Charlie and the CryptoFactory: Towards Secure and Trusted Manufacturing Environments

Michalas, A. and Kiss, T.

Charlie and the CryptoFactory: Towards Secure and Trusted Manufacturing Environments

Antonis Michalas
Network and Information Security Group,
Department of Computing Sciences
Tampere University,
Tampere, Finland
antonios.michalas@tuni.fi

Tamas Kiss
Research Centre for Parallel Computing,
School of Computer Science and Engineering,
University of Westminster,
London, U.K.
T.Kiss@westminster.ac.uk

***Abstract*—The modernisation that stems from Industry 4.0 started populating the manufacturing sector with networked devices, complex sensors, and a significant proportion of physical actuation components. However, new capabilities in networked cyber-physical systems demand more complex infrastructure and algorithms and often lead to new security flaws and operational risks that increase the attack surface area exponentially. The interconnected nature of Industry 4.0-driven operations and the pace of digital transformation mean that cyber-attacks can have far more extensive effects than ever before. Based on that, the core ideas of this paper are driven by the observation that cyber security is one of the key enablers of Industry 4.0. Having this in mind, we propose CryptoFactory – a forward looking design of a layered-based architecture that can be used as a starting point for building secure and privacy-preserving smart factories. CryptoFactory aims to change the security outlook in smart manufacturing by discussing a set of fundamental requirements and functionality that modern factories should support in order to be resistant to both internal and external attacks. To this end, CryptoFactory first focuses on how to build trust relationships between the hardware devices in the factory. Then, we look on how to use several cryptographic approaches to allow IoT devices to securely collect, store and share their data while we also touch upon the emerging topic of secure and privacy-preserving communication and collaboration between manufacturing environments and value chains. Finally, we look into the problem of how to perform privacy-preserving analytics by leveraging Trusted Execution Environments and the promising concept of Functional Encryption.**

***Index Terms*—Security, Privacy, Industry 4.0, Smart Factories**

I. Introduction

Industry is the backbone of the European Union's economy. It accounts for 80% of Europe's exports and private innovations and provides high-skilled jobs for citizens. Furthermore, about 17% of total value added in the EU comes from manufacturing. One job in manufacturing creates up to two and a half other jobs across the value-chain.

Even though the manufacturing sector traditionally used automated machines to increase productivity, adoption of other cutting-edge technologies was rather limited. However, the sector has undergone a tumultuous decade that radically changed the way it operates. Nowadays, the manufacturing industry aims to improve competitiveness and productivity, as well as to support collaboration between stakeholders by adopting a collection of cutting-edge technologies such as cloud computing, the Internet of Things and Machine Learning. Adoption of ICT technologies and their convergence with the existing manufacturing technologies enables effective and accurate engineering decision-making in real-time.

Advances in both manufacturing, computing and network communication paved the way for the adoption of Cyber Physical Systems (CPS), where data is closely monitored and synchronized between the physical factory floor and the cyber computational space. Moreover, by utilizing advanced information analytics, networked machines are able to operate in a more efficient, collaborative and resilient way. There is no doubt that the use of such technologies is transforming the manufacturing industry to the next generation. However, besides bringing more opportunities this transformation introduces several challenges. Hence, there is an urgent need to create mechanisms ensuring that the adoption of these new technologies will be done in a reliable, secure and efficient way.

The modernization that stems from Industry 4.0 started populating the manufacturing sector with several networked devices, complex sensors, and a significant proportion of physical actuation components. Until now, the main focus of this transformation was on integrating networked and smart devices into existing manufacturing environments to improve productivity, efficiency and reduce direct human effort and resources. However, new capabilities in networked cyber-physical systems demand more complex infrastructure and algorithms and often lead to new security flaws and operational risks that increase the attack surface area exponentially. The interconnected nature of Industry 4.0–driven operations and the pace of digital transformation create preconditions for cyber-attacks that are more extensive, destructive and costly than ever before. Without focused, decisive and energetic actions to improve security, manufacturers and their supply networks remain unprepared in the face of the risks. As a result, Cybersecurity is one of the key enablers of Industry 4.0.

According to EEF's[1] 2018 Cybersecurity for Manufacturing report [1], 48% of manufacturers have suffered cyber-attacks, with half of those victims sustaining financial or other business losses. NTTSecurity's 2018 Global Threat Intelligence Center report [2] identified manufacturing as the fourth-most targeted industry, behind only finance, technology, and business and professional services. Along with the transformation of the manufacturing sector the cybersecurity landscape is also under-

[1]EEF was formed in 1896 as the Engineering Employers' Federation and merged in 1918 with the National Employers' Federation.

going a metamorphosis of unprecedented scale. As a result, to adequately address cybersecurity risks in the age of Industry 4.0, cybersecurity strategies should be secure, vigilant, and resilient. They must be fully integrated into organizational and information technology strategies from the beginning of the strategic process. Cybersecurity must become an integral part of the strategy, design, and operations, considered from the beginning of any new connected, Industry 4.0-driven initiative.

Technologies for Industry 4.0 will further intensify the need to upgrade measures for internal security. The challenges to security are becoming bigger than ever, with both attackers and cybersecurity professionals vying to remain ahead. In today's hyper connected world, cyber-attacks are no longer a matter of "if", but rather "when". Industry 4.0 is becoming a reality – with all its promises and vulnerabilities. However, protecting such complicated environments is not a straightforward approach and requires designing out-of-the-box security mechanisms that will in many cases deviate from the classic security approaches.

A. Our Contribution

The contribution of this paper is twofold. First, we present a list of core security requirements that must be considered when building smart factories. These security requirements were derived based on our experience from conducting applied research in the fields of cloud security, IoT security, privacy and cryptography – areas that will form the foundations of future factories. Second, we present a forward looking design of a layered-based architecture that can be used as a starting point for building smart factories that will be resistant to a wide range of cyber attacks. Furthermore, the presented architecture is a modular one – meaning that extra components and services can be easily added. Hence, allowing several organizations to adopt a similar approach without having to sacrifice their basic functionality. Finally, we hope that this work will help protocol designers to build novel security protocols that can squarely fit the specific needs of Industry 4.0 while at the same time pave the way for secure and privacy-preserving smart factories.

B. Organization

The rest of the paper is organized as follows: Section II presents a high level overview of the basic technologies that will constitute the core of CryptoFactory architecture. Section III presents the proposed modular architecture as well as with the main functionality of the underlying components.

II. Current Technologies and Research Challenges

The complexity of technology underlying cloud computing and the Internet of Things introduces novel security risks and challenges [3]. While threats and mitigation techniques for the two fields have been under intensive scrutiny in recent years, there is only a little work that has been done in the direction of modern infrastructures protecting facilities that are based on the use of both paradigms. In this section, we present the basic concepts of the main technologies that will be used in our architecture.

A. Trustworthy Execution and Software Defined Networks for Manufacturing Environments

Creating trustworthy and verifiable infrastructures and services is of paramount importance. To do so, the most common way is to use special secure hardware that allows authorized users to verify the integrity of an entity (e.g. cloud host, IoT device, etc.). This verification process is a cryptographic protocol known as attestation and exposes an aggregated pool of isolated execution capabilities, based on hardware security features (both bare-metal and virtualized), available on commodity cloud platforms. Such hardware security features include: Trusted Platform Modules (TPMs), isolated execution enclaves based on Intel Software Guard Extensions (SGX) [4], or memory and execution isolated based on AMD Secure Memory Encryption, AMD Secure Encrypted Virtualisation (SEV) [5], or ARM TrustZone [6]. The availability of the features depends on the platform vendor (Intel and AMD are the most common vendors of cloud server platforms) or on the platform hardware configuration (especially relevant for TPMs, but also applicable for SGX and SEV features). An attestation protocol involves a target, an attester, an appraiser, and possibly other principals serving as trust proxies. The purpose of an attestation protocol is to supply evidence that will be considered authoritative by the appraiser, while respecting the privacy goals of the target (or its owner). Digitalization has a profound impact on the proliferation of computing devices in the manufacturing context. Along with improvements to manufacturing efficiency, this change also brings a set of security challenges, as more and more devices used in the manufacturing context are connected to local or public networks, are used outside of the manufacturing facilities, or are exposed as a service to users.

Apart from using secure hardware to verify the integrity and therefore the trusted state of an entity, this hardware can be also used to create an isolated execution environment (also known as a TEE). This is a technique that can significantly increase the overall security of a service since certain, usually sensitive, parts of the service will be running in a secure and isolated space where no interaction with external sources will be available. Hence, even if parts of the host or the service itself have been compromised, functions that deal with sensitive information and running in a TEE will not be affected. An isolated execution environment can be created in several ways. One approach to construct an isolated execution environment is by validating the platform's trusted computing base (TCB) using secure boot, as the TCB is by definition isolated from the rest of the system. However, this approach is progressively less suitable beyond a very compact TCB, such as a hypervisor that can be formally verified. A different approach is required when confidential information – such as cryptographic keys – is persistently maintained on the platform. To address this, some platform manufacturers have introduced support for firmware-supported Trusted Execution Environments. TEEs often include storage for a (statistically) unique device key and an execution environment in which small pieces of code can be executed in isolation from the rest of the system. Combined with the secure boot or trusted boot procedures, TEEs can become a minimal TCB for platform software. The TCB can in turn be leveraged by the booted operating system (OS), as well as

by software installed on the device or by external appraisers that aim to assess the platform's trustworthiness. A TEE is a secure, integrity-protected processing environment, with processing, memory and storage capabilities, isolated from an untrusted, Rich Execution Environment that comprises the OS and installed applications.

While the problem of integrity verification for machines occupied with specific secure hardware is a well-studied problem [7], [8], getting certain guarantees about the trusted state of a constrained device (i.e. a device that is not occupied with secure hardware) is still considered as an open and difficult to solve problem. However, due to the complex networked computing systems that electronically control modern factories (a combination of powerful machines with edge, constrained, devices) building a software-based protocol is considered as a necessary step to build trusted smart factories. By doing this, authorized stakeholders will be able to verify the integrity of devices without the need to install any special hardware.

B. Secure Cloud Storage and Operations on Encrypted Data

Cloud storage has rapidly become a cornerstone of many businesses and has moved from an early adopters stage to an early majority, where we typically see explosive deployments. Cloud technologies and in particular cloud storage plays a crucial role in the development of Industry 4.0 services. However, while joining the cloud revolution it has become necessary, the field of manufacturing is still slow in adopting such technologies due to several security issues that a remote storage implies. However, lately, we have seen some great developments in the field of cryptography that squarely fit the cloud paradigm and can give smart factories the necessary guarantees about the security of their data. For many emerging applications such as "cloud" services, where third parties can have access to your data, the traditional notion of encryption is insufficient. For example, there is often a need to specify a decryption policy in the ciphertext and only individuals who satisfy the policy can decrypt [9], or it is important to store data in an encrypted form and being able to search directly over the encrypted data or even being able to execute certain computations/functions on ciphertexts. During the last years we have seen some really interesting developments in the field of applied cryptography. Developments that move away from the traditional notion of cryptography and have the potential to change the way we use and trust cloud-based services. All of the above mentioned examples can be solved with techniques like Attribute-Based Encryption (ABE) [10], Symmetric Searchable Encryption (SSE) [11], [12] and Functional Encryption (FE) [9], [13].

ABE was first introduced by Sahai and Waters [14] to solve the problem of encrypted access control. In ABE, every secret key is generated along with a policy P while ciphertexts are generated with a set of attributes U. Decryption is possible if the list of attributes satisfies the underlying policy (i.e. $P(U) = True$).

SSE allows users to outsource encrypted data to a possibly untrusted remote location while simultaneously being able to perform keyword search directly through the stored ciphertexts. An ideal SSE scheme should reveal no information about the content of the encrypted information nor about the searched keywords and their mapping to the stored files. In [15] the authors presented a forward-looking design of a cryptographic cloud storage built on an untrusted IaaS infrastructure. The approach aims to provide confidentiality and integrity, while retaining the benefits of cloud storage – availability, reliability, efficient retrieval and data sharing – and ensuring security through cryptographic guarantees rather than administrative controls. The solution requires four client-side components: *data processor, data verifier, credential generator, token generator*.

FE is another promising technique that is a perfect candidate for solving the the problem of privacy-preserving collection of data for analytics.

FE is a cryptographic primitive that allows a user with a secret key to learn a function evaluated on some encrypted data. A trusted authority holding a master secret key can generate special functional secret keys, where each functional key is associated with a function f (or program) on plaintext data. When the functional key is used to decrypt a ciphertext, which is the encryption of some message m, the result is the quantity $f(m)$ – nothing else about m is revealed. Thus, FE is a powerful cryptographic tool that allows users to do certain computations on encrypted data without revealing anything about the actual content of the data. Hence, users' privacy can be protected from both internal and external attacks.

For many emerging applications such as "cloud" services the traditional notion of public-key encryption is

III. CryptoFactory: A Forward Looking Design for Secure and Trusted Smart Factories

Securing communication between the manufacturing stakeholders (e.g. between IoT devices and the CSP) is undoubtedly an important first step towards building a secure modern factory. However, this can be only seen as the basic step that a modern factory should follow on its way to secure its underlying important assets. Having this in mind, modern factories must further extend the security related functionality by offering several additional core features that are currently missing in existing frameworks. To this end, every smart factory will have to address the problem of hardware trustworthiness for *both* the cloud platform and the IoT devices with main aim to ensure, prior to use, that all the underlying devices, systems and services run in a trusted state. Moreover, another important CryptoFactory focus area is performing privacy-preserving analytics over factory data, since this will allow factories to determine performance improvements and support more accurate decision-making processes. Apart from that, project CryptoFactory will work on implementing another layer of protection through the use of machine learning algorithms. A concrete set of anomaly and threat detection algorithms will be implemented, capable to analyse data in real-time as well as offline and detect possible threats/malicious behaviours. Finally, CryptoFactory will promote the collaboration between multiple manufacturing environments and value chains. Attribute-Based Encryption security protocols will be designed to securely share encrypted data among manufacturing stakeholders and along their value chains.

In this section we will describe a forward looking design of an open, modular and extensible architecture, based on

individual, autonomous, reusable and self-contained building blocks. The CryptoFactory architecture consists of six discrete layers, illustrated in Figure 1: The Edge Multicloud layer, the Secure Execution layer, the Crypto Layer, the Anomaly Detection layer and the Data Analytics layer.

A. Edge Multicloud layer

The base of CryptoFactory architecture will utilize cloud resources and also incorporate a wide range of IoT edge devices with main aim to collect and process data. This, will form CryptoFactory's Edge Multicloud Platform (CEMP). CEMP should be built on existing mature components in order to speed up the design and development process. However, extension and further development of these components will still be required to achieve the desired level of integration and to support the largely distributed environment. CEMP should incorporate various cloud resources for the central processing of data in scenarios where significant computational power is required (e.g. computation intensive data analytics applications). These cloud resources can represent both public and private clouds. To achieve seamless migration and execution of applications on this heterogeneous cloud testbed, a multicloud platform should be considered. Apart from the central cloud resources, CEMP should incorporate various IoT edge devices typical in manufacturing environments. To execute applications in this heterogeneous edge multicloud environment, appropriate mechanisms for the distribution of tasks and data between the edge devices and the central cloud resources should be carefully developed. Such distribution and orchestration mechanisms will target problems such as which computation to execute locally on the edge device, when to transfer data and computation to the cloud, and how to distribute workload among edge devices.

B. Secure Execution layer

The aim of this layer will be to support the implementation of pluggable applications to enhance the security functionality of the CryptoFactory architecture. In CryptoFactory, the IaaS (Infrastructure-as-a-Service) compute hosts offered by the Edge Multicloud Layer will be equipped with trusted computing hardware and firmware security features that support the creation of trusted and isolated execution environments. Some of the trusted computing devices (such as TPM v1.2, see Section 1.4.4) have been available even prior to the emergence of cloud computing. However, they are ill-adapted to the cloud computing context and were not widely used. A new generation of hardware and firmware security features (TPM 2.0, Intel SGX, Arm TrustZone) recently became available on cloud server platforms. Unfortunately, cloud service providers provide at best only very limited access to such security enablers in their commercial offerings.

This layer should apply the advances in trusted computing to enable cloud users to assess *platform* and *software* trustworthiness, as well as to deploy software in isolated execution environments. This, will ensures the confidentiality and integrity of the loaded code and data. To do so, hardware and firmware security features will be leveraged to develop applications for isolated execution environments supporting core functionality of a factory. In particular, such secure isolated execution environments will host support functions for attesting the integrity of edge devices as well as of the launched VMs in the underlying cloud environment. An overview of the integrity verification mechanisms of this layer is illustrated in Figure 1. Furthermore, CryptoFactory will leverage isolated execution environments to host components executing privacy-preserving analytics on encrypted data (see Subsection III-E).

C. Crypto Layer

The crypto layer will be implemented as a collection of cryptographic algorithms and will be one of the key components for both the security and the main functionality of CryptoFactory. This layer will provide a complete cryptography toolkit used to protect stored data and secure the communication between connected components and entities in the system. Furthermore, it will support the secure execution layer to assess the trustworthiness of the underlying cloud platform and of the edge devices collecting and transmitting factory data. The Crypto Layer will be fully integrated with the CEMP and will secure communication on top of that platform.

Due to the special nature of smart factories (complex networking ecosystem), this layer should not rely only on the implementation of traditional cryptographic algorithms. More precisely, the novelty of this layer will be the implementation of modern encryption techniques that will allow factories not only to secure data in rest and on transit but also to perform operations on encrypted data. To this end, in the core of the Crypto Layer an implementation of an Attribute-Based Encryption (ABE) scheme and a Functional Encryption (FE) scheme should be considered. ABE will be used to allow data exchange and collaboration between the manufacturing facilities and the value chains while offering an efficient revocation mechanism[2]. By utilizing ABE, factories will be able to encrypt data by using a public ABE key and a policy that will define who is able to access and decrypt data. Therefore, the same ciphertext can be shared with multiple manufacturing stakeholders but only the ones that have been defined in the policy will be able to recover the plaintext. This functionality has a great potential since one single ciphertext will be possibly decrypted by more than one different keys. Furthermore, the access revocation of a manufacturing stakeholder will be a simplified since the owner of the underlying data will be able to revoke only the unique key of the underlying stakeholder and therefore avoiding complex revocation methods that would require the decryption and re-encryption of data with a fresh key.

Furthermore, the FE scheme will be partially operating in an isolated environment supported by the secure execution layer and will be used only by authorized stakeholders. The functionality offered by the supported Functional Encryption will allow authorized stakeholders to perform statistical operations based on encrypted data without decrypting them – hence, learning nothing about the actual content of the data. Thus, FE will pve the way for the design and implementation of privacy-preserving analytics protocols.

[2]Currently, revocation in ABE is a complex problem that has significant effect to the overall efficiency of the scheme. However, there are other promising revocation mechanisms, such as [16], that leverage the power of TEEs and offer a revocation mechanism that is separated from the actual ABE scheme.

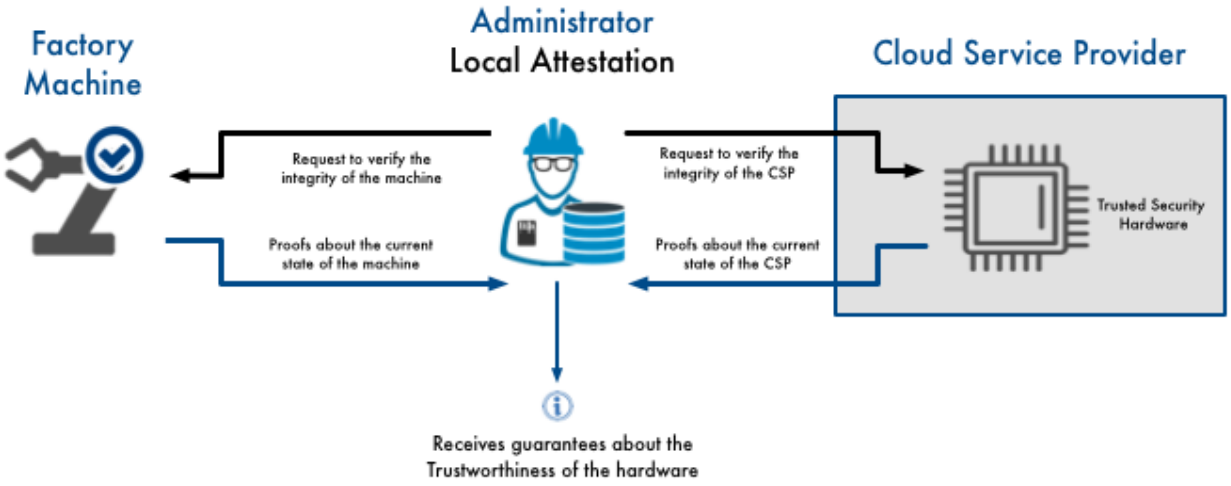

Fig. 1. Secure Execution Layer

D. Anomaly Detection layer

Anomaly detection is an important aspect of smart manufacturing. If the operation of a machine or an asset deviates from the set standards, it may affect the overall operations. To this end, mechanisms that will be dedicated to detect outliers, faults or anomalies before these actually occur should be in place in every modern factory. Such mechanisms need to deliver real-time anomaly detection paired with a deep analysis framework over streamed data. This will be used to perform machine and deep learning analysis tasks, at scale, in order to extract complex behavioural patterns and insights to timely identify evolving threats. Furthermore, additional analytic techniques and mechanisms should be implemented and customized to allow the extraction of threat indicators, including anomaly detection, robust self-learning models for advanced security in support of early warning intelligence, sophisticated reporting and cascading effects calculation, etc. Moreover, alerts for early anomaly detection, indications and recommendations will should be coupled with a rule-based machine learning approach to enact targeted mitigation measures by utilising the set of relational rules that collectively represent the knowledge captured by the traffic flows. The development and integration of such a framework in a modern factory will eventually allow to protect all phases of the manufacturing process.

E. Data Analytics layer

One of the core functionalities of CryptoFactory will be to allow authorized manufacturing stakeholders to perform analytics based on factory data. This will be done through a series of statistical functions provided by the Data Analytics Layer. The use of this layer will be to correlate and analyse data made available by the CryptoFactory platform to generate new insights and knowledge. This layer will offer a wide range of typical statistical operations needed for manufacturing data analytics. Apart from typical statistical functions and simple visualisation, this layer will be capable of performing privacy-preserving analytics. More precisely, the main novelty of this layer reflects the use of Functional Encryption in an isolated environment. CryptoFactory will be using this promising encryption technique to run statistical computation directly on encrypted data. Hence, private information contained in the individual data will be fully protected. Furthermore, this will also play a crucial role in cross-border collaboration where statistical data will be shared among multiple partners. Finally, as part of the Data Analytics Layer, CyrptoFactory will also support a mechanism to enable collecting and sharing statistical measurements about the performance of different IoT devices used in the manufacturing context. This information will be later shared in a privacy-preserving way with other manufacturing actors through a central service responsible for collecting and classifying statistical measurements from multiple manufacturing data sources. This privacy-preserving reputation system will allow other manufacturing actors to make more accurate decisions regarding the equipment they need to efficiently complete a task – hence increasing productivity. We believe that this privacy-preserving reputation system has the potential to enable a self-comparison ability, where the performance of a single machine can be compared with and rated among the fleet and, on the other hand, similarities between machine performance and previous assets (historical information) can be measured to predict the future behaviour of the machinery. An overview of the Data analytics and Threat Detection Layers is illustrated in Figure 2.

IV. Conclusion

In this paper we presented a forward looking design of a modular architecture that can fit the emerging field of smart factories. To this end, we studied several novel and promising technologies such as trusted/secure hardware, attribute-based encryption, symmetric searchable encryption, functional encryption and the application of machine learning for anomaly detection and showed how they can be proved important during the capitalization of Industry 4.0. Finally, we hope that this work will be an important reference point for protecting smart factories and other similarly complicated environments.

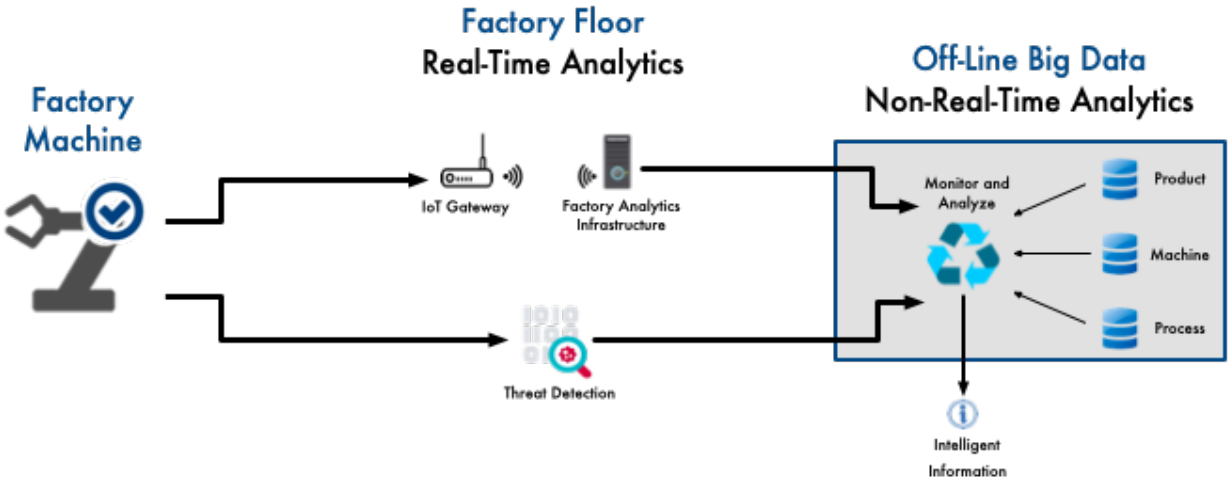

Fig. 2. Data Analytics and Threat Detection Layers

REFERENCES

[1] "Cyber security for manufacturers." https://www.eef.org.uk/resources-and-knowledge/research-and-intelligence/industry-reports/cyber-security-for-manufacturers. Accessed: 2019-03-14.

[2] "Global threat intelligence report." https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl-ntt-security-2018-global-threat-intelligence-report-v2-uea.pdf?sfvrsn=c761dd4d_10. Accessed: 2019-12-21.

[3] A. Michalas and R. Murray, "Keep pies away from kids: A raspberry pi attacking tool," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, IoTS&P '17, (New York, NY, USA), pp. 61–62, ACM, 2017.

[4] V. Costan and S. Devadas, "Intel sgx explained." Cryptology ePrint Archive, Report 2016/086, 2016.

[5] F. Hetzelt and R. Buhren, "Security analysis of encrypted virtual machines," *CoRR*, vol. abs/1612.01119, 2016.

[6] S. Pinto and N. Santos, "Demystifying arm trustzone: A comprehensive survey," *ACM Comput. Surv.*, vol. 51, Jan. 2019.

[7] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in *Proceedings of the 2009 Conference on Hot Topics in Cloud Computing*, HotCloud'09, (Berkeley, CA, USA), USENIX Association, 2009.

[8] N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," *IEEE Transactions on Cloud Computing*, vol. PP, no. 99, pp. 1–1, 2016.

[9] D. Boneh, A. Sahai, and B. Waters, "Functional encryption: Definitions and challenges," in *Theory of Cryptography* (Y. Ishai, ed.), (Berlin, Heidelberg), pp. 253–273, Springer Berlin Heidelberg, 2011.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, (New York, NY, USA), pp. 89–98, ACM, 2006.

[11] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 965–976, ACM, 2012.

[12] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," in *Financial Cryptography and Data Security*, pp. 258–274, Springer, 2013.

[13] S. Garg, C. Gentry, S. Halevi, and M. Zhandry, "Functional encryption without obfuscation," in *Theory of Cryptography - 3th International Conference, TCC 2016-A, Proceedings* (T. Malkin and E. Kushilevitz, eds.), Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), (Germany), pp. 480–511, Springer Verlag, 1 2016.

[14] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques*, EUROCRYPT'05, (Berlin, Heidelberg), pp. 457–473, Springer-Verlag, 2005.

[15] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography and Data Security*, vol. 6054 of *Lecture Notes in Computer Science*, pp. 136–149, Springer Berlin Heidelberg, 2010.

[16] A. Michalas, "The lord of the shares: Combining attribute-based encryption and searchable encryption for flexible data sharing," in *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, SAC '19, (New York, NY, USA), pp. 146–155, ACM, 2019.