Trends in IoT Security

M. Radovan[*], B.Golub[**]
[*] Daimler AG, Stuttgart, Germany
mihael.radovan@daimler.com
[**] Adnet d.o.o., Zagreb, Croatia
boris.golub@adnet.hr

Abstract – The incredible rapid development of internet technologies, primarily thanks to omnipresent access of high speed broadband internet access and supporting technologies like Big Data, Cloud Computing, REST/Web services as well as cheap electronic equipment that use new wireless communications standards, lead to equal rapid growth of number of smart devices – "things" - connected to the internet. Increased number of connected smart devices results with huge daily data traffic on the internet and data volume stored and available on the internet. IoT becomes part of our homes and our companies, and security in these systems is very important. What does that outlook hold for the next 5, 10 or 20 years, will mostly depend on the development of security standards, user behavior and education in a next few years. This paper is trying to summary and analyze trends in IoT standards regarding security.

Keywords - Internet of Things (IoT); Cybersecurity; SCADA;

I. INTRODUCTION

Each new technology potentially involves some risks. The worst of which are security threats. This is especially the case with a fast-growing technology where it is difficult to predict all possible risks involved. On the other hand, the number of skilled malignant hackers, highly motivated to abuse new technology inadequacies is rising.

Quoting Kevin Ashton, the probable author of the term "Internet of Things" [1], from 1999, the size of the Internet in 1999 was about 50 petabytes of data, and the prediction for 2020 is that the size of the Internet will be about 40 zettabytes of data.

Although the industrial giants are for security reasons very conservative with beginning to utilize new things, IoT is already there. Smart devices are everywhere around – smart wearable, smart medical devices, smart homes, smart buildings, smart cars, smart cities, smart grids, smart agriculture and many other aspects of life [2] (see Fig. 1). The challenge grows further as IoT devices have the option to control important industry infrastructure. This will certainly increase society exposure to cyberthreats. In today's approximations, the damage from cybercrime is assessed at about 400 billion dollars per year.

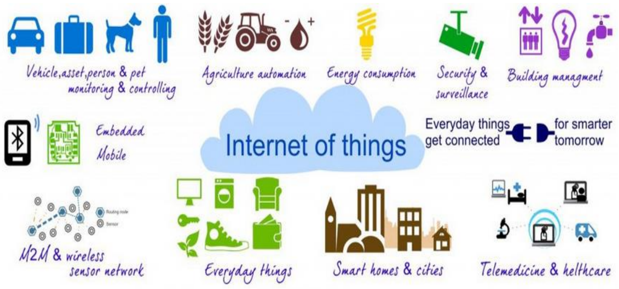

Figure 1. IoT fields of use

The smart future has already arrived. Are we ready for it? Do we behave responsibly in order to have all around us "smart"? Is it smart to be surrounded with smart things, can we be sure that our privacy is not compromised? These smart devices are smarter and smaller, but are they reliable and secure enough? Especially when we know that parts of IoT have not been well defined and designed, or still use parts of old architecture from "wired" era.

The main aim of this paper is to summarize the current state of security trends in IoT technologies and to analyze what needs to be considered to shape the security standards for the new generation of connected systems.

This paper is organized as follows: Section II gives a short timeline of IoT, the present state and predictions for the future. Section III shows security and privacy trends in the development of IoT and new protocols which cover these trends, and Section IV impact of IoT to industrial security. Section V gives a conclusion of the paper.

II. HISTORY, PRESENT AND FUTURE OF IoT

At the beginning of computer era (1950's until late 1970's), there were dominant mainframe computers with terminal-server architecture. During 1980's, the computer market takes over minicomputers and personal computers. 1990's comes internet era, first with analog modems (2400, 9600, 14400, 28800 bps) through analog telephone wire, then from 2000's with a digital connection (ISDN, DSL, VDSL) and finally with the broadband and wireless internet connectivity. Late 1990's comes mobile era, and a few years later, in the third millennium, the mobile device meets computer – first in shape of PDA's, and later as tablets and smart phones. Although the internet for commercial use was available first in the late 1980's, the first internet appliance was a Coke machine at Carnegie Melon University in 1982. The commercial internet began to exist in late 1980's as the "Internet of Computers" [3], providing global services such the World Wide Web. Broadband internet connectivity is becoming fast, cheap and omnipresent. Last 10 years Internet has changed to the Internet of People. This "network of humans" covers more than 1 billion people. According to the statistics portal Statista (https://www.statista.com), in 4th quarter 2016, just Facebook had 1.86 billion active users. A number of active e-mail accounts worldwide in 2016 was 4.626 billion, and prediction for 2019 is about 5.6 billion (see Fig. 2).

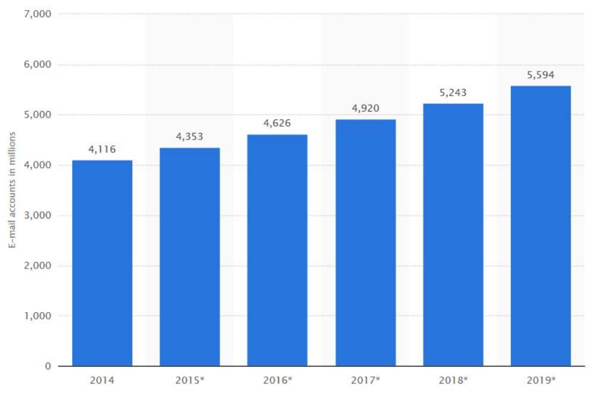

Figure 2. Number of active e-mail accounts in mil.

Fast broadband internet, Web services architecture, Big Data and Cloud Computing technologies, together with small and cheap microprocessors, led to "Internet of Things". In this case, "things" are any beings (humans, animals, plants) or items (cars, buildings, cities, factories, devices) with unique ID, internet connection and set of sensors or actuators. At any moment in time this unique items carry its status and position and provide remote access to read data from its sensors or control its actuators. It was initially proposed to use RFID to uniquely identify, track and monitor any object with RFID tag [3]. RFID is a foundational technology for IoT, while it allows microchips to transmit the ID information to a reader through wireless communication [4], widely used in industry since 1980's. Another foundational technology for IoT is wireless sensor network (WSNs), from 1990's – set of a wirelessly interconnected smart sensor attached to devices.

The newest trends in IT have established a way to Big Data era – everything goes to the Cloud. All data will be stored somewhere on the internet, or will be transferred to the storage destination through the internet. This trend can easily be seen by observing the internet size since 2000. The amount of all data published on the internet in 2000 was about 50 PB. In 2012, this size was 4 ZB, today is about 8 ZB, and expected size in 2020 is about 40 ZB (see Table 1.).

Label	Title	Size in minor unit	Size in bytes
1GB	Gigabyte	1024 MB	1024^3 byte
1TB	Terabyte	1024 GB	1024^4 byte
1PB	Petabyte	1024 TB	1024^5 byte
1EB	Exabyte	1024 PB	1024^6 byte
1ZB	Zettabyte	1024 EB	1024^7 byte
1YB	Yottabyte	1024 YB	1024^8 byte

Table 1.: Orders of magnitude of data

Just 25 years ago, in 1992 was less than 100.000 devices connected to the internet. In 2012 number of connected devices exceeded human population in the world. Predictions of Cisco [5] for 2020 is about 50 billion devices [6] (See Fig. 3).

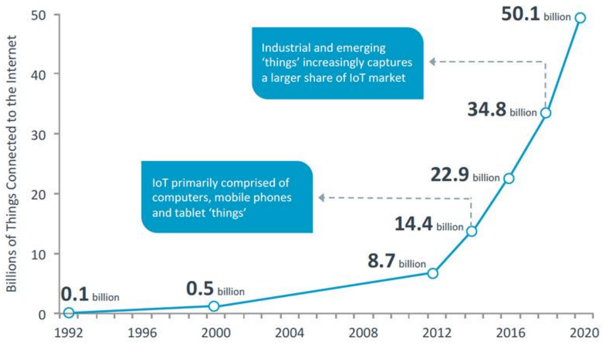

Figure 3. Number of connected devices

The numbers in the timeline – number of people connected to the internet, number of active e-mail accounts, number of connected devices, amount of published or transferred data – are just presenters of development of technology in last years, and show how fast this development is. Such a rapid development of technology enables a range of new opportunities, but also demands a development of new communications and security standards.

III. SECURITY TRENDS IN IOT

Security in IT includes availability, integrity and confidentiality. Availability means that the remote system in online and can offer the service to the customer. In the moment when system is not available, either system is down or communication is broken, the security is compromised. Integrity means that all data are the same on the source as on the destination, in communication process between client and server, or between two or more nodes in the network, and can be accessed or modified just by those authorized to do that. If during the communication process there is an unauthorized data modification the security is compromised. Confidentiality refers to the data protection on both sides in communication (client/server, sender/recipient) as well as on the network side, during data transportation. The data must be encrypted and protected, so that just sender and recipient can read it.

One of IoT technology main security challenges is in its fast growth in development of electronic devices. Security standards are often not implemented, not proven enough, or even do not exist. This is particularly the case with cheaper devices intended for home use made by no name producers. IoT technology is today still based on the standard communication architecture, which was defined for stationary clients or mobile clients under owner's control. These clients are usually located in some protected environment, and under security standards set to protect this environment from malicious interventions in every way. IoT architecture has three basic parts: Perception, Network and Application [7] (see Fig. 4).

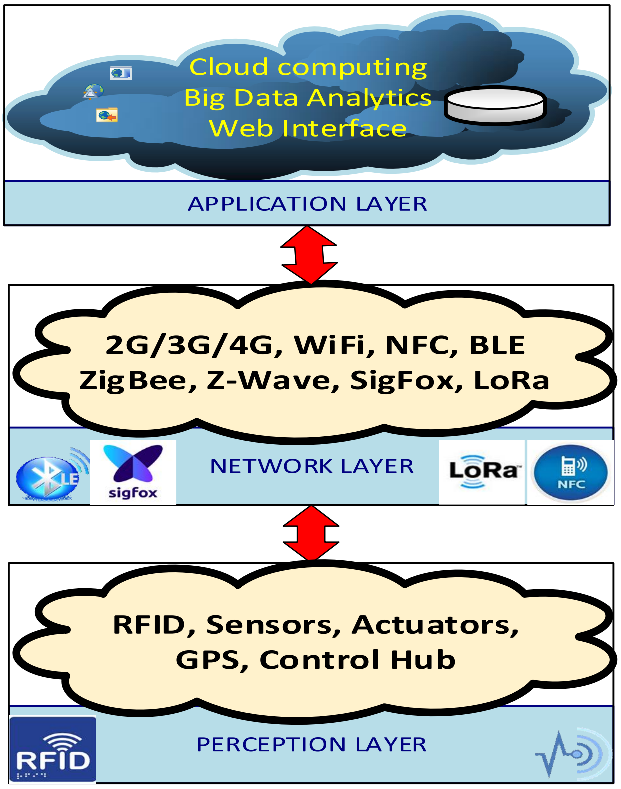

Figure 4. Architecture of IoT

Perception layer contains hardware – sensors, actuators, RFID, programmable control unit with processor and memory. These are all necessary to collect and send data or receive data. These devices are connected to the Network layer – whether standalone with independent wireless connection to ISP, or wireless grouped by hub or internet access point and through it connected to ISP. They are placed everywhere, and not always protected enough from unauthorized access, so they can easily be damaged or stolen. In this case, by unauthorized access to data or just by breaking connection between devices and the cloud, the security system will be compromised. Also, these devices are often powered by batteries or solar cells, which raises another important issue – autonomy time.

Network layer serves for the communication between sensing devices and data storage in cloud. There is a wide spectrum of technologies and standards used to exchange data. New standards are in continuous development, based on existing LAN, WLAN and WAN standards. They differ from each other by radio frequency spectrum, data exchange rate, range and power consumption. Being easily exposed target to malicious attempts security is especially important on this layer.

Highest layer is Application layer – Cloud architecture and data management systems as well as analytic and presentation software. At this point data must be protected from unauthorized access and anonymized when used for public purpose.

Together with good known WiFi, 2G/3G/4G Cellular, NFC and Bluetooth communication technologies, for industrial and commercial use are developed some new low-power and wide-range protocols: Bluetooth Low-Energy (BLE)[1], ZigBee[2], Z-Wave[3], 6LowPAN, Sigfox[4], Thread[5], LoRaWAN[6].

NFC (Near Field Communication - http://nearfieldcommunication.org/) is RFID based technology for contactless data exchange using electromagnetic induction in range of 10 cm at a rates of 106, 212 or 424 kbps [7].

BLE is Bluetooth 4.2 version designed for small chunks of data. Works at 2.4 GHz, has 50-150m range by 1Mbps speed [8].

Zigbee with last version 3.0, is based on the IEEE802.15.4 industry protocol at 2.4 GHz that require low data rates of 250 kbps within 100m range. This protocol is robust, scalable and highly secure.

Z-Wave is a low-power RF simple protocol made by Sigma Designs for home use products. Works at 900 MHz frequency within 30 m range at rates of 9.6/40/100 kbps.

6LowPAN is an acronym Ipv6 Low-Power Wireless Personal Area Networks, formed by Internet Engineering Task Force (IETF)[7]. The standard can use number of frequency band across multiple communications platforms. Its specialty is using IPv6, which offers $5*10^{28}$ addresses – practically each connected device can have its own unique IP address [9].

Sigfox is technology designed to handle low rate up to 1 kpbs, but consumes only 50 μW. for communication at range of 30-50 km in rural and 3-10 km in urban environment. For example, the solution COPERNIC (https://partners.sigfox.com/products/copernic) for monitoring of thousands of fire hydrants sending status and timestamp by an email or SMS, runs on lithium battery with estimated lifetime of 10 years. Startup Sigfox was developed in 2009. Today covers 31 countries with more than 7 million registered devices.

Thread is newer protocol based on 6LowPAN, primarily designed as a complement to WiFi on existing IEEE802.15.4. wireless chips as Freescale or Silicon Labs.

[1] Bluetooth Special Interest Group (SIG) – Ericsson, IBM, Intel, Nokia, Toshiba Alliance, https://www.bluetooth.com/

[2] Zigbee Alliance, http://www.zigbee.org/

[3] Z-Wave Protocol, http://www.z-wave.com/

[4] Sigfox, www.sigfox.com

[5] Thread Group, http://www.threadgroup.org/

[6] LoRa Alliance, https://www.lora-alliance.org/

[7] Internet Engineering Task Forces, www.ietf.org

LoRaWAN is another concept similar to Sigfox. It works over WAN area and is designed for low-power bi-directional communication for industrial purpose and smart city solutions. It uses unlicensed public spectrum called the ISM [8] (Industrial Scientific and Medical) frequency band. Its range is 2-5 km in urban and 15 km in suburban environment, at rates of up to 50 kbps. As well as Sigfox, LoRaWan is world-wide present, with more than 150 on-going trials and city deployments and more than 400 members in the Alliance. Korea's ICT giant Samsung, together with Korea's Telecom is building nationwide LoRaWAN IoT network, covering 99% of the population in South Korea.

Proposed IoT strategy to operators is to offer hybrid technologies (See Table 2). For applications that need long range and high data rates, there are existing networks such a cellular, LTE or WiFi (15% of IoT market). Short range technologies as ZigBee, NFC, Z-Wave, BLE should be used for short range systems such a smart meter systems, buildings, parking systems etc., and in this cases, it is possible to use hubs to aggregate metering devices and send data to the cloud (40% of IoT market). Nevertheless, to meet long range coverage it is necessary to use low-power WAN devices with low data rate and low cost (45% of IoT market).

Range	Long	Short	Long
Data rates	High	Low/High	Low
Market share	**15%**	**40%**	**45%**
Technology	Cellular, LTE, WiFi	ZigBee, NFC, Z-Wave, BLE	LoRa, Sigfox, 6LowPAN

Table 2: Technology usage

Here listed technologies are all based on the RF communication, and hacking a radio connection can be performed without physical access to the device. The attacker has unlimited time to try to perform malicious operation. A good protected radio communication would be a first line of defense against hackers. Second line of defense is to keep data signed with encrypted fingerprint, using hashing mechanisms as well as asymmetric mechanisms for encryption. Asymmetric mechanisms can also be used for authorization and authentication. Firmware and internal programs should be stored in the internal memory rather than to external memory and also protected with some locking mechanisms, similar to hard drive encryption software. In this way, the attacker has limited access to the communication interface through hardware using for example oscilloscope or logic analyzer. This keeps the data stored in internal memory safe and protected from unauthorized access.

IV. IMPACT OF IOT TO THE INDUSTRIAL SECURITY

Traditionally, cyber security for Information Technology (IT) focuses on the protection required to ensure the confidentiality, integrity, and availability of the electronic information communication systems. IoT imposes that cyber security must include a balance of both cyber system technologies and processes in IT and industrial system operations and governance.

For example, in the power industry, the focus has been on the implementation of equipment that could improve power system reliability [9]. Until recently, communications and IT equipment were typically seen only as supporting service. However, the distinction is getting less and less visible (OT – Operational Technology and IT Network Integration). For example, electricity transmission system operators face the challenges of adopting large amounts of energy coming from renewable sources. Many of renewables are inherently volatile and thus difficult to predict and plan. New methods and algorithms of planning had to be adopted to maintain the grid reliability. All this could not be done without the support of evolving IT technologies.

Supervisory control and data acquisition (SCADA) is an information system architecture that uses computers, networked data communications and graphical user interfaces for high-level industrial, infrastructure or facility processes supervisory management.

SCADA systems are used to control and monitor physical processes, examples of which are a transmission of electricity, transportation of gas and oil in pipelines, water distribution, traffic lights etc. The security of these SCADA systems is important because compromise or destruction of these systems can have an impact on multiple areas of society. Other systems for automatic meter reading or planning usually extend basic SCADA functionalities.

We can roughly speak of three phases of SCADA system evolution. At the beginning, SCADA systems were standalone with proprietary protocols and completely isolated thus making everything intrinsically secure.

The next phase included increased number of connections between SCADA systems, office networks and the Internet which made them more vulnerable to types of network attacks that are relatively common in IT world.

Today with the increasing availability of cloud computing, SCADA systems have adopted Internet of things technology to significantly reduce infrastructure costs and improve ease of maintenance and integration. As a result, SCADA systems can now report state in near real-time and use the horizontal scale available in cloud environments to implement more complex control algorithms than are practically feasible to implement on traditional programmable logic controllers. All these changes imply many new threat vectors to a modern SCADA system.

[8] ITU – United Nations specialized agency for ICT, http://www.itu.int

SCADA systems may differ. But from a security point of view, they can be broken down into the components that are present in every system in some form. A typical SCADA system consists of four elements.

Data acquisition includes sensors, meters and field devices, such as photo sensors, pressure sensors, temperature sensors and flow sensors. For example, in sensor accepting modifications without sufficient checks may cause the system to default to a failsafe condition. Another example could be unsecure energy meter reading devices allowing the unauthorized users to change the internal data.

Conversion and control include devices like remote terminal units (RTU), intelligent electronic devices (IEDs) and programmable logic controllers (PLC). Remote terminal units connect to sensors and actuators in the process, and are networked to the supervisory computer system. Programmable logic controllers are connected to sensors and actuators in the process, and are networked to the supervisory system in the same way as remote terminal units but have more sophisticated embedded control capabilities. Unauthenticated ports could allow modification of memory and logging. This can allow attackers to change system configuration and furthermore remove log records that indicate system change to hide malicious activity.

Communication infrastructure connects the supervisory computer system to the remote terminal units and programmable logic controllers, and may use industry standard or manufacturer proprietary protocols. Failure of the communications network does not necessarily stop the process controls, and on the resumption of communications, the operator can continue with monitoring and control. Some critical systems will have dual redundant data highways, often cabled via diverse routes. A theoretical attacker could (if gained access to the unencrypted network) retrieve sensible industry data.

The supervisory computer is the core system component responsible for gathering process data and sending control commands to the connected devices. To increase the integrity of the system the multiple servers it can usually be configured in dual configurations.

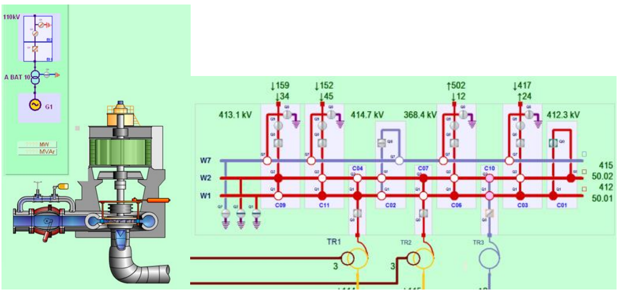

Figure 5. Screenshots from NetVision SCADA HMI

The human-machine interface presents process information to the operating personnel graphically in the form of mimic diagrams, which are a schematic representation of the process being controlled, and alarm and event logging pages (See Fig. 5).

The interface is linked to the SCADA supervisory computer to provide live data to drive the mimic diagrams, alarm displays and trending graphs. Typically, it also includes a drawing program that the operators or system maintenance personnel use to change the way these points are represented in the interface as well as historian database which accumulates time series, events, and alarms data which can then be used to populate graphic trends etc.

Majority of all SCADA vulnerabilities fall in this category. Most SCADA vendors are shifting to web based HMIs. As a result, a lot of web related vulnerabilities could affect this component. Also, traditionally IT system administrators have unrestricted access to all the system databases allowing them the possibility to change or share the data outside the organizational security perimeter.

	Traditional	**Modern**
Communication	Proprietary protocols and networks	Standard protocols and Public Networks
Systems	Custom HW and SW Centralized Architectures Physical Access	Commercial Off-The-Shelf Distributed Architectures Remote Access
Human resources	Employee	Outsourcing
Risk level	Lower	Higher

Table 3.: SCADA evolution

Traditional isolated SCADA system have security implicitly applied to it by keeping the very tight border between who has access to what particular SCADA function or data together with the dedicated secure communication channels (see Table 3.). The focus was on keeping thing tightly coupled and locked as much as possible. On the other hand, in modern systems number of different types of connections within and across network boundaries continue to grow at an accelerating rate, opening new points of exposure. The introduction of IP-based technology and general-purpose computing devices into operational environments is introducing new vulnerabilities along with their benefits. The focus is now on large scale IoT data integration and sharing information as much as possible. Now it is not only the protection of the core SCADA functionalities which has to be secured from cyber-attacks we also have to deal with security at the data layer. For example, settlement data is the pillar of modern energy market structure and can be affected with targeted subtle security attacks affecting metered data [11].

Technologies (tools, strategies) available to protect the control system:

- Access controls – authentication and authorizations at functional and data level, including industry topology segmentations
- Bidirectional gap (e.g., firewall) between control systems and rest of network
- Application whitelisting - to control which applications are permitted to install or execute on a specific host
- Anomaly detection tools
- Patch management / upgrade services
- Vulnerability scanning
- Security awareness training for staff, contractors and vendors
- Asset identification - visibility of components within the control system equipment and network activity
- Antimalware/Antivirus
- Assessment and audit
- Continuous Monitoring and log analysis
- Data forensics

The energy sector benefits from a head start. From the very beginning, cybersecurity was a key requirement of the Smart Grid initiative and significant efforts have been invested in defining requirements that have been formalized in reports such as the NIST 7628 Guidelines for Smart Grid Security. While these guidelines do not address the IoT per se, they do define the cybersecurity requirement for applications in the energy sector, from generation plants to customer premises. Furthermore, many utilities are required to meet the NERC CIP cybersecurity standards and have thus acquired valuable experience in protecting their assets.

The most common vision of IoT is thus for a loosely coupled network of devices and sensors that publish their data through a messaging architecture using web services and messaging protocols such as Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Data Distribution Service (DDS), and Advanced Message Queuing Protocol (AMQP). Besides AMQP, most of these protocols are not yet widely used. The AMQP protocol is used in the financial industry and supports a transactional model, making it more complex and not appropriate for edge devices. To our knowledge, none of these protocols are used in energy sector automation systems and devices.

IoT evolution will certainly force the industrial system architectures to change significantly. The idea is to abandon the monolithic and monolithic like designs and replace it with the more natural and simpler design paradigms which can more easily be formally checked for security deficiencies. We can think of sensors and actuators as a primary service providers in a networked environment. By using the data which those primary services provide we can add additional services to the network (secondary services) which can then be further combined or exploited by adding new services. Formally we designed a graph of interconnected nodes. Nodes represent services and edges represent the data flows between them (service dependencies). If we further exploit that idea we can easily connect the IoT with the newest information system architectural patterns of today. First major pattern is using microservices as an architectural model for the deployment of lightweight and loosely-coupled services and the second is the adoption of containers instead of virtual machines for certain types of workloads and thus benefit from the more efficient resources usage as well as easier deployment operations. Both introduce more visibility into the services topology, versions tracking, logging errors etc. This implicitly improves security model by increasing visibility, resiliency and elasticity of the system. What we described is implementation of a more agile design for failure concept where the system is structured in a way that in case of service failure the effect of the compromised service is minimized.

Another benefit of that kind of approach is the side effect of reducing the dependency on the network itself. The service nodes take on a greater role in terms of processing and behavior without hard-coding it in the communication layer (as was the case in Enterprise Service Bus component of the Service Oriented Architecture).

V. CONCLUSION

As IoT brings numerous new possibilities it is expected to be widely applied to industry and home solutions. As it integrates various internet technologies – powerful devices capable of sensing, processing and exchanging data, new low-energy communication protocols, big data and cloud systems it is obviously very important to use existing security technologies for dealing with security issues. But in the future, we will have to address this problem further by moving to a more systematic approach to IoT security. More work will have to be done in the area of communication standards of consumer IoT products as well as enforcing them. Also, new methods for testing the formal security in communication protocols will probably emerge as well. Data forensics as a tool to pinpoint and understand the subtle changes (potentially unauthorized) in the sensor data received from the smart devices is already widely used through the industry.

Systems today are reusing and repurposing existing technology in conjunction with newer, more IoT aware solutions. This is obviously only the first step towards fully interconnected IoT network.

VI. REFERENCES

[1] K. Ashton, “Internet of Things”, RFID Journal 06/2009, online available:

[2] N. Hughes, “The Internet of Things Explained”, 2014, Picture source online available: https://www.linkedin.com/pulse/20140804163105-98377657-the-internet-of-things-explained

[3] R. van Kranenburg, “The Internet of Things: A Critique of Ambient Technology and the All-Seeing Network of RFID”, The Netherlands Institute of Network Cultures, 2007

[4] L. Coetzee, J. Eksteen, “The Internet of Things – Promise for the future”, IST-Africa 2011 Conference Proceedings

[5] D. Evans, “The Internet of Things”, 2011, online available: http://blogs.cisco.com/news/the-internet-of-things-infographic

[6] CompTIA, “Sizing Up the Internet of Things”, 2015, picture source online available: https://www.comptia.org/resources/sizing-up-the-internet-of-things

[7] X. Jia, T. Fan, Q. Lei, “RFID Technology and its application in IoT”, 2nd IEEE Int. Conf. Consum. Electron., CECNet China, 04/2012, pp. 1282 – 1285

[8] J. S. Kumar, D.R. Patel, “A Survey on Internet of Things: Security and Privacy Issues”, International Journal of Computer Applications Vol. 90 – No 11, 03/2014

[9] “Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol NFCIP-1”, ISO/IEC 18092:2004 Information technology, 11/2011, online available: http://www.iso.org/iso/catalogue_detail.htm?csnumber=38578

[10] “Bluetooth low energy wireless technology backgrounder”, Nordic Semiconductor, 03/2011

[11] IETF Technical Documentation for 6LowPAN, online available: https://datatracker.ietf.org/wg/6lowpan/documents/

[12] Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security, 09/2010

[13] White Paper WP152016EN, The Internet of Things and the energy sector: myth or opportunity, Power and Energy Automation Conference Spokane, WA March 8–10, 2016

[14] Saša Radomirović, “Towards a Model for Security and Privacy in the Internet of Things”