Maximilian et al., J Inform Tech Softw Eng 2018, 8:5
DOI: 10.4172/2165-7866.1000250

Journal of
Information Technology & Software Engineering

Review Article Open Access

Cybersecurity Management for (Industrial) Internet of Things: Challenges and Opportunities

Maximilian L*, Markl E and Mohamed A

University of Applied Sciences FH Technikum Wien, Hoechstaedtplatz 6, Vienna, Austria

Abstract

The internet of things (IoT) is about an integration between the physical and the cyber worlds in several aspects of peoples' lives, with benefits of convenience and entertainment in the "smart home" domain, and process optimization, costs savings and business opportunities in the industrial, "smart city" and other domains such as power and health care, however, associated with concerns about security. Security is a must for IoT systems to protect sensitive data and critical physical infrastructure. It is estimated that the number of networked devices will reach 20-50 billion by 2020 on a global scale. Security risks can become expensive (particularly in Industrial Internet of Things (IIoT) applications) and dangerous for corporations, governments and even individuals' lives, and strategies to combat cybercrime are being developed. However, there are 3 main challenges for solving security issues in IoT and IIoT settings: Applications operate in highly distributed environments, heterogeneous smart objects are used, and sensors and actuators are limited in terms of power and computational resources. Therefore, traditional security countermeasures do not work efficiently in IoT systems. A key security challenge in the IoT context is the increase of the overall attack surface for malicious attacks, as compared to isolated (i.e., non-connected) systems. Cybersecurity management has to increase awareness, competence levels and assess novel technologies such as blockchain and SDN (Software Defined Networking). Opportunities are offered by 5G and "green" IoT, particularly with regard to energy and CO_2 emissions savings. This review article discusses the state-of-the-art, trends and developments arounds challenges and opportunities in cybersecurity management.

Keywords: Cybersecurity; Computer security; IT security; Internet of things (IoT); Safety; Industrial internet of things (IIoT); Blockchain and SDN (Software Defined Networking); 5G

Introduction

The internet of things (IoT) aims at seamlessly integrating the physical and digital world into a single system, thereby offering significant business opportunities for many sectors such as healthcare and energy. IoT suffers from several security issues which are often more challenging than those in other fields because of a complex environment and a huge number of devices, which are resources-constrained [1]. The term "IoT" was coined by Kevin Ashton, a UK technology pioneer and author, in 1999. Ashton defines IoT as a system where the Internet is connected to the physical world via ubiquitous sensors [2,3]. The Internet of things (IoT) can be described as the network of physical devices, vehicles, home appliances [4] and other gadgets and devices (mechatronic systems) with embedded electronics, software, sensors, actuators, and connectivity which enables them to connect, collect and exchange data [5] (Figure 1). An important application for IoT is a "smart factory" (Figure 2). In a smart factory, one can distinguish between four main components: person, process, technological ecosystem and intelligent object. It is estimated that IoT applications will generate 1.2–3.7 trillion USD of economic value annually by 2025 in smart factories [6]. IoT extends classic Internet connectivity of computers (desktops, notebooks, smartphones and tablets), to any range of traditionally "dumb" or non-internet-enabled physical devices and kind of "everyday objects" such as fire alarms, fridges, cars and electric hand tools. A survey on Internet of Things architectures [7]. IoT is closely related to Digital Manufacturing, which aims at creating highly customized products with high quality and low costs by integrating Industrial Internet of Things (IIoT), big data analytics, cloud computing [8], and advanced robots into manufacturing plants [9]. The IoT has become omnipresent, with the Internet-of-Medical-Things (IoMT), Internet-of-Battlefield-Things (IoBT), Internet-of-Vehicles (IoV), etc. [10].

Two of the issues that potentially threat IoT devices are the security and the privacy of ex- changed/collected data that are often deeply linked to the life of users [1]. The Security Shield for IoT has been identified by DARPA (Defense Advanced Research Projects Agency) as one of the four projects with a potential impact broader than the Internet itself [6]. The terms "safety" and "security" are often used interchangeably. Many languages, such as Hindi, German and Norwegian, only have one word for them. A working definition and distinction for safety and security is provided by Skavland Idsø and Mejdell Jakobsen [11], who writes that "Safety is protection against random incidents" and accidents. These random incidents (i.e., not intentionally done) are unwanted incidents that occur as a result of one or more coincidences, e.g., from machines to humans. On the other hand, "Security is protection against intended incidents", e.g., the protection of humans and/or machines from harmful, deliberate and planned malicious acts by other people. In other words, it is security measures that can provide safety by preventing malicious activities by people engaged in mugging, burglary, robbery, terrorist activities, etc. These can be directed against individuals, small and large organizations of any kind and government organizations, who are developing policies and programs to enhance security [12]. Security can be seen in various contexts, e.g., physical (airports, corporations, food, home), political perspective (homeland security, public security, etc.), monetary perspective (e.g., social or economic security) and IT realm (e.g., communications, data, network, internet security).

Cybersecurity is also called "computer security" or "IT security".

***Corresponding author:** Maximilian L, University of Applied Sciences FH Technikum Wien, Hoechstaedtplatz 6, 1200 Vienna, Austria, Tel: +43 681 8182 6762; E-mail: maximilian.lackner@technikum-wien.at

Received December 01, 2018; **Accepted** December 25, 2018; **Published** December 31, 2018

Citation: Maximilian L, Markl E, Mohamed A (2018) Cybersecurity Management for (Industrial) Internet of Things: Challenges and Opportunities. J Inform Tech Softw Eng 8: 250. doi: 10.4172/2165-7866.1000250

Figure 1: An Typical architecture of IoT [25].

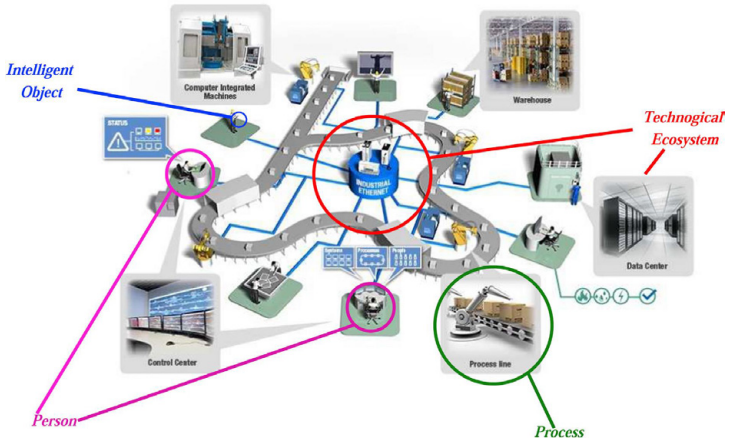

Figure 2: Smart factory. The smart factory environment is composed of persons, smart objects, processes and a technological ecosystem as the main elements of our systemic and cognitive approach for security in the Internet of Things. (©http://www.moxa.com) [6].

The Internet Society states that "as a catchword, cybersecurity is frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and 'solutions' ranging from the technical to the legislative" [13]. The International Telecommunication Union (ITU) defines cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets" [14]. Cybersecurity deals with the protection of hardware, software, data, people, and also the procedures by which systems are accessed, including the physical security of systems and the security of information stored in these. In general, security objectives include confidentiality, integrity and availability, which are also known as the CIA triad in the information security industry [15,16]. Confidentiality means that information is not improperly disclosed to unauthorized individuals or devices. Integrity means that information is protected against unauthorized modification or destruction. Availability describes timely and reliable access to data and information by authorized users [15]. Since the modern world is increasingly relying on IT systems, from desktop PCs to smartphones and other "connected" devices, which altogether form said IoT, society at large is getting more and more vulnerable to various deliberate, malicious attacks. The vulnerabilities by so-called cyber-attacks or hacking include:

Backdoors (a method of bypassing normal authentication or security controls; Backdoors can be included by original design and be added unnoticed by an intruder at a later stage.). Denial-of-service attacks (DoS; loss of access to a system by a user, e.g. by deliberately typing in a wrong password multiple times to enforce a system lock or by blocking all users of a system simultaneously by overloading the network; Techniques exist to do this from multiple IP addresses, e.g. using so-called zombie computers through internet bots).

Direct access attacks (gaining unauthorized access, e.g., to steal data or modify the system); Eavesdropping (listening to private conversations); Phishing ("fishing" for sensitive information such as usernames, passwords, and credit card details, e.g., carried out by email spoofing); Social engineering (convincing users to disclose confidential pieces of information such as passwords, credit card numbers or trade secrets, e.g., by impersonating a senior manager of the corporation, a bank, a postal service company, authorities or a customer, exploiting peoples' gullibility); Spoofing (masquerading as a valid entity through falsification of data (such as an IP address or username).

Cyberattacks can be carried out with different motives by nations, profit-driven cyber criminals, criminal organizations, hackers (black, grey or white hats), hacktivists, extremists and insiders [15].

On a global scale, the average costs of cyber-crime have reached $11.7 million per organization (2017 data) [9].

As technology becomes increasingly ubiquitous in daily life, cybercrime and cybersecurity tools and techniques evolve concurrently [17]. Basically, anything can be hacked. Cyber threats concern personal computers, networks, smartphones, power grids and the entire manufacturing sector [18]. A major reason is the lack of investment in cybersecurity [9]. The Budapest Convention, which came into force in 2004, is the oldest binding and most widely adopted legal instrument in the field of cybercrime [15]. The EU has adopted the following instruments and Strategies to combat cybercrime: the NIS Directive, the General Data Protection Regulation (GDPR) and the EU Digital Single Market strategy (DSM) [15], the first two of which are enforced from May 2018 [19]. Given the near term explosion in the use of vulnerable Internet-connected objects, enhancing security in the IoT is an issue that is critical, urgent and, as with all "cyber" things global [15]. As an example for potential IoT applications, Table 1 shows considerations for smart grids.

The severity of successfully carried out cyberattacks differs between industry; Grids, as key infrastructure element, are particularly vulnerable; Whereas in private, commercial enterprises, the violation of cybersecurity only results in financial losses, cyberattacks on (smart) grids can have an impact on the health, safety or economic situation of citizens or proper functioning of governments [20]. Governments have expressed serious concerns about cybersecurity, and there is a shortage in qualified cybersecurity professionals. [21]. As an example, Singapore has developed a cybersecurity strategy [22]. Healthcare is another vulnerable area. For a review on cybersecurity in healthcare [23]. Two main issues have been identified with cybersecurity in healthcare: There are plenty of valuable data, and defenses are typically weak [23]. Attacks can be directed against hospitals or implanted medical devices, where patient trust is at stake and human lives can be endangered [23]. Threats include trojans, viruses, worms, keyloggers and screen scrapers. Several defense strategies have been developed such as antivirus software, encryption and firewalls. Table 2 shows common vulnerabilities and associated threats. As it can be seen from Table 2, there are multiple threats [9]. Table 3 takes a specific look at digital manufacturing. Whereas IT security can be managed quite well in an organization through employee behavior and training, the risks with IoT devices are more subtle and more difficult to control.

Cybersecurity

Cybersecurity has become a large concern; "If we know that virtually everything can now be connected to the Internet, we have to recognize its corollary statement: everything that can be connected to the Internet can be hacked". It starts with intrusion detection [24]. Intrusion detection is a process where network or computer system activities are monitored for possible security issues. It includes auditing of system vulnerabilities, statistical analysis of activity patterns, and abnormal activity analysis [25]. There are two categories of intrusion detection methods: signature-based and anomaly-based detection. Signature-based detection, also known as misuse detection, detects known attacks based on system behavior. Signature-based detection methods include state transition analysis and Petri nets [9]. Anomaly-based detection detects unknown attacks using statistical methods and artificial intelligence (Table 4). Risk determination involves assessing the level of risk to a given system. The available tools include mathematical modeling methods based on probability theory and neural networks [10] (Table 5).

Energy providers Eneregy generation	Transmission	Distribution	Consumers
Real time generation monitoring	Transmission lines controlling	Underground cable system monitoring	Wireless automatic meter reading (smart metering)
Power plants controlling	Power monitoring	Transformers stations controlling	Home (Residential) eneregy management
Alternate energy sources controlling			solar panels management
Residential (distributed) Production monitoring			predicting future solar panels and wind turbine production (using sensor data like temperature or humidity)

Table 1: Potential IoT applications for smart grids [4].

Target	Vulnerability	Threat-Source
Software	Input Validation, privilege escalation, software coding vulnerabilities	Hacker, cracker, computer criminal, terrorist, industrial espionage, insiders, governments
Hardware	Malicious logic, open debugging ports	Insiders
Operating systems or firmware	Unpatched systems, vulnerable system components	Hacker. cracker, computer criminal, terrorist, industrial espionage, insiders, governments
Network	Limited bandwidth susceptible to jamming, unencrypted communication, weak network security protocols such as authentication	Hacker, cracker, computer criminal. terrorist, industrial espionage, insiders, governments
Data	Plain text with no encryption, no message integrity code (MAC)	Hacker, cracker, computer criminal, terrorist, industrial espionage, insiders, governments

Table 2: Vulnerabilities and threats in cyberspace [8].

Attack	Method	Consequence
Access attacks (e.g., Password attacks, Trust exploitation, Port scan)	Gain unauthorized access to a network. a system. An application software, or other resources	Loss of confidential information
Denial-of-Service (DoS) and service delay	Make hardware, software , or infrastructure unavailable to their intended users	Operational disruption, loss of productivity
Ma n -in-the-Middle (MITM)	Relay and alter messages between machines and remote control systems	Physical damage, poor product quality, injury or death, Joss of confidential in formation
Malicious software (e.g., Trojans, viruses, and worms)	Destroy manufacturing systems by inserting programs with malicious intent onto a manufacturing system	Operational disruption, loss of productivity, Physical damage, poor product quality, injury or death
Data manipulation	Access and change sensitive data such as the key parameters of digital models and documents	Physical damage, poor product quality. injury or death

Table 3: Potential attacks on digital manufacturing systems [8].

Internet of Things (IoT)

The Internet of Things (IoT) can be regarded as a new paradigm that integrates the internet and physical objects. The latter belong to different domains such as home automation ("smart home" [3]), industrial process, human health and environmental monitoring. The IoT significantly increases the presence of internet-connected devices in peoples' daily activities, compare Figures 3 and 4.

The omnipresent internet, apart from bringing many benefits, poses challenges related to security [25]. IoT applications range from a simple appliance for a smart home to a sophisticated equipment for an industrial plant [3,5]. In a smart home, household devices are equipped with interfaces for wireless communication, making up the home WSN (wireless sensor network). Wireless Sensor Network (WSN) is one of the major enabling technologies of IoT [26]. WSN and IoT are compared in Table 6. For a review on WSN [27-30].

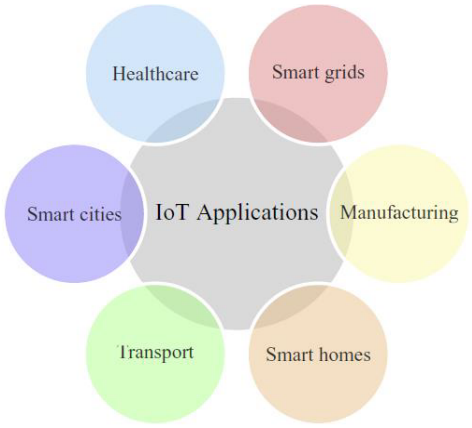

Figure 3: Internet of Things applications [2].

Cattegory	Method
Signature-based	State Transition Analysis Petri Nets
Anomaly-based	Markov Chain
	Neural Networks
	Support Vector Machines Decision Tree
	Random Forests K-means
	k-Nearest Neighbor Clustering

Table 4: Intrusion detection methods. Reproduced with permission [8].

Method
Attack graph Attack tree
Compromise graph
Augmented vulnerability tree Vulnerability tree
Petri nets
Process control network Attack countermeasure tree Digraph model
Anomaly-based intrusion detection
Boolean logic driven Markov process Game theory

Table 5: Quantitative risk analysis methods. Reproduced with permission [8].

For a smart home, offers the following advice [31]:

- Secure your devices, when possible (e.g., keep your software updated).
- Choose reputable vendors when buying smart devices.
- Upgrade the security to your home network.
- Consider whether you'll be using the public or private cloud.
- To prevent attacks that penetrate your network, use a virtual private network (VPN).

In smart cities, a market of several billion dollars, IoT has a huge potential, e.g., for smart parking, environmental monitoring, traffic management, waste management, water management and quality, and energy consumption [32,33]. More than 70% of the world's population are predicted to live in municipal cities by 2035, and there will be about 50 smart cities internationally by 2030 [2].

IoT operations include three phases: collection phase, transmission phase, and processing, management and utilization phase. In the first phase, the collection phase, the primary objective is the collection of data about the physical environment. The transmission phase transmits the collected data to applications and, consequently, to users. Ethernet, WiFi, Hybrid Fiber Coaxial (HFC) and Digital Subscriber Line (DSL) are combined with TCP/IP protocols to build a network that interconnects objects and users across longer distances [25]. In the following processing, management and utilization phase, applications process the data to obtain useful information about the physical environment.

"Green" IoT is reviewed in, where the key challenges are addressed [33]:

- Integration between energy efficiency across the IoT architecture to achieve an acceptable performance
- Minimizing their effects on the environment
- Reliability of green IoT
- Context-awareness
- Both devices and protocols used to communicate should be energy efficient with less power consumption.
- Complexity reduction of the green IoT infrastructure.
- Tradeoff between efficient dynamic spectrum sensing and efficient spectrum management.
- Efficient energy mechanism for IoT such as wind, solar, vibration, thermal
- Efficient cloud management with respect to power consumption
- Efficient security mechanism such encryption and control commands.

Characteristics	**IoT**	**WSNs**
Physical coupling	Tightly coupled	Monitoring the physical world
Communication	Two-direction communication	Mostly one-direction communication
Constraints	Computation and storage and energy	More on energy
Heterogeneity	Heterogeneous communications and devices	Mostly homogeneous devices
Scalability	Very large scale	Large scale
Privacy	Very high privacy expectation	Some privacy expectation

Table 6: Characteristics of IoT vs. classic WSNs [25].

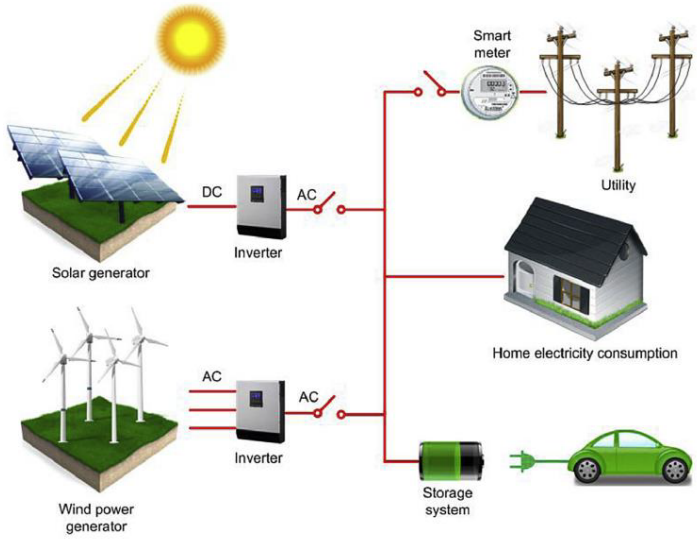

Figure 4: Smart home [5].

The industrial internet of things (IIoT)

Whereas the IoT in a domestic setting aims at increasing convenience and entertainment, in an industrial setting it is about optimizing supply chains. In an industrial context, the IIoT is synonymous with the term "Industry 4.0" or "Industrie 4.0", alluding to the creation of the term in Germany. A definition can be provided as follows: "Industrie 4.0 is a collective term for technologies and concepts of value chain organisation. Within the modular structured Smart Factories of Industrie 4.0, CPS monitor physical processes, create a virtual copy of the physical world and make decentralized decisions. Over the IoT, CPS communicate and cooperate with each other and humans in real time. Via the IoS (Internet of Services), both internal and cross- organizational services are offered and utilized by participants of the value chain". Another definition for the IoT is a "group of infrastructures, interconnecting connected objects and allowing their management, data mining and the access to data they generate" where connected objects are "sensor(s) and/or actuator(s) carrying out a specific function that are able to communicate with other equipment". These "smart objects" in the IoT require minimum or no human intervention to "generate, exchange, and consume data; they often feature connectivity to remote data collection, analysis, and management capabilities" [34].

Hacking attacks of factory industrial control systems (ICS) are on the increase [35]. The IIoT is associated with four security concerns:

- Understanding the shift from offline to online infrastructure;
- Managing temporal dimensions of security;
- Addressing the implementation gap for best practice
- Engaging with infrastructural complexity [35].

Safety and Security

Confidentiality: (information is made unintelligible to unauthorized individuals, entities, and processes); Integrity: (data is protected from modification by a third party, both accidentally and intentionally); Authentication: (verification that the data source is the pretended identity); Non-repudiation: (ensuring that the sender of a message cannot deny having sent the message); Availability: (Ensures that the services of the system is available for legitimate users).; Privacy: (Ensuring that users' identities are non-identifiable and non-traceable from their behaviors); The relationship between safety and security in cyber-physical systems (CPS) is depicted in Table 7 and Figure 5.

Challenges and Opportunities

In Table 8, the main security challenges in IoT settings are summarized. One can see that they differ between industries.

The 3 main challenges, in general, for solving security issues are [2]:

- Applications operate in highly distributed environments
- Heterogeneous smart objects are used.
- Sensors and actuators are limited in terms of power and computational resources.

Therefore, traditional security countermeasures do not work efficiently in IoT systems [25].

A key security challenge in the IoT context is the increase of the overall attack surface for malicious attacks, as compared to isolated (i.e. non-connected) systems [10].

The huge attack surface stems from the fact that IoT devices are low cost and popular, leading to high adoption rates. It is estimated that the number of networked devices in use worldwide will reach 20.8-26 billion by 2020 [25,36,37]. Cisco estimates this number at around 50 billion IoT connections by 2020 [1]. Huawei projects that such connections will hit the 100 billion figure by 2025 [15]. However, security issues can be the greatest barrier to that growth [38,39].

Basically, all these devices can be a target for attacks. Such attacks can be directed against critical infrastructure systems, such as power plants and transportation systems, or against household appliances, threatening security and privacy of individuals. A 2015 study by Hewlett Packard showed that 70 percent of IoT devices contain serious vulnerabilities [25]. Such vulnerabilities include:

- Lack of transport encryption
- Insufficient authentication and authorization

Security services	Security mechanisms	Some examples
Confidentiality	message encryption/sign-encryption	Symmetric cryptographic mechanisms (AES. CBC, etc); asymmetric mechanisms (RSA, DSA, IBE, ABE, ere).
Integrity	hash functions, message signature	has h functions (SHA-256,MDS, ere); Message Authentication Codes (HMAC)
Authentication	chain of hash, Message Authentication Code	H MAC, CBC-MAC. ECDSA
Non-repudiation	message signature	ECDSA, HMAC
Availability	pseudo-random frequency hopping, Access control, Intrusion prevention systems, firewalls	Signature-Based Intrusion Detection, Statistical anomaly-based intrusion detection
Privacy	Pseudonymity, unlinkability, k-anonymity, Zero Knowledge Proof (ZKP)	EPID, DAA, Pedersen Commitment

Table 7: Security services in the IoT [2].

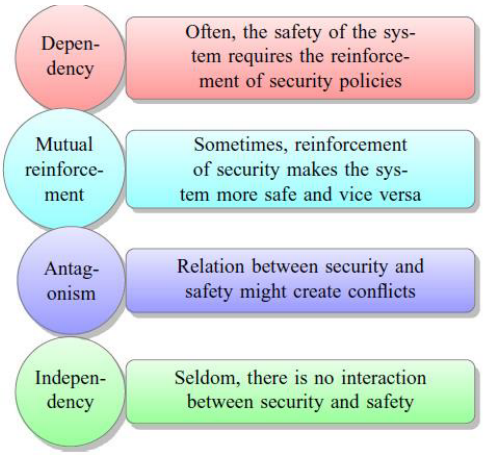

Figure 5: Relationship between safety and security in cyber-physical systems (CPS) [2].

Challenges	Applications				
	Smart grids	EHealth	Transportation systems	Smart cities	Manufacturing
Resources constraints	+	+++		++	+
Mobility	+	++	+++	+++	
Heterogeneity	++	++	++	+++	+
Scalability	+++	++	+++	+++	++
QoS constraints	++	++	+++	+++	+++
Data management	++	+	++	+++	++
Lack of standardization	++	++	++	++	+++
Amount of attacks	+	+	+++	+++	+++
Safety	++	++	+++	++	+++

Table 8: Main security challenges [2].

- Insecure web interface
- Insecure software and firmware

A CyberSecurity Audit Model (CSAM) is proposed [40].

A challenge in manufacturing comes from retrofitting existing plants and machines with new sensors and remote monitoring. New access control, encryption and intrusion detection techniques are required to manage the associated risks. Another challenge is how to detect and prevent embedded defects, which refers to defects introduced by attackers so that a system or a component can no longer perform its intended functions. As a countermeasure, monitoring of manufacturing systems and processes as well as non-destructive testing (NDT) or non-destructive inspection (NDI) techniques are to be developed and applied [9]. Common wireless technologies for IoT are 2G/3G/4G, WiFi and Bluetooth. The 2G networks (currently covers 90% of the world's population [36]. 2G is designed for voice. 3G, which currently covers 65% of the world's population [36], is designed for voice and data, and the 4G (since 2012) for broadband internet experiences. The 3G and 4G technologies, though widely used for IoT, are not fully optimized for IoT applications [36]. 5G offers opportunities here and is expected to be available in 2020 [33,41,42].

The main body of scientific and technical literature has proposed the adaption of security solutions for wireless sensor networks (WSNs) to IoT. However, most security approaches rely to centralized architectures, making their applications in IoT complex due to the large number of objects. Hence, distributed approaches are required to deal with security issues in IoT. In security approaches based on traditional cryptography and a novel approach based on new emerging technologies such as SDN (Software Defined Networking) and Blockchain are discussed, compare Figure 6.

SDN technology is an approach to cloud computing which facilitates network management and enables programmatically efficient network configuration in an attempt to improve network performance and monitoring [8,43]. Blockchain technology was originally used for recording financial transactions, where transactions are encoded and

kept by all participants (such as Bitcoins and other cryptocurrencies). This means that all transactions are transparent and modifications can be traced and detected. That very blockchain can be applied to enhance IoT security [11]. In Table 9, IoT security solutions are compared. Opportunities are offered by edge computing (fog computing), by which data processing at the "edge" of the network, i.e., at the sensors, is understood, so that the amount of data that has to be sent around is reduced. Raw data are reduced and only metadata are transmitted (i.e., data about the data). Data reduction can also avoid latency issues and saturation of the wireless channels [3]. Further opportunities lie in big data, networking and interoperability [3].

Conclusion

In the IoT, the internet meets the physical world. In contrast to normal hacking, the threat can move from manipulating information to controlling actuations [44]. The IoT generates immense amounts of data at a rate far above that of human-authored content such as the internet [45]. IoT is associated with several security risks. One reason stated in the literature is that many smart "things" are connected and

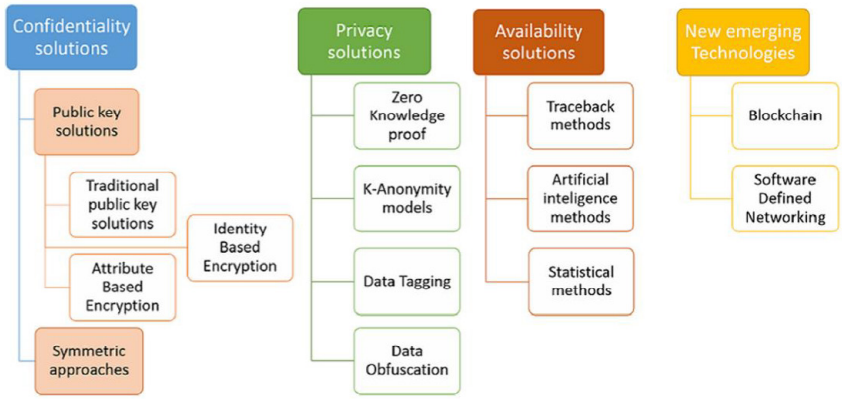

Figure 6: IoT security solutions [2].

Solutions	Challenges						
	Computation complexity	Communication complexity	Memory	Mobility	Heterogeneity	Scal ability	Quality of Service
Confidentiality	++	-	+	+	+	-	-
	+	+	-	+	-	+	+
	+	-	++	+	+	-	-
	++	+	+	+	+	-	+
	-	+	+	+	-	-	+
	-	+	+	+	-	+	+
	++	+	++	-	-	-	+
	+	+	+	+	+	-	+
Privacy	+	-	++	+	-	+	+
	++	-	++	+	+	-	+
	++	+	+	+	-	+	+
	+	-	-	+	++	+	+
	++	+	+	-	-	+	+
	+	-	+	-	-	+	+
Availability	+	+	-	+	+	-	-
	+	-	+	+	+	+	+
	-	+	-	+	+	-	+
	+	+	-	-	+	-	-
	+	+	+	+	+	-	-
Block chain	+	-	+	+	++	++	-
	-	-	-	++	+	++	+
	-	+	-	-	+	++	+
	-	+	-	-	+	++	+
	-	-	-	+	+	++	+
SDN	++	--	+	-	++	++	-
	+	-	+	+	+	-	++
	+	-	+	-	++	+	+
	+	-	+	-	+	+	++
We provide in this table a deep analysis and comparison of the solutions we presented previously in this survey according to several security challenges. We use the following notations to assess the level of satisfaction of each solution with respect to the different challenges: ++ good: + average: - poor (limited) and -- bad.							

Table 9: Comparison of IoT security solutions [2].

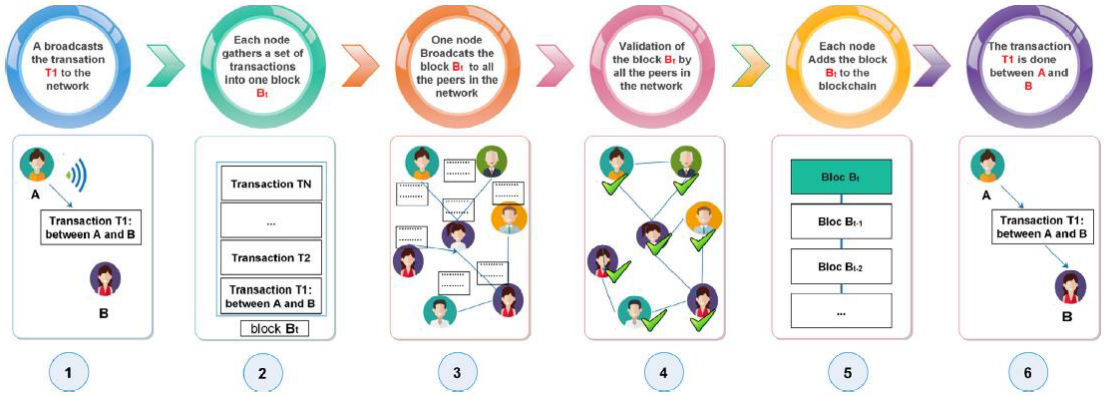

Figure 7: Blockchain steps of transactions' validation process [1].

then "forgotten", without being updated. So hackers can have easy access into different networks. Scanning IoT devices for vulnerabilities is important to ensure security and privacy [46]. Privacy, authorization, verification, access control, system configuration, information storage and management are the main security issues in IoT [18], and a cybersecurity strategy needs to be developed and implemented by organizations. Also, simple solutions like 2 firewalls from different vendors have been proposed [16], arguing that the probability for the same vulnerability is low.

Outlook

Future internet technologies with relevance to IoT are cloud computing [8], semantic technologies, autonomy and situation awareness and cognition [1]. Blockchain and SDN (Software Defined Networking), alongside 5G, are new emerging technologies that can help increase security in the IoT and IIoT in particular. The first IoT platform based blockchain solution was already developed by IBM in 2013. This platform is called ADEPT (Autonomous De- centralized Peer-To-Peer Telemetry) and shown in Figure 7. It is expected that security in IoT will have a strong emphasis on mobile and service robots, too [37]. The security breaches in the IT-intensive industry will significantly become higher competition effect than those in the non-IT-intensive industry [47,48]. Moreover, with the huge projected increase in the number of IoT devices and the spread into almost all realms of modern life, security is becoming more and more important, and a strong focus will need to be maintained in security management.

References

1. Djamel Eddine K, Abdelmadjid B, Hicham L (2018) Internet of things security: A top-down survey. Computer Networks 141: 199-221.
2. Saad Albishi, Ben Soh, Azmat Ullah, Fahad Algarni (2017) Challenges and Solutions for Applications and Technologies in the Internet of Things. Procedia Computer Science 124: 608-614.
3. http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf
4. Stojkoska BR, Trivodaliev KV (2017) A review of Internet of Things for smart home: Challenges and solutions. J Clean Prod 140: 1454-1464.
5. https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot
6. Sfar AR, Natalizio E, Challal Y, Chtourou Z (2017) A roadmap for security challenges in the Internet of Things. Digital Communications and Networks 4: 118-137.
7. Ray PP (2016) A survey on Internet of Things architectures. Journal of King Saud University - Computer and Information Sciences 30: 291-319.
8. 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.
9. Wu D, Ren A, Zhang W, Fan F, Liu P, et al. (2018) Cybersecurity for digital manufacturing. Manuf Syst, pp: 647.
10. Banerjee M, Lee J, Raymond Choo KK (2017) A blockchain future for internet of things security: a position paper. Digital Communications and Networks 4: 149-160.
11. Skavland Idsø, E. og Mejdell Jakobsen, Ø., 2000, Objekt- og informasjonssikkerhet. Metode for risikoog sårbarhetsanalyse, Institutt for produksjons- og kvalitetsteknikk, NTNU Eirik Albrechtsen, NTNU 8.
12. Aikaterini Poustourli, David Ward, Angelos Zachariadis, European Policies and Programs for the Security of Building Constructions, Eighth International Conference on Construction in the 21st Century (CITC-8), "Changing the Field: Recent Developments for the Future of Engineering and Construction" May 27-30, 2015, Thessaloniki, Greece
13. http://www.internetsociety.org/doc/some-perspectives-cybersecurity-2012
14. http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
15. Weber RH, Studer E (2016) Cybersecurity in the Internet of Things: Legal aspects. Comput Law Secur Rev 32: 715-728.
16. Jean Pierre Nzabahimana, Analysis of security and privacy challenges in Internet of Things, 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Year: 2018, pp: 175-178
17. KKR Choo, M Bishop, W Glisson, K Nance (2018) Internet- and cloud-of-things cybersecurity research challenges and advances. Computers & Security 74: 275-276.
18. Fadele AA, Othman M, Hashem IAT, Alotaibi F (2017) Internet of Things security: A survey. Journal of Network and Computer Applications 88: 10-28.
19. Urquhart L, McAuley M (2018) Avoiding the internet of insecure industrial things. Comput Law Secur Rev 34: 450-466.
20. Leszczyna R (2018) A review of standards with cybersecurity requirements for smart grid. Computers & Security 77: 262-276.
21. Krzysztof C, Dulce D, Zbigniew K, Ana Re (208) Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers & Security 75: 24-35.
22. Kah Leng TER (2018) Singapore's cybersecurity strategy. Computer Law & Security Review 34: 924-927.
23. Lynne C, Dawn B (2018) Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas 113: 48-52.
24. Sue P (2015) The Internet of Things Has a Growing Number of Cybersecurity Problems.
25. Bruno B, Rodrigo S, Cláudio T, Sean CA (2017) A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications 84: 25-37.
26. Kewei S, Wei W, Andrew TY, Zhiwei W, Weisong S (2018) On security challenges and open issues in Internet of Things. Future Generation Computer Systems 83: 326-337.

27. Habib M, Michael M (2018) Software-defined wireless sensor networks: A survey. Journal of Network and Computer Applications 119: 42-56.

28. Ying-Gao Y, Ping H (2018) A comprehensive survey on the reliability of mobile wireless sensor networks: Taxonomy, challenges, and future directions. Information Fusion 44: 188-204.

29. Fatma K, Mohamed WJ, Garcia-Ortiz A , Abid M, Obeid MA (2018) A comprehensive survey on wireless sensor node hardware platforms. Computer Networks 144: 89-110.

30. Gaurav S, Suman B, Anil KV (2012) Security Frameworks for Wireless Sensor Networks-Review. Procedia Technology 6: 978-987.

31. Francis Dinha, How To Secure The Internet Of Things.

32. Amir HA, Pengcheng J, William GB, Nizar L (2018) Internet of Things-enabled smart cities: State-of-the-art and future trends. Measurement 129: 589-606.

33. Mahmoud AMA, El-Saleh AA, Muzamir I, Wael S, Jusoh M, et al. (2017) Green internet of things (IoT): An overview Measurement and Application (ICSIMA): 1-6.

34. Hugh B, Bil H, Joe C, Tim W (2018) The industrial internet of things (IIoT): An analysis framework. Computers in Industry 101: 1-12.

35. Lachlan U, Derek M (2018) Avoiding the internet of insecure industrial things. Computer Law & Security Review 34: 450-466.

36. Shancang Li, Li DX, Shanshan Z (2018) 5G Internet of Things: A survey. Journal of Industrial Information Integration 10: 1-9.

37. Sachchidanand S, Nirmala S (2015) Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce .2015 International Conference on Green Computing and Internet of Things (ICGCIoT): 1577-1581.

38. Harald B, Ondrej B, Christian K (2017) Security in the Internet of Things.

39. Syed A, Ann B, Frank F (2018) Cybersecurity Is the Key to Unlocking Demand in the Internet of Things.

40. Regner S, Serra-Ruiz J, Victor C, Jeimy C (2017) A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance.The CyberSecurity Audit Model (CSAM), 2017 International Conference on Information Systems and Computer Science (INCISCOS): 253-259.

41. Maria Rita P, Mischa D, Alfredo G, Gianluca R, Johan T, et al. (2016) Internet of Things in the 5G Era: Enablers, Architecture, and Business Models, IEEE Journal on Selected Areas in Communications 34: 510-527.

42. Godfrey AA, Bruno JS, Gerhard PH, Adnan MA (2018) A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges. IEEE Access 6: 3619 -3647.

43. Benzekki Kamal, Abdeslam EFi Abdelbaki EE (2016) Software-defined networking (SDN): a survey. Security and Communication Networks 9: 5803-5833.

44. Mahmoud A, Giovanni R, Bruno C (2018) Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications 38: 8-27.

45. Bessis, Nik X, Fatos V, Dora H, Richard L, Maozhen (2013) Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence.

46. Linda M, George M (2015) Scanning for vulnerable devices in the Internet of Things, 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) 1: 463-467.

47. https://www.technikum-wien.at/forschung/forschungsschwerpunkte/automation_robotics/

48. Jeong CY, Lee SYT, Lim JH (2018) “Information security breaches and IT security investments: Impacts on competitors. Inf. Manage.