Exploration of Thermoelectric Energy Harvesting for Secure, TLS-Based Industrial IoT Nodes

Frederik Lauer(✉), Maximilian Schöffel, Carl C. Rheinländer, and Norbert Wehn

Department of Electrical and Computer Engineering, Microelectronic Systems Design Research Group, Technische Universität Kaiserslautern,
67663 Kaiserslautern, Germany
flauer@eit.uni-kl.de

Abstract. Security is one of the biggest challenges, particularly in the Industrial IoT and in critical infrastructures. Complex cryptographic computations are in contrast to the low energy budget of the devices, especially when independence from the power grid is required, as it is the case with retrofitted sensor nodes. Energy harvesting offers a promising alternative but tightens the energy constraints of the application further.

In this work, we investigate how IoT edge devices can be powered by thermal energy harvesting and concurrently meet the stringent TLS-based security requirements. We analyze a thermoelectric generator system at its lowest power output region and evaluate different energy storage technologies in a representative IoT architecture. Our results show that temperature gradients as low as 1 K are sufficient to enable secure connections every 20 min in a representative IIoT application.

1 Introduction

The Industrial Internet of Things (IIoT) is one of the most promising strategies towards more advanced, efficient, and interconnected industrial infrastructures. However, it also increases the risks of potential attacks and data leaks. While this is already a critical problem for the confidentiality of industrial secrets, it can lead to even more serious, unpredictable consequences for IIoT applications in critical infrastructure like cooling systems in power plants [11]. Therefore, communication security is one of the key requirements in IIoT, especially in the environment of critical infrastructure. To ensure this security cryptographic protocols such as Transport Layer Security (TLS) have been designed. TLS is one of the most established security protocols in the field of IP-based communication for years and is constantly being improved. By combining the benefits of multiple cryptographic algorithms, TLS protects communication against eavesdropping, message forgery, and tampering [3]. With quantum computers on the horizon and their potential to break conventional cryptographic techniques, algorithms that are resistant to attacks by future large quantum computers (post-quantum cryptography) [22,23,25] have even recently been incorporated into TLS. However,

B. Tekinerdogan et al. (Eds.): ICIOT 2022, LNCS 13735, pp. 92–107, 2023.
https://doi.org/10.1007/978-3-031-23585-1_7

the cryptographic computations for both post-quantum and conventional cryptography are known to be computationally complex and thus energy-intensive. In many areas, such as predictive maintenance or process monitoring in industrial plants, where sensors need to be retrofitted, the available energy is limited. Installing cables and creating an appropriate power domain is time-consuming and expensive, and batteries often do not provide the required runtime or must be replaced regularly.

Energy harvesting offers a promising alternative. Solar-powered wireless sensor nodes have already been shown to be a valid and sustainable alternative. However, the use of solar cells severely restricts the operating environment to locations with sufficient light conditions. This applies particularly to the area of predictive maintenance, where sensors often need to be retrofitted within process plants or machines.

Thermoelectric generators (TEGs) that convert a temperature gradient into electrical energy are a possible alternative. However, due to their intrinsic thermal connectivity and the absence of active cooling, only low-temperature gradients can be expected, resulting in only a low energy yield. But the resulting low power output contradicts the energy requirements of the secure data connection that is an indispensable requirement in the industrial environment.

Therefore, in this paper, we investigate the extent to which IIoT edge devices powered by TEGs are able to provide the high-security confidence of TLS-based communication.

The key contributions of this paper are:

1. A study of a TEG-based energy harvesting system and different energy storage technologies with the focus on low-temperature gradient
2. A detailed analysis of the strong interrelation between energy storage technologies as a function of thermoelectric energy harvesting and secure IIoT applications in a representative ULP, wireless system architecture
3. A quantitative evaluation of the energy-producing temperature gradient as a function of the number of secure TLS connections per time using classical and post-quantum cryptographic algorithms

The paper is structured as follows: After discussing related work, Sect. 3 and 4 describe the system setup and the performance analysis of the system modules respectively. Section 5 concludes the results and scientific contributions, followed by a brief discussion of our future work in this field.

2 Related Work and Background

The following section provides an overview of related work in the area of secure, ultra-low power (ULP) wireless IoT edge devices and thermoelectric energy harvesters as well as energy storage technologies.

2.1 ULP Secure Wireless IoT Edge Devices

Due to the ever-growing number of IoT devices, security inevitably plays a crucial role [29]. IoT botnets such as Mira or Hide'n'Seek already demonstrated the potential danger of hacked devices several years ago. However, in the IIoT area, even eavesdropping on potentially sensitive data via the network connection poses a considerable security risk [21]. Wireless data transmission is already a major problem for IoT edge devices with very low energy budgets. Additionally, computationally intensive cryptographic calculations are an even greater challenge [8]. Therefore, several implementations of lightweight security protocols for wireless data transmission have been developed in related work. But, these protocols do not achieve the same level of trust as the widely used standard Transport Layer Security (TLS). However, Lauer et al. [10] showed that by performing holistic system analysis and the usage of an off-the-shelf hardware accelerator, an end-to-end TLS-secured wireless connection can be established over Bluetooth Low Energy (BLE) with an energy cost of about 14 mJ per connection establishment. Schoeffel et al. [22,23] have shown that algorithms, which are currently considered post-quantum safe have similar energy requirements in a comparable system setup.

2.2 Thermoelectric Energy Harvesting

The term energy harvesting describes the process of converting energy from environmental sources into usable electrical energy. Commonly used energy sources are light (photoelectric effect), kinetic energy, chemical energy, radio frequencies, and thermal energy [5]. The conversion of thermal energy into electrical energy is done by a so-called thermoelectric generator (TEG) which is based on the Seebeck effect. This effect describes the phenomenon in which a voltage difference is created by the temperature difference between two different electrical conductors/semiconductors. This voltage difference, which is usually in the range of millivolts, is then converted into a voltage that can be utilized by embedded devices using dedicated boost converters. Both the structure and the materials of the TEG [7,16,24] as well as the structure of the booster circuit and its adaptation to the TEG [6,18,19] have a considerable influence on the efficiency of the system. Therefore, off-the-shelf modules consisting of TEGs and booster circuits that are precisely matched and tuned for a specific application range are available [14]. In the past, small-scale thermoelectric energy harvesting has been presented to supply wearable sensor devices [12,13] and IoT applications [9,26,27].

However, to the best of our knowledge, there is no work that considers the energy overheads for security-relevant, i.e., encryption and authentication operations of wireless IoT applications in the context of thermoelectric energy harvesting.

2.3 Energy Storage for Thermoelectric Energy Harvester

The output power of small TEGs is mostly insufficient to directly power a microcontroller with an active radio, especially at low-temperature gradients. Therefore, the energy is typically initially collected in a storage element until enough energy is available to operate the unit for a specified time [4,28]. The type of storage element is strongly application specific. Thus, size, capacity, lifetime, leakage current, pulse-current capability, and cost are only a few of the decisive factors [4]. Typically, either small rechargeable batteries or supercapacitors are used.

3 Setup

In this section, we describe the setup of our IoT system including energy harvesting and storage technologies as well as the measurement setup that provides us with the relevant data presented in Sect. 4.

3.1 ULP Secure IoT Application

The setup of the IoT system is very similar to the one used in [10]. It consists of an edge device forming an MQTT (Message Queuing Telemetry Transport) client, a Gateway, and an MQTT Broker running on a standard PC. The specialty of this system is the approach to use IPv6 throughout the system and therefore to use the gateway only as a physical bridge (transparent gateway). This is made possible by the usage of Bluetooth Low Energy (BLE) and the 6LoWPAN standard between the edge device and the gateway. Thus, classic TLS can be used as a security layer, which ensures end-to-end encryption between the edge device and the server. This system, which is based on well-known standards has already been proven in several publications to be extremely energy-efficient and, thanks to the clearly structured protocol stack, to offer great flexibility.

The hardware of the edge device is similar to the one used in [10]. An nRF52840 System on Chip (SoC) from Nordic Semiconductor with built-in BLE radio forms the core and the integrated hardware accelerator (CryptoCell) is used to efficiently speed up the cryptographic calculations. On the software side, the RIOT operating system [20] and its default Generic Network Stack (GNRC) are used. As a TLS library, mbedTLS [15] has been used, for establishing secure connections and a simple MQTT client implementation as the application layer.

TLS as a security layer supports different encryption and authentication methods that vary in computational complexity. In order to demonstrate this influence, three different authenticated key exchanges, including recently standardized Post-Quantum Cryptography (PQC) have been used:

- ECDHE-ECDSA
- Kyber512-ECDSA
- Kyber512-Dilithium2

The required energy and the resulting current profile were measured with a DMM7510 precision digital multimeter by Keithley.

3.2 Energy Harvesting Module

For our system, we chose a class-leading, off-the-shelf energy harvesting module called Prometheus from Matrix Industries [14]. The compact module consists of a TEG (MATRIX Gemini) and an energy-harvesting boost converter (MATRIX Mercury).

In the targeted use case, only small temperature gradients can be expected, mainly due to the fact that the environmental temperature will be close to the temperature that the industrial appliances, that are to be monitored, emit. Thus, with regard to the expected temperature gradient, we have a similar problem as with environmental IoT sensors where the temperatures of all objects adapt to the ambient temperature in the long term [17].

As the datasheet of the Prometheus module does not precisely state the possible output power for temperature gradients below five Kelvin, a detailed analysis has been conducted in this work.

3.3 Energy Storage Technologies

Based on our analyses, the IoT application will draw pulse currents during wireless transfer operations that cannot be supplied by the harvesting system. Furthermore, at low-temperature gradients, the harvester's output power will not even be capable of supplying the RMS current. As a solution, an energy storage is scheduled between harvester and application. This way, the harvested energy can be accumulated over time and deliver enough power to the IoT application to conduct a complete connection phase. However, the capacity of the energy storage device must be precisely matched to the application. It must be high enough to power the device during the lowest power incomes from the harvester, and low enough to quickly reach the minimum operation voltage even with little charge energy. This is particularly essential in systems with extended periods without active energy harvesting by the harvester.

There are many popular storage technologies that differ in capacity, energy and power density, cost, and losses by leakage and aging. Electrochemical storage technologies like Li-Ion batteries are well known for high energy densities, but in return also for suffering from aging effects after experiencing many charge and discharge cycles. As the targeted IoT system will experience many charge and discharge cycles, such storage technologies have not been included in this work. Instead, capacitors and solid-state batteries have been explored as they have higher endurance than conventional electrochemical batteries. However, in contrast to Li-Ion batteries, conventional capacitors usually come with a relatively high leakage current, which leads to unwanted energy losses. Therefore the use of supercapacitors is often preferred, as they are optimized to have a higher energy density and low leakage currents, similar to solid-state batteries that usually have even higher energy densities and lower leakage currents. In return, both usually come with a relatively high internal resistance, which causes the voltage to drop significantly at high current pulses. Due to this issue, a significant amount of accumulated energy cannot be exploited by the system. Because as soon as the residual energy drops to the value where the voltage falls below the minimum load operating voltage during a pulse current, the system will end up in a loop of power-on resets.

Obviously, the mentioned issues lead to a trade-off between energy storage capacity, leakage losses, and pulse current ability in order to define the best-fitting storage technology for the targeted IoT system. Therefore, an evaluation has been conducted in this work that includes the following energy storage technologies:

- **Multi Layer Ceramic Capacitor (MLCC):** This capacitor consists of a ceramic material that serves as a dielectric and is capable of delivering high peak currents. Usually, the capacitance of a single capacitor is limited to a few tens to hundreds of microfarads, which is why several capacitors must be connected in parallel if larger capacitances are required. In our case, we used twenty MLCCs by Taiyo Yuden, of 220 µF each, connected in parallel for a total of 4.4 mF.
- **Supercapacitor:** The capacitance density of supercapacitors is significantly larger than that of most other capacitors. For our setup, we use a 100 mF supercapacitor by Eaton (KR-5R5V104).
- **CeraCharge$^{\mathrm{TM}}$:** CeraCharge$^{\mathrm{TM}}$ is a solid-state SMD battery by TDK. Its capacity is around 200 mF at a maximum voltage of 1.8 V. The leakage currents to be expected are extremely low, but high peak currents are not possible due to the high internal resistance. An advantage over capacitors is the non-linear curve in terms of voltage and discharge capacity, which means that theoretically more usable energy is available until the voltage drops below a certain point. However, in our experiments, 440 µF had to be added in parallel to the CeraCharge$^{\mathrm{TM}}$ in order to compensate for the high peak currents and to prevent large voltage drops. Since our system runs with a maximum voltage of 3.6 V we connected two CeraCharge$^{\mathrm{TM}}$ cells in series.

4 Analysis and Results

In this section, we present the results structured in the requirements of the application, the energy harvested by the energy harvesting system, and the investigation of different energy buffers and their trade-offs. Finally, this is summarized by the total view in the system context.

4.1 ULP Secure IoT Application

The application on the edge device consists of the following functional sections:

- start-up of the microcontroller (1)
- establishment of a BLE connection to the gateway (2)
- execution of the TLS handshake with the MQTT server, including the cryptographic calculations (3)
- transmission of 100 bytes of user data (4)

Figure 1 shows the current profile of such a connection with the current peaks for the active radio, at a supply voltage of 3.6 V, divided into the different functional areas.

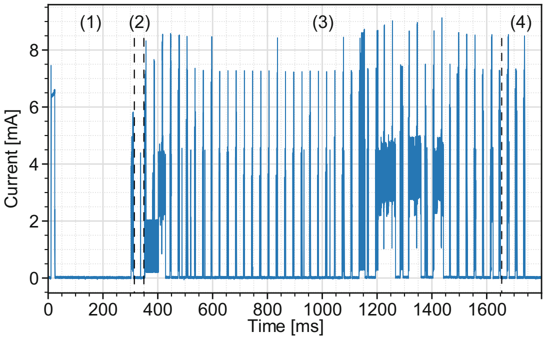

Fig. 1. Current profile of a complete connection

Table 1. Energy and time requirements of different key exchange methods (mean values of 10 measurements)

Key exchange method	Energy [mJ]	Time [s]
ECDHE-ECDSA	5.90	1.71
KYBER512-ECDSA	6.44	2.18
KYBER512-DILITHIUM2	17.98	6.51

In Table 1 the average duration and energy requirement of a complete connection, broken down by the different key exchange methods used, is listed. Based on [10,23], we selected the following key establishment methods for investigation:

- **ECDHE-ECDSA**, which represents the conventional state-of-the-art solution based on elliptic curves.
- **KYBER512-ECDSA**, which deploys the freshly standardized post-quantum key encapsulation method, signed by conventional elliptic curve cryptography.
- **KYBER512-DILITHIUM2**, thus establishing a fully post-quantum secure connection based on KYBER [1] and DILITHIUM [2].

4.2 Energy Harvesting Module

In order to analyze the performance of the Prometheus module, both sides of the TEG element had been equipped with tiny temperature sensors. The measurements have been conducted in the temperature area where the sensors are characterized with their best accuracy. As shown in Fig. 2, the temperature of

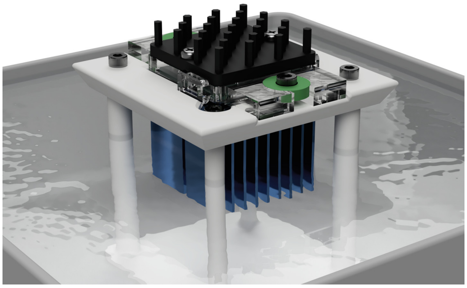

Fig. 2. Test set-up for evaluation of the TEG module

the warm side has been controlled with a heating water bath, whereas the cold side was exposed to the environmental temperature with the deployed heat sink.

As shown in Fig. 3, the thermal conductivity of a TEG causes both sides to heat up even if only one side has been exposed to hot water. The intensity of how much the cold side is heated up by the warm side depends on the material of the TEG, i.e., its thermal conductivity, the characteristics of the heat sink, and the environmental temperature.

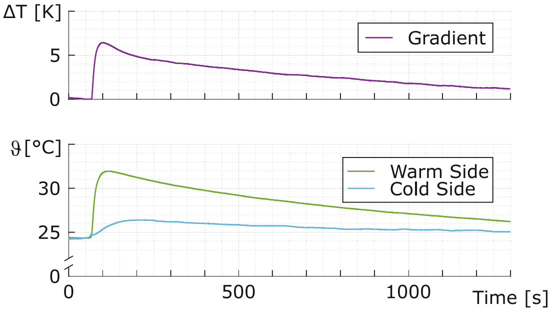

Fig. 3. Thermal impulse response of the employed TEG module

As unfavorable conditions, e.g., small heat sinks and relatively high environmental temperatures can be expected in industrial environments, the system design must be optimized to operate under these conditions. Therefore, the performance of the TEG module has been analyzed for the maximum output power in the lower temperature gradient range. By carefully controlling the water bath temperature, temperature gradients in 0.1 K-steps have been generated and the output power was measured with different loads. The analysis revealed that the maximum power point tracking (MPPT) inside the module is properly working down to a gradient of about 0.5 K. The results are shown in Fig. 4.

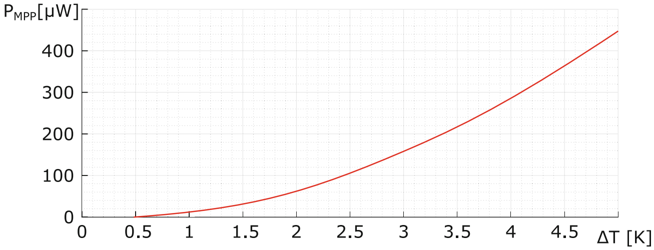

Fig. 4. Maximum output power of the TEG module

4.3 Energy Storage Technologies

In order to illustrate the voltage curve of the different energy storage technologies, the respective discharge profiles are captured without a harvesting system connected. Therefore, the storage units were charged to 3.6 V in order to supply the IoT application. A minimum operating voltage V_{min} for the presented IoT application of 1.8 V was defined, which is derived from the minimum operating voltage specified in the datasheet of the employed BLE SoC plus a headroom of 100 mV. For the sake of simplicity, we choose a high duty cycle of the IoT application for this analysis with a new connection every 10 s. This way the losses through leakage will be low and can be neglected for the calculation, but at the same time, a good statement can be made about the usable energy in the buffer.

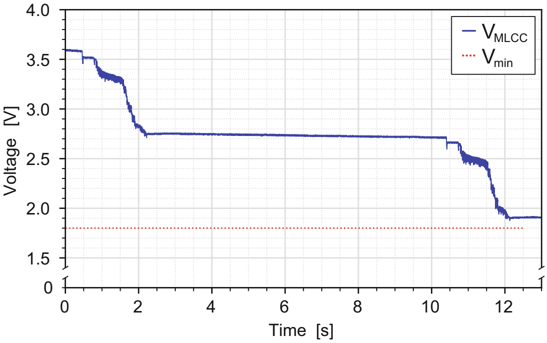

Fig. 5. Discharge curve of the MLCC; new connection every 10 s

Figure 5 shows the discharge curve of the MLCC, whose capacitance of 4.4 mF is sufficient for 2 complete connections. It is noticeable that due to the low internal resistance, there are practically no voltage drops caused by the peak currents, but only a linear drop in relation to the energy drawn. This means that the energy stored in the MLCC can be used very efficiently up to the defined minimum operation voltage of 1.8 V.

With its capacity of 100 mF, the supercapacitor was able to supply the energy for 83 successful connections. As shown in Fig. 6, the high peak currents cause

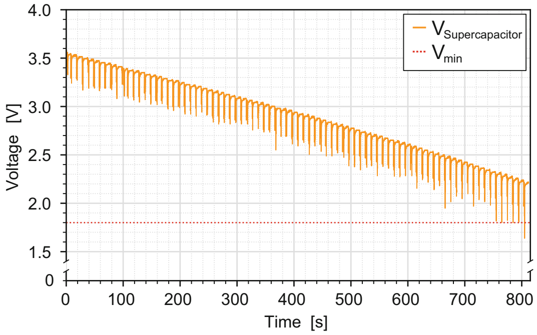

Fig. 6. Discharge curve of the supercapacitor; new connection every 10 s

voltage drops that increase significantly with decreasing storage voltage to almost 0.6 V at a remaining storage voltage of 2.2 V. This means that the supercapacitor can only reliably supply the application down to a remaining open loop voltage of 2.2 V, compared to the MLCC, which can be used down to 1.8 V.

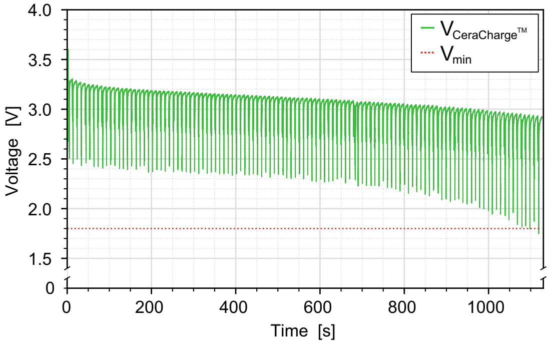

Fig. 7. Discharge curve of the CeraCharge^{TM}; new connection every 10 s

Compared to the supercapacitor, the CeraCharge^{TM} has an even higher internal resistance and was not able to supply the peak currents required in our setup on its own. Therefore, two 220 µF MLCCs were connected in parallel to slightly absorb the peak currents. This allowed the CeraCharge^{TM} to successfully power 113 connections in our setup before the voltage drops below 1.8 V by a remaining open loop voltage of 2.9 V. Figure 7 shows the voltage curve, which is not linear to the consumed energy, as well as the increasingly stronger voltage drops with decreasing remaining voltage.

The different minimum open loop voltages of 1.8 V for the MLCC, 2.2 V and 2.9 V for the CeraCharge^{TM} show that the storage technologies with relatively high internal resistance suffer significantly from the pulse currents of the IoT application. As a result, less of the available energy in the storage can be exploited. Based on the energy of the fully charged storage device and the residual energy at the point of the determined minimum open-circuit voltage, the maximum theoretically usable energy of the storage technology, E_{usable}, can be calculated as follows:

$$E_{usable} = E_{chg} - E_{res} = 0.5 * C * ((3{,}6V)^2 - V_{OLmin}^2) \quad (1)$$

where E_{chg} is the stored energy of the respective buffer at the point where it is fully charged to 3.6 V and E_{res} is the residual energy in the buffer at the point where the minimum voltage under load condition can be guaranteed. V_{OLmin} is the respective open loop voltage at this point. Regarding the MLCC, this reveals that about 75% of the stored energy is usable by the IoT application. As far as the supercapacitor is concerned, about 55% are usable. The CeraCharge reaches a rate of approximately 51% of usable energy, whereby it must be noted that, as previously mentioned, a 440 µF MLCC had to be connected in parallel for this. This value for the CeraCharge^{TM} is only an approximate value because the usable capacity strongly depends on the quantity and duration of the load. As shown above, the IoT system load consists of many different current pulses, which makes it almost impossible to theoretically determine the exact usable capacity. Furthermore, the open-circuit voltage of the CeraCharge^{TM} dropped significantly after applying the load for the first time, which makes it more difficult to compare to other storage technologies.

Another very decisive parameter of the various storage technologies is the leakage current. This is dependent on a variety of parameters. While the design of the storage unit and the materials used certainly have a major influence, parameters like for instance the ambient temperature, age, cycle count and installation parameters can also have a significant impact. In our case, we used the values from the data sheets as a rough guideline for comparison. Therefore the values we have applied for subsequent calculations are 2 µA per MLCC (i.e. 40 µA for the twenty MLCCs connected in parallel), 0.6 µA for the supercapacitor and 0.1 µA for the CeraCharge^{TM}. For the CeraCharge^{TM}, however, the leakage of the two MLCCs connected in parallel must also be taken into account, which increases the leakage to 4.1 µA in our case. Figure 8 shows the results for the different storage technologies deployed in this study.

For a qualitative comparison of the storage technologies in general Fig. 9 illustrates the different typical characteristics. All axes are arranged in such a way that the preferred path points outwards, e.g., low costs, high endurance, and high pulse current capability. The values only serve as a rough classification of the storage technologies and show the general advantages and disadvantages. MLCCs are ideal for absorbing large current peaks, have exceptional endurance, and can even be charged with large currents. The supercapacitors, on the other hand, are a good compromise in many areas with the advantage of their low cost in relation to capacity and their very high endurance. The outstanding features of the CeraCharge^{TM} are the extremely low leakage current and the comparably high density. But in return, the CeraCharge^{TM} is not capable of handling large pulse currents. In addition, the handling of the CeraCharge^{TM} is more complex due to specific characteristics such as limited charge current.

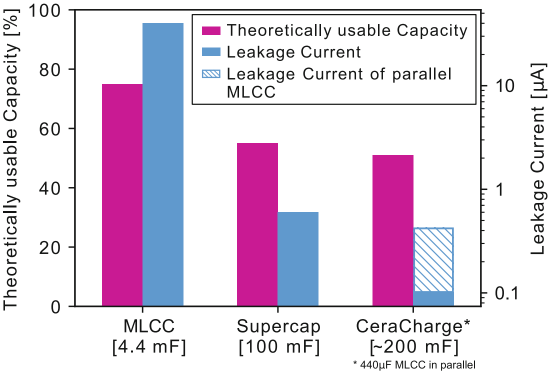

Fig. 8. Comparison of the different storage technologies with respect to the theoretically usable capacity and the leakage current

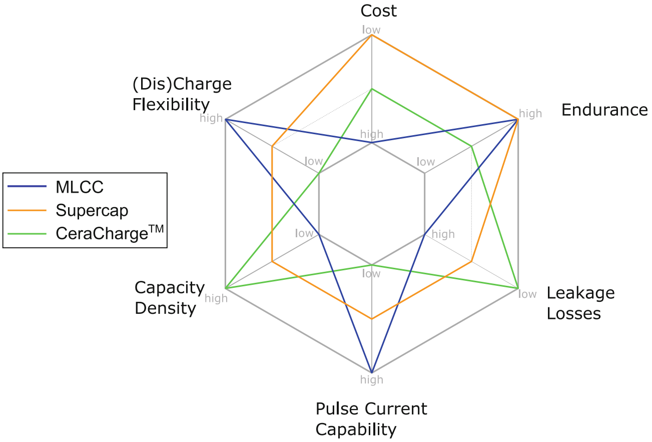

Fig. 9. Overview of the properties of the different energy storage technologies

4.4 Entire IoT System

This section combines the previous analyses and results to the context of the overall system and presents a simplified final structure of the system setup.

Figure 10 shows the minimum time required to generate the energy for one connection as a function of the temperature gradient at the TEG, taking also the leakage of the respective storage technologies into account. The graphs thus indicate a lower bound at which the charge of the energy storage technologies remains constant over a long period of time. The dots at the right-hand end of the graphs indicate the minimum temperature gradient to overcome the leakage of energy storage technologies. Due to the very similar energy requirements of ECDHE and the post quantum-safe KYBER512, the curves are almost congruent. The post-quantum secure signature method DILITHIUM2 has a significantly greater influence due to the large keys and signatures which strongly increases the amount of data being exchanged between client and server. The results clearly indicate the influence of the leakage current of the individual storage technologies. For example, in order to generate the energy for establishing a connection in 20 min, a temperature gradient of 3 K is required when using MLCCs, whereas a temperature gradient of only 1 K is required when using a supercapacitor.

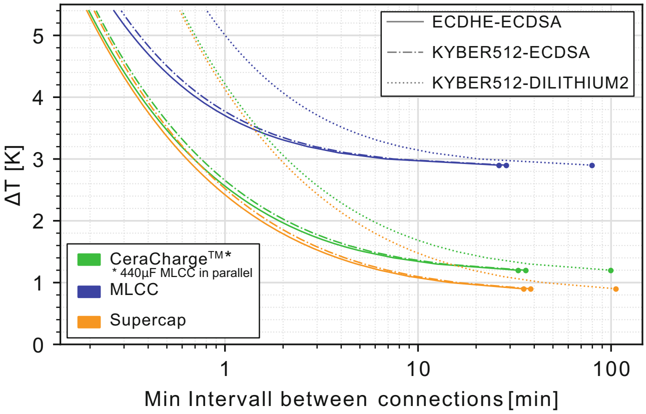

Fig. 10. Temperature gradient vs. minimal time between connections

In order to ensure reliable functionality of the system, a start-up circuit is required in addition to the three main components, the thermoelectric harvester module, the energy storage, and the actual IoT application (Fig. 11).

This circuit ensures that the application is not powered until the energy storage has reached a minimum voltage level. Whereby the minimum voltage level consists of the minimum operating voltage V_{min} as described in Sect. 4.3, i.e., the respective open loop voltage at the minimum operating voltage under load conditions. Plus a specific headroom V_{hr}, which is the energy buffer-specific voltage that the buffer will drop by after heaving supplied one connection just before reaching V_{min}.

To prevent a power-on reset oscillation of the IoT application, the circuit switches off when the minimum operating voltage is undershot once and only switches back on when 3.6 V is reached again.

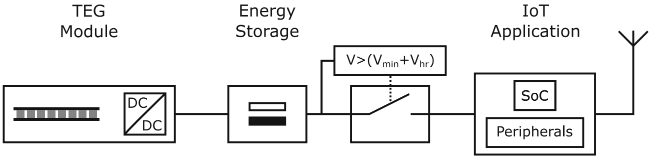

Fig. 11. Simplified circuitry of the final energy harvesting-powered IoT system

5 Conclusion

In this paper, we analyzed how IIoT devices can be powered by TEGs and concurrently provide the high security of TLS-based communication. One of the main challenges was to obtain sufficient energy for the computationally intense cryptographic algorithms even at low-temperature gradients. Due to the resulting low power output we employed and evaluated different storage technologies and how their characteristics affect the overall system performance. Our key insights are:

1. The characteristics of the applied energy storage devices have a significant influence on the overall performance of the system. Thus, the high peak currents required by the application cause more than 40% of the capacity to remain unused in storage units with higher internal resistance. Furthermore, promising solid-state batteries most likely require additional capacitors which in return substantially contradicts their additional advantages of low leakage currents.
2. The minimum temperature gradient at which a secure connection can be established at all strongly depends on the employed energy storage technologies.
3. Even a low-temperature gradient of 1 K is sufficient to establish a secure connection based on conventional cryptography every 20 min in a representative IIoT setup. A temperature gradient of 1.2 K even allows a post-quantum-safe connection at the same connection interval.

6 Future Work

The CeraCharge^{TM} is a promising energy buffer technology due to its high capacity and low leakage. As discussed above, the internal resistance of the CeraCharge^{TM} made an additional MLCC capacitor inevitable in order to reliably supply the peak loads of the IoT application. But, appended MLCC capacitance directly leads to increasing leakage losses. Thus, engaging these only in the lower voltage ranges where they become relevant, has a promising potential to increase the theoretically usable capacity of the CeraCharge^{TM} without increasing the continuous leakage losses. Therefore, determining the proper constellation of a high capacity/low leakage buffer and a low capacity/low internal resistance buffer together with the proper engagement of the latter to the former is the subject of our current research.

Acknowledgement. This paper was partly founded by the German Federal Ministry of Education and Research as part of the project “SIKRIN-KRYPTOV” (16KIS1069).

References

1. Roberto, A., Bos, J., Ducas, L., et al.: CRYSTALS-KYBER: Algorithm Specifications and Supporting Documentation (2021). https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf. Accessed 11 Feb 2022

2. Bai, S., et al.: CRYSTALS-Dilithium – Algorithm Specifications and Supporting Documentation (Version 3.1). https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf. Accessed 30 Jan 2022
3. Dierks, T., Rescorla, E.: The transport layer security (TLS) protocol version 1.2 (2008). https://tools.ietf.org/html/rfc5246. Accessed 24 Feb 2022
4. Elahi, H., Munir, K., Eugeni, M., Atek, S., Gaudenzi, P.: Energy harvesting towards self-powered IoT devices. Energies **13**(21), 5528 (2020). https://www.mdpi.com/1996-1073/13/21/5528
5. Enescu, D.: Thermoelectric energy harvesting: basic principles and applications. In: Enescu, D. (ed.) Green Energy Advances. IntechOpen, February 2019
6. Gruber, J.M., Mathis, S.: P3.6 - efficient boost converter for thermoelectric energy harvesting. In: Proceedings Sensor 2017, Wunstorf, Nürnberg, Germany, pp. 642–645. AMA Service GmbH (2017). http://www.ama-science.org/doi/10.5162/sensor2017/P3.6
7. Haras, M., et al.: Thermoelectric energy conversion: how good can silicon be? Mater. Lett. **157**, 193–196 (2015). https://linkinghub.elsevier.com/retrieve/pii/S0167577X15007235
8. Hellaoui, H., Koudil, M., Bouabdallah, A.: Energy-efficient mechanisms in security of the Internet of Things: a survey. Comput. Netw. **127**, 173–189 (2017). https://linkinghub.elsevier.com/retrieve/pii/S1389128617303146
9. Kim Tuoi, T.T., Van Toan, N., Ono, T.: Heat storage thermoelectric generator for wireless IOT sensing systems. In: 2021 21st International Conference on Solid-State Sensors, Actuators and Microsystems (Transducers), Orlando, FL, USA, pp. 924–927. IEEE, June 2021. https://ieeexplore.ieee.org/document/9495686/
10. Lauer, F., Rheinlander, C.C., Kestel, C., Wehn, N.: Analysis and optimization of TLS-based security mechanisms for low power IoT systems. In: 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID), Melbourne, Australia, pp. 775–780. IEEE, May 2020. https://ieeexplore.ieee.org/document/9139743/
11. Mades, J., Ebelt, G., Janjic, B., Lauer, F., Rheinlander, C.C., Wehn, N.: TLS-level security for low power industrial IoT network infrastructures. In: 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, pp. 1720–1721. IEEE, March 2020. https://ieeexplore.ieee.org/document/9116285/
12. Magno, M., Boyle, D.: Wearable energy harvesting: from body to battery. In: 2017 12th International Conference on Design & Technology of Integrated Systems In Nanoscale Era (DTIS), Palma de Mallorca, Spain, pp. 1–6. IEEE, April 2017. http://ieeexplore.ieee.org/document/7930169/
13. Magno, M., Wang, X., Eggimann, M., Cavigelli, L., Benini, L.: InfiniWolf: energy efficient smart bracelet for edge computing with dual source energy harvesting. In: 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, pp. 342–345. IEEE, March 2020
14. Matrix - prometheus. https://www.matrixindustries.com/prometheus
15. Mbed TLS. https://github.com/Mbed-TLS/mbedtls
16. Minnich, A.J., Dresselhaus, M.S., Ren, Z.F., Chen, G.: Bulk nanostructured thermoelectric materials: current research and future prospects. Energy Environ. Sci. **2**(5), 466 (2009). http://xlink.rsc.org/?DOI=b822664b
17. Paterova, T., Prauzek, M., Konecny, J., Bancik, K.: Thermoelectric generator powering study for an environmental-monitoring IoT device based on very low temperature differences. In: 2022 26th International Conference Electronics, Palanga, Lithuania, pp. 1–6. IEEE, June 2022

18. Pham, V.K.: A high-efficient power converter for thermoelectric energy harvesting. In: 2020 5th International Conference on Green Technology and Sustainable Development (GTSD), Ho Chi Minh City, Vietnam, pp. 82–87. IEEE, November 2020. https://ieeexplore.ieee.org/document/9303126/
19. Ramadass, Y.K., Chandrakasan, A.P.: A batteryless thermoelectric energy-harvesting interface circuit with 35mV startup voltage. In: 2010 IEEE International Solid-State Circuits Conference - (ISSCC), San Francisco, CA, USA, pp. 486–487. IEEE, February 2010. http://ieeexplore.ieee.org/document/5433835/
20. Riot operating system. https://www.riot-os.org
21. Sadeghi, A.R., Wachsmann, C., Waidner, M.: Security and privacy challenges in industrial Internet of Things. In: Proceedings of the 52nd Annual Design Automation Conference, San Francisco California, pp. 1–6. ACM, June 2015. https://doi.org/10.1145/2744769.2747942
22. Schöffel, M., Lauer, F., Rheinländer, C.C., Wehn, N.: On the energy costs of post-quantum KEMs in TLS-based low-power secure IoT. In: Proceedings of the International Conference on Internet-of-Things Design and Implementation, Charlottesvle, VA, USA, pp. 158–168. ACM, May 2021. https://doi.org/10.1145/3450268.3453528
23. Schöffel, M., Lauer, F., Rheinländer, C.C., Wehn, N.: Secure IoT in the era of quantum computers-where are the bottlenecks? Sensors **22**(7), 2484 (2022). https://www.mdpi.com/1424-8220/22/7/2484
24. Snyder, G.J., Toberer, E.S.: Complex thermoelectric materials. Nat. Mater. **7**(2), 105–114 (2008). http://www.nature.com/articles/nmat2090
25. Stebila, D., Mosca, M.: Post-quantum key exchange for the internet and the open quantum safe project. In: Avanzi, R., Heys, H. (eds.) SAC 2016. LNCS, vol. 10532, pp. 14–37. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-69453-5_2. https://openquantumsafe.org
26. Wan, Q., Teh, Y.K., Gao, Y., Mok, P.K.T.: Analysis and design of a thermoelectric energy harvesting system with reconfigurable array of thermoelectric generators for IoT applications. IEEE Trans. Circ. Syst. I Regul. Pap. **64**(9), 2346–2358 (2017)
27. Wang, W., Chen, X., Liu, Y., Wang, X., Liu, Z.: Thermo-electric energy harvesting powered IoT system design and energy model analysis. In: 2019 IEEE 13th International Conference on Anti-Counterfeiting, Security, and Identification (ASID), Xiamen, China, pp. 303–308. IEEE, October 2019
28. Yuan, F., Zhang, Q.T., Jin, S., Zhu, H.: Optimal harvest-use-store strategy for energy harvesting wireless systems. IEEE Trans. Wirel. Commun. **14**(2), 698–710 (2015). https://ieeexplore.ieee.org/document/6898878
29. Zhou, W., Zhang, Y., Liu, P.: The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Internet Things J. **6**(2), 1606–1616 (2019). arXiv:1802.03110 [cs]