Association for Information Systems

AIS Electronic Library (AISeL)

BLED 2019 Proceedings

BLED Proceedings

2019

An Approach for Secure Data Transmission in a Distributed Production Environment

Matej Vuković

Christian Kittl

Jürgen Mangler

Stefan Thalmann,

32ND BLED ECONFERENCE
HUMANIZING TECHNOLOGY FOR A SUSTAINABLE SOCIETY
JUNE 16 – 19, 2019, BLED, SLOVENIA, CONFERENCE PROCEEDINGS
A. Pucihar (ed. et al.)

University of Maribor Press

An Approach for Secure Data Transmission in a Distributed Production Environment

MATEJ VUKOVIĆ, CHRISTIAN KITTL, JÜRGEN MANGLER & STEFAN THALMANN

Abstract The exchange of data along the supply chain can be viewed as one of the key characteristics of advanced manufacturing concepts, frequently labeled as industry 4.0 . Intelligent products produced in shorter life cycles, increasing cost and quality pressures from global supply chains, increasingly complex regulatory requirements, as well as decreasing costs of advanced sensors are major drivers for this trend. Large amounts of data generated as a by-product of this trend represents an opportunity for advanced data analytics. However, the exchange of data across organizational boundaries bears also the risks of being in the focus of cyber-attacks. In this paper, we tackle the challenge of securing the data transfer in an Industry 4.0 environment. We first identify the security requirements within our use case. Based on these requirements, we present an approach for secure data transmission and discuss how our solution meets the identified requirements.

Keywords: • Digitalization • Secure architecture • Data transmission • Production environment • Encryption •

CORRESPONDENCE ADDRESS: Matej Vuković, MSc, Evolaris next level GmbH, Graz, Austria, e-mail: matej.vukovic@evolaris.net. Christian Kittl, Ph.D., Evolaris next level GmbH, Graz, Austria, e-mail: christian.kittl@evolaris.net. Jürgen Mangler, Center for Digital Production, Wien, Austria, juergen.mangler@univie.ac.at. Stefan Thalmann, PhD, University of Graz, Graz, Austria, e-mail: stefan.thalmann@uni-graz.at.

DOI https://doi.org/10.18690/978-961-286-280-0.60 ISBN 978-961-286-280-0
Dostopno na: http://press.um.si

1 Introduction

The exchange of data along the supply chain can be viewed as one of the key characteristics of advanced manufacturing concepts, e.g. industry 4.0 (Kagermann, 2015). Intelligent products produced in shorter life cycles, increasing cost and quality pressures from global supply chains and increasingly complex regulatory requirements are major drivers for this trend (Kache & Seuring, 2017). Additionally, inexpensive sensors enable companies to collect more and more data about even more diverse aspects of their production lines and affordable cloud-based services to store or compute these data. This however leads to big data sets which cannot be processed by human experts anymore. For this purpose, data analytics promise huge advantages. However, the exchange of data across organizational boundaries bears also the risks of being in the focus of cyber-attacks (Stjepandić, Liese & Trappey, 2015) or the risks of losing competitive knowledge or of revealing business insights to other companies or even to competitors (Ilvonen et al., 2018). Both threats (1) to be a possible target of a cyber-attack and (2) not to know which business insights or critical knowledge an external part can derive from shared data are major concerns of organizations in general (North et al., 2019).

To allow digital innovations by fostering digitization, companies have to balance the benefits expected from digitization and the risks may arising from those technologies (Thalmann & Ilvonen, 2018). As manufacturing data is the core of manufacturing companies' competitive advantage, security systems need to be developed to prevent unauthorized access to data and thus to reduce the risk of digitization (Thoben, Stefan, & Wuest, 2017). The challenge in this regard is, that data comes from different types of Internet of Things (IOT) devices and sensors and all of these devices need to be connected but often they are not designed with security in mind. As a result of this situation, the connection between these heterogeneous systems is often vulnerable, especially in a cross-plant scenario.

In the work of (Priller et al., 2014) migration of the existing industrial devices into the world of Smart Services was discussed and initial guide was developed for establishing efficient and secure interaction between different production subsystems. (Maritsch et al., 2015) show the superiority of MQTT over other protocols for the secure device connection in the context of smart factories. In the work of (Lesjak et al., 2015) a connection between devices on the field and the message broker was discussed. After it was shown how to securely connect and authenticate devices, an approach for data encryption on a single device was proposed in (Lesjak et al., 2016). (Maritsch et al., 2016) propose different message broker architectures. However, neither of them can be applied in our use case for various reasons (existing data transmission mechanisms in place, customer owns the data storage, etc.). Hence, we want to investigate how a system architecture can look like enabling easy integration into an already running shop floor.

2 Methodology

In our research we are following a Design Science Research Methodology (Hevner et al., 2004) (Clarke, 2017) (K. Peffers et al., 2007). In the relevance cycle we have identified the challenge of securing the data transmission within the Industry 4.0 use-case. Specifically, we investigated the case of the Smart Factory Vienna and first identified the security requirements. In our design cycle, we defined the requirements and the objectives of the new solution in the Use-Case section of this paper. In our rigor cycle, we researched the literature for existing solutions and approaches suitable for our identified design problem.

The current architectural solutions did not satisfy the requirements and objectives of the current use-case. Hence, we designed and developed a new architectural solution for the secure data transfer that is described in detail in The Proposed Solution section. This solution is then demonstrated in the “Pilotfabrik Industrie 4.0” and will be evaluated in the future work.

3 Use-Case

The “Pilotfabrik Industrie 4.0” in Vienna is a demonstrator plant that also produces parts for customers. Artefacts to exemplify production in the context of this paper are:

- EMCO MaxxTurn 45 lathe, integrated OPCUA server.
- ABB IRB 2600 industrial robot, ABB specific interface.
- Neobotics AGV, proprietary REST interface.

- UI to enter part measurements running on a Raspberry PI 3B+, proprietary REST interface.
- Inateck QR Code Scanner connected to a Raspberry PI 3B+, proprietary REST interface.

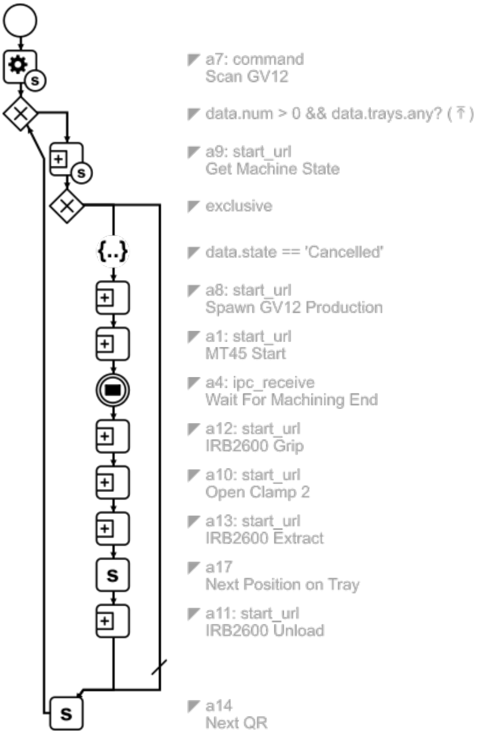

Figure 1

Artefacts consist of hardware and software that either produces data streams, or can be polled for data points. Each Artefact is wrapped by an adapter that pushes the data stream to an Extensible Messaging and Presence Protocol (XMPP) server, where it is available for consumption. The individual artefacts are independent, they do not know anything of each other. All logic how the machines interact are handled by a cloud based cell orchestration solution, in this case by centurio.work (Pauker, 2018). Centurio.work instantiates and executes process models, in order to (1) produce a specific part, (2) collect data from all participated artefacts during production, and (3) ensure that all artefacts work correctly together during production. On the left-hand side an example process is depicted. In the example process an operator scans a QR code, which results in the production of a batch of products, which are loaded on to a tray on top of an AGV. The AGV the delivers the batch of parts to the operator which can measure the compliance with tolerances, and separate good from bad parts.

The network inside the Pilotfabrik is in a demilitarized zone (DMZ) and deemed problematic, as many parties share same network / have access to network ports.

Based on this setting the following requirements can been elicited:

- Low Latency / high performance: the collected data is used to coordinate Machines, and to show real-time data about the production. The machines produce up to 2 MiB per second.
- Tamperproof Data Flow: the customers demand a detailed protocol about production for long-time warranty issues. Furthermore, tampering with data could lead to potentially fatal decisions for the interaction between the machines.
- Quality of service has to be ensured.
- Identity spoofing / man in the middle attacks should be prohibited by introducing transport layer security, and end-to-end encryption.

All the machines are configured so that the above-mentioned wrapper is the only means of accessing the machine. The wrapper is thus necessary to (1) deny access to potentially insecure resources, (2) deal with no-routable protocols.

4 The Proposed Solution

In this section we describe our proposed architecture of our approach and how it satisfies the requirements defined in the use case. In the following text our approach is described in a single tenant context. However, multi-tenant application is possible with minimal extensions to the proposed architecture. Overview of the architecture of our approach is shown in the figure 2.

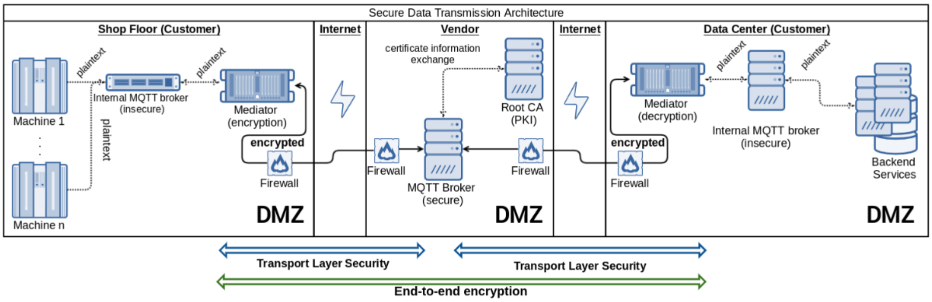

Figure 2 Architecture of the proposed approach

To satisfy the requirements defined in the use case we developed a secure data transmission infrastructure based on Message Queuing Telemetry Transport (MQTT). MQTT is providing a lightweight publish/subscribe message transport (Lampkin et al., 2012). We base our work on top of solutions proposed in (Lesjak et al., 2016), (Maritsch et al., 2016), (Priller et al., 2014) and (Lesjak et al., 2015). Selection of this technology reflected on other elements of the proposed architecture. Aside from the selection of MQTT as a base communication technology, architecture was designed around non-intrusiveness and ease of integration into the currently running system. In this sense customer sends and receives the data in non-encrypted, plain text form and message encryption, message decryption, message integrity, client authorization and other security tasks are handled by the subsystems of the secure data transmission architecture. Data exchange is secured in two layers.

In the first layer data is secured using Transport Layer Security (TLS). This protocol provides data encryption, data integrity checks and client authentication on the transport layer. Client authentication is required whenever one of the clients initiates a connection to the message broker. Using this mechanism, we make sure that the subsystems on both endpoints are authenticated and only selected subsystems can send or receive the data. However, this layer only secures single connections, as single connections are secured, by using only TLS data is decrypted when received by the broker and encrypted again when establishing the connection with the subscriber. To prevent from data being exposed in the scenario of the broker being compromised we introduce second security layer to the architecture.

Second security layer in the proposed approach is end-to-end encryption. In this layer devices that publish the data have predefined set of recipients and their public keys which they use to encrypt the data and create a so-called envelope. For each of the recipients, data is encrypted with their public key and upon receiving the data they can decrypt it using their private key. This approach creates a reasonable overhead that is a result of the multiplication of the encrypted data. Multiplication of data is happening because the encrypted message is created for each of the recipients defined on the side of the devices that publish the data. In our use case this overhead is avoided by using only one recipient that is the processing backend.
Our approach consists of several subsystems and in the following subsections these subsystems are described.

4.1 Message Broker

Message broker is a central component of our approach. Based on (Maritsch et al., 2016), we propose a new broker architecture making the integration as non-intrusive as possible and to leverage the advantages of the currently implemented infrastructure. The hybrid architecture uses one main message broker that contains a root Certificate Authority and two message brokers on the sending and the receiving end of the data transmission pipeline. Devices on the sending and receiving end of the architecture are located onsite in the DMZ. Message broker has two roles. On the one hand it mediates communication between MQTT clients (Lampkin et al., 2012) and is responsible for receiving messages, filtering and sending messages to the clients that are subscribed to them. On the other hand, within the infrastructure that message broker is running on, a Public Key Infrastructure (PKI) is created and it contains a root Certificate Authority. Root Certificate Authority signs all other generated certificates for each of the devices and clients in the data transmission pipeline. This results in a secure and trusting architecture where all of the clients must be authenticated by the certificate signed by the root Certificate Authority. If the client is not authenticated the connection to the message broker cannot be established.

With these mechanisms in place this approach allows only predefined clients to connect to the message broker and only predefined message receivers to decrypt the data. To make the integration efforts low no topics were defined in the message broker.

4.2 MQTT Clients

In our approach MQTT Clients represent subsystems that are in charge of sending the data (publishers) and receiving the data (subscribers). Both are single-board computers that have enough processing power for the tasks of encryption and decryption and running a Linux distribution.

For the devices that are sending the data we use a concept called Mediator (Priller et al., 2014). A Mediator is a gateway device that provides a modular extension to existing machines. It includes necessary computation and communication resources and can be connected with the machines via several interfaces. Usage of the Mediator addresses the legacy aspect of the machines by extending their functionality by enabling them to connect to the internet and encrypting the data. It also addresses the transparency aspect by enabling the customers to filter the data and select what do they want to transmit. Mediator device aggregates the production data produced by the machine, encrypts it, establishes the connection with the message broker and sends the aggregated data to the message broker.

5 Conclusion and outlook

Within this design science project we tackled the challenge of securing the data transfer in an Industry 4.0 use-case. We have developed an design artefact that satisfies the identified requirements. In our use case four requirements were defined: (1) low latency and high performance, (2) tamperproof data flow, (3) quality of service, (4) prevention of identity spoofing and man in the middle attacks. First requirement, (1) low latency and high performance, is addressed in related work (Lesjak et al., 2016) and proposed architecture and mediator devices provide reasonable and acceptable overhead. Second requirement, (2) tamperproof data flow, is addressed from several aspects. One aspect is TLS encryption and client authentication which ensures that only defined clients publish and subscribe to messages. Furthermore, end-to-end encryption ensures that data is transferred in the original state and no changes can be made to it without detection. Finally, mediator devices are connected to the machines via non-routable protocols and in the case of this devices being compromised, attacker is not able to penetrate the network. Requirement (3) quality of service is addressed by-design as a part of the MQTT protocol. Last requirement, (4) prevention of identity spoofing and man in the middle attack is addressed with the usage of TLS and client authentication and end-to-end encryption. Client authentication enables connection establishment to only those clients that have certificates signed by the root Certificate Authority. TLS on the other hand secures the connection to the message broker and from the message broker and encrypting and enveloping the data from sending end to the receiving end ensures that only receiving client can decrypt the data.

In future work we want to evaluate and benchmark the architecture in the pilot factory "Pilotfabrik Industrie 4.0", starting in June 2019. The system evaluation will be based on measuring the impact of securing the data transmission infrastructure compared to the insecure data transmission. Especially impact on the data velocity, volume and latency.

Acknowledgments

This research is done truly joint by the two Comet K1- Research Centers Pro2Future and Center for Digital Production (CDP). Pro2Future (Contract Nr. 854184) and CDP (Contract Nr. 854187) are funded within the Austrian COMET Program Competence Centers for Excellent Technologies under the auspices of the Austrian Federal Ministry of Transport, Innovation and Technology, the Austrian Federal Ministry for Digital and Economic Affairs and the Provinces of Upper Austria and Styria (for Pro2Future) and the Provinces of Vienna, Lower Austria, and Vorarlberg (for CDP). COMET is managed by the Austrian Research Promotion Agency FFG.

References

I. Ilvonen, S. Thalmann, M. Manhart, & C. Sillaber. (2018). Reconciling digital transformation and knowledge protection: a research agenda. Knowledge Management Research & Practice, 16(2), 235-244, DOI: 10.1080/14778238.2018.1445427

F. Kache & S. Seuring. (2017). Challenges and opportunities of digital information at the intersection of big data analytics and supply chain management. International Journal of Operations & Production Management. 37(1), 10–36. DOI: 10.1108/IJOPM-02-2015-0078

H. Kagermann. (2015). Change through digitization—Value creation in the age of Industry 4.0. In Management of permanent change (pp. 23-45). Springer Gabler, Wiesbaden

V. Lampkin, W. T. Leong, L. Olivera, S. Rawat, N. Subrahmanyam, & R. Xiang. (2012). Building smarter planet solutions with mqtt and ibm websphere mq telemetry. IBM Redbooks.

C. Lesjak, H. Bock, D. Hein & M. Maritsch, (2016, July). Hardware-secured and transparent multi-stakeholder data exchange for industrial iot. In 2016 IEEE 14th International Conference on Industrial Informatics (INDIN) (pp. 706-713). IEEE.

C. Lesjak, D. Hein, M. Hofmann, M. Maritsch, A. Aldrian, P. Priller, ... & G. Pregartner. (2015, July). Securing smart maintenance services: Hardware-security and TLS for MQTT. In 2015 IEEE 13th international conference on industrial informatics (INDIN) (pp. 1243-1250). IEEE.

M. Maritsch, C. Kittl, & T. Ebner. (2015). "Sichere Vernetzung von Geräten in Smart Factories mit MQTT [Secure connection of devices in smart factories using MQTT]," in Mensch und Computer 2015, Stuttgart, 2015, in German.

M. Maritsch, C. Lesjak & A. Aldrian, (2016, July). Enabling smart maintenance services: Broker-based equipment status data acquisition and backend workflows. In 2016 IEEE 14th International Conference on Industrial Informatics (INDIN) (pp. 699-705). IEEE.

K. North, S. Durst, A. Carvalho, J. Carvalho & S. Thalmann. (2019). Information and knowledge risks in supply chain interactions of SMEs. Hg. v. In Proceedings of the 10th Conference Professional Knowledge Management. Potsdam, Germany.

F. Pauker, J. Mangler, S. Rinderle-Ma, & C. Pollak, Pauker, F., Mangler, J., Rinderle-Ma, S., & Pollak, C. (2018). centurio.work-Modular Secure Manufacturing Orchestration. presented at the 16th International Conference on Business Process Management 2018, Sydney, Australia, 2018, pp. 164–171.

P. Priller, A. Aldrian & T. Ebner. (2014, September). Case study: From legacy to connectivity migrating industrial devices into the world of smart services. In Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA) (pp. 1-8). IEEE.

J. Stjepandić, H. Liese, & AJC Trappey. (2015). Intellectual property protection. In Concurrent Engineering in the 21st Century (pp. 521-551). Springer, Cham..

S. Thalmann & I. Ilvonen (2018). (2018). Balancing Knowledge Protection and Sharing to Create Digital Innovations. In Knowledge Management in Digital Change (pp. 171-188). Springer, Cham.

K-D. Thoben, S. Wiesner, and T. Wuest. (2017). "Industrie 4.0" and smart manufacturing-a review of research issues and application examples. International Journal of Automation Technology, 11(1), 4-16.

R. Clarke. (2017). Content Analysis in Support of Critical Theory Research: How to Deliver an Unwelcome Message Without Being Shot. In Bled eConference (p. 43).

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. MIS Quarterly, 28(1), 75-105. doi:10.2307/25148625

K. Peffers, T. Tuunanen, M. A. Rothenberger, & S. Chatterjee. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77.