MINISTRY OF EDUCATION OF THE AZERBAIJAN REPUBLIC

KHAZAR UNIVERSITY

SCHOOL OF ENGINEERING AND APPLIED SCINECES

Major :060631-Computer Engineering

MASTER THESIS

Title: Study of Security Protocols in Internet of Things

Master Student: Samir Amanov

Supervisor: PhD Mahammad Sharifov

Baku-2017

Table of Contents

Abstract

The Internet of Things is inter-connection of humans, physical devices, buildings, vehicles and many items around us which collects data and exchange it with the help of electronics, software, sensors, and actuators over the network. Main purpose of IoT is to allow all of these objects to be sensed and controlled remotely. IoT aspires to make connection between anyone and anything, anytime and anywhere over the world. Analysts and experts considering that IoT will consist of more than 50 billion devices connected over the network by 2020. IoT devices could be called smart devices. Also from the definition of smart devices we can prove it, a smart device is an electronic device, generally connected to other devices or networks via different wireless protocols.

As it is discussed above, IoT devices are connected over network and exchanging with data. Data security is one of the main goals in today world and network security is one of the important concepts in data security as the data transfered over the network should be made secure to prevent data loss and to prevent from someone who wants to read or change the data. IoT security involves securing the data and uploading the data to the cloud .There are typical security goals, Confidentiality, Integrity, Availability, Authentication, which are also applied to IoT.

Security protocols apply cryptographic methods to ensure protection of data. Generally used with communication protocols to provide secure delivery of data between two parties. To send data to the cloud first it must be encrypted. In this topic we will discuss how to apply Advanced Encryption Standard (AES) algorithm and RSA algorithm in Internet of Things to encrypt data which will be sent over the unsecure network.

1. Introduction

Internet of Things is the technology about which only in 1990's scientists started to talk, and now it is used in many fields, but after few years may be 10-15years experts expect that Internet of Things will be used in every part of our life, there will be more than 50 billion IoT connected devices by 2020. In my thesis, main goal is the study of security protocols in Internet of Things. However, to study security protocols first we need to understand IoT and its security problems.

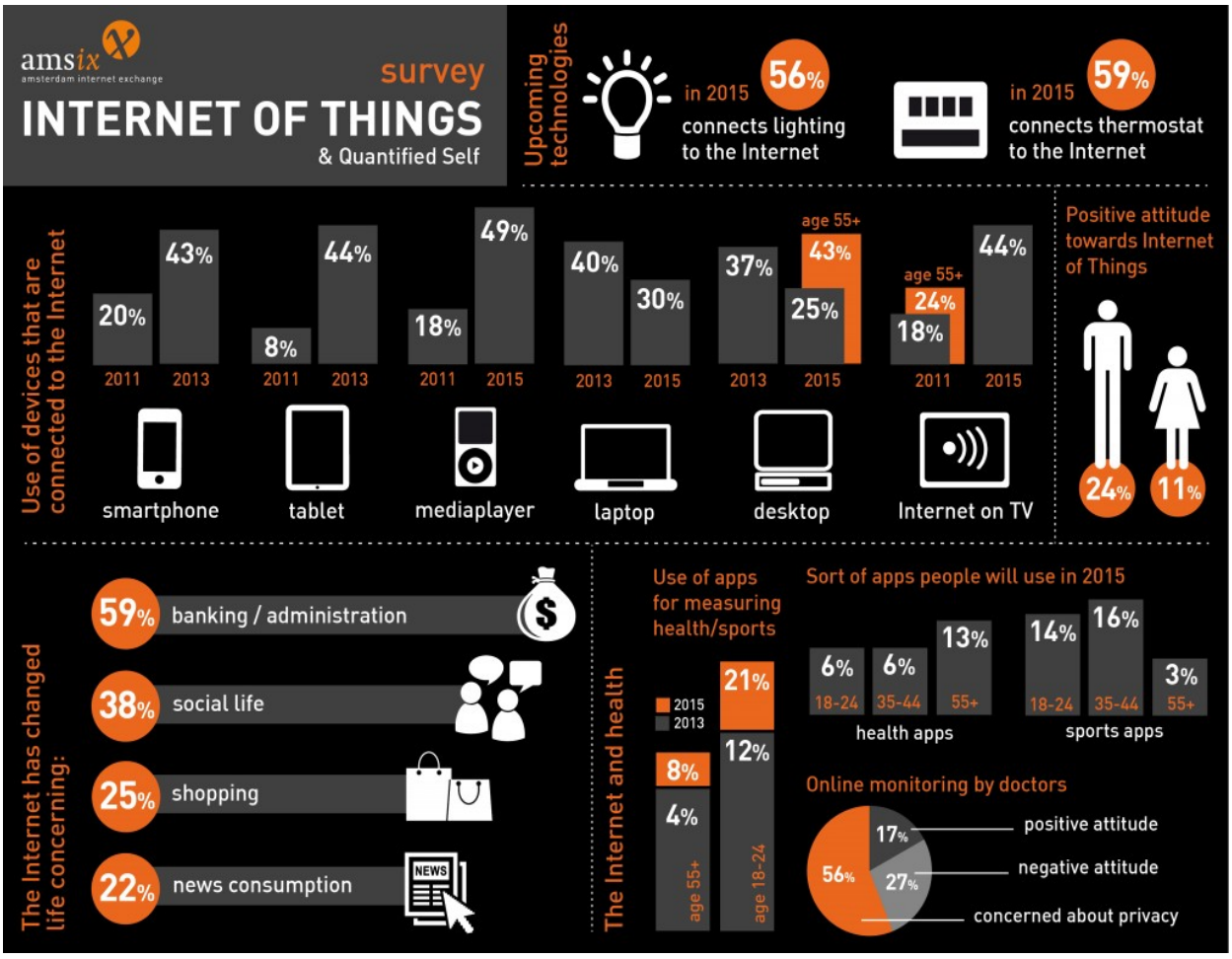


Image 1-1

1.1 History of IoT

Someday, anything that cannot be contacted over the network will seem morally obsolete to the same extent as a wooden wheel with an iron rim compared to the wheel of a modern car. Of course, both are round, but the functionality and complexity are qualitatively different. Things of the new generation (smart things) will not only be "smart", but also integrated into the network - Internet of things (Internet of Things, IoT). How will the changing of the world of things affect our life and how will the world look like in general under the influence of the forthcoming metamorphosis of the things around us in 15-20 years, no one will say for sure, but definitely one can say - the shocks will be no less than those caused by the current Internet or cellular Communication. Therefore, right now, in good time, the IoT becomes a subject of wide, including speculative, discussion.

Offering the term Internet of Things in 1999, the founder of the Auto-ID Center at the Massachusetts Institute of Technology, Kevin Ashton clearly did not anticipate the current turn of events. Over the years, the idea of IoT has significantly expanded and deepened - thirteen years ago the scale of the coming changes seemed much more modest. Now, IoT is not limited to communicating with things equipped with RFID tags, but is considered in the context of combining such modern concepts as pervasive computer systems and intelligent environments (Pervasive Computing, Ubiquitous Computing, Ambient Intelligence). Convergence creates the conditions for a new phenomenon - the Internet of the future, which includes Internet (Internet of Media, IoP) Internet media (Internet of Media, IoM), Internet services (Internet of Services, IoS) and Internet of things (Internet of Things, IoT). Let's try from three points of view to understand what IoT is.

Many great inventions of humanity require tens and even hundreds of years to move from simple in form representations to complex systems. About a hundred years it took an aviation message on the way from the simplest biplanes, sitting on a grass field, to modern air transport complexes. From the creation of prerequisites to the massive introduction of Internet people took almost a quarter of a century, but it seems that for IoT for the same it will take significantly less time. The understanding of what the Internet of things is, ripens quickly-until recently a traditional example of IoT' s potential was a refrigerator connected to the network, but it is already clear: IoT will be a fundamentally new form of organizing the space surrounding a person with consequences comparable to the invention of electricity or atomic energy.

The US National Intelligence Council, which coordinates intelligence efforts in specific geographic regions and industrial sectors, published Disruptive Civil Technologies in 2008, where IoT is named among the six civilian technologies with the greatest explosive power. According to the authors of the report, by 2025 all the objects surrounding us can become IoT nodes.

In 1999, Ashton wrote in the RFID journal: "If we had computers that knew everything there was to know about things - using data they gathered without any help from us - we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world without the limitations of human-entered data." (3)

1.2 General understanding.

There are many several definitions to Internet of Things, if to explain with simple words, Internet of Things generally refers to scenarios where network connectivity and computing capability is used by some devices to calculate and transfer any data with minimal human intervention. Any stand-alone internet-connected device that can be monitored and controlled remote is the IoT device. The word “Things” in IoT can refer to a variety of devices, for example, heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring. The physical objects that are being connected will possess one or more sensors. Each sensor will monitor a specific condition such as location, vibration, motion and temperature. In IoT, these sensors will connect to each other and to systems that can understand or present information from the sensor’s data feeds. These sensors will provide new information to a company’s systems and to people. (29)

Nowadays also it is widely using in our daily life, there are some uses of IoT in daily life: smart door locks, smart bluetooth trackers, smart bike locks, home retrofits, amazon dash buttons, smoke detectors and etc. One of the better-known examples for nowadays using is the Nest thermostat, this Wi-Fi-connected thermostat allows people to remotely adjust the temperature via mobile devices and also learns user’s behavioral patterns to create a temperature-setting schedule.

1.3Why IoT is interesting?

The Internet has as of now brought a huge number of individuals together and made associations that were at no other time conceivable - yet this is recently the start. The Internet of Things (IoT) is coming, and life as we probably am aware it will be changed.

IoT will associate basically every question the Internet, preparing everything from furniture and ways to sustenance and toiletries with sensors to gauge and send information to the cloud. At the end of the day, everything will be "savvy. The ramifications of IoT are tremendous: The whole planet will turn into a bound together, cerebrum like framework. It sounds like a distant, cutting edge idea, yet IoT is inescapable, and business people ought to be energized. Here's the reason:

1. Everything will be measured.

IoT implies that everything from family unit apparatuses, to development hardware, to vehicles and structures will transmit information and speak with different questions or individuals. That implies everything will have the capacity to be measured and followed constantly. Cloud-based applications and devices will have the capacity to break down and make an interpretation of that information into helpful data. This information can fuel better choices and help grow better results. Enormous information has officially made waves in about each industry, demonstrating the estimation of data and investigation. Envision the potential outcomes if about each question utilized as a part of a day transmitted information that could then be intelligently broke down progressively. (4)

2. Metrics will be used in real time.

IoT makes monstrous measures of information that can be investigated and used to settle on better choices. That is incredible - however it's much more energizing than that. This information can be broke down and utilized as a part of ongoing. That implies information is gathered and in a split second put to use to make upgrades. With IoT, data is transformed vigorously at an exceptional speed. Not exclusively will innovation react to information and changes immediately, however it will have the capacity to be utilized to foresee issues and take activities to counteract them. Steady checking can distinguish real issues and alleviate them before they happen.

3. Actionable data will be shared.

Every one of the information that IoT conveys won't exist in a vacuum - it will be shared among colleagues, partners and different gatherings. For instance, consider how wearable tech enables people to gather wellbeing information and offer it with specialists and suppliers, to enhance mind. At the point when this sort of innovation is connected in different businesses, the effect will be tremendous. Checking the viability of techniques, the aftereffects of crusades and the productivity of frameworks winds up plainly less demanding and more significant when more individuals are on the up and up. The capacity to interface and offer information has the likelihood to unite different divisions - like bookkeeping and HR - to settle on choices everybody can concur on.

4. Industries will become interconnected.

The more correspondence among machines - the more associated they are - the more associated everybody will be to each other. Information won't be siloed into one specific industry. It will be utilized crosswise over organizations and ventures, energizing advancement. For instance, information from keen autos can enhance activity, which can create and enhance savvy urban areas, which can make vitality utilize more effective, et cetera. The potential outcomes will

be unfathomable when machines, businesses and individuals can interface and motivate changes. For business visionaries, IoT implies new open doors for joint effort, profitable associations and outside bits of knowledge to improve their business. (4)

1.3.1 A few interesting facts from the history:

Let's see what we had interesting in history was connected with the Internet of things. Of course, there are a lot of facts: the creation of the Internet network itself, the creation of the first page in the network, etc., all probably will not be listed, so I will write the most interesting, as it seems to me, the closest things to the Internet directly.

- In 1926, Nikola Tesla, in an interview for Collier's magazine, said that in the future the radio will be transformed into a "big brain", all things will become part of a single whole, and the tools that make this possible will easily fit in your pocket.
- In 1990, a graduate of MIT, one of the fathers of the TCP / IP protocol, John Romki created the world's first Internet-thing. He connected his toaster to the net.
- The term "Internet of Things" was proposed by Kevin Ashton in 1999. In the same year, the Center for Automatic Identification (Auto-ID Center), engaged in radio frequency identification (RFID) and sensory technologies, was created, thanks to which this concept was widely adopted.
- In 2008-2009 there was a transition from the "Internet of people" to the "Internet of things", i.e. The number of items connected to the network exceeded the number of people.

1.4Background for the Internet of Things

The communication is the most imoprtant part of IoT, because to interconnect different devices they must be able to communicate. There are different properties of IoT devices, which can be used but all of them are not required everytime, such as storing, sensing, capturing, manoeuvring, processing and etc. However, without communication ability devices could not be called an IoT device. This communication can be performed in several ways, for example, via gateway, over some different networks, or may be directly. Figure 1.1 shows an overview of communication in Internet of Things.

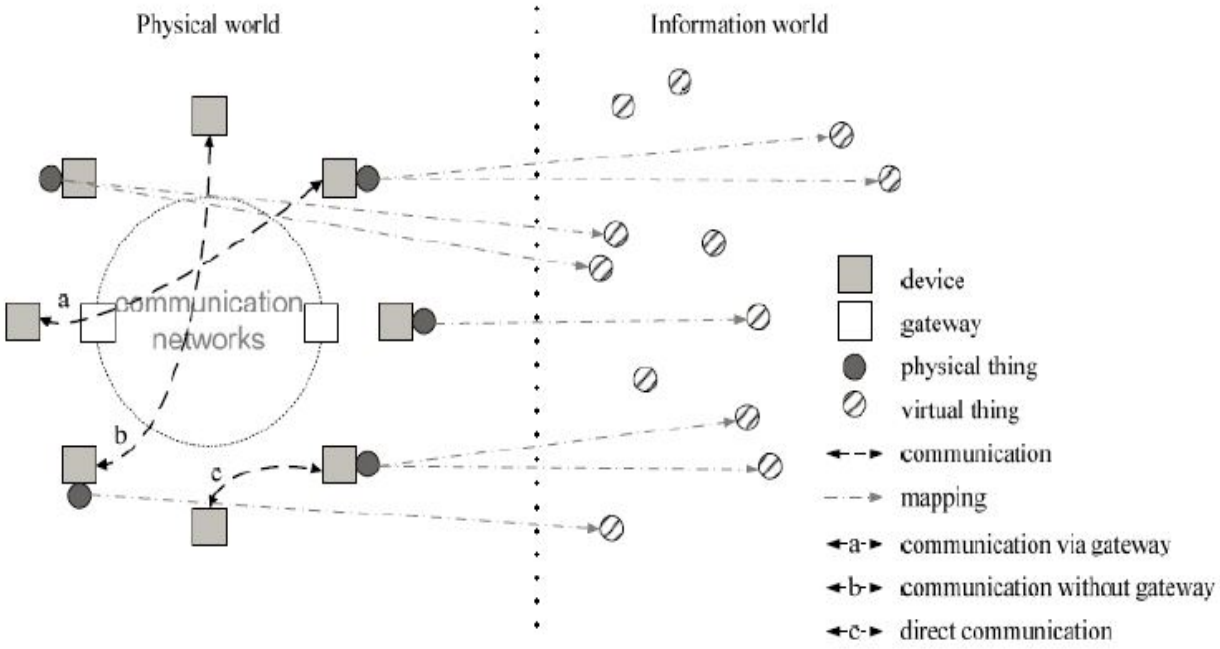


Figure 1-1

1.4.1 The Difference between IoT devices and Standard Computers.

The term standard computers refer to laptops, desktops, servers and other computers which we use for daily works. To understand IoT devices deeply, below is discussed main difference between IoT device and Standard Computers. Shortly we can say computers are general purpose devices but IoT devices are specific purpose devices. Generally, these devices not doing computations and not running some codes, because they have specific purposes, for example to collect some data and send to somewhere, but computers are running codes and make computations to give some decisions. Why computers not used as IoT device? Let's give an example, you can listen to music on your laptop but it is better to listen in music player, because a music player a device which has purpose only for listening to a music, it is cheaper, uses less power, more suitable or generally we can say it is more efficient for specific case. Modern machines and mechanisms can interact with each other (Machine-to-Machine, M2M), with the infrastructure of the environment (Machine-to-Infrastructure, M2I) and with nature (Machine-to-Nature, M2N). Inter-machine interaction is sometimes defined as a set of technologies that allow machines to exchange information with each other or transmit it unilaterally. However, machines can only exchange data, but not information, and this is important for understanding the nature of the interaction. In a number of works, M2M is identified with IoT, which is completely wrong, because today we understand the Internet extensively, not only as a way of transferring data between network nodes using certain protocols and technologies. On the Internet, we include services, and for many, if not for most users, there is no distinction between the World Wide Web and the Internet, the main thing is the possibility of human interaction with the network, with the services of the network, hence the Internet

of People. The same is the case with IoT - here under the Internet is understood the possibility of interaction between machines, and it is not at all necessary that some protocols are used for this. In other words, M2M is the physical basis of the Internet of things, while protocols are used or not used, it does not matter. Below table 1.1 shows some fundamental characteristics of an Internet of Thing device.

Characteristic	General Description
Interconnectivity	Everything should be connected to the global information and communication infrastructure
Things-Related Devices	Provides things-related services within the constraints of things, such as privacy and semantic consistency between physical and virtual thing.
Heterogeneity	Devices within IoT have different hardware and use different networks but they can still interact with other devices through different networks.
Dynamic Changes	The state of a device can change dynamically, thus the number of devices can vary.
Enormous Scale	The number of devices operating and communicating will be larger than the number of devices in the current Internet. Most of this communication will be device to device instead of human to device.

Table 1.1

1.4.2 The IoT reference model

The ITU-T has defined a reference model for Internet of Things. IoT reference model consists of four layers: application layer, service support and application support layer, network layer and device layer. Each one of these layers also includes management and security capabilities. As shown in the figure 1.2 these capabilities have both generic and specific capabilities that can cut across multiple layers.

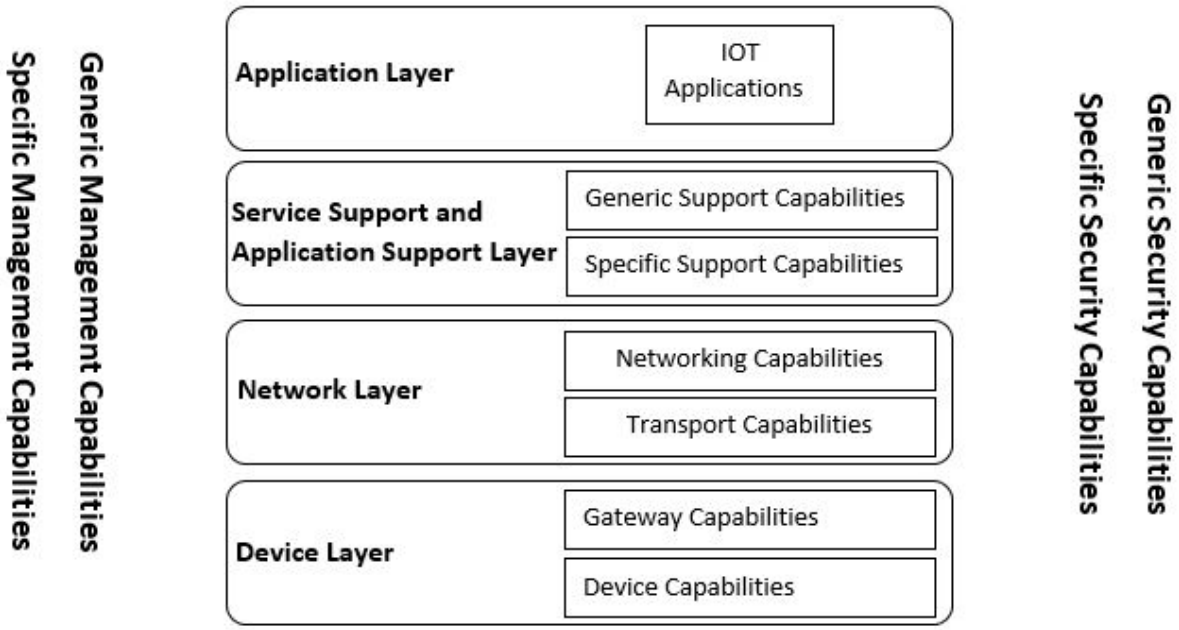


Figure 1.2 ITU-T reference model for IoT. Taken from Recommendation ITU-T Y.2060

Device Layer: The IoT Reference Model starts with Level 1: physical devices and controllers that might control multiple devices. These are the “things” in the IoT, and they include a wide range of endpoint devices that send and receive information. Today, the list of devices is already extensive. It will become almost unlimited as more equipment is added to the IoT over time. Devices are

diverse, and there are no rules about size, location, form factor, or origin. Some devices will be the size of a silicon chip. Some will be as large as vehicles. The IoT must support the entire range. Dozens or hundreds of equipment manufacturers will produce IoT devices. To simplify compatibility and support manufacturability, the IoT Reference Model generally describes the level of processing needed from Level 1 devices. (5)

Network Layer: Communications and connectivity are concentrated in one level—Level 2. The most important function of Level 2 is reliable, timely information transmission. This includes transmissions:

- Between devices (Level 1) and the network
- Across networks (east-west)
- Between the network (Level 2) and low-level information processing occurring at Level 3

Universal information correspondence networks need various functions, similarly as prove by those worldwide association for Institutionalization (ISO) 7-layer reference model. However, a finish IoT framework holds huge numbers levels furthermore of the correspondences organize. You quit offering on that one objective of the IoT reference model is to interchanges furthermore transforming to a chance to be executed Eventually Tom's perusing existing networks. The IoT reference model doesn't oblige alternately demonstrate creation of a separate network—it depends with respect to existing networks. However, a portion legacy units aren’t IP-enabled, which will oblige presenting correspondence gateways. Different gadgets will oblige proprietary controllers on serve the correspondence work. However, in time, institutionalization will expand. Likewise level 1 gadgets proliferate, those routes on which they cooperation with level 2 connectivity supplies might transform. In any case of

the details, level 1 units speak through the IoT framework Eventually Tom's perusing cooperating with level 2 connectivity supplies. (5)

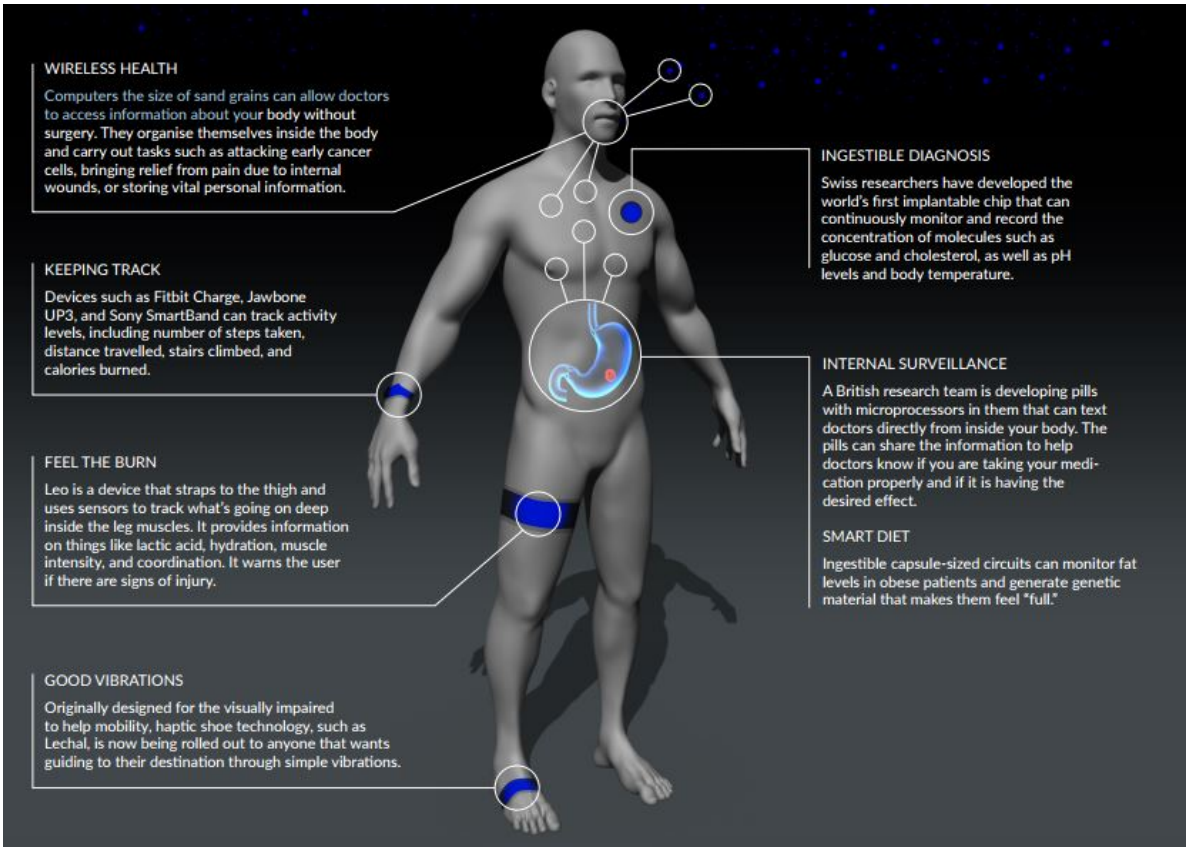
Application Layer: The application layer holds IoT provisions which require specific backing competencies from the underlying layer with capacity. The administration Also provision help layer comprises from claiming nonspecific backing abilities which camwood make utilized by IoT applications, samples about such competencies Might make information transforming alternately stockpiling. The particular help abilities would the individuals other than those nonspecific competencies which are required should make backing to differentiated requisitions.

1.5Future of the Internet of Things

There are many discussions about the future of Internet of Things, everyone expects different but may be some impossible things from IoT. But when we talk about future one of the first things people think, is it possible to make person to live more, or is it possible to control our internal organs? Some professors argue that in the future with the help of IoT we will be able to control our health. Professor of Hebrew University in Jerusalem Yuval Noah Harari considers the fusion of man and machine "the greatest evolution in the history of biology."(6)

But what role in this evolution can the Internet of things play with all its devices (which are becoming more compact and close to us)?

Meet: an electronic person (E-MAN) ... **Image 1-2**



- WIRELESS HEALTH: Computers the size of sand grains can allow doctors to access information about your body without surgery. They organize themselves inside the body and carry out tasks such as attacking early cancer cells, bringing relief from pain due to internal wounds, or storing vital personal information.
- KEEPING TRACK: Devices such as Fitbit Charge, Jawbone UP3, and Sony Smart Band can track activity levels, including number of steps taken, distance travelled, and stairs climbed, and calories burned.
- FEEL THE BURN: Leo is a device that straps to the thigh and uses sensors to track what's going on deep inside the leg muscles. It provides information on things like lactic acid, hydration, muscle intensity, and coordination. It warns the user if there are signs of injury.

- GOOD VIBRATIONS: Originally designed for the visually impaired to help mobility, haptic shoe technology, such as Lechal, is now being rolled out to anyone that wants to guide to their destination through simple vibrations.
- INGESTIBLE DIAGNOSIS: Swiss researchers have developed the world's first implantable chip that can continuously monitor and record the concentration of molecules such as glucose and cholesterol, as well as pH levels and body temperature.
- INTERNAL SURVEILLANCE: A British research team is developing pills with microprocessors in them that can text doctors directly from inside your body. The pills can share the information to help doctors know if you are taking your medication properly and if it is having the desired effect.
- SMART DIET: Ingestible capsule-sized circuits can monitor fat levels in obese patients and generate genetic material that makes them feel "full."

1.6Problem Definition

Internet of things (IoT) transforms everyday physical objects surrounding us into an ecosystem of data that quickly changes our lifestyle. Refrigerators and cars, parking and houses - all these objects are already connected to the Internet of things, and their number is growing every day. Home systems will soon be able to monitor almost every step, for example closing and opening the front door or automatically ordering the products when the refrigerator is empty.
A separate question is whether we want to move to this level of automation and whether are we ready for this. But a little time will pass, and these technologies will become the norm, and then there will be other innovations that will completely change our lives.

1.6.1 Can we trust our protection to the Internet of things?

Over the next ten years the Internet can guide the Internet of things to unite 200 billion objects - and this is not only cars and household appliances, but also any devices with embedded chips or sensors - including people. These objects, united by the common notion of "Internet of Things", are designed to simplify our lives and monitor our health, but can we trust them with our own security? Today is Monday, October 1, 2025, at 6 am. The touch electronic bracelet on your wrist receives data that you wake up and sends a signal to the coffee machine that starts to brew coffee. You delay the preparation of coffee and go for a run. While you are running along the sidewalk, the sensors in your headphones record an irregular heartbeat. The device sends the ECG results to your cardiologist. The doctor sees that the arrhythmia is only an inoffensive ectopic systole, and decides not to take any action. Returning home, you drink honestly earned coffee and send an empty cup to the dishwasher. The dishwasher is fully loaded, so it turns on and starts to wash the dishes. The built-in sensor determines that the device needs scheduled maintenance. Automatically creates an application for the service specialist, the date of his visit is marked in your diary, and you confirm it.

Twenty years ago, dishwashers were one of the main causes of fires, but these times have long passed. With the advent of the Internet of things (IoT) - a collection of devices connected to each other via the Internet - life has become much safer. By 2025, the Internet (and with it automatically driven cars, and clever capsules for internal diagnostics) will stand guard over our health and safety.

But is it reasonable to shift responsibility for actions we previously performed ourselves (for example, driving or taking medicines) to devices?

1.6.2 Dark side of IoT.

A healthy lifestyle and security is fine, but as we know, any computer can be hacked. When cybercriminals manage to bypass antivirus programs and infiltrate our computers or mobile devices, they can turn our lives into real chaos: gain access to bank accounts, steal data and rob other people. Nevertheless, no one died of this yet. But what happens if, in the future, hackers break into the system of drug administration built into the human body and inject him with a lethal dose? What will happen if they intercept the steering wheel of an automatically controlled car in which you rush along the highway? What will happen if they change the permissible level of radiation on the scanner?

Pedometers, computerized insulin dispensers, defibrillators, radio babysitters, web cameras, sports bracelets and smart toilets - these devices have already been hacked. In most cases, these attacks were carried out for public demonstration of the skill of hackers, and not for committing any crime. But this proves once again that such attacks are possible.

A study conducted by HP showed that three-quarters of IoT devices are vulnerable to hacker attacks. As for home IoT systems, where a lot of devices exchange data and make decisions about house management, it is enough to find one weak link and the entire system will be compromised.

And one more problem which was noted by Olivier Ribet vice-president of the "High Technologies" in Dassault Systems: “Currently all objects of the Internet of things [IoT] ask their owners a direct question "Do I need to perform this or that action?" However, more and more people are inclined to believe that devices should not ask any questions [let them make decisions for us].” (6)

1.7 Structure of this Thesis

Second Chapter gives wide background information about Information Security and security measures in Internet of Things. Third Chapter is general informationabout cryptography, encryption/decryption algorithms, why they are so important for Internet of Things and etc. In fourth Chapter we will analyze real security issues in Internet of Things, and some encryption algorithms to with which data should be send over untrusted networks.

2. Background

2.1What is information security?

Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats. Threats to information and information systems may be categorized and a corresponding security goal may be defined for each category of threats. A set of security goals, identified because of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment. (30) The currently relevant set of security goals may include: confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability. (7)

Information security, as well as information protection, is an integrated task aimed at ensuring security implemented by the security system. The problem of information protection is multifaceted and complex and covers many important tasks. The problems of information security are constantly aggravated by the processes of penetration into all spheres of society.

The goal of information security is to provide the three most important security services: confidentiality, integrity and accessibility.

Confidentiality is a guarantee that information can be read and interpreted only by those people and processes that are authorized to do this. Ensuring confidentiality includes procedures and measures to prevent unauthorized users

from disclosing information. Information that can be considered confidential is also called sensitive information. An example is an e-mail message that is protected from reading by anyone other than the recipient.

Integrity is a guarantee that the information remains unchanged, correct and authentic. Ensuring integrity involves preventing and determining the unauthorized creation, modification or deletion of information. An example can be measures to ensure that the mail message has not been changed in transit. (8)

Availability is the guarantee that authorized users can access and work with the information assets, resources and systems that they need, while ensuring the required performance. Accessibility includes measures to maintain the availability of information, despite the potential for interference, including system failure and intentional attempts at breaching availability. An example is access protection and the provision of the capacity of the mail service. (9)

Three main services - CIA - are the foundation of information security. To implement these three basic services, the following services are required: Identification is a service that specifies unique user attributes that allow users to be distinguished from each other, and the ways that users specify their identities to the information system. Identification is closely related to authentication. Authentication is a service by which it is proved that the participants are required, i.e. Evidence of identification is provided. This can be achieved with the help of passwords, smart cards, biometric tokens, etc. In the case of sending a single message, authentication must ensure that the recipient of the message is the one who needs it and the message is received from the claimed source. In the case of establishing a connection, there are two aspects. First, when the connection is initialized, the service must ensure that both parties are required. Secondly, the service must ensure that the connection is not affected in such a

way that a third party can be masked under one of the legal sides after the connection is established.

Accountability is the ability of the system to identify an individual and the actions that he performs. The presence of this service means the ability to associate actions with users. This service is very closely related to the service of failure.

Failure to refuse is a service that ensures the inability of an individual to abandon his actions. For example, if a customer has made an order and there is no service of failure in the system, then the consumer can refuse the fact of purchase. Failure to provide a refund provides ways of proving that a transaction has occurred, whether the transaction is an online order or an email that has been sent or received. To ensure the impossibility of failure, digital signatures are usually used.

Authorization - the rights and permissions granted to the individual (or process) that provide access to the resource. After the user is authenticated, the authorization determines which rights of access to which resources the user has.

Privacy protection - the level of confidentiality that is provided to the user by the system. This is often an important security component. The protection of private information is not only necessary to ensure the confidentiality of the organization's data, but is also necessary to protect the private information that will be used by the operator.

If at least one of these services does not work, then we can talk about the violation of the entire original triad of the CIA.

To implement security services, a so-called "defense in depth" must be created. For this, the followings should be done:

1- It is necessary to ensure the performance of all security services.

2- A risk analysis must be performed.

3- It is necessary to implement authentication and Identity management.
4- You must implement authorization for access to resources.
5- Accountability is essential.
6- It is necessary to guarantee the availability of all services of the system.
7- Configuration management is required.
8- Incident management is necessary.

2.1.1Guaranteed performance

Ensuring the execution of security services perform the following:

- Develop an organizational security policy.
- Review existing regulatory requirements and acts.
- Provide training for staff responsible for information security.

Guaranteeing performance, along with risk analysis, is one of the most important components that ensure the creation of defense in depth. This is the basis on which many other components are built. The assessment of performance assurance can largely determine the entire state and level of maturity of a reliable infrastructure.

The organizational policy contains guidelines for users and administrators. This policy should be clear, clear and understood not only by technical specialists. The policy should cover not only the current conditions, but also determine what and how should be done if an attack occurred.

2.1.2Risk analysis

When analyzing risks, the first thing to do is to analyze the information assets that must be protected.

Any discussion of risk involves the identification and evaluation of information assets. The asset is everything that is important for the organization. A critical asset is an asset that is vitally important for the functioning of the organization, its reputation and further development.

Risk analysis is the process of identifying risks for information assets and deciding which risks are acceptable and which are not. Risk analysis includes:

- Identification and prioritization of information assets.
- Identification and categorization of threats to these assets.
- Prioritization of risks, i.e. Determination of what risks are acceptable, what should be reduced, and what to avoid.
- Reducing risks with various security services.

A threat is any event that may have undesirable consequences for the organization. Examples of threats are:

- The possibility of disclosure, modification, destruction or inability to use information assets.
- Penetration or any malfunction of the information system.

Examples can be:

  - Viruses, worms, Trojan horses.
  - DoS attacks.
  - View network traffic.
  - Data theft.
- Loss of information assets because of having a single point of failure. Examples can be:
  - Critical data for which there is no backup.
  - The only critical place in the network infrastructure (for example, the basic router).
  - Improper access control to keys that are used to encrypt critical data.

Possible risk management strategies:

1. Take the risk. In this case, the organization should have a full understanding of the potential threats and vulnerabilities for information assets. In this case, the organization believes that the risk is not sufficient to defend against it.
2. Reduce the risk.
3. Pass the risk. The organization decides to enter into an agreement with a third party to reduce the risk.
4. Avoid the risk.

2.1.3Authentication and Identity Management

Identification of the user enables the computer system to distinguish one user from another and to provide high accuracy of access control to services and resources. Identifications can be implemented in various ways, such as passwords, including one-time, digital certificates, biometric parameters. There are various ways of storing identities, such as databases, LDAP, smart cards. The system should be able to verify the validity (authenticity) of the provided identification. The service that solves this problem is called authentication.
The term entity is often better suited for identifying the bearer of identification than the term user, since the participants in the authentication process can be not only users, but also programs and hardware devices, for example, web servers or routers.
Different security requirements require different methods of identification and authentication. In many cases, it is enough to provide security with a username and password. In some cases, you need to use stronger authentication methods.

2.1.4Reporting

Reporting is an opportunity to know who did what in the system and the network. This includes:

- Creation and audit of system logs.
- Monitoring of systems and network traffic.
- Intrusion detection.

Providing reporting allows you to know what is happening in computer systems or networks. This can be implemented in many ways, but the most commonly used are:

- Configure the system in such a way that interesting activities are recorded, such as attempts to log users into the system or network (successful or not successful).
- Inspect the use of the network to determine the types of network traffic and its volume.
- Automatic monitoring of systems to determine service outages.
- Using intrusion detection systems to alert administrators of unwanted activity in computer systems or networks.

2.1.5Cryptographic security mechanisms

Let’s list the main cryptographic mechanisms of security:

Symmetric encryption algorithms, are encryption algorithms in which the same key is used for encryption and decryption.

Algorithms of asymmetric encryption, are encryption algorithms in which two different keys are used for encryption and decryption, called open and private keys, and knowing the public key, it is difficult to determine the closed one.

Hash functions, are functions whose input value is a message of arbitrary length, and the output value is a fixed length message. Hash functions have several properties that allow you to determine the change in the input message with a high degree of probability.

2.2. Internet of Things and Information Security

IoT is relatively a modern concept that is why it has many security problems. We need to define IoT security goals. To do this before it is important to understand how it is working. Let's analyze IoT structure with example, consider that a sensor at our home turns on or off gas, we send message from our mobile phone and sensor turns on gas, or another example, consider a sensor in some secret are collects data about weather conditions and sends this data to cloud and some people check this data every day from cloud. From this example, it understandable that there can be attacks to cloud where data is saved to read or modify this data, or can be network attacks which will send to gas sensor false signal, which may be will start a fire in our home. The most important security objective of IoT is to protect collected data, since the collected data may include many sensitive and secret information. So, the security of any IoT system needs to be strong and protectable to data-related attacks and provide trust, data security and privacy.

2.2.1Real life IoT security vulnerability examples

Victor Alyushin and Vladimir Krylov from company Kaspersky made investigation about security issues of IoT. The idea came from their colleague, who one day at his home looked around him and thought that all devices which

are connected to the network are danger for him and his family. For exmperiment they choose some devices like, chromecast, IP-camera controlled from a smartphone, coffee machine controlled from a smartphone, Home security system, also managed from a smartphone. (10)

- **IP Camera**

Risk: An attacker gets access to email addresses of all users who have had technical problems using the camera.

The IP camera which was examined was claimed by the manufacturer as a "baby monitor" - a device for tracking a baby. The camera is installed in the nursery, a special application is installed on the smartphone, and the camera connects to the Wi-Fi network, connects to the application, and is ready: you can see your baby at any time, wherever you are.

Someone might ask: why would someone need to hack into a baby monitor? It turns out that several cases of hacking a children's monitor have been recorded. Two such cases were back in 2013 and 2015.

(http://www.cbsnews.com/news/baby-monitor-hacked-spies-on-texas-child/)

(http://www.kwch.com/news/local-news/whitewater-woman-says-her-baby-monitor-was-hacked/32427912)

When we explored our camera, two applications were available to the clients to communicate with the camera; both applications contained some security issues. Later we found out from the manufacturer that one of the applications was obsolete, but some camera owners still used it. We found that this legacy application contained data in the "wired" form for accessing the account on Gmail.

```
public static final String EMAIL_FROM = «*****@gmail.com»;
public static final String EMAIL_PASSWORD = «*******»;
public static final String EMAIL_PORT = «465»;
public static final String EMAIL_SMTP_HOST = «smtp.gmail.com»;
public static final String EMAIL_TO;
public static final String EMAIL_TO_MAXIM = «maximidc@gmail.com»;
public static final String EMAIL_TO_PHILIPS = «*****@philips.com»;
public static final String EMAIL_USERNAME = «*****@gmail.com»;
```

Image 2-1

The manufacturer later told us that this email address was used to collect reports on technical problems from camera owners.

The problem in this case is that the reports were sent to this "wired" address from the users' personal mail addresses. Thus, the attacker did not even need to buy a camera; it was enough to download and decompile one of the applications, get access to a "technical" mailbox that received reports on technical problems, and collect electronic addresses of all camera users who had technical problems. Is the problem great that your address may have become known to a third party because of exploiting this vulnerability? Yes, potentially this can be a problem. Of course, it is unlikely that this vulnerability will attract the attention of cybercriminals in the context of mass gathering of users' personal information, primarily because of the relatively small number of potential victims. Technical problems are rare, at the time of the study the application was obsolete and not very popular. In addition, the baby monitors are a niche product, so the size of the potentially accessible e-mail address database is relatively small.

On the other hand, if you have a baby monitor, then most likely you have a child, and this fact makes you (and, correspondingly, your email address) a much more attractive target if the attacker has specific, well-defined plans Fraud. It will be easier for him to develop social and engineering elements of an attack against such a user.

In other words, this vulnerability does not apply to critical ones, but there is a possibility of its malicious exploitation. However, this is not the only vulnerability that we found in the study of the camera and the application.

- **A coffee machine controlled from a smartphone**

Risk: A password leak for accessing your home wireless network.

A coffee machine, which we randomly selected for analysis, can remotely prepare a cup of coffee exactly at the time you need it. You just need to set the time: when the coffee is ready, the application will send you a push notification. You can also track the application status of the coffee machine through the application - for example, whether the coffee is currently being cooked, whether the machine is ready to weld the coffee, or perhaps it is time to pour the water into the container. In other words, this is a very nice device, which unfortunately gives an attacker the opportunity to steal a password to your local Wi-Fi network.

Before using the device, you need to configure it. This happens in this way: when the device is turned on, it creates an unencrypted access point and listens for UPNP traffic. A smartphone running an application for communicating with a coffee machine is connected to this access point and sends a broadcast UDP request for whether there is a UPNP device on the network. Since our coffee machine is such a device, it responds to the request. This is followed by a brief communication session, during which, among other things, a network ID (SSID)

and a password to the home wireless network are sent from the smartphone to the device.

This is where we discovered the problem. The password is sent in encrypted form, but the encryption key components are sent through an open unprotected channel. Among such components - the Ethernet-address of the espresso machine and some other unique credentials. Using this data, an encryption key is generated on the smartphone. The password to the home network is encrypted with this key using the 128-bit AES algorithm and sent to the Base64 machine. The coffee machine also generates a key from these components, with which the password is decrypted. Then the coffee machine connects to the home wireless network and ceases to be an access point until the RESET button is pressed). From this moment, access to the espresso machine is possible only through a home wireless network. However, it does not matter, since the password is already compromised.

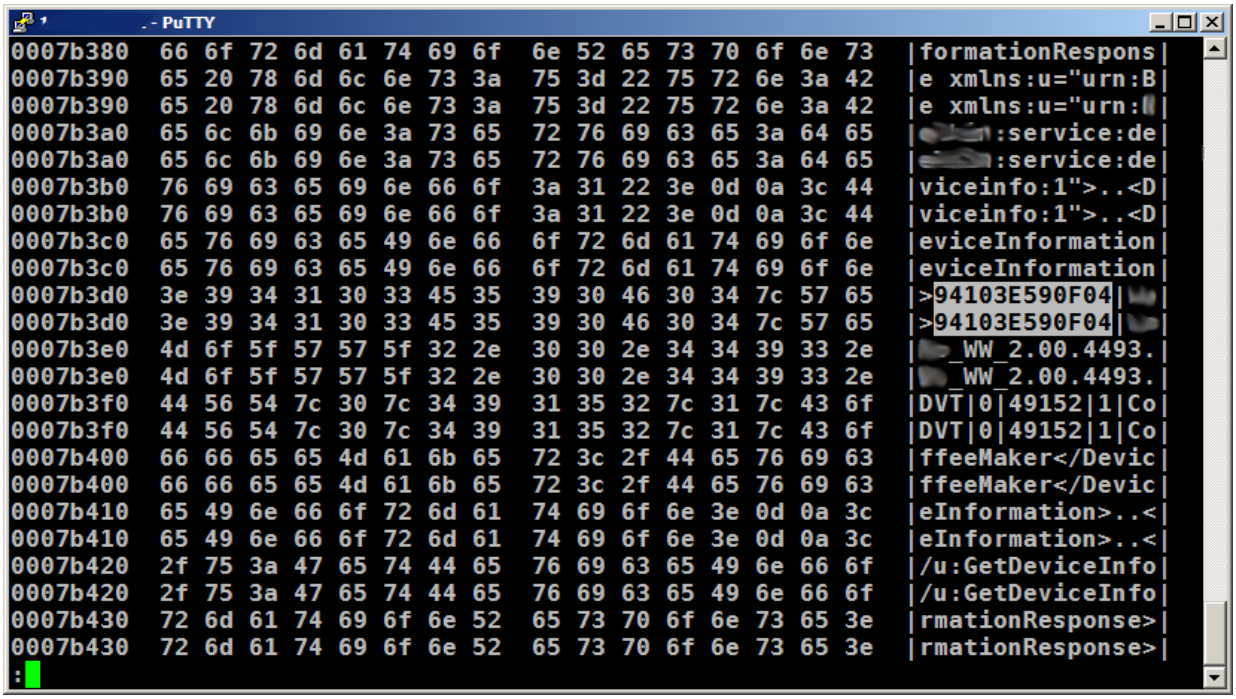


Image 2-2

2.2.2 Security threats associated with the Internet of Things

IOT safety issues consist mainly of and are easily divided into two areas: virtual (see Table 2-1) and physical (see Table 2-2). Physical threats increase as things become increasingly perimetralized. Virtual threats are tightly coupled with threats in any other IT environment and consist primarily of obtaining data and information (an asset) or taking control of the device itself. In addition, the application of the methods used to protect an IoT environment is limited, since many devices are limited when it comes to performance and power.

Since this thesis is mainly concerned with the concept of information security, the starting point of the threat analysis was the object itself, which is information (data). The threat identifier was not identified, because this analysis addresses more general threats, rather than specific ones.

Considering different attack points, it is easier to determine what threats are associated with IoT, and what anti-virus attacks should be eliminated to protect each part of the IoT environment. Three identified attack points: the connection between the objects, the IoT devices themselves, and in the third case, when the gateway is used, the central collection point of several sensors or the controller for several actuators.

Table 2-1

Virtual Threats affecting Information Security in IoT [36]			
Asset	Data & Information		
Point of Attack	Communication	IoT device(s)	Gateway
Threats	Interference (Denial of Service) Signal interception (Man in the middle) (Privacy Concerns)	Intrusion Exploitation (Privacy Concerns)	
Vulnerabilities	Uncontrolled or unprotected traffic flow	Insufficient authentication or authorisation Insecure user interfaces Insecure network services Insecure software/firmware Unprotected data	
Impact/Consequences	Compromised data Data loss Communication loss Inaccessible data Lose control of device	Compromised data Data loss Data corruption Inaccessible data Communication loss Lose control of device	
Information Security concepts affected	Availability Confidentiality Integrity Possession	Availability Confidentiality Integrity Possession Accountability Authenticity	
Countermeasures	Encryption of transport data Keep identification (IP-address) hidden	Reviewed applications, hardened operating systems, detailed traceability Secure environment and routines for development Security analysis and verification by third party The network uses strong encryption and signing Secure routines for physical access, log analysis, administration	

Table 2-2

Physical Threats affecting Information Security in IoT			
Asset	Data & Information		
Point of Attack	Communication	IoT device(s)	Gateway
Threats	Interference (Electromagnetic compatibility)	Power loss Network loss Theft Sensor/device modification/ replacement	
Vulnerability	Wireless communication	Physical access to device Insufficient authentication	
Impact/Consequences	Communication loss Inaccessible data	Communication loss Inaccessible data Data loss Data corruption	
Information Security concepts affected	Availability	Availability Possession Integrity Confidentiality	
Countermeasures	Alternative (wired) network connection	Alternative power source Alternative network connection Move device to inaccessible area Authentication	

2.2.2.1 Communication

There are two types of virtual threats in the message, which can arise, Table 2-1. Interference occurs when a traffic stream (data) intended for reference is somehow broken or eliminated due to other unwanted traffic streams occupying a physical link. A practical example of this - when a denial-of-service attack occurs - is an attempt to make a machine or network resource unavailable, which can be destructive in an IoT environment that requires constant

communication (11). Intervention can also be performed at the physical level, for example, by jamming wireless communication between nodes (12).
The interception of the signal can be performed in several steps in the communication chain, depending on what device or signals the attackers can listen to, for example, sensors, drives, gateways, etc. D. During the actual sending of data, a person in middle attack could perform a secret relay and in some cases, change the relationship between the two parties (13).
Confidentiality issues arise when cybercriminals can interpret personal data because of insufficient authentication, unprotected traffic flows or unsafe network services, both in communication and at the device level (14).

2.2.2.2 IoT-device

When looking at the IoT-device, there are mainly threats in the form of intrusion and exploitation at the virtual level. An invasion is possible when an attacker uses security holes in unsecured user interfaces, software or firmware or network services. There is also the possibility of an intrusion when there is insufficient or nonexistent authentication and authorization to access the system, device or data.
Operation occurs when the user has access to a component (device or gateway) in an IoT environment. This exploitation can be in the form of reading additional information, destroying the data or interfering with the connection of this component or others like it. For example, if an attacker can authenticate against a system, it is likely that he / she will be able to access some of the device's features. That's why access control to restrict user access rights is very important.

Physical threats can affect confidentiality, integrity and availability in cases where an attacker has physical access to an IoT device or gateway. Thanks to the intervention or the replacement of the device everything can be done from reading or modification to falsifying the data. Therefore, limiting physical access and increasing protection against unauthorized access is a very important part of ensuring the security of many IoT environments.

2.2.2.3 Gateway

Things like street lights and household appliances are physically in specific conditions, and, instead of disabling them, hackers can try to extract information from these things. Instead of attacking the device itself, a hacker can be targeted at the infrastructure used to store the organization's data or for data processing. If, on the other hand, the factual data on the Internet of things are distributed, then various objects will be used to create and process information. This means that hackers will need a lot of time and effort to control so many resources. Nevertheless, it was found that the distribution of resources acts as a double-edged sword. If intruders are interested in this or that piece of information, they can be guided by systems that manage specific information located in central entities. Indeed, attackers can use the "guerrilla" strategy, taking control of a small section of the network, and covertly affect the entire system.
Due to the limited resources of the nodes, the distributed organized structure and the dynamically changing network topology, there are many threats, including the possibility of physical capture, because many nodes are fixed and can be easily compromised by physical access. Another threat comes from brute force (brute force) attack, which is especially critical in the case when the size of the node storage and its computing power are severely limited. In addition, the

hardware structure of some nodes is easy and understandable, which makes it possible for an attacker to compromise it. Routed attacks are also possible on the Internet of things, especially in cases where retransmission and data transfer are carried out within the framework of a vulnerable data collection process. Nodes are also vulnerable to capture during a DoS attack because of their ability to process them, while attackers can actively or passively steal confidential information.

2.2.2.4 Physical security of sensors

Physical attacks can damage the sensors of the Internet devices of things or even bring them to a completely inoperative state, which is a clear security risk. For example, an attacker can enter the house where the sensor is located and detect the accompanying electronic and physical signals of other sensors using equipment for detecting radio, heat, magnetic, visual and other electronic signals. The attacker can then determine the location of the sensors based on the properties of the received signals, after which they can be physically disabled, destroyed, or stolen. Physical damage can be accomplished by using heat, physical strength, or disruption of the integrity of the sensor circuit, which makes the sensor non-functioning. In addition, it is easy to launch physical attacks using old technologies because of the vulnerability of sensors, especially small ones. Attacks of this kind are inevitable for sensory networks of the Internet of things. Since an attacker is near the network in an attack of this kind, he can respond to defense mechanisms, unlike remote attacks.

2.3 IPv6 over Low-Power Wireless Personal Area Networks

6LoWPAN (abb. IPv6 over Low Power Wireless Personal Area Networks) is the standard for IPv6 communication over low-power wireless personal networks of the IEEE 802.15.4 standard, as well as the name of the IETF working group that is designing this standard.

The power of the network is determined by the number of nodes involved in it and the ability of protocols to effectively use the inherent capabilities. Networking capabilities are used in many fields of activity - monitoring and management of objects; Collection, transfer and primary processing of data and much more. At the same time, network nodes can have significant differences in computing, communication resources and memory resources.

Especially valuable quality of the network is its ability to integrate different devices with different functions and resources. A decisive role in this play network protocols - a stack of protocols. A striking example of this is the TCP / IP protocol stack, which underlies most of, many of modern networks of various levels, scale and purpose. The largest and most used of them is the Internet, which provides global communications, services, and services. A more important factor is that standards have been developed for processing information and developing applications for TCP / IP networks. Internet network already includes several billion nodes and is on the verge of transition to a new version of the IP - IPv6 protocol, which provides a more flexible addressing scheme and a decent amount of address space.

The widespread introduction of automation and automation systems, despite the apparent redundancy, has shown its effectiveness. This is based on branched networks of sensors (sensors), controllable nodes and mechanisms. Even for a small automated object, their number can exceed several hundred. Moreover,

modern automation tasks require transparent inter-machine interaction (M2M interaction), developed services, interaction with databases and even the user interface. In this vein, using the Internet infrastructure to build a distributed, scalable system looks very tempting.

Main applications:

- Intellectual accounting systems;
- Management of street lighting;
- Industrial automation;
- Logistics systems, tracking of goods or inventory objects;
- Commercial security systems, access control systems;
- Some military applications.

The architecture of 6LoWPAN networks differs somewhat from the traditional architectures of IP networks (the availability of specialized switching equipment, routers, and media converters) and the existing architectures of wireless data collection networks. The closest thing to it is the architecture of Wi-Fi networks, although there are several differences from it.

First of all, 6LoWPAN are subnets of IPv6 networks, i.e. they can interact with other networks and nodes of the IP network, but are not transit for its network traffic. 6LoWPAN networks consist of nodes that can also act as routers, and there may be one or more edge routers on the network. Participation in routing is not a requirement for a network node, and it can play a role similar to the role of the end device in ZigBee networks or a device with limited functionality for 802.15.4 networks, in the 6LoWPAN terminology "host". A node capable of routing within a 6LoWPAN network is called a router or router. The boundary router is responsible for the interaction of the 6LoWPAN subnet with the IPv6 network, participates in the initialization and routing procedure on the 6LoWPAN subnet, performs compression / decompression of the IPv6 headers

when communicating with the external network, in case of connection to the network, IPv4 can act as the IPv6 <> IPv4 gateway. The subnet nodes share the 64-bit IPv6 prefix, which is also part of the boundary router's network address. For addressing within the network, you can use the remaining sixty-four bits (the MAC address of the network interface) or use address compression and a truncated 16-bit addressing scheme (the lowest two bytes of the MAC address). It is assumed that the network address directly includes the address of the network interface, this eliminates the need for a network address resolution protocol (ARP).

There are three types of 6LoWPAN networks:

1- ad-hoc

2- a simple 6LoWPAN-network

3- an extended 6LoWPAN-network

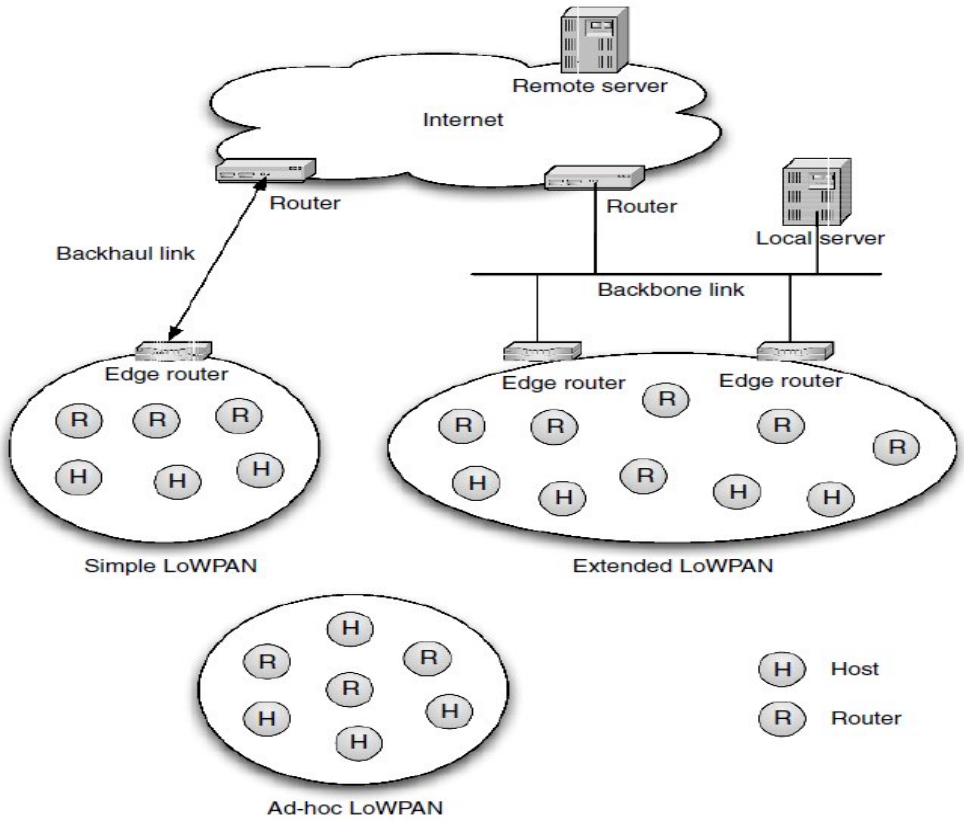


Image 2-3

Ad-hoc-network does not have a connection to an external IP-network, it does not have a boundary router. It is a self-organizing network that uses the 6loWPAN protocol stack to organize work and transfer data between nodes.
A simple 6LoWPAN network is connected to another IP network using a single edge router. A boundary router can be connected to an external IP network directly (a point-to-point connection, for example, a GPRS / 3G modem) or it can be part of a campus network (for example, an organization's network).
The extended 6LoWPAN network consists of one or more subnets connected to an external IP network through several edge routers connected to the same network (for example, an organization's local network). In this case, the boundary routers in the extended network share the same network prefix. The nodes of the extended network can freely move within the network and exchange with the external network through any edge router (usually the route with the best signal quality parameters - error level, signal level) is selected. (15)(16)

3. Methodology

A cryptographic protocol is an abstract or specific protocol that includes a set of cryptographic algorithms. The protocol is based on a set of rules that regulate the use of cryptographic transformations and algorithms in information processes. (17)

Functions of cryptographic protocols: Authenticating the data source; Authentication of the parties; Privacy Policy; Failure to refuse; Failure to refuse with proof of receipt; Failure to refuse with proof of source; Data Integrity; Ensuring the integrity of the connection without recovery; Ensuring integrity of connection with recovery; Access control.

Classification:

1- Encryption / decryption protocols
2- Electronic digital signature protocols (EDS)
3- Authentication / Authentication Protocols
4- Authenticated Key Distribution Protocols

3.1 Encryption / Decryption protocols

The protocol of this class contains some symmetric or asymmetric encryption / decryption algorithm. The encryption algorithm is performed on the sender's transmission of the message, as a result of which the message is converted from an open form to an encrypted one. The decryption algorithm is executed on reception by the recipient, as a result of which the message is transformed from the encrypted form to the open one. This ensures the property of confidentiality. To ensure the integrity of transmitted messages, symmetric encryption / decryption algorithms are usually combined with algorithms for calculating the

IMO on the transmission and checking the IMS at the reception, for which the encryption key is used. When using asymmetric encryption / decryption algorithms, the integrity property is ensured separately by calculating the electronic digital signature (EDS) in the transmission and checking the digital signature at the reception, which also ensures the properties of the fail-safe and authenticity of the received message.

3.2 Electronic digital signature protocols (EDS)

At the heart of the protocol of this class there is some algorithm for calculating the digital signature on the transmission using the secret key of the sender and checking the digital signature at the reception with the corresponding public key extracted from the open reference book, but protected from modifications. In the case of a positive result of the verification, the protocol is usually completed by the operation of archiving the received message, its EDS and the corresponding public key. The archiving operation may not be performed if the EDS is used only to provide integrity and authenticity properties of the received message, but not reliability. In this case, after verification, the EDS can be destroyed immediately or after a limited waiting period.

3.3 Authentication Protocols

The authentication protocol is based on some algorithm for verifying the fact that the identifiable object (user, device, process ...) presenting some name (identifier) knows the secret information known only to the claimed object, and the verification method is, of course, indirect, then there is no presentation of this secret information.

Usually, each object's name (identifier) is associated with a list of its rights and authorities in the system, written in a secure database. In this case, the authentication protocol can be extended to the authentication protocol, in which the identified object is checked for eligibility of the ordered service.
If the EDS protocol is used in the identification protocol, the secret key is played by the secret key of the EDS, and the EDS check is carried out using the public key of the EDS, the knowledge of which does not allow the corresponding secret key to be determined, but makes sure that it is known to the EDS author.

3.4 Authenticated Key Distribution Protocols

Protocols of this class combine user authentication with the protocol for generating and distributing keys on the communication channel. The protocol has two or three participants; the third participant is the key generation and distribution center (SCMC), which is called for brevity by the server S. The protocol consists of three stages, named: generation, registration and communication. At the generation stage, the server S generates numerical values of the system parameters, including its secret and public key. At the registration stage, the server S identifies users by documents (in person or by authorized persons), for each object generates key and / or identification information and generates a security token containing the necessary system constants and the server's public key S (if necessary).

3.5 Encryption Algorithms

At the present time, various encryption methods are at the heart of all data protection technologies. Encryption refers to a reversible process of converting information with a view to concealing them from unprivileged individuals. An important feature of any encryption method is the use of a key that asserts the choice of a certain transformation from all possible for this method.

In order for encrypted information to become a meaningless set of characters for a foreign user, special encryption algorithms were developed. In general, all algorithms can be divided into 2 groups: symmetric and asymmetric.

Symmetric algorithms (AES, CAST, GOST, Blowfish, and DES) use one data key for encryption and decryption. The main disadvantage of these algorithms is that if an encryption key is stolen, an attacker can steal and decrypt the data. In addition, there are crypto attack technologies that allow you to decrypt data without using an encryption key.

Asymmetric algorithms (El-Gamal, RSA) use different keys for encryption - open and closed. The public key is transmitted over an unprotected channel and is designed to check the digital signature and encrypt the message. To generate EDS and decryption a secret key is used. Asymmetric encryption algorithms partially solve the problem of intercepting keys. If an attacker decrypt information even if he intercepts the key.

It should be taken into account that any encryption system, with the exception of crypto-resistant ones, can be hacked with a simple search of keys. Another way to crack encryption systems is to intercept messages and analyze them. The ability of cipher systems to resist burglary is called cryptographic resistance. When choosing an encryption system, you should rely, mainly, on this indicator.

Now the market of information security offers many tools and systems that implement time-tested cryptographic algorithms. All these systems combine the principle of "transparent encryption", the meaning of which is that the data is encrypted in real time, without being a separate operation.

- *Brief description of encryption algorithms*

  The DES algorithm was developed in 1975 and adopted as a standard by the US National Institute for Standardization (ANSI) in 1981. The length of the cryptographic key is 56 bits. The development of computer technology has led to the fact that a complete search of all 56-bit keys is possible. Therefore, DES can no longer be used as a reliable means of protecting electronic information. It can be recommended only for testing purposes.

  The Triple DES algorithm is a triple data transformation using the DES algorithm with three different 56-bit keys. Thus, the length of the Triple DES key is 168 bits. Triple DES is significantly more reliable than DES. A full bust of 168-bit keys in our time is considered impossible. But the data transformation using the Triple DES algorithm is three times slower than the DES algorithm. Therefore, the use of Triple DES in the products of the Secret Disk NG family leads to a significant slowdown in the processes of accessing data on encrypted disks.

  Advanced Encryption Standard (AES), also known as Rijndael, is a symmetric block cipher algorithm (block size 128 bits, key 128/192/256 bits), accepted as the encryption standard by the US government as a result of the AES competition. This algorithm is well-analyzed and is now widely used, as it was with its predecessor DES. Secret Disk Crypto Extension Pack allows you to use the algorithm AES with key lengths of 128 and 256 bits.

The algorithm Twofish was proposed in 1998 and developed on the basis of algorithms Blowfish, SAFER and Square. Information is also encrypted with 128-bit blocks. Secret Disk Crypto Extension Pack allows you to use the Twofish algorithm with a key length of 256 bits.

Algorithm GOST 28147-89 is the Soviet and Russian standard for symmetric encryption, introduced in 1990, is also a standard in the CIS countries. It is a block cipher algorithm with 256-bit key and 32 conversion cycles, operating with 64-bit blocks. The advantage of the algorithm is the hopelessness of attack by brute force and high speed.

3.6 General Understanding Advanced Encryption Standard (AES)

Advanced Encryption Standard is a symmetric block encryption algorithm adopted by the US government as a standard as a result of a competition held between technology institutes. It replaced the outdated Data Encryption Standard, which no longer met the requirements of network security, which became more complex in the 21st century.

This algorithm, other than the AES abbreviation, is sometimes also called Rijndael, an anagram from parts of the names of Belgian programmers Joan Daemen and VinentRijmen, who developed AES. Strictly speaking, AES and Rijndael are not exactly the same, since AES has a fixed block size of 128 bits and key sizes of 128, 192 and 256 bits, while for Rijndael any block and key sizes can be specified from a minimum of 32 bits to a maximum of 256 bits.

The AES algorithm was approved by the US National Security Agency as suitable for encrypting sensitive information. However, the government decided that AES should be periodically inspected and improved to reliably store the encrypted data.

Information identified as secret must be protected by AES with a key length of 128, 192 and 256 bits. For information defined as highly secret, this length is 192 or 256 bits. The essence of AES is that any "frontal attack" on the protected data - that is, the selection of all possible passwords - in the long run is very much stretched. If we imagine that the burglar has huge resources, that is, a whole collection of supercomputers, then with diligent efforts, access to encrypted data could be obtained in tens of years. If at his disposal there is nothing of this, then AES hacking will take an astronomically long time.

3.6.1 The reliability of the AES encryption algorithm

It is believed that the 128-bit key used in Advanced Encryption Standard is quite reliable protection against frontal attack, that is, from a purely mathematical point of view, to pick one correct password out of all possible - an impossible task. Despite even some of the shortcomings of AES, it is almost impossible to crack the information protected by this algorithm.
Any cryptographic algorithm requires a key size of a particular number of bits to encrypt the data, as shown in the image 3.1:

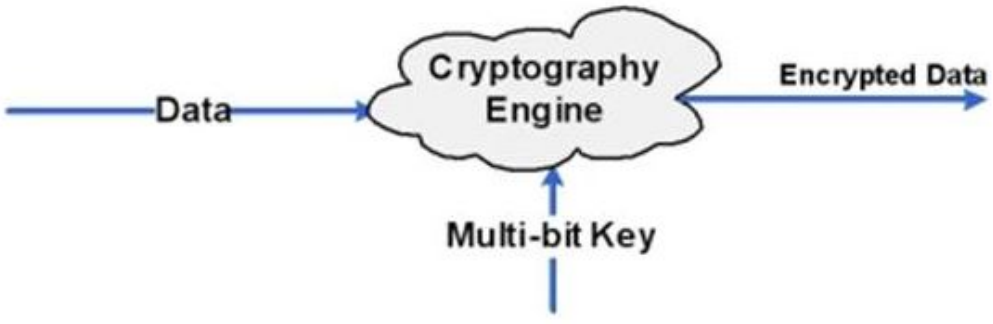


Image 3-1

The length of the key used in encryption determines the practical feasibility of performing a full search, because the information encrypted with longer keys is exponentially more difficult to crack than with short ones.

Here is an example of a search for a 4-bit key:

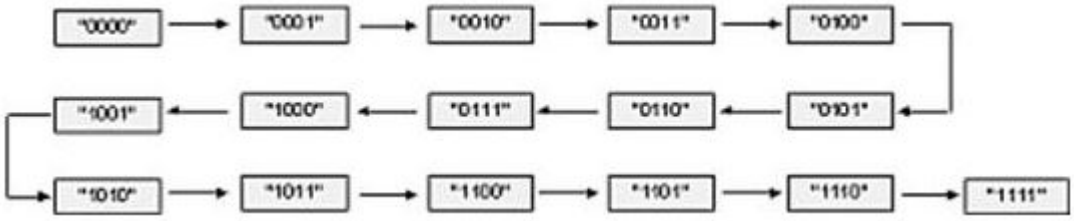


Image 3-2

It will take a maximum of 16 steps to check every possible combination, beginning with "0000". Frontal attack for some time can break such a simple algorithm.

The table in the figure below shows the possible number of combinations given the size of the key:

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^9
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Image 3-3

Pay attention to the fact that as the size of the key increases, the number of combinations increases exponentially. Mathematical calculus proves that the size of the 128-bit key protects the frontal attack in the most reliable way:

Key size	Time to Crack
56-bit	399 seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

Image 3-4

Thus, even a supercomputer would need an innumerable amount of time to gain access to information protected by AES through a frontal attack.

For comparison: the age of the universe is somewhere between 13 and 14 billion years. Even if we assume that some super-supercomputer could cope with the DES algorithm in one second, then it would take about 149 trillion years to break into AES.

As you can see, the size of the 128-bit key is quite enough, although top secret information is still encrypted with a size of 256 bits. The following assumption proves that the 128-bit standard will remain relevant in the future.

Imagine:

- Every person on Earth has ten computers on Earth
- On Earth, seven billion people
- Each of these computers can test one billion combinations per second
- The key is considered hacked if 50% of all possible combinations are checked

Under all these conditions, the entire population of the planet would be able to crack one key ... for 77,000,000,000,000,000,000,000,000 years.

It is interesting to note that the difference between the key size of 128 bits and 256 bits is not so important. If someone came up with a program capable of hacking a 128-bit system, 256 bits for this genius would not be a hindrance. Finally, the best statistics for AES are statistics: the data protected by this algorithm has never been hacked. However, all this works with a key size of at least 128 bits, since earlier cryptographic algorithms still did not withstand the strength test.

Despite the fact that the computing speed increases exponentially according to Moore's law, a 128-bit key should be sufficient for many years to come.

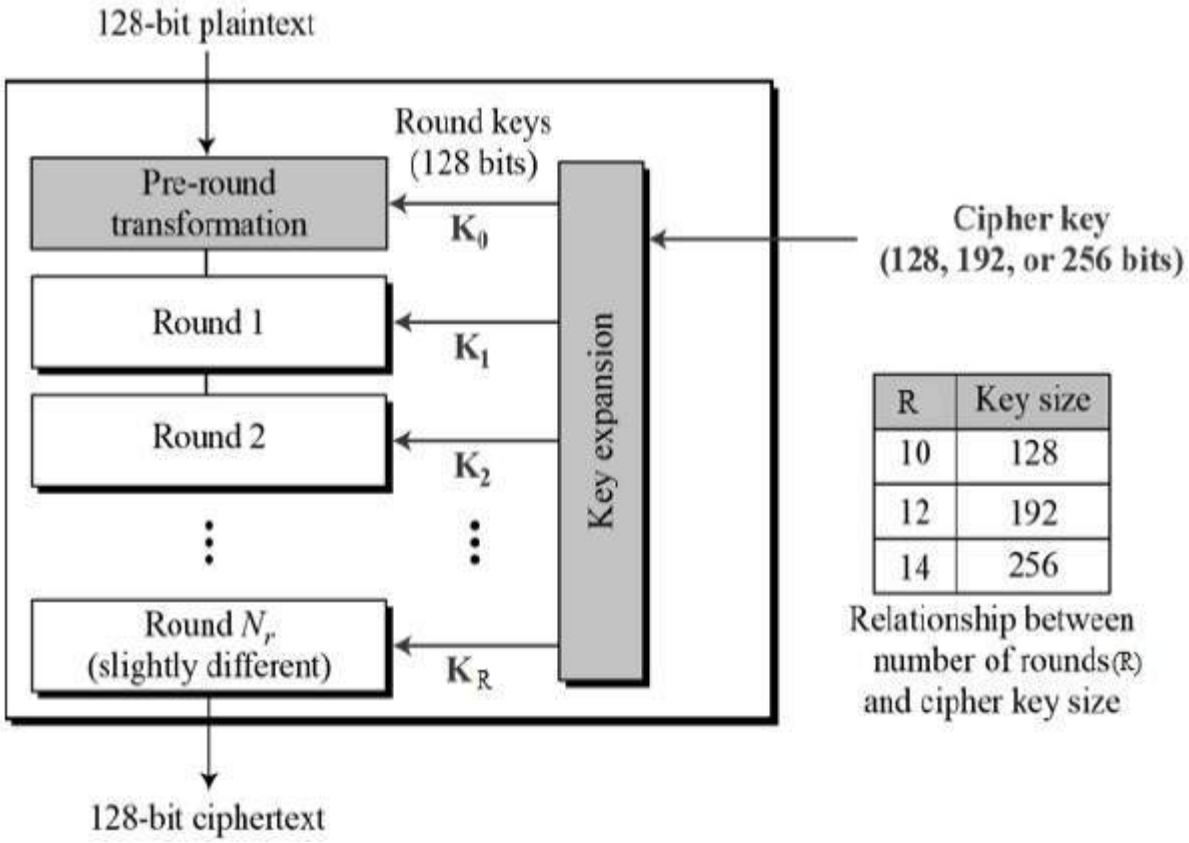
3.6.2 Steps in the AES Encryption Process

AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). (18)

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. (19)

The schematic of AES structure is given in the following illustration −



R	Key size
10	128
12	192
14	256

Relationship between number of rounds (R) and cipher key size

Image 3-5

3.6.2.1Encryption Process

For encryption, you need a key. Key size in the algorithm AES is 128 bit, the key is usually represented as a 4-4 byte matrix.

At the beginning of the encryption process, the input data is divided into blocks the size of 16 bytes or 128 bits. If the total size of the data is not a multiple of 16 bytes – data is supplemented to a multiple of 16 bytes. The data block in Algorithm AES is called state and is usually represented as a 4 × 4 matrix byte. The operation of encryption of each data block is carried out regardless of the contents of other blocks. At the end of encryption of the block the matrix is filled with the next piece of data and the process is repeated. By virtue of

independence of encryption of one block from another encryption process it can be paralleled.

Each block is encrypted in several stages – rounds. Scheme crypto-conversion can be written as follows.

1. Key Expansion.
2. Initial operation – AddRoundKey – summation with the main key.
3. 9 rounds of four steps each.
    3.1. Sub Bytes - replacement of state bytes by the replacement table.
    3.2. Shift Rows - a circular shift of the state.
    3.3. Mix Columns - permutation of the state.
    3.4. AddRoundKey - summation with a round key.
4. The final 10th round
    4.1. Sub Bytes - replacement of state bytes by the replacement table.
    4.2. Shift Rows - a circular shift of the state.
    4.3. AddRoundKey - summation with a round key.

3.6.2.2 Decryption Process

All encryption conversions are unambiguous and, therefore, have inverse transformation; can be inverted and executed in reverse order to perform the decryption for the AES algorithm.

The crypto-conversion scheme can be written as follows.

1. Key Expansion.
3. 9 rounds of four steps each.
    3.1. AddRoundKey - summation with a round key.
    3.2. InvMixColumns - reverse permutation of the state.
    3.3. InvShiftRows - reverse cyclic shift of state.

3.4. InvSubBytes is the reverse substitution of state bytes for the replacement table.

4. The final 10th round

4.1. AddRoundKey - summation with a round key.

4.2. InvShiftRows - reverse cyclic shift of state.

4.3. InvSubBytes is the reverse substitution of state bytes for the replacement table.

4. A security services in internet of things

4.1 Identification and authentication (Trust model)

With a recommendation for a model to interestingly distinguish our gadgets, we will now propose an idea to confirm them keeping in mind the end goal to empower correspondence and trust. The accompanying subsections portray a proposed rearranged method for overseeing personalities and trust in an IoT domain utilizing a Public key foundation (PKI). Take note of this is a proposition and not a pertinent arrangement. The proposition ought to be portrayed in more detail and amid this lined up with current prescribed procedures before actualized. Besides, IoT gadgets that can't store a declaration and the endorsement of a CA are not considered in this area and are left for future work. (20)

4.2.1 Trust

At the point when a device or gateway is selected, the devices own authentication should be put away some place in the top level order server (CA). With the private key of the declaration securely remade each time it is utilized with a PUF, it gets hard for an aggressor to distort this current gadget's character (i.e. recovering the private key). A gadget or entryway likewise has to know who it ought to associate with, that is, the portal or server testament should be known before arrangement. This declaration can be pre-put away on the gadget together with testaments from the CA (where these authentications are for the gadget itself and for the CA).
Organizations will dependably need to make their own particular administrations and pitch them to different organizations or individuals. That is the reason a chain of trust with cross affirmation is a decent method for designating rights and approval to others by pushing data to effectively put stock in gadgets.
The proprietor (organization or individual) of nature will fill in as an expert for the entire trust chain made amongst entryways and gadgets. The Server/Cloud will make a trust amongst itself and the portals. The passages will thusly do likewise with these gadgets associated with it. There are likewise conceivable outcomes for gadgets to interface straightforwardly to the Server/Cloud similarly as a door.
In the accompanying areas the nuts and bolts of character administration and confirmation of hubs in an IoT-situation is appeared. The names of the distinctive authentications (GW/D/S/NS-IoTcert) are just used to clear up which personality is being sent. The declaration ought to contain no less than an open key which is adequate to distinguish a gadget. (21)

4.2.2 Authentication of gateway

Those personality card (public key) of the gateway needs will make saved in the server and the other way around will empower best possible verification throughout the introductory organization. For example, at a gateway needs should validate a server/cloud it will do those taking after steps. (shown in Figure 4—1):

1- The gateway sends a message encrypted with the Server/Cloud public key and then signs it with its private key. This ensures that the gateway sent the message and only the server will be able to decrypt it.
2- The server will be able to verify the gateways identity or not depending on which keys were used. The server tries verifying the signature with the public key of the gateway and then decrypting the message with its own private key.
3- The Server/Cloud sends back a response only if it verifies the gateway's identity. The response is a message encrypted with the gateways public key and thereafter signed with the Server/Cloud private key.
4- The gateway verifies the server the same way as in Step 2 since the gateway knows the public key of the Server/Cloud as this was installed into the gateway pre-deployment. (32)

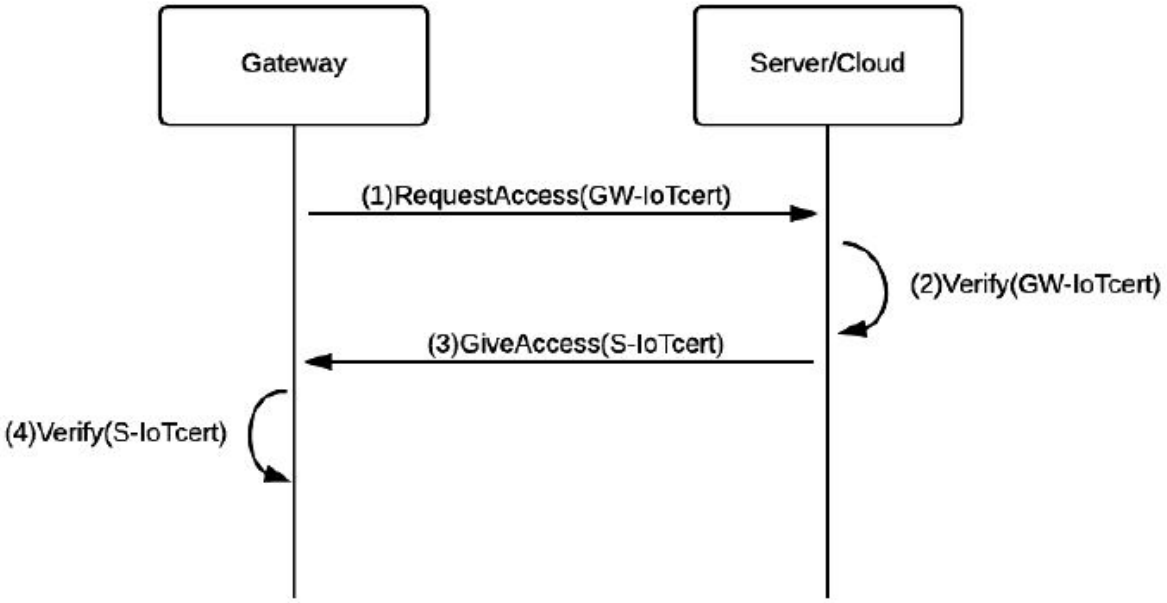


Figure 4-1

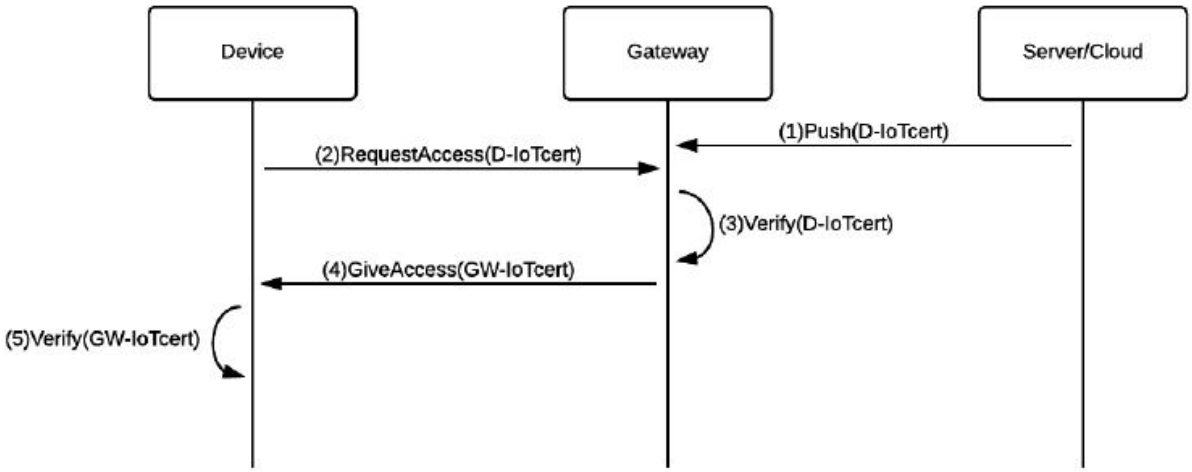


Figure 4-2

4.2.3 Authentication of IoT-device

Since those gateway may be currently trusted, we might begin authenticating gadgets against it. Each recently deployed gadget is expected to need been pre-configured with those personality of its gateway; consequently it need a

duplicate of the gateway's testament. On it doesn't realize who should validate with, that point it Might fundamentally interface for anything. The process of authenticating IoT devices is shown in Figure 4—2 and consists of:

1- The new device's identity is pushed to the gateway from the server, so that the gateway can learn about the new device and hence can communicate securely with it.

2- When a device connects to the gateway it sends a request for access to the gateway, same as Step 1 in Chapter 4.2.1.

3- Since the gateway knows the identity of the device it tries to verify the identity of this device, same as Step 2 in Chapter 4.2.1.

4- The gateway sends a response if it successfully verifies the identity of the device.

5- The device verifies the gateway in the same way (as Step 3) since it knows the identity of the gateway prior to its deployment.

Since there now is a chain of trust in the environment we can manage, revoke, and give other systems access to our gateways or devices.

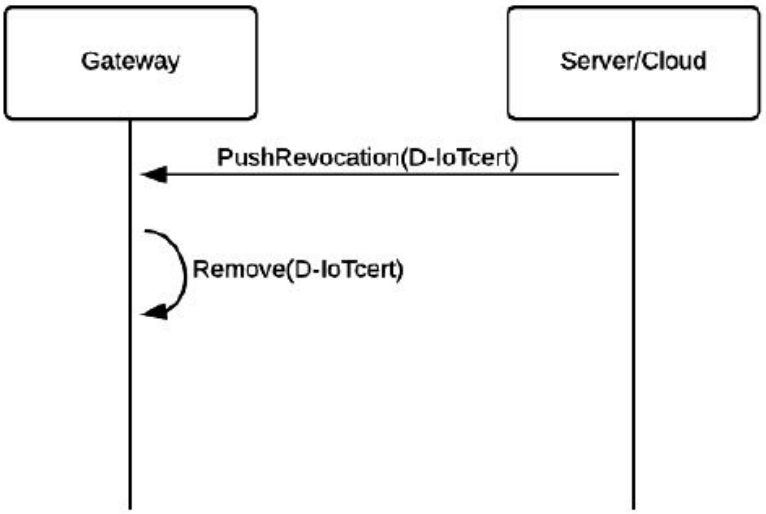


Figure 4-3

4.2.4 Access control

Whether another organization needs get on our sensors or gateway for example, the Emulating technique Might be utilized allowing right. It Might Additionally make used to exchange proprietorship. We expect that those highest priority on those progressive structure server takes in the personality (NS-IoTcert) of the new Server/Cloud (other PKI CA) requesting right. (This Might make completed clinched alongside a few separate routes.) Right away those procedure returns concerning illustration takes after. (as shown in Figure 4—4):

1- The Server/Cloud pushes the identity of requested gateway to the New Server/Cloud.

2- The identity of the New Server/Cloud is pushed to the gateway that it wants to connect to.

3- The gateway now waits for an access request from the New Server/Cloud.

4- When a request for access has been received, the gateway verifies the sender with the identity pushed from the Server/Cloud.

5- If the New Server/Cloud identities matched, the gateway sends a response to the new server.

6- The New Server/Cloud authenticates the gateway with the identity given from Server/Cloud.

7- A response is sent back to the gateway if the authentication was successful. (31)

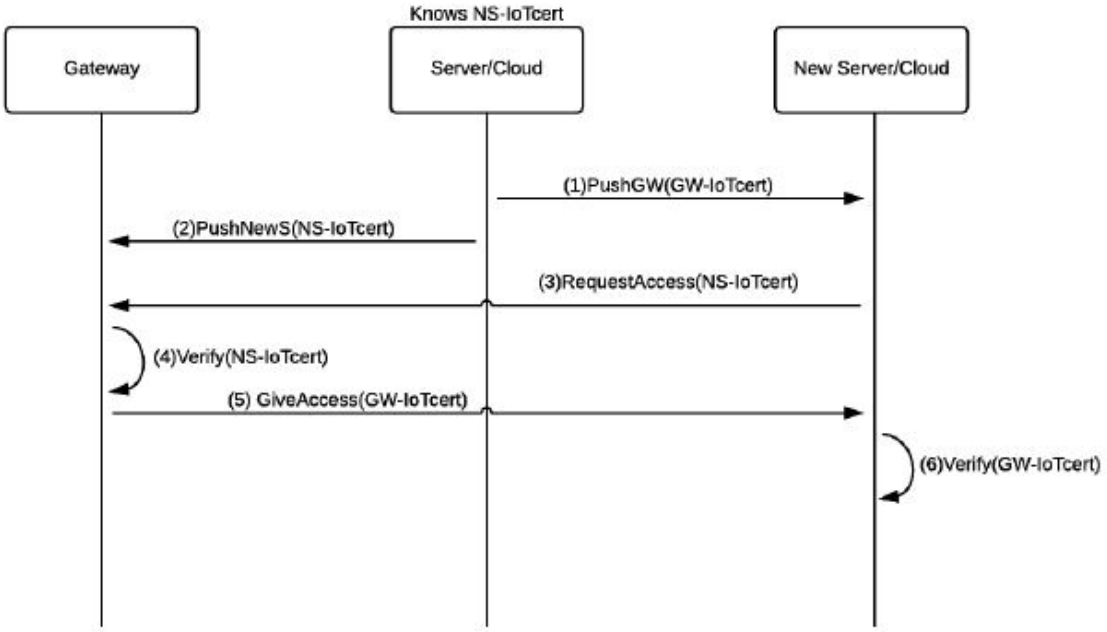

Knows NS-IoTcert
Gateway
Server/Cloud
New Server/Cloud
(1)PushGW(GW-IoTcert)
(2)PushNewS(NS-IoTcert)
(3)RequestAccess(NS-IoTcert)
(4)Verify(NS-IoTcert)
(5) GiveAccess(GW-IoTcert)
(6)Verify(GW-IoTcert)

Figure 4-4

5. Lightweight Cryptography for the Internet of Things.

Cryptographic technologies promotion: new attack methods, development and implementation are widely studied. One of the technical embedded is "easy encryption (LWC)". Light is an encryption algorithm or a cryptographic protocol adapted for deployment in confined environments, such as RFID tags, sensors, contactless smart cards, healthcare devices and so on.
The properties of lightweight encryption have already been discussed in ISO / IEC 29192 ISO / IEC JTC 1 / SC 27 ISO / IEC 29192 is a new lightweight cryptographic standardization project and the project is standardized. In ISO / IEC 29192, the lightweight properties are described based on the target platforms. In the hardware implementation, the size of the chip and / or energy Consumption is an important measure for assessing the properties of light. In a software implementation, the smallest code and / or RAM size is preferred for lightweight applications. In terms of the properties of implementation, primitive readings surpass ordinary cryptographic, is currently used in Internet security protocols, for example. IPsec, TLS.
Lightweight cryptography also delivers acceptable and fairpreservation. Lightweight cryptography does not regularlyaccomplishment the security-efficiency trade-offs.

5.1 Symmetric Key Cryptography

Block ciphers. Many block ciphers with lightweight properties have been proposed since Advanced Encryption Standard (AES) was chosen. Among them, CLEFIA [23] and PRESENT [24] are thoroughly researched about its

security and implementation. Both algorithms are under discussion in ISO / IEC 29192 "Lightweight Cryptography". The cipher is ready for use in the actual system.

Stream ciphers. The ECRYPT II eSTREAM project [25] held from 2004 to 2008 selected a promising new stream cipher portfolio. Seven algorithms are included in the current eSTREAM portfolio. Grain v1, MICKEY v2, and Trivium have lightweight properties among these algorithms.

Hash functions. The competition of NIST's new cryptographic hash algorithm "SHA-3" is attracting a lot of people's attention. SHA - 3 is expected to be a general - purpose hash function, and none of the current finalists meet lightweight properties. A study on lightweight dedicated hash function began [26]. They are immature to adopt now. It is possible to construct lightweight hash functions based on lightweight block ciphers.

5.2 Public Key Cryptography

Although lightweight public key primitives are required for the key management protocol of the Smart Object Network, the resources required for public key primitives are much larger than the resources of symmetric key primitives. At the moment there are no promising primitives that satisfy sufficient security and lightness compared to conventional primitives such as RSA and ECC.

Several public key primitives (eg, ECC) can be implemented with a relatively small footprint, but cannot be executed within a reasonable amount of time. (27)

5.3 Why is lightweight cryptography required for IoT?

We propose to adopt new advanced technology "lightweight encryption" at IoT. I will explain two reasons for supporting the proposal.

1. Efficiency of end-to-end communication

In order to achieve end-to-end security, symmetric key algorithms are implemented in the end nodes. Low resource devices, for example cryptographic operations with a limited amount of energy consumption, are important. By applying a lightweight symmetric key algorithm, we can reduce energy consumption of end devices.

2. Applicability to lower resource devices

The footprint of lightweight cryptographic primitives is smaller than conventional cryptographic primitives. Lightweight cryptographic primitives will open up the possibility of more network connections with lower resource devices.

A comparison between lightweight properties and conventional cryptographic primitives is shown in the Appendix. Comparison of the appendix focuses on the properties of the hardware. Some end nodes can incorporate general purpose microprocessors and software properties are considered important in such platforms. However, with the lowest cost device, hardware characteristics are decisively important and cost and power consumption is limited, so you can incorporate only application specific ICs.

In conclusion, lightweight cryptography contributes to the security of smart objects networks because of its efficiency and smaller footprint. We believe that lightweight primitives should be considered to be implemented in the networks. Especially, lightweight block ciphers are practical to use now.

5.4 Hardware Properties of Lightweight Block Ciphers

Figure 5-1 shows hardware efficiency of 128-bit block ciphers. Hardware efficiency is defined as the ratio of throughput (speed) to gate size (area). In this graph, higher slope (marked yellow area) indicates higher efficiency, which leads to low energy consumption. This figure compares a lightweight block cipher CLEFIA with conventional block ciphers: AES (FIPS197), Camellia (RFC3713), and SEED (RFC4269). These ciphers are also used in TLS/IPsec. CLEFIA has an advantage in hardware gate efficiency over these ciphers. (28)

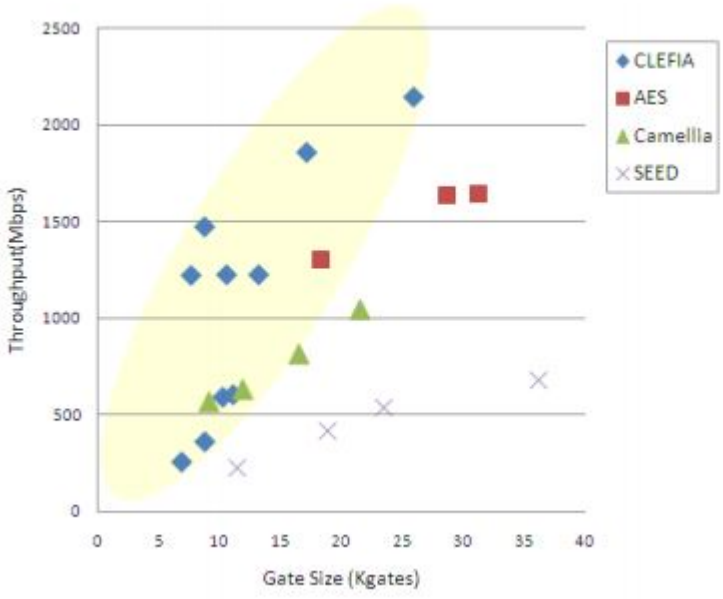


Figure 5-1

Hardware performance of the lightweight block ciphers is shown in Table 1. PRESENT and CLEFIA are the lightweight block ciphers proposed and under consideration in ISO/IEC 29192-2. For reference, the results of AES are shown in the table. The “area” is a metric for cost and power consumption when the chip is clocked at a low frequency of a few hundred kHz. The product of “area”

and “cycle” is a metric for energy consumption. Table 1 shows that the lightweight ciphers can be implemented with smaller area and less energy consumption. Note that PRESENT is a 64-bit block cipher while CLEFIA and AES are 128-bit block ciphers. Generally speaking, 64-bit block ciphers can be implemented with smaller gate counts, but there are certain security limitations.

	mode	block size [bits]	key size [bits]	cycle	area [GE]	frequency [MHz]	throughput [Mbps]	technology [μm]
Serialized Implementation (Area Optimization)								
PRESENT [6]	enc	64	80	547	1075	0.1	0.0117	0.18
PRESENT [6]	enc	64	128	559	1391	0.1	0.0115	0.18
CLEFIA [1]	enc	128	128	176	2893	67	49	0.13
CLEFIA [1]	enc/dec	128	128	176	2996	61	44	0.13
AES [5]	enc	128	128	177	3100	152	110	0.13
AES [4]	enc/dec	128	128	1032	3400	80	10	0.35
Round-based Implementation (Efficiency Optimization)								
PRESENT [6]	enc	64	80	32	1570	0.1	0.20	0.18
PRESENT [6]	enc	64	128	32	1884	0.1	0.20	0.18
CLEFIA [8]	enc/dec	128	128	36	4950	201.3	715.69	0.09
CLEFIA [8]	enc/dec	128	128	18	5979	225.8	1605.94	0.09
AES [7]	enc/dec	128	128	11	12454	145.4	1691.35	0.13
AES [7]	enc/dec	128	128	54	5398	131.2	311.09	0.13

Table 5-1. Results on Hardware Performance

Summary

The goals of this thesis were to introduce the reader to the IoT concept, identify security challenges that need to be addressed in order to secure IoT, propose a solution to them. In first chapter, there is a general introduction to IoT, where is spoken about IoT history, what is IoT, what is the importance of it and how it will affect our future. Second chapter, explains general security issues and vulnerabilities, and interaction of security with IoT. Security over internet bases on cryptography, encryption, decryption algorithms, that is why in this thesis widely explains encryption algorithms, for example AES algorithm.

A major part of the research concerned IP-based communication based on IPv6. The use of IPv6 will probably be crucial for finding and addressing unique devices on the Internet since the number of available addresses will enable every device to have its own IP address.

At the end, Lightweight Cryptography for the Internet of Things is discussed, which is also main part of this thesis. In first chapters was explained that IoT devices are low power devices with low memory, RAM, that is why it is important to use light algorithms for encryption.

As the conclusion in Chapter 4, the proposed authentication method needs extensive analysis, for example how to deal with replay attacks, identity management on the device, which protocols to be used for communication, which cryptographic algorithms and keys to use, etc. These properties need to be carefully chosen and implemented if a standard is to be developed, which is put off to future work.

References

(1) G. E. Moore, “Cramming More Components onto Integrated Circuits,”

(2) J. G. Koomey, S. Berard, M. Sanchez and H. Wong, “Accessing Trends in The Electrical Efficiency Computation Over Time,” 2009.

(3) http://www.howtoflyahorse.com/2009/06/22/the-internet-of-things/

(4) https://www.entrepreneur.com/article/271188 (article by: ZACH CUTLER GUEST WRITER Founder & CEO, Cutler PR)

(5) http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf

(6) Sources: Frog Design, Fit Guard, Fit Bit, Leo Helps, SmartSensing.fr, Microchips biotech, LG, Digital Trends, Boogio, TraxFamily.com, IndieGoGo, V1bes.com, GPSshoes.com, Runaroundtech.com, Emotiv.com, AmpStrip.com, smartcaptech.com, Hovding, venturebeat.com, extremetech.com, BBC News, metriaih1.com.

(7) Cherdantseva Y. and Hilton J.: "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals". In: Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (eds.). IGI Global Publishing. (2013)

(8) Boritz, J. Efrim. "IS Practitioners' Views on Core Concepts of Information Integrity". International Journal of Accounting Information Systems. Retrieved 12 August 2011.

(9) Loukas, G.; Oke, G. (September 2010). "Protection Against Denial of Service Attacks: A Survey" (PDF). Comput. J. 53 (7): 1020–1037. doi:10.1093/comjnl/bxp078.

(10) Learning to live in the "Internet of things" How to use smart devices and protect yourself from intruders Victor Alyushin, Vladimir Krylov - November 5, 2015

(11) M. McDowell, "Understanding Denial-of-Service Attacks US-CERT," United States Computer Emergency Readiness Team, 2013. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-015. [Accessed 25 May 2015].

(12) IEC, "IEC - Electromagnetic compatibility - EMC explained EMC and the IEC," 2015. [Online]. Available: http://www.iec.ch/emc/explained/. [Accessed 25 May 2015].

(13) OWASP, "Man-in-the-middle attack - OWASP," OWASP, 8 April 2014. [Online]. Available: https://www.owasp.org/index.php/Man-in-the-middle_attack.

(14) OWASP, "Top 10 2014-I5 Privacy Concerns - OWASP," OWASP, 2 April 2015. [Online]. Available: https://www.owasp.org/index.php/Top_10_2014 I5_Privacy_Concerns. [Accessed 25 May 2015].

(15) Zach Shelby, Carsten Bormann 6LoWPAN: The Wireless Embedded Internet. John Wiley & Sons Ltd. 2009. 245 c.

(16) CC-6LoWPAN – Texas Instruments Embedded Processors Wiki//http://processors.wiki.ti.com/index.php/CC-6LoWPAN

(17) "Cryptographic Protocol Overview" (pdf). 2015-10-23.

(18) www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

(19) "Efficient software implementation of AES on 32-bit platforms". Lecture Notes in Computer Science: 2523. 2003

(20) S. Raza, S. Duquennoy and G. Selander, “Compression of IPsec AH and ESP Headers for Constrained Environments,” Internet-Draft, 3 September 2013.
(21) J. Hui and P. Thubert, “Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks,” RFC 4944 (Standard Draft), September 2011.
(22) Symantec Corporation, “Man-in-the-middle attack,” Symantec Corporation
(23) T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, “The 128-bit blockcipher CLEFIA.” In Proceedings of Fast Software Encryption – FSE’07 (A. Biryukov, ed.), no. 4593 in LNCS, pp. 181–195, Springer-Verlag, 2007.
(24) A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, “PREsSENT: An Ultra-Lightweight Block Cipher.” in CHES 2007, no. 4727 in LNCS, pp. 450–466, Springer-Verlag, 2007.
(25) “The eSTREAM project.” 2004–2008. http://www.ecrypt.eu.org/stream/.
(26) J.-P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia, “Quark: A Lightweight Hash.” in CHES 2010, no. 6225 in LNCS, pp. 1–15, Springer-Verlag, 2010.
(27) T. Akishita and H. Hiwatari, “Compact Hardware Implementations of the 128-bit Blockcipher CLEFIA.” in Proceedings of Symposium on Cryptography and Information Security –SCIS 2011 (in Japanese), 2011.
(28) Lightweight Cryptography for the Internet of Things - Masanobu Katagi and Shiho Moriai - Sony Corporation.
(29) http: //www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf
(30) Cherdantseva Y. and Hilton J.: "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals". In:

Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (Eds.). IGI Global Publishing. (2013)

(31) https://people.kth.se/~maguire/DEGREE-PROJECT-REPORTS/150615-Cristian_Bude_Andreas_Kervefors_Bergstrand-with-cover.pdf

(32) Networks, Crowds, and Markets - By David Easley and Jon Kleinberg