Challenges of Securing the Industrial Internet of Things Value Chain

Stefan Forsström, Ismail Butun, Mohamed Eldefrawy, Ulf Jennehag and Mikael Gidlund
Department of Information Systems and Technology, Mid Sweden University, Sundsvall, Sweden
e-mails:{*stefan.forsstrom, ismail.butun, mohamed.eldefrawy, ulf.jennehag, mikael.gidlund*}*@miun.se*

***Abstract*—We see a shift from todays Internet-of-Things (IoT) to include more industrial equipment and metrology systems, forming the Industrial Internet of Things (IIoT). However, this leads to many concerns related to confidentiality, integrity, availability, privacy and non-repudiation. Hence, there is a need to secure the IIoT in order to cater for a future with smart grids, smart metering, smart factories, smart cities, and smart manufacturing. It is therefore important to research IIoT technologies and to create order in this chaos, especially when it comes to securing communication, resilient wireless networks, protecting industrial data, and safely storing industrial intellectual property in cloud systems. This research therefore presents the challenges, needs, and requirements of industrial applications when it comes to securing IIoT systems.**

***Index Terms*—Security, IoT, IIoT, Industry 4.0, vulnerabilities, trust, metering, metrology, application, end-device**

I. Introduction

Today we can observe large global trends in the digitalization of all aspects of our everyday life. In particular, we see applications that can utilize information from sensors attached to things in order to provide more personalized, automatized, and intelligent behavior. This concept is commonly referred to as the Internet-of-Things (IoT) [1]. IoT is a collective term for the development of machinery, vehicles, goods, appliances, clothes, etc. to become equipped with small embedded sensors and actuators that can also communicate among each other over the Internet. This means that these devices can perceive their surroundings, communicate with others, have situational behavior, and create new forms of smart, intelligent, and autonomous services [2]. This development is not only important for a digitalized and connected society, but also for the industry and the economy as a whole. Current estimations claim that there will be over 50 billion connected devices on the Internet as soon as year 2020 and many of these devices will be sensors, actuators, and small computers [3], [4]. All these IoT devices will together create new types of services by sharing sensor information ubiquitously between each other on a global scale and controlling different types of actuators. Thus, heavily relying on metrology systems to acquire the sensor information [5]. From this we also see trends in IoT cloud computing for large scale data storage [6], big data analytics on massive amount of gathered data from IoT sources [7], and incorporation of cyber-physical systems into machine to machine (M2M) systems [8]. In relation to this, there is much work being done in the Industrie 4.0 initiative [9], including smart cities, smart industry, factories of the future, and smart manufacturing. Furthermore, as Industry 4.0 catching a faster pace than ever imagined industrial automation is not only getting smarter by using artificial intelligence methods, but also freeing itself from wired components by exploiting wireless technology. This is being possible by employing IIoT in a standardized fashion and seeking technological breakthrough from industrial automation researchers. Hence, forming the need for research in Industrial IoT (IIoT) [10]. However, the industrial demands are quite different from non IIoT services, especially when it comes to time criticalness and reliability [11]. For example, an industrial process might have to react quickly to small changes in the sensor values to maintain a high quality of the product or to avoid a catastrophic failure. Because of this, industrial communication systems often consider a five nines availability [12], [13], meaning an uptime of at least 99.999%. Industrial applications and IIoT have much higher security demands, to avoid downtime and to protect sensitive information related to the industrial process. Including protecting the networks from denial of service attacks, data protection and privacy of the sensitive industrial data, and timely updates to avoid weakness exploitation by different on-line attacks. It is this area that will be the focus of this paper where surveys and related works by Sadeghi *et al.* [14], Sicari *et al.* [15], Borgia *et al.* [16], and the references therein introduce and summarize the current state of the art well.

The overall goal of this research is to provide insights into securing the IIoT, with a particular focus on the IIoT value chain. Which ranges from sensor value generation and transmission over the Internet, to finally the cloud servers and end user applications. It is paramount important to solve and address security aspects of the IoT and IIoT, if this vision will expand beyond the simple applications we see today. To achieve these, the research needs to be built up on the existing works in security guidelines, industrial security frameworks, secure-by-design principles for ecosystems, secure remote code execution, homomorphic encryption, and software guard extensions. Hence, the purpose is to investigate the disadvantages and limitations of the cloud based approaches current in use. An additional purpose of this research is to present a more viable and future proof approach. Finally, this project will aid in establishing a critical mass in IoT and IIoT research to increase the awareness, completeness, and extensiveness of

This research was supported by grant 20150367, 20150363, 20140319, and 20140321 of the Swedish Knowledge Foundation.

978-1-5386-2497-5/18/$31.00 ©2018 IEEE

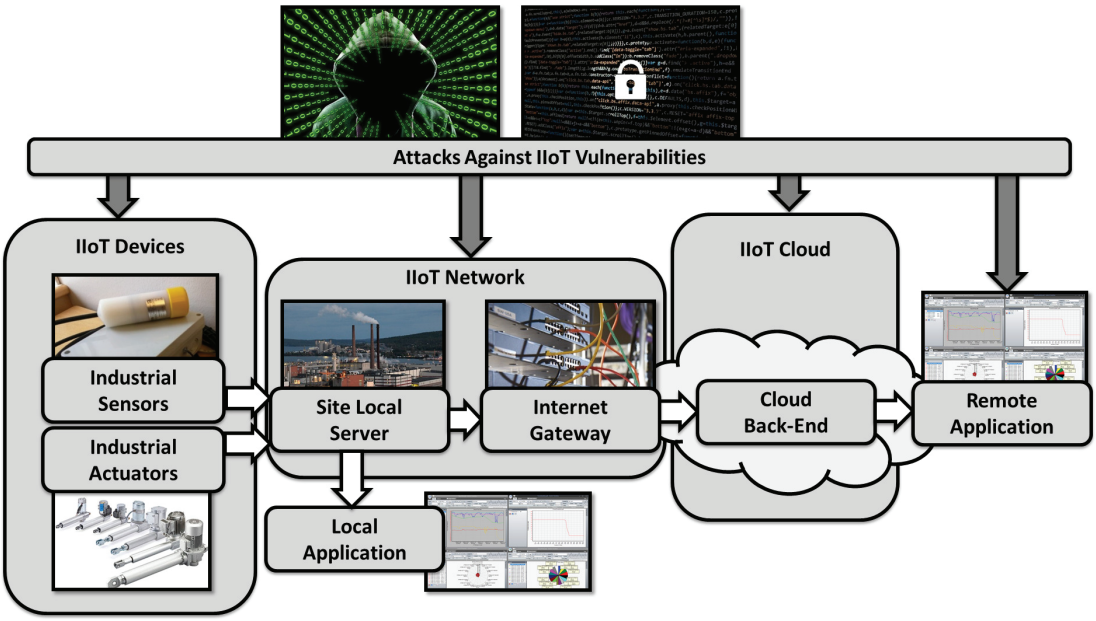

Fig. 1. An overview of a typical IIoT value chain and highlighted challenging areas related to security

the IIoT security research. Even though security in industrial systems and the IoT have been investigated for some time now, this brings novelty to the field with its holistic view of the IIoT value chain and by securing both the devices and the industrial data within the actual IIoT systems. Hence, the research work presented in this paper seeks to answer the following two research questions:

1) What requirements can be identified and highlighted, to show security and trust challenges on a holistic point of view in all the steps of an industry value chain that includes an IIoT and measurement system.
2) Which upcoming security research areas are most important for the proliferation of Industry 4.0 and the IIoT, and what are the major obstacles to focus future work on?

From these two research questions, our contribution in this paper is to highlight and illuminate problems, challenges, and the issues when securing the IIoT. Hence, this article will only provide an overview of the problems and short explanations of possible solutions, since solving these problems still are ongoing research.

The remainder of this article is organized as follows: Section II outlines and presents the challenges that have been identified that the IIoT is facing, split into five highlighted areas. Section III presents a use case study on how these challenges can appear in a typical IIoT scenario. Finally, Section IV presents our conclusions and directions for future work.

II. Securing the IIoT Value Chain

The IIoT Value Chain can be illustrated in many different ways, depending on the type of industry. One simplified and holistic view of the a typical IIoT value chain can be seen in Figure 1. This figure will be used in this research as a basis for understanding where the challenges, research problems, and implementation issues exists. Hence, this figure shows the IIoT devices such as industrial sensors and actuators. The IIoT networks, consisting of both communication networks, site local severs and gateways. The IIoT cloud, forming a back-end system for the IIoT data. The end user applications, such as monitor applications, business logic systems, and process management systems. Finally, all parts of the IIoT value chain can be vulnerable to different types of malicious attacks. The remainder of this section will present details on some of the identified challenges in each of these areas.

A. IIoT System Model Security Challenges

The first identified challenge was to investigate the security demands in IIoT systems and to define a general model for evaluating security of the IIoT. Including mathematical models, evaluating metrics, and needed measurements. Resulting in a concrete list of IIoT demands and requirements based on information from actual problem owners and an evaluation model to assess the security of different IIoT systems. There is a need to collect, compile, and relate all the gathered results from a holistic point of view. With the intention of creating a set of guidelines for secure IIoT systems and their communication. Because of this, actual problem owners are an integral part of solving these challenges, because they can provide vital information on the state of the industry that can otherwise be very difficult to survey from an academic perspective. There is a need for creating a set of guidelines and instructions for how industries can secure their value chains, securing their devices, and securing their cloud systems. Hence, there is a need to survey previous work and existing security guidelines, industrial security frameworks and secure-by-design principles for ecosystems. Highlight the impact and importance of secure IIoT systems. Modeling the

parameters that has impact on the security of IIoT systems in terms securing devices, communication, and cloud systems. To finally, compiling related work and results into a set of guidelines for how industries can secure their IIoT value chains.

B. IIoT End-Device Security Challenges

One must also take the device themselves into consideration, because securing devices that a malicious person have might have access to is extremely difficult. Since all application layer security mechanisms require some form of key management, storing the keys and handling them in a secure way becomes paramount. It is also not uncommon to see hard-coded keys or group keys systems on IoT devices, where a single compromised device can compromise the whole systems security. One must always take into consideration that the devices are put into untrusted environments, both from a physical and logical point of view. Even if we protect our industrial sites with walls, barbed wire and virtual private network systems. A single breach of any of these systems, be it physical or logical, takes an attacker inside the protected system and has access to the device. There are many examples of extracting keys from devices if one has access to the physical device, for example physical side channel attacks, tampering, reverse engineering, power/electromagnetic analysis, timing attacks, known fault attacks, and clock glitches.

One common approach trough history is to ensure device security though obscurity. Which is also surprisingly easy to break, given access to the device. One example is how Mifare Classic RFID cards, which are still used for bus cards and access cards, were reverse engineered and exploited. In detail, researchers could reverse engineer the cipher by analysis of the integrated circuit (IC) architecture under microscope [17]. Thus seeing the structure of the IC gates and could reconstruct the cipher from that. Another clear example of device security problems is problems related to timing [18]. Where an otherwise secure algorithm can still be broken by physical access to the device, because of poor or unthoughtful programming. For example, a simple 8 character password check implemented as a for loop checking character by character for matches, can be timed for each pass or fail to reduce the brute force complexity from for example 256^8 tries to $256 * 8 = 2048$ tries.

Finally, one must investigate what the implications of compromised device are. Sometimes a single compromised devices cannot perform much harm by itself, but the fact that one device have been compromised means that the others are vulnerable as well. There is also the threat of using multiple compromised devices as botnets, which from an industrial point of view can have serious impact. For example if the device prioritizes down vital sensing, because they are actively taking part in botnet activities instead.

C. IIoT Network Security Challenges

Network Security is a challenging task, especially for an IIoT, owing to the heterogeneous network architecture with multiple network components using different hardware and software implementations. Additionally, the wireless communications medium of IIoT introduces extra vulnerability and open venue for wide range of attacks from passive attacks such as eavesdropping, to more advanced active attacks such as jamming. There are various vendors producing plethora of devices that can be employed under IIoT. Therefore, network security of IIoT is often achieved by custom proposals rather than generic ones. For instance, in LoRaWAN which is a proprietary Low Power Wide Area Network (LPWAN) application that has the highest market dominance at the moment, security of the network is achieved by issuing a well-known symmetric key cryptography algorithm i.e. AES128 [19]. The distribution and management of the keys is a very customized solution and open to enhancements. For example, there is a drastically change in the versions of LoRaWAN v1.0 and v1.1, in terms of number of session keys as well as the secret lifetime keys. This proves that future network security solutions for IIoT will be more customized rather than being generic ones. It can be stated that the network security of an IIoT system should be custom tailored, according to the vulnerabilities of that specific IIoT system along with the trust metrics of the network and depending on the security requirements of the IIoT system managers and the users. As in the case of industrial automation and control domains, the resulting security design of an IIoT system should be dynamic, where security level of the design could be improved at will via updates with patch distribution or with version updates [20].

D. IIoT Cloud Security Challenges

IoT and IIoT are exploring the benefits of Cloud and Cloud-based-services, it is inevitable to think Cloud to be an extended part of these networks. However, adoption of Cloud by IIoT will bring plenty of new security challenges especially in data management, access control, identity management, complexity scaling, compliance issues, legal issues, and last but not least, emerging Cloud decentralization [21]. Therefore, security solutions that are devised for IIoT need to consider the Cloud extension as well. For example a security plane for Cloud-based-services should be used at the front-end IoT devices and can be employed as an interface between the IIoT and the Cloud [22]. In Cloud supported IIoT systems, not only forward secrecy of the user data stored at the Cloud is important, but also the backwards non-traceability of the end devices from the stored data at the Cloud. Therefore, a security plane can effectively be leveraged to take on several security services such as authentication, access control, etc., for assuring privacy of user data stored at the Cloud and security of IIoT devices at the same time. The Cloud systems also need to employ functions for high scalability, good redundancy, multiple network connections, and failsafe systems. So that if parts of the Cloud systems fails or becomes under attack, the system should still function good enough to maintain the service level agreements to avoid catastrophic failures in the IIoT applications.

E. IIoT Application Security Challenges

According to the Open Web Application Security Project (OWASP) a list of top 10 vulnerabilities that can influence the IIoT security has been announced in [23]. The following challenges and countermeasures, *directly related to the IIoT application security*, have been split into two categories, application interface and malicious software.

To attain a secure web interface, it needs to prohibit weak passwords process and have a lockout mechanism, both temporary and permanent, after certain number of unsuccessful trials. The interface must be biased to strong passwords registration side by side to force password restarting after a certain time-period. Security credentials such as user-name and password, should be available for updates. In addition, a mechanism of multi-factor authentication should be deployed where possible. Furthermore, password recovery solutions have to be available in case of forgetting the present password. There is also a need to check the web applications against certain vulnerabilities, such as Cross-site Scripting (XSS), SQL Injection (SQLi), and Cross-Site Request Forgery (CSRF) attacks. These three are the most common web application vulnerabilities nowadays and they are related to the web application development. Hence, secure coding must be considered accordingly when creating the web applications. HTTPS (HTTP Secure) needs to be presented to protect the exchanged data on all IIoT applications, as well as firewalls need to be present to restrict global access of the web interfaces.

Malicious software or Malware as a short, refer to a range of forms of aggressive or destructive software, for example but not limited, worms, Trojan horses, spyware, viruses, and much more. It worth to mention Mirai worm [24] which is a malware that turns connected devices over Linux platform into controlled ”bots” to launch large-scale botnet attacks. It has been recruited in some of the highly disruptive distributed denial of service (DDoS) attacks. The Mirai botnet was first found in August 2016. It attacks on-line devices connected to the Internet such as IP surveillance cameras, sensors and actuators. It works by detecting weak IoT nodes with a dictionary attack of predefined security login credentials to log into these devices to infect them. Infected devices will continue to work normally, except for some occasions when it utilizes the IoT nodes resources to launch a DDoS attack. It use a large number of IoT devices to bypass DoS anomaly detection software which monitors the IP address of received requests to block if it recognizes an irregular pattern.

F. IIoT Trust Challenges

This challenge is on securing sensitive industrial data in the IIoT cloud systems. Including technologies for hiding and protecting the sensitive industrial data, such as sensor values, algorithms, and industrial process information. Furthermore, the amount of collected personal information must be restricted by a certain limit. Gathering of personal information must be done over a secure communication channel. Consumers should also be given an option for data is being collected and what is required for certain processes. To further complicate this, all this information will need to be stored on different IIoT cloud systems where the system itself can not be trusted. The sensitive industrial information must be protected against compromising of the IIoT cloud or system provider, as well as eavesdropping and reverse engineering. In particular, there is need for research and development of an encrypted computational component to perform secure industrial processing in an insecure cloud environment. Hence, there is a need to highlight how different cloud systems handle trust for the IoT and IIoT. As well as proposing a method for securing industrial information, sensor values, and algorithms on IIoT systems where the system itself cannot be trusted. Including evaluating the performance and the level of security that different IIoT system providers can provide.

This challenge also includes trust issues with the IIoT devices, such as issues with adding, removing, or changing devices in the IIoT systems. The idea is that the IIoT should be self-configuring, with little to no human intervention and difficult setup. Which means there is a need for establishing trust when new devices being added into an existing IIoT system, to identify and deny potential malicious devices. There is also a need to look into secure and automatic updates of existing devices, to ensure all devices can be safely updated when a new exploit is discovered and at the same time avoid malicious software being pushed onto the devices. In particular, a method for pushing verifiable updates to protected devices through insecure channels is needed. In order to perform large scale updating of secure industrial software without physical interactions with the hardware. Hence, there is a need for highlighting existing systems for securing IoT devices, such secure remote code execution and software guard extensions. As well as evaluating different methods for pushing verifiable updates to protected devices through insecure channels.

G. Exploitation of IIoT System Vulnerabilities and Attacks

IIoT network cyberattacks are very harmful as they can make physical damage that could lead to human life loss. The complex nature of the IIoT systems and the possible negative consequences of cyberattacks can carry out and introduce new threats. IIoT networks are susceptible to numerous types of cyberattacks, including, node capture attack, side-channel analysis, eavesdropping, man-in-the-middle, denial of service, and much more. Unfortunately, traditional security solutions cannot address IoT vulnerabilities due to the different nature of the IIoT [14]. Node capture attack is a unique and challenging attack for IIoT networks. It deals with the physical nodes. Owing to the spreading topology of the IIoT networks, physical nodes usually run in unbounded and uncontrolled areas, which makes it vulnerable to be captured effortlessly. Involving tamper-resistant nodes is not a reliable solution as it increases the network cost extremely. The detection of node capturing can contribute to solving this tricky issue [25], [26]. Side-channel analysis attack is based on the information that can be recovered from the analysis of encryption/decryption apparatus during the encryption/decryption process. These apparatuses

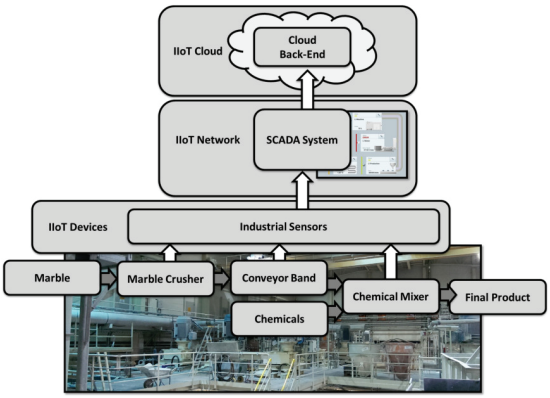

Fig. 2. An example of an IIoT installed factory with metering system

show timing and/or power consumption figures that could be easily traced and determined. The gathered information could led to discover the system security credentials i.e., shared session key, ciphering method. Keeping in mind that the IIoT nature makes it easier for the intruder to launch this sort of attack [27]. Eavesdropping is an action of listening in a live communication to gather information that could help the intruder to launch an attack accordingly. In the IIoT, which relays on wireless communication means, anyone can get an access to the medium to start eavesdropping. Confidentiality is the default security guard against eavesdropping condition that secure and reliable key establishment is guaranteed. It is well known to use implicit certificate to assure reliable key agreement for IIoT. In addition, when it comes to reaching a determined key lifetime a key revocation and/or re-keying mechanism needs to take place [28]. The Man-In-The-Middle (MITM) attack is one of the most famous attacks in network security generally, and in IIoT particularly. It is one of the major concerns for cybersecurity experts. MITM objects the real data that runs or exchanged between communication partners to eavesdrop, alter, modify, and falsify it [29]. Denial of Service (DoS) attacks, which are well-determined attempts, by a malicious party, to prohibit genuine users from reaching their network resources. It targets the system availability by heavily overwhelming the system resources to isolate it from its genuine users. This attack is very critical to IIoT networks as they are made up of constrained devices with very limited resources [30].

III. Use Case Examples

Metrology measurements of the IIoT sensors working at critical infrastructures can be very important and even effect safety of human lives. As seen in many cases in the history; industrial sites have been targeted by hackers and subject to cyber-attacks, such as the Stuxnet incidence [31] in which SCADA systems of Iranian nuclear facilities effected with millions of dollars estimated property damage. These critical infrastructures may vary from bridges, tunnels to nuclear power plants and in this section we provide two specific examples from real life of automation world:

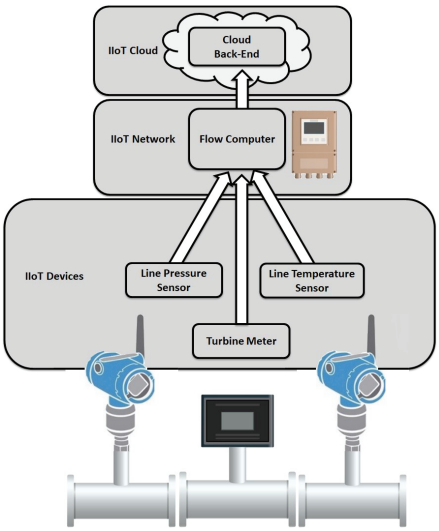

Fig. 3. An example of an IIoT natural gas metering system

A. Factory Metering System

A real world factory process for creating minerals to be used in paper the paper industry, has much connected IIoT equipment with sensors and actuators. Such as a verity of grinders, mixers, heaters, conveyor bands, see Figure 2. These IIoT sensors and actuators facilitates mainly three functions. Namely digitized on-the-go remote monitoring and control of equipment, optimization of machines within a production line due to collected process related data, and instant alarming for shutting-down of the equipment in the case of emergency situations. In this specific factory example, malicious adversaries can target these functions to bring great harm to the business. In this specific facility, especially heat and pressure sensors are highly critical. Any kind of outsider intervention might cause malfunctions, which eventually would end-up with not only batch and property damage, but also health hazards due to the unpreventable machine failures. Hence, there is a need for factory automation systems to take the challenges that have been highlighted in this article into consideration. In order to deploy sufficient cyber-security precautions to protect the business.

B. Natural Gas Metering System

In Gas Pressure Reduction Stations (GPRS), an integrated metering system must be involved to measure the fuel consumption. It consists of a turbine meter, pressure transmitters and temperature transmitters, see Figure 3. These IIoT transmitters and meters are usually connected to each other over wireless HART/Profibus communicator to transfer their measurements to a remote flow computer. The turbine flow meter reading indicates the volume of the pressure and base temperature condition. The flow computer needs to receive very accurate values of the (line) pressure and temperature to be able to convert this base value to the real consumption. Accordingly, we need to be assured that the flow computer is receiving the accurate values of the line temperature, the

line pressure as well as the base volume (turbine pulses) to calculate the real volume consumption. As any error in these calculations can lead to a huge financial loss, these systems need to consider the challenges that have been highlighted in this article, to protect their business.

IV. Conclusions

This article explored the challenges of securing metrology data for the IIoT, where we investigated seven areas in particular. Namely the challenges in: IIoT system model security, IIoT end device security, IIoT network security, IIoT cloud security, IIoT application security, IIoT trust, and IIoT attacks. In response to these, we have highlighted some of the outstanding problems, the issues when creating real-life implementations, and the research needed to solve this for a future IIoT. As mentioned earlier, nowadays there is a demand on custom security solutions: Rather than using generic solutions, security experts are devising highly customized security solutions for each network that is being designed. This brings the advantages of rapid act on fixing the security vulnerabilities of that specific network by releasing patches timely manner and/or enhancing the security level in the next release by closing all the gaps that are recognized. In this context, IIoT systems security is projected to follow this trend of customized approach in ensuring the security of IIoT value chain. Hence, this brief summary of security measures along with presented topics and ideas will help researchers not only enhancing security-awareness in IIoT as a whole system but also in securing its sub-components such as devices, networks, clouds, and applications. In these areas there is much future work left to be performed, which is why our own research will primarily be focused on the following items:

1) Security requirement analysis of IIoT (obtaining vulnerabilities list according to the various attack vectors).
2) Design of a customized security architecture for a conceptual IIoT setup.
3) Theoretical and practical security analysis of the proposed solution (customized security architecture).
4) Comparison of the proposed security solution to its' rivals in the literature (if any).

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] G. Abowd, A. Dey, P. Brown, N. Davies, M. Smith, and P. Steggles, "Towards a better understanding of context and context-awareness," in *Handheld and ubiquitous computing*. Springer, 1999, pp. 304–307.

[3] Ericsson. (2013, December) More than 50 billion connected devices. White Paper. [Online]. Available: http://www.ericsson.com/res/docs/whitepapers/wp-50-billions.pdf

[4] M. Kocakulak and I. Butun, "An overview of wireless sensor networks towards internet of things," in *Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual*. IEEE, 2017, pp. 1–6.

[5] A. Lazzari, J.-M. Pou, C. Dubois, and L. Leblond, "Smart metrology: the importance of metrology of decisions in the big data era," *IEEE Instrumentation & Measurement Magazine*, vol. 20, no. 6, pp. 22–29, 2017.

[6] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "On the integration of cloud computing and internet of things," in *Future Internet of Things and Cloud (FiCloud), 2014 Int. Conf. on*. IEEE, 2014, pp. 23–30.

[7] M. Chen, S. Mao, and Y. Liu, "Big data: A survey," *Mobile Networks and Applications*, vol. 19, no. 2, pp. 171–209, 2014.

[8] J. Kim, J. Lee, J. Kim, and J. Yun, "M2m service platforms: Survey, issues, and enabling technologies." *IEEE Communications Surveys and Tutorials*, vol. 16, no. 1, pp. 61–76, 2014.

[9] H. Kagermann, J. Helbig, A. Hellinger, and W. Wahlster, *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*. Forschungsunion, 2013.

[10] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[11] J. Åkerberg, M. Gidlund, and M. Björkman, "Future research challenges in wireless sensor and actuator networks targeting industrial automation," in *Industrial Informatics (INDIN), 2011 9th IEEE International Conference on*. IEEE, 2011, pp. 410–415.

[12] I. Silva, L. A. Guedes, P. Portugal, and F. Vasques, "Reliability and availability evaluation of wireless sensor networks for industrial applications," *Sensors*, vol. 12, no. 1, pp. 806–838, 2012.

[13] S.-e. Yoo, P. K. Chong, D. Kim, Y. Doh, M.-L. Pham, E. Choi, and J. Huh, "Guaranteeing real-time services for industrial wireless sensor networks with ieee 802.15. 4," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 11, pp. 3868–3876, 2010.

[14] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*. IEEE, 2015, pp. 1–6.

[15] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[16] E. Borgia, "The internet of things vision: Key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1–31, 2014.

[17] G. de Koning Gans, J.-H. Hoepman, and F. D. Garcia, "A practical attack on the mifare classic," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2008, pp. 267–282.

[18] Q. Ge, Y. Yarom, D. Cock, and G. Heiser, "A survey of microarchitectural timing attacks and countermeasures on contemporary hardware," *Journal of Cryptographic Engineering*, pp. 1–27, 2016.

[19] "LoRaWAN 1.1 Specification, Oct. 2017," http://lora-alliance.org/lorawan-for-developers, accessed: 2018-01-22.

[20] F. Al, L. Dalloro, H. Ludwig, J. Claus, R. Fröhlich, and I. Butun, "Networking elements as a patch distribution platform for distributed automation and control domains," Dec. 27 2012, patent App. PCT/US2012/043,084. [Online]. Available: https://www.google.com.pg/patents/WO2012177597A1?cl=en

[21] A. Cook, M. Robinson, M. A. Ferrag, L. A. Maglaras, Y. He, K. Jones, and H. Janicke, "Internet of cloud: Security and privacy issues," in *Cloud Computing for Optimization: Foundations, Applications, and Challenges*. Springer, 2018, pp. 271–301.

[22] I. Butun, B. Kantarci, and M. Erol-Kantarci, "Anomaly detection and privacy preservation in cloud-centric internet of things," in *Communication Workshop (ICCW), 2015 IEEE International Conference on*. IEEE, 2015, pp. 2610–2615.

[23] (2016) Iot testing guides. [Online]. Available: https://www.owasp.org/index.php/IoT_Testing_Guides

[24] B. Krebs, "Who is anna-senpai, the mirai worm author," *Krebs on Security*, 2017.

[25] M. Abomhara *et al.*, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65–88, 2015.

[26] S. Jokhio, I. A. Jokhio, and A. H. Kemp, "Node capture attack detection and defence in wireless sensor networks," *IET wireless sensor systems*, vol. 2, no. 3, pp. 161–169, 2012.

[27] O. El Mouaatamid, M. Lahmer, and M. Belkasmi, "Internet of things security: Layered classification of attacks and possible countermeasures," *Electronic Journal of Information Technology*, no. 9, 2016.

[28] M. A. Iqbal, O. G. Olaleye, and M. A. Bayoumi, "A review on internet of things (iot): Security and privacy requirements and the solution approaches," *Global Journal of Computer Science and Technology*, 2017.

[29] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Com. Sur. & Tut.*, vol. 18, no. 3, pp. 2027–2051, 2016.

[30] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *IEEE Comm. Surveys & Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[31] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society*. IEEE, 2011, pp. 4490–4494.