SIKUR Connect

WHITE PAPER

Version: February 2020

find out more at **sikur.com**

1 - About Sikur

The Company

Sikur is defining the future of secure communication, operating globally, through its offices and Distributors in Brazil, the United States, Europe, the Middle East, and Japan. Sikur works alongside governments and corporations that believe security is fundamental to the integrity of their work. We believe that security is not only about platforms and digital systems but is a mindset that surrounds every aspect of a business.

According to Gartner (Market Guide for Secure Instant Communications Report), Sikur is a vendor that has relevant solutions to this technological space.

The Products

Sikur is the result of a fusion between the most advanced types of technology currently available on the information security market. We are bringing the most innovative form of online technology and privacy while ensuring the messages, calls, chats, and documents exchange in an extremely secure way.

Not just with an encrypted military-grade App, but going one step further, integrating the concept of private cloud and security down to the endpoint. This model is guaranteed by the exclusive model for App authentication, its operating system, and software suite with specific guidelines to provide security and privacy at the App and hardware level.

As mobility grows and Digital Transformation takes place, a set of new technologies also appears, and one of them is the IoT (Internet of Things). Sikur has a deep experience in cybersecurity, where IoT is currently struggling to take off once and for all. These same problems that Sikur is solving for companies and governments, through Sikur Messenger, will now be addressed by our new research and development cell in Sophia Antipolis, France, with a focus on IoT.

Sikur Lab (https://sikur.com/labs/)

To keep our most significant asset (the technology), Sikur has established a new R&D center at Sophia Antipolis´s Science Park, a notable and global technology and innovation center near Nice, France. In this same region, Sikur has become member of the SCS Cluster, which is one of the most prestigious cybersecurity centers in Europe, with a focus on secure communication, where we are working inside an environment full of specialized and global companies, accessing high-quality human resources, participating in strategic projects and leveraging our products and technology to a higher level.

Innovation and Future

Our thoughts are not only on Secure Communication solutions but also in a foundation that makes possible shielding communication in different situations. We did invest a lot of time developing a scalable technology, able to solve other problems that could not even be imagined, but which we know that time would bring them to us, like the IoT market and its branches in smart meters, autonomous cars, healthcare, smart cities, and many other industries. The features are applicable and still under discussion in the IoT industry. By our innovative methodology, we found that there is no challenge to port these technologies to this new market, just some customizations, based on our strong foundation.

We are the foundation. We are the New Secure Communication Mindset.

2 - Abstract

IoT devices have specific characteristics and features, which present several security vulnerabilities. This paper, based in our preprint “A method for securely connecting and managing IoT devices and networks (2020)“, discusses these features, how to deal with them in terms of cybersecurity, and general solutions. A practical method to guarantee the identity and secure connection and management of IoT devices, in a typical human-to-machine platform, is proposed and applied. Two case studies are showed to exemplify the method in real-world applications.

This paper also describes the main characteristics and features of IoT devices and how each one of these features opens vulnerabilities to different threats in cyberspace. Those vulnerabilities vary accordingly to different approaches to communication. Here the focus is on the H2M problem, and chapter III presents a method for secure connection and management of IoT devices in different networks. The final section (chapter 7) shows two real-world case studies, one where Sikur Connect manages a cluster of intelligent robots working at the factory shop floor, and another is a network of CCTV cameras used to monitor and control end-user customers on a chain of retail stores.

3 – Introduction

Several vulnerabilities and security issues are related to the Internet of Things, and these problems are happening in a very quick pace as the Internet of Things is becoming part of every single social and economic aspect of our daily lives, our commercial relationships and, in special, our critical industrial processes. IoT means a whole realm of concepts, stems, and technological platforms, as several standards and organizational bodies, are presenting [1,2]. This paper pays attention to the security vulnerabilities of IoT devices, and on specific solutions for H2M (Human-to-Machine) communications.

4 - IoT devices and network vulnerabilities

The Internet of Things – IoT – has come to expand and dominate the realm of the Internet, bringing great benefits and advantages, but also big problems and new challenges. Everything is connected, from the elementary object to the most complex environment, in a certain way that some companies and influencers are calling this “Internet of everything.” However, besides all social and technological IoT challenges brought together, security issues are perhaps the most fundamental ones because they imply on privacy and sustainability of the whole system. An extra example is the Sikur ID solution, a perfect match for the emerging IoT market, which has a tough challenge to ensure H2M (human to machine or machine to machine) authentication.

In the Internet scenario, generally speaking, we have mostly Human-to-Human (H2H) communications, where passwords occupy a central security role. But in the IoT domain, the amount of Human-to-Machine (H2M) communication grows every day, besides increasingly Machine-to-Machine (M2M) connections that are assuming a significative part of the communication process, where simple passwords do not work. It defines a new problem to tackle when we think about security. When working in the H2H security issues, we use encryption and authentication processes, well dominated in tools like the Sikur Messenger platform [8] and several others already present in the market.

The new issues brought by H2M and M2M demand new solutions, and H2M secure communication is the first step to achieve, as several IoT devices are coming to the networks, managed by a central monitoring and control system. The second step is a full M2M secure communication, with no human intervention, where devices could come in and out of a network without security vulnerabilities.

We can explore the problem of vulnerabilities and security issues of IoT devices through three questions [3].

1. What are the features that define and distinguish an object as an IoT device and not a single piece of equipment connected to the Internet?

2. Defined the IoT device, what are the security issues, vulnerabilities, and challenges for the device and its environment as a whole? Considering, on the one hand, the IoT device and, on the other hand, the security issues
3. What are the susceptibilities of each for those security issues? How to deal with them both as units and as a system?

Let´s go through each question with the concepts and solutions underpinning them [3].

First question: what are the features that define and distinguish an object as an IoT device and not a single piece of equipment connected to the Internet? The object, that is, the “thing” of the IoT environment, has three sets of features, which distinguish it as a typical and unique IoT device. These features, as described in [4], are:
a) the set of its specific Characteristics,
b) the set of its Relations, and
c) the set of its interface.

Some of these features are essential; others may, or not, be present.

The IoT device set of Characteristics is:

- **Processor** – the computational processing embedded in the object, able to make it act and answer to requests from the Internet and its applications (essential).
- **Addressability** – the device address, to locate it in the Internet network via routing (essential).
- **Identification** – which refers to the identity of each object, making it unique in the entire network (essential).
- **Localization** – attribute related to its physical location, its geographic position (not essential, depends on application)

The set of Relations has the following features:

- **Communication** – the IoT object's ability to receive and/or send messages to other objects in the network (essential).
- **Cooperation** – its ability to cooperate with other objects, aiming activities and cooperative applications, i.e., joint actions and collaboration (not essential, depends on application).
- **Sensing** – its ability to capture data, by sensors, from its environment and/or from other objects (not essential, depends on application).
- **Actuation** – its ability to act on its environment, operating and modifying the condition of a given medium (not essential, depends on application).

The set of the interface has one feature:

- **Interface** – refers to the interface that allows a user to interact with the object directly, to view object information, perform settings and modify its condition (depends on the application, can be local or remote).

Second question: defined the IoT device, what are the security issues, vulnerabilities, and challenges for the device and its environment as a whole? IoT devices are currently being deployed for home, building and industry automation, health and fitness platforms, vehicles and transport systems, smart cities and utilities, smart grids and infrastructure facilities, and much more. Despite so many different industry sectors, the IoT device security issues remain the same, independent of the sector applied. Reference [5] lists several of these issues and the most important of them we highlight here, among our achievements, exploring where the breaches are and how to manage to protect the singular device, the network, and the IoT platform as a whole. Some of these IoT security issues, vulnerabilities, and challenges are:

- **Impersonation/Identity Spoofing** – this means that the attacker uses a false identity, communicating with the IoT device on behalf of a legitimate entity.
- **Eavesdropping** – this is the interception of electronic communication, which happens because IoT devices often use public communication infrastructure.
- **Data tampering** – the unauthorized alteration of data, what could be done in the IoT device, or when it is exchanging data with the network.

- **Authorization and Control Access issues** – the attacker gains access to the device and then manipulates the device itself and/or the network.
- **Privacy issue** – the attacker uses private data hosted in the IoT device to explore them for unknown/unauthorized reasons.
- **Compromising and Malicious code** – the attackers can target the IoT devices with malicious code or software infection, since they usually are no-tamper-resistant, and then physically compromising them.
- **Virtual Availability and DoS (Denial-of-Service) issues** –the attackers can make IoT devices partially or totally unavailable as a result of a DoS attack. An example of this problem was described in [6], when a Distributed DoS attack targeted the east of USA internet through thousands of very simple IoT devices, like CCTV cameras and other home appliances, resulting in a huge communications blackout.
- **Physical availability** – the attacker can target the physical characteristics of the IoT device to partially or totally destroy/alter it, aiming to send erroneous messages to the network.
- **Interoperability and gateways** – as several IoT devices don´t communicate using TCP/IP, but other protocols, gateways, and other communication processes come to the network, and these are open-doors for attackers.

To deal with these security issues, a few procedures must be into account [5] when considering IoT devices:

- **Authentication** – the identity of any device must be checked and ensured every time, at every connection.
- **Data integrity** – received/sent data must be ensured that any unauthorized entity did not modify them.
- **Confidentiality** – it means that data stored or transmitted by an IoT device is not accessible by any unintended recipient.
- **User´s privacy** – it guarantees that data related to an IoT device cannot be obtained without its explicit approval.
- **Authorization and Control Access** – it means that only authenticated and authorized devices can access and/or use data of the specific IoT device, according to granted rights to specific tasks.

Taken all that into account comes the third question: what are the susceptibilities of “each” feature of an IoT device for those security issues? How to deal with them both as units and as a system? To tackle the problem of security in the new and fast-growing world of the Internet of Things, we consider the IoT security issues, vulnerabilities, and challenges, and then relate each one to the possible breaches of each device in terms of its features, as detailed in [3]. For each case, we present possible solutions and perspectives, which have to be developed as the next steps for IoT security.

From [3], we depict a list of solutions that are related to one or more of the IoT device features, which are not exclusive but are an interrelated platform. A suite of solutions defined in [3] includes:

- IoT-OS (Operating System) with the capability to analyze data alteration, embedded checker of identity, and embedded tamper-resistant identification.
- AI capability to analyze data pattern anomalies, to detect environment unexpected anomalies, and to discover network pattern anomalies.
- Statistics learning (ML techniques) to verify behavior patterns and to verify data collection patterns.

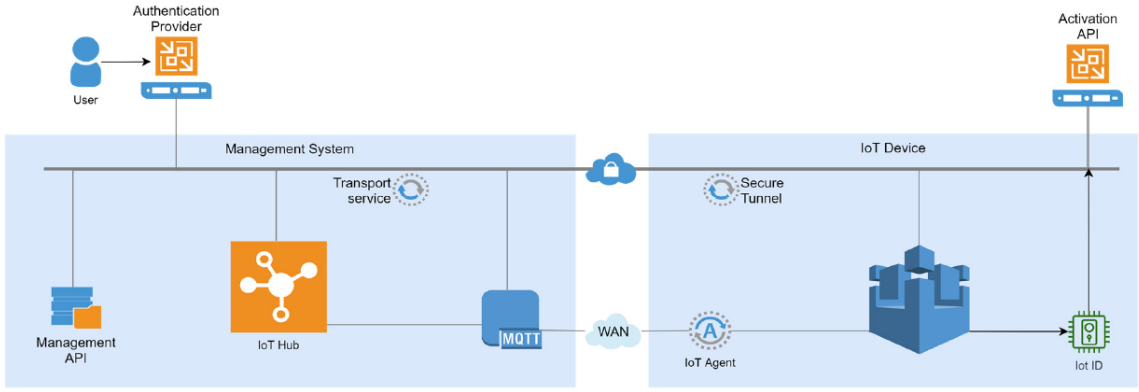

Fig. 1. General diagram of a secure H2M communication system, connnecting IoT devices to IoT Hub at the central management system.

The next section shows how we tackle the H2M problem through the introduction of a connecting application in the IoT device, enabling an exclusive and closed communication tunnel through the device to the central management system.

5 – The method for Secure IoT connection and management

To match the five security procedures defined in the previous section (Authentication, Data Integrity, Confidentiality, User privacy, Authorization, and Control Access), Sikur developed an H2M method to guarantee a secure IoT device and its network communication. Figure 1 shows the schematic diagram of our solution, using the WAN to the IoT starting up in the network, and the subsequent connections occur through the secure tunnel.

Devices get provisioned with two software components at the manufacturing stage. The first is the Sikur Connect Agent, which is responsible for:

a) activate the device on the Management System;
b) to manage and control the device operation, i.e., to receive notifications from the Management System, open the Secure Tunnel, reset the device, update the IoT device software and other Linux commands, and to control the reverse tunnel creation when communicating with open networks.

The second is the Sikur ID software, which provides a strong, unique identifier for the device that cannot be shadow copied, cloned, or tampered.

A. Secure H2M IoT device activation

The activation process can be automatic or manual (illustrated in Fig. 2 and Fig. 3, respectively). The “Automatic Activation” is done after turning on the device for the first time, and it happens through the following automatic flow process:

1. On the device's first run, through Sikur Connect Agent, the device registers itself on the Management System (through WAN) using the Management API, passing its unique identification (IoT ID) and credentials.
2. The Management System verifies the IoT device ID and credentials, authorizes the device to join the Sikur Connect inventory (a manual verification and authorization is also possible).
3. The Management System sends authorization keys to the IoT Device using the Secure Tunnel, and the Sikur Connect starts to accept connections from the IoT Device.
4. The IoT Device gets activated in the secure platform, and the Sikur Connect Agent starts listening for commands through the Secure Tunnel.

An IoT Device “Manual Activation” is also possible, following these steps:

1. In the Management System interface, the user (authorized administrator) adds the new IoT Device in the Sikur Connect inventory, when a unique shortcode is generated onscreen.
2. Through WAN, the user runs the Sikur Connect Agent “manual activation process,” inputting the shortcode.
3. The Management System verifies the IoT device ID and credentials and authorizes the device to join the Sikur Connect inventory.
4. The Management System sends authorization keys to the IoT Device through the Secure Tunnel (instead of WAN).
5. The IoT Device gets activated in the secure platform, and the Sikur Connect Agent starts listening for commands through the Secure Tunnel.

B. Secure H2M IoT device operation

As soon as the IoT Device has joined the secure IoT platform, it is ready to work and operate securely (Fig. 4 illustrates the operation process). Initially, the IoT Device starts receiving commands through Sikur Connect, which uses the MQTT protocol [7]. Each command is sent to the IoT Device with a cryptographic signature; thus, the Sikur Connect Agent can validate that the command came from an authorized actor through the Management System. Then the Sikur Connect Agent opens the Secure Tunnel following these steps:

1. The Management System receives the command to open the Secure Tunnel. The Sikur Connect agent checks the Management API to assure that the command is still valid and to define which IoT Hub and port should open the tunnel.
2. The Sikur Connect Agent opens a reverse secure connection using SSH (Secure Shell protocol).
3. Once the IoT device is connected, the Sikur Connect updates the Management API to signal that it can receive connection requests inside the secure tunnel.
4. The user then connects to the IoT device using the Secure Tunnel based on the password-less infrastructure.

The user session is recorded for analysis if necessary. Other commands present in the H2M secure Management System are:

- **Update base software**: on receiving this command, the Sikur Connect Agent checks for newer software and update itself if necessary.
- **Reboot**: upon receiving this command, Sikur Connect Agent reboots the device.
- **Send stats**: on receiving this command, Sikur Connect Agent gathers IoT OS stats and send it back to the user. It is possible to send custom status from other software using the same secure channel.
- **Run command**: on receiving this command, Sikur Connect Agent forwards commands to the IoT OS.

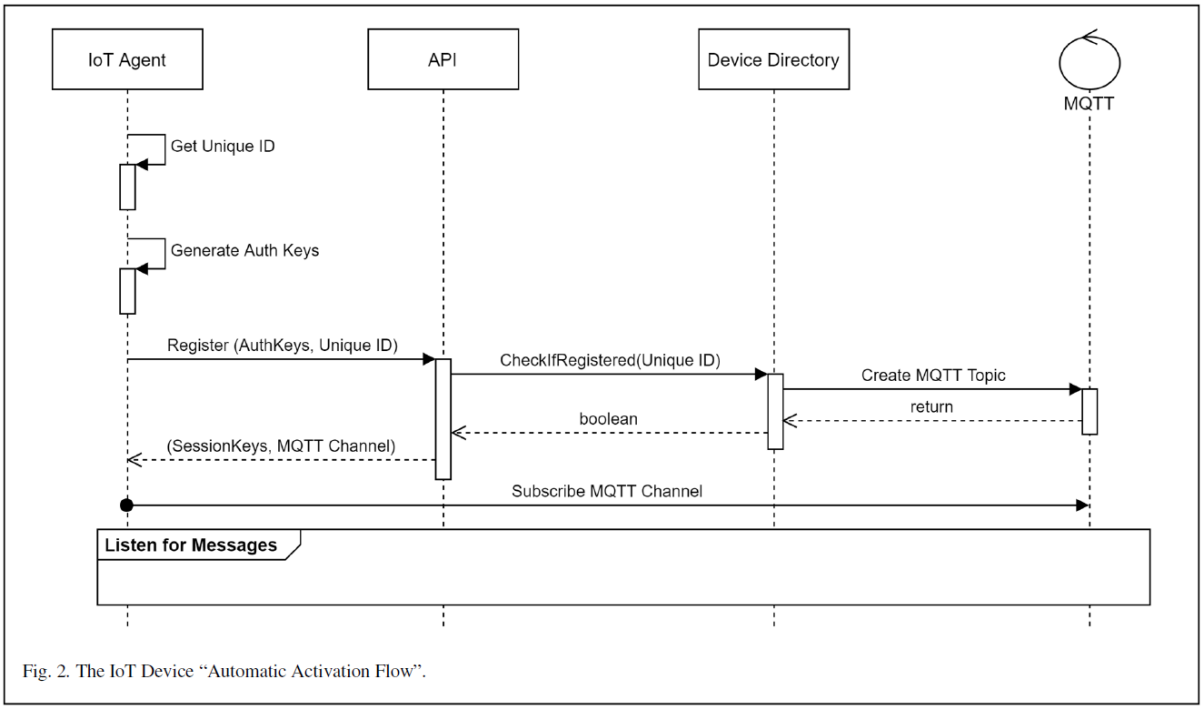

Fig. 2. The IoT Device "Automatic Activation Flow".

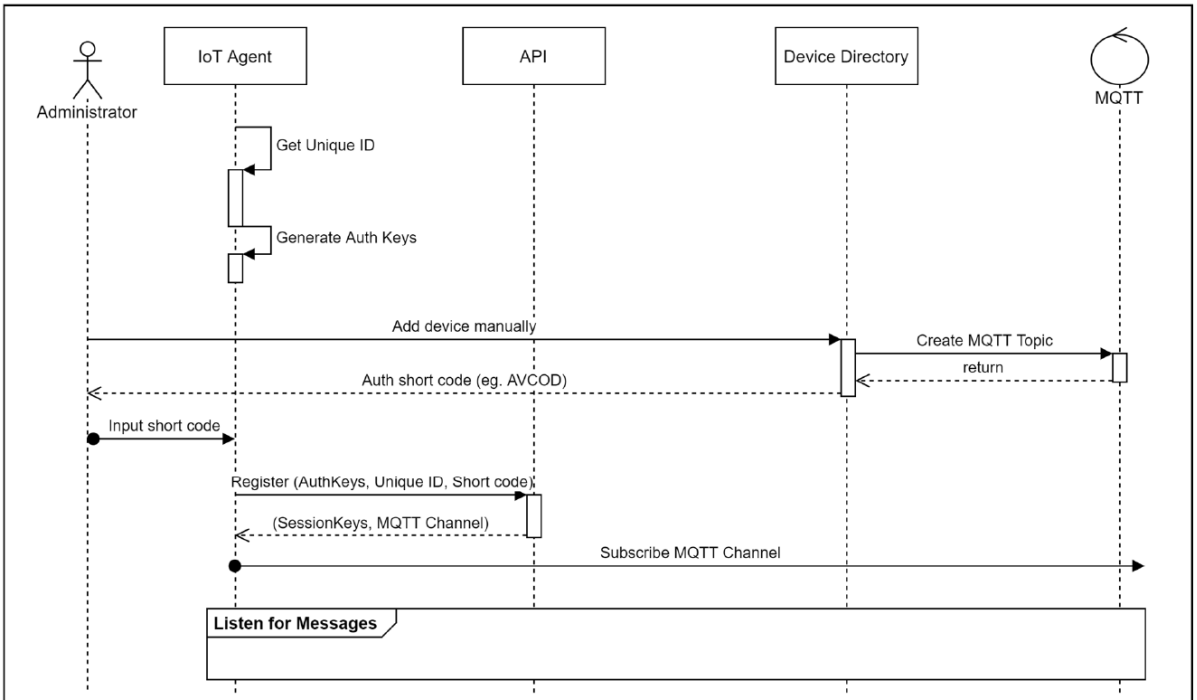

Fig. 3. The IoT Device "Manual Activation Flow".

6 – Why is Sikur Connect safe?

In a short sentence: it is all about keeping the private key safe.

It is not possible to go further when the central piece of information is not decently protected. An authentication system grail is a private key (sometimes called a token) because it opens doors to user information. Sikur ID, together with Sikur Connect, implements several security layers, as previously mentioned, making private key protection complete.

A recurrent question is about where and how to store sensitive data, like passwords, secrets, and keys. Sikur products use industry-standard storage equipment for this kind of data, a FIPS-compliant HSM (Hardware Security Module). Building security in a layered approach is also about taking advantage of what is available in terms of cloud infrastructure, like Microsoft Azure capabilities. So, in the cloud level, for public and private clouds projects using Azure, Sikur leverages Microsoft's latest threat management and mitigation protocols, including intrusion detection, distributed denial of service (DDoS) attack prevention, anti-malware, penetration testing, analytics, and machine learning tools to help mitigate threats.

Deploying encryption with the most proven industry algorithms (like RSA and AES) is nothing new, and many vendors do it. Putting its products to the test by ethical hacking companies, periodically, is also good practice; it helps to keep the product up to date and safe from the latest attack trends. Researching and developing new or better ways to safeguard data and mitigating threats as Phishing, like the Sikur Smart MFA, is a task that demands time, effort, and expertise. All of this improves product security, making it safer.

The majority of Identity Providers target user information. So, for them – even claiming privacy and regulatory compliance – accessing personal data (again, claiming anonymity) is part of their businesses. Sikur, as a security provider, has only one goal: keeping user data accessible safe and only available to its owner.

7 – Our real-world cases and Conclusions

The IoT market is still a new concept in many businesses, and there are a lot of uncertainties when deploying it in an organization. For large and industrial systems, the concern is significantly more profound, and implementing it correctly from the start is essential. Sikur Connect secure platform started as proof-of-concept research and turned to be an industrial Management and IoT Hub system for the IoT market. It takes advantage of Sikur's long-term engineering experience in cybersecurity, turning it into a flexible and robust product, ready for all-size organizations.

Two case studies below show different approaches by the users and their main outcomes. One case is related to control and manage industrial robots used on the factory floor; the other is related to cameras for physical security CCTV (closed-circuit television) applied by a chain of retail stores. Both were aware of security issues and vulnerabilities of their IoT devices, especially because of their mission-critical functions.

A. Case study: the cluster of intelligent robots

The robots, developed by the company AVGs [9], are used for intelligent transportation and towing of materials on the shop floor of vehicle manufacturers. It is a cluster of robots working together to execute different tasks (Figure 5). These robots are typical IoT devices, presenting all the nine features described previously in Section II: Processor, Addressability, Identification, Localization, Communication, Cooperation, Sensing, Actuation, and Interface.

The security issues for the robot provider were the following: how to make an H2M connection. That is, the manager performs updates and monitors the self-guided robots in real-time, using network environments where connection confidentiality is not guaranteed? To update or execute maintenance tasks its self-guided vehicles, the provider often needed to send the technical team to the factories, because external connections are difficult to configure (or not allowed by the customer). Each customer has a customized infrastructure due to the security policies of the company itself. Sometimes the issues are related to the internet connection quality for external access.

Sikur Connect fixes two issues. The first is the security problem through the authentic IoT ID plus the Secure Tunnel defined by the IoT Hub. The second is the connection quality, as the Secure Tunnel uses our extra-low band private channel for communication, which means that even with poor internet speed, the technical team can remotely monitor and control the robots using Sikur Connect Management System, directly and transparently.

B. Case study: the CCTV system

The platform developed by Dod Vision [10] uses cameras, installed in several retail stores, to get real-time images for marketing campaign management and customer behavior analysis. These cameras are IoT devices presenting six of the IoT features described previously: Processor, Addressability, Identification, Communication, Sensing, and Interface.

Through the Dod platform, the manager can create goals for different stores, track results, and estimate return on investment to optimize marketing investment. It analyzes the daily conversion rate on different days of the week and monthly. As the cameras take images from customers, the platform has strong responsibilities on confidentiality and security issues are the most sensitive (Figure 6).

Here again, the provider faced two different problems. The first was how to access equipment in heterogeneous networks (for maintenance, for example) where there is no possibility of configuring the connection, especially for allowing external access in the firewalls to every device. The second was the device security itself, not admitting any other unauthorized user to get access, locally or remotely. Sikur Connect solved it both by installing the Sikur Connect Agent, which activates each device to the Management System, creating the Secure Tunnel for each connection command. Through the platform, no other access is possible instead of the one defined by the Sikur Connect Agent and the corresponding Sikur Connect inventory.

C. Conclusions

Both study cases are examples of successful applications of the Sikur Connect H2M method, where, from the device perspective, no passwords are necessary. This solution eliminates problems as malware installation from unauthorized users or DDoS attacks, as described in [5].

The Sikur Connect method is in industrial use, and a few notes are important to mention to reiterate its capabilities:

- It is an H2M secure platform to guarantee the identity of the IoT device.
- It guarantees that only the authorized manager, through the Sikur Connect Management System, will be able to configure, install/uninstall software, manage and reset the IoT device;
- It does not guarantee the quality or content of the end-user solution, transmitted through the WAN. For example, the data transmitted by the case studies of robots (their instructions) or cameras (images) are not part of the security process.

The next step for Sikur Connect is the M2M secure authentication and communication, to be achieved through an automatic password-less platform of Sikur Connect agents, connecting machine-to-machine through our IoT Hub and with no human management intervention.

8 - References

[1] RECOMMENDATION ITU-T Y.2060. Overview of the Internet of things. ITU-T – International Telecommunication Union, 2012
[2] 2413-2019 - IEEE Approved Draft Standard for an Architectural Framework for the Internet of Things (IoT).
[3] M. Fazion, “Vulnerabilities and security issues of IoT devices”. Sikur Report number #01022020, January 2020. DOI: 10.13140/ RG.2.2.14211.86562.
[4] M. Fazion. Designing “things” for the Internet of Things. In: I Congresso Internacional & Workshop Design & Materiais VII, Universidade Anhembi Morumbi, São Paulo: 2016.
[5] C. Bekara. “Security Issues and Challenges for the IoT-based Smart Grid”. International Workshop on Communicating Objects and Machine to Machine for Mission-Critical Applications - COMMCA-2104.
[6] M. Fazion, P. Marin. “Information Security and ESS in the age of Internet of Things”. ICT TODAY BICSI. , v.38, p.16 - 23, 2017.
[7] MQTT Protocol, OASIS - Organization for the Advancement of Structured Information Standards

[8] Sikur platform, www.sikur.com.
[9] AGVs Company (agvs.com.br)
[10] Dod Vision Company, dodvision.com.