# Security Aspects of Digital Twins in IoT

Vitomir Pavlov, Florian Hahn and Mohammed El-Hajj[a]
*Twente University, EEMCS (SCS), Enschede, The Netherlands*

Keywords: Digital Twin, IoT, Security, Authentication Arduino, Raspberry PI.

Abstract: The number of Internet-connected devices are expected to reach almost 30 billion by 2030, and already today the Internet of Things (IoT) technologies is a part of everyday life in sectors like public health, smart cars, smart grids, smart cities, smart manufacturing and smart homes. An even tighter integration between IoT technology and physical objects within these sectors has been made possible by the Digital Twin (DT) technology providing better abilities for real-time monitoring, data-driven modeling and process optimization. One integral aspect of this approach is the connection between IoT end-devices and their corresponding digital twins for real-time data communication. Depending on the envisioned scenario, the involved data and derived processes affect the safety of human lives, hence an authentic connection is of major importance. At the same time, IoT devices have restrictions on the available power sources and provided computing resources. In this work we report on our experiments with the Azure IoT Hub, the commercial platform that supports digital twins offered by Microsoft. First, we set up a real-time connection between the cloud platform and two different IoT devices and explore how an authentic connection is established between IoT devices and their corresponding DTs. Based on a test bed consisting of widely used IoT devices we analyse the power consumption and execution time of the offered authentication mechanisms that are based on general symmetric or asymmetric encryption. While the authentication time for a Raspberry Pi is below 0.5 seconds, the same task took above 4.5 seconds for an Arduino, highlighting the importance of lightweight authentication mechanisms for real-time communication between IoT devices and DT platforms.

## 1 INTRODUCTION

Advancements in sensor, microprocessor, and battery technology in recent years has given rise to small, low-powered devices that can be used to collect information about the physical world (El-hajj et al., 2017; El-Hajj et al., 2019). Due to their relatively low cost and small form factor, these sensing devices can be embedded into objects ranging from buildings, shipping containers, and infrastructure to airplanes and automobiles (El-Haii et al., 2018). Connecting these devices together over wireless communication creates the Internet of Things (IoT), a term initially coined by Kevin Ashton in 1999 when he proposed linked RFID enabled devices to the internet for Proctor and Gamble (Ashton et al., 2009). The technology has applications in various fields, such as logistics tracking, environmental monitoring, theft prevention (a recent example being the Apple AirTag, and patient monitoring in a medical context (Datta and Sharma, 2017). As an emerging technology, IoT has to deal with a number of growing Challenges (El-Hajj et al., 2019; El-Hajj et al., 2021). Managing the vast amount of data coming from myriad sensors poses new networking and data science challenges, and optimizing software for low-power, battery restrained devices is being actively worked on. Another challenge is the security of the IoT devices and the data transferred between them. Due to the low-power nature of many IoT sensor nodes, traditional security techniques no longer work efficiently (Elhajj et al., 2022), and literature reports the absence of proper lightweight encryption and authentication mechanisms (El-Hajj et al., 2019). Recently, the new concept of Digital Twins (DTs) has been introduced (Fuller et al., 2020) in various sectors such as industrial production, building management, health care, and smart cities. With the help of a completely digital representation of a physical system, its full life-cycle can be monitored, analysed, controlled, and optimized (Liu et al., 2021). The integration of this new technology into existing IoT systems is becoming more and more popular and commercial platforms are offered, for example by Microsoft or Nvidia providing this comprehensive tool

[a] https://orcid.org/0000-0002-4022-9999

Pavlov, V., Hahn, F. and El-Hajj, M.
Security Aspects of Digital Twins in IoT.
DOI: 10.5220/0011714500003405
In *Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023)*, pages 560-567
ISBN: 978-989-758-624-8; ISSN: 2184-4356

with small adoption overhead.

In this work we study the security of data that is being gathered by IoT devices and then forwarded to Azure Digital Twins, the popular digital twins platform offered by Microsoft. Despite the ongoing research activities in lightweight cryptography, the default authentication mechanisms supported by Azure Digital Twins all rely on general symmetric and asymmetric cryptography including full-fledged X.509 certificates. Our practical experiments are based on the simulation of a minimal real-life scenario where the Digital Twin is provided with real-time data from real IoT devices via a mutually authenticated channel. In this testing environment, we have analyzed the power consumption and execution time for different authentication schemes on two popular IoT end-devices, that is, the Raspberry Pi 3 Model B and Arduino MKR 1010 WiFi.

The rest of this paper is structured as follows: section 2 provides general background information on digital twins and then explore related work in the field of security and current use-cases for Digital Twins. In section 3 we detail the setup of our experiment to show how Digital Twins can be utilised to improve the security of IoT devices. Section 4 goes into the results of our experimentation, and section 5 is a discussion of the work done. Finally, section 6 concludes the research and presents areas of interest for further research.

## 2 BACKGROUND

In this section, we first review the state of the art in Digital Twins applications, focusing on application in the context of IoT. Then, we combined these reviews to argue that the current issues in the state of the art motivate the creation of a framework to apply DTs IoT-based applications.

### 2.1 What is a Digital Twin?

A digitally determined model that uniquely represents a physical instance, process, system, or similar abstraction is known as a Digital Twin (DT) in broad terms(Vrabič et al., 2018). The Digital Twin was first introduced by Michael Grieves in a 2003 presentation on Product Life-cycle Management (PLM), where Grieves was working with John Vickers of NASA (Grieves, 2014). Following that, in the PLM courses, this conceptual model served as a ”Mirrored Spaces Model” by Grieves (Grieves and Vickers, 2017). Grieves in (Grieves, 2014) also defined the architecture to be used while dealing with digital twins. This architecture consisted of three main components: The physical component, the virtual one and a communication channel between the physical and virtual component. The whole process is illustrated in Figure 1.

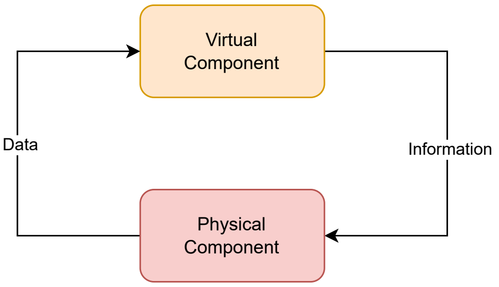


Figure 1: The Twinning between Physical and Virtual components.

In the current state of the art, the only consensus is that a Digital Twin is a virtual representation of a physical object. The majority of reviewed literature also considers a bi-directional connection and the ability to perform simulations on the digital representation as an integral part of the definition of Digital Twins. The ability to persist across multiple phases in the physical object's life cycle is explicitly mentioned in about one third of the reviewed literature according to (Kuehner et al., 2021).

### 2.2 Digital Twin Use-Cases

Industrial applications, platforms for life-cycle management, preventive maintenance, and the automobile industry are examples of where DTs are used more broadly (Liu et al., 2021). Irrigation (Purcell and Neubauer, 2022), medical (Ahmadi-Assalemi et al., 2020), supply chain (Defraeye et al., 2021), infrastructure (Hou et al., 2020), education (Vikhman and Romm, 2021), natural disaster detection (Fan et al., 2021), telecommunication (Seilov et al., 2021), and cybersecurity (Sousa et al., 2021; Saad et al., 2020; Salvi et al., 2022; Schellenberger and Zhang, 2017) are some of the most current and upcoming DT uses.

In (Ivanov et al., 2020) authors show that DTs serve as the foundation for smart communities and areas in a smart city, which is defined as a strategic approach to incorporate data and digital technologies to assure sustainable development, population safety, and economic development of the urban environment. Smart cities and city planning are two fields that have recently experienced a rise in the incorporation of the DT idea. Along with the focus on smart digital buildings, their servicing, and asset management, there is a shift toward creating digital twins of entire communities, or so-called smart Digital Twin cities. Recently, the literature has begun to report on the use of DTs in medicine(Ahmadi-Assalemi et al., 2020). Numerous uses have been mentioned, including in the areas of athletics, viral infection simulations, well-being in smart cities, telemedicine, and healthcare monitoring. Cybersecurity and social ethics issues are framed as two of the major barriers facing the conceptual model of a human Digital Twin (HDT) as mentioned by the authors in (Shengli, 2021). Their main objective was to create a virtual representation of the body of a person by utilizing data from wearable devices, mobile phone and medical records. Web services are used to update the content of the virtual representation on a regular basis. The HDT concept incorporates a certain index that is given to humans at birth, and as they develop, their biological data is continuously sent into the HDT as an input.

For modeling, simulating, and improving cyber-physical systems, the DT idea is essential. Through application services related to evaluation, modeling, tracking, optimizing, and predictive management, it can offer a deeper understanding of complicated physical processes (Hou et al., 2020). The goal of DT engineering applications is to anticipate future behavior and efficiency of physical systems and to produce useful data that enable the devices to behave autonomously and providing support in decision-making process (Zhou et al., 2019). For example a DT multi-dimensional model used in construction as an illustration was created by authors in (Liu et al., 2020) to monitor pre-stressed steel structures in real-time for safety estimations. Although the usage of DT principles in the automobile industry has increased, the majority of the current research is concentrated on the automotive assembly processes and design implementation of automobiles (Sharma and George, 2018). Even there was a great effort to use DT in the production of electrical vehicles with the introduction of IoT and network technologies that enables the ability to convert offline digital model into DT. Authors in (Van Mierlo et al., 2021) show that the development of DT in electrical vehicles could lead to the ability to prognosis and planning of future maintenance events, monitoring system, fault prediction and fault location, etc.

Based on this review we conclude that DT applications are increasingly being used in a wide range of fields. This technology – if merged with enabling technologies like big data, simulation, Information Technologies (IT) and communication interfaces – be a novel, useful tool for designers and operators at the same time. It is clear that DT technology is still in its early life-stages; overcoming profound challenges that face a modern DT implementation, such as costs, information complexity and maintenance, a lack of rules and regulations, and problems with cybersecurity and communications, will be necessary before DT technology reaches its full potential.

## 3 METHOD AND EXPERIMENT SETUP

In this section we detail our methodology for setting up a test bed for the chosen DT platform and then testing the authentication done between the physical component and the virtual one before start communicating in a real time manner. We first list the components of our test bed, then explain the setup of the Digital Twin, and finally show how the authentication schemes occurred between the physical and virtual device.

### 3.1 Framework Overview

For our study we first prepared a working scenario for the deployment of DTs and before we conduct our analysis later. We used the following components in our test bed:

1. **IoT Hub:** An IoT application and the connected devices use the managed Azure IoT Hub service, which is hosted in the cloud and serves as a central messaging hub. Millions of devices and their backend programs can be securely and reliably connected. Several messaging patterns are supported, including device-to-cloud telemetry, uploading files from devices, and request-reply methods to control your devices from the cloud. IoT Hub offers tracking to assist you in keeping track of the creation, connections, and failures of your devices. To serve your IoT workloads, IoT Hub expands to millions of devices connected at once and millions of events per second.
2. **Azure Digital Twin:** Using digital models of complete environments, such as buildings, factories, farms, energy networks, railways, stadiums, and more, Azure Digital Twins is a platform as a service (PaaS) solution that makes it possible to create twin graphs. Twin graphs may even be created for entire cities. These digital models can be utilized to gather data that leads to breakthrough consumer experiences, process optimization, better products, and lower costs.
3. **Physical Device:** We deployed a Raspberry Pi 3B+ as the physical device. Boasting a 64-bit quad core processor running at 1.4GHz, dual-band 2.4GHz and 5GHz wireless LAN, Blue-

tooth 4.2/BLE, faster Ethernet, and Power over Ethernet (PoE) capability via a separate PoE HAT. And for the purpose of comparison and benchmarking, we also used Arduino MKR 1010 WiFi which includes a 32-bit Cortex-M0+ ARM micro-controller (programmable like a conventional Arduino) running at a clock speed up to 48 MHz,providing up to 20 analog inputs and up to 8 digital I/O ports, Wi-Fi and Bluetooth connectivity, and a crypto-chip for secure communication using SHA-256 hashing algorithm. In addition, it has 32 KB of Static Random Access Memory (SRAM) and 8 general purpose digital pins that can be either outputs or inputs.

4. **DHT11 Sensor:** It is a sensor for collecting the Temperature and Humidity data. It measures the airflow using a sensitive humidity sensor and a thermostat and outputs a digital signal on the data pin (no analog input pins needed).

## 3.2 Experimental Setup

Our experimental setup implements the framework described in section 3.1. The source code is available in Gitlab[1]. Figure 2 describes our prototypical implementation and documents technology and data flows. It shows all processes that are executed during the communication between the IoT device and the temperature sensors, all the applications and the Azure services. Certificate based authentication is build upon X.509 public key infrastructure (PKI) standard between the physical device and the DTs (a more detailed description about authentication process is given in section 3.3). The two temperature sensors are connected to the IoT device and each sensor is authenticated via a separate certificate. When the device application authenticates the sensors with the X.509 certificates, there are two possible outputs: first, *IoTHubDeviceClient* indicating a working connection or second, *empty* indicating a failed authentication and hence no connection. If the clients are authenticated, then the data from both of the sensors is formatted as reported properties [2] and sent to the Azure IoT Hub which will then update the Digital Twins that are related to the physical sensors. We activated a twin patch handler which listens for any changes of the desired properties, which are usually updated from the Azure or via backend program. In our case, we have implemented a back-end program that authenticates with the connection string, which contains the private key of the IoT Hub and connects the sensors via their Digital Twin IDs. If authentication is successfully achieved, then the desired properties are updated and the twin patch handler reacts that was activated on the IoT device. However, if authenticated failed, then the *IoTHubRegistryManager* is not initialized and an error will be shown. Our test program also indicates where the sensors are hosted and which are connected via WiFi. For the purposed of comparison regarding the performance analysis we deployed our framework on two physical IoT devices, that is, the Raspberry Pi 3B+ and the Arduino MKR1010 WiFi.

## 3.3 Mutual Authentication Between Physical and Digital Twin

Certificate based authentication is built by leveraging the X.509 public key infrastructure (PKI) standard. Stronger security is provided via certificate authentication, which uses a Certificate Authority (CA) to mutually authenticate the client and the server. Devices can be authenticated to an Azure IoT Hub using X.509 certificates. A certificate is a digital record that includes a device's public key and can be used to authenticate itself. X.509 certificates using ECDSA and the RSA signature algorithms were used in our proof of concept framework. We used OpenSSL to create a certification authority (CA), a subordinate CA, and a device certificate. The example then signs the subordinate CA and the device certificate into a certificate hierarchy. The X.509 digital certificate contains various fields like *version, serial number, signature (hash) algorithm, issuer, valid from, valid to, subject, the public key of the entity that is the certificate is issued for and its parameters, enhanced key usage, subject alternative name, subject key identifier, key usage, basic constraints, and the thumbprint*. Figure 3 shows the list of fields created for each certificate.

The authentication process between the physical device and the DT is illustrated in Figure 4.

Initially, the IoT device will instantiate the X.509 Certificate as an object with the pre-generated key pair from the certificate files that we already moved to the device. Then, it will send the public data of the document to the Azure CA and the IoT Hub. The CA and the hub will verify the device's certificate and, if everything is correct, it will instantiate the AzureIoTHubClient[3] and establish a secure connection. The IoTHubClient[4] will have access to the DT public key

[1] Removed for blinded submission purposes. Available upon request

[2] In a JSON-like language format called Digital Twins Definition Language (DTDL)

[3] The IoT Hub service client is used to communicate with devices through an Azure IoT hub.

[4] Is the primary interface for developers using the Azure

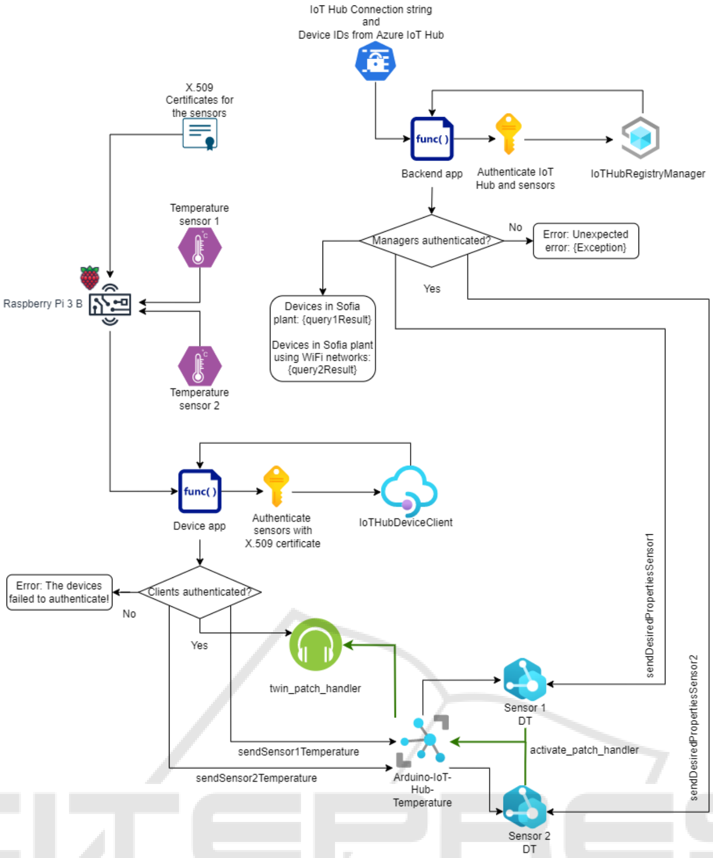
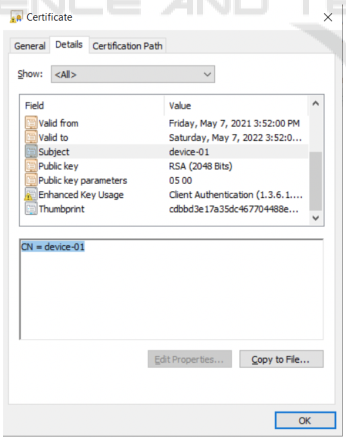

IoT Hub Connection string
and
Device IDs from Azure IoT Hub
func( )
Backend app
Authenticate IoT Hub and sensors
IoTHubRegistryManager
X.509 Certificates for the sensors
Managers authenticated?
No
Error: Unexpected error: {Exception}
Yes
Temperature sensor 1
Raspberry Pi 3 B
Devices in Sofia plant: {query1Result}
Devices in Sofia plant using WiFi networks: {query2Result}
Temperature sensor 2
func( )
Device app
Authenticate sensors with X.509 certificate
IoTHubDeviceClient
sendDesiredPropertiesSensor1
sendDesiredPropertiesSensor2
Error: The devices failed to authenticate!
Clients authenticated?
No
Yes
twin_patch_handler
Sensor 1 DT
activate_patch_handler
sendSensor1Temperature
sendSensor2Temperature
Arduino-IoT-Hub-Temperature
Sensor 2 DT

Figure 2: Framework Overview.


Certificate

General | Details | Certification Path

Show: <All>

| Field | Value |
|---|---|
| Valid from | Friday, May 7, 2021 3:52:00 PM |
| Valid to | Saturday, May 7, 2022 3:52:0... |
| Subject | device-01 |
| Public key | RSA (2048 Bits) |
| Public key parameters | 05 00 |
| Enhanced Key Usage | Client Authentication (1.3.6.1.... |
| Thumbprint | cdbbd3e17a35dc467704488e... |

CN = device-01

Figure 3: X.509 Certificate Fields.

which help the device to encrypt the messages. Afterwards, when the device is authenticated correctly, it will start sending the sensor data using the IoTHubDeviceClient[5] which will encrypt this data and send it to the IoTHub[6]. This is verified by the IoT Hub using the root certificate, then the data is decrypted and the used to update the DT properties. Whenever the Digital Twin make a change from its behalf, it will fire up patch event which will then be noticed by the IoT Hub. Then, it will encrypt the modified data and send the desired proper- ties to the physical device. Finally, the physical device, by using the IoTHubDeviceClient, will decrypt the data passed in the event handler and will receive it successfully. All the scripts used for this work can be seen in Github[7]. Additionally, screenshots with the results from our experiments are in the *pics-results* folder.

## 4 RESULTS

After we prepared the simulation and everything was running smoothly, we decided to evaluate the sym-

IotHub client library

[5] A synchronous device client that connects to an Azure IoT Hub instance.

[6] Azure IoT Hub is a managed service hosted in the cloud that acts as a central message hub for communication between an IoT application and its attached devices.

[7] https://github.com/Vitomir2/Digital-Twins-Azure-IoT-Hub

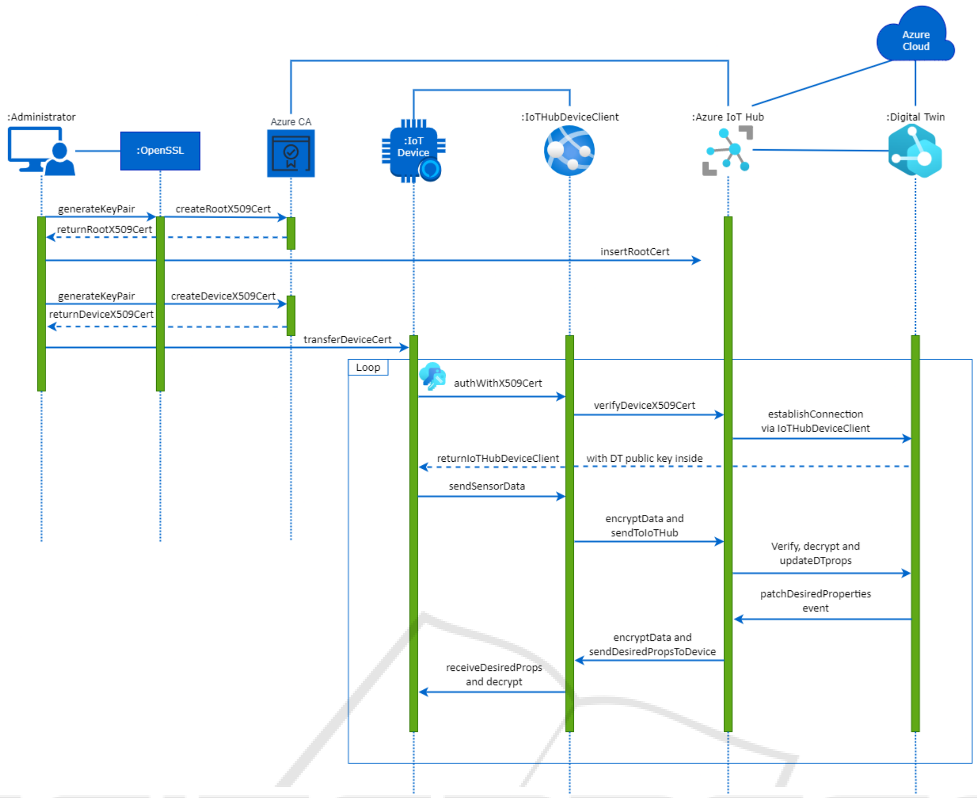


Figure 4: Authentication Process.

metric key authentication and the X.509 certificates by measuring the power consumption. We did this by using a USB power consumption tester which has the ability to monitor the energy consumption. Additionally, we executed test scenarios to monitor the execution time of the authentication which was our second metric used to compare both authentications. The results can be seen in Table 1. We created two additional test scripts that are only authenticating the devices, in order to have more precise results. You can find them on the repository, in folder *test-scripts*. For the power consumption we ran the script ten times and then took the average values that the USB tester was giving in amperes and volts. In all authentication types, the Raspberry Pi was working on 5.32 volts. For the execution time, we decided to execute the run the script ten times and calculate the average execution time. Then, we ran this additional ten times in order to get the more accurate average results for the execution time. Furthermore, we measured the generation time of the device certificates and the generation time for the root certificates. The overall results are presented in Table 2.

Table 1: Measurement Results.

| IoT Hardware Platform | Authentication protocol | Current(mA) | Power(W) | Execution time(s) |
|---|---|---|---|---|
| **Raspberry PI** | Symmetric key | 112 | 0.596 | 0.0452 |
| | X.509 with ECDSA | 151 | 0.803 | 0.412 |
| | X.509 with RSA | 163 | 0.867 | 0.396 |
| **Arduino MKR 1010** | Symmetric key | 12 | 0.061 | 4.683 |
| | X.509 with ECDSA | 15 | 0.076 | 5.121 |

Table 2: Certificate Generation Time.

| Certificate | Generation time(s) | Root Generation time(s) |
|---|---|---|
| **X.509 with ECDSA** | 1.4 | 5.3 |
| **X.509 with RSA** | 1.8 | 6.5 |

## 5 DISCUSSION

Our environment used a bidirectional communication which enables both, the physical devices and the DTs, to communicate to each other. They provide the new data via the reported and desired properties which are in a JSON object format. One can add any property and value and if there is a change of the value of an already existing property it will then trigger an event and will update the data accordingly. However, if the physical twin passes the same data twice, it will update it only once. The same goes for the updates from the DT to the physical device. From the measurement results, for both boards, we see that the execution time of the connection authenticated by a string derived from symmetric cryptography is faster than the both certificate options. For the Raspberry Pi, it is approximately 0.0452 seconds, whereas for the certificates it is 0.412 seconds and 0.396 seconds for the ECDSA and RSA certificates, respectively. For the Arduino board symmetric key authentication requires 4.683 seconds for the connection string versus 5.121 for the ECDSA certificate. Additionally, we can see that it uses approximately 112 mA for the current and 0.596 watts for the power, whereas the certificates use approximately 151 mA and 0.803 watts, and 163 mA and 0.867 watts, respectively. These power measurements show that the digital certificates are less efficient, in the manner of the energy consumption, than the symmetric key authentication. Furthermore, we can see that both certificates have slight differences in both the power consumption and the execution time measurements. For the power consumption on the Arduino MKR 1010 board, we can see for symmetric and X.509 it consumes a less power but for the execution time Raspberry PI is faster. Lastly, from the certificate generation times, we can see that both, the generation time for the root certificates and the devices' certificates, are faster for the ECDSA. We measured approximately 5.3 seconds for the generation of the Root ECC certificate and 1.4 seconds for the generation of the certificates for the devices with ECC. However, for the RSA, we evaluated the generation time and it was a bit higher of 6.5 seconds for the root certificate and 1.8 seconds for the devices' certificates. This execution time might be higher, because of the larger keys for the RSA 2048 bits, whereas in the ECC, the key was 256 bits. We conclude that the symmetric key encryption is much faster than the digital certificates, and requires less energy. However, the certificates give us the opportunity to have better security, to keep the private keys securely only on the devices and to have a relation with a specific identity, e.g, the IoT devices or individual sensors.

## 6 CONCLUSION

We study how mutual authentication between physical devices and Digital Twins is currently implemented at Azure IoT Hub - the commercial platform by Microsoft. Our experiments based on a proof of concept successfully established an authenticated communication between IoT end-devices and its mapped Digital Twins. To our surprise, no authentication mechanisms offered by this platform are particularly lightweight and hence specifically tailored towards low-power consumption - a requirement often formulated for IoT applications. Our performance analysis measuring the execution time and the power consumption of two hardware platforms show difference in execution time that are of one order of magnitude and a similar difference is measured for the power consumption necessary for the authentication process between IoT devices and DTs. Specifically, the authentication process for the Arduino MKR 1010 required more than 4.5 seconds and hence are of limited use for real-time applications. From our results we conclude that further studies are necessary when combining IoT solutions with the recent Digital Twins technology. Especially the security challenges for real-time monitoring are of high relevance. In future, we are going to work with a lightweight authentication schemes to ensure the mutual authentication between the DT and its physical device and then we will compare the performance analysis with the traditional authentication schemes like the ones provided by Azure.

## REFERENCES

Ahmadi-Assalemi, G., Al-Khateeb, H., Maple, C., Epiphaniou, G., Alhaboby, Z. A., Alkaabi, S., and Alhaboby, D. (2020). Digital twins for precision healthcare. In *Cyber defence in the age of AI, Smart societies and augmented humanity*, pages 133–158. Springer.

Ashton, K. et al. (2009). That 'internet of things' thing. *RFID journal*, 22(7):97–114.

Datta, P. and Sharma, B. (2017). A survey on iot architectures, protocols, security and smart city based applications. In *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–5.

Defraeye, T., Shrivastava, C., Berry, T., Verboven, P., Onwude, D., Schudel, S., Bühlmann, A., Cronje, P., and Rossi, R. M. (2021). Digital twins are coming: Will we need them in supply chains of fresh horticultural produce? *Trends in Food Science & Technology*, 109:245–258.

El-Haii, M., Chamoun, M., Fadlallah, A., and Serhrouchni, A. (2018). Analysis of cryptographic algorithms on iot hardware platforms. In *2018 2nd Cyber Security in Networking Conference (CSNet)*, pages 1–5. IEEE.

El-hajj, M., Chamoun, M., Fadlallah, A., and Serhrouchni, A. (2017). Analysis of authentication techniques in internet of things (iot). In *Cyber Security in Networking Conference (CSNet), 2017 1st*, pages 1–3. IEEE.

El-Hajj, M., Fadlallah, A., Chamoun, M., and Serhrouchni, A. (2019). Ethereum for secure authentication of iot using pre-shared keys (psks). In *2019 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pages 1–7.

El-Hajj, M., Fadlallah, A., Chamoun, M., and Serhrouchni, A. (2019). A survey of internet of things (iot) authentication schemes. *Sensors*, 19(5):1141.

El-Hajj, M., Fadlallah, A., Chamoun, M., and Serhrouchni, A. (2021). A taxonomy of puf schemes with a novel arbiter-based puf resisting machine learning attacks. *Computer Networks*, 194:108133.

Elhajj, M., Jradi, H., Chamoun, M., and Fadlallah, A. (2022). Lasii: Lightweight authentication scheme using iota in iot platforms. In *2022 20th Mediterranean Communication and Computer Networking Conference (MedComNet)*, pages 74–83. IEEE.

Fan, C., Zhang, C., Yahja, A., and Mostafavi, A. (2021). Disaster city digital twin: A vision for integrating artificial and human intelligence for disaster management. *International Journal of Information Management*, 56:102049.

Fuller, A., Fan, Z., Day, C., and Barlow, C. (2020). Digital twin: Enabling technologies, challenges and open research. *IEEE access*, 8:108952–108971.

Grieves, M. (2014). Digital twin: manufacturing excellence through virtual factory replication. *White paper*, 1(2014):1–7.

Grieves, M. and Vickers, J. (2017). Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. In *Transdisciplinary perspectives on complex systems*, pages 85–113. Springer.

Hou, L., Wu, S., Zhang, G., Tan, Y., and Wang, X. (2020). Literature review of digital twins applications in construction workforce safety. *Applied Sciences*, 11(1):339.

Ivanov, S., Nikolskaya, K., Radchenko, G., Sokolinsky, L., and Zymbler, M. (2020). Digital twin of city: Concept overview. In *2020 Global Smart Industry Conference (GloSIC)*, pages 178–186. IEEE.

Kuehner, K. J., Scheer, R., and Strassburger, S. (2021). Digital twin: Finding common ground – a meta-review. *Procedia CIRP*, 104:1227–1232. 54th CIRP CMS 2021 - Towards Digitalized Manufacturing 4.0.

Liu, M., Fang, S., Dong, H., and Xu, C. (2021). Review of digital twin about concepts, technologies, and industrial applications. *Journal of Manufacturing Systems*, 58:346–361.

Liu, Z., Bai, W., Du, X., Zhang, A., Xing, Z., and Jiang, A. (2020). Digital twin-based safety evaluation of prestressed steel structure. *Advances in Civil Engineering*, 2020.

Purcell, W. and Neubauer, T. (2022). Digital twins in agriculture: A state-of-the-art review. *Smart Agricultural Technology*, page 100094.

Saad, A., Faddel, S., Youssef, T., and Mohammed, O. A. (2020). On the implementation of iot-based digital twin for networked microgrids resiliency against cyber attacks. *IEEE transactions on smart grid*, 11(6):5138–5150.

Salvi, A., Spagnoletti, P., and Noori, N. S. (2022). Cyber-resilience of critical cyber infrastructures: Integrating digital twins in the electric power ecosystem. *Computers & Security*, 112:102507.

Schellenberger, C. and Zhang, P. (2017). Detection of covert attacks on cyber-physical systems by extending the system dynamics with an auxiliary system. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pages 1374–1379. IEEE.

Seilov, S., Kuzbayev, A., Seilov, A., Shyngisov, D., Goikhman, V. Y., Levakov, A., Sokolov, N., Zhursinbek, Y. S., et al. (2021). The concept of building a network of digital twins to increase the efficiency of complex telecommunication systems. *Complexity*, 2021.

Sharma, M. and George, J. (2018). Digital twin in the automotive industry: Driving physical-digital convergence. *Tata Consultancy Services White Paper*.

Shengli, W. (2021). Is human digital twin possible? *Computer Methods and Programs in Biomedicine Update*, 1:100014.

Sousa, B., Arieiro, M., Pereira, V., Correia, J., Lourenço, N., and Cruz, T. (2021). Elegant: security of critical infrastructures with digital twins. *IEEE Access*, 9:107574–107588.

Van Mierlo, J., Berecibar, M., El Baghdadi, M., De Cauwer, C., Messagie, M., Coosemans, T., Jacobs, V. A., and Hegazy, O. (2021). Beyond the state of the art of electric vehicles: A fact-based paper of the current and prospective electric vehicle technologies. *World Electric Vehicle Journal*, 12(1):20.

Vikhman, V. and Romm, M. (2021). “digital twins” in education: Prospects and reality. *Vysshee Obrazovanie v Rossii= Higher Education in Russia*, 30(2):22–32.

Vrabič, R., Erkoyuncu, J. A., Butala, P., and Roy, R. (2018). Digital twins: Understanding the added value of integrated models for through-life engineering services. *Procedia Manufacturing*, 16:139–146. Proceedings of the 7th International Conference on Through-life Engineering Services.

Zhou, M., Yan, J., and Feng, D. (2019). Digital twin framework and its application to power grid online analysis. *CSEE Journal of Power and Energy Systems*, 5(3):391–398.