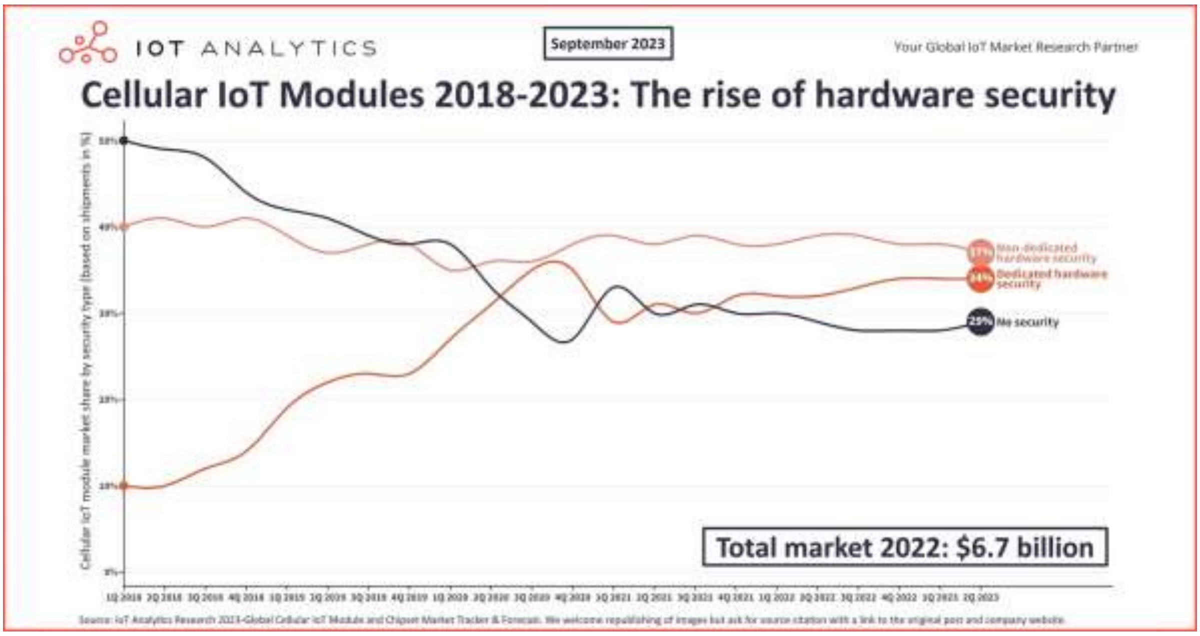
IOT ANALYTICS

IoT Analytics GmbH
Zirkusweg 2
D-20359 Hamburg

T: +49 (0) 40- 63911891
M: press(at)iot-analytics.com
www.iot-analytics.com

FOR IMMEDIATE RELEASE

Cellular IoT module market Q2 2023: 66% of IoT modules shipped without dedicated hardware security



Hamburg, Germany, September 21, 2023: IoT Analytics, a leading provider of market insights and strategic business intelligence for the Internet of Things (IoT), has published its latest research on the global cellular IoT module and chipset market for Q2/2023. The report reveals that 66% of IoT modules shipped in Q2 2023 had no dedicated hardware security and 29% had no security features at all, exposing them to potential risks and vulnerabilities.

The research analyzes the security features of 772 unique modules from 36 vendors and 150+ chipsets from 13 vendors that IoT Analytics tracks. It shows that only 30% of the modules available on the market, had dedicated hardware security features. Additionally, the article highlights the differences between the global and North American markets, where the latter has a higher share of non-dedicated hardware security features, such as TrustZone or secure boot.

The report is part of IoT Analytics' Global Cellular IoT Module and Chipset Market Tracker & Forecast, which provides a quarterly look at the revenues and shipments of the companies providing IoT modules and chipsets for cellular IoT deployments. The tracker also includes a quarterly and annual forecast from Q3 2023 to 2027.

Key quotes

Commenting on the importance of IoT security, Principal Analyst Satyajit Sinha noted, "*As cybercrime operates much like a business, criminals invariably opt for the path of least resistance. Implementing multiple layers of security increases the time and cost required for hackers to breach a system, thus making it more likely for them to abandon the effort and seek out less well-protected targets*."

Mr. Sinha added, "*Cellular IoT modules are crucial for connectivity in IoT devices across industries. They provide a vital connection to the internet and are managed remotely. Ensuring their security is vital for safeguarding the broader IoT ecosystem*."

Key insights

- The cellular IoT module market was stagnant in Q2'23 according to IoT Analytics latest data.
- Although IoT modules with dedicated security features are increasingly adopted, 66% of IoT modules shipped in Q2'23 had no dedicated hardware security and 29% had no security features at all.
- Recent demonstrations of vulnerabilities in non-dedicated hardware security features should drive the market further towards hardware-based security. Post-quantum cryptography is also an important consideration in IoT module security.

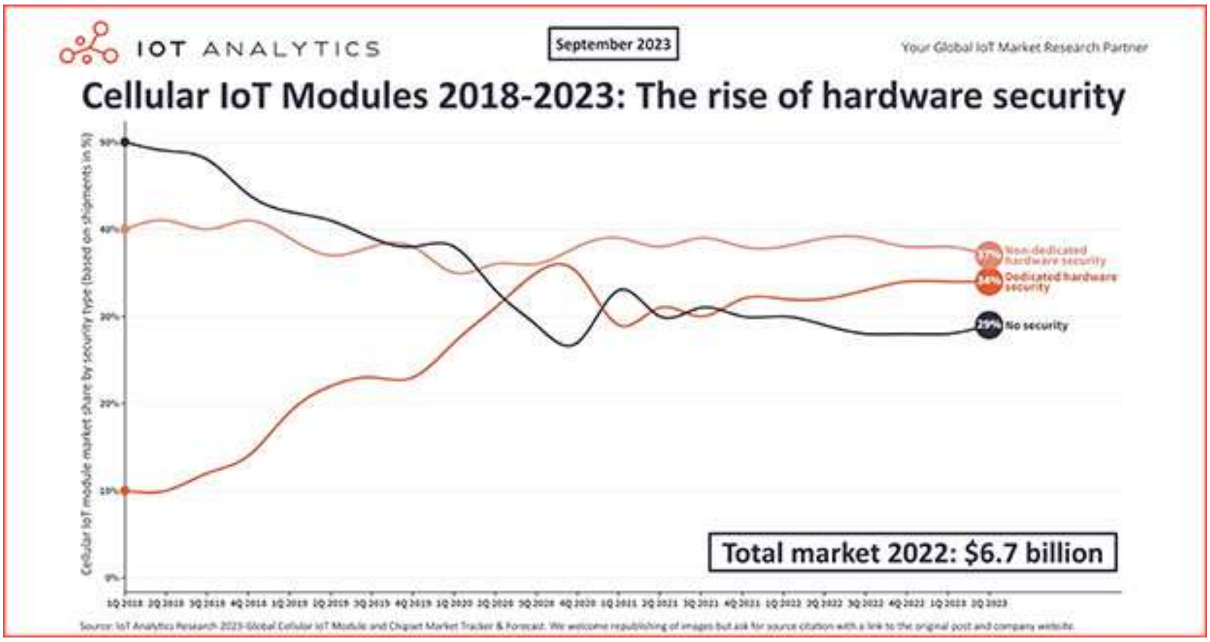
[The full research article is attached below]

IOT ANALYTICS

IoT Analytics GmbH
Zirkusweg 2
D-20359 Hamburg

T: +49 (0) 40- 63911891
M: press(at)iot-analytics.com
www.iot-analytics.com

Cellular IoT module market Q2 2023: 66% of IoT modules shipped without dedicated hardware security



Source: IoT Analytics Research 2023-Global Cellular IoT Module and Chipset Market Tracker & Forecast. We welcome republishing of images but ask for source citation with a link to the original post and company website.

Updated cellular IoT module market

29% of cellular IoT modules shipped in Q2 2023 had no dedicated security features and only 34% had hardware-based security. This is one of the key statistics from IoT Analytics updated in-depth **Global Cellular IoT Module and Chipset Market Tracker & Forecast Q2 2023**, which provides a quarterly look at the revenues and shipments of the companies providing IoT modules and chipsets for cellular IoT deployments. Overall, the shipment and revenue of the $6.7 billion market (2022) remained generally flat in Q2'23 quarter-over-quarter, with 0% shipment and 0% revenue growth. Reasons for this stagnation include a weakened demand environment, which we discussed in our Q1'23 analysis of the cellular IoT module market.

IoT module security at the center of attention

With markets stagnating, we are putting a spotlight on cellular IoT module security by looking at the security features of 772 unique modules from 36 vendors and 150+ chipsets from 13 vendors that we track. IoT module security is of particular interest right now in light of the US Congress' 7 August 2023 letter to the US Federal Communications Commission (FCC) regarding potential security risks of using Chinese cellular IoT modules.

Our analysis of the updated tracker and forecast shows the following breakdown of IoT module security features out of the aforementioned modules/chipsets available on the market in Q2'23:

- 30% had **dedicated hardware** security features, often embedded in chipsets or standalone components implemented through hardware security modules
- 42% had **non-dedicated hardware** security features, or features used to either create secure environments for processes to run or ensure only authorized firmware is loaded on the device
- 28% had no security features

However, the share of purchased/shipped modules with these security classifications in Q2'23 differs, with a significant difference between the global and North American markets as well:

Module security type	Global market	North American market
Dedicated hardware security	34%	24%
Non-dedicated hardware security	37%	68%
No security	29%	8%

While the global market shows a relatively balanced share of these three categories, the North American market skews heavily toward non-dedicated hardware security features. The low share of cellular IoT modules without security features in the North American market indicates that module security is a concern for its consumers, though there appears to be a reliance on non-dedicated hardware security features, such as TrustZone or secure boot.

This indication is consistent with recent concerns that the US Congress expressed to the **FCC** regarding the security of Chinese-made cellular IoT modules within US infrastructure (either directly or as part of the manufacturing supply chain), such as **FirstNet** Authority networks and devices used by first responders across the country

(**Quectel** and **Fibocom** have published press releases responding to the US Congress's concerns in early September 2023).

Why dedicated hardware security is the way forward amid supply chain concerns

Software and network security solutions have historically overshadowed dedicated hardware security features in IoT since they are more visible and easier to address, while dedicated hardware security features can be more complex and costly to implement. An alternative to software and network security solutions are non-dedicated hardware security features, such as **ARM's TrustZone**, which creates a secure environment for processes to run, and **secure boot**, which ensures systems boot without intrusions.

Unfortunately, researchers recently demonstrated side-channel attacks against TrustZone during the Black Hat Asia 2023 conference. For their part, ARM has responded to this demonstration by stating that the attack is not unique to ARM's Cortex-M architecture or TrustZone; rather, it's a failure in application code—such attacks "may apply to any code with secret-dependent control flow or memory access patterns." However, such attacks, no matter the core system they possess, demonstrate that adding dedicated hardware security solutions to these non-dedicated hardware security solutions can enhance the overall security of a module.

Shahram Mossayebi, Ph.D., founder and CEO of **Crypto Quantique**, explained the following to IoT Analytics when asked about cellular IoT module security:

"*[W]e rely on security features such as TrustZone, but to achieve trust, we need to go beyond them. A root of trust is a set of cryptographic features (which soon must be quantum secure) for encryption, digital signature, and device identity. The hardware root of trust is the foundation for building trust with any IoT [device] and it is a crucial part of hardware security*."

With a hardware-based root of trust, manufacturers and consumers can ensure the authenticity of the modules—helping to address cloning and counterfeiting—and protection of the device's keys. Once manufacturers can guarantee the authenticity and security of these keys, they can add additional security components like TrustZone and secure boot.

Where hardware security should be implemented

Implementing security measures at the device level during manufacturing is a foundational step, aiding in establishing device authenticity and partially curbing the infiltration of counterfeit components in the supply chain. However, this strategy only offers a partial solution since vulnerabilities still exist, particularly in the potential theft and cloning of device identities within supplier factories. Thus, an even more nuanced approach is required to bolster the defenses against such nefarious activities that seek to undermine the system from its very core.

To combat these risks more effectively, embedding hardware security at the MCU level within typical modules is highly recommended. This strategic positioning not only presents a formidable barrier against cloning and counterfeiting issues but also fosters the establishment of secure authentication protocols and the creation of unique device identities. Secure MCUs can provide a seamless integration of essential security features, such as robust authentication processes, potent encryption capabilities, and secure boot functionalities. These functionalities come together to create a fortified environment, essential for the optimal functioning of connected IoT applications, thereby ensuring a safer, more reliable network where devices can communicate and operate with an enhanced level of security and trust.

IoT module security outlook: Post-quantum security is becoming crucial for IoT

Currently, the general life span of most IoT devices is 8–12 years, with automotive 5G module applications lasting 10–15 years. With these long life spans, when building cellular IoT modules, it is essential that manufacturers look beyond current threats; specifically, they should start planning for the commercialization of quantum computing and the potential for state actors and cybercriminals to crack complex, commonly used encryption methods.

In October 2019, **Google** announced quantum supremacy in the journal *Nature* with its 54-qubit Sycamore processor, which Google claims was able to perform a complicated task in 200 seconds that would take the world's most powerful supercomputer 10,000 years to perform. Many countries and companies are also advancing with quantum computing, such as the **Chinese Academy of Sciences** and **QuantumCTek**, a quantum information technology developer. Other Google competitors, such as **IBM**, **Microsoft**, **Amazon**, and **Intel**, along with several new startups, have all invested heavily in developing quantum computing hardware in recent years.

While quantum chips have not reached widespread commercialization yet, manufacturers can start considering quantum security solutions today. Governments are already looking at standards and quantum-proofing solutions for their agencies and companies, and the following are just some examples:

- In January 2022, the French **National Agency for IT Systems Security (ANSSI)** published its views and recommendations for PQC transition, offering a 3-phase process expected to last at least until 2030.
- In July 2022, the US Department of Commerce's **National Institute of Standards and Technology (NIST)** announced its selection of four quantum-resistant cryptography algorithms, constituting "the beginning of the finale of the agency's post-quantum cryptography (PQC) standardization project," which NIST expects to complete and publish in 2024.
- In August 2023, the US **National Security Agency (NSA)**, **Cybersecurity and Infrastructure Security Agency (CISA)**, and NIST published a PQC migration readiness sheet to help the government and private sector start planning their quantum readiness.

Further, some companies are already developing post-quantum solutions. For example, **Thales Group** offers 5G security solutions with end-to-end encryption and authentication to safeguard organizational data as it moves across front-haul, mid-haul, and back-haul operations. These solutions rely on Thales' 5G Luna Hardware Security Modules (HSMs). Further, in February 2023, Thales Group announced that it successfully piloted what it called a post-quantum resilient, end-to-end encrypted call using its Cryptosmart mobile app and its 5G SIM.

What it means for cellular IoT module manufacturers

5 key questions that cellular IoT module manufacturers should ask themselves based on the insights in this article:

1. **Product strategy and security implementation:** How can we realign our product strategy to prioritize the implementation of dedicated hardware security features without significantly escalating costs?
2. **Response to political and legislative changes:** How are we positioning ourselves to address the potential political and legislative changes affecting the market, particularly concerning the US Congress's concerns regarding Chinese cellular IoT modules?

3. **Security standards and compliance:** Are we in line with the recent security standards and guidelines issued by agencies like ANSSI, NIST, and NSA, and are we preparing for the expected security transitions in the coming years?
4. **Consumer education and advocacy:** How can we educate consumers on the importance of dedicated hardware security features and advocate for a broader shift towards these in the market?
5. **Post-quantum security solutions:** Are we collaborating with communications companies and other stakeholders to develop and pilot post-quantum security solutions that can safeguard organizational data across various operations effectively?

What it means for users of cellular IoT modules

5 key questions that device/equipment makers and end users that adopt cellular IoT module should ask themselves based on the insights in this article:

1. **Security implementation:** Given the demonstrated vulnerabilities in non-dedicated hardware security features, what strategies should we adopt to integrate dedicated hardware security features without escalating costs significantly?
2. **Compliance and legislation:** In light of the concerns raised by the US Congress regarding the use of Chinese cellular IoT modules, how can we ensure compliance with evolving regulations and maintain the trust of our North American consumers?
3. **Post-quantum security:** Given the advancements in quantum computing, what steps should we take to incorporate post-quantum security solutions in our cellular IoT modules, keeping in mind the projected long life span of these devices?
4. **Research and development:** How can we foster innovation in our R&D department to develop unique hardware security features that offer robust protection against present and future threats?
5. **Customer education:** How can we educate our customers on the security features we use, developing trust into the security of the devices they use?

For more information or media inquiries, please contact:

Hoang Pham Van
IoT Analytics
+49 (0) 40 6391 1891
press(at)iot-analytics.com

For further reading please visit:

www.iot-analytics.com/research-blog

About IoT Analytics

IoT Analytics, founded and operating out of Germany, is a leading global provider of market insights and strategic business intelligence for the IoT, AI, Cloud, Edge, and Industry 4.0.
Our key workstreams across the tech stack include IoT applications, IoT platforms and software, IoT connectivity and hardware, and industrial IoT.
We are trusted by 1000+ leading companies around the world for our market insights, including globally leading software, telecommunications, consulting, semiconductor, and industrial players.

###