UNIVERSITY OF TWENTE.

**Faculty of Electrical Engineering,
Mathematics & Computer Science**

Security Aspects of Digital Twins in IoT platform

Vitomir Pavlov

M.Sc. Thesis
August 2022

Supervisors:
Dr. Ing. Mohammed El-Hajj
Dr. Ing. Florian Hahn

External Committee Member:
Dr. Ing. Yanqiu Huang

Services and CyberSecurity
Faculty of Electrical Engineering,
Mathematics and Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede
The Netherlands

Abstract

With the number of Internet-connected devices (things), expected to be almost 30 billion by 2030, the Internet of Things (IoT) technologies already became a part from everyday life, various areas like public health, smart cars, smart grids, smart cities, smart manufacturing and smart homes. Therefore, the companies started to implement and improve the Digital Twin technology. It is not widely understood and secured, that is why we are going to provide current state of the art for the authentication protocols in the IoT and the Digital Twins relationship.

In this paper, we investigate whether the DT and IoT devices communicate efficiently and securely. This is done by doing extensive literature review of what are the IoT authentication schemes we currently have and what proposals are made by many encouraged researchers. Additionally, we aim to deliver good insight on the Digital Twin (DT) history and the current state of this amazing technology, and how it can be deployed in the IoT platform. Moreover, we prepared a simulation of a real life scenario with the goal of showing how the DTs can be used with real-time data provided from real IoT devices and how these devices are authenticated with the related DTs. Lastly, we performed power consumption tests, and execution time, with various authentication options, that the simulation platform provides, and compare them in order to find the one with the best performance. The tests are performed on two different IoT boards - Raspberry Pi 3 Model B and Arduino MKR 1010 WiFi.

Key words: IoT, Digital Twins, Security, Authentication, Industrial IoT (IIoT), Encryption schemes, Lightweight encryption, Security protocols, Raspberry Pi, Arduino, MKR 1010, IoT boards

CONTENTS

1 INTRODUCTION

The IoT is a large network of smart devices connected via the internet, e.g., sensors, smart homes, manufacturing machines, smart vehicles, agriculture, healthcare, etc. [39–41]. This network has already grown a lot and it is continuing to grow exponentially. There are statistics that show a forecast on how the number of IoT devices will grow during the current decade (2020-2030)[1]. IoT devices are fast in-creasing in popularity, creating a significant impact which is major beneficial factor to our daily lives, society, and industries through time; even though, the secure devices and communication that the technology requires are not yet matured. Due to this growth of the the number of connected devices, attackers will have more opportunities to gain access over them, and they will be able to execute large-scale attacks, e.g., Distributed Denial-of-Service (DDoS) attack. In addition, some researchers pointed out that many IoT devices have security concerns due to the fact that they are using a default, easy to remember password, or no password at all [3]. Therefore, these weaknesses in the security of devices give an advantage to hackers easily to access these devices and turn them into a vulnerable objects.

In addition, other authors presented various very exciting and promising ways to authenticate the IoT devices in the most secure way. For example, there are 3GPP authentication protocols, mutual authentication key exchange protocols [4], Physical Unclonable Function (PUF) based authentication key exchange protocols [30], schemes that are using Artificial Intelligence (AI) techniques [3,45], privacy-preserving authentication schemes [36], hands-free authentication with trusted IoT device and Machine Learning(ML) [59], and many more. We are going to review diverse of authentication schemes which are going to help us to understand better what is needed for efficient IoT ecosystem. However, sometimes it is almost impossible to fully secure all types of IoT devices, because some of them are not even so significant and not aimed by adversaries. For instance, just a normal smart bulb at home is not so important to be secured as much as possible, compared to a smart surgery robot which must be secured as much as possible.

The security of the IoT devices and sensors, and the network at all, are quite important for the Digital Twin technology. Due to this, if IoT authentication is weak, this can lead to exploits in the DTs that are connected to these devices. DT technology is a concept that was used long time ago, but not directly specified that way. In [53], the authors mentioned when the concept was initially used and this was in a National Aeronautics and Space Administration (NASA) rescue mission for Apollo 13, the models were called "simulators“[2]. It is said that there has been an explosion that shook the spacecraft of three astronauts which have been about 210,000 miles away from the Earth. The NASA has used 15 simulators which were controlled by a network of virtual computers and they were useful in preventing the disaster in Apollo 13. However, the spacecraft had not been using any IoT devices, thus, NASA team have been using state-of-the-art communications technology in order to stay connected with the spacecraft and the crew. Then, the DT concept was introduced in Michael Grieves presentation for Product Lifecycle Management (PLM) model in the early 2000's, but it was too

[1] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[2] https://blogs.sw.siemens.com/simcenter/apollo-13-the-first-digital-twin/

complex to implement such technologies at that time. This is due to the fact that DTs need to use a combination of multiple technologies, the potential of the DT was not explored a lot, until other fields were improved like IoT, AI, ML and Big Data.

Therefore, with this paper, we are going to provide good understanding how efficient the DT is communicating with the IoT device. This will be done by showing how the DT is deployed in the IoT platform and how they are authenticated. We prepared an experiment that will simulate a real life communication between two temperature sensors, connected to Raspberry Pi board, and the Azure IoT Hub where the corresponding DTs live. With this simulation, we are going to provide a comparison between the different options that Azure provides for authentication - we will show an overview of them and then will monitor their power consumption and execution time for the Raspberry Pi and the execution time of the Arduino MKR, and will make a comparison. Therefore, the document will be entirely based on one main research question and three sub-questions to support it.

The rest of the chapter will be structured as follows: in Section 1.1 we are going to provide the open challenges related to the IoT and its authentication. In Section 1.2, we provide briefly what motivate us to do this research. Moreover, in Section 1.3, we state our main research question the sub-questions that will be covered with this work. Lastly, Section 1.4 will summarize the outline of the paper.

1.1 Open Challenges

The limitations and the requirements of the IoTs raise multiple challenges like connectivity for the billions of devices that communicate to each other, security challenges because of the need of a secure IoT networks and also a need to protect them of being taken as an attack tool, e.g., the Mirai botnet Attack[13]. Therefore, the authentication is considered as a key requirement, for the IoT devices[39–41]. The biggest challenge with the authentication is that the IoT devices are resource-constraint by nature which makes the security schemes and protocols inefficient and useless for them. However, there are already many lightweight proposals, but how secure are they? Probably not that secure as the ones used for powerful machines like PCs, servers and workstations. Additionally, due to the lack of proper authentications for many IoT devices, other challenges appear like Denial-of-Service (DoS) and DDoS attacks, Replay attacks or Fake Node attacks.

Other challenges that we encounter are the ones related to the storage cost and the key management. For example, many IoT devices are using lightweight solutions based on the public key encryption, which means that someone need to store and manage all the keys or certificates. This is additional cost and usually, for the certificates, people are dealing with a Certified Authority (CA) for this purpose. Lastly, the authors in [66] listed multiple open issues related to the authentication of the IoT like mutual authentication, confidentiality, integrity, availability, computational overhead and device identification.

1.2 Context and Motivation

While there are already researches for the authentication schemes for the IoT and efforts to explore new fields for the DTs, where the IoT devices and sensors are used a lot, there is a lack of explanation how they are connected and how the security of each of the technologies is important. Moreover, the DTs are mostly used separately and not aggregated or communicated to each other. The authors of an aggregation layer proposal [105] explored exactly such case where one can aggregate multiple digital twins. Additionally, there are multiple simulation platforms that can be used, but there is no summary of their pros and cons, and what scenarios they can fit.

Here are several reasons why the mentioned gaps are not fixed already:

1. The DT technology is not so widely adopted yet;
2. Implementing such technology for the companies and the corporations is still expensive, which is related to the adoption;
3. In order to fully take advantage of the benefits of the technology, quite a few different technologies must achieve synergy and to have joint requirements. Such technologies are AI, ML, Big Data and IoT. A joint requirement might be a necessity of strong security and there is a need of a standard that will ensure the security when they are used together.

1.3 Research Questions

From the given introduction, we can see that the IoT field is growing rapidly and it also includes multiple other technologies in order to provide efficient and secure services to the companies and users. This paper will provide a comprehensive survey on already existing authentication schemes for the IoT systems, which will theoretically answer the first sub-question 1a. Then, we present a literature review on current state of the DT technology and prepared simulation in order to cover the other two sub-questions, 1b and 1c. Answering these questions will help us to show the main purpose of the paper and to answer the main research question 1. The following questions are:

1. How efficient are authentication protocols currently used in industry for the communication between Digital Twins and IoT devices and what are the alternative protocols proposed in the academic literature?

    a) What are the existing authentication schemes for IoT that were presented in the literature?

    b) How DT could be deployed in the IoT use-cases?

    c) How to ensure authenticity between the DT and the IoT device?

Answering these questions will help the other researchers and readers to better understand how important is the authentication phase in any system, what is the current state of the innovation, how multiple technologies interconnect with each other like the IoT technology and the DT technology, and many others - AI, ML, Big Data, Cloud Computing and so on. For example, the DT technology can use AI or ML algorithms that are providing good overview of the work of the physical device, additionally, can provide sophisticated statistics that can help the companies to act in one way or another. These algorithms usually can be combined with big data and cloud computing. In addition to the third question, the authenticity will be in the following way: the physical device (the IoT) is authenticating, or connecting, to the DT. Then, if the IoT device is authenticated successfully, it will be able to send data and will have the possibility to attach to an event from the DT. For instance, if the state of the DT is changed, that will fire up an event which will be caught from the physical device that is already connected and authenticated.

1.4 Outline

The outline of the paper is organized as follows: the main purpose of Section 1.3 is to pose our research questions that we are going to answer throughout the paper. Section 2 will present the background that is required in order to become familiar with the topic and to have more understandable view on while going through the document - IoT specifications, authentication and security concerns around the topic, IoT adoption and lightweight encryption; and the section will end with the DT specifications, challenges and opportunities in the IoT platform. Then, Section 3 will summarize the existing researches, results and surveys for the different authentication schemes for the IoT and the relationship with the DTs. Section 4 describes the methodologies that will be used for this research paper. After that, Section 5 will provide explanation for our experiment setup, sequence and component diagrams, the experiment results and then a discussion on the results. Lastly, Section 6 will provide brief summary of what we achieved, summary of our results, will expose some of the limitations of the work and will point out some further discussions that can be made.

2 Background

This chapter discusses the history of the IoT technology, the authentication and the security concerns related to this, IoT adoption and lightweight encryption and lastly, the Digital Twins specifications and its challenges and opportunities integrated in the IoT platform. It will be organized as follows: In Section 2.1 we provide some background of the IoT in order give you better experience while going through the whole work; Afterwards, in Section 2.2, we discuss the authentication of the IoT and mention the security concerns that exists; Lastly, in Section 2.3 we will give better understanding of the DT technology and the related challenges.

2.1 IoT background

The Internet of Things (IoT) are physical objects that consist of sensors, ability to do a processing of information, software and many other technologies used to exchange data with other devices or systems over a network (private or public). They can be used in a very large range of fields like wireless sensor networks, manufacturing and automation, smart cities, smart homes, smart wearables, healthcare, etc.

Theoretically, it can be said that the beginning of the IoT started in 1969, when the Advanced Research Projects Agency Network (ARPANET) was established. [3]. However, the first usage of the term and the concept of Internet of Things, was used in a speech, in September 1985[4]. Despite that, the ARPANET was made public in 1980s and two years later, programmers connected the first device, that was executing 'smart' things, with the Internet and it was a Coca-Cola vending machine[5]. Then, the connection of devices to the Internet has started and various devices were used like a toaster connected to the Internet (in 1990), the first webcam (in 1993) and GPS satellites for getting the locations (in 1995). Afterwards, in order to increase the capabilities of the Internet, the IPv6 standard was invented in 1998, which enabled more devices to be connected to the Internet. With that change the revolution began and many researchers started to explore different areas, like the mentioned above, and devices that can be used for the IoT.

The field evolved a lot with usage of ubiquitous computing, sensors, machine learning, artificial intelligence, progressively powerful embedded systems, wireless sensor networks and so on. Therefore, in the recent years, using the IoT, smart devices and other technologies, the industry evolved to the so called generation 4.0. This increased the automation, improved the communication between the devices and the self monitoring, the use of smart machines that can analyze and diagnose problems without the need of people to act[6].

[3] https://en.wikipedia.org/wiki/ARPANET

[4] https://en.wikipedia.org/wiki/Internet_of_things

[5] https://www.iottechtrends.com/history-of-iot/

[6] https://en.wikipedia.org/wiki/Fourth_Industrial_Revolution

2.2 Authentication and security concerns

In this section we are going to discuss the IoT deployment challenges, security challenges and concerns, and mainly focus to the authentication challenges. In addition, we will be mainly focused on the 3-layer IoT architecture, namely application layer, network layer and perception layer, but in the literature some authors consider a 4-layer IoT architecture that add up a supporting layer between the application and network layers.

There are multiple challenges that can appear when deploying an IoT infrastructure and it can depend on the size of the system, for what environment it is going to be used and so on. However, there are some main challenges that can be faced related to connectivity, continuity, compliance, coexistence and cybersecurity[7], also called "5C's of IoT".

1. The **connectivity** requires a seamless flow where the information is going to be transferred between the devices, applications and the cloud. Thus, it can become complicated to manage the various types of devices, because the IoT standards are still in an evolving phase.
2. In the **continuity** aspect, the main concerns are related to the life of the batteries of the devices and how the life can be extended. It is quite important, especially for healthcare devices like pacemakers, because a failure can cost a life.
3. Then, in the **compliance** aspect, the devices must follow some radio standards and global requirements for regulations which can be quite complicated and also time-consuming.
4. For the next aspect, there are challenges related to the **coexistence** testing, because the devices are working over the wireless or with radio channels in an environment of billions of IoT devices and they must operate properly in order to avoid potential risks and unintended signals.
5. Lastly, for the **cybersecurity** aspect, the devices must be regularly tested for some potential threats or attacks, also called over-the-air (OTA) vulnerabilities. Such risks should be identified using a database with already known threats that is constantly updated.

The IoT technology growth is accompanied with a lot of security concerns that can include a weak authentication, keep using the default credentials for the devices, weak encryption (or no encryption at all) when transfer messages between the devices, insufficient regular security testing and updating, poor IoT device management, insufficient data protection and so on. Our focus will be the authentication, because it is considered as the weakest link for the hackers[8]. This security aspect is very crucial for the IoT environment, because it is efficient to be used in the whole process of the communication between the various devices, applications and cloud servers. In addition, the lack of computational power is a huge concerns, because it requires comprehensive lightweight authentication schemes and protocols to be implemented which comes with its drawbacks. The lightweight authentication schemes are hard to be that secure as the conventional authentication schemes, due to the lack of compu-

[7] https://itchronicles.com/iot/iot-deployment-and-its-challenges/

[8] https://www.techtarget.com/iotagenda/post/Solving-IoT-authentication-challenges

tational power and storage. There are multiple problems that can occur if there is no proper authentication like DDoS attacks, MITM attacks, brute-force attacks, social engineering attacks and malware attacks.

2.3 Digital Twins

This section will be mainly focused on the Digital Twins and it will be separated into multiple sections for more clear explanation and understanding: 2.3.1 the history of the DTs; 2.3.2 the specifications of the DTs and 2.3.3 challenges related to the technology.

2.3.1 History

Firstly introduced in a presentation for product lifecycle management (PLM) by Michael Grieves in the early 2002 [51]. However, implementing this technology required a lot of other improvements in various technologies, thus, it was considered as a complex procedure. The first usage of the DT was by NASA, in 2010, and it was used to mirror airspace conditions and then to execute test for flight preparation [94]. This delay for the implementation was due to the need of the improvement of numerous technologies like cloud computing, IoT and big data, machine learning (ML) and artificial Intelligence (AI). These technologies are so important because they can improve the work of the DTs at all. For example, the cloud computing and the IoTs can provide better connection between all the devices that are connected in such an environment, will provide quicker updates on the data received from the sensors and will improve the quality of the DT. With other words, it will promote a higher scalability, adaptability and interoperability. On the other hand, the ML and the AI technologies can help with the training data and validation data sets. Therefore, they can be used to gain better solutions for some future implementations by analyzing previously gathered data and what will be the outcome of them, to overcome the challenges with the significant developments, testing and validations, and to make decisions and suggestions on how to improve processes.

2.3.2 Specifications

DT technology gives the opportunity to fully represent potential physical device or a process. Additionally, the device or the process can be already existing one. The DT concept is divided into three types - Digital Twin Prototype (DTP), Digital Twin Instance (DTI) and Digital Twin Aggregate (DTA) [51, 52]. Where the DTP is when the digital twin exists before the manufacturing of the product, usually contains processes, engineering designs, proper analysis and a visual representation. For example, a prototype can be a new engineering design of a car model. The DTI is basically every digital representation of each instance of the manufactured product. For instance, digital instances can be a thousand cars of the same model, e.g. NIO ET5 model, in a factory. Lastly, the DTA is used when the DTIs data is collected and information about the physical product, prognostics, and learning is queried, e.g, an aggregate of the thousand NIO ET5 instances. Digital twin technology aims to combine the twinning, simulation, real-time monitoring and analysis in order to achieve its goals. Thus, the integration of this technology can save cost, time and resources for prototyping a product or improving already existing ones. In addition, it is considered as one of the top technology trends for previous years[62].

2.3.3 Challenges

There are still multiple challenges related to the DTs and this is mainly because it rely on sensors, IoT, AI, ML and Big Data, as we mentioned earlier. There are cybersecurity concerns around the technology, the IoT security is quite important and it is hard to achieve high level security in all the devices and domains, and the security of some industrial partners. An example challenge is that if there is a security breach in an IoT device, then, the DT can be exploited, too. In addition, data handling (AI, ML and Big Data) is a big challenge for the technology, because the large organizations are collecting data from plenty of IoT devices which results a huge dataset in various dimensions. Thus, the big data has a challenging task to preprocess the input to the machine learning. There are various other challenges like the use of new types of sensors or multimodal sensors,the integration of legacy sensors, evaluating the uncertainty for new sensors, the integration of a huge number of sensors with variety of sensors, continuous collection of a real-time sensor data, the validation and the verification of heterogeneous models, and the uncertainty for the quantification in the development of the models and their integration [9]. Additionally, there is huge number of opportunities around DT technology, especially in the recent years when the technology growth increased enormously. For example, there is a need of a general definition of DT, which will help to clarify its concept. Initially, in the presentation for the PLM by Michael Grieves, it was defined as "conceptual ideal for product lifecycle management (PLM)“ which was referenced in Grieves et al.[51]. Then, in the same paper, the DT definition evolved as "Digital Twin is a set of virtual information constructs that fully describes a potential or actual physical manufactured product from the micro atomic level to the macro geometrical level.“. Recently, Guo et al. [53], reviewed multiple definitions for DTs such as "DT is a comprehensive multi-physical, multi-scale, probabilistic simulation system for vehicles or systems. It uses the best physical model to describe the historical use of equipment to reflect the life of its corresponding physical equipment“[47] or "A DT is a digital representation that contains the feature description of its selected object or its product and service system, and obtains the attributes, conditions and behaviors of the object through models, information and data in a single or even multiple life cycle stages“[117]. In addition, the large usage of IoT devices in the DT, opens room for further research on IoT standards and improvement in the authentication. Lastly, the need of a framework is huge opportunity for researchers, because in that way, the designed framework will be easily managed by programmers and developers for various domains.

[9] https://neutronbytes.com/2022/02/14/challenges-and-opportunities-for-nuclear-digital-twins/

3 Related work

In this chapter, there will be a comprehensive survey of plenty already published surveys and proposed authentication schemes for the IoT environment (from the early 2008 to 2022). The section will be separated into multiple domains: 3.1 for the smart healthcare, 3.2 Internet of Vehicles (IoV) systems, 3.3 smart grids, 3.4 industrial environments, 3.5 Wireless Sensor Networks (WSN), 3.6 cloud environments and lastly 3.7, surveys and authentication protocols used for multiple domains. Our motivation to cover these domains is because the DT technology is deployed mostly within these environments. For instance, the DT can be used in smart manufacturing in order to simulate a car construction before really doing so or to simulate an upgrade of a vehicle. This gives the manufacturer the opportunity to know if this construction or modification will be efficient or not. In addition, a literature review will be conducted related to the DT technology in general, definitions and current state-of-the-art, the security aspects and related issues to it. It will be separated into two categories: 3.8 DTs literature with focus on the security and 3.9 DTs literature without focus on the security.

3.1 Authentication for the smart healthcare systems

In [90], the authors proposed a simple architecture machine-to-machine (M2M) service that can be used in any hospital. In addition, they applied a dynamic ID-based authentication scheme which use pairwise key distribution. Then, the work in [102] is discussing the secure remote user authentication, which is a technique where the remote server authorizes the identity of the user over an insecure network channel. The authors of the paper presents an analytical and comprehensive survey of various remote user authentication techniques and classified them in different applications. In addition, they explained the state of the art of the recent user authentication techniques, compared them, their advantages, key features and computational, storage, and communication costs. Another proposal for real-time healthcare was given in [37]. The authors did a review of previous work that has been done and they proposed a new scheme. Due to the fact that the real-time healthcare information and data collection are very crucial and important, they need to have a sophisticated secure protocols and encryption schemes. However, they also need to be lightweight, because the IoT devices and sensors are usually resource constrained. There is an explore for data modification during the data transmission through the insecure wireless sensor networks. Therefore, they proposed such an scheme and gave the following key aspects that needs to be considered while designing a new authentication schemes for the IoT and the healthcare apps:

1. In a sensor-based scenario, the most important thing is to make the scheme lightweight, to build an exchange amid protection and utilization of the power;
2. The scheme must be protected under multiple attacks like sybil, node capture, password guessing, replace, MITM, DoS, etc;
3. The messages interconnected between the verification parties must be as small as possible, because of the power constraint factor.

In [71], the authors proposed a procedure known as Efficient-Strong Authentication Protocol that is proposed for the wireless healthcare applications. It consists of two phases - two-factor verification,e.g., smart card and password, justification between the sensing devices and also encoding technique that will ensure the confidentiality of the messages. Since the Internet medical things are quite sensitive and one major tool used for maintaining the security is the biometric technology. Therefore, the authors from [54] proposed a new standard for applying such an biometric technology for smart healthcare using IoT. Their method enhanced the smart healthcare security by the biometrics and fast identity standard. Chaudhary et al.[23] proposed another efficient technique, a modified Block Cipher Technique (MBCT), that was designed in combination of one Matrix Rotation, XOR and the Expansion function. It was using 256 bit key length, 256 bit block plain text and 32 rounds encryption. However, the algorithm needs less processing time than AES, DES and SIMON. There is also a modified version that is using even less memory. In [57], the authors proposed a privacy-preserving cryptosystem for the E-health. It is an interesting technique for fast and safer authentication than the other currently proposed algorithms. It is named as Chaos-based PRNG encryption that is meant to maintain patient data confidentiality. It using one set of confusion and diffusion processes, and a new PRNG based on Zaslavsky's chaotic and 2D logistic. Another interesting lightweight protocol was proposed in Suganthi et al.[118]. It is an end-to-end mutual authentication protocol used for the healthcare. In addition, it is mainly focused on the security and privacy protection of the patient data, which is quite important in such environment. In addition, in [12], the authors proposed an provably secure lightweight authentication protocol. It is an improved AKA scheme for Wireless Body Area Network (WBAN) and they employ BAN logic for the security analysis and the ProVerif for the automated simulations. In [129], the authors proposed a multi-factor mobile based user-to-device protocol in order to provide even higher security. In addition, user uses a username and password, and biometric information in order to verify itself. Lastly, in [36], the authors proposed a seamlees authentication framework with privacy-preservation (SAF-PP) protocol for the IoT in the e-Health. This authentication system is using lightweight encryption operations like hashing and MAC verification, which provide lower computational and communication overhead. In addition, the authors made a formal analysis that proved their proposal has sufficient security properties and it can increase the efficiency rate. Lastly, they executed another analysis to check the performance of the protocol which concluded that it is more efficient than other schemes, provide longer lifetime of the network and better transmission rate.

3.2 Authentication for the IoV systems

The IoV systems are quite important area, because if a hacker is able to intrude the vehicle network, he might be able to lead it to a crash. In addition, if an electric charger is hacked it can easily spread around huge network which can lead to terrible outcomes. Due to the rising number of EVs around the world and their adoption, there is a need of novel authentication designs and protocols and some improvements in the cloud and edge computing networks, too[10]. Therefore, we will cover various proposals that are using various authentication schemes in the IoV systems.

[10] https://news.bloomberglaw.com/privacy-and-data-security/electric-vehicle-infrastructure-push-brings-cyber

The usage of sessions keys will reduce the number of authentication steps while providing sufficient confidentiality. Therefore, the authors in [137] proposed an authentication scheme where the OBUs fully trust the RSUs, thus, the OBU needs to be authentication only. This lead to a huge drawback, because the RSU can control the route of the vehicle, when this method is used, and that leads to vulnerabilities. In [21], the authors have studied the secure and timely handover of IP services in an asymmetric vehicular ad-hoc networks (VANETs) and proposed a multihop-authenticated method with Proxy Mobile IP (MA-PMIP). This proxy provides an improved IP mobility scheme for the infrastructure-to-vehicle-to-vehicle (I2V2V) communications that uses the traffic and location information. Another proposal was given in [16], which is quite efficient because of its lightweight behavior and it is suitable solution for the EVs and the charging stations security concerns. In addition, the solution is a secure PUF-based authentication (SUKA) protocol for V2G systems where the Physical Unclonable Function (PUF) is used for two-step mutual authentication. Next given proposal in [61] was using zero knowledge proofs. It is an efficient multi-factor authentication that is being used for the vehicular cloud computing environment. Adversaries are not able to trace any vehicle, due to its good privacy preservation mechanism. Then, another paper that proposed a novel, lightweight, adaptive group-based zero knowledge proof authentication protocol (AGZKP-AP) was published [104]. The protocol is offering multiple options for level of privacy and the user is able to make this critical decision of what level to use and what amount of resources to be used. An efficient survey related to the vehicular systems was provided in [130]. The authors presented state-of-the-art of the vehicular cloud comping and a taxonomy for the vehicular cloud with focus on the cloud formations, key management, cloud systems for inter communications, and various security and privacy problems. As a result of this survey, the authors designed an architecture for VCC and emphasized some important features required for the vehicle cloud to support their model. In [79], the authors found an efficient way to gain sufficient level of vehicle privacy protection in the VANETs using the anonymous authentication. They proposed an algorithm that is based on vehicle group signature authentication which is a proper solution for vehicle networks. It works as follows: the vehicle joins a group, then the administrator of the group is generating a certificate for the vehicle in order to sign messages without changing other vehicle keys or certificates in the group. If the vehicle exit the group, then the administrator is responsible to prevent the left vehicle to continue be able to use the group membership. With other words to destruct the certificate that was made for the vehicle authentication. In [6], the authors proposed an authentication system that applies multiple security algorithms in order to improve the authentication in the VANETs. It uses a four stage cryptography methods - challenge and response authentication, digital signature, timestamps and encryption/decryption. In addition to this, they designed a framework and an algorithm model, then implemented a challenge and response authentication scheme. At the end, they provided some measures and evaluations for the implementations. In addition, other interesting work was published in 2017 by Vijayakumar et al. [126]. In the framework proposed by the authors, there is a prover that generates a MAC using a shared secret key, then the verifier is verifying the prover using this MAC and then receives the message that needs to be transmitted. it is using anonymous privacy preserving approach and keeps the vehicle user's anonymity while authenticate and also improve the message integrity while transmitting messages. In addition, they executed an experimental analysis that output promising results for the efficiency of the authentication regarding the verification and the computational costs. In [78, 88], the authors propose a ring signatures for the authentication. In order to generate a signature, the signator need to receive the public keys of all the participants and use them with his own secret key. In that way, the verifier does not know who is the signer, but he knows that the signatory is one of the list with legal users. The main downside of this method is that there is a need for the keys of all vehicle owners, thus, the risk of exploitation is increasing. In [58], there was a suggestion for a novel distributed key management system for group based VANETs. The protocol is forming groups with vehicles located close to the RSUs and they will be responsible for distributing private keys of the group. It is expected the proposed protocols to be able to identify compromised RSUs and their collusion with the malicious vehicles, if there are any. In addition, they executed a security analysis and demonstrated the performance of their proposal with regards to various possible attacks. Then, in [135], the authors proposed a novel authentication protocol scheme that is using a sub-tree method to achieve better revocation in order to provide greater forward security. In addition, their aim is to cope with some concerns like privacy challenges and the ones for the increased workload of the remote authority. The proposed scheme has enhanced features like forward security, CCA2-anonymity, traceability, non-frameability and unforgeability. In addition, they are using a decentralized approach for the group model, thus, the whole VANETs domain is separated into multiple sub-regions. An interesting clustering proposal was given in [8]. The authors are using algorithm based on the Graph Classification Method with Attribute Vectors (GCMAV) and its purpose is to longer lifetime, improved rate of the information delivery, reduce the overload and to optimize the global criterion. In order to handle the security and performance challenges, they are using a urban VANET (UVANET) environment and an efficient key management scheme that is based on symmetric and asymmetric cryptosystem. Lastly, the authors did a simulations with realistic scenarios and using the Open Street Maps for better results. Lastly, the authors reviewed a proposal of authentication system that is using an optimized signature generation and verification protocol that is based on the lattice cryptography [24]. Using the lattice theory problems allows all of the signatures to be produced based on asymmetric encryption. The advantage in here is the reduction in the length of the blind signature and reduction in the generation time of the signature by 18% and 30%, respectively. Despite that, assessing the complexity of the lattice algorithms is a significant drawback, in other words, there is no formal proof of security.

3.3 Authentication for the Smart Grid systems

In [27], the authors proposed a scheme that is used for the application layer of the IoT. The protocol is used for the authentication of the power usage information for smart grid (SG). To reduce the total traffic volume in the communications, the scheme allows gateway smart meters to help to filter messages before they arrive at the control center. For the authentication it is using RSA with SHA hashing algorithm or MD5. However, the authors do not consider the DDoS attacks. Then, a lightweight message protocols was provided in [81]. It is used in both, the application, and the network layers. It is a hybrid Diffie-Hellman based lightweight authentication scheme using AES and RSA for the session key generation. The scheme provides integrity using the advantages of hashing and ensures the mutual authentication. Although the scheme is reducing the overall overheads for computations and communication, it is still proved to be resistant to replay attacks, MITM, message analysis and modification attacks. However, the authors do not consider the location privacy. In [74], the authors proposed a new one-time signature multicast scheme based on requirements that they identified during their work. This scheme is able to reduce the storage costs significantly and also to reduce the size of the signature almost by half. Therefore, the proposal is suitable for smart grid environments that have limited storage or where data communication is frequent and short. The scheme is separating the computation between the sender and the receiver, thus, it is reducing the overload. With this scheme, they are avoiding various attacks and one of them are forgery attacks. In [76], the authors proposed a lightweight design, which is used in IoT security assurance, ensures the secured broadcast of data and bi-directional authentication of the identities between the IoT devices and the terminals. The authentication of the terminal is executed by the protocol during the key agreement which increase the system's security over the SG. Another interesting proposal was using the blockchain technology for the smart grids and it was proposed in Wang et al.[128]. The authors discussed a blockchain-based AKA protocol for SG systems that is applying the edge computing technology. The protocol is able to synthesize efficient conditional anonymity and key management without the usage of complex cryptographic primitives. The security analysis that was execute shown that this method is a perfect candidate for the SG deployment. In [121], the authors proposed a lightweight PUF-based AKA protocol to strengthen the security of the SGs. The scheme was an end-to-end AKA protocol which is protected against physical, leakage, and other forms of attacks. In addition, the scheme is using reasonably lower computation and communication overheads. An ultra-lightweight and provably secure broadcast authentication protocol for smart grid communications was proposed in [1]. It is a novel protocol for AKA purposed and its concept is designed on unicast and broadcast technique using one-way hash functions which makes it efficient in terms of communication and computational costs. In addition, it is shown that the scheme is resilient against a variety of attacks. In [48], the authors proposed a Privacy-aware multi-factor authenticated key establishment (PMAKE) protocol for Advanced Metering Infrastructure (AMI) in SG. It aims to promote the security of the Smart Meter (SM) and it claims to be energy and processing efficient. Reza et al.[106] discussed a novel AKA security mechanism combining ECC and Salsa20 stream cipher algorithm in order to improve the security of the network system.The main benefit of this protocol is that it has a lightweight security and is energy efficient. Therefore the scheme is suitable for the adoption for SMs, because of the reduced power consumption together with less time for encryption/decryption.

3.4 Authentication for Industrial environments

In [33], the authors proposed an protocol called Optimization of Communication for Ad-hoc Reliable Industrial (OCARI) networks. It is a promising protocol for the WSNs, but it still had to be secured against various risks, especially the threats related to the confidentiality, data integrity and entities authentication. Then, another proposal for the M2M was given in [43]. The authors designed a lightweight authentication scheme to ensure secure integration of Industrial Internet of Things (IIoT) solutions. In addition, they used a scenario where the machine is equipped with Secure Element (SE) and is authenticated by a network element with Trusted Platform Module (TPM). The scheme consists of two phases - 1) registration phase and authentication phase, and it provides low computational cost, communication and storage overhead. In [49], the authors proposed a lightweight and privacy-preserving mutual authentication protocol was proposed for users. In this protocol, only the users with trusted devices are given the authority to access the industrial wireless sensor network (IWSN). The proposed protocol is using a lightweight cryptographic primitives like PUF, one-way cryptographic hash functions and bitwise exclusive operations which provides a physical layer security for the sensor nodes. The scheme is shown to be secured even if the nodes are compromised and it is efficient for resource-limited sensing devices in IWSN. Kumar et al.[70] released another proposal for a PUF-based protocol, but customized for the characteristics and deployment of IWSN. It was proven that the protocol is robust towards malicious security acts such as device loss, DoS attack and more. The formal security is done using the random oracle model and formal verification done by the ProVerif tool. In [115], another interesting proposal was made for a new lightweight user authentication key agreement scheme. The authorized users will be able to access the facilities from the designed IoT sensing devices mounted in the IIoT environment. For the purpose of the biometric verification, the fuzzy extractor is used, which is enhancing the privacy protection and the security of the biometric data.

3.5 Authentication for the WSNs

In this section I will mentioned multiple authentication schemes for the wireless sensor networks and the first one to mention is Wenliang et al.[38]. The authors provide a framework in which researchers can study the security of key pre-distribution schemes and propose a new pairwise key pre-distribution scheme, for WSNs, which significantly improves the strength of the network compared to other previous schemes. It is using a symmetric encryption and is resistant to node capture. However, the scheme uses slightly high energy cost to establish a key. In [77], the authors proposed a novel pairwise key pre-distribution technique using a general framework. It is establishing keys between sensors and the protocol is based on the polynomial-based key pre-distribution protocol [19]. This method is using symmetric encryption, too, and is token-based protocol used in the network layer of the IoT. This framework is resistant to node capture and has low communication overhead which makes it suitable for the IoT devices. However, the authors do not consider the locations privacy. Then, the authors in [124], proposed a novel user authentication and key agreement scheme for heterogeneous ad-hoc WSNs. It uses a lightweight key agreement protocol in order the remote user to securely communicate a session key with a general sensor node. In addition, it ensure the mutual authentication between three participants - a user, a sensor node and the gateway node (GWN). It uses simple hash and XOR computations, thus, it is suitable for resource-constrained WNS architecture. No matter the simple operations, the scheme has higher communication costs than other ones. However, the protocol is resistant to replay attacks, MITM attacks, impersonation attacks, privileged insider attacks, stolen smart card attacks, and so on. In [96], the authors provided an implicit certificate-based authentication mechanism for WSNs in distributed IoT environments. It is a two-phase authentication protocol that helps users and sensor nodes to authenticate each other and to communicate through a secured channels. In addition, it is sustainable with resource scarcity of the sensor nodes, heterogeneity and the scalability of the network. That makes this method resistant to DoS and malicious users attacks, but there is high memory consumption for the certificate authority (CA) operations and it is not resistant to node capturing attacks. For the multi-gateway WSNs, the authors from [116], proposed a unique authentication and key agreement scheme for WSNs which is using biohashing. This technology is eliminating the false accept rates without increasing the occurrence of the false rejection rate. The scheme is using dynamic node addition and there is a friendly password change mechanism for the users. They also proved that the scheme provides mutual authentication using the BAN-logic. Lastly, they executed an informal security analysis that proved the scheme is secure against MITM attacks, replay attacks, spoofing and gateway impersonation, using the AVISPA tool. However, according to the El-Hajj's conclusion, the authors of the papers have not considered possible wormhole and blackhole attacks. The proposals in [34, 111] were using the biometrics of a user, e.g., the fingerprint. This scheme requires the users to register their biometric data with the BS before they can access the data from the servers. It consists of four phases:

1. Pre-deployment phase where the BS is assigning a unique ID and generates a special master key for each sensor in the network;
2. registration phase is where the user is providing its biometric data and a password to the BS. This is done in the secure channel. After receiving the data, the BS is generating a master card by hashing the provided biometric data and then sends it back to the user;
3. This phase is the login of the user where he/she enters his smart card and the biometric information to the terminal device;
4. If the login from the previous step completes successfully, then the BS authenticate the user and he/she can use the requested service.

Multiple ID-based authentication techniques were proposed in [86,92,107,110,123], which are similar to the biometric based scheme. However, in these the user is registering just credentials to the BS and again receiving an smart card that will be used for the next verifications. One of the techniques [107] is using two phases - offline and online. In the offline phase the general parameters and the public key of the BS are stored in each node, then a trust value is generated for each node and after completing this, the second phase comes into play, which is the mutual authentication. In [136], the authors proposed another one-way authentication scheme. There are two offline stages included in this method. It requires these stages in order to preload network nodes with sensors IDs, private keys, and the master key. All the sensors are generating also a trusted value and store them on the BS. Afterwards, another two stages are performed which are online - registration and authentication. This scheme differs from the previous ones, because here the trust values are generated by the nodes and not by the BS. Then, Chung et al.[32], suggested an improved lightweight scheme, that provides hop-by-hop authentication and untraceability using anonymous features, was proposed [32]. The authors used one-way hash functions and XOR operations in order to be used in capability-constrained devices like roaming service in localized domains of WSNs and sensor nodes. In addition, the scheme is robust to key compromise and node capture impersonation attack, but the location privacy is not considered. In [65], the authors proposed a scheme called PAWN, which stands for payload-based mutual authentication, and it is extremely lightweight solution for cluster-based hierarchical WSN. It also consists of two phases - 1) token-based cluster election and 2) payload-based mutual authentication. Afterwards, in [50], the authors provided a verification procedure that will be used in the WSNs. It will be able to offer a protection of various characteristics like confidentiality of the user, unreachablity, backward privacy and forward privacy. This one is flexible under node confine and key imitation attacks. The last proposal that will be reviewed is a user verification method with 2FA-based design for WSN [35], which is using passwords and smart cards. The scheme is protected from masquerade, stolen-verifier and node imitation attacks.

3.6 Authentication for the Cloud environments

This section will be focused on proposals for authentication protocols for the cloud environments. Thus, in [44], the authors proposed an efficient and scalable solution such an environments. There are two distinct servers that stores the authentication and cryptography resource from the main servers in order to reduce the costs for the main servers. There is a client-based user authentication agent to confirm the identity of the user in the client-side and a cloud-based SaaS used to confirm the authentication of the unregistered devices. The registered ones are authenticated using AES and the non-registered ones using Diffie-Hellman. Therefore the protocol makes the environment resistant to MITM, brute-force and timing attacks. In a International Conference on Circuits, Power and Computing Technologies work, the authors of [114] proposed a secured and more advanced multi-tier authentication scheme than the previous ones. It consists of two tiers - the first one is the verification of the username and the password of the user, if the verification is completed successfully, then the authentication is forward to the second tier. Its main purpose is to allow the user to enter a registered and predefined sequence of events like a mouse activity or a menu. This protocol is used for accessing cloud services and it is said to be resistant to replay attacks. However, the authors do not consider the DoS attacks. In [25], the authors presented an ID-based mutual authentication that is based on ECC. It consists of three phases - initialization phase, registration phase and the last mutual authentication phase. In the initialization, the general parameters are chosen by the AS. Then, in the registration the AS calculates the user's smart card based on the selected parameters and the user password, then sends it to the user. At the end, the mutual authentication is executed between the AS and the user using the smart card and the password. Yang et al.[132] proposed an ID-based authentication technique, which includes three roles - the user, the target server and the ID provider server. The user is communicating with the target server through the ID provider. Initially, the user is sending his ID together with the ID of the target server. Then, the ID provider is hashing these IDs and the output to the user and the target server. Afterwards, there is a mutual authentication step that consists of one-way hash and XOR operations, in order to establish the communication between the authenticated user and the target server. There are also inter-cloud authentication proposal in [97, 101]. In the first one, from the [97], there are linked distributed cloud systems that will interoperate and provide their resources to the users. Each cloud should register its service to an inter-cloud management server using a Single Sign-On authentication scheme. On the other hand, the second one [101], is using a hierarchical model that is based on the user identity. This identity is used as authentication of the users throughout multiple clouds. In [17], the authors proposed a mutual authentication scheme that beats the problems with the traditional cryptography solutions, relying on the PUFs. It introduces the special integrated circuits, uniqueness, unclonability and tamper-evident characteristics. Then, they also published an interesting additional mutual authentication scheme based on PUF that is using cloud automated framework with fog nodes and resource-controlled IoT device [18]. It is proposed in the form of as-a-service and it is easy to setup. A survey for the mobile cloud computing (MCC) was released [9]. The authors presented a comprehensive survey of the authentication methods in MCC and compared it with the cloud computing. In addition, they did a comparison based on five evaluation metrics and they conclude that there is a need for futuristic authentication methods. Lastly, they discussed various open challenges based on the weaknesses and strengths of already existing authentication schemes. In [140], the authors provided a survey on lightweight authentication for cloud computing and discuss a novel lightweight verification scheme that is using a two-factor based authentication based on the XOR and one-way hashing operations. In result, the efficiency is enhanced, the scheme removes the computation burden and also make the scheme a proper solution for resource-limited devices and objects. In addition, the authors used ProVerif in order to ensure the robustness of the security of the authentication scheme and did a performance evaluation that shown the computational cost efficiency.

3.7 General authentication protocols for IoTs

This section will initially begin with the papers that were made by my superviser, Mohammed El-Hajj, and his team. Starting with the first paper [40], its aim is to provide an analysis of the various authentication schemes that were proposed till then. The authors used a multi-criteria classification, that is comparing and analyzing the existing protocols, and they provided a figure that describe all of criterias in their paper. This criteria will be also suitable for the DTs used in the IoT platform, because there is huge usage of IoT devices, therefore since it can help us in the IoT, then it will be useful when integrate the DTs in the IoT platform. We can have different types of authentication factors, deployment time, methodology, distributed/centralized authentication techniques, flat/hierarchical, etc. Furthermore, the authors explained the advantages and disadvantages of the proposal they reviewed. The following summary was taken from their analysis:

- Yanling et al.[138] did a research on the data security technology in IoT and proposed a protocol that was used in the Application layer of the IoT architecture. The credentials were encrypted and the benefit of this protocols was the packet encapsulation used to reduce the overhead of the data resources;

- In [68], the authors introduced the first two-way authentication based on Datagram Transport Lyaer Security (DTLS). The protocol is used in the Application and the Network layers. The scheme is using an asymmetric encryption scheme, namely RSA, that is designed to work with communications that are using UDP/IPv6 networking for low power wireless personal area networks (6LoWPANs). The protocol comes with its strength - low overhead and high interoperability, but the drawback is that the use of UDP over DTLS can lead to unreliable communications;
- In [56], the authors are proposing a protocol used in the Perception layer of the IoT. It is a proposal for a robust Wireless Sensor Network (WSN) lightweight mutual authentication protocol and the method design is using asynchronous symmetric One Time Password (OTP) with a Challenge/Response mechanism. As the previous one, there are benefits and drawbacks. It is beneficial that the scheme is resistant to replay attacks and some DoS, but the authors do not provide a performance measurement with comparison to other schemes. A bit more about this work will be given later in the literature review;
- Wenliang et al.[38] provides a framework in which researchers can study the security of key pre-distribution schemes and propose a new pairwise key pre-distribution scheme, for WSNs, which significantly improves the strength of the network compared to other previous schemes. It is using a symmetric encryption and is resistant to node capture. However, the scheme uses slightly high energy cost to establish a key;
- Another asymmetric, public key infrastructure (PKI) encryption proposal is made for securing and governing the access in ad-hoc networks of IoTs[98]. It is a framework for authentication, authorization and access control for an IoT environment, and is used in the application and the network layers. The framework is using capability tokens and the PKI, which aims to use low computing power and makes it a nice candidate for the IoT. It is resistant to malicious entities, because of the PKI, but the authors did not provide performance measurement;
- Ning et al.[63] proposed a security framework for the IoT based on the PKI. It is used in the application and the network layers. The framework aims to solve the security problems in the communication between the client operation and the server operation. The beneficial outcome from the work is that the compatibility problems are solved, but there is no performance measurement provided;
- Zhen-Qiang et al.[131] proposed a novel transmission model of IoT that is using a trusted computing technology. The protocol is resistant to attacks, data confidentiality, access control and client privacy. In addition, it is used in all the three layers - application, network and perception;
- A lightweight authentication protocol is proposed, which encryption method is based on a symmetric encryption with XOR manipulation[72]. It avoids the usage of complex encryption, like hashing, and it is used for anti-counterfeiting and privacy protection. The protocol is used in the network and perception layers of the IoT and uses authen-

tication of Radio-frequency identification (RFID) tags with readers. RFID uses smart barcodes that are attached to items and people use it to easily identify them by using radio frequency technology. With other words, there are radio waves that transfer the information from the data to the reader which then transmits the data to a RFID program;

- Turkanovi et al.[124] proposes a novel user authentication and key agreement scheme for heterogeneous ad-hoc WSNs. It uses a lightweight key agreement protocol in order the remote user to securely communicate a session key with a general sensor node. In addition, it ensure the mutual authentication between three participants - a user, a sensor node and the gateway node (GWN). It uses simple hash and XOR computations, thus, it is suitable for resource-constrained WNS architecture. No matter the simple operations, the scheme has higher communication costs than other ones. However, the protocol is resistant to replay attacks, MITM attacks, impersonation attacks, privileged insider attacks, stolen smart card attacks, and so on;
- In [134], the authors propose an efficient authentication and access control scheme that is used in the network and perception layers. Its advantage is that the establishment of the session keys is based on Elliptic Curve Cryptography (ECC) and this enhance the mutual authentication and the intermediate processes between the user and the sensors. In addition, it solves the resource constraints in the perception layer;
- The authors from [112] proposed an optimized two-way authentication scheme for tiny devices (TinyTO) that combines the end-to-end secured communication with WSN design. The protocol is using fast and secure handshake that works with ECC public key cryptography for the message encryption and authentication, thus, it ensures the confidentiality and integrity. In addition, the ECC reduces the resource consumption;
- Pawani et al.[96] provided an implicit certificate-based authentication mechanism for WSNs in distributed IoT environments. It is a two-phase authentication protocol that helps users and sensor nodes to authenticate each other and to communicate through a secured channels. In addition, it is sustainable with resource scarcity of the sensor nodes, heterogeneity and the scalability of the network. That makes this method resistant to DoS and malicious users attacks, but there is high memory consumption for the certificate authority (CA) operations and it is not resistant to node capturing attacks;
- In [22,42], the authors proposed a protocols that are used in the application layer of the IoT applications and they are using Access Tokens and OAuth2.0 protocol. They provide one-way authentication and it is going through TLS. Their strength is to be resistant to replay and impersonation attacks, but the authors did not provide a performance measurement;
- Another interesting proposal, that is efficient and scalable, is made for cloud computing environments[44]. There are two distinct servers that stores the authentication and cryptography resource from the main servers in order to reduce the costs for the main servers. There is a client-based user authentication agent to confirm the identity of the user in the client-side and a cloud-based SaaS used to confirm the authentication of the unregistered devices. The registered ones are authenticated using AES and the

non-registered ones using Diffie-Hellman. Therefore the protocol makes the environment resistant to MITM, brute-force and timing attacks;

- Yang et al.[133] provides a token based protocol that is used in the perception layer. It is an RFID-enabled solution that aims to protect the endpoint devices in the IoT supply chain. It enables data transfer from tag memory to centralized database for authentication once it is deployed, as an advantage of the connection between RFID tag and the control chip of the IoT devices. It is resistant to split and one-to-one mapping attacks, but the location privacy is not considered;
- In [15], the authors propose a novel continuous authentication protocol for the IoT, which is based on a secret sharing scheme (SSS). It provides secure and efficient authentication for continual transition of messages in a short session time intervals. Using the novel SSS, the secret is considered as an authenticator and the shares are used as authenticator tokens. They provided a performance evaluation which shown that the protocol is lightweight in respect of computation and communication costs, therefore, it is suitable for resource-constrained IoT devices. The protocol provides resistance to MITM, DoS and eavesdropping attacks, but has a high storage cost;
- In a International Conference on Circuits, Power and Computing Technologies work, the authors of [114] proposed a secured and more advanced multi-tier authentication scheme than the previous ones. It consists of two tiers - the first one is the verification of the username and the password of the user, if the verification is completed successfully, then the authentication is forward to the second tier. Its main purpose is to allow the user to enter a registered and predefined sequence of events like a mouse activity or a menu. This protocol is used for accessing cloud services and it is said to be resistant to replay attacks. However, the authors do not consider the DoS attacks;
- Jian-Zhu et al.[80] demonstrate multiple vulnerabilities on two previously proposed biometrics-based authentication schemes that are using smart cards. Then, the authors provide an enhanced scheme that aims to eliminate all the identified security flaws of the previous schemes. The proposed scheme has a second-tier authentication that is done at client-side and also resistant to inside attacks. However, the credentials cannot be changed in both tiers, which is a drawback of the proposal;
- In [29], the authors proposed an identity authentication scheme, for the application layer, that is based on public key encryption using ECC. The authors did simulation with OPNET and it proved that the protocol to be safe and effective, thus, it makes it resistant to DoS and MITM attacks. However, the drawback is that the users must authenticate multiple times in a distributed multi-server environment;
- The authors from [27] proposed a scheme that is used for the application layer of the IoT. The protocol is used for the authentication of the power usage information for smart grid (SG). To reduce the total traffic volume in the communications, the scheme allows gateway smart meters to help to filter messages before they arrive at the control center. For the authentication it is using RSA with SHA hashing algorithm or MD5. However, the authors do not consider the DDoS attacks;

- The last two papers are used in both the application, and the network layers. An hybrid Diffie-Hellman based lightweight authentication scheme using AES, and for the sessions key generation - RSA, was proposed in [81]. The scheme provides integrity using the advantages of hashing and ensures the mutual authentication. Although the scheme is reducing the overall overheads for computations and communication, it is still proved to be resistant to replay attacks, MITM, message analysis and modification attacks. However, the authors do not consider the location privacy. On the other hand, in [116], the authors proposed a unique authentication and key agreement scheme for WSNs which is using biohashing. This technology is eliminating the false accept rates without increasing the occurrence of the false rejection rate. The scheme is using dynamic node addition and there is a friendly password change mechanism for the users. They also proved that the scheme provides mutual authentication using the BAN-logic. Lastly, they executed an informal security analysis that proved the scheme is secure against MITM attacks, replay attacks, spoofing and gateway impersonation, using the AVISPA tool. However, according to the El-Hajj's conclusion, the authors of the papers have not considered possible wormhole and blackhole attacks.

We can see that there are some enhanced proposal for authentication protocols, but there are still some vulnerabilities that needs to covered, like MITM attacks, replay attacks and so on, and the need of general framework is appearing to be important. The second work provides, a second survey of different authentication schemes and then compares and analyzes the protocols showing their advantages and disadvantages. The reviewed works are provided in the same tabular way and they can be seen in the paper[41]. The authors concluded that a research and development has already started and is performed by the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF) to re-engineer the existing technologies and to enhance them. However, there is still a room for improvements in the security and the energy consumption of the proposed techniques, and for sure there have been many enhancements in the recent years and there will be a review of some recent works. Then, the third paper[39] provides a summary of large range of authentication protocols, compares and evaluates them by showing their strengths and weaknesses using a multi-criteria that they introduced in previous work [40]. Lastly, the authors provided a number of requirements and open issues that the developers and researchers needs to take into account while developing new authentication schemes for the IoT environments:

1. The authentication protocols must be proven to be secure against multiple attacks like sybil, replay, brute-force, message forgery, node capture, DoS and DDoS, MITM and so on;
2. The location and identity privacy is an important feature that needs to be ensured, especially for smart grids (SGs) and vehicle ad-hoc networks (VANETs);
3. Since most of the devices are resource-constrained, the communication and authentication overhead is a key factor for the protocols. The number of messages should be kept as low as possible, as well the size of these messages, because we can have also a restricted bandwidth. Such an example are the sensor-based applications;
4. In relation to the previous requirement, there is a need of a lightweight cryptographic

algorithms and protocols, because of the computations costs that are required for the naive schemes;

5. Designed authentication schemes need to be scalable, because the IoT environments usually require the managing of large amount of nodes and also adding new nodes is very common;
6. The authentication service should be ensure for the three layered IoT architecture;
7. While designing the authentication schemes, the developers and researchers need to consider the heterogeneity of the devices in the IoT networks;
8. The usage of PUF is an emerging trend and the combination between software solutions and hardware solutions is an efficient way to ensure lower cost and security.

These papers were quite useful for further researches and improvements in the already implemented protocols. The rest of this section will continue with other works that seems to be useful and will be ordered by year, as mentioned earlier.

In the following paper[31], the authors give a security model for multi-server environment, proposing an ID-based mutual authentication and key agreement scheme based on bilinear maps for mobile multi-server environment. There are few encryption schemes that were made for multi-server environment and none of them is suitable for covering the user anonymity, which was a big drawback at these times. The authors discussed schemes that were made to achieve the user's anonymity, but these were for a single server environment. People needed something like single sign-on (SSO) to access multiple environments with only 1 account (authentication). The proposed scheme from the authors was implemented with three phases - setup phase, extract phase and the mutual authentication and key agreement phase (MAKA). Lastly, the authors provably demonstrated that the scheme is secure against user impersonating and server impersonating attacks, as well as provides forward secrecy. In addition, they have demonstrated that the proposed protocol is well suited for multi-server environment with low-power mobile devices. In [139], the authors used a custom data packet encapsulation mechanism, reducing the overhead of data resources. In addition, the authors focused on the 4-layer architecture of the IoT security and connected the security of each layer as follows: in the application layer we have the privacy security, in the supporting layer we need the information processing security, the network layer consist of the information systems security and lastly, the perception layer is responsible for the security of the information collection. In [46], the authors presented a comprehensive survey of authentication protocols for IoT systems. In addition, they started with reviewing all the existing survey articles, then, review the threat models, countermeasures, and formal security verification techniques used in the IoT authentication protocols. Moreover, they provide a taxonomy and comparison of authentication protocols for the IoT in form of tables, divided into the four categories mentioned above - M2M, IoV, IoE and IoS. At the end, the authors discussed the open issues in all the areas that were covered, including the pattern recognition and the biometrics in the IoT. The authors of [109] also performed a survey of IoT authentication techniques which were proposed previously. The aim of the paper is to help the other researches to dive more into the details of such techniques through the classification and comparison. The classification is made as distributed vs. Centralized, flat vs. Hierarchical, and number of authentication levels among others. They reviewed authentication schemes that cannot fit a constrained devices, but they also have their benefits. In addition, they investigated other proposals that specifically aim the resource-constrained devices, too. However, they found that there is a possibility for some security attacks like forgery, DoS, and stolen smart card attacks in the provided proposal. Therefore, they recommended other researchers to focus on distributed and hierarchical approaches considering the aforementioned security attacks. In *Park et al.*[91], the author provided an cryptanalysis of another proposed authentication scheme and found that it does not provide sufficient security for WSNs and fails to provide proper password updates. In addition, the authors demonstrated that the proposal has lack of forward secrecy, vulnerable to password guessing attack, etc. Therefore, he proposed a security-enhanced authentication and key agreement scheme, that uses a biometric, and it aims to overwhelm these security flaws. It is using fuzzy extraction and an ECC encryption. In order to fulfill the needs for security and the usage in the constrained IoT devices, It uses simple ECC operations, hash functions and exclusive OR (XOR) operations. The scheme was proposed in 4 phases - registration phase, login phase, authentication and key agreement phase, and password change. In addition, the authors proved that it withstands the security attacks described in the paper and provides better security functionality than previous schemes by using biometric information and ECC. In [20], the authors provided an efficient overview of IoT authentication techniques. The main outcome from their survey is that the mutual authentication is crucial for the IoT and the lightweight option will be very useful with networks with low bandwidth. In addition, after the review, they concluded that a combination of a various encryption and authentication methods might be an efficient way for the other researchers to explore a more secure and lightweight solutions. In [30], the authors proposed the first PUF based AKE protocol for IoT without verifiers and explicit CRPs, where the IoT nodes can freely authenticate each other without the need of any server or verifier. They also compare the proposed protocol with 27 relevant PUF based AKE protocols to show the efficiency of the protocol. In addition, they define the adversarial model of a PUF based AKE protocol and formally prove its security. Lastly, the security of the protocol is based on the Elliptic Curve Discrete Logarithm (ECDL), Elliptic Curve Computational Diffie-Hellman (ECCDH) and the Decisional Bilinear Diffie-Hellman (DBDH) assumptions. A proposal for smart home (SHome) was provided in [10], where the authors have decided to cover the security of the IoT devices in SHome. Initially, the authors shows a general model that is extracted from a use-case scenario in SHome environment. Based on this model, authors executed a threat analysis in order to find possible attacks which will help defining a set of beneficial security requirements for the design of authentication mechanisms for SHome. Lastly, based on these requirements, they will analyze some existing authentication proposals and will suggest some ideas for efficient authentication schemes in the IoT environments. In [122], the authors perform a comprehensive empirical survey with a comprehensive literature review. In a result, the readers can gain in-depth understanding of the various authentication schemes and the related vulnerabilities and drawbacks. Afterwards, on the basis of the determined limitations, they will recommend various strategies to mitigate them and will discuss the practical ramifications of the findings. As we understood from recent studying, there is a need of lightweight encryption and now we will review such a survey [103]. The authors discussed state-of-the-art lightweight cryptographic protocols and presented a comprehensive analysis. The main goal is to answer the following questions: 1) What lightweight cryptography has been developed to address the many IoT security issues?; 2) How can lightweight cryptography secure an IoT structure?; What consequences do the findings have on the future of IoT research?; Then, they concluded that a lightweight protocol is required for the IoT networks in order to secure the resource-constrained devices. Therefore, it could be great opportunity for the researchers to focus on reducing the key size, usage of dynamic key, decreasing the block size, introducing more straightforward rounds and designing simple key schedules. Another comprehensive survey was reviewed in order to get even more knowledge and it was recently publiced [82]. The PUFs are essentially lightweight, secured and privacy preserving. They are categorized as lightweight, because they are very efficient for IoT devices - faster runtime, less power consumption and less memory usage. Thus, the authors reviewed the PUF authentication protocols that already exists, with respect to the following three focused areas: PUF user authentication key agreement for IoT settings, PUF user authentication and key agreement for WSNs and PUF user authentication and key agreement for SGs. In result, the authors noticed that there two limitations around the PUF-based AKA protocols - the majority of the schemes are vulnerable to PUF modeling attacks and the other one is the rising temperature on PUF-embedded devices that leads to performance issues. Therefore, these boundaries could be a good starting point for future researches. In [125], a student from the University of Twente made quite efficient comparative study on the lightweight authentication protocols in IoT environment. The author, considered various metrics in order to investigate and analyze the recent lightweight authentication protocols elected by NIST like AM and ROM occupation, gate area, latency, throughput and energy consumption. The main disadvantage of most authentication protocols is the use of symmetric and asymmetric encryption systems to ensure high cryptographic strength. As a result, there is a problem in delivering keys to the sides of the prover and the verifier. At the same time, compromising of keys will lead to a decrease in the level of protection of the transmitted data. Zero-knowledge authentication protocols (ZKAP) are able to eliminate this disadvantage [28]. In [55] authors provided a bubbles of trust mechanism. It is a decentralized solutions that ensures a robust identification and authentication of the devices, and protects data integrity and availability, using the security advantages provided from the blockchains. The system is using the Ethereum blockchain and serves to create a secured virtual zones, called bubbles, where devices can identify and trust each other in order to communicate securely. In [87], the authors proposed a scalable lightweight mechanism for the authentication of resource-constrained devices and they presented a demo to prove that. It is an identity-management system with a lightweight consensus authentication mechanism. They used a private blockchain solution based on Ethereum smart contracts, which actually improves the speed compared to other public blockchain-based solutions. The usage of blockchain and smart contracts provides a reliable level of security with scalability. However, the private system is still a contrary to the principle of decentralization and further improvements in the blockchains' speed and the number of transactions per second might give more room for the researchers to use the public solutions. Lastly, in [2], the authors concluded that there is a challenging task that the protocol designers face and that is to build a mutual authentication scheme for smart environments based on radio frequency identification. In addition, previously introduced mutual authentication protocols for the closed-loop systems and the open-loop systems rely on a centralized database but they fail to address decentralized mutual authentication and their related attacks. Therefore, they decided to propose two decentralized mutual verification protocols for IoT systems. The first one is for closed-loop RFID systems (CLAB) and the other for open-loop RFID systems (OLAB). In the meanwhile they examine the security of the Chebyshev authentication algorithm and confirm that the algorithm is unprotected against tag and reader impersonation attacks. Moreover, the authors proposed a blockchain network that comprises of multiple connected nodes. There is a block for each transaction receiving from tag which is handled by the corresponding reader and server. Then, they are using PoS consensus method to manage the blocks (local Ethereum blockchain network).

After reviewing all the surveys, literature and the proposed authentication schemes, I think there is still a need for some improvements in the current implementations. We can see that there are some enhanced proposal for authentication protocols, but there are still some vulnerabilities that needs to covered and the need of general framework is appearing to be important. In addition, the blockchain technology started to get a lot more attention in the recent years and it can be an efficient solution for the authentication in the IoT environments.

3.8 Digital Twins literature with focus on the security

This section will be focused on papers that are gathered to provide good understanding of the Digital Twins and also their security aspect, known gaps and issues related to that. In [14], the main resources, that the authors used, came from an overhead crane ’Ilmatar’, including its interface and a 3rd party IoT platform, that was located at university premises. They analyzed, presented and gave recommendations based on this Ilmatar project and built a multi-component DT for an industrial overhead crane. This DT was developed as an integration of multiple systems and stakeholders, based on what the authors explained. The authors found that there is a demand of a coordination work in building digital twins using the current tools. Thus, the lack of efficient tools is the main problem in the integrated DTs development. In addition, the authors reviewed the Application Programming Interface (API) usage and found that a user-friendly APIs, e.g, to have easy to use interfaces and understandable documentation, can significantly accelerate the development of the application and they can be set as a prerequisite when building innovative applications. Furthermore, such an APIs will also need user-friendly and secured authentication which will be quite useful feature that will provide security and confidentiality. The APIs are used to fetch the data in and out of the DT core and various operations can be made, like create, update, delete and read. Additionally, there are standard Structured Query Language (SQL) operations executed to the database and analytical operations of the DT core. Thus, each query is secured via security policies and is authenticated whenever needed. However, using efficiently such APIs might require new skills that need to be learned from the workers like understanding of what can be obtained with APIs, improve the technical know-how to use the APIs and how they can benefit from them, and lastly, they need to improve their skills to provide APIs as service to the other employees. Additionally, the authors think that there is still room for improvements in the security solutions before the public Internet can be used in DT environments. Lastly, they described the integrated DTs concept and considered eight DT related hypotheses which are:

1. DTs are able to transform the data from a physical object into a useful digital knowledge, and they can offer this data to all stakeholders throughout the whole product lifecycle;
2. DTs are able to integrate the digital models and the data from various providers and sources which can offer a customized overview of the product;
3. DTs are enabling the business and the networking, e.g, the APIs can be the networking and if they are efficient a business, they can be used in there;
4. DT can provide useful data that can redefine the machine design dimensioning and the product development processes in a positive direction;
5. Nevertheless that the only use case was the overhead crane located at university, it provides industrially relevant applications like plugging DT as a product configuration, design and life-cycle management;
6. One of the most important features of the DT is that it can behave as an interface for all Industrial Internet data, which enables the enormous amount of data to be efficiently used;
7. Using APIs is exploring the 'developer culture' from the 'software world' to the 'physical world' which enables faster product development cycles;
8. DT does not require to be built by selecting a central visualization and simulation model.

And also there were two limitations of the paper and the first one was that their study could pose a risk of researcher bias, thus, they decided to show all the matters that do not go well during the study in order to avoid such risks. And the second limitation is that the authors were mainly concentrated and obtained information of one industry-university project. Additionally, discussed limitations of the integration were not very user-friendly APIs as a whole, such as the Postman API that was mentioned in the paper, the need of a purposeful use case is also important thing that is usually overlooked, the need of freely accessible open standards and some traditional payable standards, and lastly, many companies avoid open-source software which is quite unique because of its feature to benefit of a community creation and developer friendliness.

The study in [93] organizes the existing studies on DTs and the authors focused on the enablers and the barriers related to the technology. In this regard, the authors developed a framework by the categorization of DT barriers and enablers, and the connection of the barriers and enablers. The barriers were categorized as follows:

- System integration issues, e.g., lack of system integration and difficulties in ensuring interoperability;
- Security issues, e.g., security and privacy, difficulties with ensuring data transparency and protection of the IP;
- Performance issues, e.g., difficulties to ensure low latency and efficient communication, and the analysis of the large volumes of data;
- Organizational issues, e.g, lack of expertise and specialists, and difficulties to ensure centralization and standardization;

- Data quality issues, e.g., data unavailability, data validity and data ownership;
- Environment issues, e.g., difficulties to choose the correct software for simulation and virtual testing, and lack of education on the topic at universities.

These barriers are indirectly connected, thus, the environment barriers can affect the organizational factors and that will lead to an impact on the system integration, system and data security, and data quality. Then, the impact will spread on the DT development, which will lead to effects on the DT performance. On the other hand, they categorized also the enablers:

- AI, e.g, ML, big data storage, processing and analytics;
- IoT/IIoT, e.g., sensors and actuators;
- VR/AR, e.g., virtual/augmented reality;
- Hardware, e.g, high computational power, resource visualization and decreasing hardware costs;
- Communication technologies, e.g, OPC-UA, 5G/6G networks, MQTT, MTConnect, network visualization and the seamless data transfer between the lifecycle phases;
- Knowledge building, e.g., dynamic knowledge bases and upskilling of the workforce;
- Design processes, e.g., asset modeling, autonomy and decentralization of DTs, and rapid individualized design;
- Development technologies, e.g., blockchain, virtual machines and open-source software.

By understanding the enablers and the barriers, the authors were able to connect them. For example, the AI, VR/AR and the development technologies are said to be capable to mitigate the development issues. For the security issues, the authors mentioned that the Blockchain can be an effective solution to provide security and transparency through the advanced cryptography that it is using, because the data security is significant concern in every industry sector. Currently, these issues are minimized by the usage of communication protocols like Open Platform Communication Unified Architecture (OPC UA). This is an open-source cross-platform standard that is approved by the International Electrotechnical Commission (IEC) - IEC62541. It is developed to provide secure communication (security and integrity), real-time performance and reliability, integration and interoperability between productions and IT systems. Thus, this standard has the ability to offer a secure communication between the DTs - the data confidentiality and the information exchange is secured using the OPC UA where the messages transferred between the devices are encrypted. In [105], the authors proposed the Six-Layer Architecture for Digital Twins with Aggregation (SLADTA) extension to the Six-Layer Architecture for Digital Twins (SLADT) that helps for the aggregation of multiple DTs. This helps multiple digital twins to communicate with each other. It consists of 6 layers, which are:

1. Layer 1 - a layer with the devices and the sensors;
2. Layer 2 - this layer consist of the data sources which are usually controllers, e.g, in the construction these are the Programmable Logic Controllers (PLCs), or in my case this is the Raspberry Pi;

3. Layer 3 - a layer with the local data repositories;
4. Layer 4 - this layer contains the IoT gateway;
5. Layer 5 - a layer with the cloud-based information repositories;
6. Layer 6 - this layer consist of the emulations and the simulations.

This system provides the required characteristics of modularity, flexibility and aggregation that can be re-configured. In addition, the architecture allows the ability to control the access to the information, hence, there is ability to prevent the access by one DT to confidential data in another, and when instructions are send from higher level DTs, then each level of DT will implement a safeguards. In this new architecture, the communication of the DTs is restricted to only their respective data repositories (Layer 3). This restriction helps the aggregation to be done using software with great cybersecurity mechanisms like OPC UA. Lastly, the decision-making is encapsulated to the data that is available for each DT. In [64], after reviewing plenty articles in the field of construction safety, involving sensor and visualization technologies, the authors were able to describe the state-of-the-art of these systems. In addition, they found out that the DTs, combined with sensors, visualization technologies and IoTs, are providing the capability to synchronize construction activities automatically, which can help the improvement in the construction workforce safety. Moreover, the authors were able to identify and describe a few challenges by using the sensor and visualization technologies. The main ones are challenges related to the information processing and synchronization:

1. A lack of methods that are able to synchronize a complex and dynamic information of the construction;
2. The information that is processed is limited when working with complex logical relationships between objects, hazards and safety rules;
3. There is still unclarity related to the mechanism that is going to be used to provide the safety information, and warnings, to the on-site workers.

Because of all the benefits that are already mentioned, the DT technology becomes quite attractive for the businesses. The concept allows companies to analyze and upgrade their systems, and implement new designs. However, the interest in the technology also raises a lot of new cybersecurity challenges. Therefore, the authors in [62] explore the risks related to the Cyber Physical Systems (CPS) that are using the DT technology and it will also enable distributed remote control of industrial assets, which will place an increasingly heavy burden on IoT identity management, authentication and authorization. Some previously executed attacks are the BlackEnergy malware attack in 2015 directed to an utility provider in Ukraine [85], cyber attacks on multiple US pipeline companies for natural gas in 2018 [5] and Darkside Ransomware as a Service (RaaS) attack directed to the Colonial Pipeline in US [127]. Here are also some security challenges that the authors provided:

- If the communication between the DT and the physical asset is not properly secured, then an adversary can take advantage of this and to introduce a divergence in the state or the behavior of the digital twin or the physical representation, or even both;
- If there are some confidentiality concerns created by the use of a DT, an adversary will have the opportunity to easier learn trade-secrets;

- The possibility of a Cyber Digital Twin (CDT) to contain various security configurations of a whole Information and Communications Technology (ICT) or Operational Technology (OT) infrastructure and if an adversary is able to gain some control, this will expose all the data for the configurations and the attacker will be able to implement zero-day attack, for example.

Despite these security concerns, the authors consider ways to mitigate the cybersecurity risks by using the DTs, which will include them as an important part of cybersecurity defence. If the DTs and CDTs are applied, they can provide considerable opportunities for security improvements in critical infrastructures. For example, CDT technology is able to provide the opportunity to a cybersecurity professional to exploit tool automation and AI to simulate and assess possible attack scenarios which will help for protecting the physical infrastructure. Another study for the cybersecurity for the DTs is published, Alshammari et al.[11]. The authors reviewed multiple significant papers related to the IoT technology in the built environment and they analyze the recent practices. Additionally, they show how the IoT can be used to improve the construction and the living experience of the residents. Furthermore, they discussed the role that the DTs play in the various CPSs, from physical objects to information models. Lastly, the authors provided guidance on how the Building Information Modelling (BIM) specifications can be enhanced and to be more compliant with the IoTs, how the DTs and the city standards can be integrated, and how to improve the cybersecurity in order to have secure environments. Architecture, engineering, construction, and facilities management (AECFM) industry has adopted BIM as a new stage in the expanded digitalization of built environment data. Example if BIM is an information model that is used in the built environment.

In [119], the authors discuss the integration of the DT technology and the blockchain technology in order to cover the issues with the management and the security in the IIoT. These issues are covered into two steps:

1. Provide trustworthiness for the data sources and the data transit
   a) Prevent device tampering - using the blockchain's public keys and digital certificates, the sensors, gateways, and other types of digital equipment are required to register as approved devices on the chain.
   b) Prevent data forgery - to achieve this prevention, the authors rely on the provenance data and the twinned data.
   c) Identify malicious entities - first, to meet the International Organization for Standardization (ISO), there is a need of regulatory bodies which can periodically provide inspection of the entities to issue or revoke the certificates for participation; second, categorize the participating units by given reputation rating that is based on the trust valuation. Then, one can implement a punishment system that will reward the honest entities and will punish the dishonest ones.
2. Provide distributed, decentralized and secure data storage - this is covered by using a tamper-proof and immutable ledger of the blockchain where the essential data is stored (provenance data, models data and the DT data). By using a permissioned blockchain,

they aim to enable the coexistence of the transparency and the privacy in order to execute confidential data flows and to avoid espionage. Additionally, the authors defined policies that gives access only to units within the organization.

Additionally, they want to address the difficulties of the distinct data repositories, dishonest transfer of the data, and the fault diagnosis. For this purpose, they proposed a framework that aims to address the challenges of data management, data security and predictive maintenance in IIoT. It consists of three layers - application layer, storage layer and data layer. In the data layer we have the physical space and the devices, and also the DTs (the virtual space) where the sensory data, the history data and the domain knowledge are gathered. Then, this data is forwarded to the storage layer where the data is stored and analyzed. This layer contains the lightweight, scalable and quantum-immune blockchain technology that is used in the framework. Lastly, the analyzed data is forwarded to the application layer, which consist of control units, remote offices and data analysts. The framework address technical and non-technical challenges. The technical ones are separated into infrastructure, data management, data security and performance categories:

- Infrastructure - Avoiding a failure in centralized architectures and providing distributed and decentralized infrastructure for widespread industrial units; scalability - the system have to be able to handle the increasing number of actors, like sensors, actuators and equipment, and activities, like processes and trade events; deployment of robust IoT solutions which can help the recovery from various failures, like accidental and malicious, without taking down the data or service availability; deployment of automation technologies that will be used to speed up the processes in IIoT;
- Data management - there are challenges related to the data collection and the collation from distinct data sources, to organize and determine the types of data and the data transparency;
- Data security - challenges with the data trustworthiness that needs to be ensured, the confidentiality of sensitive data, the integrity between the different parties of the lifecycle and distribute the data accessibility and auditability based on ownership, roles and levels of access;
- Performance - challenges to maximize the system throughput, to ensure a deterministic and reliable data transfer, real-time analysis for scenarios sensitive to latency, to optimize the energy usage of resource-constrained devices and to provide freshness of data.

The non-technical challenges are related to the cost management, upgrading of the legacy systems and the risk management which aims to identify risk events and activating preventive and proactive plans like fault diagnosis, aging management and predictive maintenance, in order to mitigate the identified risks. For example, the risk events can be deterioration of the equipment, outage, shrinkage and natural disasters. Additionally, the authors discussed the challenges that can be addressed via the integration of the DT and the Blockchain in the IIoT. For example, the anomalies with the diagnosed data in the system can be detected based on digital-physical mapping in DTs. This is connected with the technical issues related to the trustworthiness of data sources and data in transit. Another example will be for the distributed, decentralized and secure data storage challenge which can be addresed by the blockchain technology.

In [120], the authors analyzed possible sources of data breaches and possible attacker perspectives. Some possible attacks are the reconnaissance attacks which involve the collection of data intelligence. The adversaries are able to achieve such attacks by exploiting zero-day vulnerabilities, network scanning and service enumeration to identify some security loopholes. For instance, there were some attacks like the Triton malware that succeeded to gain access to the IT/OT networks of a petrochemical plant in Saudi Arabia and targeted the Safety Instrumented Systems (SIS). In addition, the Stuxnet malware in 2010 [83], demonstrated how one can overcome some air gaps and the target was an Uranium enrichment plant. Lastly, the inappropriate security level of the communication channels between the DTs and the physical assets can provide significant advantage to the adversaries to exploit a system. In regards to the security concerns, the authors also provided some countermeasures. The DT data is used as an input in most of the assets and CPS physical processes, therefore, a DT must have secured and trusted data. A possible technology for this can be the blockchain technology, because this will allow the companies to handle the data on a distributed ledger which will ensure a trusted DT data coordination between various stakeholders. A list of the solutions that could mitigate some of the identified attacks: 1) Orchestrating provenance; 2) Securing lifecycle data; and 3) Use of smart contract. Additionally, the authors found that the gamification can provide better security for the DTs. They proposed a gamification approach which gives the opportunity for twin evaluation and learning environment for the security analysts. Such an example for gamification are the Capture-The-Flag (CTF) challenges. Lastly, the authors provided a couple of security techniques that can limit the damage of an exploited DT:

- Using intelligence-driven solutions like data analytics or threat intelligence, which will help to collect data on the attackers' behaviors;
- Implementing a blockchain-based solutions track and trace the DTs which changed some simulation parameters or state data;
- Developing a system that is fault-tolerant, which will help to not shut down the whole system, but it will steadily close parts of a system until it enters a fail-safe state.

Thus, it seems that the gamification really can help to improve the field and it can be achieved even with some fun. The authors in [60] focused on the importance of the security in the DT platforms and how to harden its software. The aim is to provide safety for both the DT and the physical asset or system that it monitors. This paper also reviewed some possible vulnerabilities and then provided a methodology that can be used when developing a new system, but some of them might be used also for companies that already have working products. The first step is to have a clear and well-defined secure software development lifecycle (SDLC) management process. It will include the whole lifecycle from the beginning to the retirement of the system. Then, there is a need for comprehensive requirements or goals in order to start the project. They should include security requirements for sure and they have to be understood properly, to be specific and measurable. Additionally, a good security testing in the early stage is highly beneficial. Then, the implementation phase can begin with agreed design, test and the security specifications. In the best case scenario, the tests will be automated. For example, automatic scripts that are scanning the source code for language compliance, code style, and known flaws and vulnerabilities. In addition, if the team can implement fuzzing and penetration testing, whether possible, then it should be employed. Lastly, any third-parties should also be secured properly, otherwise this will cause risks, no matter how secure the system is. Thus, some techniques that can lock the software and the data to particular machines will provide extended protection. Lastly, the hardened APIs are a must in nowadays applications, because almost every system or application is working with APIs. In [7], the authors found that some researchers described the DT definition in three separate aspect classifications, while reviewing the literature. The first one was focused on the identity, the nature and the structure of the DT. Then, the second was the aim, the purpose and the function of a DT. And lastly, the third one, is related to the main constituents of a DT, like components, elements or aspects. Additionally, they reviewed and analyzed the preceding literature, related to the DT technology, but there is still no consensus for one specific definition for the DT, but it is clear that the core features of the technology are the bi-directional connection with the physical world and the intelligence of a DT. These capabilities are enhanced by taking advantage of the new comprehensive technologies like AI, Big Data and ML, which gives huge potential to various technologies to explore the usage of the DT technology. Moreover, the authors noticed some challenges that come with the DT technology. They categorized them as: 1) Open Data challenges and 2) Other Challenges. In 2), they mentioned the main challenge that is related to the main pillar of DTs, open data - how the data can be shared, integrated and made accessible throughout numerous entities and sectors. There are different aspects related to this challenge like technical, contractual, commercial and cultural issues. On the other hand, in 2), we have challenges like the connectivity of DT in a system(s), the security of the data provider and the DT, the privacy for the data sources and the users, and inclusiveness. Through appropriate data protection procedures, the source's security as the data provider and the security of the DT's vast data pool and federated models are both guaranteed. Data security is strongly tied to the security of DT users, who may rely substantially on the company's services. The privacy is related to how to preserve proper privacy levels across all users and data sources in order to protect individuals and commercial rights. A state of the art paper was published [113] where the authors reviewed work that has been already done and defined their DT reference model which is based on these previous works, including important components. Such components can be defined as the core of a DT, like bijective relation between DT and the physical asset, transfer of the info, IoT, data analytics and ML. As DTs include many sub-components, there is a need of developing regulations and security mechanisms in order to widespread the adoption and to overcome the difficulties in the data sharing. ML is a technique that can be useful in this direction. However, no matter that the DT is a powerful tool that combines simulation, autonomy, ML, big data, agent-based modeling, prototyping and optimization, this is one of the drawbacks of the technology. The reason is that the DTs are directly connected to the enhancement level of these sub-components, or sub-technologies. Additionally, the DT technology operates for multiple industrial partners and inventory sites which makes the security issues unavoidable. A corporation may be in danger from both cross-industry security concerns and the release of real-time monitoring data. In [67], the authors had a couple of goals that were achieved with this work:

- To clarify the terminology and to identify the similarities and the dissimilarities between the DTs for cities and 3D city models;
- To present various examples of DTs for cities;
- To discuss how the DTs for cities can be used for several perspectives like modelling, visualization, simulation, citizen participation and planning for the urbans;
- To determine what are the challenges for the future developments and the implementations of DTs in cities.

In order to achieve these goals, they examined the terminology for the DTs for cities, how this terminology has evolved in the academic context and described some essential characteristics of DTs for cities. In addition, they presented an overview of some important examples of DTs and presented the main applications of DTs for cities. Lastly, they succeeded to find some challenges related the technology like security, privacy and accountability challenges, integration and multidisciplinarity, and market readiness and collaboration. For example, if a big city starts to use DTs that will serve as the main authoritative platform of the city, the public and political acceptance are going to be crucial for the success of this. However, in this case the security and privacy of the DT will have significant concerns. For instance, which part of the data should be open, what people or systems will have a legitimate access to it, and what privacy framework will be used for this. The review of these challenges is out of the scope of this paper [67], but we are going to give an example for security concerns. Imagine that a huge city integrates DTs, therefore, there will be a flow of huge amounts of data that should be collected from numerous endpoints. The main concern here will be their security and the other one will be when there is a new connection to the twin, because this can increase the chance for compromising, if the new connection has weak security or if it is a malicious one.

3.9 Digital Twins literature without focus on the security

This section will review the literature that was collected to gain additional information related to the Digital Twins, but without clear focus on the security aspects. The first paper that we will discuss is the "The impact of smart materials, digital twins (DTs) and Internet of things (IoT) in an Industry 4.0 integrated automation industry“ [100]. The authors provided some applications where the DTs can be used, such as in the aircraft industry, the production systems that collaborate with human-friendly robots and in the production management for product assembly. However, there are still issues that need to be considered like the risks for a collision or errors in the systems that are using collaborative human-friendly robots, also called human-robot collaboration (HRC) systems. In addition, they explained how the IIoT is able to benefit the producer-customer chain in various ways: 1) production lines can be customizable which will enable customers to search for a product for any particular need; 2) companies that are using IIoT are able to adapt to the changing demand in the market by using fewer number of production plants and to put less funds for different products; 3) the product manufacturing assigned to the RFID requires quite less professionals work. From these statements we can see how both technologies (DTs and the IIoT) can achieve synergy and this combination will enable some benefits - help to predict some assembly errors, to reduce the production costs and to help the improvements in the Industry 4.0. The authors from paper [53] aim to provide good understanding of the application status of the DT technology. They mentioned various applications where the technology is used in like modern medicine, smart cities, aerospace and the business. For instance, the DTs can be deployed perfectly in smart cities with the help of the IoT. The smart devices can provide all the data for the DT deployments of the smart cities. Additionally, with the information gathered from the review, the authors discussed the current development status of the DT and provided some future predictions for the development. For example, there is a need for some international common standards for multiple (or all) industries, that way the DT technology can become even more popular in the real production. Applying the technology to the industrial production can help the IoT, simulation technologies, Big Data and AI to be deeply integrated. In [75], the authors found that there is a lack of a comprehensive reviews that analyze the benefits of the DT in the emerging Product Lifecycle Management (PLM) and business environments. Thus, they conducted a state-of-the-art survey of DT by reviewing previous works. Additionally, the authors identify some future perspectives for the DT technology like modeling consistency and accuracy, incorporation of Big Data analytics in the DT models, VR integration in the DT, improvements in the simulations in the DT, expansion of the DT domains, the efficient mapping of the cyber-physical data and the integration of the cloud and edge computing. And more specifically, DT can be deployed in the production digitalization and with the help of the the IoT data can create simulations. For example, the DT technology can be used in the textile industry which can reduce the costs and to increase productivity by using IIoT data and analytical techniques. In [26], the authors proposed a novel IoT based methodology to build a digital twin of the fused deposition modeling (FDM) technology based on the additive manufacturing system in order to monitor the system through various side-channels. Example channels are acoustic, magnetic, vibration and power. Based on the signals from the side-channels, the authors provided a clustering algorithm that is used to generate a fingerprint library that can illustrate the physical status or the physical twin of the system. In addition, the authors proposed an algorithm for updating the digital twin and inferring the quality deviation. The digital twin modeling was performed on additive manufacturing system. The main devices that are used in the proposal are the IoT and the low-end IoT sensors, because they make it possible to model and maintain real DT system for product quality. As a conclusion, their methodology is able to update itself, infer quality deviation and localize anomalous faults in the additive manufacturing system. In [84], the authors defined that the DT can be a digital representation of simply any object, asset or product. There are variety of simulations that can use plenty data types like sensors data, business data and contextual data. However, the authors stated that this cannot be done without the help of the IoT and the Big Data technologies. The IoT enables the real-time data gathering and the Big Data is the dataset that contains large and complex data that is fetched from the IoT devices and the sensors. In addition, they found that, there is a lack of compliant planning systems and the available real-time data which leads to complications in the adaptations. Their work provides an extensive literature review of the current stage of the DTs, including analysis of almost five thousand searches with various DT keywords combinations. The main difference between the simulations of the digital twins and the other general types is that it uses three information types - sensor data, contextual data and business data, which is achieved with the help of the IoT and Big Data technologies. With the help of the DTs and the real-time information, the technology can help to make better and quicker decisions and to improve all the flaws that can also be detected a lot earlier. In addition, they concluded after the literature review that there are some issues that are need to be addressed:

- Information technology integration - there is a need of an interface for the data sharing and the continuous flow of results, that is user-friendly and efficient;
- Integration of partner companies - there is a need to have an efficient relationship between the businesses;
- Digital security and information rights - there is still need for improvement in this and the blockchain technology gives optimism to the community and the research working on solutions.

In [95], the authors introduced the White Label Digital Twins (WLDT), a general-purpose library that provides the opportunity to the developers to create DTs in terms of modular, adaptable, and interoperable software agents. This library is novel, powerful, modular and flexible solution. It supports various standard protocols, software processing pipelines, caching and monitoring of a selected metrics, which makes the library robust. Additionally, the main layer of the solutions is the "WLDT engine" that is defining the behavior of the digital twin and the active modules are denoted as Workers. A worker is used to implement a feature or task of a particular DT which can be associated with the synchronization between the DT and the physical counter part through an protocol like MQTT, HTTP, CoAP or WebSocket. These protocols can require authentication in order to be used, e.g., the HTTP protocol can be authenticated via username and password or via token, in order to make requests. Moreover, by using the implementation of dedicated modules, the worker can support legacy protocols in some particular IoT deployments. Lastly, it can be easily adopted which is used to create DTs for different applications. In [99], the authors employed a mixed method approach with which the they can investigate the value that the DTs can provide to the agriculture. Afterwards, they proposed a roadmap for the DTs in the agriculture based on the DT applications which can be used for future extension in the adoption. At the end, they identified the distinctive agricultural DTs' characteristics - operation streamlining, personalized curation of complex systems, permission level controls, information fusion, uncertainty quantification and human centered intelligence. Furthermore, while reviewing the literature and proposing the roadmap, the authors discovered two characteristics of DT in agriculture that differ from the other disciplines. The first one is that the most of the DTs in the agriculture include directly or indirectly living systems and products that are impermanent. For example, the plant DTs are such products. Then, the second difference is in the dimension that are used in the agricultural DTs. For example, they are ranging from individual plants and animals to DTs of farms, land parcels or regions, whereas in other environments they can vary between the size of an airplane to the size of a factory. In addition, the agricultural DT can require quite slower response rate of their DT compared to other systems. For instance, processes such as growing a plant require less frequent interactions between the physical and digital twins because the growing of a plant is comparatively slow. The information taken from the plant growing or any other agriculture activities can be only simulated and monitored properly when the DT is deployed with proper IoT devices and sensors that will provide the required data for all the processes.In [89], the authors did a review that aims to provide insights of the progress on the usage of the DT technology in the livestock farming. A digital twin can point to one physical device (theoretically), due to that, the DT has the ability to go beyond the constraints of most of the computer models. DTs are able to reproduce the changes of the physical assets in real-time with only some minimum delays like a microsecond to a couple of minutes. In addition, the DTs are able to collect and analyze significantly more information than the most computer models, which leads to the ability to make more realistic what-if scenarios. The traditional farming is based on weather and dynamic forecasts, human considerations, and the experience of the farmer. DT will be probably able to totally change this model by using real-time data, manipulated by the analysis of an AI system, which can lead to better business decisions, by improving the health and the well being of the animals, and to increase the return from the agricultural resources. In addition to these benefits, there is opportunity to take actions remotely and will not require to be always at the farm. The authors used a balanced approach and acknowledges in this paper and they provided the benefits from the DT technology and simultaneously discussed the limitations of its adoption that currently exists for the livestock farming. They concluded that the farmers need more evidence, facts and case studies related to the DT technology, in order to be encouraged to take a step into adopting it. In [73], the authors proposed an innovative framework, called Function-Structure-Behavior-Control-Intelligence-Performance (FSBCIP), that will show how the DTs are integrated into the Smart Manufacturing System (SMS) design. They came up with this framework with the help of the literature review that they have made. They fetched the data from a database called Web of Science and they separated the process into three phases:

1. Filtering related papers via keyword retrieving. With other words, they used two combinations, by two, keywords - "digital twin" with combination of "manufacturing system design" and "digital twin" combined with "manufacturing system planning". They retrieved 202 papers and 54 papers, respectively. However, there were some duplications and after the deletion they were 220 papers in total;
2. Identifying the high-quality theoretical works related to the concept, various key techniques, systems, models, frameworks and SMS design case studies. They finalized this phase by including 159 papers in order to reveal some key issues, challenges, new solutions and advantageous directions in the research of the usage of DTs technology in the SMS design process;
3. Finally, they presented statistics of the collected literature and described everything they explored in the previous section.

The authors of “Digital Twin: Finding Common Ground - A Meta-Review" [69], analyzed 24 previously published reviews that are concerning the DTs in order to identify common ground that most of the papers can agree on. At the end, the goal is to have a meta-review (a review of reviews) that will provide more structure to the straggling field of DTs. As a conclusion, the authors found that there are different terminologies and there is a lack of standardization in the conceptualization and implementation. They reviewed previous works and came up with understanding of the term and proposed a definition that is based on the majority-opinion of the considered reviews. The definition states the following: "A Digital Twin is a virtual representation of its physical counterpart. Its components provide the basis for a simulation or are simulation models themselves. The Digital Twin has an automated bidirectional data connection with the represented physical counterpart. This connection may span across several life phases of the system." However, they do not introduced a common understanding of the DT concept, but this definition will ensure the clarity and the precision of the DT terminology. Moreover, the authors found that the results of this meta-review are used for other larger research projects. The first one aims to explore the conceptualization, implementation and the use a standardization of the DT concept in the assembling production system environment. The second one is focused on the use of a DT in the logistics, which currently lack of popularity and there is no much work on it. In another meta-review [108], the authors managed to create a meta-review of 14 systematic literature reviews on DTs. The outcome of this was the important insights for the current state of the conceptualization, the reference architecture, the application areas and some directions for future research on DTs. They concluded that there are several essential implications for research and practice on DTs. Firstly, the conceptualization of DTs is determined by the area of the application that used for, which in the early usages was the smart manufacturing. However, there is a need of general understanding of the concept and they specified the DT as a CPS with physical and digital parts. Secondly, the conceptualization of DTs have to be expanded with additional properties like data models, accuracy, connectivity and synchronization. The reason for this is that the application areas where the DTs are used is also expanding to various environments like healthcare, smart cities, economics, business and logistics. Thus, there is a need of unified architecture and the authors provided such one with nine different layers:

1. Physical entities and the physical twin
2. Data generation
3. Network and connectivity
4. Data storage and data integration
5. Data preparation and data representation
6. Data models, algorithms, the virtual entity and twin
7. Micro-services and deployment process
8. System security and data privacy
9. Business model and processes

Finally, the authors provided distinct future directions for researchers, in eight separate areas:

1. Concept development
2. Business models
3. Integration

4. Data entry, data preparation, data augmentation
5. Big data
6. Data analysis, ML and simulations
7. Standardization
8. Security and privacy

After reviewing all this literature related to the DT technology, and proposals, we think the there is still much more room for improvements and there is still no specified framework, no specified regulations and the reliance on multiple technologies that need other requirements is a vulnerability that needs to be mitigated as much as possible. For example, a DT environment can be using multiple technologies like IoT, ML, AI and Big Data, which means that all of them need to be securely developed and configured, using the best security practices, otherwise there will be open rooms for the attackers to harm companies and corporations. However, we can see that researchers are increasingly looking for solutions, other proposals for fixing issues related to the technologies and new environments where the DT technology can be beneficial. Additionally, the vulnerabilities related to the data security, transparency and integrity, can possibly be reduced, or avoided, by using the blockchain technology, as we discussed earlier while reviewing some of the papers.

4 Methodology

This chapter is about to describe the methodologies that will be used in this work to answer all the sub-questions that will help to answer the main research question. They will be separated into three sections where each will briefly explain what we did in order to answer the respective question and then we will give more details on the experiment in Section 5.

4.1 Methodology for research sub-question 1

In order to answer the first sub-question for this study, we provided advanced overview of the current state of the authentication, how they perform in the various IoT environments and future direction for the other researchers. The review was separated by the domain where the IoT authentication is proposed to be used to and they are published in multiple years with the earliest in 2008 till recent ones from 2022. In addition, we are going to make a conclusion that will help us to understand how exactly the IoT and DT technologies work currently and what problems exists. Lastly, by analyzing the gathered data from the literature review, and the outcomes from the readings, we are going to be able to conclude some gaps in the current authentication protocols.

4.2 Methodology for research sub-question 2

This section of the project will be separated into two different parts: 4.2.1 Choosing a DT platform and 4.2.2 Deploying DT in an IoT use-case. These parts will help us to answer the second sub-question.

4.2.1 Choosing a Digital Twin platform

For this part of the project, we need to choose efficient platform for our Digital Twins environment. Therefore, we reviewed multiple simulation platforms before starting the implementation for the practical part and they can be seen in Table 4.1. In the table, you can see a brief overview of what features the Azure, Simio, Simul8, Simumatik and Ditto platforms have and do not have. Therefore, we decided to use Azure and more specifically, the Azure IoT Hub and Azure Digital Twins (ADT) platforms. Additionally, we came up with the following arguments, next to our summary in Table 4.1, in order to strengthen our choice:

1. Azure platform provides the IoT Hub and the Digital Twins - everything that we are going to need for the prototype;
2. It gives us the opportunity to have everything needed in one place - web portal, digital twins, IoT hub, custom self-signed or CA-signed authentication protocols, cloud storage, device visualisation, security, free trial and free resources with a usage limit and proper documentation.

   Additionally, the web portal gives us the ability to control everything in one place and also give us to execute code and commands in the Azure shell;

3. Azure Digital Twins (ADT) and the IoT Hub have only some basic requirements like to have installed python (or other language like node.js, C# or Java), openssl for the certificate generation and IDE to code the programs.

The other platforms are not so efficient and not that easy to setup, especially for our needs. The first one, that we started to research, was Ditto. After spending some time on reviewing and testing, we concluded that it is not very suitable choice, especially for the testing purposes of this thesis work, and the time that we have. The platform requires much more technical knowledge related to the IoT and how actually the whole infrastructure works, than the others. It requires to have multiple softwares and platforms in order to make your IoT environment to work. We followed a guideline[11] that initially required three applications - Docker, nginx and mongoDB, because we need to run them locally. The reason for that is docker needs to run multiple instances locally like docker_concierge_1, docker_connectivity_1, docker _gateway_1, docker_mongodb_1, docker_nginx_1, docker_policies_1, docker_swagger-ui_1, docker_things-search_1, docker_things_1. These all are required because we have to run custom API for the communication. Another platform that is used by Ditto is the eclipse mosquitto and there are additional configurations for this. Mosquitto is an open source message broker which is able to build on MQTT protocol. Additionally, Eclipse Ditto secures each API access to the managed twins by applying authorization of the authenticated user. Thus, we are required to define our own policies which are going to be used for all twins. By the tutorial mentioned above, the authors recommend using the 'The Things Network' (TTN) platform, which is a global IoT ecosystem that creates networks, devices and solutions using the LoRaWAN technology. Using this platform, we were able to create an application (network) and to add end devices in there. The connection of the app is established by application ID and API key and you can add multiple devices in there. Unfortunately, TTN supports LoRaWAN devices only, and the current tests are going to be made using Arduino MKR 1010 WiFi and Raspberry Pi 3 Model B, which does not cover the requirements.

To conclude, all the information above gives me insight that Ditto will not be that efficient in our case scenario, especially with all these services running locally and the custom API. Ditto is supposed to help companies that want to make a custom environment for the IoT devices they are using, e.g., for a smart manufacturing company.

The other platform that was reviewed was the Simio tool. It provides a 3D object-based modeling environment that is used for the construction of a 3D model in a single step - adding it in a 2D view and then you are able to switch to a 3D view of the model. This tool is quite powerful and useful, but it does not cover our requirements because it is mainly used for big environments like manufacturing, healthcare and packaging companies, and airports. Additionally, the data input is static and there is no bi-directional connection between the software and the devices. Therefore, this solution could not satisfy our needs.

The other options that were reviewed are the Simul8[12] and Simumatik[13], but they even do not have a free trial period for their software, thus, they are not suitable for the current project

[11] https://www.eclipse.org/ditto/2020-04-16-connecting-to-ttn-via-mqtt.html

[12] https://www.simul8.com/software/pricing

[13] https://simumatik.com/subscription-plans/

at all.

Platform Name	Communication Type	GUI	API	Custom authentication	Subscription
Azure	Two-way	✓	✓	✓	Paid (free trial)
Simio	One-way, static	✓	×	×	Free
Simul8	Two-way	✓	✓	×	Paid
Simumatik	Two-way	✓	✓	×	Paid
Ditto	Two-way	×	✓	✓	Free

Table 4.1: Digital Twin platforms overview

4.2.2 DT DEPLOYMENT IN AN IOT USE-CASE

In order to precisely answer this research sub-question, we decided to prepare a working scenario on the deployment of an DT and to analyze it. To achieve this, we decided to use the Azure IoT Hub and the Azure Digital Twins services. Additionally, we chose to use Raspberry Pi 3 Model B board as our physical device for the tests. We connected two temperature sensors to the board, then it is reading and passing their information to the IoT Hub, which updates the DT properties. This setup will provide us with good overview on how the physical device is communicating with DT, how it authenticates and how the DT can also send back data to the physical device. More details for the whole process on the setup, diagrams how the whole environment is working, the results and discussions on the results will be provided in Section 5.

4.3 METHODOLOGY FOR RESEARCH SUB-QUESTION 3

This question is related to the authenticity of the DT or with other words, how the physical device and the DT are authenticating. For the verification of the devices, Azure provides three authentication types with different options:

1. Symmetric key - this option is based on symmetric key encryption algorithm which is pre-built in the Azure platform. It generates the key using Hash-based Message Authentication Code (HMAC) using SHA-256 cryptographic hash function. This key is included in the connection string that is generated automatically in the following form: “HostName=<IoT-Hub-name>.azure-devices.net;DeviceId=<device-name>;SharedAccessKey=<HMACSHA-256-key>". The connection string is used in order to be able to connect the physical device with its digital twin;
2. X.509 Self-Signed certificate - this one requires to have already produced primary and secondary X.509 fingerprints that are representing SHA-1 or SHA-256 hashes of the X.509 certificate that is already generated and signed. Azure requires size of 40 hex characters and 64 hex characters for SHA-1 and SHA-256, respectively;
3. X.509 CA Signed certificate - this one is a CA authentication based on a full chain and

it is using a hierarchical list of all the certificates needed to authenticate the device, e.g., the root certificate should be the one of the IoT Hub. This option provides us the opportunity to use RSA or ECC (ECDSA with SHA-256 hash function) algorithms for the certificate generation.

We analyzed all the options and we have decided to evaluate the symmetric key and the X.509 certificates. The first one was automatically generated symmetric key, by Azure, using HMAC with SHA-256 hash function. Then, for the certificates that we generated, we used ECDSA and RSA algorithms with SHA-256 hashing function for the signing In our experiments, in Section 5.4, you will be able to see the comparison between the different authentication options with the two boards we used for this. We can clearly see that the certificates work quite slower, but sometimes they can require less energy. Additionally, in theory, they are much more secure than the symmetric key. For more details on the different encryption algorithms, you can navigate to Table 4.2, where you can see an overview of all the options and algorithms with their pros and cons. Additionally, we evaluated both types of authentication, which gave us the opportunity to compare them, by measuring the power consumption and the execution time. In Section 5, we are going to provide more details on the whole evaluation process which gave us insights and a good understanding of how the authenticity is ensured.

Authentication type	Benefits	Drawbacks
Symmetric key	simple low cost straightforward use	shared private key easy to have bad practices [14]
X.509 certificate at general	very secure high-level control common use by vendors	rely on external vendors costly solution if logistics is complex, the certificate lifecycle management can be a challenge[15]
RSA	well established based on factorization problem simple & fast [15]	not scalable[16] vulnerable against quantum computers and brute force attack[16] slow key generation[16] high resource consumption[16]
ECC (ECDSA)	smaller key & certificate sizes less computing power, memory and bandwidth easier implementation resistant to brute force[16]	vulnerable against quantum computers not fast as RSA in some environments[16] require special adjustment[16]

Table 4.2: Authentications overview

[14] https://azure.microsoft.com/en-us/blog/iot-device-authentication-options/

[15] https://www.ssl2buy.com/wiki/rsa-vs-ecc-which-is-better-algorithm-for-security

5 Experiments

This chapter will deeply explain our experiment that we prepared in order to answer the second and the third sub-questions that aims to provide better understanding for the main research question. It will be separated into three different sections as follows: Section 5.1 will describe the setup that we prepared for our experiment and the comparison between all the boards that we have used; then, Section 5.2 will provide better understanding on how the authentication works in our simulation and will provide good overview via sequence diagram; with Section 5.3 we want to briefly clarify the communication between the physical devices and the DTs and to show the output from the terminal and the Azure overview; Section 5.4 will show the results that we received from the applications that we implemented and the results from the measurements for the power consumption and the execution times of verification of the different authentication option for both boards, the Raspberry and the Arduino. Additionally, we measured the completion time for the generation of the X.509 certificates using ECDSA and the RSA hashing algorithms; Lastly, in Section 5.5 we discuss the results that we extracted from the experiment.

5.1 Experiment Setup

As we mentioned in the previous section, to precisely answer the other two questions, we decided to prepare a working scenario on the deployment of an DT and then to analyze how the physical device will authenticate to the DT. In order to achieve this, from the arguments given in Section 4.2, we decided to use the ADT services. For the project, we started to work with Arduino Nano which was the initial physical device for our tests. The communication was made in the following way: the board is sending message to the desired COM port, a middleware program (application service) is reading the data from the COM port and then passing this data as telemetry to ADT. Then, we decided to add real data, thus, connected two temperature sensors to the Arduino board. Both temperature values were properly read and passed to ADT. The communication was done via MQTT network protocol and, at that point, the device was authenticated by using a symmetric key, that is generated using HMAC with SHA-256 hashing algorithm. Then, the key is included in the connection string that is passed to the Azure libraries when connecting to the client. Each device is using a different connection string, therefore, separate keys. After executing a couple of simulation and discussion with the team, we came up with the conclusion that this scenario is not ideal, because we had this middleware program that is placed on the Windows machine and is reading the data from the COM port, instead of communicating directly with the board. Additionally, it is way better to create an IoT Hub, add the digital devices in there and then communicate with them. This is because we have the opportunity to manage a well organized Hub, with all the Digital Twins in there, instead of just having the DTs. This way we have better structure (IoT Hub > Device 1, properties; Device 2, properties, ..) and this way we add additional layer of security, because when connecting to it, you will have to authenticated with the IoT Hub and then to the devices (there is also a connection between the root certificate, which is the IoT Hub certificate, and the certificates of the physical twins). Moreover, we changed the device to a

Raspberry Pi 3 Model B board, replacing the Arduino Nano, which gave us the ability to have direct communication from the Raspberry to the Azure and vice versa. The Azure IoT Hub is a managed service which is hosted in the cloud, where all the data is stored, and it acts as a central message hub for the communication between the IoT applications and its attached devices. We are going to use it in order to connect our physical sensor devices with the DT devices. In Figure 5.1, you can see a component diagram with detailed information about the setup. It shows all the processes that are executed during the communication between the Raspberry Pi and the temperature sensors, all the applications and the Azure services. You can see that we are using X.509 Digital Certificates that are kept on the IoT device. They are used for the authentication of the device and we are going to give more explanation on how exactly that works in Section 5.2. Then, we can see that we have two temperature sensors connected to the Raspberry board and we have separate certificate for each of them. When the device application authenticates the sensors with the X.509 certificates, there are two outputs - working IoTHubDeviceClient connection or empty connection that will cause error for failed authentication. However, if the clients are authenticated, then the data from both of the sensors is formatted as reported properties (json format) and sent to the Azure IoT Hub which will then update the Digital Twins that are related to the physical sensors. We also activate a twin patch handler event which will wait for any changes of the desired properties, which are usually updated from the Azure or via backend program. In our case, we have backend program that authenticates with the connection string, which contains the private key, of the IoT Hub and also connects the sensors via their digital twin IDs. When they are not authenticated successfully, then the IoTHubRegistryManager is not initialized and an error will pop up. However, if authentication is done successfully, then the desired properties are being updated and this will fire up the twin patch handler that was activated on the IoT device. The program is implemented also to show where the sensors are hosted and which are connected via WiFi.

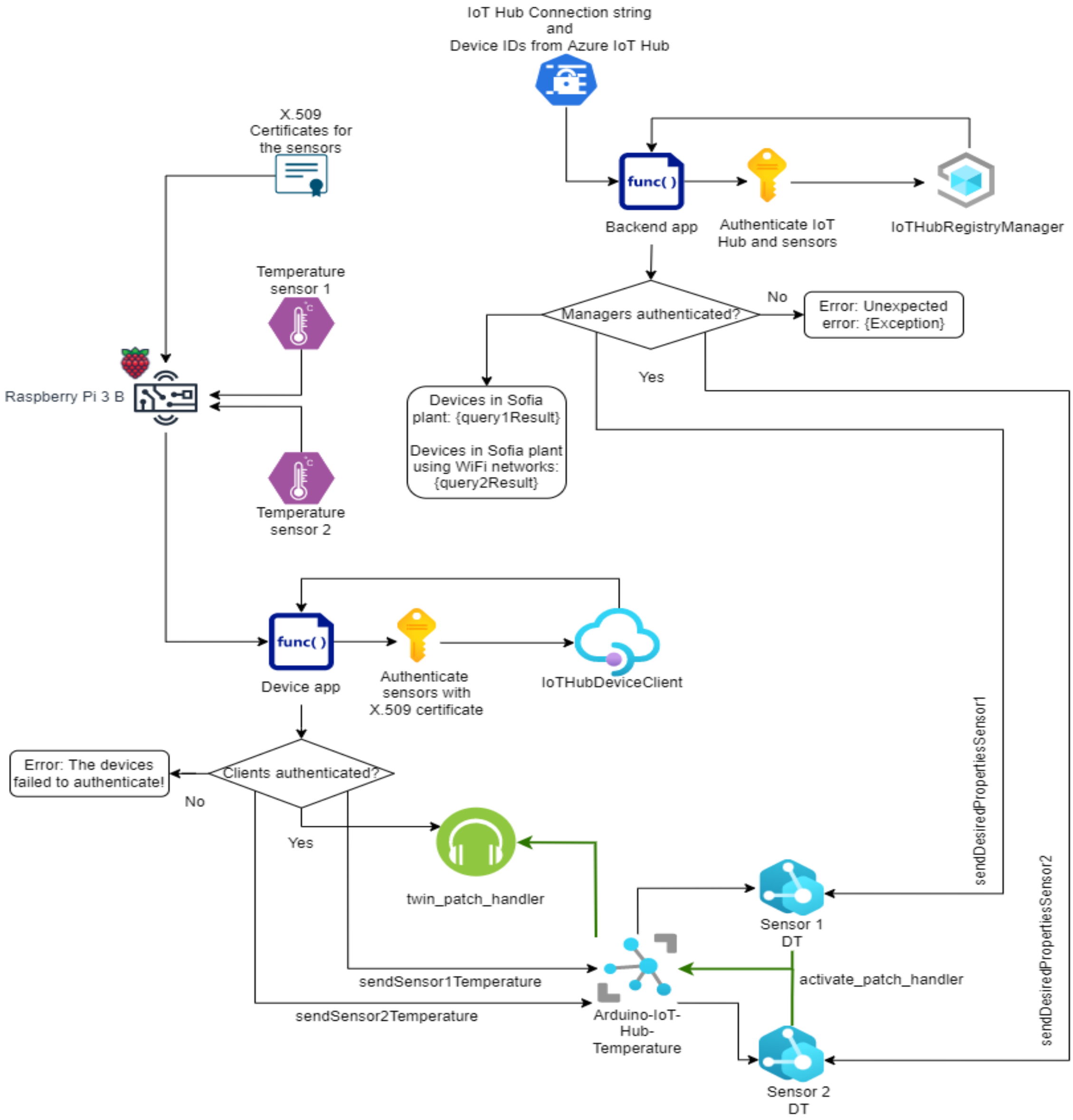


Figure 5.1: Component diagram

Moreover, we decided to make a comparison between two boards, because this will give us good understanding and view which is better for IoT devices. However, the Arduino Nano board does not provide neither an encryption chip to read the certificate, nor WiFi module that will provide the network connection needed to interact with Azure. Therefore, we found another Arduino board that we are going to use for the comparison - Arduino MKR 1010 WiFi. In table 5.1, you can see briefly what all the boards and does not have. We can concluded that the Raspberry Pi is the most powerful board, but it is used as a computer, not just a simple board, that is the reason why it is more expensive, too. However, it gives the best experience and many possibilities if you use to build IoT Devices, but many of them need to be less expensive which leads to some alternative variants like Arduino MKR 1010 WiFi board. The program on the Arduino MKR board is quite similar as on the Raspberry Pi board, but it is using different libraries to connect to Azure, because it is written in the C programming language, whereas the Raspberry is written in Python.

Feature	Arduino Nano [16]	Arduino MKR 1010 WiFi [17]	Raspberry Pi [18]
Price	€11.5 - €22.0	€33.5	€120 - €200
Dimensions	18 x 45 mm	25 x 61.5 mm	85mm x 56mm
Microcontroller	ATmega328	SAMD21 32-bit Cortex-M0+	ARM Cortex-A53 CPU
Clock Speed	16 MHz	32.768 kHz (RTC), 48 MHz	1.2 GHz
Memory	32 kB	256 kB	512 kb Cache and 1GB Max memory
WiFi	No	Yes	Yes
Cryptographic chip	No	Yes	Yes
USB	No	Yes	Yes

Table 5.1: Boards Overview

5.2 Authentication

As it was mentioned earlier, we started the tests by using the symmetric key option for the authentication, because it was easier to setup, basically, just using the connection string that is automatically generated with the private key inside, which also is auto-generated from Azure. However, during our process, we decided to switch to more secure authentication - X.509 CA Signed certificates, because the symmetric key is shared between device and the cloud, which means that the key needs to be secured in two places. With the certificates, the challenge will be to prove possession of the key without revealing anything private. Additionally, people that are using the symmetric keys most likely are storing the keys in plaintext (unencrypted) on the devices, which makes the keys vulnerable. Another reason why we moved from just symmetric keys to the certificates is that the certificates are storing also the identity of the specific device (prove its authenticity) and not just using a randomly generated key where the identity of the device is not encrypted in. We followed a tutorial, that is provided from Azure, which can be used for testing purposes only [19]. In Figure 5.2, you can see the sequence diagram that shows the process interactions for the certificate generation and briefly shows the interaction of the messages sent to the Azure services. We can see that the Administrator (this is us in our case) is generating the certificates by using the OpenSSL and the Microsoft Cryptography API: Next Generation (CNG). The X.509 digital certificates are documents that can represent a device, service, or a user. Commonly, in the companies, they are generated

[16] https://store.arduino.cc/collections/boards/products/arduino-nano
[17] https://store.arduino.cc/collections/boards/products/arduino-mkr-wifi-1010
[18] https://www.raspberrypi.com/products/raspberry-pi-3-model-b/
[19] https://docs.microsoft.com/en-us/azure/iot-hub/tutorial-x509-scripts

by a third-party that is called Certificate Authority (CA) and in our case this will be Azure. The certificate contains various fields like version, serial number, signature (hash) algorithm, issuer, valid from and to date, subject, the public key of the entity that is the certificate for and its parameters, enhanced key usage, subject alternative name, subject key identifier, key usage, basic constraints, and the thumbprint. You can see the example in Figure 5.3 and the three subfigures that shows the General information and the Detailed information of the certificate. They bind to an identity and the public key that the digital signature is using. Then, one can use this public key to establish a secure communication with the other party. Additionally, the certificates are resistant to Man-in-the-Middle attacks, which makes them very useful in the authentication between the IoT and DT environments.

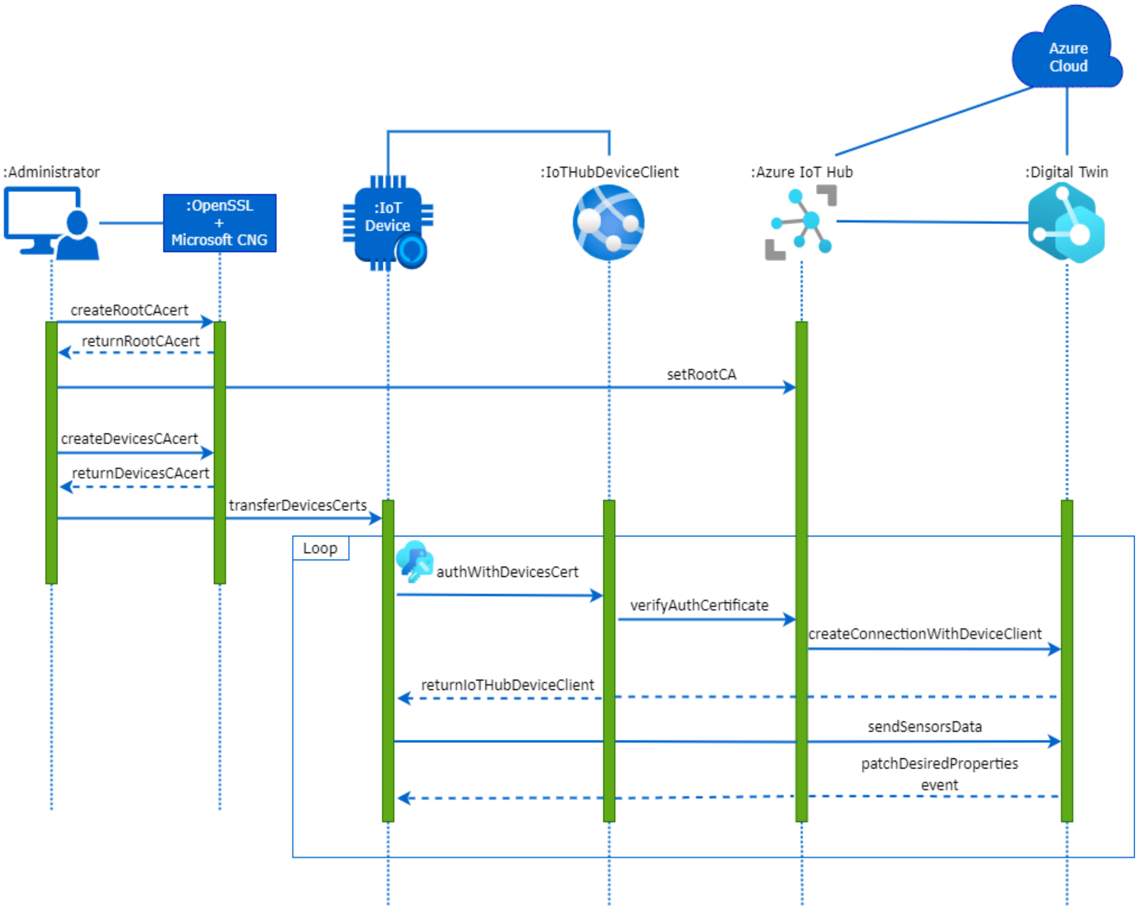
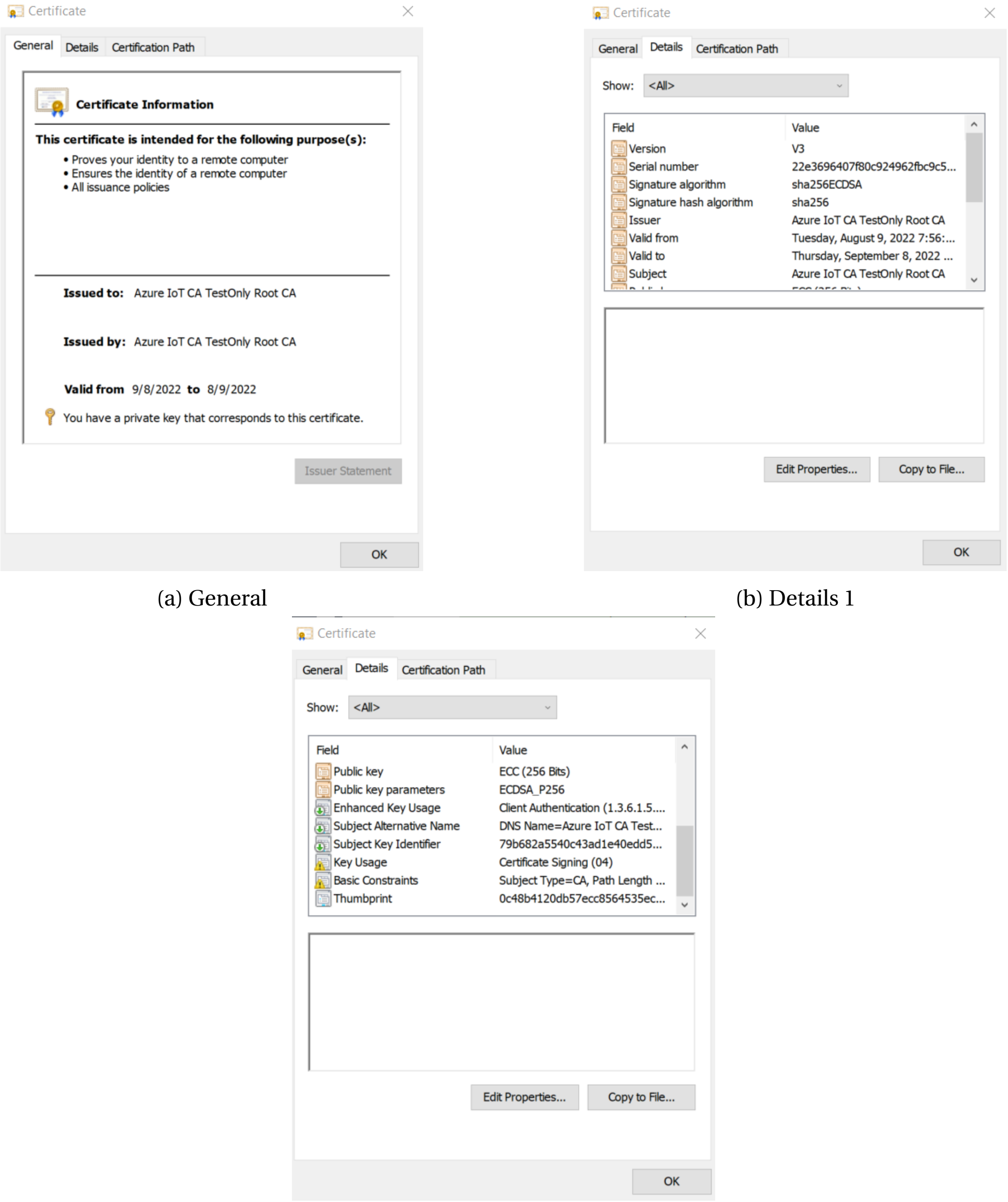


Figure 5.2: Sequence Diagram



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- All issuance policies

Issued to: Azure IoT CA TestOnly Root CA

Issued by: Azure IoT CA TestOnly Root CA

Valid from 9/8/2022 **to** 8/9/2022

You have a private key that corresponds to this certificate.

(a) General

Show: <All>

Field	Value
Version	V3
Serial number	22e3696407f80c924962fbc9c5...
Signature algorithm	sha256ECDSA
Signature hash algorithm	sha256
Issuer	Azure IoT CA TestOnly Root CA
Valid from	Tuesday, August 9, 2022 7:56:...
Valid to	Thursday, September 8, 2022 ...
Subject	Azure IoT CA TestOnly Root CA

(b) Details 1

Show: <All>

Field	Value
Public key	ECC (256 Bits)
Public key parameters	ECDSA_P256
Enhanced Key Usage	Client Authentication (1.3.6.1.5....
Subject Alternative Name	DNS Name=Azure IoT CA Test...
Subject Key Identifier	79b682a5540c43ad1e40edd5...
Key Usage	Certificate Signing (04)
Basic Constraints	Subject Type=CA, Path Length ...
Thumbprint	0c48b4120db57ecc8564535ec...

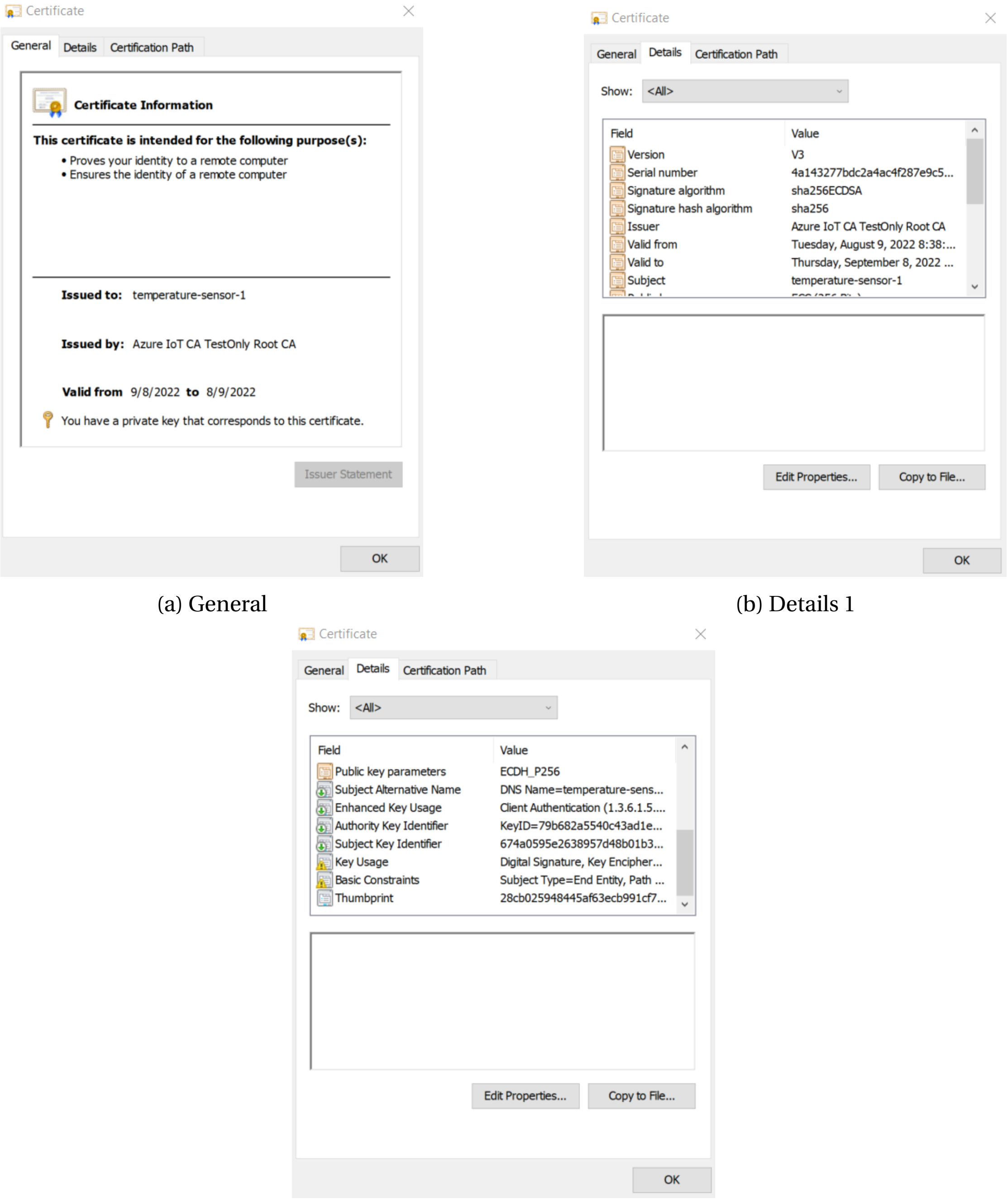
(c) Details 2

Figure 5.3: Root X.509 Certificate Example

Therefore, the first step is to get the pre-built scripts from Azure, then to configure some environment variables that will ensure that the scripts will be using OpenSSL (one need to ensure that OpenSSL is setup correctly as suggested in the official website[20]). Afterwards, when we want to generate the root certificate, we need to choose what algorithm to be used for the digital signature - RSA or ECC (ECDSA with SHA-256 hash function). We decided to use ECDSA for the main simulation, because it provides smaller key size and less computing power, as it was shown in 4.2 and as we could conclude from the measurements that we made. More details on the results from these tests can be seen in Section 5.4. Then, we requested the certificate generation with one of the pre-built scripts from Azure and it automatically returned 6 files - algorithmUsed.txt that contains the name of the algorithm used for the signing, three intermediates .pem files that can be used also for signing device certificates, RootCA.cer and RootCA.pem. The last two files contain the data for the certificate like who is the owner and the specific public key, and the public key in base64 format, respectively. Afterwards, we go to Azure portal and upload the generated root certificate to the IoT Hub, which will be our main point for the authentication. Then, we generated the certificates for the devices with only two differences - we do not set what hashing algorithm to be used for the signing, because it will take the one used for the root certificate, and we will set which device the certificate will represent (by device ID). Example of such certificate can be seen in Figure 5.4. Thus, the device's digital certificate will be closely related to the root one and will be like a 'child' (leaf) of the root. The certificates for the IoT devices (the sensors) are uploaded on the Raspberry board using a secure external storage (USB flash drive). They are used to authenticate the physical devices with their digital twins in the IoT Hub. After all the certificates are set, we can start the communication between the physical sensors and the DTs.

Initially, the IoT device will create IoTHubDeviceClient objects that are provided from the Azure library, and they will be the connection with the Azure. The initialization requires the X.509 certificate of each device which on its side is initialized by passing the paths of the public key and the private key, and the pass phrase that in our case is a default one. Additionally, we need to give the IoTHubDeviceClient the host name of the IoT Hub and the device ID. When pass this, Azure starts to authenticate the device, it verifies the device identity with the help of the CA's public (Azure CA in this case) and then create the connection with the corresponding DT. Afterwards, if the authentication is successful, Azure will return the IoTHubDeviceClient, otherwise it will fail. When we have the clients authenticated, the temperature sensors start to pass the live data to their equivalent DTs and wait for updates from the DTs.

[20] https://www.openssl.org/source/



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer

Issued to: temperature-sensor-1

Issued by: Azure IoT CA TestOnly Root CA

Valid from 9/8/2022 **to** 8/9/2022

You have a private key that corresponds to this certificate.

(a) General

Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	4a143277bdc2a4ac4f287e9c5...
Signature algorithm	sha256ECDSA
Signature hash algorithm	sha256
Issuer	Azure IoT CA TestOnly Root CA
Valid from	Tuesday, August 9, 2022 8:38:...
Valid to	Thursday, September 8, 2022 ...
Subject	temperature-sensor-1

(b) Details 1

Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Public key parameters	ECDH_P256
Subject Alternative Name	DNS Name=temperature-sens...
Enhanced Key Usage	Client Authentication (1.3.6.1.5....
Authority Key Identifier	KeyID=79b682a5540c43ad1e...
Subject Key Identifier	674a0595e2638957d48b01b3...
Key Usage	Digital Signature, Key Encipher...
Basic Constraints	Subject Type=End Entity, Path ...
Thumbprint	28cb025948445af63ecb991cf7...

(c) Details 2

Figure 5.4: Device X.509 Certificate Example

For the device application, we are using the following python script:

```python
# The Device app
import os
import time
import glob
import asyncio
import json
from azure.iot.device.aio import IoTHubDeviceClient
from azure.iot.device import Message, X509

SLEEP_TIME = 15

device_folders = glob.glob(base_dir + '28*')

# main method and run app
async def main():
    print("IoT Hub - Simulating Device to Digital Twin Communication ...")

    clients = []
    for certificate in CERTIFICATES:
        try:
            # The device that has been created on the portal using X509 CA signing or Self signing capabilities
            # The certificate file should be with the same name as the device
            device_id = os.path.basename(certificate["certFile"]).strip('-public.pem.pfx')
            print("Connecting to device {} ...".format(device_id))
            temp_client = await create_client(certificate["certFile"], certificate["keyFile"], certificate["pass"], device_id)
            clients.append(temp_client)
        except:
            print("Warning: Could not authenticate or find device for the following certificate {}".format(certificate))
            continue

  if (len(clients) == 0):
    print("Error: The devices failed to authenticate!")
    await close_clients(clients)
    return;

    if (len(clients) != len(device_folders)):
        print("Error: The number of device clients mismatch the number connected physical devices!")
        await close_clients(clients)
        return

    print("IoTHubDeviceClient waiting for commands, press Ctrl-C to exit")

    try:
        # Update reported properties with WiFi information and send
    telemetry message
        print("Sending data as reported property...")

        # Update the temperature until the program exit
        while True:
            client_index = 0
            for folder in device_folders:
                temp_c, temp_f = read_sensors_data(folder)
                if (temp_c != None):
                    print("temperature(C): {}, temperature(F): {}".format
    (temp_c, temp_f))

                    reported_patch = {"currentTemperatureC": temp_c, "
    currentTemperatureF": temp_f, "connectivity": "WiFi"}
                    await clients[client_index].
    patch_twin_reported_properties(reported_patch)
                    await send_telemetry_message(clients[client_index],
    reported_patch)
                    client_index += 1

            print("The reported properties of the sensors are updated")
            time.sleep(SLEEP_TIME)
    except KeyboardInterrupt:
        print("IoT Hub Device Twin device sample stopped")
    finally:
        # Graceful exit and shut down all clients
        print("Shutting down IoT Hub Client")
        await close_clients(clients)
        clients = []

if __name__ == '__main__':
    asyncio.run(main())
    print("done")
```

Listing 1: Python device app

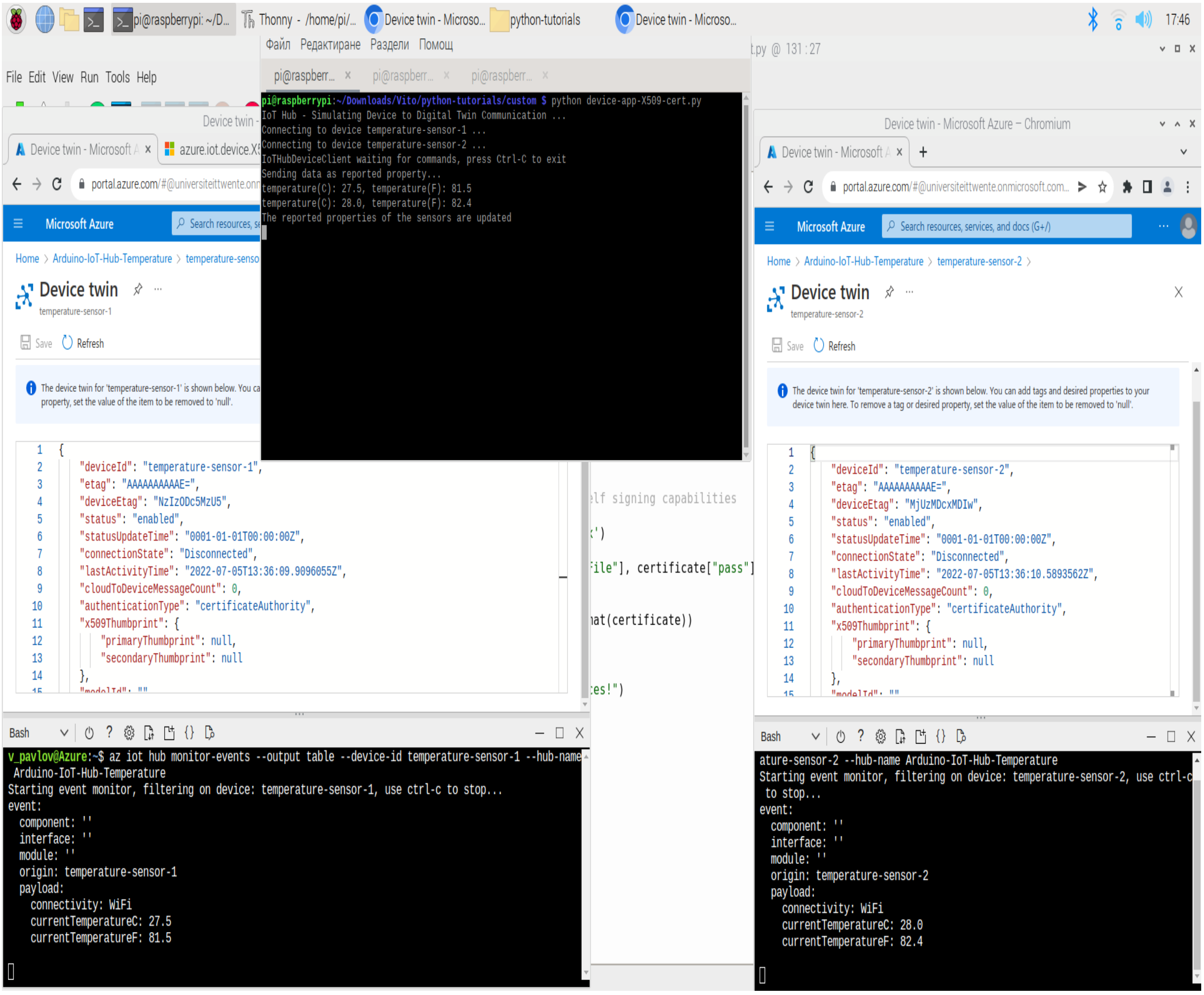
This is only the main method that is used for the device app, but in the GitHub repository[21], the full code of the device and the backend applications can be seen. Additionally, the pictures with the results are in the “pics-results" folder.

5.3 Communication between the real device and the Digital Twin

In Figure 5.5, you can see the results from the script listed above. From the console, one can see that the program starts and connects to each device that is listed, in our case these are the temperature-sensor-1 and temperature-sensor-2. Then, the program says that it will wait for a command, e.g., to stop the process you can use “Ctrl-C". Then, whenever the temperature sensor send the data, this will automatically grab it and pass it as a telemetry to the Digital Twin, and the value will be added in the reported properties (can be seen in Figure 5.6 and it will store the information for what connectivity the devices are using, in our case it is WiFi.

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

These properties can be edited only by the Device app (in our case, the physical device) and they can be read from the Azure IoT Hub and the Digital Twin (read-only mode).



```
pi@raspberrypi:~/Downloads/Vito/python-tutorials/custom $ python device-app-X509-cert.py
IoT Hub - Simulating Device to Digital Twin Communication ...
Connecting to device temperature-sensor-1 ...
Connecting to device temperature-sensor-2 ...
IoTHubDeviceClient waiting for commands, press Ctrl-C to exit
Sending data as reported property...
temperature(C): 27.5, temperature(F): 81.5
temperature(C): 28.0, temperature(F): 82.4
The reported properties of the sensors are updated
```

Device twin
temperature-sensor-1

The device twin for 'temperature-sensor-1' is shown below. You ca
property, set the value of the item to be removed to 'null'.

```
{
    "deviceId": "temperature-sensor-1",
    "etag": "AAAAAAAAAAE=",
    "deviceEtag": "NzIzODc5MzU5",
    "status": "enabled",
    "statusUpdateTime": "0001-01-01T00:00:00Z",
    "connectionState": "Disconnected",
    "lastActivityTime": "2022-07-05T13:36:09.9096055Z",
    "cloudToDeviceMessageCount": 0,
    "authenticationType": "certificateAuthority",
    "x509Thumbprint": {
        "primaryThumbprint": null,
        "secondaryThumbprint": null
    },
    "modelId": ""
```

```
v_pavlov@Azure:~$ az iot hub monitor-events --output table --device-id temperature-sensor-1 --hub-name
 Arduino-IoT-Hub-Temperature
Starting event monitor, filtering on device: temperature-sensor-1, use ctrl-c to stop...
event:
  component: ''
  interface: ''
  module: ''
  origin: temperature-sensor-1
  payload:
    connectivity: WiFi
    currentTemperatureC: 27.5
    currentTemperatureF: 81.5
```

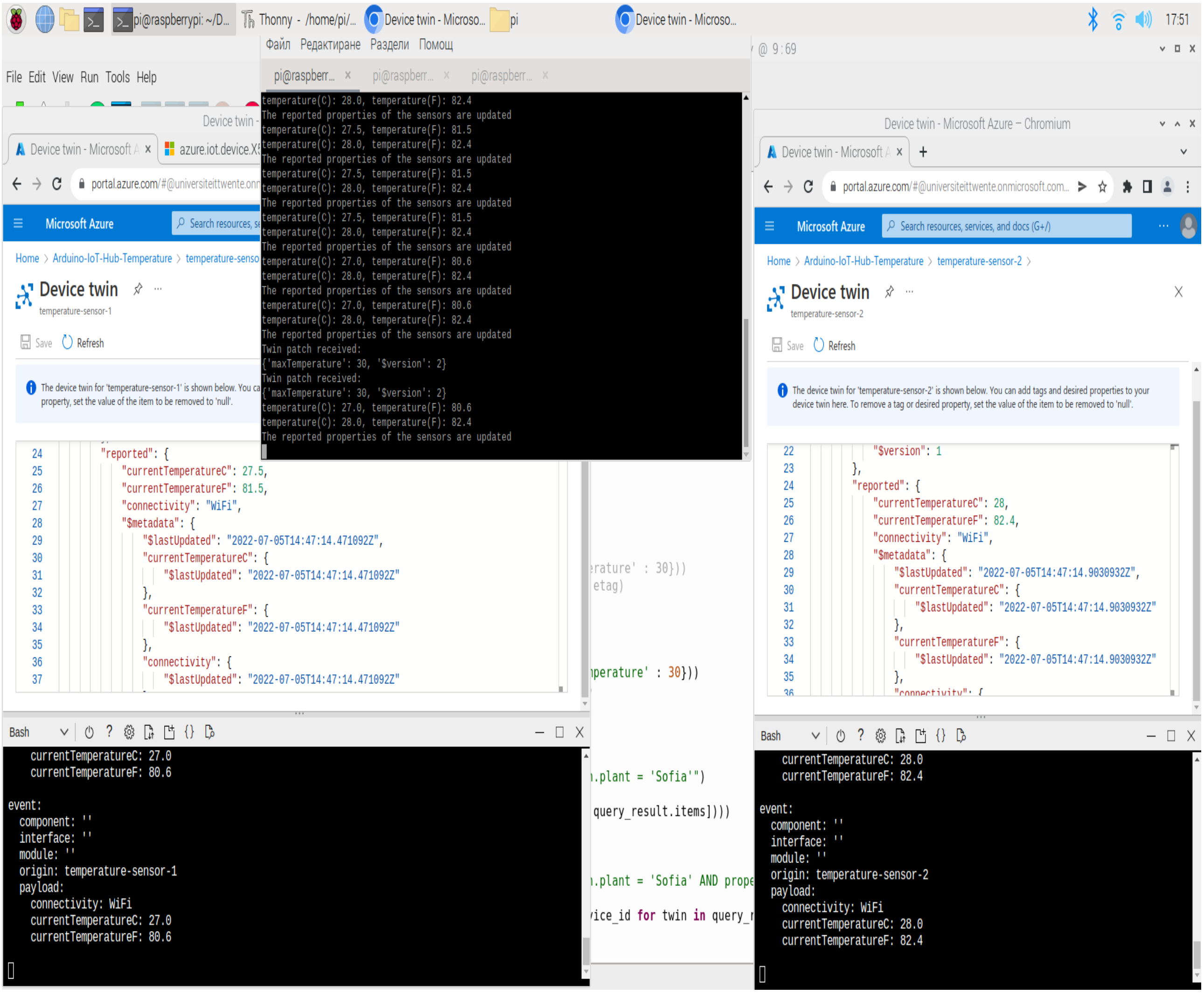
Device twin
temperature-sensor-2

The device twin for 'temperature-sensor-2' is shown below. You can add tags and desired properties to your device twin here. To remove a tag or desired property, set the value of the item to be removed to 'null'.

```
{
    "deviceId": "temperature-sensor-2",
    "etag": "AAAAAAAAAAE=",
    "deviceEtag": "MjUzMDcxMDIw",
    "status": "enabled",
    "statusUpdateTime": "0001-01-01T00:00:00Z",
    "connectionState": "Disconnected",
    "lastActivityTime": "2022-07-05T13:36:10.5893562Z",
    "cloudToDeviceMessageCount": 0,
    "authenticationType": "certificateAuthority",
    "x509Thumbprint": {
        "primaryThumbprint": null,
        "secondaryThumbprint": null
    },
    "modelId": ""
```

```
ature-sensor-2 --hub-name Arduino-IoT-Hub-Temperature
Starting event monitor, filtering on device: temperature-sensor-2, use ctrl-c
 to stop...
event:
  component: ''
  interface: ''
  module: ''
  origin: temperature-sensor-2
  payload:
    connectivity: WiFi
    currentTemperatureC: 28.0
    currentTemperatureF: 82.4
```

Figure 5.5: Device App console output



```
temperature(C): 28.0, temperature(F): 82.4
The reported properties of the sensors are updated
temperature(C): 27.5, temperature(F): 81.5
temperature(C): 28.0, temperature(F): 82.4
The reported properties of the sensors are updated
temperature(C): 27.5, temperature(F): 81.5
temperature(C): 28.0, temperature(F): 82.4
The reported properties of the sensors are updated
temperature(C): 27.5, temperature(F): 81.5
temperature(C): 28.0, temperature(F): 82.4
The reported properties of the sensors are updated
temperature(C): 27.0, temperature(F): 80.6
temperature(C): 28.0, temperature(F): 82.4
The reported properties of the sensors are updated
temperature(C): 27.0, temperature(F): 80.6
temperature(C): 28.0, temperature(F): 82.4
The reported properties of the sensors are updated
Twin patch received:
{'maxTemperature': 30, '$version': 2}
Twin patch received:
{'maxTemperature': 30, '$version': 2}
temperature(C): 27.0, temperature(F): 80.6
temperature(C): 28.0, temperature(F): 82.4
The reported properties of the sensors are updated
```

Device twin
temperature-sensor-1

The device twin for 'temperature-sensor-1' is shown below. You ca property, set the value of the item to be removed to 'null'.

```
"reported": {
    "currentTemperatureC": 27.5,
    "currentTemperatureF": 81.5,
    "connectivity": "WiFi",
    "$metadata": {
        "$lastUpdated": "2022-07-05T14:47:14.471092Z",
        "currentTemperatureC": {
            "$lastUpdated": "2022-07-05T14:47:14.471092Z"
        },
        "currentTemperatureF": {
            "$lastUpdated": "2022-07-05T14:47:14.471092Z"
        },
        "connectivity": {
            "$lastUpdated": "2022-07-05T14:47:14.471092Z"
```

```
    currentTemperatureC: 27.0
    currentTemperatureF: 80.6

event:
  component: ''
  interface: ''
  module: ''
  origin: temperature-sensor-1
  payload:
    connectivity: WiFi
    currentTemperatureC: 27.0
    currentTemperatureF: 80.6
```

Device twin
temperature-sensor-2

The device twin for 'temperature-sensor-2' is shown below. You can add tags and desired properties to your device twin here. To remove a tag or desired property, set the value of the item to be removed to 'null'.

```
            "$version": 1
        },
        "reported": {
            "currentTemperatureC": 28,
            "currentTemperatureF": 82.4,
            "connectivity": "WiFi",
            "$metadata": {
                "$lastUpdated": "2022-07-05T14:47:14.9030932Z",
                "currentTemperatureC": {
                    "$lastUpdated": "2022-07-05T14:47:14.9030932Z"
                },
                "currentTemperatureF": {
                    "$lastUpdated": "2022-07-05T14:47:14.9030932Z"
                },
                "connectivity": {
```

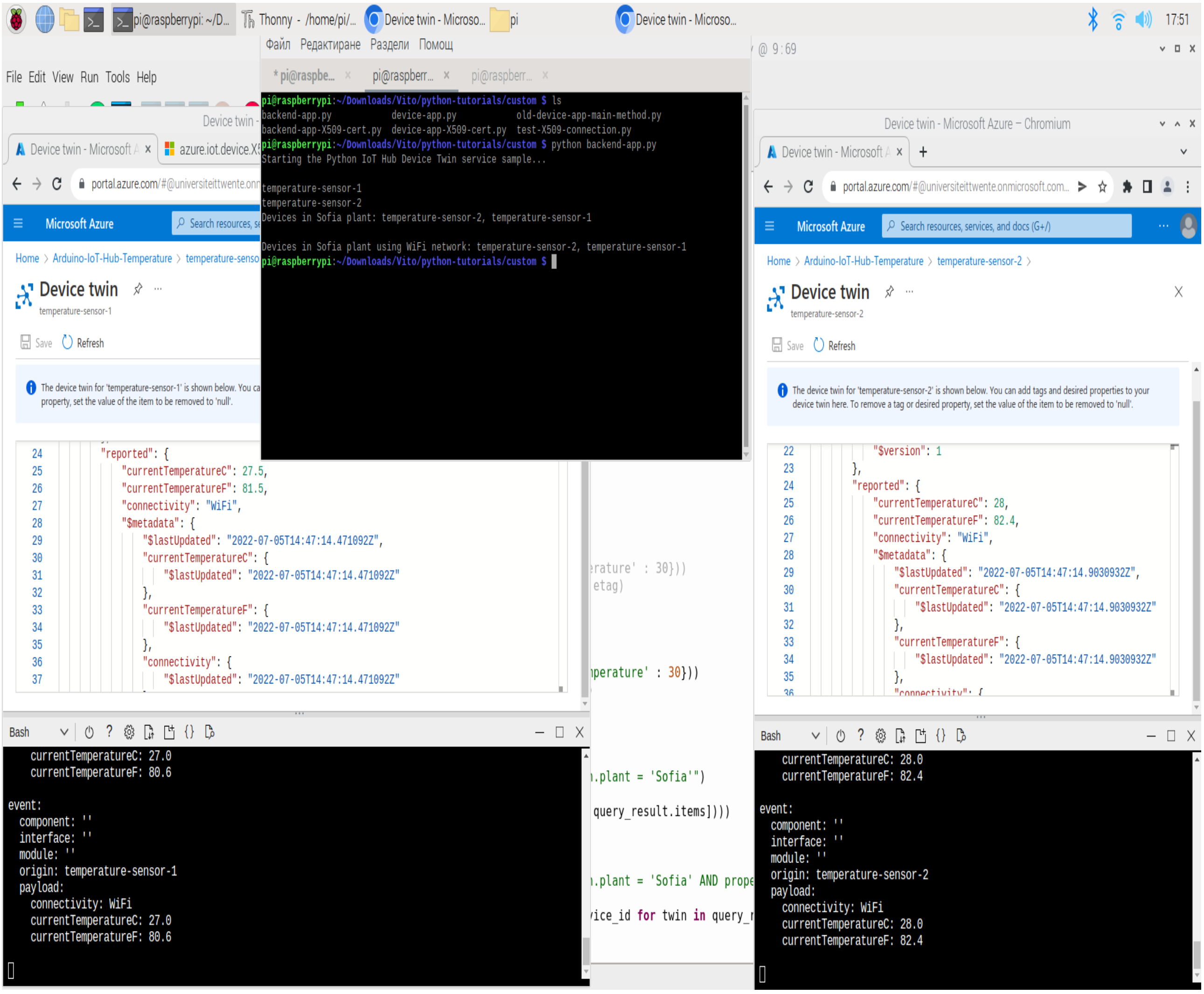
```
    currentTemperatureC: 28.0
    currentTemperatureF: 82.4

event:
  component: ''
  interface: ''
  module: ''
  origin: temperature-sensor-2
  payload:
    connectivity: WiFi
    currentTemperatureC: 28.0
    currentTemperatureF: 82.4
```

pi@raspberrypi: ~/D...
Thonny - /home/pi/...
Device twin - Microso...
pi
Device twin - Microso...
17:51
File Edit View Run Tools Help
Файл Редактиране Раздели Помощ
pi@raspberr...
Device twin - Microsoft Azure – Chromium
Device twin - Microsoft
azure.iot.device.X5
portal.azure.com/#@universiteittwente.onmicrosoft.com...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Arduino-IoT-Hub-Temperature > temperature-sensor-2 >
Save
Refresh
Bash

Figure 5.6: Device App console output and reported properties of the DT

Furthermore, the device application is constantly listening for patch events made from the Digital Twins, that each physical device corresponds to. These events usually change the desired properties which can be used to make various actions based on their values, e.g., if the maximum temperature is set to be 30C, then the device might display an alert for too hot place. These properties are the opposite to the reported ones. They can be edited from the Azure IoT Hub and the Digital Twin (backend app), but from the physical device, they can only be read. In Figure 5.7, you can see the console output from the backend app and then in Figure 5.8, you can see the updated desired properties. This application is responsible to update the “maxTemperature" property and the tags of the devices for their location, then it filters and shows all the devices that are located in Sofia and are using WiFi.



Thonny - /home/pi/...
Device twin - Microso...
pi
Файл Редактиране Раздели Помощ
* pi@raspbe... × pi@raspberr... × pi@raspberr... ×
File Edit View Run Tools Help
Device twin - Microsoft Azure – Chromium
portal.azure.com/#@universiteittwente.onmicrosoft.com...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Arduino-IoT-Hub-Temperature > temperature-sensor-2 >
Device twin
Save
Refresh
Bash
17:51

```
pi@raspberrypi:~/Downloads/Vito/python-tutorials/custom $ ls
backend-app.py           device-app.py           old-device-app-main-method.py
backend-app-X509-cert.py  device-app-X509-cert.py  test-X509-connection.py
pi@raspberrypi:~/Downloads/Vito/python-tutorials/custom $ python backend-app.py
Starting the Python IoT Hub Device Twin service sample...

temperature-sensor-1
temperature-sensor-2
Devices in Sofia plant: temperature-sensor-2, temperature-sensor-1

Devices in Sofia plant using WiFi network: temperature-sensor-2, temperature-sensor-1
pi@raspberrypi:~/Downloads/Vito/python-tutorials/custom $
```

Device twin
temperature-sensor-1

The device twin for 'temperature-sensor-1' is shown below. You ca
property, set the value of the item to be removed to 'null'.

```
        "reported": {
            "currentTemperatureC": 27.5,
            "currentTemperatureF": 81.5,
            "connectivity": "WiFi",
            "$metadata": {
                "$lastUpdated": "2022-07-05T14:47:14.471092Z",
                "currentTemperatureC": {
                    "$lastUpdated": "2022-07-05T14:47:14.471092Z"
                },
                "currentTemperatureF": {
                    "$lastUpdated": "2022-07-05T14:47:14.471092Z"
                },
                "connectivity": {
                    "$lastUpdated": "2022-07-05T14:47:14.471092Z"
```

```
    currentTemperatureC: 27.0
    currentTemperatureF: 80.6

event:
  component: ''
  interface: ''
  module: ''
  origin: temperature-sensor-1
  payload:
    connectivity: WiFi
    currentTemperatureC: 27.0
    currentTemperatureF: 80.6
```

Device twin
temperature-sensor-2

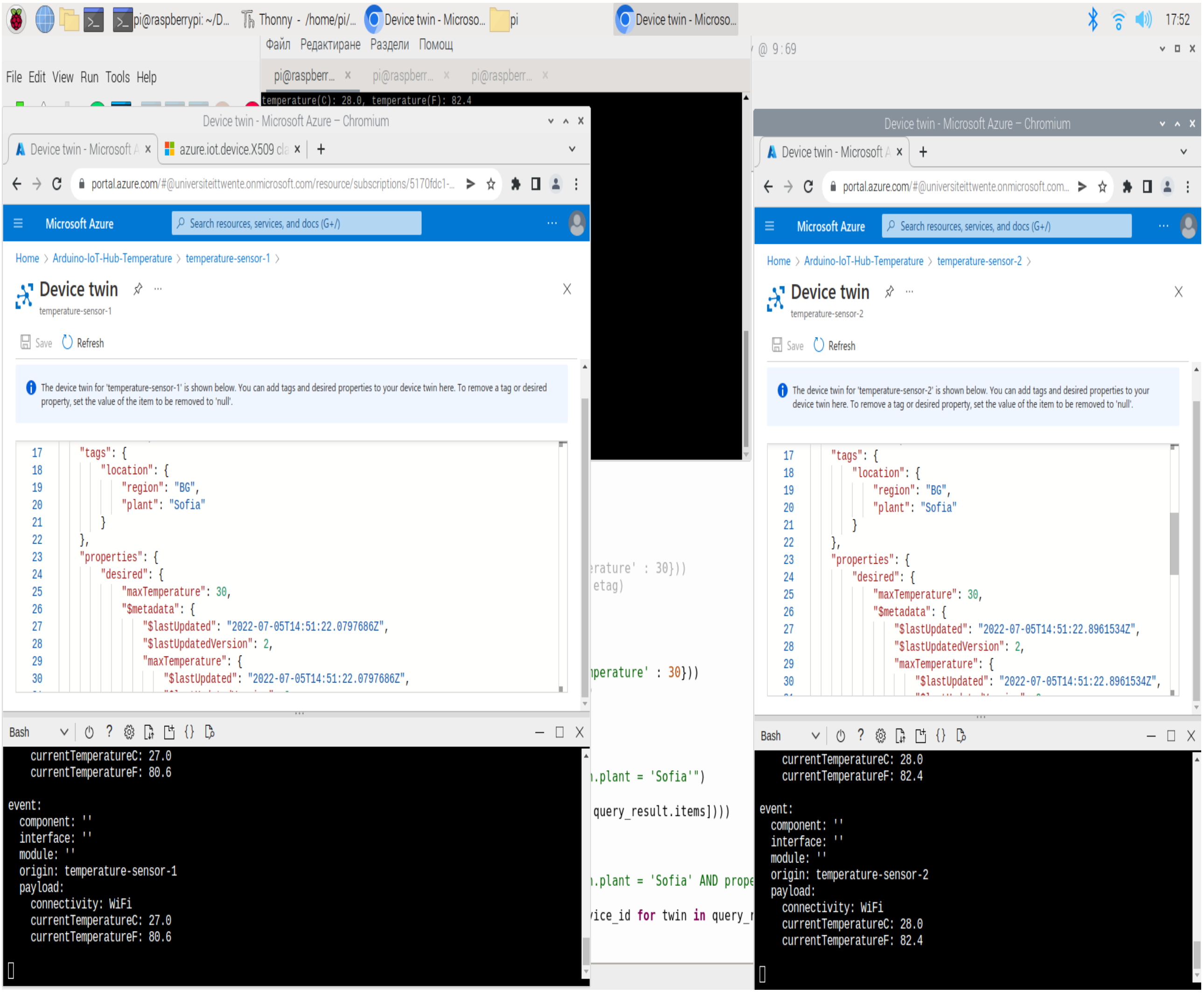
The device twin for 'temperature-sensor-2' is shown below. You can add tags and desired properties to your device twin here. To remove a tag or desired property, set the value of the item to be removed to 'null'.

```
            "$version": 1
        },
        "reported": {
            "currentTemperatureC": 28,
            "currentTemperatureF": 82.4,
            "connectivity": "WiFi",
            "$metadata": {
                "$lastUpdated": "2022-07-05T14:47:14.9030932Z",
                "currentTemperatureC": {
                    "$lastUpdated": "2022-07-05T14:47:14.9030932Z"
                },
                "currentTemperatureF": {
                    "$lastUpdated": "2022-07-05T14:47:14.9030932Z"
                },
                "connectivity": {
```

```
    currentTemperatureC: 28.0
    currentTemperatureF: 82.4

event:
  component: ''
  interface: ''
  module: ''
  origin: temperature-sensor-2
  payload:
    connectivity: WiFi
    currentTemperatureC: 28.0
    currentTemperatureF: 82.4
```

Figure 5.7: Backend App console output


pi@raspberrypi: ~/D...
Thonny - /home/pi/...
Device twin - Microso...
pi
Device twin - Microso...
17:52
File Edit View Run Tools Help
Файл Редактиране Раздели Помощ
pi@raspberr...
@ 9 : 69
Device twin - Microsoft Azure – Chromium
Device twin - Microsoft A
azure.iot.device.X509 cla
portal.azure.com/#@universiteittwente.onmicrosoft.com/resource/subscriptions/5170fdc1-...
portal.azure.com/#@universiteittwente.onmicrosoft.com...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Arduino-IoT-Hub-Temperature > temperature-sensor-1 >
Home > Arduino-IoT-Hub-Temperature > temperature-sensor-2 >
Device twin
temperature-sensor-1
temperature-sensor-2
Save
Refresh
Bash

```
temperature(C): 28.0, temperature(F): 82.4
```

The device twin for 'temperature-sensor-1' is shown below. You can add tags and desired properties to your device twin here. To remove a tag or desired property, set the value of the item to be removed to 'null'.

```
"tags": {
    "location": {
        "region": "BG",
        "plant": "Sofia"
    }
},
"properties": {
    "desired": {
        "maxTemperature": 30,
        "$metadata": {
            "$lastUpdated": "2022-07-05T14:51:22.0797686Z",
            "$lastUpdatedVersion": 2,
            "maxTemperature": {
                "$lastUpdated": "2022-07-05T14:51:22.0797686Z",
```

```
    currentTemperatureC: 27.0
    currentTemperatureF: 80.6

event:
  component: ''
  interface: ''
  module: ''
  origin: temperature-sensor-1
  payload:
    connectivity: WiFi
    currentTemperatureC: 27.0
    currentTemperatureF: 80.6
```

The device twin for 'temperature-sensor-2' is shown below. You can add tags and desired properties to your device twin here. To remove a tag or desired property, set the value of the item to be removed to 'null'.

```
"tags": {
    "location": {
        "region": "BG",
        "plant": "Sofia"
    }
},
"properties": {
    "desired": {
        "maxTemperature": 30,
        "$metadata": {
            "$lastUpdated": "2022-07-05T14:51:22.8961534Z",
            "$lastUpdatedVersion": 2,
            "maxTemperature": {
                "$lastUpdated": "2022-07-05T14:51:22.8961534Z",
```

```
    currentTemperatureC: 28.0
    currentTemperatureF: 82.4

event:
  component: ''
  interface: ''
  module: ''
  origin: temperature-sensor-2
  payload:
    connectivity: WiFi
    currentTemperatureC: 28.0
    currentTemperatureF: 82.4
```

Figure 5.8: Azure overview of the desired properties

5.4 Experiment Results

After we prepared the simulation and everything was running smoothly, we decided to evaluate the symmetric key authentication and the X.509 certificates by measuring the power consumption. We did this by using a USB power consumption tester [22] 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 5.2. We created two additional test scripts that are only authenticating the devices, in order to have more precise results. You can find them

[22] https://elimex.bg/product/68491-usb-tester-ut658

on the repository, in folder test-scripts. Moreover, we measured the average values because it was giving slightly different times for both of the metrices. 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. Then just calculated the milliamperes manually and the watts using an online calculator [23]. In all authentication types, the raspberry was working on 5.32 volts. For the execution time, we decided to make the scripts to run ten times and automatically to 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. You can see the results in Table 5.3.

Board	Authentication Type	Current (mA)	Power (W)	Execution time (s)
Raspberry Pi	Symmetric key connection string	≈ 112	≈ 0.596	≈ 0.0452
	X.509 Certificate with ECDSA	≈ 151	≈ 0.803	≈ 0.412
	X.509 Certificate with RSA	≈ 163	≈ 0.867	≈ 0.396
Arduino MKR 1010	Symmetric key connection string	≈ 12	≈ 0.061	≈ 4.683
	X.509 Certificate with ECDSA	≈ 15	≈ 0.076	≈ 5.121

Table 5.2: Measurement Results

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

Table 5.3: Certificate Generation Times

5.5 Results Discussion

As we can see from the console results, in Section 5.3, our environment uses a bidirectional communication which helps 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. You can add any property and value and if there is a change of the value of an already existing property it will then fire up an event and will update the data. 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 could see that the execution time of the symmetric connection string 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 it is faster by about 0.5 seconds, 4.683 seconds for the connection string versus 5.121 for the ECDSA

[23] https://www.electricaltechnology.org/2014/03/power-voltage-current-resistance-pvir-calculator.html

certificate. This is already known by theory that the symmetric encryption works faster, but the public key encryption provides more security.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 encryption (more time = more energy usage). 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 a lot similar results, just the values are different. Thus, we can conclude here that the Arduino board works with less energy consumption, which is understandable because it has much less power, but that increases the authentication time a lot. Additional factor for this big difference in the execution time might be that in the Arduino we are using totally different librariers for the communication.

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 - 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 is 256 bits.

As a conclusion for this section, we can say that the symmetric key encryption is much faster than the digital certificates, and requires less energy, but it provides lower level of security. As we know, and learnt from the research that we have made for the authentication schemes, the symmetric key encryption schemes can pose more risks for exposing the private key. 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 device. Additionally, in some cases the symmetric key options use more energy than the certificates, as we could see from our results. Finally, both types of certificates are having almost the same performance and energy usage, thus, it is a matter of priorities which one of the standards will suit the most the use case.

6 Conclusion

Nowadays, there is a lot of attention for the Internet of Things devices and their authentication. From our literature study in this work, we found that there are a lot of weaknesses in many devices around the world which gives the opportunity to the attackers to exploit that and execute their attacks. Additionally, the Digital Twins is also an disruptive and emerging technology that can connect to physical devices like IoT devices and sensors. They can interact with each other in a bi-directional manner, which opens additional doors for various attacks like MITM, DoS and DDoS, Data & Identity theft and Malware as a Service (MaaS).

The organization of the rest of the chapter is as follows: in Section 6.1 we are going to summarize the results from the paper; Then, in Section 6.2 we will explain the limitations of the paper and some of the reasons; In 6.3 we will give ideas to other researchers for future work.

6.1 Empirical Findings

We were able to discover that the field of IoT authentication techniques and protocols has a considerable amount of relevant and advantageous scientific work. Thus, with this paper, we present an overview of the IoT background, what are the concerns related to the authentication and the security, what are the existing authentication schemes and what proposals we have in the recent years. Additionally, we provide good insight of the Digital Twins technology - the history, the specification, literature review of the current development of the technology, what are the benefits and the challenges of its implementation. Additionally, we prepared a simulation that shows how the DT technology can be deployed in the IoT platform and how the devices can be authenticated. Lastly, we executed various comparison experiments between the different authentication options and the two boards that we used. The measurements were based on the power consumption and the execution time of the verification with the different authentication types that Azure provides and the time for the generation of the certificates with the ECDSA and RSA signing algorithms. Unfortunately, for the Arduino, we could not measure the metrices for the X509 RSA certificates, however, we still were able to measure everything for the symmetric key option and the X509 ECDSA certificates. In addition to the metrices, we were able to measure the power consumption of the generation of both certificates - using ECDSA and using RSA. This gave us clear view which certificate is generated faster. However, since the certificates are most likely generated once, this does not matter that much.

6.2 Research Limitations

The first limitation that we encounter was the lack of papers that are reviewing the authentication between DT and its physical mapping. Most of the DT related papers that were covering the security were discovering issues related to the security aspect, how they are current used within the IIoT sector, smart cities and the IoT in general. Additionally, the rest of the papers were discovering more what fields the DT can be applied to and not any security or authentication aspects.

The second limitation is that in our experiments, we were measuring the power consumption using a USB tester only, which might not be perfectly accurate.

Another limitation is that the our experiment is covering only one working scenario, for bi-directional communication, using only the Azure platform that provides the IoT Hub and the ADT. The reason is that the implementations for the other platforms and various scenarios require much more time and resources, especially when some of the platforms require to fully configure everything or they are with fully paid subscriptions that are no very cheap. Moreover, the Azure IoT Hub provides only few authentication types, which does not give much room for experiments with other ones.

Finally, another limitation can be seen in our experiments and the number of devices that were connected to the board and their DTs. The reason for that is the huge experiments, where we can test the scalability of the solution, require more resources like funding, people to help with the integration and the configurations, and time.

6.3 Future Work

We were able to find that there is a significant amount of relevant and encouraging scientific work in the area of IoT authentication schemes and protocols. However, we could not find any relevant literature that covers the exact authentication between the IoT devices and the DTs, which was our main goal to explore how this is done in a real-case scenario using a Raspberry Pi board and Azure. Despite that, there is a lot of room to discover new architectures or new authentications to provide better experience for companies and people that are using the DT technology with their IoT devices.

Additionally, it might be a good idea for other researchers to measure and compare the power consumption using other tools than the USB tester, because we are not perfectly sure how accurate the tester is. For example, other professional tool can be used - Power and Harmonics Clamp Meter[24] which will be the most accurate option, in my opinion. However, this is quite expensive option that can start from €50 to more than €450. Moreover, future improvement could be to find a way to use X509 certificate with RSA hashing algorithm on the Arduino, in order to be able to have better comparison between both boards. Even for more precise results and comparison, one can research what are the most used boards and chips which will be more accurate and will give the best results[25].

The Azure documentation states that the people that are using the IoT Hub are able to connect millions of devices and their applications are going to work reliably and securely. This is quite an intriguing challenge to test the scalability of this service, thus, this is another future opportunity for other researchers with more resources.

Lastly, other future experiments that can be made is with other platforms which could give more room for creativity like Ditto. We think that this platform is a good point for other studies to explore and to compare if the platform will be more efficient, and in what environments, than Azure. This will further give opportunity to compare more authentication types

[24] https://meters.uni-trend.com/product/ut243/

[25] https://www.intuz.com/guide-on-top-iot-development-boards

and not just the ones that Azure provides. Additionally, other researchers can think of a way, with a strong proposal, how to implement the blockchain technology into the IoT and DT platforms. For example, something similar to Suhail et al.[119]. The authors of the paper proposed a framework that consists of three layers - application, storage and data layers. In the data layer we have the physical space and the devices, and also the DTs (the virtual space) where the sensory data, the history data and the domain knowledge are gathered. Then, this data is forwarded to the storage layer where the data is stored and analyzed. This layer contains the lightweight, scalable and quantum-immune blockchain technology that is used in the framework. Lastly, the analyzed data is forwarded to the application layer, which consist of control units, remote offices and data analysts. In my opinion, this is a huge opportunity and will help a lot to explore more of all the technologies. However, this might be a task for the corporations, because most of the DT platforms are already made by big companies and it will not be possible one to just integrate or propose the usage of the blockchain technology in the already existing DT platforms, like Azure.

REFERENCES

[1] S. Aghapour, M. Kaveh, D. Martín, and M. R. Mosavi. An ultra-lightweight and provably secure broadcast authentication protocol for smart grid communications. *IEEE Access*, 8:125477–125487, 2020.

[2] S. F. Aghili, H. Mala, C. Schindelhauer, M. Shojafar, and R. Tafazolli. Closed-loop and open-loop authentication protocols for blockchain-based iot systems. *Information Processing Management*, 58(4):102568, 2021.

[3] T. A. Ahanger, A. Aljumah, and M. Atiquzzaman. State-of-the-art survey of artificial intelligent techniques for iot security. *Computer Networks*, 206:108771, 2022.

[4] M. Ahmad Jan, F. Khan, M. Alam, and M. Usman. A payload-based mutual authentication scheme for internet of things. *Future Generation Computer Systems*, 92, 09 2017.

[5] F. Akbarian, E. Fitzgerald, and M. Kihl. Intrusion detection in digital twins for industrial control systems. In *2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 1–6. IEEE, 2020.

[6] R. Al-Mutiri, M. Al-Rodhaan, and Y. Tian. Improving vehicular authentication in vanet using cryptography. *International Journal of Communication Networks and Information Security*, 10(1):248–255, 2018.

[7] R. Al-Sehrawy and B. Kumar. Digital twins in architecture, engineering, construction and operations. a brief review and analysis. In *International Conference on Computing in Civil and Building Engineering*, pages 924–939. Springer, 2020.

[8] B. Alaya and L. Sellami. Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban vanet networks. *Journal of Information Security and Applications*, 58:102779, 2021.

[9] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, and K. Sakurai. Authentication in mobile cloud computing: A survey. *Journal of Network and Computer Applications*, 61:59–80, 2016.

[10] S. AlJanah, N. Zhang, and S. Tay. A survey on smart home authentication: Toward secure, multi-level and interaction-based identification. *IEEE Access*, PP:1–1, 09 2021.

[11] K. Alshammari, T. Beach, and Y. Rezgui. Cybersecurity for digital twins in the built environment: current research and future directions. *Journal of Information Technology in Construction*, 26:159–173, 2021.

[12] B. A. Alzahrani, A. Irshad, A. Albeshri, and K. Alsubhi. A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks. *Wireless Personal Communications*, 117(1):47–69, 2021.

[13] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, et al. Understanding the mirai botnet. In *26th USENIX security symposium (USENIX Security 17)*, pages 1093–1110, 2017.

[14] J. Autiosalo, R. Ala-Laurinaho, J. Mattila, M. Valtonen, V. Peltoranta, and K. Tammi. To-

wards integrated digital twins for industrial products: Case study on an overhead crane. *Applied Sciences*, 11(2):683, 2021.

[15] O. O. Bamasag and K. Youcef-Toumi. Towards continuous authentication in internet of things based on secret sharing scheme. In *Proceedings of the WESS'15: Workshop on Embedded Systems Security*, WESS'15, New York, NY, USA, 2015. Association for Computing Machinery.

[16] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani. Lightweight mutual authentication protocol for v2g using physical unclonable function. *IEEE Transactions on Vehicular Technology*, 69(7):7234–7246, 2020.

[17] M. Barbareschi, A. De Benedictis, E. La Montagna, A. Mazzeo, and N. Mazzocca. A puf-based mutual authentication scheme for cloud-edges iot systems. *Future Generation Computer Systems*, 101:246–261, 2019.

[18] M. Barbareschi, A. De Benedictis, E. La Montagna, A. Mazzeo, and N. Mazzocca. Puf-enabled authentication-as-a-service in fog-iot systems. In *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, pages 58–63. IEEE, 2019.

[19] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-secure key distribution for dynamic conferences. In *Annual international cryptology conference*, pages 471–486. Springer, 1992.

[20] M. Bobby and D. Usha. A survey of internet of things (iot) -authentication schemes. XII:535–540, 07 2019.

[21] S. Céspedes, S. Taha, and X. Shen. A multihop-authenticated proxy mobile ip scheme for asymmetric vanets. *IEEE Transactions on Vehicular Technology*, 62(7):3271–3286, 2013.

[22] C.-J. Chae, K.-N. Choi, K. Choi, Y.-H. Yae, and Y. Shin. The extended authentication protocol using e-mail authentication in oauth 2.0 protocol for secure granting of user access. *Journal of Internet Computing and Services*, 16:21–28, 02 2015.

[23] R. R. K. Chaudhary and K. Chatterjee. An efficient lightweight cryptographic technique for iot based e-healthcare system. In *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*, pages 991–995, 2020.

[24] L. Chen, T. Tu, K. Yu, M. Zhao, and Y. Wang. V-ldaa: A new lattice-based direct anonymous attestation scheme for vanets system. *Security and Communication Networks*, 2021, 2021.

[25] T.-H. Chen, H.-l. Yeh, and W.-K. Shih. An advanced ecc dynamic id-based remote mutual authentication scheme for cloud computing. pages 155–159, 06 2011.

[26] S. R. Chhetri, S. Faezi, A. Canedo, and M. A. A. Faruque. Quilt: Quality inference from living digital twins in iot-enabled manufacturing systems. In *Proceedings of the International Conference on Internet of Things Design and Implementation*, pages 237–248, 2019.

[27] T. W. Chim, S.-M. Yiu, V. Li, and J. Zhong. Prga: Privacy-preserving recording gateway-

assisted authentication of power usage information for smart grid. *IEEE Transactions on Dependable and Secure Computing*, 12:85–97, 01 2015.

[28] N. K. Chistousov, I. A. Kalmykov, D. V. Dukhovnyj, M. I. Kalmykov, and A. A. Olenev. Adaptive authentication protocol based on zero-knowledge proof. *Algorithms*, 15(2), 2022.

[29] F. Chu, R. Zhang, R. Ni, and W. Dai. An improved identity authentication scheme for internet of things in heterogeneous networking environments. pages 589–593, 09 2013.

[30] Y.-H. Chuang and C.-L. Lei. Puf based authenticated key exchange protocol for iot without verifiers and explicit crps. *IEEE Access*, PP:1–1, 08 2021.

[31] Y.-H. Chuang and Y.-M. Tseng. Towards generalized id-based user authentication for mobile multi-server environment. *International Journal of Communication Systems*, 25:447–460, 04 2012.

[32] Y. Chung, S. Choi, Y. Lee, N. Park, and D. Won. An enhanced lightweight anonymous authentication scheme for a scalable localization roaming service in wireless sensor networks. *Sensors*, 16(10):1653, 2016.

[33] T. Dang and C. Devic. Ocari: Optimization of communication for ad hoc reliable industrial networks. In *2008 6th IEEE International Conference on Industrial Informatics*, pages 688–693. IEEE, 2008.

[34] A. K. Das and B. Bruhadeshwar. A biometric-based user authentication scheme for heterogeneous wireless sensor networks. In *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, pages 291–296. IEEE, 2013.

[35] M. L. Das. Two-factor user authentication in wireless sensor networks. *IEEE transactions on wireless communications*, 8(3):1086–1090, 2009.

[36] B. D. Deebak, F. H. Memon, X. Cheng, K. Dev, J. Hu, S. A. Khowaja, N. M. F. Qureshi, and K. H. Choi. Seamless privacy-preservation and authentication framework for iot-enabled smart ehealth systems. *Sustainable Cities and Society*, 80:103661, 2022.

[37] K. Dewangan, M. Mishra, and N. Dewangan. A review: a new authentication protocol for real-time healthcare monitoring system. *Irish Journal of Medical Science (1971 -)*, 190, 11 2020.

[38] W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, and A. Khalili. A pairwise key predistribution scheme for wireless sensor networks. *ACM Trans. Inf. Syst. Secur.*, 8:228–258, 05 2005.

[39] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni. A survey of internet of things (iot) authentication schemes. *Sensors*, 19(5), 2019.

[40] M. El-hajj, C. Maroun, A. Fadlallah, and A. Serhrouchni. Analysis of authentication techniques in internet of things (iot). pages 1–3, 10 2017.

[41] M. El-hajj, C. Maroun, A. Fadlallah, and A. Serhrouchni. Taxonomy of authentication techniques in internet of things (iot). pages 67–71, 12 2017.

[42] S. Emerson, Y.-K. Choi, D.-Y. Hwang, K.-S. Kim, and K.-H. Kim. An oauth based authen-

tication mechanism for iot networks. In *2015 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 1072–1074, 2015.

[43] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. G. Tauber, C. Schmittner, and J. Bastos. A lightweight authentication mechanism for m2m communications in industrial iot environment. *IEEE Internet of Things Journal*, 6(1):288–296, 2017.

[44] F. Fatemi Moghaddam, S. Moghaddam, S. Rouzbeh, S. Kohpayeh, N. Alibeigi, and S. Varnosfaderani. A scalable and efficient user authentication scheme for cloud computing environments. 04 2014.

[45] M. A. Ferrag, L. Maglaras, H. Janicke, and J. Jiang. Authentication protocols for internet of things: A comprehensive survey. 12 2016.

[46] M. A. Ferrag, L. Maglaras, H. Janicke, and J. Jiang. Authentication protocols for internet of things: A comprehensive survey. 12 2016.

[47] E. Glaessgen and D. Stargel. The digital twin paradigm for future nasa and us air force vehicles. In *53rd AIAA/ASME/ASCE/AHS/ASC structures, structural dynamics and materials conference 20th AIAA/ASME/AHS adaptive structures conference 14th AIAA*, page 1818, 2012.

[48] P. Gope. Pmake: Privacy-aware multi-factor authenticated key establishment scheme for advance metering infrastructure in smart grid. *Computer Communications*, 152:338–344, 2020.

[49] P. Gope, A. K. Das, N. Kumar, and Y. Cheng. Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks. *IEEE transactions on industrial informatics*, 15(9):4957–4968, 2019.

[50] P. Gope and T. Hwang. A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. *IEEE Transactions on industrial electronics*, 63(11):7124–7132, 2016.

[51] M. Grieves. Origins of the digital twin concept. *Florida Institute of Technology*, 8, 2016.

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

[53] J. Guo and Z. Lv. Application of digital twins in multiple fields. *Multimedia tools and applications*, pages 1–27, 2022.

[54] H. Hamidi. An approach to develop the smart health using internet of things and authentication based on biometric technology. *Future generation computer systems*, 91:434–449, 2019.

[55] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni. Bubbles of trust: a decentralized blockchain-based authentication system for iot. *Computers Security*, 78, 06 2018.

[56] M. T. Hammi, E. Livolant, P. Bellot, A. Serhrouchni, and P. Minet. A lightweight mutual authentication protocol for the iot. pages 3–12, 06 2018.

[57] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna. A privacy-preserving cryptosystem for iot e-healthcare. *Information Sciences*, 527:493–510, 2020.

[58] Y. Hao, Y. Cheng, and K. Ren. Distributed key management with protection against rsu compromise in group signature based vanets. In *IEEE GLOBECOM 2008-2008 IEEE global telecommunications conference*, pages 1–5. IEEE, 2008.

[59] V. T. Hayashi and W. V. Ruggiero. Hands-free authentication for virtual assistants with trusted iot device and machine learning. *Sensors*, 22(4), 2022.

[60] M. Hearn and S. Rix. Cybersecurity considerations for digital twin implementations. *IIC J. Innov*, pages 107–113, 2019.

[61] N. Hegde and S. S. Manvi. Mfzkap: Multi factor zero knowledge proof authentication for secure service in vehicular cloud computing. In *2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP)*, pages 1–6. IEEE, 2019.

[62] D. Holmes, M. Papathanasaki, L. Maglaras, M. A. Ferrag, S. Nepal, and H. Janicke. Digital twins and cyber security–solution or challenge? In *2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, pages 1–8. IEEE, 2021.

[63] N. Hong. A security framework for the internet of things based on public key infrastructure. In *Construction and Urban Planning*, volume 671 of *Advanced Materials Research*, pages 3223–3226. Trans Tech Publications Ltd, 6 2013.

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

[65] M. Jan, P. Nanda, M. Usman, and X. He. Pawn: a payload-based mutual authentication scheme for wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 29(17):e3986, 2017.

[66] R. S. M. Joshitta and L. Arockiam. Authentication in iot environment: A survey. *International Journal of Advanced Research in Computer Science and Software Engineering*, 6, 2016.

[67] B. Ketzler, V. Naserentin, F. Latino, C. Zangelidis, L. Thuvander, and A. Logg. Digital twins for cities: A state of the art review. *Built Environment*, 46(4):547–573, 2020.

[68] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle. Dtls based security and two-way authentication for the internet of things. *Ad Hoc Networks*, 11(8):2710–2723, 2013.

[69] K. J. Kuehner, R. Scheer, and S. Strassburger. Digital twin: finding common ground–a meta-review. *Procedia CIRP*, 104:1227–1232, 2021.

[70] D. Kumar, S. K. Pachigolla, S. S. Manhas, and K. Rawat. Cryptanalysis and improvement of mutual authentication protocol for real-time data access in industrial wireless sensor networks. *International Journal of Computers and Applications*, pages 1–14, 2020.

[71] P. Kumar, S.-G. Lee, and H.-J. Lee. E-sap: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. *Sensors*, 12(2):1625–

1647, 2012.

[72] J.-Y. Lee, W. C. Lin, and Y.-H. Huang. A lightweight authentication protocol for internet of things. *2014 International Symposium on Next-Generation Electronics (ISNE)*, pages 1–2, 2014.

[73] J. Leng, D. Wang, W. Shen, X. Li, Q. Liu, and X. Chen. Digital twins-based smart manufacturing system design in industry 4.0: A review. *Journal of manufacturing systems*, 60:119–137, 2021.

[74] Q. Li and G. Cao. Multicast authentication in the smart grid with one-time signature. *IEEE Transactions on Smart Grid*, 2(4):686–696, 2011.

[75] K. Y. H. Lim, P. Zheng, and C.-H. Chen. A state-of-the-art survey of digital twin: techniques, engineering product lifecycle management and business innovation perspectives. *Journal of Intelligent Manufacturing*, 31(6):1313–1337, 2020.

[76] D. Liu, X. Liu, H. Zhang, H. Yu, W. Wang, L. Ma, J. Chen, and D. Li. Research on end-to-end security authentication protocol of nb-iot for smart grid based on physical unclonable function. In *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, pages 239–244. IEEE, 2019.

[77] D. Liu, P. Ning, and R. Li. Establishing pairwise keys in distributed sensor networks. *ACM Trans. Inf. Syst. Secur.*, 8:41–77, 02 2005.

[78] J. Liu, Y. Yu, J. Jia, S. Wang, P. Fan, H. Wang, and H. Zhang. Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular ad-hoc networks. *Tsinghua Science and Technology*, 24(5):575–584, 2019.

[79] X. Liu, Y. Yang, E. Xu, and Z. Jia. An authentication scheme in vanets based on group signature. In *International Conference on Intelligent Computing*, pages 346–355. Springer, 2019.

[80] J.-Z. Lu, T. Chen, J. Zhou, J. Yang, and J. Jiang. An enhanced biometrics-based remote user authentication scheme using smart cards. volume 3, pages 1643–1648, 12 2013.

[81] K. Mahmood, S. Chaudhry, H. Naqvi, T. Shon, and H. Ahmad. A lightweight message authentication scheme for smart grid communications in power sector. *Computers Electrical Engineering*, 52, 02 2016.

[82] P. Mall, R. Amin, A. K. Das, M. Leung, and K.-K. Choo. Puf-based authentication and key agreement protocols for iot, wsns and smart grids: A comprehensive survey. *IEEE Internet of Things Journal*, PP:1–1, 01 2022.

[83] Malwiki. Stuxnet, 2010.

[84] J. A. Marmolejo-Saucedo, M. Hurtado-Hernandez, and R. Suarez-Valdes. Digital twins in supply chain management: a brief literature review. In *International Conference on Intelligent Computing & Optimization*, pages 653–661. Springer, 2019.

[85] C. Miller. Throwback attack: Blackenergy attacks the ukrainian power grid, 2015.

[86] A. Mnif, O. Cheikhrouhou, and M. B. Jemaa. An id-based user authentication scheme for wireless sensor networks using ecc. In *ICM 2011 Proceeding*, pages 1–9. IEEE, 2011.

[87] M. Mukhandi, E. Andrade, F. Damião, J. Granjal, and J. P. Vilela. Blockchain-based scalable authentication for iot. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, pages 667–668, 2020.

[88] P. Mundhe, V. K. Yadav, S. Verma, and S. Venkatesan. Efficient lattice-based ring signature for message authentication in vanets. *IEEE Systems Journal*, 14(4):5463–5474, 2020.

[89] S. Neethirajan and B. Kemp. Digital twins in livestock farming. *Animals*, 11(4):1008, 2021.

[90] T.-D. Nguyen and E.-N. Huh. A dynamic id-based authentication scheme for m2m communication of healthcare systems. *Int. Arab J. Inf. Technol.*, 9(6):511–519, 2012.

[91] Y. Park and Y. Park. Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks. *Sensors*, 16:2123, 12 2016.

[92] S. Peng. An id-based multiple authentication scheme against attacks in wireless sensor networks. In *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, volume 3, pages 1042–1045. IEEE, 2012.

[93] M. Perno, L. Hvam, and A. Haug. Implementation of digital twins in the process industry: A systematic literature review of enablers and barriers. *Computers in Industry*, 134:103558, 2022.

[94] R. Piascik, J. Vickers, D. Lowry, S. Scotti, J. Stewart, and A. Calomino. Technology area 12: Materials, structures, mechanical systems, and manufacturing road map. *NASA Office of Chief Technologist*, pages 15–88, 2010.

[95] M. Picone, M. Mamei, and F. Zambonelli. Wldt: A general purpose library to build iot digital twins. *SoftwareX*, 13:100661, 2021.

[96] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila. Two-phase authentication protocol for wireless sensor networks in distributed iot applications. In *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 2728–2733, 2014.

[97] C. Powell, T. Aizawa, and M. Munetomo. Design of an sso authentication infrastructure for heterogeneous inter-cloud environments. pages 102–107, 11 2014.

[98] I. Pranata, R. Athauda, and G. Skinner. Securing and governing access in ad-hoc networks of internet of things. 12 2012.

[99] C. Pylianidis, S. Osinga, and I. N. Athanasiadis. Introducing digital twins to agriculture. *Computers and Electronics in Agriculture*, 184:105942, 2021.

[100] A. M. Qazi, S. H. Mahmood, A. Haleem, S. Bahl, M. Javaid, and K. Gopal. The impact of smart materials, digital twins (dts) and internet of things (iot) in an industry 4.0 integrated automation industry. *Materials Today: Proceedings*, 2022.

[101] A. Qousini. Role-based access control model for privacy preservation in cloud computing environment. *The University of Jordan, Amman*, 2015.

[102] V. Rajasekar, P. Jayapaul, S. Krishnamoorthi, and M. Saračević. Secure remote user au-

thentication scheme on health care, iot and cloud applications: A multilayer systematic survey. *Acta Polytechnica Hungarica*, 18:87–106, 01 2021.

[103] M. Rana, Q. Mamun, and R. Islam. Lightweight cryptography in iot networks: A survey. *Future Generation Computer Systems*, 129:77–89, 2022.

[104] A. A. Rasheed, R. N. Mahapatra, and F. G. Hamza-Lup. Adaptive group-based zero knowledge proof-authentication protocol in vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 21(2):867–881, 2019.

[105] A. Redelinghuys, K. Kruger, and A. Basson. A six-layer architecture for digital twins with aggregation. In *International Workshop on Service Orientation in Holonic and Multi-Agent Manufacturing*, pages 171–182. Springer, 2019.

[106] S. S. Reza, M. M. Arifeen, S. K. Tiong, M. Akhteruzzaman, N. Amin, M. Shakeri, A. Ayob, and A. Hussain. Salsa20 based lightweight security scheme for smart meter communication in smart grid. *Telkomnika*, 18(1):228–233, 2020.

[107] R. Rosli, Y. M. Yusoff, and H. Hashim. Performance analysis of id-based authentication on zigbee transceiver. In *2012 IEEE Symposium on Wireless Technology and Applications (ISWTA)*, pages 187–191. IEEE, 2012.

[108] A. Rossmann and D. Hertweck. Digital twins: A meta-review on their conceptualization, application, and reference architecture. In *HICSS*, pages 1–10, 2022.

[109] M. Saadeh, A. Sleit, M. Qatawneh, and W. Almobaideen. Authentication techniques for the internet of things: A survey. pages 28–34, 08 2016.

[110] M. Sarvabhatla, L. N. Kodavali, and C. S. Vorugunti. An energy efficient temporal credential based mutual authentication scheme for wsn. In *2014 3rd International Conference on Eco-friendly Computing and Communication Systems*, pages 73–78. IEEE, 2014.

[111] M. Sarvabhatla and C. S. Vorugunti. A secure biometric-based user authentication scheme for heterogeneous wsn. In *2014 Fourth international conference of emerging applications of information technology*, pages 367–372. IEEE, 2014.

[112] C. Schmitt, M. Noack, and B. Stiller. Chapter 13 - tinyto: two-way authentication for constrained devices in the internet of things. In R. Buyya and A. Vahid Dastjerdi, editors, *Internet of Things*, pages 239–258. Morgan Kaufmann, 2016.

[113] A. Sharma, E. Kosasih, J. Zhang, A. Brintrup, and A. Calinescu. Digital twins: State of the art theory and practice, challenges, and open research questions. *arXiv preprint arXiv:2011.02833*, 2020.

[114] A. Singh and K. Chatterjee. A secure multi-tier authentication scheme in cloud computing environment. pages 1–7, 03 2015.

[115] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar. Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things. *IEEE Transactions on Dependable and Secure Computing*, 17(6):1133–1146, 2018.

[116] J. Srinivas, S. Mukhopadhyay, and D. Mishra. Secure and efficient user authentica-

tion scheme for multi-gateway wireless sensor networks. *Ad Hoc Networks*, 54:147–169, 2017.

[117] R. Stark and T. Damerau. *Digital Twin*, pages 1–8. Springer Berlin Heidelberg, Berlin, Heidelberg, 2019.

[118] S. Suganthi, R. Anitha, V. Sureshkumar, S. Harish, and S. Agalya. End to end light weight mutual authentication scheme in iot-based healthcare environment. *Journal of Reliable Intelligent Environments*, 6(1):3–13, 2020.

[119] S. Suhail, R. Hussain, R. Jurdak, and C. S. Hong. Trustworthy digital twins in the industrial internet of things with blockchain. *IEEE Internet Computing*, 2021.

[120] S. Suhail, S. Zeadally, R. Jurdak, R. Hussain, R. Matulevičius, and D. Svetinovic. Security attacks and solutions for digital twins. *arXiv preprint arXiv:2202.12501*, 2022.

[121] M. Tahavori and F. Moazami. Lightweight and secure puf-based authenticated key agreement scheme for smart grid. *Peer-to-Peer Networking and Applications*, 13(5):1616–1628, 2020.

[122] M. Taleby Ahvanooey, M. Zhu, W. Mazurczyk, Q. Li, K.-K. R. Choo, B. B. Gupta, and M. Conti. Modern authentication schemes in smartphones and iot devices: An empirical survey. *IEEE Internet of Things Journal*, 9:1–25, 12 2021.

[123] H.-R. Tseng, R.-H. Jan, and W. Yang. A robust password-based authentication scheme for heterogeneous sensor networks. *Communications of IICM*, 11(3):1–13, 2008.

[124] M. Turkanović, B. Brumen, and M. Hölbl. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. *Ad Hoc Networks*, 20:96–112, 04 2014.

[125] T. van de Meent. A comparative study on lightweight authentication protocols in iot, 2022.

[126] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy. Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks. *cluster computing*, 20(3):2439–2450, 2017.

[127] Votiro. The colonial pipeline ransomware attack: Everything we know, 2021.

[128] J. Wang, L. Wu, K.-K. R. Choo, and D. He. Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. *IEEE Transactions on Industrial Informatics*, 16(3):1984–1992, 2019.

[129] M. Wazid, A. K. Das, and A. V. Vasilakos. Authenticated key management protocol for cloud-assisted body area sensor networks. *Journal of Network and Computer Applications*, 123:112–126, 2018.

[130] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya. A survey on vehicular cloud computing. *Journal of Network and Computer applications*, 40:325–344, 2014.

[131] Z.-Q. Wu, Y.-W. Zhou, and J.-F. Ma. A security transmission model for internet of things. *Chinese Journal of Computers*, 34:1351–1364, 08 2011.

[132] J. Yang and P. Lin. An id-based user authentication scheme for cloud computing. pages

98–101, 08 2014.

[133] K. Yang, D. Forte, and M. Tehranipoor. Protecting endpoint devices in iot supply chain. pages 351–356, 11 2015.

[134] N. YE, Y. Zhu, R.-c. WANG, R. Malekian, and L. Qiao-min. An efficient authentication and access control scheme for perception layer of internet of things. *Applied Mathematics Information Sciences*, 8, 07 2014.

[135] X. Yue, B. Chen, X. Wang, Y. Duan, M. Gao, and Y. He. An efficient and secure anonymous authentication scheme for vanets based on the framework of group signatures. *IEEE Access*, 6:62584–62600, 2018.

[136] Y. M. Yussoff, H. Hashim, and M. D. Baba. Identity-based trusted authentication in wireless sensor network. *arXiv preprint arXiv:1207.6185*, 2012.

[137] C. Zhang, X. Lin, R. Lu, and P.-H. Ho. Raise: An efficient rsu-aided message authentication scheme in vehicular communication networks. In *2008 IEEE international conference on communications*, pages 1451–1457. IEEE, 2008.

[138] Y. Zhao. Research on data security technology in internet of things. *Applied Mechanics and Materials*, 433-435:1752–1755, 10 2013.

[139] Y. Zhao. Research on data security technology in internet of things. *Applied Mechanics and Materials*, 433-435:1752–1755, 10 2013.

[140] L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu. Lightweight iot-based authentication scheme in cloud computing circumstance. *Future Generation Computer Systems*, 91:244–251, 2019.