sciendo

IoT Communication Security Issues for Companies: Challenges, Protocols and The Web of Data

Alin ZAMFIROIU
Bucharest University of Economic Studies, Bucharest, Romania
National Institute for Research- Development in Informatics Bucharest
alin.zamfiroiu@csie.ase.ro

Bogdan IANCU
Bucharest University of Economic Studies, Bucharest, Romania
bogdan.iancu@ie.ase.ro

Catalin BOJA
Bucharest University of Economic Studies, Bucharest, Romania
catalin.boja@ie.ase.ro

Tiberiu-Marian GEORGESCU
Bucharest University of Economic Studies, Bucharest, Romania
tiberiugeorgescu@ase.ro

Cosmin CARTAS
Bucharest University of Economic Studies, Bucharest, Romania
cosmin.cartas@csie.ase.ro

Marius POPA
Bucharest University of Economic Studies, Bucharest, Romania
marius.popa@ie.ase.ro

Cristian Valeriu TOMA
Bucharest University of Economic Studies, Bucharest, Romania
cristian.toma@ie.ase.ro

Abstract. *This article analyzes and highlights the security perspective of Internet of Things (IoT) connected devices and their communication challenges, as IoT is considered one of the key emerging fields in Industry 4.0. The IoT architectures can consist of physical systems, virtual ones or even hybrids, combining a collection of different physically active things, sensors, cloud services, specific IoT protocols, communication layers, users and developers. On top of all, it is the business layer, because the scope of the entire IoT environment is to deliver data, to monitor and to facilitate the management of complex processes. In order to facilitate the data exchange between the IoT layers, there have been developed a series of protocols particular to the IoT domain. As in many IT related fields, the solutions are not perfect from the data security and privacy perspectives, many challenges being still open research issues. As the two concepts of IoT and Cloud of Things are connected, bringing real world data into the Cloud to process it, raises Cloud Computing security concerns regarding the privacy and security of data. Although in recent years, many efforts have been made to improve Cloud Computing security, there are risks that need to be taken into consideration. From the Web of Data's point of view, things are even more prone to security risks. Because privacy is one of the fundamental right of digital users, it is extremely important for new technologies to comply with privacy regulations and policies, such as the new European data protection*

DOI: 10.2478/picbe-2020-0104, pp. 1109-1120, ISSN 2558-9652| Proceedings of the 14th International Conference on Business Excellence 2020

and privacy frameworks. In this context, companies must take into account standards, challenges and new trends in IoT. In the absence of specific measures, raw or processed data can be easily stolen from the Web of Data. In this paper we analyze and present the main protocols of communication in the IoT field from a data security perspective. Also, we do a review of the main architectures that can improve the security of the communication between IoT devices and the Cloud data storage.

Keywords: IoT, security, communications, Industry 4.0, business digitization, protocols, web of data.

Introduction

Various articles such as Xu et al. (2018) or Bologa et al. (2017) consider that mankind is already in the midst of an industrial revolution, this period being known as Industry 4.0. The evolution of modern technologies, the fast implementation of automation and the exchange of data within the manufacturing technologies represent the main vectors that delimit the current period as a transition from the third industrial revolution to the fourth (Bologa et al., 2017).

The idea of Industry 4.0 started from the current trend of automation and data exchange in manufacturing technologies (Kagermann et al., 2013). At the base of it are Internet of Things (IoT), cyber-physical systems, cloud computing, artificial intelligence (AI) and machine learning (ML) based solutions, as well as other emerging technologies. And, no matter the socio- economic field considered, the core characteristic of the new industrial evolution is the data, which can be collected in real time from almost any system and can be stored indefinitely without any limit. All these trends have been facilitated by the fast evolution of Internet networks, digital communication channels and devices and by the continuous decrease of computing power and data storage costs. In parallel, hardware devices have become smaller, more affordable and able to communicate in real time despite their limited computing power. Nowadays, you can measure and collect data in real time, with affordable costs, for almost any business. Theoretically, and practically, it is possible to monitor and control all the processes of a business by using software robots, cloud services and a wide range of IoT devices. This article focuses on IoT and analyzes the main issues of interest related to communication security in IoT, from the companies' perspective.

Lower costs for sensors as well as the introduction of broadband radio access technology (LoRaWAN) have substantially contributed to the massive development of the usage of smart devices in an IoT architecture (Raman, 2017). The basic architecture for IoT systems is based on four layers as shown in Figure 1:

- Sensors – includes the wide range of Smart devices that have at least limited computing power and communication capabilities. Minimally the sensor is able to monitor a specific event, record its data and sends it to a remote database or service. Optionally, the sensor can be control in a certain degree by the remote service.
- Network – represents the hardware infrastructure that allows devices to connect to remote sensors. Table 1 describes different communication technologies that define this layer.
- Middleware – is the transparent layer, based mostly on software services that link the components together; This layer incorporates the data flow as it records the data, process it into results and manages the digital requests flow from other services or from end-users.
- Data-using applications – incorporates the business logic of the entire solution. It allows clients and other services to query processed data and to interact with the entire system. At this level end-users have the possibility to see the data, either raw or processed by other means.

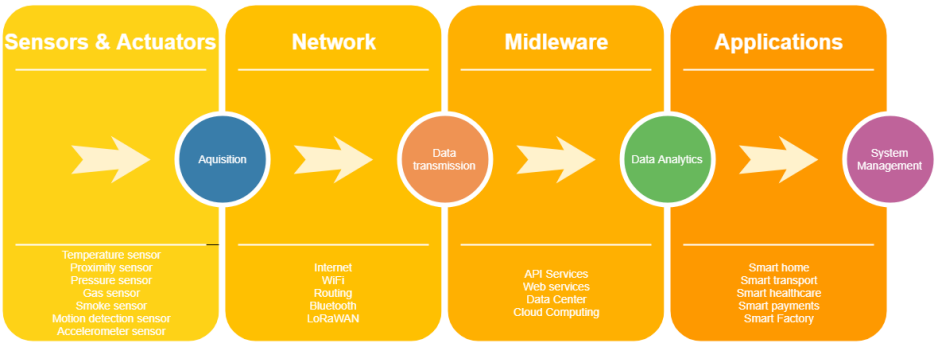

Figure 1. Layers of IoT Architecture

Wireless communications technologies facilitate the exchange of data and the interaction between remote devices. Table 1 describes the main communication technologies used in IoT, illustrating both technologies specifications as well its costs levels. As a comparison, the NFC (Near Field Communication) tags are becoming omnipresent in many industries, such as food, retail, fashion, etc, because their cost is almost zero. At the other boundary, a device that is capable to communicate over 4G data networks requires a dedicated module and also involves a cost of using the service itself, provided by a telecommunications company.

Table 1. Wireless communications technologies

	NFC	RFID	Bluetooth	WiFi	ZigBee
Distance	<10cm	<3m	<30m	4-20m	10-300m
Speed	400kbs	400kbs	700kbs	10-100mbs	250kbs
Network	PAN	PAN	PAN	LAN	LAN
Topology	P2P	P2P	Star	Star	Mesh, star, tree
Applications	Payments, access, settings	Object tracking	Data network	Internet, multimedia	Sensor network, industrial automation
Power	Very Low	Very Low	High	Low-High	Very Low
Costs	low	low	low	medium	medium

	WirelessHart	6LoWPAN	WiMax	3.5 - 4G
Distance	225m	800m	50km	Cellular network
Speed	250kbs	250kbs	10-110mbs	7.2-100mbs
Network	LAN	LAN	MAN	WAN
Topology	Mesh, star	Mesh, star	Mesh	Mesh
Applications	Industrial sensor networks	Construction of sensor networks	Broadband internet connection	Mobile phones, telemetry
Power	Very Low	Very Low	High	High
Costs	medium	medium	high	high

Sources: Sahmim & Gharsellaoui (2017); Rose Mary (2013); Svetoslav (2013); Goldsmith (2005).

When choosing technologies, companies make decisions based on costs, benefits and performance reports. IT projects are influenced by the technologies used and especially by the IoT technologies. As new IoT technologies are easily integrated into different business, without proper testing or analysis, in certain circumstances there is the possibility to insert vulnerabilities in the entire system, even if they were audited before. Therefore, companies are subjected to new threats

by integrating these technologies in secure systems. Figure 2 shows the architecture of a data protection system and a secure communication system. The same data security principles have been implemented in similar architectures proposed by Rose Mary (2013) and Tedeschi et al. (2017).

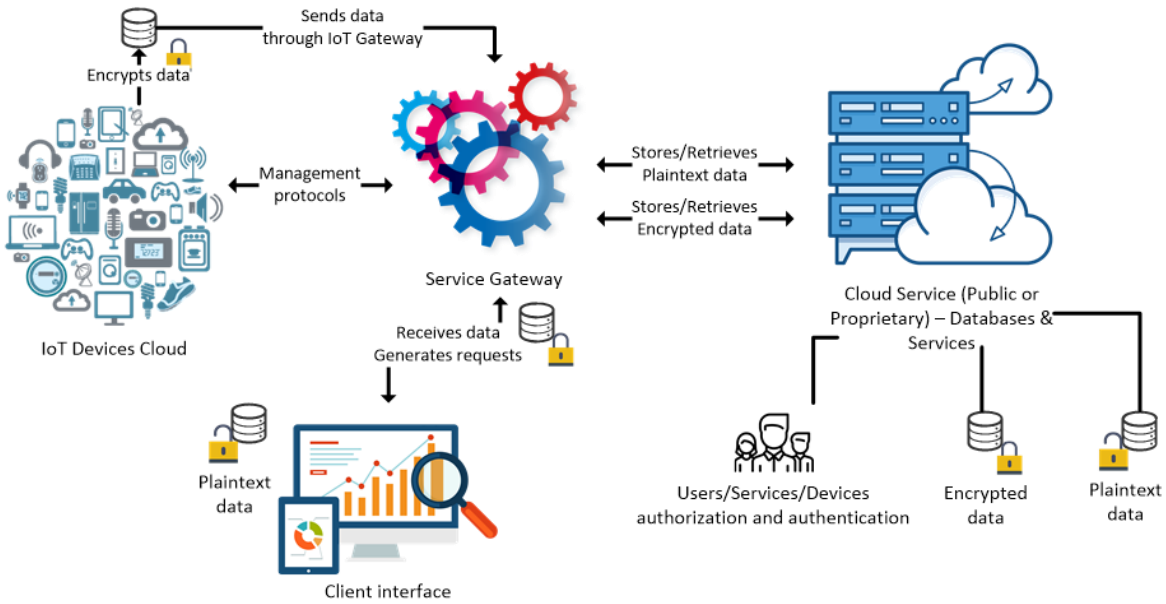

Figure 2. Data protection system and secure communication architecture for an IoT environment

The starting hypothesis of analyzing an IoT ecosystem is that the collected data is not stored in the IoT sensor, but it is transferred to the storage units and it is made accessible only to accredited persons through the cloud services. The IoT devices have limited to none storage capacity and because they have limited computing power they are not able to implement complex services, being limited by their overall performance.

In order to protect the data over the communication channel, the system uses a combined solution based on the HTTP protocol and an encryption mechanism, such as Secure Sockets Layer (SSL). The acquired data is therefore transferred securely to the cloud system over a public network. The SSL protocol itself offers guarantees of the security of the connections.

The next sections presents the key points of the IoT systems security and their impact on the company overall system. The third section is dealing with used protocols in IoT communication and the security of these protocols. The fourth section presents the integration of Web of Data and the new trends in the technology. The paper ends with the presentation of the new directions in IoT, conclusions and future work.

Challenges of the IoT

This section discusses the main challenges of IoT communication security for companies. Besides the general cybersecurity aspects, the IoT model has a number of features that generate specific challenges. As IoT objects communicate through wireless technologies and are integrated in the company system, the attackers that are succeeding in attacking them may gain a facile access to the network. Moreover, due to their increase in popularity and also due to their real advantages, the average number of connected objects in an IoT network is growing. Not only the large number of objects in a network can increase the likelihood of vulnerabilities occurrence, but also their diversity. Being in the same IoT environment, once an attacker gains control over one node, he can

carry out malicious activities towards other devices (Khan et al., 2019) or the system itself. It is well known the case of the hacker that was able to gain access in a secure casino system by hacking the thermometer of a fish tank placed in the lobby (Wang, 2018). A very expensive and complex system has been compromised because of a single cheap IoT device. In 2019 was estimated that the IoT world had 25 billion devices interconnected and by the year 2025, it is expected to grow to about 60 billion (Balaji et al., 2019).

Besides the wide distribution and variety of nodes, IoT devices are usually low-power, with small memory and limited processing capability. As a consequence, it is not feasible or is not possible entirely to incorporate malware protection or any security measures on most of the IoT devices. As IoT devices are characterized by resource-constrained nature, the security solutions used on traditional networks cannot be easily implemented on IoT networks (Hameed et al., 2019). Based on these constraints, the IoT communication challenges can be classified in 3 categories:

1. security related;
2. reliability or Quality of Service (QA) related;
3. efficiency related.

Improving one of the three, may decrease at some level one or both the other two. This is usually the case with cybersecurity, where increased security measures can slow down a system's performance (Zhang et al., 2019).

Another key cybersecurity problem that companies need to address is the users' poor security knowledge, digital security awareness culture, as social engineering remains one of the most common cyberattacks. This is also the case in IoT, where users can easily compromise an IoT environment, by connecting unsecure devices to it, or connecting a device from the environment to unsecure networks. Security misconfiguration of devices can make them publicly accessible, which can offer the hackers the entrance gate to the entire IoT network. Therefore, security awareness is a key aspect to ensure good overall security in IoT. This should be taken even more seriously considering that the IoT market is in full progress and more and more diversified devices are created, which users are eager to adopt (Ahmad et al., 2019). The most common risks of successful attacks in IoT networks usually consist of data theft, but there are also many IoT solutions which, if compromised, they can put users in real danger (e.g. medical devices, smart cars). When addressing IoT security it is important to take into account the impact they can have on the human lives (Yaqoob et al., 2019).

Given the characteristics of IoT environments, Hameed et al. (2019) identify several challenges regarding IoT communication:

a. from a privacy point of view, securing data transmission is crucial, as some IoT devices store sensitive information about things and people;
b. other challenges are connected with proper securing of routing and forwarding in IoT. The key aspects are securing route establishment, isolate malicious nodes from the network and self-stabilization of the security protocol;
c. another key aspect refers to the necessity of lightweight cryptographic solutions, considering the resource constraints of IoT devices;
d. DoS/DDoS (CISA, 2019) are important challenges, as they are some of the most common attacks in IoT. Resource efficient DoS/DDoS attack detection, as well as resource efficient countermeasures are required;
e. as IoT environments involves many devices connected in networks, insider attack detection is an important issue to be considered. The challenges are considerable, as if one wants to implement such solutions in IoT networks, they have to be resource efficient.

Security of used Protocols in IoT communication

When adopting new IT technologies, one of the main concerns for the companies is to make sure that their systems are secure. The most common approaches used in IoT communication are implemented over HTTP (Fielding et. al., 1999) or based on an event strategy. When it comes down to data transfer there is a set of key factors that needs to be checked: usage of bandwidth, power consumption, failover and security. Implementation of these items can generate some tradeoffs depending on the functional requirements that needs to be satisfied (Lea, 2016).

HTTP communication in IoT systems

IoT architectures that are built over HTTP work in a client-server manner. The actors are transferring information by using the known methods GET, POST, PUT and DELETE. In order to obtain the data produced by one of the clients from the system a GET operation should be performed by the main server. The server should be the single source of trust for the clients and it should be the only party that knows all the available resources to be consumed. The most popular protocols that are built over HTTP for IoT are CoAP and XMPP.

Event-based communication in IoT systems with light protocols

Using the HTTP protocol has the benefit of using the existing Internet infrastructure but this is comes with a cost. The protocol requires computing power and is not efficient for most IoT devices. An alternative, is to use a dedicated lightweight protocol, like MQTT (OASIS , 2019), one of the most used event-based protocols.

Adopting an event-based implementation for an IoT system involves a message broker and publishers. Even though multiple publishers can send messages to a single broker, the devices are allowed to communicate with each other. Depending on the number of fields sent over the network the payload size increases significantly but if the same connection is used to send multiple messages will result in performance benefits over HTTP with the keep-alive header set. Figure 3 illustrates a comparison between HTTP and MQTT. The differences will influence the communication speed, the cost of the IoT device and the cost of the service.

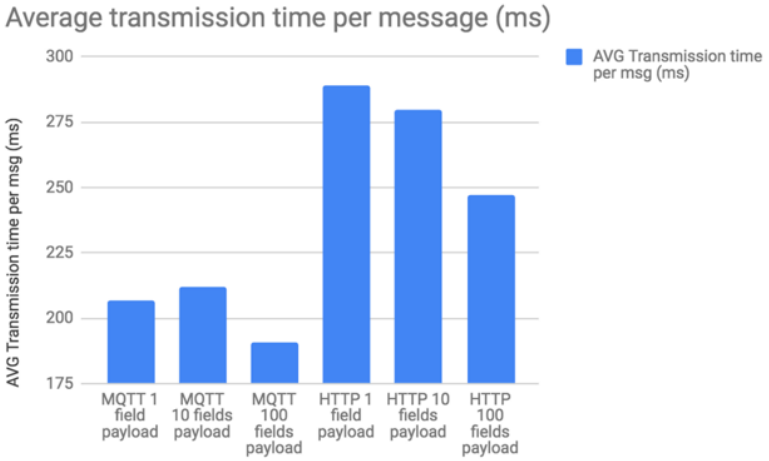

Figure 3. Performance measurement of MQTT vs HTTP

Source: https://cloud.google.com/blog/products/iot-devices/http-vs-mqtt-a-tale-of-two-iot-protocols.

Security challenges

The main security threats of all the used protocols for IoT derive from the following aspects: authentication, authorization and package encryption (Russel & Van Duren, 2016).

By default, the messages transferred over the network are not secured in any way, being sent in plaintext. TLS is used to secure the connections but that can lead to overheads related to bandwidth and CPU.

For authentication the cryptographic secure solution is to use Public Key certificates, as X.509 certificates, from a trusted certificate authority and avoid self-signed certificates instead of a basic username and password mechanism. An attacker can easily obtain the certificate from a device firmware and even easier the account credentials if no additional enhancements are implemented (Guzman & Gupta, 2017).

Setting up the authorization for each node of the system is a key factor for accessing the exposed resources. Even if a node is compromised it shouldn't have the permission to perform any malicious operation that can affect the system.

In terms of confidentiality, providing appropriate authorization roles and policies, transparently ensuring that only authorized persons have access to sensitive data, is still a challenge, especially when data integrity must be ensured in response to authorized changes.

The Web of Data

New technologies are nowadays key drivers for obtaining strategic advantages in many industries. Therefore, companies need to be extra watchful on new trends in technology.

The Web of Data started as an idea of the creator of the classical web, Tim Berners-Lee. As the web grew larger and larger, he realized that it would be harder and harder for the machines to understand it. So he proposed a new kind of web, generically called semantic web (Berners-Lee et al., 2001), where the machines can also understand the documents' content. In order to achieve this, the documents must be enriched with specific meta-data written in some specific formats. Depending on the type of format, Tim Berners-Lee even proposed a five-star system to rank the openness of data (Berners-Lee, 2006). Nowadays, DBpedia is arguably the largest collection of open linked data, being considered the nucleus of Web of Open Data (Auer et al., 2007).

But we are living a paradigm shift. In the following years the number of smart devices (things) connected to Internet will probably overcome the number of computers. Therefore, besides the classical web, organizations need to consider Web of Things (WoT) with its own advantages and drawbacks.

Some authors are going a step further and even propose a Semantic Web of Things (SWoT), a place where things can seamless communicate with one another by using specific meta-data (Jara et al., 2014). By doing this, a worldwide ecosystem of smart devices is created, a place where things can exchange, extract and process data with the scope of taking intelligent decisions. In fact, intelligent computing can be defined as the intersection of cognitive, semantic and perceptual computing paradigms (Sheth, 2016). Figure 4 depicts the evolution towards SWoT.

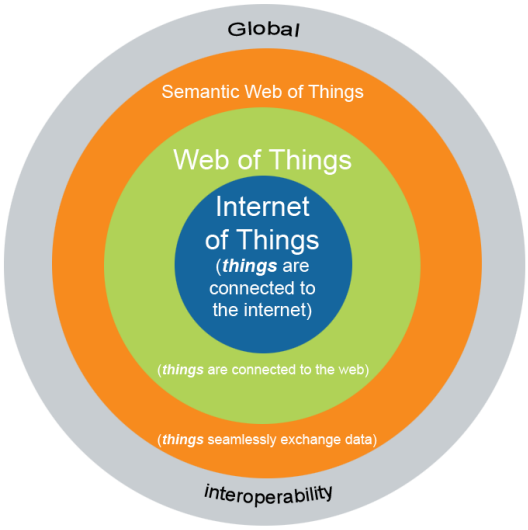

Figure 4. The evolution towards Semantic Web of Things and global interoperability
Source : Jara et al. (2014).

The biggest challenge that the "things" are facing right now in order to be connected to the WoT consists in the heterogeneous data sources and data formats. Constrained Application Protocol (CoAP) seems to be the optimal existing solution for resolving this problem (Jara et al., 2014). In a nutshell, CoAP is an open standard for building embedded RESTful web services optimized for IoT devices with limited capabilities. Another project aimed for linking things which are using different technologies to the WoT is Node-Red (Blackstock & Lea, 2014). The two projects don't necessary exclude each other, libraries for generating CoAP code from Node-Red being already developed (Ažna, 2017). As the IoT industry develops, more and more standards will be adopted.

But all this openness, comes with a risk, each and every IoT network administrator being in charge with the anonymization of public data. As we are facing similar issues nowadays related to social networks and personal data, maybe a solution found for this field can be adapted to work for WoT, too.

With this in mind, we can conclude that the road towards SWoT just started and, as usual, nobody can predict exactly what turns it might take at different crossroads or if it will leverage existing technologies or make use of new ones. Nevertheless, European projects created with the scope of sematic integration of the IoT devices are ongoing (Jara et al., 2014): OpenIoT, SENSEI, IoT-A and IoT.est, just to name a few. Future will show to what extent and how fast companies will embrace the web of data.

Securing the Access to Cloud Services

In terms of communication security in the Cloud, since most IoT Cloud solutions support HTTP(s) -REST, then must be considered security elements over the TCP / IP protocol stack.

Representative State Transfer (REST) facilitates communication between computer systems on the web. The implementation of REST is done using the following elements:

- The resources provided by the access director structures in URI format (Universal Resource Indicator).
- Structured files (eg JSON, XML) as a representation of objects and attributes.
- HTTP methods for sending messages on the web (GET - for retrieving resources, POST - for creating resources, PUT - for updating / modifying resources, DELETE - for deletion).
- The session status is maintained only by the clients.

The REST-ful API offers high flexibility to software developers for designing, implementing and maintaining applications, due to the state-of-the-art protocol principles and REST modularity. RESTful APIs are suitable for web applications, but are also successfully used in the implementation of cloud computing and micro-services.

Since REST services are used on the web, security must be the main concern and challenge for the implementers and integrators of REST-ful applications. According to OWASP (Open Web Application Security Project), the following technologies and security measures can be used when RESTful APIs are implemented for IoT cloud solutions:

- Using HTTP (S) - HTTP secure - is mandatory because the RESTful API transmits sensitive web information related to passwords, API keys, tokens (tokens), JSON Web (JWT), etc. to authenticate IoT devices or IoT gateways to the Cloud infrastructure. This information must be protected by encryption on the transport level of the computer network infrastructure. HTTPS must be implemented by both IoT client devices and Cloud servers.
- Access control - is implemented for each REST endpoint and is linked to authentication and authorization. For reasons of efficiency, access control decisions are made locally by the REST endpoint, and access tokens / tokens are issued by a centralized server that acts as an identity provider. There are different protocols that need to be used to manage access control to the cloud infrastructure.
- JSON Web Tokens (JWT) - represents the JSON data structures used by the RESTful API for access control. The JWT must be protected by encryption or message authentication code (MAC) to avoid lack of integrity. JWT is an RFC document that d scribes security requirements, constraints and considerations and provides examples for them. The JWT must be validated against the integrity and claims contained therein.
- API access keys - are used by the endpoint to create HTTP requests to the server. API keys are unique byte streams and are usually included in the request HTTP header or URI itself. However, the second approach will expose the key in browser history and server-level API logs. API keys are a security REST implementation for the public cloud infrastructure where there is no strict control over access to it. Therefore, endpoint accesses are limited to those with API keys. Also, certain access filters are applied, depending on the final category of the client.
- Restrictions applied on HTTP-REST methods - not all terminals (endpoints / clients, software devices and IoT hardware) have access to all RESTful services provided by the Cloud infrastructure. This is implemented by restricting some HTTP REST methods or by creating blacklists of endpoints / terminals / client, software devices and IoT hardware.

Conclusions

As the cost of storing data is very low, business are recording almost everything about their user's behavior, about their processes parameters, inputs and outputs. The real costs are given by the complex and processing intensive task to process that data in order to extract meaningful results. Despite this real limit, it is a good strategy to store any data. Even if you can't process it now,

maybe others are able to do it for you or you will have the necessary resources in the future. Since the adoption of Internet as a digital extension of real life, businesses were able to get data either from monitoring users behavior or by manually inserting data recorded by other means. That was offering a narrow perspective and was also time consuming. In some industries, like oil and gas, maybe it was not even possible to manually record different data and manually insert it in decision making systems in real time. Today the evolution of the IoT environment, mainly because the recent advances in hardware manufacturing on top of the existing Internet infrastructure of services, is giving business the opportunity to monitor almost everything in real-time. All these advantages come with another problem. The digital data is more and more valuable and losing it can endanger the business itself. IoT breaks physical limits but it will also increase the complexity of digital systems and services, affecting in complex ways, sometimes not obvious, the security of the entire system. Securing data and digital services is a cost that business need to pay in the digital era and protecting IoT devices will increase that cost as more security risks need to be taken into account.

Acknowledgments. This paper presents results obtained within the PN-III-P1-1.2-PCCDI-2017-0272 ATLAS project ("Hub inovativ pentru tehnologii avansate de securitate cibernetică / Innovative Hub for Advanced Cyber Security Technologies "), financed by UEFISCDI through the PN III – "Dezvoltarea sistemului national de cercetare-dezvoltare", PN-III-P1-1.2-PCCDI-2017-1 program.

References

Ahmad, M., Younis, T., Habib, M. A., Ashraf, R., & Ahmed, S. H. (2019). A review of current security issues in Internet of Things. In Jan, M.A., Khan, F., Alam, M. (Eds.). *Recent Trends and Advances in Wireless and IoT-enabled Networks*(pp. 11-23). Springer, Cham.

Auer, S., Bizer, C., Kobilarov, G., Lehmann, J., Cyganiak, R., & Ives, Z. (2007). DBpedia: A Nucleus for a Web of Open Data, The Semantic Web. *ISWC 2007, ASWC 2007. Lecture Notes in Computer Science*, 4825, Springer, Berlin, Heidelberg.

Ažna, J. (2017). *node-red-contrib-coap (git repo).* Retrieved from https://github.com/reederz/node-red-contrib-coap.

Balaji, S., Karan N., & Santhakumar, R. (2019). IoT Technology, Applications and Challenges: A Contemporary Survey. *Wireless Personal Communications*, 108, 363-388.

Berners-Lee, T. (2006). *Linked Data*, *W3C*. Retrieved from https://www.w3.org/DesignIssues/LinkedData.html.

Berners-Lee, T., Handler, J., & Lassila, O. (2001). The Semantic Web. *Scientific American*, 284(5), 34-43.

Blackstock, M., & Lea, R. (2014). Toward a Distributed Data Flow Platform for the Web of Things (Distributed Node-RED). *Proceedings of the 5th International Workshop on Web of Things*, 34-39.

Bologa, R., Lupu, A. R., Boja, C., & Georgescu, T. (2017). Sustaining employability: A process for introducing cloud computing, big data, social networks, mobile programming and cybersecurity into academic curricula. *Sustainability,* 9(12), 2235.

Cybersecurity and Infrastructure Security Agency – CISA (2019). *Security Tip (ST04-015) Understanding Denial-of-Service Attacks. US-CERT*. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-015.

Fielding, R.T., Gettys, J., Mogul, J.C., Nielsen, H.F., Masinter, L., Leach, P.J., Berners-Lee, T. (1999). *Hypertext Transfer Protocol – HTTP/1.1. IETF.* Retrieved from https://tools.ietf.org/html/rfc2616.

Goldsmith, A. (2005). *Wireless Communications*.Cambridge University Press.

Guzman, A., & Gupta, A. (2017). *IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices*. Packt Publishing Ltd.

Hameed S., Khan, F.I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things (IoT): A Review. *Journal of Computer Networks and Communications*, 2019, 9629381.

Jara, A. J., A., Olivieri, A. C., Bocchi Y., Jung, M., Kastner, W., & Skarmeta, A. F. (2014). Semantic web of things: an analysis of the application semantics for the IoT moving towards the iot convergence. *International Journal of Web and Grid Services*, 10(2-3), 244-272.

Kagermann, H., Wahlster, W., & Helbig, J. (2013). *Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry; final report of the Industrie 4.0 Working Group.* Technical, Forschungsunion.

Lea, P. (2018). *Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security.*Packt Publishing.

Rose Mary (2013).*Wireless Communication and types*Retrieved from https://www.engineersgarage.com/articles/wireless_communication.

OASIS (2019). *MQTT Version 5.0 OASIS Standard Specification. OASIS.* Retrieved from https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.pdf.

Raman, N. (2017). *How low-powered Wi-Fi sensors are the future of the IoT, Imagination*. Retrived from: https://www.imgtec.com/blog/how-low-powered-wi-fi-sensors-are-the-future-of-iot/.

Russel, B., & Van Duren, D. (2016). *Practical Internet of Things Security: Design a security framework for an Internet connected ecosystem*. Packt Publishing Ltd.

Sahmim, S., & Gharsellaoui, H. (2017). Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: a review. *Procedia Computer Science*, 112, 1516-1522.

Sheth, A. (2016). Internet of things to smart IoT through semantic, cognitive, and perceptual computing. *IEEE Intelligent Systems*, 31(2), 108-112.

Svetoslav, A. (2013). An Overview of Wireless Communication Technologies Used in Wireless Sensor Networks. *International Scientific Conference eRA-8,*11-18.

Tedeschi, S., Mehnen, J., Tapoglou, N., & Roy, R. (2017). Secure IoT Devices for the Maintenance of Machine Tools. *Procedia CIRP*, 59, 150-155.

Wang, C. (2018). *HTTP vs. MQTT: A tale of two IoT protocols*. Retrieved from https://cloud.google.com/blog/products/iot-devices/http-vs-mqtt-a-tale-of-two-iot-protocols.

Wang, W. (2018). *Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer, The Hacker News.* Retrieved from https://thehackernews.com/2018/04/iot-hacking-thermometer.html.

Xu, L. D., Xu , E. L., & Li, L. (2018). Industry 4.0: state of the art and future trends. *International Journal of Production Research, 56*(8), 2941-2962.

Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. A., & Hong, C. S. (2019). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems*. 92, 265-275.

Zhang, M., Jiang, X. F., & Hodges, S. (2019). Communication Challenges in the IoT. *IEEE Pervasive Computing*, 18(1), 8-9.

DOI: 10.2478/picbe-2020-0104, pp. 1109-1120, ISSN 2558-9652| Proceedings of the 14th International Conference on Business Excellence 2020