

Securing the Future of IoT: How

# RIoT Secure

is Redefining Device Security and  
Lifecycle Management

**Aaron Ardiri,**  
CEO & Co-Founder

---

In today's hyperconnected world, the Internet of Things (IoT) is not just a convenience—it's an essential infrastructure. From manufacturing plants and smart cities to healthcare devices and supply chain sensors, billions of embedded devices are collecting, processing, and transmitting data every second. Yet, beneath this digital revolution lies a ticking time bomb: security. As device deployments grow, so do vulnerabilities. Security breaches are no longer a hypothetical threat—they are a present and persistent reality.

While many companies scramble to patch vulnerabilities reactively, one company is taking a radically different approach. **RIoT Secure**, based in Stockholm, Sweden, is changing how the world thinks about embedded security. Founded by **Aaron Ardiri** and **Bjorn de Jonge**, veteran technologists with over two decades of experience in mobile, embedded systems, and cybersecurity, the company is building a future where IoT devices are secure by design—not by afterthought.

RIoT Secure's breakthrough lies in its “secure by design” end-to-end IoT security and lifecycle management platform. Unlike traditional systems that bolt on security at the final development stages, RIoT Secure integrates it from day one. The result is a hardware-anchored platform that provides lifecycle management, secure communications, and seamless over-the-air (OTA) updates for even the most resource-constrained devices—all while being accessible and intuitive for developers.

## From Prototype to Scale—Without the Pain

One of the most common frustrations in the IoT space is the chasm between prototyping and production. Developers can build a proof-of-concept with relative ease using off-the-shelf modules and cloud tools. But when it's time to scale—when hundreds or thousands of devices need to be deployed securely and maintained over years—that's when things fall apart. Security protocols become harder to manage, update mechanisms start failing





# Security is no longer optional in IoT. It's fundamental. We built RIoT Secure to be the foundation for this next generation of connected systems.

— Aaron Ardiri, CEO & Co-Founder  
RIoT Secure

in the field, and teams are forced to re-engineer the entire stack just to meet upcoming government compliance standards.

RIoT Secure's platform was purpose-built to eliminate this pain. By providing a unified framework for device onboarding, secure communication, monitoring, updates, and eventual decommissioning, the platform makes it possible for companies to move from idea to deployment without compromise. Developers can continue using their preferred microcontrollers and programming languages while the platform abstracts away the complexities of encryption, key management, firmware updates, and communication protocols.

What makes this especially powerful is that RIoT Secure supports edge environments—places where connectivity is poor or intermittent, power is limited, and cloud access isn't guaranteed. In these situations, traditional cloud-based security approaches fall short and RIoT Secure's solution thrives, providing optimized data transfer and reliable messaging capabilities.

## A New Model for Embedded Security

At the core of RIoT Secure's technology is its **microTLS protocol**, a secure communication model engineered

specifically for low-power, embedded devices, which includes patented communication techniques. Unlike traditional HTTPS or MQTT implementations—which are often too resource-intensive—microTLS delivers robust encryption while drastically minimizing data usage. In fact, RIoT Secure reports up to **90% less data transfer** compared to conventional methods, a huge benefit for battery-powered or bandwidth-limited devices.

This isn't just a communications breakthrough—it's a shift in the security model. Devices using RIoT Secure operate within an isolated hardware sandbox, keeping critical processes separated from application logic. This isolation prevents lateral attacks and offers strong protection against remote tampering, even in physically vulnerable deployments.

Additionally, RIoT Secure's OTA system uses differential updates and partial patching to keep devices up to date while conserving resources – particularly in low-bandwidth networking environments. With built-in version control and integrity checks, updates can be validated in real time, reducing the need for field technicians and significantly lowering operational costs.

Perhaps most impressively, this secure architecture is achieved without placing a burden on developers. Everything is pre-integrated, optimized for performance, and ready to deploy.

## Enabling AI at the Edge

While many security platforms focus on cloud-based anomaly detection, RIoT Secure takes a different path—empowering developers to embrace edge intelligence. The platform supports the deployment of **machine learning models directly on-device**, within the secure application sandbox. This approach allows real-time anomaly detection, predictive maintenance, and localized decision-making, even in environments without reliable internet access.

For industries like manufacturing, logistics, and energy—where downtime or data breaches can carry enormous financial and reputational consequences—this is a critical capability. And it's one that puts RIoT Secure ahead of the curve, especially as edge AI adoption accelerates globally.



As Ardiri puts it, “Our goal is to give developers everything they need to build secure, intelligent devices that run reliably in the real world—not just in the lab.”

## Built for What Comes Next

RIoT Secure isn't building for today's problems alone—it's anticipating tomorrow's. The platform is modular and future-ready, designed to adapt to new protocols, evolving network standards, and rapidly changing cybersecurity regulations.

The company actively tracks global legislation, including the **EU Cyber Resilience Act**, and ensures that its cryptographic framework complies with modern standards while remaining lightweight and developer-friendly. In contrast to legacy solutions that require complex integrations, RIoT Secure's system works out of the box—and continues to evolve with the landscape.

This future-first philosophy is a major reason RIoT Secure has earned industry-wide recognition. The company has already been named **IoT Startup of the Year** by IoT Breakthrough, and it was selected for **TechCrunch Disrupt Startup Battlefield 200**, a signal of both its technological leadership and market potential.

Now, with pilot projects successfully deployed and momentum building, the company is preparing for a **global scale-up**. Over the next 12–18 months, RIoT Secure plans to onboard strategic partners, expand its engineering and sales teams, and bring its platform to industries that demand secure, scalable IoT deployments—from energy and defense to smart cities and connected agriculture.

Ardiri envisions the company not just as a vendor, but as an **innovation hub**—constantly experimenting with new ideas and exploring ways to redefine how IoT devices operate, communicate, and protect themselves in increasingly complex environments.

“Security is no longer optional in IoT. It's fundamental. We built RIoT Secure to be the foundation for this next generation of connected systems,” says Ardiri.

## Final Thoughts

The future of IoT is full of promise—but only if it's secure, scalable, and sustainable. RIoT Secure is delivering on that promise with a platform that combines cryptographic excellence, developer simplicity, and lifecycle control in a single solution.

By giving companies the tools to deploy secure devices from day one and maintain them for years, the company is rewriting the rulebook for embedded security. In a space where most providers patch after the fact, RIoT Secure designs security into the DNA of every device. It's not just about protecting networks—it's about empowering innovation.

