CloudWoT - A Reference Model for Knowledge-based IoT Solutions

Abdelkader Magdy Shaaban  
University of Vienna  
Währingerstr. 29  
Vienna, Austria A-1090  
shaabana52@univie.ac.at

Christoph Schmittner  
Austrian Institute of Technology  
Giefinggassee 4  
Vienna, Austria A-1210  
christoph.schmittner@ait.ac.at

Thomas Gruber  
Austrian Institute of Technology  
Giefinggassee 4  
Vienna, Austria A-1210  
Thomas.Gruber@ait.ac.at

A. Baith Mohamed  
University of Vienna  
Währingerstr. 29  
Vienna, Austria A-1090  
abdel.baes.mohamed@univie.ac.at

Gerald Quirchmayr  
University of Vienna  
Währingerstr. 29  
Vienna, Austria A-1090  
gerald.quirchmayr@univie.ac.at

Erich Schikuta  
University of Vienna  
Währingerstr. 29  
Vienna, Austria A-1090  
erich.schikuta@univie.ac.at

ABSTRACT

Internet technology has changed how people work, live, communicate, learn and entertain. The internet adoption is rising rapidly, thus creating a new industrial revolution named "Industry 4.0". Industry 4.0 is the use of automation and data transfer in manufacturing technologies. It fosters several technological concepts, one of these is the Internet of Things (IoT). IoT technology is based on a big network of machines, objects, or people called "things" interacting together to achieve a common goal. These things are continuously generating vast amounts of data. Data understanding, processing, securing and storing are significant challenges in the IoT technology which restricts its development. This paper presents a new reference IoT model for future smart IoT solutions called Cloud Web of Things (CloudWoT). CloudWoT aims to overcome these limitations by combining IoT with edge computing, semantic web, and cloud computing. Additionally, this work is concerned with the security issues which threatens data in IoT application domains.

KEYWORDS

CloudWoT, Cloud Computing, CPPS, IACS, Edge Computing, IoT, Semantic Web

1 INTRODUCTION

Cyber-physical Production Systems (CPPS) consist of smart objects cooperating and exchanging information on a global scale. They combine and build on a variety of existing technologies and components such as robotics, industrial automation and control, Internet of Things (IoT), Big Data, and Cloud Computing [18]. IoT is considered a significant improvement for Industrial Automation Control Systems (IACS), where billions of things, with smart data processing capabilities, are connected by the internet [32]. The IoT design is based on smart and self-configuring nodes interconnected dynamically through global network infrastructure [7]. IoT technology has been applied in various application domains such as smart cities, healthcare, automated driving, farming, industrial, logistics, and transportation [23]. IoT things can be remotely controlled as physical devices to perform a particular functionality [16]. That can be achieved by executing the operation on any device having sufficient computational resources [8].

Many limitations are affecting the development rate of IoT technology. Computational power, storage, data heterogeneity, and security are on the top list of IoT challenges [7]. IoT needs support from other technologies to overcome these limitations. However, the integration between IoT and other technologies is a difficult and challenging topic. Accordingly, a reference architecture model is needed to imagine how multiple technologies can integrate into an IoT system. Even more, no explicit model is describing the integration scenario between IoT and other technologies.

This paper proposes, a new IoT architectural model to cope with the limitations of IoT technology. The Cloud Web of Thing (CloudWoT) model integrates edge computing, cloud computing, and semantic web in one model with IoT technology. This model enables IoT things to foster more computational power, memory, storage, energy, and context awareness. Additionally, it provides a standard communication methodology aiming to solve the heterogeneity between things and other cloud resources. Cloud, IoT, and semantic web technologies that have many security issues that have been discussed in different studies. In the course of our research, we proposed a security-aware model for smart agent systems. This model aims to map each security vulnerability in the CloudWoT to suitable security requirements. Our contribution delivers a new IoT model for smart future IoT applications while addressing the
security vulnerabilities which threaten the data integrity in the IoT domains.

This paper is organized as follows. The related work on Industry4.0 and IoT technologies is presented in section 2. Section 3 discusses the importance of integrating Cloud Computing, Edge Computing, and Semantic Web with the IoT technology to overcome the challenges in the IoT domain. The proposed CloudWoT model is presented in section 4. Security issues in CloudWoT model are depicted in section 5. The smart farming and automated driving case studies are discussed in section 6. The paper ends with a summary and presents our plans for future work.

2 RELATED WORK

Industrial technology has been transformed towards a smart manufacturing architecture model which is called Industrial Internet and is one of the pillars of Industry 4.0, which comes as a new advancement concept of the industrial revolution, introducing a broad utilization of Internet technologies. Industry 4.0 involves the technical integration of Cyber-Physical Systems (CPS) into manufacturing and logistics and the use of IoT and other services in industrial processes [15]. That concept aims to integrate diverse technological resources into the industry field, which enables the communication between the two worlds: the physical and the cyber worlds. This integration aims to migrate typical industrial scenarios into a smart one, managed and controlled by machines and intelligent components. This contributes to a new revolution of the industrial concept which will be based on highly automated, intelligent, interconnected, and interoperable production ecosystem across all segments in the value chain and product development lifecycle.

The Industry 4.0 working group in Germany developed a Reference Architecture Model for Industry 4.0 (RAMI 4.0) [36]. RAMI 4.0 is a three-dimensional layered model, mainly concerned with information relevant to assets along its life cycle. Regarding the architecture design of the RAMI4.0, there are some of the benefits of this design [1] [36]:

- RAMI 4.0 is a service-oriented architecture.
- RAMI 4.0 combines all elements and IT components in a layer and life cycle model.
- RAMI 4.0 breaks down complex processes into easy-to-grasp packages, including data privacy and IT security.

RAMI 4.0 aims to describe a system in more details with properties and functionalities to be satisfied in the CPS to be applicable for the Industry 4.0 [36].

RAMI 4.0 is a similar, and compatible structure to IoT approaches. Most of the physical devices, like smartphones, vehicles, sensors, actuators, and other embedded devices will be connected and communicate with data centres, exchange information, and introduce the next massive jump in a scale of data production [38]. The IoT technology is a variety of elements, standards and applications, communicating together through the Internet for simple as well as highly complex applications.

In 2012, the number of interconnected elements was increased to nine billion devices [11]. A wide range of researchers expects the rate of using IoT to increase [22] [38]. The future estimation of the IoT technology assumes that the number of interconnected IoT elements will reach 75 billion around 2020 [25] [38].

3 INTEGRATION OF IOT WITH OTHER TECHNOLOGIES

Cloud computing, Edge computing, Semantic Web, and the Internet of Things are four different technologies which consider the main part of our life. The integration of these four technologies introduces a novel paradigm, for future IoT scenarios.

3.1 Internet of Things (IoT) Architecture

IoT architecture has three major phases. These phases are structured to deliver data from things to production and IT infrastructure. Figure 1 shows, the different phases of the IoT architecture model.

![IoT architectural phases](image)

Phase 1. It is the input/output phase, which connects the IoT system with the external environment. This phase consists of wireless sensors and actuators.

Phase 2. It is responsible for collecting data from/to IO devices and perform analogue-to-digital or digital-to-analogue conversion.

Phase 3. Once the data is digitalized, it requires further analyzing and processing.

3.2 Cloud Computing for IoT Technologies

The cloud computing paradigm offers access to a large amount of computing power by combining and providing various hardware and software resources into a single virtual system. It hides all implementation and management details of software and hardware from the end user. Cloud computing has evolved from technologies like cluster computing and grid computing and has given rise to sky computing [26]. Sky computing is a computing model where resources from multiple clouds are leveraged to create a large-scale scattered infrastructure. Sky computing copes with the difficulty of vendor lock-in and increases the flexibility, transparency and elasticity of the combined infrastructure as compared to that of a single cloud [27].
Cloud computing is a successful service that offers numerous benefits to IoT domains. IoT technology involves millions of interconnected elements that are working together to perform a specific task. These elements are collecting vast amounts of data which needs to be processed and stored. Cloud computing needs to consider a model for big data storage and analysis. The integration between cloud computing and IoT will provide new monitoring services and robust data processing in complex situations [20]. Figure 2 illustrates, the IoT-Cloud solutions in the real environment.

Figure 2: CloudIoT applications

Cloud computing and IoT are expected to be more pervasive and integrated in the future. The integration between these technologies will introduce CloudIoT [7] as a new concept of IoT able to cope with the computational and storage problems.

3.3 Edge Computing with IoT Technology

Regarding the fast development in the number of IoT devices, traditional centralized cloud computing is striving to satisfy the criteria of the quality of service (QoS) for many IoT applications. Calling data from a centralized location will lead to raising rates of network congestions and increasing data exchange latency, which is not acceptable in real-time applications. Edge computing moves the processing units near IoT gateways between the cloud and the source of the data (IoT device). That aims to reduce transmission times and decrease network bandwidth. Also, it helps to keep data private by doing the data processing locally [14]. Edge computing is the best solution to overcome the problem of the IoT data processing over the cloud [38]. Figure 3 illustrates, a simple structure of the edge computing technology.

The structure has three hierarchical layers; each one has its contents. The lowest layer contains all IoT field devices such as sensors, motors, pumps, robotic arms, turbines and others. These devices generate a lot of information from the environment. The middle layer contains edge networks, which make data computation close to the sources of data. The upper layer, managing the storing process and handling the big data, which needs high computational power.

3.4 Semantic Web in IoT Domains

The semantic web describes data in terms of well-defined vocabularies and comprehends both data and knowledge to cope with the semantics itself. It provides standard formats and protocols enabling data to be exchanged among various devices. World Wide Web Consortium (W3C) [37] defines several standards of the semantic web as XML, RDF, RDFS, OWL, and Ontology. Semantic Web makes machines need to act more intelligent to comprehend the semantics of the data [17]. Figure 4 illustrates, the semantic web architecture.

The syntax and semantics are two major parts representing the structure and the meaning of the semantic web. The XML and XMLS represent the structure or the grammar of the semantic web. Resource Description Framework (RDF) is a general-purpose language used for representing information in the Web. Where RDF schema is only for describing simple RDF vocabularies on the Web; the RDFS or Resource Description Framework Schema is an extension of RDF which can be used to describe the basic concepts of the syntax of RDF. Web Ontology Language (OWL) provides an
additional vocabulary which represents sophisticated knowledge about the things, and relations between elements [37] [3].

One of the most significant challenges in IoT technology is the diversity of things, which have the difficulty to understand each other regarding the heterogeneity of their data formats. Semantic technologies have been noticeably effective to address the heterogeneity challenge between things. The semantic technologies can deduce new knowledge to build smart applications and maintain interoperability at data processing, management and storage [12]. Combining semantic web with IoT paves the way for a new concept of technology named Semantic Web of Things (WoT). This integration introduces a new generation of IoT technologies able to cope with the data diversity of the future implementation of intelligent things.

4 CLOUDWOT: CLOUD WEB OF THINGS

In IoT, millions of sensors and devices are generating a big amount of data and exchanging messages through multiple network channels like machine-to-machine communication [38]. The communication standards are essential criteria to make the processing and storing of data possible. Many challenges are facing the adoption of standards within IoT; here are the main three points [4]:

- The structure of data: the heterogeneity of the data formation makes the handling process is impracticable.
- The data formats: regarding the diversity of devices in IoT makes the communication between these elements difficult.
- Limitation of the processing capacity: the data collected from IoT devices need to be processed for the decision making.

This work realizes the importance of semantic technologies; various IoT applications have been suggested to address the data heterogeneity issues using the semantic web technologies [5] [12].

Similarly, edge computing aims to introduce a new methodology to solve IoT computation demands. Edge computing migrates the data computation units to the nearest point to the source of the data. Therefore, many computation nodes will be allocated across the network, which leads to decreased computational stress at the data center. This helps to reduce the latency of data transfer over the cloud. This structure is considered a suitable solution for real-time IoT applications [38]. In addition, this workproses to integrate the cloud technology to allow IoT to use the adequacy of cloud computing for accessing unlimited capabilities of resources over the cloud [7].

Figure 5 illustrates the structure of the proposed CloudWoT framework which integrates four different technologies to introduce a newly developed model able to be used in future smart IoT solutions.

- **Field Layer:** this layer accommodates sensors able to receive information from the environment and actuators able to control and affect the world around. For example, in a smart grid, sensors collect data for grid conditions, recognizing outages, overloads or faults, then after processing the actuators can be controlled, alarms can be triggered or something similar depending on the situations can be caused.

- **Communication Layer:** this layer collects and exchanges data from different things in distributed locations. The communication among IoT devices could be wired or wireless connections. The most common communication type in IoT is the wireless connection. Protocols which are used in IoT applications are Internet Protocol Version 6 (IPv6), Low power Wireless Personal Area Networks (LoWPAN, ZigBee, Bluetooth Low Energy (BLE), and Near Field Communication (NFC)) [2].

- **Data Processing Layer:** this layer has semantic web middleware which generates common data formats and vocabularies to maintain the interoperability of the data in processing, management and storage [12]. For fast responding, edge computing is the best solution for critical data processing at the nearest point to the source of data. Microsoft recently announced an IoT Edge technology called Azure IoT Edge. Azure IoT Edge is a new service for deploying and running artificial intelligence (AI), Azure services, and custom logic directly on cross-platform IoT devices [10]. The third layer integrates the edge computing, to improve the performance of the data transmission and increases the computational power.

- **Cloud Computing Layer:** this layer is concerned with storing the data and managing the data processing which needs high computational power. Smart applications in IoT technology in many cases require more computational power and big data storage than locally available. Therefore, cloud technology will be the best option to interact with IoT things like sensors, cameras, regulators, and controllers which require a massive data warehouse. In complex data processing situation, cloud computing is the preferred solution in a big computational scenario [24].

5 SECURITY ISSUES IN CLOUDWOT

Security aims to protect computer systems and information from numerous illegal acts: hacking, intrusion, data disclosure, or damage to information intentionally. Information security involves three main dimensions: confidentiality, availability, and integrity. Information security is concerned with application security, management of security, compliance with security standards with monitoring and mitigating a broad range of threats. Summarized security supports the achievement of business success by reducing the impacts of information security incidents. Information security can be achieved by choosing risk management, policies, processes, procedures, and other security solutions to protect assets. Furthermore, a systematic and standard based approach such as an information security management system ISMS [13] should be applied to manage sensitive information so that it remains secure. ISMS is a big family of policies and procedures for managing sensitive data [19]. The target of an ISMS is to minimize risk and to limit the impact of a security breach. ISMS analyses security requirements for the protection process of information and applies appropriate controls to ensure the protection of this information. ISMS is based upon risk assessment and the organization’s risk acceptance levels designed to treat and manage risks effectively [19] [13].

IoT applications increasingly use commercial-off-the-shelf (COTS) network devices that are inexpensive, and inefficient. These devices may increase the opportunity for cyber-attack against the whole system. As explained earlier the concept of CloudWoT consists
of different and separate technologies, each one of these has various security vulnerabilities. The following subsections discuss the security issues in cloud computing and semantic web technology.

5.1 Security in IoT

Connecting IoT devices is considered a critical security issue, which must be addressed to provide secure digital access to those devices. Many studies have discussed the security issues in the IoT technology. The most common security standards in the IoT domains are the International Organisation for Standardisation (ISO) 27000 and IEC 62443 for information and control system security respectively [34]. The ISO/IEC 27000 family of standards helps organizations to keep information assets secure [9]. The security standard IEC 62443 provides the cybersecurity requirements for the industrial components of IoT technology. The recommended solution is to divide the IoT system into several components/zones able to mitigate the security risks from the other parts in the system [6] [31]. This solution divides the system into zones, determines security levels for each zone and defines security capabilities that enable a component to be combined into a system context at a given security level (SL) [31]. The security standards IEC 62443 provides the cybersecurity requirements for the components of IoT technology.

The IEC 62443 aims to break down the system components into zones named security zones based on required security levels [31]. Each zone has its data authorization and authentication requirements. These zones help to isolate damage and restrict the impact of low trust zones on higher trust zones [6]. Besides, IEC 62443 standard offers a framework that addresses current and future security vulnerabilities in industrial systems [31].

Figure 6 shows a simple IoT example, where sensor and actuator devices are connected with a field IoT gateway. Then, the data is transferred to a data factory for data storage, processing, and other activities. Afterwards, the data is stored in the cloud. This example has two separate zones, the IoT Device Zone, and Trust Boundary, and each one has a combination of different IoT devices. The zone is noted as a dotted red rectangle; it represents a transition of data from one source to target. During this transition, the data could be subject to different types of threats (i.e. Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege (STRIDE)).

The Microsoft threat modelling tool [35] helps to identify various security threats which threaten the whole system. By applying this example to the threat modelling tool, there are 42 threats identified. Table 1 explains the details of one of the spoofing threats which are detected by the tool.

| Category | An adversary may spoof a device and connect to field gateway |
|----------|-------------------------------------------------------------|
| Justification | <no mitigation provided> |
| Possible Mitigation(s) | Authenticate devices connecting to the Field Gateway |

Table 1: Examples of spoofing threat
This table explains a spoofing threat, which an adversary may spoof any of the IoT devices in the IoT device zone and connect to the field gateway. That may be achieved even when the device is registered in the cloud gateway since the field gateway may not be in sync with the device identities in the cloud gateway.

5.2 Information Security in the Cloud

Information stored over the cloud needs to be kept confidential, maintaining the integrity, and availability. Figure 7 shows a simple sketch about the scenario of storing data remotely over the cloud. Both, the Internet and the cloud are insecure; there are many security vulnerabilities which threaten the data security, privacy, availability and integrity.

Database as a Service (DBaaS) is one of cloud computing’s secondary service models and a key component of anything as a service (XaaS). DBaaS consists of a database manager component, which controls all underlying database instances via an API. DBaaS protects application data for large-scale web, and mobile apps can be complex; especially with distributed and NoSQL (Not only SQL) databases. There are several security difficulties of DBaaS infrastructure [21]:

- **Availability**
  - DOS (Denial of Service) Attacks, natural disasters, equipment failure.
- **Access Control Issues**
  - Physical, personnel and logical control missing on organization’s internal and DBaaS Provider’s employees.
- **Integrity Check**
  - Need to avoid modification of configuration, access and data files.
  - Require accuracy and integrity of data.
- **Auditing and Monitoring**
  - Important for avoiding failures, backup maintenance, configuration of auto fail-over mechanisms.
- **Data Sanitization**
  - Recovery of data by malicious sources if not properly discarded.
- **Data Confidentiality**
  - Unencrypted data in memory, disk or in network may cause data breaches.
  - Co-located application data is vulnerable to software bugs and errors in the Cloud.

5.3 Security Issues in Semantic Web

The semantic web consists of various kind of data which need more confidentiality and privacy. Several attacks can disclose the sensitive information of the semantic web to malicious users and their agents.
The design aims to map each element of the query engine with the security viewpoint in order to facilitate security-related activities and to support security management. The proposed security viewpoint includes most of the security requirements to handle existing security gaps. It has four categories as security requirements, security analysis, security design, and security verification and validation [19]. The security design describes the security methodology of the CloudWoT components. Lastly, the security verification and validation come at the last cycle to confirm that the security requirements satisfy the actual requirement. The loopback arrow means restarting this cycle in case of the chosen security requirements are not viable [19].

As a part of our research towards the security analysis process, we developed the Model-based Security Requirement Management Tool (MORETO) as a tool for security requirements analysis, allocation, and management using modelling languages such as SysML/UML. MORETO is developed by AIT Austrian Institute of Technology, at the centre for Digital Safety and Security. It offers the versatility of the modelling process in various SysML diagrams. MORETO is an Enterprise Architect (EA) plugin for managing the IEC 62443 security standard. EA is a visual modelling software and design tool based on UML provided by Sparx Systems [33]. MORETO is reliable and flexible to model safety & security requirements suited to different components and system architectures.

6 CASE-STUDIES

This section shows how the CloudWoT proposed model can be applied into two different examples. The first case-study based on the smart-farming scenario and the second one is the automated-driving. These two examples describe briefly how the various components can be integrated regarding the hierarchical structure of CloudWoT model (e.g. Field, Communication, Data Processing, and Cloud Computing).

6.1 Case-Study one: Smart Farming Example

Smart Farming is one of the IoT and Industry 4.0 application which concerns the agricultural domain. The agricultural domain has several challenges, such as the shortage of the number of the labours, and the declining attractiveness of agriculture jobs. Future farming needs integration with the new technologies to adopt and expand production processes. “Smart Farming” applies and combines smart things with approaches from industry4.0 and smart mobility to address the challenges and develop a holistic system. Figure 11 illustrates a simple example of the IoT Smart Farming in the context of the CloudWoT structure which discussed in section 4.

The example divides the components of the smart-farming regarding the CloudWoT layers (e.g. Field, Communication, Data Processing, and Cloud Computing). The sensors in the field detect bugs and detect the change in the environmental conditions. The data travel through the communication channels via network devices, then the data send to semantic web middleware to generate common data formats and vocabularies regarding the diversity of the communication protocols from network devices. The edge points enable fast reaction, adaptation and simultaneously control actuators and automated vehicles in the field. The automated vehicles compensate for the decreasing rate of the labour power in the agriculture domain; plus, maintaining the farming precision by managing the feedback between field elements and actuators. The cloud integrates for storing data in the backend, allows charters simultaneously and monitors long-term trends and analyzes production rate and conditions over the years [28].
The necessity in this work is the safety and security of all involved system components [30]. Sensors and actuators in the agricultural domain must cope with higher needs on the robustness against damages. At the same level of the importance is the security of these components against a different type of attacks. The semantic web faces many security issues which threaten the integrity of the data itself. Additionally, the safe operation and secure communication are critical topics in the automated farming vehicles which need more concern in the future plan [28]. These issues with the technical details will be addressed in the recently started project Aggregate Farming in the Cloud "AFarCloud". 

6.2 Case-Study Two: Automated Driving

Automated driving research is one of the IoT applications which concerns the traffic domain. Automated driving is taking place in complex and multi-modal environments; smart urban mobility needs approaches which interconnect vehicles with other road users and infrastructure. The main advantages of connected vehicles are the reduction of accidents rate and improve the traffic efficiency based real-time traffic monitoring and control.

Current approaches towards stand-alone vehicles are sufficient for highway or country roads, but not for urban environments. For the urban environments, it is essential to integrate automated driving vehicles into a smart transportation system to enable the vehicle to interact with the environment around. Future automated driving needs the cooperation of all stakeholders, i.e., automotive Original Equipment Manufacturers (OEM), infrastructure providers and road service operators, transport facilitators, end user, physical and ICT infrastructure providers, and authorities [29].

Regarding the context of the CloudWoT structure which was discussed in section 4. Vehicles and other road elements such as RoadSide Unit (RSU), smart traffic signs or smart traffic lights are interacting together by broadcasting information about the position

---

1https://www.ecsel.eu/projects/afarcloud
of cars, car condition, or speed. The data travel through communication channels via network devices, then the data is sent to a semantic web middleware to generate a standard data format and vocabularies regarding the diversity of the communication protocols of network devices. The edge points enable fast reaction, adaptation, and simultaneously control the traffic from different traffic situations like nonexistent barriers, road works or vehicle positions ahead leading to slowing down or even stopping the traffic culminating to accidents [29]. The cloud is used for storing data in the backend and allows to simultaneously monitor the traffic for a larger environment (city, highway system).

6.3 Security Analysis in Use-cases
For the security analysis process, we applied the MORETO tool on the smart-farming and automated-driving examples based on the proposed CloudWoT model. MORETO scans all of the components in both cases and generates a list of security requirements based on IEC 62443 standard for each modelled element separately. Many security gaps have been detected by the MORETO tool; however, figure 12 illustrates a list of security requirements for the gateway device.

As illustrated in figure 12, there is a list of security requirements for the gateway device which includes network segmentation, session integrity, session lock, auditable events, and other relevant security standards. The user can check the contents of each of the generated security requirements by double-click on any one of these. Then, MORETO opens a new sub-form which has a full description of the security requirement based on the documentation of IEC 62443 standard.

Finally, MORETO creates a comprehensive report, describing the security gaps which are identified, and the security requirements which have been selected to cover these gaps.

Figure 11: A simple smart farming example based on the CloudWoT proposed framework

Figure 12: Security requirements of the IoT gateway device

7 CONCLUSIONS AND FUTURE WORK
This work introduced a new architectural model named CloudWoT. CloudWoT combines four distinct technologies (i.e. IoT, edge computing, semantic web, and cloud computing) to present a newly advanced framework able to be applied to the future IoT applications. Edge computing is integrated with this work to migrate data computation or storage to the network “edge” near the data source, which improves the system response time against urgent
situations. The semantic technology is considered an integral part of the CloudWoT model. It helps the IoT to overcome the challenges of data diversity and heterogeneity. For complex data processing, and storing a huge amount of data, the cloud technology is included with the CloudWoT model. CloudWoT model is applied to smart-farming and automated driving examples as applications of modern information and communication technologies in the IoT domain. Additionally, this work discusses security issues in the CloudWoT framework and integrate the security viewpoint model with the hierarchical layers of the CloudWoT model. Security viewpoint model purposes to be combined with the CloudWoT model, which able to map security breaches of the components of the CloudWoT with one or more of security requirements. That aims to minimize impact in anticipation of security vulnerabilities when security flaws are detected. This integration will be a new methodology for building future secure IoT applications, which considers as different as other IoTs’ middlewares or frameworks. Furthermore, MORETO tool applied for security requirements analysis on the smart-farming and automated driving examples. MORETO scans all the components of these two case-studies and generates a list of security requirements based on IEC 62443 standard for each modelled component separately. The future work will include the technical details of the how the layers of the CloudWoT proposed model could be connected and interacted. Moreover, investigates security measurements in the CloudWoT to cover security vulnerabilities against internal or external attacks.

ACKNOWLEDGMENT

The authors would like to thank DI (FH) Erwin Kristen for his support and help. “AfarCloud” is partially funded by the EC Horizon 2020 Programme, ECSEL JU, and the partner National Funding Authorities (for Austria these are bmvit and FFG) under grant agreement #783221.

REFERENCES

[1] RAMI 4.0 (Part 1): Smart Electronic Industry 4.0 Architecture Layers. https://dzi.zone/articles/part-1-rami-4-0-startup-of-smart-electronic-industr.
Accessed: 03.07.2018.
[2] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzahabi. Internet of things (iot) communication protocols. In Information Technology (ICT), 2017 8th International Conference on, pages 685–690. IEEE, 2017.
[3] W. Alakwaa and A. Salih. Ontology modeling profile, an extension for the ontology uml profile. International Journal of Computer Applications, 6(12):21–28, 2010.
[4] A. Banafa. Three major challenges facing iot. https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot.html. Accessed: 2018-06-30.
[5] P. Barnagli, R. Tönjes, J. Höller, M. Hauswirth, A. Sheth, and P. Anantharam. Citypulse: Real-time iot stream processing and large-scale data analytics for smart city applications. In European semantic web conference (ESWC), volume 2014, sn, 2014.
[6] D. Betts and B. Lamos. Internet of things security architecture. https://docs.microsoft.com/en-us/azure/iot-foundamentals/iot-security-architecture. Accessed: 2018-07-16.
[7] A. Botta, W. De Donato, V. Persico, and A. Pescapè. Integration of cloud computing and internet of things: a survey. Future Generation Computer Systems, 56:684–700, 2016.
[8] J. Deling. Iot automation: Arrowhead framework. CRC Press, 2017.
[9] I. F. O. for Standardization. Iso/iec 27000 family - information security management systems. https://www.iso.org/isoiec-27001-information-security.html. Accessed: 2018-07-20.
[10] K. Gremban. What is azure iot edge. https://docs.microsoft.com/en-us/azure/iot-edge/about-iot-edge. Accessed: 2018-07-09.