A Systematic Hardware Solution for GDPR Compliance

Yi-Chun Yang , Ren-Song Tsay
Logos Lab, Department of Computer Science, National Tsing Hua University, Taiwan

***Abstract*—The increasing deployment of Internet of Things (IoT) devices presents significant challenges for compliance with the General Data Protection Regulation (GDPR) due to their inherent privacy concerns and often opaque operational nature. This paper introduces GDPR-Guard, a novel and systematic hardware-based solution embedded within IoT devices to ensure GDPR compliance. By shifting control from enterprises to users through a transparent "glass box" approach, GDPR-Guard enhances accountability and transparency by auditing the entire device lifecycle from manufacturing. This paper details the architecture and functionality of the GDPR-Guard hardware component, its integration into the device manufacturing process under supervisory authority (SA) oversight, and its mechanisms for enforcing consent-based access control and generating tamper-proof audit records. A proof-of-concept implementation and security/performance evaluations demonstrate the feasibility and effectiveness of GDPR-Guard as a systematic hardware solution for achieving GDPR compliance in IoT networks.**

Keywords—Access control, accountability, data ownership, data privacy, GDPR, IoT, hardware security.

I. INTRODUCTION (*HEADING 1*)

The General Data Protection Regulation (GDPR) [1] aims to protect user privacy by regulating the collection and processing of personal data. However, the widespread adoption of IoT devices has amplified privacy concerns [2], making technical compliance a significant challenge. Traditional centralized, cloud-based IoT frameworks often operate as opaque "closed box" systems, potentially enabling data collection without explicit user consent and hindering reliable investigations by supervisory authorities (SAs) [3, 4, 5, 6]. While recent blockchain-based solutions have addressed some transparency issues at the transaction level, they often overlook the control enterprises retain over user devices [7, 8].

To overcome these limitations, this paper proposes a novel "glass box" solution centered around a secure hardware component called GDPR-Guard, which is embedded within each IoT device during manufacturing. This approach systematically addresses GDPR compliance from the hardware level by transferring device control to the data subject (DS), enhancing transparency through lifecycle-wide auditing, and ensuring accountability via tamper-proof records. The SA plays a crucial role in overseeing the manufacturing process to ensure the secure integration and trustworthiness of the GDPR-Guard. This paper focuses on the hardware design principles and functionalities of the GDPR-Guard as a foundational element for systematic GDPR compliance in IoT environments.

II. RELATED WORK

Existing approaches to GDPR compliance in IoT often rely on software-based mechanisms within proprietary cloud frameworks [3, 4, 5, 6]. These centralized systems have been criticized for their lack of transparency and potential for unauthorized data access. Blockchain-based solutions have emerged to enhance transparency and auditability by recording data subject consents on a distributed ledger [7, 8]. However, these solutions primarily focus on transaction-level activities and do not fully address the "closed box" nature of the IoT devices themselves, which remain under enterprise control. This leaves vulnerabilities for unauthorized modifications and off-chain data processing activities to go unrecorded.

Unlike these prior efforts, our work proposes a systematic hardware-centric approach with the GDPR-Guard embedded in the device. This ensures transparency and security from the device's inception, starting with the manufacturing process, which is a critical aspect often neglected by existing solutions. By focusing on a hardware root of trust for GDPR compliance, we aim to provide a more robust and auditable solution compared to purely software-based or transaction-focused blockchain approaches.

III. GDPR-GUARD HARDWARE DESIGN AND ARCHITECTURE

The GDPR-Guard is envisioned as a trusted and SA-certified security guard embedded within the hardware of each IoT device. Its core function is to shield personal data at its source, securely manage cryptographic keys, enforce owner-defined access permissions, and generate tamper-proof audit records to ensure GDPR compliance and accountability.

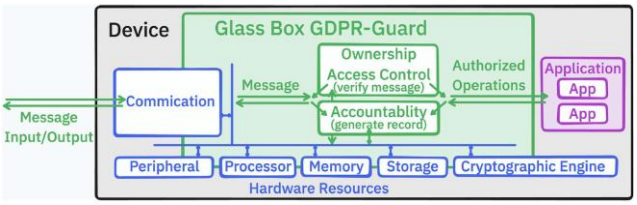

Fig. 1: The embedded GDPR-Guard within the target device permits only owner authorized accesses and approved operations, and cryptographically logs all events.

As depicted in Fig. 1, the GDPR-Guard acts as a gatekeeper, controlling all hardware resources including storage, communication interfaces, and peripherals. Key aspects of its hardware design and architecture include:

- Secure Storage: The GDPR-Guard incorporates a secure element for the tamper-proof storage of cryptographic keys, including the device's unique private key and the initial Device Owner's (DO) public key. This secure storage is crucial for maintaining device identity and ensuring that only authorized operations can be invoked.
- Cryptographic Engine: A dedicated cryptographic engine within the GDPR-Guard handles asymmetric and symmetric cryptographic operations, including digital signature generation and verification, as well as data encryption and decryption. This hardware acceleration enhances security and performance.
- Access Control Logic: The GDPR-Guard enforces fine-grained access control using usage tickets (U-Tickets) issued by the data owner (DO) and return tickets (R-Tickets) generated by the device. This U/R-Ticket pair ensures a closed

access loop. To prevent ticket reuse, each ticket includes a sequentially incremented identifier. Additionally, a challenge-response authentication mechanism is employed to validate the ticket holder. This hardware-enforced access control guarantees that data processors (DPs) can only access data or perform actions explicitly authorized by the data subject (DS) acting as the DO.

- Tamper-Proof Logging: All critical authorization processes—including device manufacturing, application deployment, ownership transfer, and consent-based data access—are recorded as tamper-proof logs, digitally signed using the device's private key. These logs are attached to the R-Ticket, providing an auditable and verifiable history of the device's lifecycle for supervisory authorities (SAs).

- Secure Boot and Attestation: To ensure the integrity of the GDPR-Guard itself, the hardware design incorporates secure boot mechanisms that verify the authenticity of the boot code and operating environment. Furthermore, the GDPR-Guard supports remote attestation, allowing new owners or the SA to verify the device's integrity and authenticity.

IV. SYSTEMATIC GDPR COMPLIANCE THROUGH GDPR-GUARD

The integration of the GDPR-Guard into the device manufacturing process, overseen by the SA, provides a systematic foundation for GDPR compliance. This process includes:

- Certified Hardware Manufacture: The SA ensures that the device manufacturer (DM) integrates a certified and trusted GDPR-Guard into each device. The architecture and security protocols of the GDPR-Guard are disclosed, verified, and certified by the SA through attestation methods.

- Controlled Application Deployment: Application deployments are authorized through digitally signed "Deployment U-Tickets," limiting enterprise control and preventing unauthorized application installations or updates. The GDPR-Guard acts as a gatekeeper, ensuring that only authorized applications can operate on the device.

- Reliable Ownership Transfer: Upon sale, the device manufacturer (DM) or current device owner issues a digitally signed Ownership Transfer U-Ticket to the new data owner (DO), transferring control of the device and its data. Once the ticket is validated, the GDPR-Guard securely stores the new DO's public key, replacing the previous owner's key. This process establishes the new DO as the sole authority over the device.

- Consent-Based Data Access: Data processors (DPs) must obtain explicit consent from the DS (acting as the DO) before accessing personal data. This consent is formalized through a "Data Collection U-Ticket" issued by the DO. The GDPR-Guard enforces this consent, allowing access only within the specified scope and generating tamper-proof records of the data access.

- Lifecycle Auditing: The GDPR-Guard maintains a comprehensive audit trail of all access and operation events throughout the device's lifecycle, using digital signatures to ensure non-repudiation. U-Tickets authorize specific events, while the corresponding R-Tickets capture tamper-proof records of those events. These records can be securely stored and made available for SA investigations, promoting accountability and transparency.

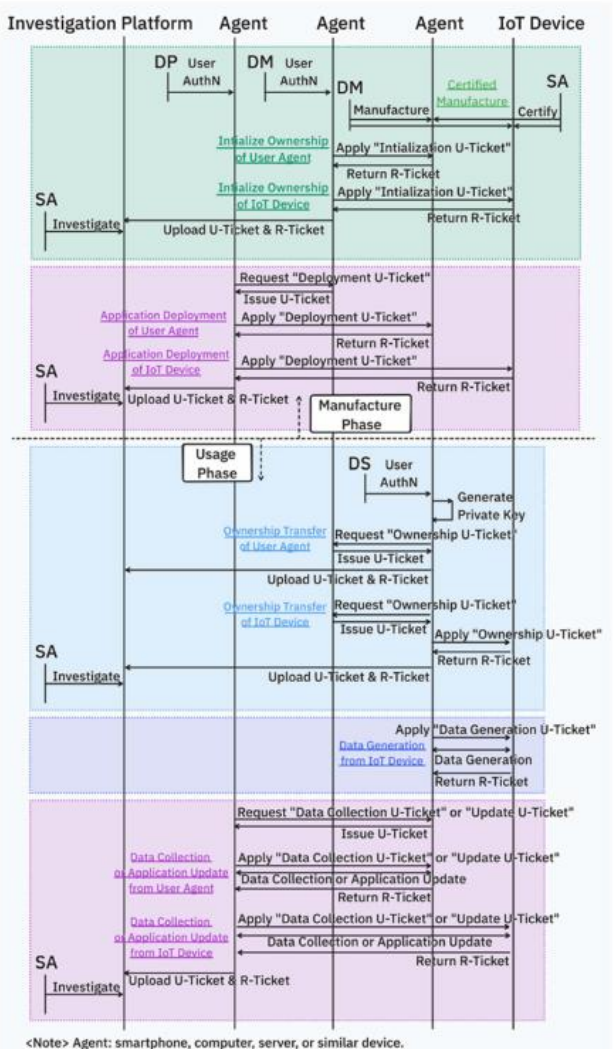

Fig. 2: The proposed GDPR-Guard access control and auditing protocols across the entire device lifecycle.

Fig. 2 illustrates the proposed access control and auditing protocol enabled by the GDPR-Guard hardware, which enforces a closed-loop accountability mechanism. The DO issues U-Tickets to grant specific access rights, while the device generates R-Tickets to confirm the execution of authorized operations. These digitally signed tickets provide irrefutable evidence of consent and data processing activities.

V. IMPLEMENTATION AND EVALUATION

A proof-of-concept implementation of the GDPR-Guard was developed using Raspberry Pi 4 Model B boards [9], simulating resource-constrained IoT devices. The secure storage requirement is less than 500 bytes, and the U/R-Tickets, formatted in JSON, are each under 1 KB in size. This prototype demonstrated the feasibility of embedding the core functionalities of the GDPR-Guard within a hardware-constrained environment.

We conducted thorough security evaluations based on the STRIDE threat model and successfully demonstrated that the GDPR-Guard mitigates various threats—including counterfeit devices, malicious updates, unauthorized access, and data tampering—through hardware isolation, secure storage, secure boot, and ticket-based access control mechanisms.

Bluetooth Classic was adopted for ticket and data communication to evaluate the solution's applicability in off-internet scenarios and its suitability for typical IoT environments. Performance evaluations showed that the GDPR-Guard introduces minimal overhead: access control operations, including cryptographic key handling and digital signature computation, added approximately 32 milliseconds, while encrypted data retrieval incurred only a 6-millisecond delay. These results indicate that the GDPR-Guard delivers strong security and GDPR compliance with negligible impact on the performance of resource-constrained IoT devices.

VI. DISCUSSION

The GDPR-Guard offers a systematic hardware solution to address the challenges of GDPR compliance in IoT networks by embedding trust and control directly into the device hardware. This approach contrasts with software-centric and transaction-level solutions by providing a hardware root of trust for data protection and auditability across the entire device lifecycle.

The requirement for SA oversight during manufacturing ensures the initial trustworthiness of the GDPR-Guard. The ticket-based access control mechanism empowers data subjects with fine-grained control over their data, aligning with GDPR principles of data ownership and consent. The tamper-proof audit logs generated by the GDPR-Guard facilitate reliable GDPR investigations, enhancing accountability for both data controllers and processors.

Furthermore, the GDPR-Guard's ability to function offline offers a significant advantage for resource-constrained IoT devices in environments with limited or no internet connectivity. The decoupling of access control and record submission makes it a practical and scalable solution for diverse IoT deployments.

Future work includes exploring the implementation of GDPR-Guard on a dedicated hardware security module to enhance security, as well as developing a more concrete framework for hardware certification by supervisory authorities (SAs).

VII. CONCLUSION

This paper has presented GDPR-Guard, a systematic hardware-based solution designed to ensure GDPR compliance in IoT networks. By embedding a trusted security guard within the device hardware and involving the supervisory authority in the manufacturing process, GDPR-Guard shifts control to users, enhances transparency, and provides tamper-proof auditability throughout the device lifecycle. The proof-of-concept implementation and evaluations demonstrate the feasibility and minimal performance overhead of this approach. We believe that GDPR-Guard represents a significant step towards establishing a more trustworthy and GDPR-compliant IoT ecosystem.

REFERENCES

[1] Voigt, Paul, and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)." A practical guide, 1st ed., Cham: Springer International Publishing 10.3152676 (2017): 10-5555.

[2] Alwarafy, Abdulmalik, et al. "A survey on security and privacy issues in edge-computing-assisted internet of things." IEEE Internet of Things Journal 8.6 (2020): 4004-4022.

[3] Politou, Eugenia, Efthimios Alepis, and Constantinos Patsakis. "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions." Journal of cybersecurity 4.1 (2018): tyy001.

[4] Houser, Kimberly A., and W. Gregory Voss. "Gdpr: The end of google and facebook or a new paradigm in data privacy?." Rich. JL & Tech. 25 (2018): 1.

[5] Ammar, Mahmoud, Giovanni Russello, and Bruno Crispo. "Internet of Things: A survey on the security of IoT frameworks." Journal of information security and Applications 38 (2018): 8-27.

[6] Indu, I., PM Rubesh Anand, and Vidhyacharan Bhaskar. "Identity and access management in cloud environment: Mechanisms and challenges." Engineering science and technology, an international journal 21.4 (2018): 574-588.

[7] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." 2015 IEEE security and privacy workshops. IEEE, 2015.

[8] Truong, Nguyen Binh, et al. "GDPR-compliant personal data management: A blockchain-based solution." IEEE Transactions on Information Forensics and Security 15 (2019): 1746-1761.

[9] " Raspberry Pi 4 model B," 2019. [Online]. Available: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/