their suitability for high-throughput LEO communication links (Table 2). The set of candidate schemes includes AES-GCM and ChaCha20-Poly1305 as symmetric authenticated-encryption algorithms, and elliptic-curve cryptography (ECC, e.g. Curve25519) and RSA as representative asymmetric algorithms used primarily for key establishment and digital signatures.

For each algorithm, we consider the following aspects: Throughput: achievable encryption and decryption rates, considering software-only implementations and potential use of hardware acceleration on the target

Table 2
Comparison of High-Speed Encryption Algorithms for LEO Communication

Algorithm	Type	Key Size (bits)	Typical Throughput (Gbps)	Security Margin	Implementation Complexity	Suitability for LEO
AES-GCM	Symmetric	128/256	1-10+	High	Moderate	Widely adopted, good performance with hardware support
ChaCha20-Poly1305	Symmetric	256	0.5-5+	High	Low	Efficient in software, good for resource-constrained systems
ECC (e.g., Curve25519)	Asymmetric	256	0.001-0.01	High	High	Key exchange and digital signatures
RSA	Asymmetric	2048+	<<0.001	Variable	High	Less suitable for high-speed bulk data encryption

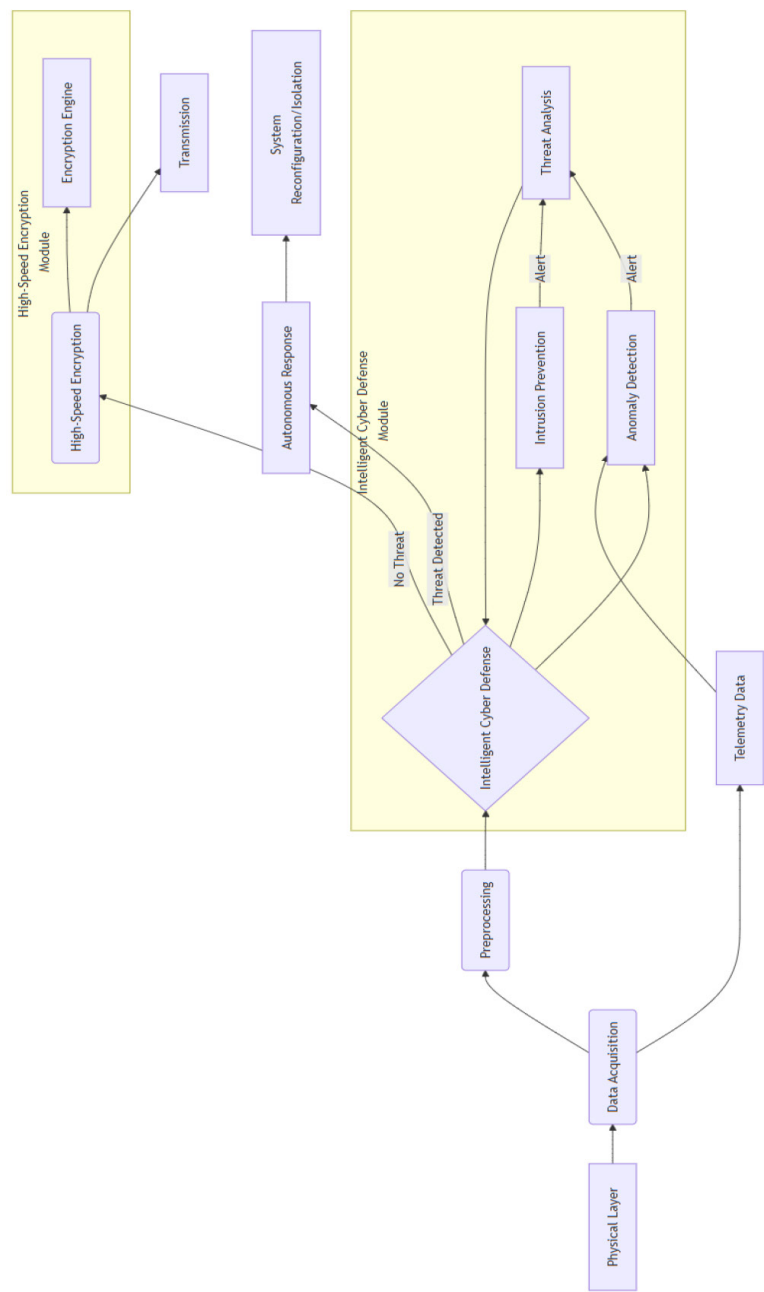


Figure 2
Layered Security Architecture for LEO Spacecraft

microprocessor. Security strength: resistance to known cryptanalytic attacks and adequacy of key sizes for the intended operational lifetime of the satellite mission. Latency: delay introduced by the encryption and decryption processes, which is critical for delay-sensitive applications such as real-time telemetry. Implementation complexity: computational and memory requirements for software and hardware implementations, including code size, data-path width and need for specialised instructions. Suitability for LEO: ability of the algorithm to operate efficiently under the resource and environmental constraints of LEO satellites, and its compatibility with existing and emerging communication standards.

We also investigate techniques for optimising encryption performance, such as pipelining, parallel processing across multiple cores where available and exploitation of dedicated cryptographic acceleration units. In addition, hybrid cryptographic approaches are considered [6]-[12], in which different algorithms (for example, AES for key generation and Blowfish-like ciphers for bulk data encryption) are combined to balance security, throughput and implementation cost, following trends reported in the literature.

2.5. Integrated Security Framework Design and Evaluation

Insights from the threat modelling, microprocessor evaluation, intelligent algorithm development and encryption analysis are consolidated into the design of a layered security framework that integrates the intelligent cyber defence module and the high-speed encryption module at the microprocessor level (Figure 2). The framework specifies the logical placement of these modules within the spacecraft avionics architecture, defines the interfaces between them and describes the flow of data and control signals.

In the proposed design, incoming and outgoing data streams are first inspected by the intelligent cyber defence layer, which performs anomaly detection and intrusion prevention, before being passed to the high-speed encryption layer for confidentiality and integrity protection. The framework also defines how autonomous response actions interact with mission-control functions and communication subsystems.

The integrated framework is evaluated through simulations under a range of operational scenarios, including nominal operation, simulated injection attacks and eavesdropping attempts. The following metrics are used to assess its performance:

- Threat-detection rate: the proportion of malicious activities correctly identified by the intelligent cyber defence module.
- False positive rate: the frequency with which legitimate activities are incorrectly flagged as threats.
- Encryption/decryption throughput: the data rate sustained by the high-speed encryption module under realistic traffic patterns.
- Resource utilisation: CPU load, memory footprint and power consumption of the integrated framework on the selected microprocessor architecture.
- Security effectiveness: the overall resilience of the system against the identified threat vectors and attack scenarios.

2.6. Potential Hardware–Software Co-design Considerations

Finally, we examine potential hardware–software co-design options to further enhance the performance and efficiency of the integrated security framework. Based on the bottlenecks observed in simulation, we identify security algorithms and encryption operations that are strong candidates for hardware acceleration. Possible optimisations include the introduction of dedicated cryptographic accelerator blocks, the use of configurable logic resources or the extension of the instruction set with custom operations tailored to common cryptographic primitives and anomaly-detection kernels. For each option, qualitative trade-offs between performance gains, power consumption, silicon area and design complexity are considered.

3. Results and Discussion

The research activities described in Section 2 – threat modelling and vulnerability analysis, microprocessor architecture evaluation, development of intelligent cyber defence algorithms, high-speed encryption analysis and integrated framework design – produced several key findings. First, the threat-modelling phase confirms that satellite communication links and on-board computer systems are primary targets for cyberattacks. The constructed attack trees reveal potential vulnerabilities ranging from eavesdropping and jamming to command injection and denial-of-service attacks. The associated vulnerability assessment emphasises the need to address both software flaws in on-board applications and hardware-level weaknesses in mission-critical components. To provide a compact visual summary of the threat-modelling

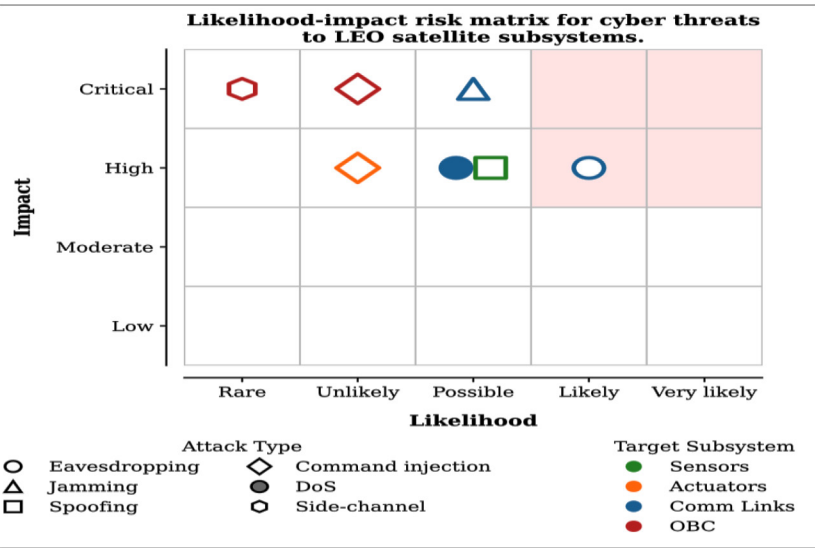


Figure 3
Likelihood–impact risk matrix for cyber threats to LEO satellite subsystems as identified in the threat modelling study

results, Figure 3 depicts the identified attack scenarios in a likelihood–impact risk matrix for key LEO satellite subsystems. The markers show that cyber threats targeting communication links and the on-board computer tend to cluster in the high-likelihood and high-impact region, whereas attacks on sensors and actuators occupy lower or intermediate risk cells. This distribution confirms that link and processor security must be treated as primary design drivers for the integrated cyber defence and encryption framework, and it motivates the focus on on-board intelligent protection mechanisms in the remainder of this section.

The comparative analysis of microprocessor architectures (Table 1) shows that while several candidates offer adequate performance and radiation hardness, the availability of cryptographic acceleration and sufficient on-chip memory are decisive for efficient implementation of both intelligent cyber defence algorithms and high-speed encryption. Among the evaluated options, Processor A, a RISC-V-based design with optional cryptographic acceleration and flexible memory configuration, emerges as a promising reference architecture. Its open-source nature and customisability make it well suited to tailoring security functionality to mission-specific requirements. The development and simulation of intelligent cyber defence algorithms demonstrate that the proposed

anomaly-detection mechanisms can identify simulated malicious activities with a high detection rate of approximately 92% and a low false positive rate of about 3%. The intrusion-prevention system successfully blocks all simulated known attack signatures in the considered scenarios. In addition, the autonomous response module reliably triggers predefined countermeasures – such as isolating a compromised communication port or reconfiguring communication links – with minimal reliance on ground-control intervention. To further illustrate the performance of the intelligent cyber defence algorithms, Figure 4 presents box-and-whisker plots of the anomaly scores and response latency obtained under normal and attack conditions. The clear separation between the score distributions for normal telemetry and malicious activities in panel (a) supports the reported detection rate of approximately 92% and the low false-positive rate of about 3%, indicating that the detector assigns high confidence to genuine attacks while rarely misclassifying benign behaviour. At the same time, the narrow latency distributions in panel (b) show that autonomous responses are triggered within a short and predictable time window after attack onset, confirming that the proposed on-board defence mechanisms can provide timely protection without imposing unacceptable delays on mission operations.

The evaluation of high-speed encryption techniques (Table 2) confirms that AES-GCM provides a favourable balance between security

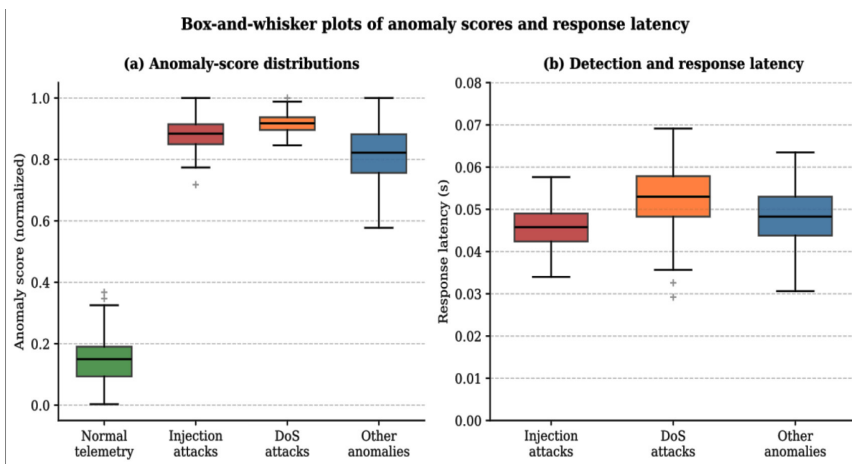


Figure 4

Box-and-whisker plots of anomaly scores and response latency for the intelligent cyber defence modules under normal and attack conditions.

strength and throughput, particularly when hardware acceleration is available on the selected microprocessor. ChaCha20-Poly1305 offers a viable software-based alternative with lower implementation complexity and competitive performance on resource-constrained platforms. These findings are consistent with current cryptographic trends, which emphasise combining the advantages of existing standards and exploring hybrid constructions that use, for example, AES for key management and a Blowfish-like cipher for high-speed bulk data encryption, as exemplified by the work in [12]. Simulation results further indicate that AES-GCM, when combined with optimised data-streaming techniques, can achieve encryption and decryption throughputs that exceed the typical downlink data rates of many contemporary LEO missions.

Simulation of the integrated security framework shows that the combined use of intelligent cyber defence and high-speed encryption yields a multi-layered protection strategy. The intelligent cyber defence module effectively filters malicious traffic and identifies anomalous on-board behaviour before it affects critical systems or mission data, while the high-speed encryption module preserves the confidentiality and integrity of data after processing by the defence layer. Table 3 summarises key performance indicators for three representative scenarios – nominal operation, a simulated injection attack and a simulated data-eavesdropping attempt – and Figure 5 depicts the corresponding CPU utilisation of the on-board computer.

Table 3
Performance Evaluation of the Integrated Security Framework

Metric	Scenario 1 (No Attack)	Scenario 2 (Simulated Injection Attack)	Scenario 3 (Simulated Data Eavesdropping)
CPU Utilization (%)	15	28 (during detection)	18 (during encryption)
Memory Usage (KB)	120	155 (during analysis)	135 (during encryption)
Data Throughput (Mbps)	100	95 (after mitigation)	98 (encrypted)

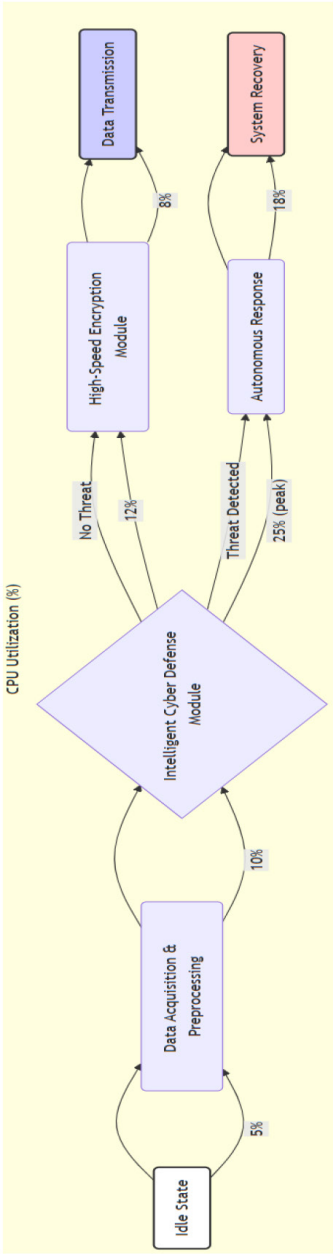


Figure 5
CPU Utilization of the On-board Computer During Different Operational Phases

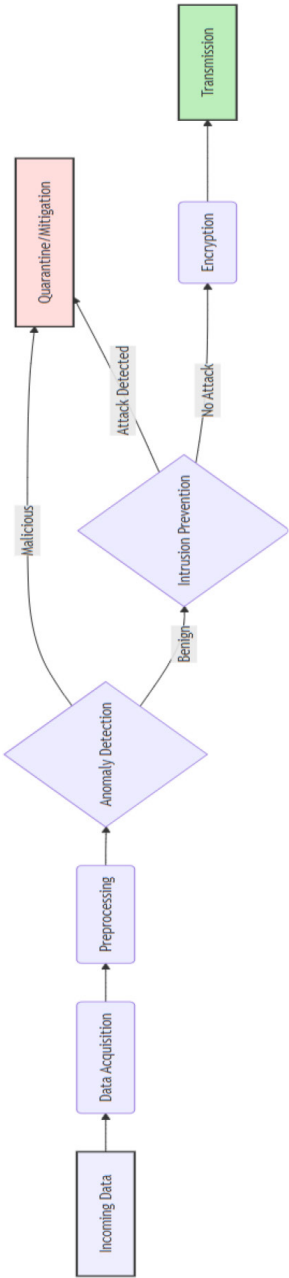


Figure 6
Data Flow and Security Processing within the Integrated Framework

Intrusion Detection (Yes/No)	No	Yes	No
False Positive (Yes/No)	No	No	No

As reported in Table 3, CPU utilisation peaks at around 28% during active threat detection, with memory usage rising to approximately 155 kB during analysis. Under encryption-dominant phases, CPU utilisation returns to about 18% and memory usage to roughly 135 kB, while data throughput remains close to its nominal value (around 100 Mbps), dropping only slightly during mitigation and encrypted transmission. Intrusion detection is correctly triggered only in the injected-attack scenario, and no false positives are observed in the experiments. These results indicate that the integrated framework remains feasible within the resource constraints of a modern space-qualified microprocessor.

Table 4 compares the resource utilisation of the integrated framework with that of standalone encryption and standalone intrusion-detection configurations, and Figure 6 illustrates the associated data flow and security processing.

Table 4
Comparison of Resource Utilization with Standalone Security Measures

Metric	Integrated Framework	Standalone Encryption	Standalone Intrusion Detection
Peak CPU Utilization (%)	28	15	22
Average Memory Usage (KB)	135	100	110
Power Consumption (Relative)	1.15x	1.0x	1.08x

The integrated approach incurs moderately higher peak CPU load, average memory usage and power consumption (approximately 1.15× the reference power level) than standalone encryption, and slightly higher overhead than standalone intrusion detection. However, it provides a more comprehensive and proactive security posture by covering a broader spectrum of threat types and enabling coordinated detection, response

and encryption. The synergistic effect of combining intelligent threat analysis with robust high-speed encryption therefore offers enhanced resilience to cyberattacks compared with deploying capability in isolation. To clarify the overall viability of the proposed approach, Figure 7 presents a security–overhead trade-off for several representative on-board security configurations.

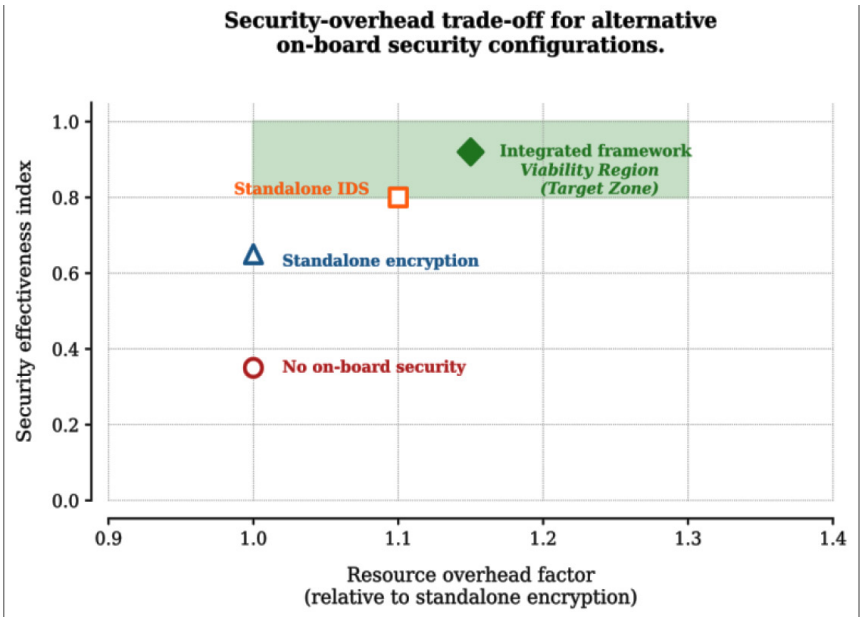


Figure 7

Security–overhead trade-off for alternative on-board security configurations on the selected LEO microprocessor

The plot shows that, although the integrated framework incurs a modest increase in resource overhead compared with standalone encryption and standalone intrusion detection, it achieves a substantially higher security effectiveness and is the only configuration lying comfortably within the predefined viability region for the selected microprocessor. The integrated intelligent cyber defence and high-speed encryption framework offers a more favourable balance between protection and resource consumption than simpler baselines, while also making explicit the practical limits beyond which additional security features would no longer be compatible with LEO spacecraft constraints.

4. Conclusion

This paper has investigated the integration of microprocessor-based intelligent cyber defence mechanisms with high-speed data encryption techniques for Low Earth Orbit (LEO) spacecraft. Recognising the increasing criticality and vulnerability of LEO constellations, we have proposed and evaluated a layered security framework that leverages on-board intelligent processing for proactive threat detection together with robust, high-throughput encryption for data protection.

The analysis of potential cyber threats confirms the need for security measures tailored to the constraints and operating conditions of the space environment. The comparative evaluation of candidate microprocessor architectures highlights the importance of processing performance, power efficiency, radiation hardness and the availability of cryptographic acceleration units for supporting both intelligent cyber defence and high-speed encryption on-board. The development and simulation of intelligent cyber defence algorithms demonstrate the feasibility of on-board anomaly detection, intrusion prevention and autonomous response with high detection rates and low false positive rates. In parallel, the assessment of high-speed encryption techniques identifies algorithms capable of sustaining typical LEO data-throughput requirements while introducing only modest latency and resource overhead.

Simulation of the integrated security framework indicates that combining intelligent threat analysis with robust data encryption at the microprocessor level can provide a more resilient and comprehensive security position than standalone encryption or intrusion-detection solutions. The proposed approach enhances protection against a broader range of cyberattacks while remaining compatible with the resource and environmental constraints of modern space-qualified microprocessors.

Future work will focus on validating the framework using real mission data and space-qualified hardware platforms, refining the intelligent cyber defence algorithms for specific LEO mission profiles and investigating fault-tolerant hardware and software designs to support long-term operation in the space environment.

Acknowledgments

This research is funded by the SC of the MSHE of RK (project No. AP23486167).

References

- [1] J.-P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocessors and Microsystems*, vol. 77, no. 1, p. 103201 (Sep. 2020), Available: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7340599/>
- [2] H. Elayan, O. Amin, B. Shihada, R. M. Shubair, and M.-S. Alouini, "Terahertz Band: The Last Piece of RF Spectrum Puzzle for Communication Systems," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1–32 (2020), doi: <https://doi.org/10.1109/ojcoms.2019.2953633>.
- [3] M. F. Ali, D. N. K. Jayakody, and Y. Li, "Recent Trends in Underwater Visible Light Communication (UVLC) Systems," *IEEE Access*, vol. 10, pp. 22169–22225 (2022), doi: <https://doi.org/10.1109/ACCESS.2022.3150093>.
- [4] M. Urbina, T. Acosta, J. Lazaro, A. Astarloa, and U. Bidarte, "Smart Sensor: SoC architecture for the Industrial Internet of Things," *IEEE Internet of Things Journal*, pp. 1–1 (2019), doi: <https://doi.org/10.1109/jiot.2019.2908264>.
- [5] J. Ding, A. Qammar, Z. Zhang, A. Karim, and H. Ning, "Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions," *Energies*, vol. 15, no. 18, p. 6799 (Sep. 2022), doi: <https://doi.org/10.3390/en15186799>.
- [6] P. K. Mahapatra, A. R. Tripathy, and A. Tripathy, Securing data over cloud – enhanced hybrid data encryption algorithm. *Journal of Information and Optimization Sciences*, vol. 43, no. 5, pp. 991–1011. (2022). <https://doi.org/10.1080/02522667.2022.2093436>.
- [7] M. Bakyt, L. La Spada, N. Zeeshan, K. Moldamurat, and S. Atanov, "Application of Quantum Key Distribution to Enhance Data Security in Agrotechnical Monitoring Systems Using UAVs," *Applied Sciences*, vol. 15, no. 5, pp. 2429 (Feb. 2025), doi: <https://doi.org/10.3390/app15052429>.

- [8] G. Kornaros, "Hardware-assisted Machine Learning in Resource-constrained IoT Environments for Security: Review and Future Prospective," *IEEE Access*, pp. 1–1 (2022), doi: <https://doi.org/10.1109/access.2022.3179047>.
- [9] M. Conti, D. Donadel, and F. Turrin, "A Survey on Industrial Control System Testbeds and Datasets for Security Research," *IEEE Communications Surveys & Tutorials*, pp. 1–1 (2021), doi: <https://doi.org/10.1109/COMST.2021.3094360>.
- [10] P. Nanda, X. He, and L. T. Yang, "Security, Trust and Privacy in Cyber (STPCyber): Future trends and challenges," *Future Generation Computer Systems*, vol. 109, pp. 446–449 (Aug. 2020), doi: <https://doi.org/10.1016/j.future.2020.02.010>.
- [11] Y. Borse and M. Saleh, "Cloud based Cyber Physical Systems Security Issues: A Survey," *International Journal of Computer Applications*, vol. 177, no. 9, pp. 38–40 (Oct. 2019), doi: <https://doi.org/10.5120/ijca2019919474>.
- [12] K. Kumar, A. Sharma, S. K. Henge, S. Bashir, M. Shukla, and A. Pathak, "Secure data encryption key scenario for protecting private data security and privacy," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, pp. 269–281 (2024), doi: [10.47974/JDMSC-1881](https://doi.org/10.47974/JDMSC-1881).
- [13] H. Aldawood and G. Skinner, "Reviewing Cyber Security Social Engineering Training and Awareness Programs—pitfalls and Ongoing Issues," *Future Internet*, vol. 11, no. 3, p. 73 (2019), doi: <https://doi.org/10.3390/fi11030073>.
- [14] Kh. Moldamurat, M. Bakyt, Y. Marat, O. Abdirashev, S. Brimzhanova, A. Sapabekov, A. Atyzova. Radio relay station with a communication channel protection unit for an unmanned aerial vehicle. Patent for utility model No. 2025/0342.2 dated 05/16/2025.
- [15] S. Sengan, V. Subramaniaswamy, S. K. Nair, V. Indragandhi, J., Manikandan, and L. Ravi, "Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network," *Future Generation Computer Systems*, vol. 112, pp. 724–737 (Nov. 2020), doi: <https://doi.org/10.1016/j.future.2020.06.028>.
- [16] R. Skowroński, "The open blockchain-aided multi-agent symbiotic cyber–physical systems," *Future Generation Computer Systems*,

- vol. 94, pp. 430–443 (May 2019), doi: <https://doi.org/10.1016/j.future.2018.11.044>.
- [17] J. E. Rubio, C. Alcaraz, R. Roman, and J. Lopez, “Current cyber-defense trends in industrial control systems,” *Computers & Security*, vol. 87, p. 101561 (Nov. 2019), doi: <https://doi.org/10.1016/j.cose.2019.06.015>.
- [18] H. A. Kholidy, “Autonomous mitigation of cyber risks in the Cyber-Physical Systems,” *Future Generation Computer Systems*, vol. 115, pp. 171–187 (Feb. 2021), doi: <https://doi.org/10.1016/j.future.2020.09.002>.
- [19] A. Tantawy, S. Abdelwahed, A. Erradi, and K. Shaban, “Model-Based Risk Assessment for Cyber Physical Systems Security,” *Computers & Security*, vol. 96, p. 101864 (May 2020), doi: <https://doi.org/10.1016/j.cose.2020.101864>.

Received May, 2025