Towards secure convergence of Cloud and IoT

1 Cloud computing and the IoT ecosystem

During the last few years we have witnessed the burst of Internet of Things (IoT) products. As the IoT market grows bigger year by year billions of new devices are deployed online. Gartner forecasts that connected *things* will reach up to 20.4 billion by 2020.[1] These things (or devices), connect to the network to provide information they gather from the environment through sensors, or to allow other systems to reach out and act on the world through actuators.[2] ENISA defines IoT as **"a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making"**.[2] Information lies at the heart of IoT, feeding into a continuous cycle of sensing, decision making, and actions.

IoT devices generate vast amount of data. The Cloud, as part of the IoT ecosystem[2], manages the flow, the process, the analysis and the storage of these data. Especially in enterprise environments, IoT can be most rapidly and cost-effectively deployed when integrated with Cloud-based services.

With the prevalence of IoT, Cloud Computing evolved in such a way to accommodate the needs of the IoT ecosystem and provided many **new features specific to aggregating, storing and processing data generated by IoT**. Among these features are device virtualisation, business intelligence tools, machine learning, command and control (C&C), processing to perform complex analytics, and Application Programming Interfaces (APIs).[3]

While this convergence of Cloud Computing and IoT brings opportunities, it also raises new risks and challenges. In short, this paper attempts to:

- identify and discuss security challenges coming from the convergence of IoT and Cloud;
- highlight the security issues through four representative attack scenarios;
- map the identified challenges to security takeaways.

The aim of this work is to provide a high-level overview on the security issues to the audience below:

- **IoT developers and IoT integrators** that make use of IoT Cloud Computing;
- **Cloud service Providers (CSPs)** of IoT Cloud offerings.

According to the ENISA Baseline security recommendations for IoT[2], the IoT ecosystem is comprised of three basic components, **devices (or things)**, **communications**, and **Cloud platform, backend and services**. These components and their interactions are depicted in Figure 1 below.

[1] See https://www.gartner.com/newsroom/id/3598917
[2] See https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
[3] See https://www.postscapes.com/internet-of-things-platforms/

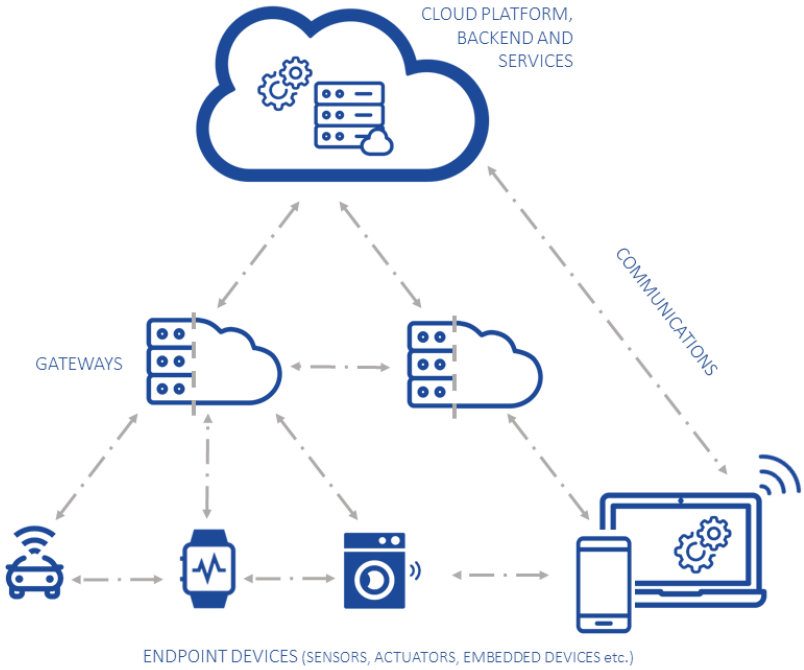

Figure 1. Architecture for IoT ecosystem with IoT Cloud

Prior to the IoT boom, Cloud Computing would traditionally host persistent work, which demands attributes such as elasticity, multitenancy, scalability or adaptability. With the advent of IoT, Cloud enhanced further its characteristics to manage and respond to events anywhere and at any time[4] creating a new model called "IoT Cloud". New features such as response agility, ubiquity and flexibility are now sought, and IoT Cloud has the potential to deliver them. Cloud providers now support functional programming in the form of micro-services, which respond to the characteristics of the demanded service[5] allowing event-driven applications rise in the Cloud.

In short, this new model enables IoT developers to perform remotely tasks on IoT devices, such as to assess the status of their assets, review their specifications, configure or re-configure them, command or update them and extract any kind of statistics, values, and settings. This introduces new risks on the IoT devices managed from an IoT Cloud should the latter be compromised. Security configurations in Cloud become even more critical in the case of IoT Cloud where such numerous and diverse devices are being monitored and managed.

[4] See https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/making-sense-of-internet-of-things-platforms
[5] See http://searchcloudcomputing.techtarget.com/opinion/Event-driven-applications-drive-next-wave-of-IaaS-evolution

Cloud security is still an issue as ENISA has depicted and analysed in various past publications[6] [7] [8]. It faces multidimensional challenges that have not been addressed totally yet. In this short paper, we focus on the specific security challenges emerging from this new model of IoT Cloud and its convergence with the IoT ecosystem and their bidirectional interaction. According to OWASP, both aspects of security in this convergence are facing challenges from each other. Cloud Web Interface is listed as one of the attack surfaces of IoT[9], while Cloud Top 10 Security Risks[10] include Service and Data Integration, which is bounded to the security of IoT devices.

Based on the ENISA IoT high-level reference model and the interactions of its elements (see Figure 1), we classify the security aspects of the IoT and Cloud convergence in the following three main categories:

- **Connectivity:** interactions and communications among endpoints, gateways and Cloud;
- **Analysis:** processing ,filtering and aggregation of the data coming from the IoT devices in different levels of the IoT ecosystem;
- **Integration:** features that enable real-time bidirectional flow of data (eg. Cloud APIs and remote command and control (C&C) of IoT devices through Cloud).

2 Security challenges

Apart from sensors and actuators, IoT often connects legacy and new systems together to enable interoperability. These systems connect through gateways to the Cloud where sensors' data are being processed, in order to make a decision. Occasionally, this interoperability issue applies in environments where critical operations take place, such as Healthcare, Energy, Aviation.

There is a growing concern about security for the IoT ecosystem in its entirety. Attacks to IoT devices can potentially facilitate stepping stone attacks and access to network or Cloud resources and vice versa. Having said that, new attack surfaces for both Cloud and end-devices of the IoT ecosystem are being revealed. Poor security on the level of the IoT devices or the IoT gateways can potentially result in insecure connectivity and data flow towards the Cloud with consequences to the overall security of the ecosystem.

ENISA identified the following security challenges falling under each of the three main categories derived from the ENISA IoT high-level reference model. An analysis of these challenges is presented in this section.

CONNECTIVITY	• Heterogeneous protocols for communication • Insecure data flow from the Edge to the Cloud
ANALYSIS	• Real-time processing at the edge overshadows security • Impact of Cloud decentralisation on security
INTEGRATION	• Security depends on the vertical that Cloud is serving • Security relies much on the implementation from IoT developers • Outdated devices

[6] See https://www.enisa.europa.eu/publications/exploring-cloud-incidents
[7] See https://www.enisa.europa.eu/publications/security-aspects-of-virtualization
[8] See https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
[9] See https://www.owasp.org/index.php/IoT_Attack_Surface_Areas
[10] See https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project

It is worth to note here that, in addition to the analysis of the challenges, ENISA has developed specific attack scenarios utilising input from interviews with experts on the specific topic in order to highlight specific security challenges. These attack scenarios are presented in the Attack scenarios section with the aim to complement and contextualise the security challenges presented in this chapter.

2.1 Connectivity

Heterogeneous protocols for communication [11]

IoT applications range from smart homes to smart industry resulting in diverse scope, hardware, operating systems, protocols and network connectivity methods for IoT. Within these IoT solutions some are legacy systems that rely on proprietary technology, while others adopt more open IoT standards such as MQTT[12] and the IETF protocol stack for (constrained) IoT devices[13]. This diversity often results in vertical silos which hinder development of value-added services using low-resource IoT devices and also differentiates levels of security in each implementation. Having said that, developers looking to add value on top of existing IoT systems are faced with either legacy devices or devices and systems, which implement a wide variety of network connectivity options, protocols and communication methods. Integrating new devices with legacy ones usually brings an uncalculated impact on security. Even within one IoT standard, a device typically has multiple options for communicating with others and again the level of security implemented in each case will probably differentiate.

Insecure data flow from the Edge to the Cloud

Another interesting part of the IoT model is the processing of data. Processing of data can be done either at the edge (aka edge computing[14]) or at the Cloud. Edge computing provides a way to allow applications and services to gather or process data to the local computing devices, away from centralized nodes enabling analytics and knowledge generation to the logical extremes of the network. Although edge computing enhances instantaneous response and subsequent decision making (e.g. use of machine learning to make autonomous decisions), it also results in a distributed, unsafe and uncontrollable disarray of data which can become critical when taking into account the amount and the sensitivity of data that is transmitted. Limited processing and storage capabilities of some endpoints may restrict security features, such as authentication, encryption and integrity protection mechanisms, jeopardizing both access control as well as the confidentiality or integrity of data transmitted to the Cloud[15]. Even when security features are enabled, faulty implementation can have great impact on security of the entire model.

2.2 Analysis

Real-time processing at the edge overshadows security

According to IDC forecast, 43% of IoT computing will occur at the edge by 2021[16]. Especially in the case of IoT, edge computing can provide performance benefits such as real-time computation and a reduction of

[11] http://journals.sagepub.com/doi/full/10.1155/2015/683425
[12] http://mqtt.org/
[13] https://tools.ietf.org/pdf/draft-moore-iot-security-bcp-00.pdf
[14] See https://www.forbes.com/sites/jonmarkman/2018/04/03/this-is-why-you-need-to-learn-about-edge-computing/
[15] See https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php
[16] See http://techblog.comsoc.org/2017/03/04/idc-directions-2017-iot-forecast-related-sessions/

dependence on network connectivity into the Cloud. However, the edge is physically accessible and harder to secure in comparison to the Cloud, so it is more prone to attacks that require attacker's physical presence. Due to the nature of IoT, edge computation can happen on devices, which could be located anywhere, from highly secure to less secure environments; in many cases network isolation cannot be ensured, nor restrained physical access to the actual devices[15]. Compromising security of the edge device and accessing unencrypted data used for the real-time processing on it can break the trusted link between the IoT device and the Cloud and expose information that was supposed to remain encrypted. In addition, regular security tasks performed in the Cloud such as monitoring, which could prevent such attacks against devices, become harder and less manageable[17].

Impact of Cloud decentralisation on security

As mentioned before, not only IoT devices are scattered around, but with edge computing, parts and capabilities of the Cloud are also spread around the environment. Despite having some positive aspects on security (e.g. less things directly interacting with the remote Cloud services implies a reduced Distributed Denial of Service (DDoS) attack surface), this Cloud decentralisation brings some challenges to the table. For example, the limitation in terms of elasticity in comparison to the Cloud makes the edge of IoT more vulnerable to DoS attacks, and the complexity of the coordination of application of security mechanisms (such as software / firmware updates / patches) increases[18].

2.3 Integration

Security depends on the vertical that Cloud is serving

Intended use of the IoT plays an important role. There are still many cases in which the overall security in place can influence the security of the IoT ecosystem – including Cloud. Especially when IoT is applied to Infrastructures where critical operations take place (eg. Smart Hospital), cyber security can be potentially bound to safety. Although IoT security should be robust enough to fit in all environments there are still many issues due to increased complexity of interconnected platforms and their management.

Security relies a lot on the implementation from IoT developers

The security knowledge base of IoT developers regarding the smart things is still low. Fundamental security elements on the smart device side, including secure boot, thing authentication, message encryption and integrity, and a trusted key management and storage scheme, are not always implemented. It is very challenging to define secure software/hardware development lifecycle guidelines for IoT due to the many different hardware, protocols and network connectivity methods used in the IoT development.

Outdated devices

Many devices may never receive a software update, either because the manufacturer may not provide updates or because consumers may not apply the updates that are already available or even worse because the IoT device does not even support a user interface to allow for a manual update of its software.

[17] See https://www.sciencedirect.com/science/article/pii/S0167739X15003015
[18] See https://ieeexplore.ieee.org/document/7165580/

3 Attack scenarios

Extrapolated from the challenges, there are some prominent threats that refer to the combination of Cloud and IoT. Some of these biggest threats are instantiated by attacks such as DDoS, tampered data on the sensors, Structured Query Language (SQL) injection, or compromised Firmware-Over-The-Air (FOTA)[19]. In this section, we present some attack scenarios illustrating these main concerns regarding the combination of Cloud and IoT.

3.1 Hosting the enemy

On a normal basis, Mr. Soulful was very happy with the present her children bought her for Christmas, a brand new system for making her kitchen 'smart'. However, when she saw the incomprehensible notification that popped up in her brand new tablet she started to stress out; her daughter told her loud and clear 'do not install anything you do not understand'. The truth is that she does not want to bother her daughter anymore, so she clicks on 'Postpone update' again, until she can ask someone about it.

Meanwhile, Mrs. Darkhat is now in possession of the last patch that was included in such update, and plans to take advantage of the security hole present now in all outdated devices bearing that software; she will add them to a botnet form of IoT devices.

A few days later, Mr. Soulful becomes very irritated when she experiences some usability issues with the fancy new cooking devices: they respond in a very slow way, and sometimes even do not accomplish the tasks she is commanding from her tablet. Still thinking on how these devices should make her life easier and not harder as they are currently doing, her attention is caught by the news on the television. Apparently, a hospital has fallen into a crisis, because their Cloud services have been disrupted and the data hosted there are now inaccessible, denying the service it normally provides. Not only they cannot access crucial data for their patients, but also the smart medical devices currently in use cannot get updates and consequently do not operate properly. 'Exactly what I was saying, these clever thingies only bring trouble' exclaims Mr. Soulful. What she cannot even imagine is that, ironically, it was regular people just like her hosting the zombies which perpetrated the attack, without them even knowing.

Leaving to the users the option to decide whether an important update should be installed or not has a high risk. In this attack, an attacker intercepts the patch that was distributed to the users so they could update their devices, performs reverse engineering against it, and discovers the vulnerability this patch tried to fix. The attacker creates an exploit fitted-for-purpose to take advantage of such vulnerability and releases it into the wild, so all outdated devices are infected and become part of an IoT botnet. Afterwards, the attacker commands and controls this botnet to launch a DDoS attack against a Critical Infrastructure, causing a disruption of the services and of the data availability and therefore producing a huge impact in the society. This could have been avoided if a system for secure automated software updates was in place.

IMPACT	APPLICATION DOMAIN
High: botnet targets CII, impact on society	Consumer, Smart Homes

[19] See https://tools.ietf.org/pdf/draft-moore-iot-security-bcp-00.pdf

SECURITY THREATS / CHALLENGES	SECURITY TAKEAWAYS
• Outdated IoT devices • Heterogeneous protocols for communication • Insecure data flow from the Edge to the Cloud	• Secure communications, security stream analysis and security of data at rest • Addition of security elements to IoT environment • Automated, secure software updates

3.2 Poisoned routes

John Prompt could not be happier with the new smart ambulances the hospital provided them a few months ago. Among many enhancements, his preferred one is the new route calculator: taking into account real-time traffic information collected directly from sensors spread around the region, the system automatically suggests the optimal route for him to get to the hospital as fast as possible, which can make a difference if the patient is in a serious state of health. These functionalities are enabled and supported by machine learning processes hosted in the hospital Cloud[20]. Information gathered by sensors placed around the city is analysed and processed so they best route can be calculated, learning from their mistakes and refining the process with continuous training.

Nevertheless, it has been a few days now that John is encountering several problems with the new system. Not only he has been stuck in more traffic jams than ever, but the other day a patient passed away in the ambulance while they were trying to figure out why the route calculator made them go through a street without an exit. He suspects that the routing service is not working properly, but when he raises his concerns to the responsible team in the hospital, they do not seem to find any irregularities in the systems, neither the smart devices spread around the region monitoring the traffic, not the processing of the data sent back to the Cloud by these devices.

And indeed, the routing system is not the problem. Some weeks ago, Mr. Sly got physical access to some of the smart devices monitoring the traffic in his area, and stole their credentials or digital certificate. Using them, he could successfully authenticate to the Cloud and gained access to a meaningful number of devices. This way, he was able to modify some of the values of their parameters and thresholds, therefore tampering the data they were sending back to the Cloud. Since a significant number of devices were affected, this produced a big impact on the Cloud's machine learning actions which resulted on biased and faulty routes, having a huge impact as lives are at stake.

Nowadays IoT devices are spread in the wild, without owners having proper control of them. In this scenario, an attacker physically accesses several IoT devices placed along the roads and stole their credentials/digital certificate. Afterwards, the attacker authenticated successfully to the Cloud using them, and got access to a high number of devices. He then commanded such devices to send poisoned data to the Cloud, which affected the machine learning processes, therefore influencing the training of the devices (commonly known as a poison attack). In consequence, the whole process was destabilised, causing erroneous results when calculating the routes. This is extremely sensitive considering that lives

[20] See https://www.infoworld.com/article/3140545/artificial-intelligence/how-to-approach-machine-learning-in-the-cloud.html

depend on the efficiency of these routes. This could have been avoided if the devices had more physical protection, as the certificates would not have been stolen in the first place.

IMPACT	APPLICATION DOMAIN
High: Potential life loses.	Critical Information Infrastructure
SECURITY THREATS / CHALLENGES	**SECURITY TAKEAWAYS**
• Insecure data flow from the Edge to the Cloud • Real-time processing at the edge overshadows security	• Device virtualization to bring homogeneity • Secure communications, security stream analysis and security of data at rest • Physical and cyber security in edge devices

3.3 Reaping the harvest

Greenheart family business has been growing at an amazing pace since they incorporated smart devices to their ranch, becoming the first smart farm of the region[21]. Their self-driving tractors save them a lot of effort and time, as they can control them remotely. Moreover, the soil sensors optimise the harvest, as they regulate the watering accordingly, and alert if irregular conditions are detected.

Greenhearts' success infuriates Brownsoul family members, the owners of the nearby farm who struggle to compete with the modern and innovative solutions the neighbours have. The youngest son, who has studied computer science, decides to take action, and contacts a colleague who has some hacker experience to help him out. Fortunately, for them, the authentication form to get access to the Cloud administrative panel of the Greenhearts' smart farm was not properly secured, and the input was not properly validated. Unfortunately, developers left the login form untested and a blind SQL injection could let them get access to the control Cloud web-application without having valid credentials. They then accessed the dashboard, which centrally administers all the smart devices, and corrupted the parameters that leaded the behaviour of the soil sensors without raising any alarm.

Some weeks later, when the harvesting took place, the Greenhearts could not understand why the whole batch was ruined, and more important, why the smart system did not alert them that something was going wrong. It was almost as annoying as having to hear the Brownsouls lecturing about the traditional ways of harvesting being better at the end.

The Cloud in most cases allows the command and control of the IoT devices for the convenience of the administrators, so it remains a key element to secure. In this scenario, the attacker took advantage of an untested and not sanitised authentication form, and by means of a blind SQL injection, got access the Cloud administrative panel. The result of this is that the attackers got access to command and control features of the IoT devices, corrupted the parameters that leaded the behaviour of the soil sensors without raising any alarm. This could have been avoided if the authentication form had been properly

[21] See https://www.link-labs.com/blog/iot-agriculture

tested and sanitised and if a proper access control schema was in place, with different layers of security and access depending the actions the users want to perform.

IMPACT	APPLICATION DOMAIN
Medium: Considerable financial losses	Small / Medium Enterprise
SECURITY THREATS / CHALLENGES	**SECURITY TAKEAWAYS**
• Security depends on the vertical that Cloud is serving • Security relies much on the implementation from developers	• Adoption of baseline security measures • End-to-end security, through the whole environment

3.4 Open House

It is a busy activity period in SharpLocks Inc., and employees in the premises are working extra hard to keep the business afloat. They used to provide residential smart locks systems and their success led them to expand their target market to also cover corporate environments.

Ms. Gold is going to take advantage of the stir, and pretending she is doing her regular monitoring and adjustment tasks on the smart locks, she is planning to abuse the Firmware Over The Air updating mechanism the brand follows. Her 'sponsors' have provided her with a malicious firmware for the smart locks, which will give their RFID card access rights for any SharpLock smart lock, and making them able to access any premise guarded by them, providing them with a 'master' card. Leveraging from the fact that in two days a new firmware update is programmed to be automatically pushed down to the devices, she intends to make the malicious update immediately effective. The API Gateway, as the face of the Cloud towards the outside applications and devices, presents an abstraction layer with management and security roles like access control, traffic balancing or updates. Ms. Gold takes advantage of this, accesses the administrative console of the API gateway and forces a previous update with the malicious firmware.

During this period, the mysterious sponsors manage to physically access to a law firm they had been targeting for a while, using their temporary master card. Their presence remains unnoticed, given the big size of this specific firm and the huge amount of people working within their premises. They steal a series of highly confidential documents they had been after for a long time, and exit the building without any mishap.

Two days later, the programmed update is pushed, and the devices go back to normal operation. At the same time, Ms. Gold's bank account receives the first payment of some lessons she opportunely started teaching recently.

Insider threats have been identified as one of the most worrisome among CSPs. In this case, an insider attacker access the administrative console of the API gateway to force a malicious update to the IoT devices (smart locks in this case). The API Gateway, as face of the Cloud towards the outside applications and devices, presents an abstraction layer with management and security roles like access control, traffic balancing or updates; having access to it means that she is able to abuse the FOTA mechanism, and leave

all the devices managed by the API Gateway unsecured. Until the programmed updated is pushed, the locks are opened to the attackers to access the facilities guarded by them, causing in this case the theft of highly confidential documents, affecting the firm and its clients. This could have been avoided if an active monitoring system would have alerted about this unplanned update, and if the company followed a canary deployments' policy so not all devices are updated until making sure the update works properly.

IMPACT	APPLICATION DOMAIN
High: Confidentiality breach, client data stolen	Big Enterprise
SECURITY THREATS / CHALLENGES	**SECURITY THREATS / CHALLENGES**
• Security relies much on the implementation from IoT developers • Insider[22]	• Secure communications, security stream analysis and security of data at rest • End-to-end security, through the whole environment

4 Security takeaways

The issues discussed above can seriously compromise the security of the Cloud or IoT ecosystem as a whole. For that reason, several practices, technologies, methods and products can be used and applied. In what follows, we present a list of generic directions that indicate how to achieve secure solutions.

4.1 Connectivity

Device virtualization to bring homogeneity

To begin with, virtualization techniques are, apart from well-known to the Cloud, extremely useful to hide complexity under an adaptation layer. This way, a uniform device abstraction can be achieved in such a heterogeneous environment, in terms of both communication and security[23]. Device virtualization can be applied at several levels within the environment: it goes from containerization[24] within the IoT device OS to isolate and integrate applications, to the instantiation of entire IoT devices in the Cloud to have a virtual equivalent there. These practices allow this desired decoupling of the Cloud and heterogeneous IoT endpoints, providing security in the form of a management layer, which ensures the security of the device seen from Cloud's side.

As stated before, a variety of endpoints communicate using heterogeneous protocols with different levels of security, so the natural way to go to improve things would be to foster homogenization. Heterogeneous

[22] Although not analysed in the security challenges of this paper as a threat specific to the issue of IoT and Cloud convergence, it is a considerable threat which applies in many cases including this one.
[23] See http://journals.sagepub.com/doi/full/10.1155/2015/683425
[24] See https://www.scribd.com/document/360971818/Exploring-Container-Virtualization-in-IoT-Clouds

requirements of the devices such as bandwidth, latency, availability or reachability should be considered in the process.

Secure communications, security stream analysis and security of data at rest

As a very first step to secure the flow between Cloud and Edge, there is a need to understand and classify the data being transmitted (e.g. public or confidential), and ensure confidentiality and integrity. For this, encryption should be utilised both in transit, e.g. by using a Virtual Private Network (VPN) to connect to the Virtual Private Cloud (VPC) and Transport Layer Security (TLS) protocol in communications, and at rest, e.g. by means of tokenization or nonrelational databases with built-in security [25].

Even when properly controlled and managed, the large amount of data generated by numerous endpoints needs to be dealt with in terms of security. The same way filtering and aggregation techniques are applied to manage and trim the data at the edge, they can be leveraged to increase/add security at this level. We can take advantage of this early data processing actions to look for malicious streams, ensure authentication and authorisation of the devices, detect anomalies or identify possible data flooding[26]. This way, the flow directed to the Cloud would be checked and secured in advance.

4.2 Analysis

Physical and cyber security in edge devices

One step further in providing security to the environment would be addressing the physical security of the endpoints directly. As the scattering of edge devices makes easier the physical access to them, security hardened hardware needs to be deployed to counteract this risk[27]. Features such as renewable security, failure reporting to Cloud, or compartmentalization[28] lead to a hardened intelligent edge device, which would prevent an attacker from taking advantage of it even when having physical access.

Moreover, given that edge computing faces challenges when adding security to its processes due to limited capabilities of the edge devices, the intermediate approach of Fog Computing can be taken. As described in the recent publication of NIST [29], Fog Computing can bring Cloud scalable capabilities close to the edge devices with the purpose of enhancing the performance, functionality and security in the edge.

4.3 Integration

Addition of security elements to IoT environment

In order to relieve developers and manufacturers from some of the burden, security can be reinforced by introducing new elements in the environment, which focus exclusively on delivering security. Security appliances, routers and gateways are a way to add security at the edge level, strengthening control over the more problematic domain in terms of heterogeneity and amount of data and devices. As an example, a security gateway placed in a smart home environment would not only control and monitor the devices

[25] See https://www.slideshare.net/AmazonWebServices/deep-dive-aws-security-by-design
[26] See https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-017-0090-3
[27] See https://azure.microsoft.com/en-us/blog/securing-the-intelligent-edge/
[28] See https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf
[29] See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf

behaviour, data and communication activities, but also provide some decoupling of this insecure and vulnerable network area from the rest of the environment[30]; so security within the home network area plus security towards Cloud can be incorporated.

Moving towards the Cloud side, there is one element that, incorporated to the network, adds a control layer and provides this separation between the edge and the backend in terms of security. We are referring to the API gateway, which corresponds to an intermediate element with the potential to perform security processes such as canary testing[31] [32], packet inspection, authentication / authorization and access control[33], or protection against attacks such as DDoS or FOTA processes.

Adoption of baseline security measures

The efforts spent on security vary among organizations, companies, sectors and verticals, depending on their criticality, budget and priorities. As a solution to this problem, having a collection of horizontal baseline security measures for IoT would harmonise and increase the level of security throughout the whole IoT spectrum. Regarding to this matter, ENISA has made an effort towards this direction and has provided guidelines and practical recommendations in the context of Critical Information Infrastructures[34]. This will ensure a baseline security level throughout the environment, regardless of the vertical.

Automated, secure software updates

On the one hand, IoT devices themselves are heterogeneous and on the other hand, Edge computing exacerbates a decentralised model, making it harder to control them. Cloud can help securing the devices adapting its centralised model of security to the IoT environment. This can be done by considering some high-level security measures; secure software updates mechanisms, such as FOTA processes[35], allow the Cloud (given its centralised vision of the whole environment) to distribute security in a rapid and effective manner, preventing this way attacks and minimising disruptions[15].

For example, the recovery of a device after a cyber attack can be achieved more effectively by Over-The-Air recoverability, where security updates are pushed to the device via the internet.

A secure object format in which software updates are encoded, managed and deployed in a potentially automated manner, and through the whole device security stack can reduce effort, time and complexity of security maintenance [35].

End-to-end security, through the whole environment

---

[30] See https://www.rcrwireless.com/20170320/opinion/reality-check-csps-need-to-take-a-leadership-role-in-securing-iot-tag10
[31] See https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-api-gateway-supports-canary-release-deployments/
[32] See https://docs.aws.amazon.com/apigateway/latest/developerguide/canary-release.html
[33] See https://azure.microsoft.com/en-us/blog/securing-the-intelligent-edge/
[34] See https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
[35] See https://ieeexplore.ieee.org/document/8110218/

Holistically securing the IoT environment is a very challenging issue, even more taking into account the need for end-to-end security through the whole value chain to achieve distributed security. Some high-level security takeaways to look upon would correspond, for example, to a complete and efficient access control schema, which shall be applied throughout the whole environment[36], from Cloud to the tiniest sensor. This is achieved by means of a strong identity foundation (defining users, groups, services and roles) to serve as basis for strong authentication prior to any communication among elements, followed by the use of fine grained authorisation (with properly designed roles and policies). In order for this schema to function properly, encryption and key management represent the foundations and need to be implemented. Key management plays a crucial role when it comes to device security as it involves creating, renewing, transferring, and accounting for cryptographic items (i.e., keys and certificates). In that sense, it is imperative for the IoT devices to be able to store private keys on an HSM[37] and support generated keys and certificates to be directly distributed to on-premise IoT devices. Moreover, the existence of general guidelines[38] and considerations for key management can provide IoT developers with guidance for implementation of cryptographic key management within an application in a secure manner.

The next aspect to tackle corresponds to apply security in each and every layer of the environment, which we have mentioned along these security takeaways; from physically securing the devices, through network security actions and mechanisms (Virtual Private Clouds, API gateways…) and system security by means of FOTA, to data protection, by data classification and encryption.

Last aspect to highlight corresponds to the integration of such security into the already deployed networks and systems. For that, first measure would be to introduce secure software development lifecycle as a good practice within the normal activities of the IoT environment; processes such as version control systems or continuous integration and delivery can help and ease the application of security within the whole environment in a seamless way. As an example, canary deployment principles allow to securely deploying new features or code in a small number of systems for a small period to test them in live[39]; it allows the evaluation in the real scenario of the new deployment to identify issues, and makes it much easier to reduce the impact if something goes wrong.

5 Conclusions

In concluding this paper, we presented the security challenges of IoT and Cloud convergence as well as the way towards their potential security solutions.

Taking as basis the ENISA Baseline security recommendations for IoT, and specifically the IoT ecosystem architecture definition and the IoT high-level reference model, we defined the three main categories for the security challenges and security recommendations of this paper. Based on these three categories we classified and mapped a list of security challenges to security takeaways as illustrated below:

CATEGORY	SECURITY CHALLENGES	SECURITY TAKEAWAYS
CONNECTIVITY	• Heterogeneous protocols for communication	• Device virtualization to bring homogeneity

[36] See https:// www.slideshare.net/jsoldat/05-internetofthingsio-tcloudcomputing
[37] See https://safenet.gemalto.com/data-encryption/hardware-security-modules-hsms
[38] See https://www.owasp.org/index.php/Key_Management_Cheat_Sheet
[39] See https://searchaws.techtarget.com/tip/Enable-canary-deployments-with-Lambda-API-Gateway

CATEGORY	SECURITY CHALLENGES	SECURITY TAKEAWAYS
	• Insecure data flow from the Edge to the Cloud	• Secure communications, security stream analysis and security of data at rest
ANALYSIS	• Real-time processing at the edge overshadows security • Impact of Cloud decentralisation on security	• Physical and cyber security in edge devices
INTEGRATION	• Security depends on the vertical that Cloud is serving • Security relies much on the implementation from IoT developers • Outdated devices	• Addition of security elements to IoT environment • Adoption of baseline security measures • Automated, secure software updates • End-to-end security, through the whole environment

Acknowledgements

Over the course of this study, we have received valuable input and feedback from subject matter experts. We would like to thank the experts who participated in interviews and provided their expertise and useful comments on earlier drafts of this document: Jesus Luna Garcia (Bosch), Caroline Greer and Dani Grant (Cloudflare), Luciano Santos and John Yeoh (CSA), Benedikt Abendroth and Mark Smitham (Microsoft) and Jay Thoden van Velzen (SAP).

Special thanks for the contribution to Apostolos Malatras (ENISA) and Dimitra Liveri (ENISA).

Authors

Christina Skouloudi, Gema Fernández

Contact

For contacting the authors please email to resilience@enisa.europa.eu

For media enquires about this paper, please email to press@enisa.europa.eu