Poster:
Towards a Digital Payment System for the Constrained Internet of Things

Mikolai Gütschow
TU Dresden
mikolai.guetschow@tu-dresden.de

Matthias Wählisch
TU Dresden and Barkhausen Institut
m.waehlisch@tu-dresden.de

***Abstract*—In this poster, we start the discussion of the potentials and challenges of digital payment systems to advance digital services in the Internet of Things. We specifically focus on devices with constrained hardware resources. To enable multi-stakeholder machine-to-machine scenarios, we propose an e-cash approach that is privacy-friendly and allows for autonomous payment. We implement our approach using GNU Taler, a free-software e-cash implementation, and RIOT, a free and open-source operating system for the IoT. Our preliminary findings suggest that the deployment of e-cash systems is feasible in constrained IoT scenarios. They underscore the importance of concise, standard-compliant data encoding over computationally intensive compression techniques.**

1. Introduction

The Internet of Things (IoT) is projected to consist of 30 billion interconnected devices by 2030 [1]. Most of them will be constrained in terms of hardware resources to reduce manufacturing costs, enabling mass deployment of many different new applications. In principle, each of these IoT devices provides a service (*e.g.,* sensing data, acting to external input), often in multi-stakeholder environments in which not all stakeholders necessarily collaborate in a peer-to-peer manner. How to seamlessly offer advanced services in such networks is still an open topic.

Providing an economic incentive could be one reason for cooperation. To enable, for example, data sharing between different stakeholders then requires *autonomous machine-to-machine (M2M) payments* such that the payment is integrated with and running directly on the (constrained) IoT devices, keeping the overhead of accounting and payment processing low. Additionally, such an IoT payment system must prioritize *(meta-)data privacy protection* due to the sensitivity and scale of data involved.

In this poster, we propose payments in the IoT based on blind signatures and a centralized architecture. Such a token-based approach allows for payer privacy and enables autonomous usage by design, thereby meeting two fundamental requirements. Section 2 gives some examples of payment scenarios and typical constraints in the IoT, and shows that other approaches to digital payments do not fit the IoT use-case well. Section 3 discusses the required functionality to participate as a constrained device in such a system, elaborates on design choices for data transmission formats, and briefly evaluates the proposed design using a proof-of-concept implementation of GNU Taler on RIOT. Section 4 concludes the poster by presenting challenges left for future work.

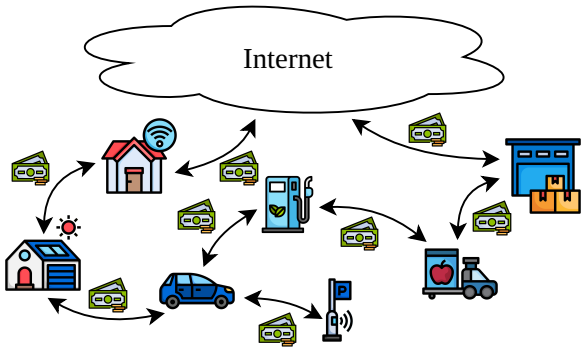

Figure 1: A distributed IoT economy needs autonomous and privacy-respecting machine-to-machine payments.

2. Background and Problem Statement

This section discusses some common IoT scenarios depicted in Figure 1, how these scenarios benefit from IoT-integrated payments, and the requirements and challenges imposed by limited hardware resources. We also analyze currently available or proposed digital payment systems.

IoT Scenarios. The vision of the Internet of Things (IoT) revolves around the seamless cooperation of interconnected devices, operating autonomously without direct human intervention. These devices exchange data or, more generally, services, often involving sensitive information regarding privacy. For instance, smart household appliances such as refrigerators can autonomously order supplies. Industry scenarios may involve the cooperation of many entities, for example, when goods are tracked from manufacturing to warehouse until hand-over to the end-customer, including automatic ordering of new supplies. Similarly, vehicles can autonomously handle payments for parking, tolls, and fuel, benefiting both autonomous and conventional car users. Furthermore, smart grid energy trading relies on IoT devices to coordinate local electricity sharing among buildings equipped with renewable energy sources, ensuring efficient energy management within communities. Even scenarios involving human intervention, such as pay-as-you-go public transportation, can benefit from compact and cheap IoT-based wallets which improve the user experience.

TABLE 1: Comparison of digital payment approaches.

Features	Approach		
	Traditional	Crypto-currencies	Our: E-Cash
Autonomy	✘	✓	✓
Privacy	✘	pseudonymity	payer
Resources	•	••••	••

IoT Payment Requirements. The provision of services (*e.g.,* data sharing) among diverse stakeholders based on an economic incentive model requires economic remuneration. While subscription models suit static scenarios, they fall short in dynamic environments in which IoT devices interact only sporadically. Autonomous machine-to-machine payment might offer a solution by enabling billing and transactions without human intervention. However, concerns about privacy arise due to possible payment observations by third parties, either directly [2] or through metadata analysis [3]. Ensuring payment privacy becomes crucial in scenarios lacking mutual trust among devices. Having an openly standardized privacy-preserving payment system at hand would also counteract monopolies and discriminatory treatment against devices of a certain owner or manufacturer, and allows for true competition and interoperability across devices.

IoT Device Constraints. In scenarios requiring large-scale deployments at minimal cost, devices are typically selected to precisely match the use-case, resulting in a significant number of highly constrained devices. These devices face severe limitations in available memory, including RAM, ROM, and persistent mass storage, which impacts system design in terms of storage requirements and processing overhead. Several IoT scenarios also involve off-the-grid deployments and battery-powered devices, which require the use of low-power wireless networking protocols with small packet sizes and low data rates. A universal IoT payment system must account for these constraints, minimizing storage, processing, and transmission requirements to ensure compatibility with low-end devices.

Payment Options for the IoT. Traditional payment systems, such as credit card payments, bank transfers, and third-party payment providers, are widely utilized by the public for in-store and online transactions. These systems rely on centralized databases storing the account balances, allowing transactions to be initiated through simple means like NFC interactions. However, authentication mechanisms typically require human confirmation, hindering autonomous payments. [4] Moreover, access to the central databases compromises transaction privacy, violating payment privacy requirements. On the other hand, cryptocurrencies offer digital payment alternatives with their decentralized design, seemingly suitable for IoT scenarios. Yet, their reliance on resource-intensive consensus mechanisms and transaction confirmation delays pose challenges. Verifying transactions independently is unfeasible for constrained IoT devices using such approaches. [5] Furthermore, while cryptocurrencies offer pseudonymity, transaction traceability and potential account identity associations remain concerns.

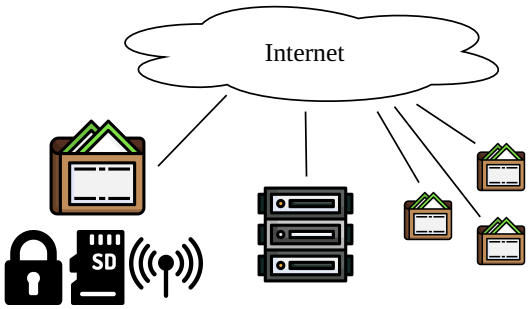

Figure 2: Architecture of an e-cash payment system: Participating devices ( ) need to perform cryptographic operations, store tokens, and communicate with a central service provider ( ) over the Internet.

Our approach: E-Cash. A third approach to digital payments, based on the e-cash scheme pioneered by Chaum [6], offers cash-like anonymity for payers through blind signatures of tokens by a central authority. Each token, signed and backed by a certain value held by the central authority, can be redeemed once by a payee for an authorized payment. Utilizing tokens instead of identity-bound accounts facilitates autonomous operation and hinders transaction linkability. However, the self-custody aspect of e-cash schemes entails token storage requirements for the users, a crucial consideration for deployment on resource-constrained IoT devices. The original design proposed by Chaum could not give unlinkable change and thus had linear complexity for variable amounts. Dold [7] solved this critical issue, allowing for logarithmic complexity in GNU Taler.

Table 1 summarizes our comparison of traditional payment systems, cryptocurrencies, and e-cash concerning the essential requirements identified for the IoT. To the best of our knowledge, this poster represents the first exploration of integrating an e-cash-based payment system with the constrained IoT.

3. Design and Implementation

Design Aspects. Figure 2 shows a typical e-cash system consisting of two basic components: a central *provider*, which issues blind signatures on cryptographic tokens, and *users*, which hold these tokens in self-custody. IoT devices operate as users. Therefore, they need to support three basic functions: (*i*) cryptographic operations such as blinding and signature verification, (*ii*) the storage of signed tokens and metadata, and (*iii*) the communication with the provider via the Internet. We propose to build the payment system integration on top of an IoT operating system with a universal API, abstracting hardware details such as hardware-based cryptographic acceleration, storage, and physical-layer protocols. This approach enables a hardware-agnostic implementation for diverse IoT devices, promoting reusability across deployments.

Currently, our focus has been on efficient data formats for the transmission protocol. In the IoT, reducing packet sizes is crucial because (*i*) low data rates and small Maximum Transfer Units (MTUs) are prevalent in the IoT,

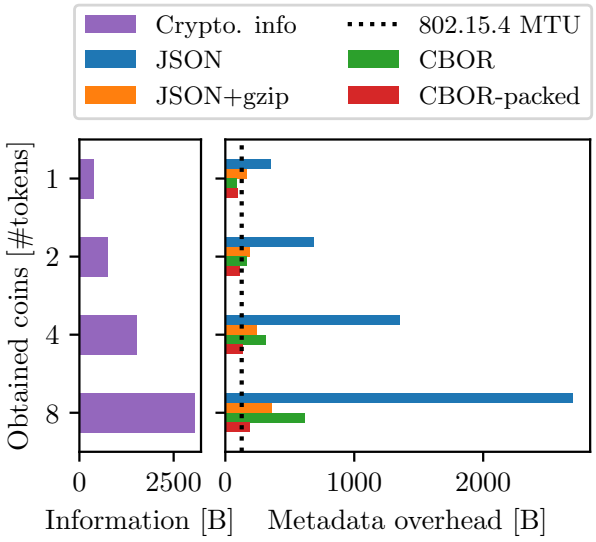

Figure 3: GNU Taler withdraw request payload sizes composed of cryptographic information (left) and metadata overhead depending on the encoding (right): Packed CBOR achieves the smallest format overhead, still fitting one 802.15.4 MTU of 127B for a withdrawal of up to 4 tokens, while avoiding the additional, computationally-intensive compression step of JSON+gzip.

and because (*ii*) fragmentation may lead to additional delay [8]. While the encoding of cryptographic data such as tokens and signatures cannot be reduced below their information content, the accompanying metadata may contain redundant information. Human-readable formats such as JSON or XML may be effective for the broader Internet, where they can be compressed efficiently with methods such as gzip or brotli. Compression, however, introduces complexity on end devices, leading to larger code sizes, higher energy consumption, and additional computation time—all of these characteristics conflict with low-end-device constraints. Introducing a custom binary format containing only the raw cryptographic data in a predefined order is not an option either since it challenges debugging, protocol updates, and forward compatibility. To balance resources and flexibility, we advocate for using CBOR [9], a concise binary data format standardized by the IETF. CBOR efficiently accommodates metadata alongside the data and provides streaming capabilities. Packed CBOR [10], an extension of CBOR, further enhances this efficiency by minimizing metadata redundancy through optimized encoding of repeated information.

Implementation and Evaluation. To evaluate our proposal, we have picked GNU Taler, a free and open-source digital payment system implementing a logarithmic e-cash scheme [7], and RIOT, an free and open-source operating system for the constrained IoT, which provides support for over 270 IoT platforms [11]. Compared to other operating systems, RIOT offers a standardized API for cryptographic operations that can flexibly make use of hardware acceleration and secure key storage where available [12]. The Taler APIs[1] are specified as HTTP-based RESTful protocols using JSON as a data format, with cryptographic data encoded in base32. Figure 3 compares the payload lengths for Taler withdrawal requests encoded in various formats, including JSON, compressed JSON, CBOR, and packed CBOR. Regardless of the number of digital coins acquired, packed CBOR encoding consistently outperforms other schemes, exhibiting approximately half the relative overhead compared to compressed JSON encoding.

1. https://docs.taler.net/core

4. Conclusion and Outlook

In this abstract, we argued that the IoT will benefit from autonomous and privacy-friendly payments as a common service. Our approach, unlike prior work, suggests a centralized system architecture inspired by the e-cash model. We introduced design choices of our proof-of-concept, which suggest that digital payment is doable even if memory and CPU are constrained. We proposed an efficient standard-compliant data encoding for the communication between user and provider. Future work should focus on token storage efficiency and user-friendly provisioning of IoT devices with digital coins.

References

[1] L. S. Vailshery, "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030," Jul. 2023. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[2] J. Lauer, "Plastic surveillance: Payment cards and the history of transactional data, 1888 to present," *Big Data & Society*, vol. 7, no. 1, pp. 1–14, Jan. 2020.

[3] Y.-A. De Montjoye, L. Radaelli, V. K. Singh, and A. S. Pentland, "Unique in the shopping mall: On the reidentifiability of credit card metadata," *Science*, vol. 347, no. 6221, pp. 536–539, Jan. 2015.

[4] M. N. M. Bhutta, S. Bhattia, M. A. Alojail, K. Nisar, Y. Cao, S. A. Chaudhry, and Z. Sun, "Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS)," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–10, Jan. 2022.

[5] S. Mercan, A. Kurt, K. Akkaya, and E. Erdin, "Cryptocurrency Solutions to Enable Micropayments in Consumer IoT," *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 97–103, Mar. 2022.

[6] D. Chaum, "Blind Signatures for Untraceable Payments," in *Advances in Cryptology*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Boston, MA: Springer US, 1983, pp. 199–203.

[7] Florian Dold, "The GNU Taler System: Practical and Provably Secure Electronic Payments," Ph.D. dissertation, Université de Rennes, Rennes, France, Feb. 2019. [Online]. Available: https://taler.net/papers/thesis-dold-phd-2019.pdf

[8] M. S. Lenders, T. C. Schmidt, and M. Wählisch, "Fragment Forwarding in Lossy Networks," *IEEE Access*, vol. 9, pp. 143 969–143 987, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3121557

[9] C. Bormann and P. E. Hoffman, "Concise Binary Object Representation (CBOR)," Internet Engineering Task Force, Request for Comments RFC 8949, Dec. 2020.

[10] C. Bormann and M. Gütschow, "Packed CBOR," Internet Engineering Task Force, Internet Draft draft-ietf-cbor-packed-12, Mar. 2024. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-cbor-packed

[11] E. Baccelli, C. Gundogan, O. Hahm, P. Kietzmann, M. S. Lenders, H. Petersen, K. Schleiser, T. C. Schmidt, and M. Wählisch, "RIOT: An Open Source Operating System for Low-End Embedded Devices in the IoT," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4428–4440, Dec. 2018.

[12] L. Boeckmann, P. Kietzmann, L. Lanzieri, T. C. Schmidt, and M. Wählisch, "Usable Security for an IoT OS: Integrating the Zoo of Embedded Crypto Components Below a Common API," *Proc. of 19th International Conference on Embedded Wireless Systems and Networks (EWSN)*, pp. 84–95, 2022.