Internship title: Digital Twins Based Key Management for IoT Networks

Location: ERIC Lab

Internship supervisors (Emails):

- Mohamed-Lamine Messai (mohamed-lamine.messai@univ-lyon2.fr)
- Fadila Bentayeb (fadila.bentayeb@univ-lyon2.fr)
- Jérôme Darmont (jerome.darmont@univ-lyon.fr)

Keywords: IoT Security, Key Management, Digital Twins, Artificial Intelligence, Lightweight Cryptography

Duration: 5 months.

Desired starting date: February / March 2026

Context: The rapid development of the Internet of Things (IoT) go on transforming numerous domains, including healthcare, smart cities, industry and critical infrastructures. However, this expansion also introduces major cybersecurity challenges. Among these, **key management,** which includes key generation, distribution, renewal and revocation, is fundamental for ensuring secure communications. Traditional key management protocols are often ill-suited for IoT devices, which are highly heterogeneous and constrained in memory, computation and energy.

Digital Twins (DTs) offer a promising avenue to enhance IoT security. By maintaining a virtual, real-time representation of each physical device, DTs make it possible to monitor system behavior, detect anomalies, simulate security events, and support proactive decision-making. Integrating Digital Twins into key management may enable more adaptive, context-aware, and resilient cryptographic mechanisms.

This internship aims to investigate how DT technologies can improve key management processes in IoT networks. Potential enhancements include:

- optimized key distribution based on real-time device states,
- intelligent key refresh triggered by predicted compromise risk,
- improved resilience and self-healing capabilities,
- energy-aware security adaptation based on DT-driven analytics.

Objectives and Methodology

The internship will begin with a detailed literature review covering:

- existing lightweight key management schemes for IoT,
- self-healing and key refresh techniques,
- digital twin architectures applied to cybersecurity,
- AI/ML approaches supporting security decision-making.

The student will then:

1. **Design a Digital Twin model** representing IoT devices, their security states, and key lifecycle operations.
2. **Propose and implement** a DT-assisted key management mechanism (e.g., adaptive key refresh, risk-aware distribution).
3. **Develop a prototype.**
4. **Evaluate the system** in terms of:
    - computational/communication overhead, scalability,
    - energy consumption,
    - resilience against node compromise and common attacks.

To apply, the candidate must have advanced skills in computer science (computer security skills are highly desirable). Please send your application with a CV, a cover letter, as well as your grades for the current academic year and last year to Mohamed-lamine.messai@univ-lyon2.fr, fadila.bentayeb@univ-lyon2.fr, jerome.darmont@univ-lyon.fr

Références

[1] Naveen, P., Maheswar, R., & Ragupathy, U. S. (Eds.). (2025). Digital twins and cybersecurity: safeguarding the future of connected systems. John Wiley & Sons.
[2] Huang, J., & Yi, J. (2024). The key security management scheme of cloud storage based on blockchain and digital twins. Journal of Cloud Computing, 13(1), 15.
[3] Wang, Y., Su, Z., Guo, S., Dai, M., Luan, T. H., & Liu, Y. (2023). A survey on digital twins: Architecture, enabling technologies, security and privacy, and future prospects. IEEE Internet of Things Journal, 10(17), 14965-14987.