INTERNET OF THINGS: CHALLENGES AND OPPORTUNITIES FOR PRIVATE SECURITY PERSPECTIVE

Dobre Valentin
Thesis
Summer 2017
Business Information Technology
Oulu University of Applied Sciences

ABSTRACT

Oulu University of Applied Sciences
Business Information Technology

Author(s): Dobre Valentin
Title of thesis: Internet of Things: Challenges and Opportunities for Private Security Perspective
Supervisor(s): Viitala Matti
Term and year when the thesis was submitted: Summer 2017 Number of pages: 24

This topic was chosen due to the author's long work history in a private security firm, and experience in using Access Management tools with Surveillance tools.

The object of the thesis is to analyze the Internet of Things of today's networks tasked with monitoring security and consider the devices that are the main components of these networks. Considerations include their current technologies and operation, and possible improvements aimed to improve future products and services that private security companies will be available to provide.

The author's practical experience will be complemented by the following books: The Internet of Things, Collaborative Internet of Things for Future Smart Connected Life and Business, and Enterprise IoT: Strategies & Best Practices for Connected Products & Services. Further sources of information include technical documents and user manuals of devices, tools, and services that are available to today's employee working in private security.

The Internet of Things is already in use in many aspects of security services, specifically access control and surveillance technology. However, there is room for considerable improvement in making these two systems more reliable and there is potential for great improvement of security services effectiveness by unifying these two systems, and work is being done to do just that.

The future may see security companies providing completely mobile video surveillance services. Drone technology, as it matures, is likely to play a big role in the implementation of such services, making them a possibility to consider, when providing flexible services to clients.

Keywords: Internet of Things, IoT, Security, Services, Sensors, Network,, IP, Camera, Surveillance, Access Control, Fleet, Tracking

CONTENTS

1 INTRODUCTION TO INTERNET OF THINGS

Internet of Things is a concept that has now been talked about for decades; To put it shortly, IoT is a system of connected digital devices, each being indentifiable from the others, within a network that can communicate independently without the need for human interaction. This thesis focuses on the impact IoT is having in private security companies, the type of services they can offer, the technologies they use, and how IoT can improve security services and efficiency as IoT becomes more integrated as a part of their operations.

The author of the Thesis has close to 11 years working experience working in private security in diverse roles, using various technologies, and has witnessed the change in technologies first hand. All the way from alarms' identifiers being printed on paper, to alarms' location being highlighted on a computer screen, using the floorplan of the building as a map.

The knowledge base for the thesis comes from years of experience in working with security devices and services. Samuel Greengard's book The Internet of Things has provided a wider understanding of IoT and it's history while the book Collaborative Internet of Things had good information of possible future applications and requirements. Technical documents and user manuals for security specific devices and services were also used as references where needed.

Security companies use networks of various sensors to measure and monitor the real world, react to it and present the necessary information to security officers for evaluation and action. These sensors include, but are not limited to; Motion sensors, Entry Sensors for doors and windows, Glass Break sensors and Video Cameras. The majority of sensor technology relies on detecting changes in Infra Red light, Acoustics, and Magnetic fields.

The use of magnetic fields is particularly important when combined with Radio Frequency Identification tags. RFID tags are small electronic devices that consist of a small small chip and an antenna that activate when moving through a magnetic field. They carry a small amount of data on them that they transmit for short distances. In fact, in his book, Greengard describes RFID tags as perhaps as the most crucial part of IoT in their ability to connect any physical object to the digital world.

2 SENSORS AND PERIMETER MONITORING

”Sensors are the eyes, ears, nose and fingers of the IoT”(Greengard 2015, 121)
In his book, Greengard furter explains how humans relied on analog and low tech solutions for detecting changes in their environment. Any devices from thermometers that used mercury, to more modern analog devices were useful in measuring the environment when calibrated correctly, but fell short in connectivity and accuracy. (2015, 122)

In practice the change from analog devices to digital devices has made a considerable change in how security systems work and their effective utilisation. When movable Dome security cameras were considered new technology, and a shopping center was being closed for the night, the security officers would point some of the dome cameras to strategic locations eg. outer doors for the night, while others would be put on a ”patrol” mode that meant the cameras would continuously pan, tilt and zoom on a pre-programmed path throughout the night.

Today’s digital Dome cameras can be programmed to react to a variety or alerts being triggered. If a door is opened and a Door Entry Sensor triggered an intrusion alert, the Camera network can immediately react and point the nearest Dome camera to the area the alert originated from. The network of devices reacting to alerts is rarely limited to security cameras, since usually the building’s lighting system is also among the list of systems reacting to alerts, and can be programmed to provide light throughout the building in order to improve filming conditions for the cameras.

2.1 Types of Sensors

Sensors are how the digital world measures and reacts to the physical world, and the sensors that security services utilize today are almost all sensors that are designed to detect fluctuations in one of the following: Magnetic forces, Light, Infra Red light, and Acoustics.

Key elements to the efficiency of the networs of devices is reliability of individual sensors. Each sensor being resistant to interference and tampering has long been a priority in the development of these devices, but with the addition of IoT the list of requirements grows larger. As the amount

of devices interconnected to the network, things like computing power and distribution of computing are things that have become much more important. (Behmann & Wu 2015, 2.4.3.)

2.1.1 Door and Window Entry Sensors and Panic Buttons

Door and Window Entry sensors are essentially made of two pieces that are designed to work together to determine whether a door is closed or open. One piece is a magnet that is installed on the opening element of a door or window, while the other is a detector element sensitive to the presence of the magnet, and is installed on the frame of the door or window. When the door, or window, is opened and the magned gets pushed far enough from the sensor, the door can be detected as being open.

Security systems are sophisticated enough not to treat all opening events as alarms. However, in the event of an alarm, in addition to activating the lighting and repositioning security cameras, the system can also relay the alarm to a central control room and a security officer may be dispached to verify the reason for the alarm.

Entry sensors are mostly used to detect unknown entries through possible entrances and therefore alerts are usually classified as Intrusion alerts, and require a human to verify the reasons for the alert. Intrusion alerts are usually relayed directly to a local security officer aswell as a central control room simultaneously. Often, if a security officer has not verified the alerting area in due time, the control room may call the officer in order to further assess the situation.

Panic buttons require human interaction to function, and are normally located at cashier points in retail sores. When an alarm is recieved from a panic button, the response is very similar to intrusion alerts originating from Entry sensors. While the alert may be simultaneously relayed to a control room and an officer, the control room can often immediately respond by viewing footage from the corresponding security camera and act according to the situation. Almost always the minimum reaction to alerts from panic buttons is a telephone call between the control room and the personnel working in the property the alarm originated from.

2.1.2 Radio Frequency Identification tags and Alarm Gates

”RFID technology helps in automatic identification of anything they are attached to, acting as an electronic barcode.” (Bechmann & Wu 2015, 2.7.3.)

RFID tags are very important in that every physical object that has a RFID also has a digital identity and so can be tracked and monitored by a network of devices. Active RFID tags have an internal power source and can transmit data over longer distances while passive tags do not have internal power but can generate it when near a reading device. (Bachmann & Wu 2015, 2.7.2.)

A good example of an active RFID is a car key that unlocks the car remotely. When the user presses the button on the key, the RFID inside the key transmits its data around the user to a radius of about 15m. Not all of the cars within radius will detect the presence of the signal, however, since different cars can use different frequencies. Only the cars that can receive the correct frequency will detect the signal and receive the data. Once the data has been received, it still has to be decrypted, and only if the correct encrypted ID was transmitted the door will open.

Passive RFID tags are extremely useful in that they can remain dormant for decades and still function propely when necessary. Passive tags do not have an internal power source, instead, they create their own power when brought close to a reader device. RFID readers are capable of generating a small magnetic field, which the passive tag then uses, to create the necessary power to function (Greengard 2015, 17). In security services such reading devices are often Alarm Gates in retail stores, or reader devices of Access Control Systems.

Alarm Gates are essentially a form of access control. RFID tags are glued on the products located inside the store, and as the products go through the cashier point the RFID tags are also scanned by the cashier. Scanned tags are automatically whitelisted by the system and the tag is allowed to pass through the gate without an alarm. Unscanned tags are very likely to not have passed through proper checkout procedure and thus not whitelisted, so the gates are programmed to sound the alarm in the presence of a non-whitelisted tag.

Considering the layout of modern retail stores, with multiple Alarm Gates, entrances, and exits, the security systems often are sophisticated enough to highlight the specific gate the alarm originates from on a map of the property, in the control room where the security officers are. This same alarm event can also be used as a trigger to focus the nearest dome camera towards the area of the alert, or display the view of the appropriate static camera. All without requiring input from the human operator.

2.1.3 Motion Detection Sensors and Glass Break Sensors

Motion detectors are used to increase surveillance in a specific area and are best suitable to be used indoors. The most used type of motion detector reacts to Infra Red light, and detects heat sources, other type of detectors work by using ultrasound and microwaves. Motion detectors can come equipped with a combination of sensors, eg. Infra Red and Ultrasound, in an attempt to increase reliability and tamper proofing.

Modern motion detectors can contain onboard microprocessors, capable of analysing the object being detected, in an attempt to minimize the amount of false alarms. Some of the newest solutions for industrial areas include motion sensors prioritising certain areas, and security cameras being pointed to these prioritized areas when the Motion Detectors indicate movement.

Today, there are two type of Glass Break Sensors that being used, Seismic and Acoustic sensors. Seismic sensors are glued to the glass directly and they detect the vibrations produced in the glass when it breaks. Acoustic sensors are essentially a microphone that detects the sound that glass produces when it breaks and they are installed inside the room, typically on the roof of the room, in proximity to the wall and one sensor can monitor several windows. Due to their ability to monitor several windows at a time, Acoustic Glass Break Sensors are the most cost effective.

2.1.4 Photoelectric Beam Sensors

Photoelectric Beam sensors are widely used in a variety of solutions and most people are completely unaware of their existence. These sensors project a curtain of light that is designed to remain uninterrupted in all weather conditions. In security services they are commonly used in front of windows of buildings to detect possible attempts of entry through windows and other sensitive areas such as roof access points.

Beam Sensors are typically placed on the outside wall of a building along the windows, and can sometimes give false alarms in extremely bad rain, thick fog, or when a large enough animal obstructs the beam. The beam may also become obstructed during the winter by thick snow forming on the window's ledge, or if ice is allowed to accumulate on the sensor itself. This type of mounting could have its benefits, however, since outdoor mounting may make it possible to power Photoelectric Beam Sensors by harvesting solar energy.

2.2 Sensor improvements for IoT applications

Improvement to sensor technology is important to increase accuracy and reliability of all detectors, generating fewer false alarms means the security officer, and indeed the network, can direct their focus better towards areas where it's needed.

However, with the amount of data the IoT network is required to handle, stable connections with sufficient capacity to transmit data are located high on the list of things to improve. Only with dependable networks can IoT provide consistent and predictable results, increasing reliability of communication between humans and devices. (Greengard 2015, 125.)

Power over Ethernet is also an option available for increasingly power efficient devices as their power requirements become low enough, to be sustainable via the PoE standard. This means decreased need for cabling for each sensor or detector, since data and power can be delivered throug just one cable, and makes building of networks alot more cost-effective. (Behmann & Wu 2015, 2.4.3.6.)

Furthermore, according to Greengard, scientists are already hard at work developing not just more efficient battery technologies, but development of wireless power delivery technology is already ongoing. These technologies include the more traditional Magnetic Induction and Solar Charging, while trying to push the limit of technology even further. Attempts are ongoing to generate energy from wireless signals such as Wi-Fi, Television-, and Cellular signals, that surround the sensors (Greengard 2015, 126.). Devices such as Motion sensors, Glass Break Sensors and Entry sensors, may soon become completely wireless as technology moves forward and power delivery can be just as wireless as data transfer.

3 VIDEO SURVEILLANCE SYSTEMS

Modern digital Internet Protocol Cameras are designed to function in a connected environment and can utilise onboard computing to reduce load from the network in situations, where the images need to be post-processed. IP Cameras have quickly adapted higher resolutions and practically all of their images are compressed by the microprocessors within the camera unit, before being permanently recorded by a Network Video Recorder, or Network Storage.

IP Cameras send their images to a central server where the video is stored and can be accessed from authorised desktops over the internet. IP Cameras attempt to reduce the required disc space, and network traffic, by compressing the video, and only recording when movement is detected. Most cameras are also equipped with a genuine Infra Red filter, and are thus capable of providing very good video footage regardless of time of day. (Behmann & Wu 2015, 2.4.3.)

3.1 360° Panoramic cameras

This type of camera is also known as a fisheye camera and it's often a 360° Panoramic camera that utilises just one wide angle lens. It can be a very useful tool in monitoring a wide area, providing one continuous image, clear of any seams or sudden changes in directions of filming. Normal operation includes the ability for the video to be digitally post-processed by the camera in order to remove distortions, and provide a natural looking rectangular image of a small portion of the camera's total view. (Axis 2017, cited 30.5.2017.)

Using a fisheye camera makes it alot easier to follow an individual's movement through a given space, since there is no need for the human operator to change between cameras and adjust his perception to the different directions the cameras are viewing from. The Fisheye camera has a smaller resolution when compared to solutions that utilise multiple lenses to achieve similar results, however, this is a drawback that is hardly noticeable unless trying to view images at a considerable distance from the camera, optimizing for indoor usage.

3.2 Facial recognition

Facial recognition is still a relatively new feature and is really made possible by the rising affordability of high resolution IP cameras, and increased computing power onboard the camera units themselves. The cameras used for their facian recognition abilities are recommended to be atleast 1080p, and that the face should occupy an area approximately 100px wide, while the distance between the eyes be approximately 50px. As a rule of thumb, an overall pixel density of 6px / cm is what is recommended for reliable recognition, and that is with good ambient lighting, preferrably indoors where it's more controllable. (Axis 2017, cited 30.5.2017.)

When camera facial recognition does work it can be used to compare the faces, of the people the cameras are monitoring, against a database of people eg. employees, and security personnel be alerted to possible misuse or wrongful access.

Facial recognition can also be a very useful tool when trying to find a specific event or tracking the movements of a certain individual, throughout a given event area or a mall. Cameras at the entrances may be used to identify a person of interest and then the cameras may display only recorded events where that person was present during a given time frame. This can be a very powerful tool, and it would make it considerably easier to access recorded information.

3.3 People Counting

Tracking human activity and movement starts as soon as a person enters the guarded property and businesses like retail stores are especially interested in how much traffic they can attract. Security services can offer services in measuring the amount of customers by positioning digital cameras dedicated to this task near the entrances.

Where traditional methods would use a simple Photoelectric Beam sensor, digital cameras can be a much more effective tool in counting human traffic. Cameras can utilize image analysis and determine the direction a person is walking, thus counting incoming traffic and outgoing separately in the same spot. (Axis 2017, cited 30.5.2017)

3.4 Drones and Video Surveillance

As drone technology becomes increasingly affordable and longer flight times more sustainable, security companies will undoubtedly incorporate these devices as part of their operations to increase the quality, and type of service they can provide. Already, drones are being used in the oil industry to perform large scale survey of roads and other infrastructure (Behmann & Wu 2015, 2.9.3).

One possible use for this technology could be at large scale public events, such as rock concerts, since events with a large concentration of people increase the need for versatile security services. Currently video surveillance can be rather limited at these types of events due to the venues being built and dismantled as the artist or event changes location. Security companies could one day provide a basic mobile video surveillance service with a single drone, thus removing the necessity of building infrastructure for surveillance hardware altogether.

3.5 IP Cameras continue to improve for IoT applications

Making it easier for camera operators to manage cameras and video streams is a constant process and there is an increase in support, and interest, for intelligent features that help manage videos. IP Cameras also benefit greatly from the increase in availability of high bandwidth networks paired with improved trasmission possibilities, and compression of data, over wired and wireless networks (Behmann & Wu 2015, 2.4.7).

IP Cameras also have the capacity to detect movement and currently mainly use this capability to reduce excess recording. However, fisheye cameras with motion sensing capabilities can be used as a 360° motion sensor aswell as a camera, providing redundancy in motion sensing for the entire security network. Such use-cases are a new approach, and provide a good example in the versatility of video cameras. Furthermore, utilizing facial recognition in combination with access control may make it possible to alert security personnel of possible suspicions, of an individual moving inside the property with an access key that is registered to someone else. Facial recognition may also be used to signal an alert when an unauthorised person gains access to an area by following someone else to said area.

4 ACCESS CONTROL SYSTEMS

Access Control Systems(ACS) are designed to restrict physical access of humans to areas according to their role or given authorisation in a an environment or organisation. These systems are widely used in workplaces and are of high importance when ensuring security of property, both material and intellectual. At the most basic level you have a door and a lock, but even relatively small environments and organisations can benefit from more complicated digital systems that are available.

Most common modern ACS's are designed using RFID-tags that are given to users and are then used within the environment as keys to open doors. These systems are known as Swipe Access and are often complemented with the use of Electro-Mechanical locks. eLocks are a relatively new technology and are often a completely separate system of Access Control, complementing the main Swipe Access System.

4.1 Swipe Access Systems

Today's Swipe Access Systems utilize RFID tags to identify people accessing doors in a given environment, to the users, these tags serve as keys that open doors. The RFID tags are passive RFID's in the vast majority of cases, and the only information they contain is a serial number.

Each door within the system is equipped with its own identifiable RFID Reader unit, and is connected to a central database where all the user specific access information is stored. Some readers are equipped with a numerical keypad in order to provide an additional layer of security, these kinds of readers are typically located on the outside doors. Virtually all readers are also equipped with lights and are capable of giving an audio tone so that the result of the Access Control check can be indicated to the user.

Access controlled doors are locked 24/7 thus, from a user's point of view, usability and accessibility is improved, by eliminating the need to use a mechanical key to open each and every door. Employers and businesses benefit from an increase in security since doors can be

locked and access restricted according to person and security companies can log the movement of people within the environment being monitored.

4.1.1 Passing through an Access Controlled Door

When a key is swiped the reader sends the serial number of the RFID to the database, where the serial number is used to identify the user and his access rights, which are then compared to the door reader's ID. When access through the door can be granted, the system notifies the user and also sends a signal to the lock within the door telling it to open. When a reader is equipped with a keypad, the reader first asks for the code before the lock can be given the signal to open.
The basics of this process is illustrated in Figure 1.

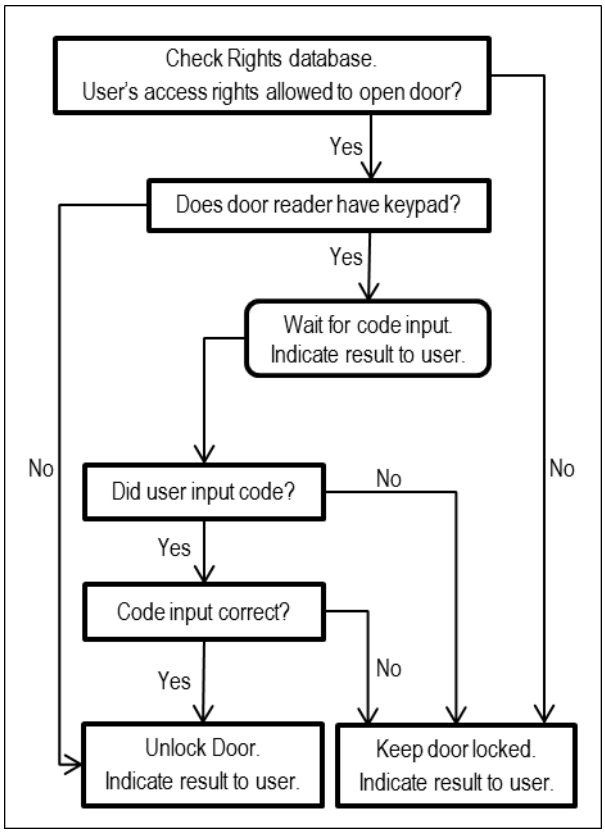

FIGURE 1 Basic communication between door reader and database after a key is swiped.

4.1.2 Benefits of Access Control

Customer companies benefit from an increase in security, and are afforded more flexibility in how to limit people's movement inside their premises. Property owners can have multiple customers

renting within the same building by having separate areas that each group of people can access, without the need to build physical walls or keep doors permanently locked.

Security services benefit from a database of information tracking people's movements in the environment, while also having the ability to improve surveillance, by detecting users' attempts to access unauthorised areas. The access Control System can be programmed to detect repeated attempts resulting in unauthorised access, and can send a signal to a security camera that can be automatically positioned to record the area of interest. (Schneider Electric 2015, cited 30.5.2017)

RFID's that are used in Access Control are also mostly passive and thus relatively inexpensive to replace compared to mechanical keys in the event one gets misplaced, or lost. There have also been cases where al mechanical key with strong access capabilities has been lost, resulting in the need to replace all of the locks in a building. Losing a RFID that belongs to a user with strong access rights would only necessitate replacing the RFID for that user, thus removing the lost RFID from the system, denying it all access. (Schneider Electric 2016, cited 30.5.2017)

4.1.3 Administration of Access Control

Networks of Access Control systems are made up of door readers, these door readers have their own ID, and can be assigned into groups and given a group name. This makes it easier to create entire areas of access and assigning those areas to a user, the user then has the ability to open any door within the areas that he has been granted access to. (Schneider Electric 2016, cited 30.5.2017)

Searching through the stored access information can be done in several ways, two of which are by user, or by door. Searching by users makes it easy to verify how an individual has moved within the environment, and searching by door makes it possible to identify people who, for some reason, may have access through a door they are not supposed to. (Schneider Electric 2016, cited 30.5.2017)

4.2 Electro-Mechanical locking systems

Electro-Mechanical locks are a combination of mechanical locks and digital access control authorisation. They represent a cost-effective option in adding programmable access control to existing doors/locks without the necessity of complicated cabling for power and data transfer.

Electro-Mechanical locks' cylinders are capable of generating all the electric power needed for the digital authorization process, from the movement of the key as it's inserted into the lock. This has removed the need for any batteries for the lock's standard features, and is why the need for cabling is minimised (iLOQ 2017, cited 30.5.2017). iLOQ is an electro mechanical lock developed in Finland and is widely used internationally, this is why it has been selected as an example.

4.2.1 Standard operation of Electro-Mechanical Lock (iLOQ)

Standard features of iLOQ cylinders do not need any power sources to function when operated by a human. Batteries are not needed in the lock cylinder, or the key, in order to perform their basic function. Mechanically the keys are identical, what sets the keys apart is the digitally encrypted information stored in in the key. (iLOQ 2017, cited 30.5.2017)

The first step of the opening procedure happens when the key is inserted and it powers the lock's electric components. The second step takes place as the electronics inside the lock cylinder compares the information of the lock with the information on the key. The final step happens when a key with valid access rights is detected and the lock's internal electronics allow the mechanical cylinder to turn, opening the door. (iLOQ 2017, cited 30.5.2017)

4.2.2 iLOQ Programming device, Remote management and Time restricted access

The iLOQ Programming device consists of three notable components: Main device, an attached programming key and the iButton-token, which is a component used for user identification, whithout which, the programming device does not work. The iButton-token is essentially a

magnetic RFID that is required to be attached to the programming device whenever the user wants to manage iLOQ keys and locks, it is also used as additional part of a user's credentials when logging in to the iLOQ control software. (iLOQ 2017, cited 30.5.2017)

When updating manually, the necessary lock cylinders are individually given the updated information, using the attachment of the programming device that resembles an iLOQ key. Programming the locks with the remote software can be made from a desktop, in real time, using the programming device and iButton-token when logging in. Remote management is an additional feature for these locks as well as Time Restricted Access Control. Cylinders that are equipped with Time Restricted Access control also require a battery to keep the timing clock powered. (iLOQ 2017, cited 30.5.2017)

4.2.3 IoT possibilities of electro mechanical locks (iLOQ)

iLOQ's design for electro magnetic locking is designed to be a cost effective solution fitting existing locks, and in their most basic configuration are not ideal for IoT solutions. However, with the ability to connect the lock cylinders to a network the cylinders could be upgraded with Power over Ethernet. Furthermore, mechanical keys are often and without permission shared among colleagues, especially during vacation times. Giving the lock cylinder the ability to check if an employee has indeed clocked into work on a given day would minimise misuse of keys and further improve access control reliability.

5 SMART FLEET TRACKING

Security companies operate a fleet of cars driven by their employees while performing their duties. Security officers use company cars to investigate intrusion alarms, amont other things, while marketing representatives set meetings with clients and manage customer relations. There are several aftermarket telematics solutions available, and security companies often have these installed in their cars to monitor the efficiency of their fleet.

5.1 Fleet Data and Management

Telemetry gathered from the vehicles often includes vehicle speed, location, engine parameters and the G-forces the car experiences resulting from cornering, braking and acceleration (Morrish, Puhlmann, Slama & Bhatnagar 2016). This information can be used in an attempt to manage employee's driving habits, through feedback from an employee's supervisor. Thus making it possible to reduce fuel consumption through less aggressive driving, and by analyzing driving routes in order to find more efficients routes.

With the recent trend of insurance companies adapting more customisable service packages and personalized premiums, sometimes based on driver performance and driving kilometers, even further increases in long-term efficiency of car fleet may come in the form of decreased insurance costs. (Morrish et al. 2016.)

5.2 Practical Implementation and Future Usability

Data collected by the telemetrics is stored in the cloud, meaning employees responsible of the fleet management can review results, and make decisions anywhere at any time by just logging in to the service. Decisions are often made with the intention to reduce fuel consumption, and identifying vehicles that consistently are consistently in a better situated to carry out a given task.

Third party, or aftermarket, installations of telematics can be rather fickle in practical terms. While the fleet's communication with the cloud can be stable and fast enough using today's technology,

the telemetry itself can be unreliable and inconsistent. Two cars of the same manufacturer and model, using the same telematics system and both being driven by the same driver in identical conditions, can produce differing telemetry results. This issue may well be resolved, however, as technology becomes more affordable, and the sensors and systems required for reliable telematics become a part of standard equipment of car manufacturers.

6 CONCLUSIONS

In discussing the Internet of Things, security services are already able to use it effectively, particularly when providing services of video surveillance and access control. Security companies use the Internet of Things to increase the efficiency and versatility of their services, while customer companies benefit from improved coverage and efficiency.

Key areas of development include the network's data transferring capacity and the compression of data. Hardware improvements are being researched in matters of power delivery and – efficiency of individual devices, and possible energy harvesting ability of devices.

Security companies also utilize IoT in monitoring their own performance, in order to identify areas where refinements can be made. Digital tools such as fleet tracking may one day become critically important in determining the driving routes of patrols, as client companies are added and removed from the list of locations requiring security officers to patrol.

As technology advances, making it possible for sensors and cameras to be increasingly wireless, the time and money needed for the installation of even larger systems will be reduced. Furthermore, security companies may find themselves needing to innovate a completely new portfolio of mobile products and services, in order to provide their customers a variety of services where, and when they are needed.

7 BIBLIOGRAPHY

Greengard, S. 2015. The Internet of Things. Massachusetts: Massachusetts Institute of Technology.

Behmann, F & Wu, K. 2015. Collaborative Internet of Things for Future Smart Connected Life and Business. West Sussex: John Wiley & Sons Ltd.

Morrish J., Puhlmann F., Slama D & Bhatnagar R. 2016. Enterprise IoT: Strategies & Best Practices for Connected Products & Services. United States of America: O'Reilly Media.

Duroc Y & Andia Vera G 2014 Towards Autonomous Wireless Sensors: RFID and Energy Harvesting Solutions. In Book S. C. Mukhopadhyay (Edit.)Internet of Things Challenges and Opportunities. London: Springer, 233 – 253.

Axis Communications 2017. Facial recognition. Date of retrieval 30.5.2017.

Axis Communications 2017. Facial recognition. Technical document. (no maker). Date of retrieval 30.5.2017.

Axis Communications 2017. People counting. Date of retrieval 30.5.2017.

Axis Communications 2017. 3D People counter. Date of retrieval 30.5.2017.

Axis Communications 2017.Axis M3007-PV Network Camera. Date of retrieval 30.5.2017.

Axis Communications 2017.Panoramic Cameras. Technical document. (no maker). Date of retrieval 30.5.2017.

WorldEyeCam 2012. GeoVision Fisheye IP Camera Retail Store Demo GV-FE520, GV-FE420, GV-FE110. Video. Date of retrieval 30.5.2017.

Schneider Electric 2016. Esmi Access v16.1 January 2016 release. Technical document. (no maker). Date of retrieval 30.5.2017.

Schneider Electric 2015. Esmi Integration Agent. Technical document. (no maker). Date of retrieval 30.5.2017.

Schneider Electric 2013. Esgraf 5.1 Graphical User Interface and Configuration Server. Technical document. (no maker). Date of retrieval 30.5.2017.

iLOQ Oy 2017. iLOQ D10S.500, D10S.510, D10S.500A, D10S.510A Europrofile Half-Cylinders. Technical document. (no maker). Date of retrieval 30.5.2017.

iLOQ Oy 2017. iLOQ P10S.10 Programming Device. Technical document. (no maker). Date of retrieval 30.5.2017.

iLOQ Oy 2017. iLOQ Key K10S.3 (K10S.5, K10S.6, K10S.7). Technical document. (no maker). Date of retrieval 30.5.2017.

iLOQOy 2010. iLOQ – The Key to Security. Video. Date of retrieval 30.5.2017.