Submitted: 05/11/2024 Accepted: 20/12/2024 Published 23/12/2024

Low-Power ADCs for Secure AIoT Devices: Design and Implementation Challenges

Abstract:

In the rapidly evolving landscape of the Internet of Things (IoT), devices that rely on Artificial Intelligence (AI) have emerged as central components in a variety of applications. Security, energy efficiency, and processing capability are among the key aspects that determine the viability of these devices. Low-power Analog-to-Digital Converters (ADCs) play an essential role in ensuring the reliability and longevity of AIoT (Artificial Intelligence of Things) systems, where sensors and processors often operate in power-constrained environments. However, the integration of security features in low-power ADCs presents a complex challenge due to trade-offs between performance, power consumption, and security. This paper delves into the design and implementation challenges of low-power ADCs for secure AIoT devices. The discussion focuses on the unique requirements for low power consumption, enhanced security features, and efficient data conversion in AIoT systems. The work also explores various design methodologies and the constraints that influence the implementation of ADCs in this domain, offering insights into the state of the art and future research directions.

Keywords: Low-power ADCs, AIoT, Secure Devices, Design Challenges, Implementation, Security, Power Consumption, Analog-to-Digital Conversion

I. Introduction:

The AIoT represents a convergence of Artificial Intelligence and the Internet of Things, combining intelligent decision-making with connected, embedded devices. AIoT devices, which include everything from smart home devices to industrial sensors, require real-time data processing, often with limited energy budgets [1]. This makes the performance of Analog-to-Digital Converters (ADCs) particularly crucial, as ADCs are responsible for converting real-world analog signals, such as temperature, pressure, or light intensity, into digital data for processing. As AIoT devices are commonly deployed in environments where power availability is restricted, ensuring the low-power operation of ADCs is a primary consideration. However,

Submitted: 05/11/2024 Accepted: 20/12/2024 Published 23/12/2024

these devices must not only be power-efficient but also secure to mitigate the increasing risks of cyberattacks. This brings about the challenge of designing ADCs that can provide both energy efficiency and security, as both of these goals often demand conflicting design strategies. The demand for ADCs with lower power consumption has led to the exploration of various techniques for reducing power dissipation without compromising the accuracy or speed of the conversion. However, as security breaches in AIoT networks continue to escalate, the need to integrate secure features directly into ADCs has gained prominence. This presents challenges in terms of balancing power efficiency and robust security measures, such as encryption and tamper resistance. To address these challenges, design innovations are needed that incorporate low-power circuits, secure data paths, and enhanced resistance to side-channel attacks and other vulnerabilities [2].

Thus, the design of low-power ADCs for secure AIoT devices is a multifaceted problem, requiring engineers to balance conflicting demands while ensuring that the ADC can integrate seamlessly into the overall system architecture. This paper aims to discuss the major challenges in the design and implementation of such ADCs, highlighting how security concerns and power efficiency can be reconciled within the constraints of AIoT devices. AIoT systems typically comprise multiple interconnected devices that perform data collection, processing, and communication. As these systems handle vast amounts of sensitive information, such as health data or industrial monitoring data, security becomes an even more critical aspect of the ADC design. If the ADC’s output is compromised or intercepted, the entire system’s integrity could be at risk. Therefore, ensuring the privacy and security of the data in both the analog and digital domains is paramount. While the need for low-power consumption has driven the development of ADCs that work efficiently in power-constrained environments, security features such as encryption and error detection can increase the power load. This trade-off forces engineers to carefully design ADCs that meet both power and security goals. Addressing these challenges requires a deep understanding of the performance requirements of AIoT devices, alongside the limitations imposed by the power budgets of portable systems [3].

Thus, the design of ADCs for AIoT devices must consider a delicate balance between power, performance, and security. New research into hybrid architectures, such as low-power multi-bit and successive approximation register (SAR) ADCs, presents promising pathways to meet these

Submitted: 05/11/2024 Accepted: 20/12/2024 Published 23/12/2024

requirements. It is also crucial for system designers to account for the entire AIoT system's energy consumption, ensuring that each component, including the ADC, operates within a holistic energy-efficient framework. Additionally, security in the AIoT context goes beyond preventing unauthorized data access. It involves defending against attacks that could manipulate sensor data at the ADC level, such as signal manipulation or spoofing, which would lead to corrupted decision-making processes in AI systems. These unique challenges further complicate the design of secure and power-efficient ADCs, pushing the boundaries of current research in the field. Finally, an effective AIoT system must be scalable. As IoT devices become more widespread, ensuring that low-power ADCs are adaptable to various power budgets and security requirements is crucial [4]. There is no one-size-fits-all solution, and the design of secure low-power ADCs will need to evolve as AIoT systems scale in terms of both deployment and complexity. Therefore, this paper aims to investigate the challenges faced in creating ADCs that meet both power and security requirements for a wide range of applications.

II. Power Constraints in AIoT Devices:

Power consumption remains one of the most significant challenges in the development of AIoT devices. These devices are typically battery-powered or operate on limited energy sources, such as energy harvesting mechanisms, making power optimization a critical design criterion. ADCs, being a key component in data acquisition, must operate with minimal power consumption to extend the operational lifespan of AIoT devices. In most cases, the sensors integrated into AIoT devices require continuous or periodic sampling of analog signals, necessitating that the ADCs perform frequent conversions, which adds to the overall power load. In AIoT systems, the amount of data that needs to be processed, coupled with the frequency of sensor readings, places a significant demand on the ADC's performance [5]. Low-power ADCs must handle high-throughput data with minimal power dissipation to meet these demands. Achieving this balance requires innovations in ADC architectures and efficient design strategies that ensure ADCs can work in real-time while operating under the constraints of low power. One of the most common approaches is the use of low-voltage operation, where ADCs are designed to function at lower supply voltages, thus reducing the overall power dissipation. Additionally, power-saving modes, such as duty cycling, are often used to switch off parts of the ADC circuitry when not in use, minimizing the power draw during idle periods. Another technique is the use of simplified ADC architectures, such as flash ADCs or successive approximation register (SAR) ADCs, which inherently consume less power compared to more complex architectures like pipeline or delta-sigma ADCs.

Despite these efforts, power consumption remains a crucial trade-off, especially in AIoT systems where real-time processing and constant monitoring are required. The challenge lies in ensuring that these power-saving measures do not compromise the accuracy or speed of the data conversion, which are crucial for AI-driven applications. The implementation of low-power ADCs for AIoT systems requires careful consideration of the sampling rate, resolution, and power dissipation to ensure that the overall system performs optimally within the available power budget [6]. Furthermore, system designers must consider the power consumption of the entire sensor node, which often includes the sensor, ADC, microcontroller, communication interfaces, and other components. Energy-efficient ADCs alone will not solve the power problem; the entire system must be optimized to minimize energy consumption. This requires close collaboration between hardware and software components to ensure efficient power management strategies are applied at all levels. Another key consideration is the trade-off between resolution and power consumption. Higher-resolution ADCs consume more power due to the increased complexity in the conversion process. Therefore, finding the optimal resolution for a given application is crucial.

In some cases, the need for ultra-low power may limit the capabilities of the ADC itself, requiring compromise on resolution or speed. For example, AIoT devices used in environmental monitoring may not require high-speed data conversion, and designers can choose low-power ADCs with reduced speed and resolution [7]. However, for devices in fields such as healthcare or autonomous driving, the ADC must still deliver high performance while operating within power constraints. Finally, AIoT devices often need to function for extended periods, especially when deployed in remote areas or for continuous monitoring. This raises the need for ultra-low-power ADCs that can sustain long operation times without frequent battery replacements or recharging.

Submitted: 05/11/2024 Accepted: 20/12/2024 Published 23/12/2024

III. Security Threats to AIoT Devices:

As AIoT devices become more integrated into sensitive applications, the security of these devices has emerged as a major concern. These devices often handle sensitive data, such as health metrics, financial transactions, or industrial processes, making them attractive targets for malicious actors. Security vulnerabilities in the ADC stage can lead to the leakage of confidential data or enable attackers to manipulate the conversion process, potentially altering the output data in ways that undermine the security of the entire AIoT device [8]. One of the most significant threats to ADCs in AIoT devices is side-channel attacks, where an attacker exploits physical information leaks—such as timing, power consumption, or electromagnetic emissions—to infer secret information or manipulate the ADC's behavior. These attacks are particularly problematic because they do not rely on direct access to the digital data, making them difficult to detect and counter. Table given below highlights the common security threats to AIoT devices.

Security Threat	Description	Potential Impact	Countermeasures
Side-Channel Attacks	Attacks where physical information leaks (e.g., timing, power consumption, electromagnetic emissions) are exploited to extract sensitive data.	Exposure of private data, such as cryptographic keys or sensor readings.	Shielding, noise injection, power consumption monitoring, and implementing secure hardware designs.
Fault Injection Attacks	Attacks that inject faults into the device's circuitry (e.g., voltage spikes or environmental changes) to manipulate its behavior or outputs.	Corruption of data, unauthorized control over the device, or system crashes.	Fault detection and correction mechanisms, redundant components, tamper detection.
Physical Tampering	Attackers physically alter or manipulate the device's hardware to compromise its functionality.	Data corruption, loss of integrity, or unauthorized access.	Tamper-resistant enclosures, secure storage for keys, and physical security measures.
Eavesdropping	Unauthorized interception of data during transmission between the ADC and other system components.	Sensitive data, such as personal information or system parameters, could be exposed to unauthorized parties.	Encryption of data in transit, secure communication protocols (e.g., TLS/SSL), and key management.
Replay Attacks	Attacks where previously captured data or communications are retransmitted to deceive the system.	Unauthorized commands or actions based on old data, potentially affecting system decisions.	Use of timestamps, unique session identifiers, and non-repudiation mechanisms to detect anomalies.

Table 1: key security threats to AIoT devices

Submitted: 05/11/2024 Accepted: 20/12/2024 Published 23/12/2024

Another important security challenge is the susceptibility of ADCs to physical tampering. Attackers can physically modify the device or its environment, inducing faults in the ADC circuitry that can lead to incorrect or manipulated output. Such attacks, known as fault injection attacks, are increasingly becoming a concern in secure AIoT systems, particularly in critical applications such as autonomous vehicles or medical devices. These security threats necessitate the inclusion of robust countermeasures within the ADC design itself, such as error detection and correction mechanisms, encryption, and secure key management systems. Moreover, AIoT devices often have wireless communication capabilities, which can further expose them to security risks [9]. If the communication link between the ADC and other system components is not secure, attackers could intercept or modify the data being transmitted, leading to data corruption or unauthorized access to sensitive information. Encryption protocols are essential to secure the communication channel, but these protocols also add overhead and increase power consumption, presenting additional challenges for low-power ADC design.

The increased complexity of AIoT devices, often involving multiple sensors and interconnected systems, also introduces the risk of broader system vulnerabilities. A flaw in the ADC could provide an entry point for attackers to compromise the entire system, giving them control over the data acquisition process and potentially the broader network. The distributed nature of AIoT systems means that securing each individual component, including the ADC, is critical to preventing systemic vulnerabilities. Ensuring the security of low-power ADCs in AIoT devices requires a holistic approach, addressing potential attack vectors at both the hardware and software levels. Security measures must be implemented at the design stage, with built-in resilience to a wide range of attack types. This includes both passive measures, such as secure data storage, and active countermeasures, such as real-time detection of anomalies in the data conversion process.

IV. Security Features for Low-Power ADCs:

To mitigate the security threats faced by low-power ADCs in AIoT devices, several design strategies must be integrated into the ADC architecture. One of the most common approaches is the implementation of hardware-based encryption. Encrypting the data immediately after the ADC conversion helps ensure that sensitive information is protected as soon as it is digitized,

Submitted: 05/11/2024 Accepted: 20/12/2024 Published 23/12/2024

preventing exposure to unauthorized parties even if the data path is intercepted. Moreover, secure boot and secure key storage mechanisms are vital in ensuring that the ADC operates in a trusted environment. These mechanisms help protect the device from unauthorized firmware updates or alterations that could lead to vulnerabilities. Another critical security feature is the inclusion of tamper detection and response circuits within the ADC [10]. These circuits are designed to detect physical tampering, such as voltage fluctuations or environmental changes that could indicate an attempted attack. Upon detecting tampering, the ADC can trigger a response, such as erasing sensitive data or activating a self-destructive mode. Another important security feature is the inclusion of redundancy and error detection mechanisms in the ADC design. These mechanisms help identify and correct faults that could result from side-channel attacks or other security threats.

For instance, using multiple ADCs in parallel can allow for cross-validation of conversion results, making it more difficult for an attacker to introduce errors without detection. The implementation of these security features must be balanced with power consumption requirements to ensure that the overall system remains energy-efficient. In addition to hardware-based features, software-based security mechanisms can be employed to enhance the security of ADCs in AIoT devices. For example, cryptographic algorithms can be applied to ensure that the data captured by the ADC is securely transmitted to the processing unit. Error detection protocols, such as checksums or cyclic redundancy checks (CRC), can also be used to ensure data integrity during transmission. By applying these techniques, the system can guarantee that the converted data is both accurate and secure.

Moreover, monitoring the operating environment of AIoT devices can help mitigate certain security risks. For instance, sensors that detect environmental changes such as temperature or pressure could be integrated with the ADC to identify physical tampering attempts. Similarly, the inclusion of motion sensors and accelerometers could help detect if the device has been moved or altered, further enhancing the device's security posture. Some recent advancements in the field focus on integrating machine learning techniques directly into the ADC to detect anomalies in real-time [11]. By using AI algorithms to monitor the performance of the ADC and flag potential security breaches, the system can adapt to evolving threats and respond in real-time to safeguard the data being converted.

V. Balancing Power and Security:

One of the most significant challenges in the design of low-power ADCs for secure AIoT devices is balancing the conflicting requirements of low power and robust security. Security features, such as encryption, error detection, and tamper resistance, often add extra overhead, increasing power consumption and potentially compromising the energy efficiency of the device. This creates a fundamental trade-off between maintaining low power consumption for prolonged operation and providing sufficient security to safeguard against attacks. To address this challenge, designers must prioritize security features based on the threat model and the specific requirements of the application. For instance, devices that handle critical or sensitive data may require more robust encryption and error detection, whereas lower-security applications might allow for more relaxed security measures, resulting in lower power consumption. Furthermore, innovative ADC architectures, such as those that implement power-saving modes during idle periods, can help reduce overall power consumption without sacrificing performance. Dynamic power management is another approach that can help balance power and security requirements. By dynamically adjusting the power usage of the ADC based on real-time conditions or workload, the device can optimize power consumption while ensuring that security features are still in place when needed. For instance, during periods of low activity, the ADC could enter a low-power mode that disables non-essential security features, such as encryption or error detection, until the device returns to an active state.

Designers can also explore hybrid solutions, such as integrating separate low-power modes and secure processing units, which can be activated as needed based on the current system demands. This approach would allow the ADC to operate with minimal power under normal conditions, but when higher security is required, the system could switch to a more secure mode that consumes more power. Additionally, intelligent systems that dynamically adjust security protocols, based on environmental risk assessments, could help provide enhanced security while reducing unnecessary power consumption. To further address the power-security trade-off, researchers are exploring alternative ADC architectures, such as approximate computing techniques, which allow for reduced accuracy in certain circumstances without compromising overall system performance. By tolerating small inaccuracies in the conversion process, these techniques can reduce the power consumption of the ADC, while still maintaining an acceptable level of security.

Lastly, collaboration between hardware designers and software engineers is essential to achieve an optimal balance between power and security. Software techniques, such as secure communication protocols and lightweight cryptography, can supplement the hardware-based security features of the ADC, ensuring that power consumption remains low while still safeguarding sensitive data. These hybrid solutions are likely to become increasingly important as AIoT devices evolve and are deployed in more complex and demanding environments.

VI. Future Directions in ADC Design for Secure AIoT Devices:

The design of low-power ADCs for secure AIoT devices is a rapidly evolving field, driven by the increasing demand for intelligent, interconnected devices and the growing need for enhanced security in these devices. Future research is expected to explore new ADC architectures that integrate more advanced power-saving techniques without sacrificing security. Additionally, the integration of emerging technologies, such as quantum computing and advanced cryptography, could significantly impact the design of secure ADCs for AIoT systems. One promising direction involves the development of energy-efficient ADCs that can adapt to varying operational conditions, such as fluctuating power availability or changing security requirements [12]. These adaptive ADCs would be able to dynamically adjust their power consumption based on the specific task at hand, ensuring that security measures are always in place when needed while minimizing power consumption during periods of low activity.

Another key area of research is the development of novel algorithms for anomaly detection and real-time threat mitigation. AI-based systems could be employed to continuously monitor the operation of ADCs, detecting any deviations from normal behavior that might indicate a security breach. This could involve using machine learning models to detect patterns in the data or identify side-channel leaks, enabling the system to respond to threats proactively. Furthermore, integrating low-power, secure ADCs with emerging communication protocols, such as 5G or low-power wide-area networks (LPWAN), will be critical for enabling the next generation of AIoT systems. These communication networks will provide more bandwidth and lower latency,

Submitted: 05/11/2024 Accepted: 20/12/2024 Published 23/12/2024

allowing for more sophisticated data collection and processing while still meeting the stringent power and security requirements of AIoT devices.

In addition to the hardware advancements, software solutions will continue to play a vital role in securing AIoT devices. Lightweight cryptographic algorithms and secure data storage mechanisms will be essential for ensuring that ADCs can operate securely without consuming excessive power. As software and hardware co-evolve, it is likely that new system-level architectures will emerge that integrate both power-efficient and secure processing, communication, and storage solutions. The miniaturization of AIoT devices and the continued push for reduced energy consumption are also likely to drive further innovations in ADC design. As sensors and microprocessors become smaller and more energy-efficient, ADCs will need to scale accordingly, ensuring that their power consumption remains within acceptable limits without compromising functionality or security.

VII. Conclusion:

The design and implementation of low-power, secure ADCs for AIoT devices present significant challenges, balancing the need for low power consumption with the increasing demands for security. As AIoT devices become more pervasive in sensitive applications, ensuring that ADCs can securely convert analog data while maintaining low power consumption is paramount. This requires novel design approaches, integrating power-efficient architectures with robust security measures to protect against various types of cyberattacks. Future research directions will focus on the development of adaptive ADCs, novel anomaly detection techniques, and the integration of emerging technologies such as quantum computing and advanced cryptography. Achieving a balance between power and security will be critical in the continued evolution of AIoT systems, enabling them to function efficiently and securely in a wide range of applications.

REFERENCES:

[1] T. Andrulis, R. Chen, H.-S. Lee, J. S. Emer, and V. Sze, "Modeling analog-digital-converter energy and area for compute-in-memory accelerator design," *arXiv preprint arXiv:2404.06553,* 2024.

Submitted: 05/11/2024 Accepted: 20/12/2024 Published 23/12/2024

[2] M. Alioto, "Aggressive design reuse for ubiquitous zero-trust edge security—From physical design to machine-learning-based hardware patching," *IEEE Open Journal of the Solid-State Circuits Society,* vol. 3, pp. 1-16, 2022.

[3] R. Chen, "Analog-to-Digital Converters for Secure and Emerging AIoT Applications," Massachusetts Institute of Technology, 2023.

[4] A. Alzuhair and A. Alghaihab, "The design and optimization of an acoustic and ambient sensing AIoT platform for agricultural applications," *Sensors,* vol. 23, no. 14, p. 6262, 2023.

[5] R. Chen, H. Kung, A. Chandrakasan, and H.-S. Lee, "A bit-level sparsity-aware SAR ADC with direct hybrid encoding for signed expressions for AIoT applications," in *Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design*, 2022, pp. 1-6.

[6] E. H. Fort *et al.*, "Wireless and low-power system for synchronous and real-time structural-damage assessment," *IEEE Sensors Journal,* vol. 23, no. 12, pp. 13648-13658, 2023.

[7] F. Graf, T. Watteyne, and M. Villnow, "Monitoring performance metrics in low-power wireless systems," *ICT Express,* 2024.

[8] Y.-C. Hsu and R. C.-H. Chang, "Intelligent chips and technologies for AIoT era," in *2020 IEEE Asian Solid-State Circuits Conference (A-SSCC)*, 2020: IEEE, pp. 1-4.

[9] C.-J. Jhang, C.-X. Xue, J.-M. Hung, F.-C. Chang, and M.-F. Chang, "Challenges and trends of SRAM-based computing-in-memory for AI edge devices," *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol. 68, no. 5, pp. 1773-1786, 2021.

[10] R. Jian *et al.*, "Ambient IoT: Insight and Challenge of Enabling Technologies for Future Study," in *2024 6th International Conference on Electronics and Communication, Network and Computer Technology (ECNCT)*, 2024: IEEE, pp. 451-458.

[11] E. Nemlaha, P. Střelec, T. Horák, S. Kováč, and P. Tanuška, "Suitability of MQTT and REST communication protocols for AIoT or IIoT devices based on ESP32 S3," in *Proceedings of the Computational Methods in Systems and Software*: Springer, 2022, pp. 225-233.

[12] S. Tabrizchi, S. Angizi, and A. Roohi, "TizBin: A low-power image sensor with event and object detection using efficient processing-in-pixel schemes," in *2022 IEEE 40th International Conference on Computer Design (ICCD)*, 2022: IEEE, pp. 770-777.