Semantic Digital Twins: Security and Scale for Constrained IoT Devices

*Evandro Pioli Moro[1] and Alistair K Duke[2]

[1]p/p 9, 5th floor, Orion Building, Adastral Park,
Ipswich, IP5 3RE, United Kingdom

[1]*evandro.moro@bt.com
[2]alistair.duke@bt.com

* Corresponding Author

Abstract. Digital twins are largely used to enable the Industry 4.0 and other Internet of Things applications. This approach has been built to support the entire product lifecycle and has advantages such as interoperability, availability, and simulation capabilities. If integrated with distributed ledger technologies, such as blockchains, digital twins can augment their applications, becoming an anchor of trust for constrained IoT devices. This paper describes the Constrained Devices Management Platform, a British Telecommunications plc (BT) research system designed to enhance the security of IoT systems, with an especial focus on data provenance, immutability, and integrity. Lastly, the paper describes how semantics can enhance the Constrained Devices Management Platform (CDMP) capabilities through interoperability.

Keywords: Digital twins, internet of things, distributed ledger technologies, blockchain, cybersecurity, ontology, interoperability.

1   Introduction

Digital Twinning can be described as a method for turning physical devices into digital services [1]. These services can be used to satisfy the interaction requirements placed on physical devices in a more efficient and scalable way [2]. Application Programming Interfaces (APIs) allow control and access to the digital assets either by direct communication or to replicate this behaviour if the devices are not online or only send data periodically [3]. The APIs typically support requests such as 'What is the latest data?' and 'What are the changes to the state of the device?'. It is also possible to enhance the capability of the APIs with value-added data from elsewhere [4], semantical operations [5], or via analysis [6].

The approach has been developed to support the lifecycle of devices throughout design, manufacture, and operation [7]. During the design process, the APIs can be used in simulations before the device itself even exists. During manufacture, the results from the simulations can be used to enhance and optimise the manufacturing processes. While during operations, the digital twins (DTs) can provide a virtual simulation environment and optimise data operations, reducing the communications requirements, hence reducing the latency and increasing battery life.

One of the most prominent applications of DTs is to support the enablement of the Industry 4.0 [8]. Industry 4.0 provides data operations to devices and products throughout their entire lifecycle—from concept to recycling [9]. It is often branded as the Industrial Internet of Things (IIoT). This data can be used to influence the manufacture of the product, for example, or to provide real-time lifecycle management to an entire line of products. DTs are centric to this approach, as it enables a virtual entity of the physical devices so that other processes can provide insight and actuation to the entire system.

2   Internet of Things

2.1   Introduction

The Internet of Things (IoT) has various meanings in different applications. However, one standard definition that is central to the concept of DT is the provision of connectivity and data exchanging facilities to various devices for real-time data operations [10].

The rapid deployment of IoT systems has delivered exceptional opportunities to various industries, especially regarding data capture and observability. The cost of deployment of IoT has been decreasing over time, but the attention to cybersecurity has not accompanied the pace of IoT developments, once it is often seen as an economic harness to the solution [11]. More cheap and computational constrained devices are being connected, making running traditional cybersecurity protocols on them unfeasible.

2.2   Relevance of DT for IoT cybersecurity

Centric to the research that British Telecommunications (BT) does on IoT systems is applying breakthrough networking technologies to enhance the cybersecurity of constrained IoT devices. Recently, the combination of DTs and blockchain has proven useful to counteract cyber threats. DTs provide four main advantages to

support cybersecurity applications at a networking level:

- Simulation environment. By using real-time data, the DT may incorporate predictive analytics so that it can help to determine when an asset is likely to fail and what are the potential consequences of such fault. Alternatively, predictive analytics can be used to optimise the overall system operations [6] and cybersecurity.

- Data sharing across siloes. DT can act as a data proxy to collect data from sensors in different environments, instead of each silo capturing their own data, enhancing interoperability [12]. Interoperability, at the same time, increase the overall system observability, improving the understanding of the system's global security.

- Real-time operations management. The digital assets create situational awareness by building a holistic picture of the environment it represents. By enabling real-time visibility, recommendations and actions, the users can perform real-time operations using decisions based on data [3]. With the aid of real-time operations management, the system administrator can then counteract cybersercurity events quicker.

- Availability and reliability. Because DT does not rely on the availability of communication channels, DT provides a globally shared understanding of what an entity looks like in near real-time [3]. The increased reliability and availability reduces the attack surface for external sources, making the system less prone to failures and attacks.

2.3   Relevance of Distributed Ledger Technologies for IoT cybersecurity

Distributed Ledger Technologies (DLT) have their most prominent application on blockchains. DLT is a peer-to-peer networking system where a ledger of transactions is synchronised among peers [13]. If the transactions ledger is immutable and structured in the form of blocks of information linked to the previous blocks via a hashing operation, then the DLT is called a blockchain. The transactions synchronisation process occurs via a protocol called consensus. The consensus protocol is often a computationally-intensive process [14] to chose the peer responsible for generating the new block by validating and aggregating the transactions. Consensus protocols also set how long it takes for a block to be generated (and consequently, how long it takes for the transactions to be validated). Various consensus protocols exist, and their choice is paramount to the success of the blockchain [15].

Blockchain networks offer various advantages when compared to traditional distributed data sharing facilities (including databases). These include immutability, enhanced fault tolerance, auditability, transparency, and decentralised trust provision [16]. However, blockchains might also offer drawbacks such as increased computational power consumption and longer transaction processing times [14] (in 2020, the public Bitcoin network took between 8-11 minutes to validate a transaction by creating a new block [17]).

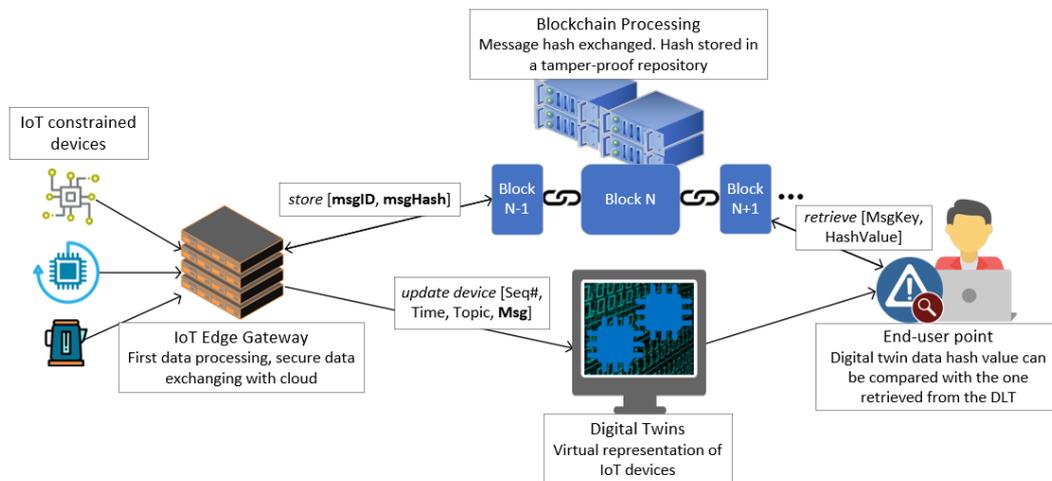## 3   Constrained Devices Management Platform

Combining the aforementioned cybersecurity advantages of DT with the unique trustless and immutability features of blockchains, BT introduced a prototype platform called Constrained Devices Management Platform (CDMP).

With a particular focus on data integrity and data provenance for battery and network-constrained IoT devices, the CDMP reduces the networking requirements of the IoT sensors by performing the heavy security operations on a cloud service. The cloud operations include data integrity, provenance, and immutability by combining sensors digital twinning with blockchain storage and hashing operations.

The data from a sensor is transferred in a local area network (LAN) to a network gateway. Upon arrival at the gateway, the message is signed using blockchain scripts (smart contracts) where the message identifier (msgID) and the message hash (msgHash), along with other use case-specific parameters, are stored within the blockchain, and hence are immutable. The gateway will then update the DT with the latest data available. Upon retrieval, the end-user can verify the integrity and provenance of the IoT data fetched from the DT by retrieving the msgHash from the blockchain and comparing it with the hashing operation performed locally. The protocols/APIs used to exchange data with the CDMP are secured on the enhanced gateways, where outgoing communications are completed over a virtual private network (VPN).

The DT framework utilised on this technology concept was Eclipse Ditto. Ditto was integrated with a private instance of the Ethereum blockchain framework, set with a proof-of-authority (POA) consensus algorithm. With POA, the transactions could be processed quicker (in less than a second) without compromising security. POA is also very computational power and energy efficient. While providing the system the necessary immutability and verifiability, this consensus algorithm optimise the costs of deployment and operations of the blockchain.

The CDMP, therefore, offers the end-users the ability to perform digital twinning of physical assets while being able to verify the integrity of the messages via crypto operations. Upon delivery, platform indicates whether the message is integral and issues an alert if it is not. In this case, the platform also indicates the unreliable link, if there are more than one signing gateway, and indicates whether the data is ready to be consumed. The diagram in Fig. 1. depicts the data flow on a generic IoT environment where the CDMP is used.

Fig. 1. Constrained Devices Management Platform basic components architecture and data flow

4 Semantics in a Digital Twins for cybersecurity context

In the current platform, devices are reflected in the DT by a set of attributes and features. The attributes represent the more static properties of the device. The features, which might include a set of properties and a set of desired properties, are used to model the more dynamic aspects of the physical device. Because this framework favours flexibility, allowing the DTs to be very closely aligned with the physical asset, various data models might co-exist in the virtual world. This makes it challenging to manage a system involving many device types where data might be defined in different and even contradictory ways. From a cybersecurity perspective, identifying problematic devices or messages using a collective threat model becomes difficult, potentially requiring bespoke translation to each type of device or message, increasing the complexity of such a system.

Adopting an approach based on a common ontology will help to solve these issues. One such approach would be to introduce an abstraction layer between the different devices and the DT. One example is the one employed by Eclipse Vorto[1]. Vorto allows the creation and management of technology agnostic, abstract device descriptions. An alternative approach would be to create a relationship between the more device-specific twins and a generic ontological representation that forms the abstraction layer. Here, the twin features would contain metadata creating a mapping to an ontology describing the device type or data type concerned. This way, the device data can be expressed in terms of one or more ontologies, facilitating querying and reasoning over the data at the ontological level. Further on, research and standardisation bodies, such as the W3C Web of Things, the Asset Administration Shell, and the Industrial Internet Consortium, define and encourage the use of standardised data models, also in the form of ontologies. Increasing the use of these well-defined data models increase the interoperability, reuse, and reliability of DT systems and would, at the same time, improve cybersecurity mechanisms. All of the aforementioned approaches would allow threat models, which describe suspicious behaviour associated with particular types of devices, to be evaluated in systems involving multiple instantiations of those device types (e.g., different manufacturers or versions).

5   Conclusion

This paper explored the use cases of semantic digital twins for light-weight cybersecurity, focusing on battery and network-constrained IoT devices. It discussed the Constrained Devices Management Platform (CDMP), a system leveraging the combination of DT and blockchain to provide data integrity and data provenance for battery and network-constrained IoT devices. The CDMP improves the network operations and security of IoT devices, reducing the battery and computational power requirements. The paper then discussed the impact of the semantics in DT and how interoperability is vital in an IoT cybersecurity scenario.

The next steps for the CDMP development include customer trials scheduled to start in May 2021. The DMP will incorporate the systems of the ongoing project i-Trace[2], and Innovate UK project with Costain, Cısco, the University of Warwick, and Senseon. i-Trace is an end-to-end cybersecurity solution using DT,

---

[1] http://www.eclipse.org/vorto/

[2] https://www.i-trace.co.uk/

blockchain, and artificial intelligence to provide a resilient security framework to IoT devices. The use cases will likely be related to smart construction sites. The CDMP will compose the overall architecture to provide the data integrity and data provenance facilities.

References

1. Stojanovic, V., Trapp, M., Richter, R., Hagedorn, B., & Döllner, J. (2019). Semantic Enrichment of Indoor Point Clouds-An Overview of Progress towards Digital Twinning.
2. Schleich, B., Anwer, N., Mathieu, L., & Wartzack, S. (2017). Shaping the digital twin for design and production engineering. CIRP Annals, 66(1), 141-144.
3. Platenius-Mohr, M., Malakuti, S., Grüner, S., Schmitt, J., & Goldschmidt, T. (2020). File-and API-based interoperability of digital twins by model transformation: An IIoT case study using asset administration shell. Future Generation Computer Systems, 113, 94-105.
4. Malakuti, S., & Grüner, S. (2018, September). Architectural aspects of digital twins in IIoT systems. In Proceedings of the 12th European conference on software architecture: companion proceedings (pp. 1-2).
5. Datta, S. P. A. (2016). Emergence of digital twins. arXiv preprint arXiv:1610.06467.
6. Erikstad, S. O. (2017). Merging physics, big data analytics and simulation for the next-generation digital twins. High-Performance Marine Vehicles, 141-151.
7. Canedo, A. (2016, October). Industrial IoT lifecycle via digital twins. In Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis (pp. 1-1).
8. Preuveneers, D., Joosen, W., & Ilie-Zudor, E. (2018, October). Robust digital twin compositions for Industry 4.0 smart manufacturing systems. In 2018 IEEE 22nd International Enterprise Distributed Object Computing Workshop (EDOCW) (pp. 69-78). IEEE.
9. Vaidya, S., Ambad, P., & Bhosle, S. (2018). Industry 4.0–a glimpse. Procedia manufacturing, 20, 233-238.
10. Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. Ad Hoc Networks, 56, 122-140.
11. Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. Computers in industry, 102, 14-22.
12. Alam, K. M., & El Saddik, A. (2017). C2PS: A digital twin architecture reference model for the cloud-based cyber-physical systems. IEEE access, 5, 2050-2062.
13. Ben Mariem, S., Casas, P., & Donnet, B. (2018). Vivisecting blockchain P2P networks: Unveiling the Bitcoin IP network. In ACM CoNEXT student workshop.
14. Golosova, J., & Romanovs, A. (2018, October). Overview of the blockchain technology cases. In 2018 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS) (pp. 1-6). IEEE.
15. Shahaab, A., Lidgey, B., Hewage, C., & Khan, I. (2019). Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: A systematic review. IEEE Access, 7, 43622-43636.
16. Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). Applications of blockchains in the Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(2), 1676-1717.
17. Bitcoin Block Time Chart. (2021). Retrieved 2 March 2021, from https://bitinfocharts.com/comparison/bitcoin-confirmationtime.html