

The Role of IoT and Cloud Computing in Health Monitoring Systems

E. G.M. Petrakis, S. Sotiriadis, T. Soultanopoulos, P. Tsiachri Renta, K. Tsakos

School of Electrical and Computer Engineering

Technical University of Crete (TUC)

Chania, Crete, Greece

Abstract—Cloud computing emerges as the key platform for IoT data storage, processing and analytics due to its simplicity, scalability and affordability (i.e. no up-front investment, low operation costs). Remote patient monitoring in particular can benefit from this technology in many ways: (a) the new solution is acceptable by many user categories and provides invaluable assistance to chronic patients and the elderly, (b) it is expected to increase users autonomy and confidence and enable self-managing of their condition with the help of caregivers remotely, (c) it reduces the need for face-to-face appointments with doctors and days in hospital. This work reviews key challenges for reliable and secure remote health monitoring based on experience and lessons learned from applying the above technology to the problem of real-time data collection using both wide-range and short-range wireless protocols and health sensors.

Index Terms—Cloud computing; Internet of Things; Remote patient monitoring; Health sensors; Bluetooth; LoRa

I. INTRODUCTION

Internet of Things (IoT) and cloud computing are getting prominence over the recent years, due to the increasing usage of smart devices and sensors in many application areas (e.g. assisted living, remote health monitoring etc.). The widespread use of smart devices and sensors acting as data aggregators connected to the cloud (over the internet) where data are transferred for storage and analysis, shape a promising future and a great opportunity for new businesses to increase their clients and support new functionality. Cloud is the ideal platform for deploying IoT applications and many of them have been implemented in commercialized platforms [1].

Existing work on remote patient monitoring focus on (a) synergies between the sensing environment and the cloud, (b) device to platform connectivity and data aggregation, (c) persistent data storage, (d) data analysis and decision making. Biswas and Giaffreda [2] focus on the identification of requirements for ubiquitous accessibility, connectivity, dynamic user management and scalability. Theummler et al. [3] focus on infrastructure requirements considering patient monitoring parameters, the nature of data (e.g. images and multimedia), user interactions (e.g. between patients and health providers) outside the hospital. Emerging infrastructure technologies for supporting high quality services include narrow-band IoT such as Low Power Wide Area Networks (LPWAN) [4], Edge computing [5] and 5G [6]. 5G in particular (the new cellular

standard) will not only support mobile telephony but also services through net slicing: different bands of the spectrum are assigned to support services in different application domains (e.g. remote health monitoring and personalized medicine in the narrow band). Telecom providers can operate services such as Software Defined Networks (SDN) and establish Virtual Private Network (VPN) services specifically for healthcare providing increased security of the communications.

Petrakis et al. [7] introduce services for data collection using Bluetooth sensors and smart devices (e.g. mobile phones) as gateways. Guoqiang et al. [8] propose a configurable smart IoT gateway supporting different communication protocols. IoT data are translated to JSON and are transferred to the cloud. Douzis et al. [9] introduce micro and macro-benchmarking techniques for IoT gateway devices. Balabanis et al. [10] propose an activity monitoring solution using motion sensing devices (i.e. Microsoft Kinect¹). The system provides assistance to people who are hospitalized or at home and their condition requires uninterrupted monitoring.

Emerging technologies and technological challenges that will shape the remote health monitoring landscape are discussed in Sec. II. iTaaS approach for IoT data collection (at network front-end) and for processing health data in the cloud (back-end), is presented in Sec. III. Lessons learned from integrating LPWAN technology for enhancing patient autonomy and Quality of Service (QoS) in the remote patient monitoring scenario are discussed as well, followed by conclusions, system extensions and issues for future research in Sec. IV.

II. RESEARCH CHALLENGES

Most IoT systems address the requirements of a single domain focusing on scalability, availability, user friendliness and performance. Others, are fully customized solutions or they have not been designed based on standards [11], [12]. Important issues such as openness and interoperability are not considered at all. Future work in IoT systems design should go beyond these limits and towards more secure, open, re-configurable systems.

¹<https://developer.microsoft.com/en-us/windows/kinect>

A. Security Challenges

Although cloud infrastructures are considered to be secure, IoT is generally less protected than the cloud. New security issues emerge also due to the fact that IoT nodes may be untrusted. Regulatory entities recommend that the principles of security by design and security and privacy by default² should be applied to IoT. The Security Framework³ by Industrial Internet Consortium (IIC) highlights the need for monitoring devices, networks and applications at the edge of the network and the cloud [13]. The security pillar of the OpenFog reference architecture [12] specifies the FaaS (Fog-as-a-Service) security monitoring functionality for devices at network end. EU's GDPR⁴ has a significant impact on IoT systems design. Data protection in e-health is crucial, as potential intrusion may not only lead to vulnerable systems (e.g. susceptible to personal data theft) but also lead to risks in human life (e.g. disruption of important sensors monitoring patients etc.). An IoT deployment should use latest virtualization and security technologies to enhance the performance of IoT platforms [14]. Anonymization, pseudonymization and data protection techniques can also be applied to avoid exposing data to unauthorized third parties. Distributed and hybrid identity and authorization management must be applied (e.g. un-authorized access to data and services is protected by OAuth2.0⁵).

B. Low Power Wide Area Networks (LPWANs) and 5G

IoT manufacturers have developed products (e.g. sensors), which typically use short range protocols such as Bluetooth⁶ and later Bluetooth Low Energy (BLE) to connect to a gateway (a smartphone or tablet) and then to the cloud via some backhaul (e.g. a cellular network and the internet). However, the commercial success of this solution is questionable as the number of IoT devices (sensors) that can be connected to a smart device using Bluetooth is limited (especially for sensors and gateways running on battery and unless the gateway is connected to a sustainable power source). Bluetooth and BLE, the same as WiFi and Zigbee, are not suited for long-range performance, while cellular networks are costly, consume a lot of power, and are expensive.

Low Power Wide Area Network (LPWAN) technologies [4] fill the gap between cellular (e.g. 3G, 4G, LTE) and short-range wireless (e.g. Bluetooth, WiFi and ZigBee) networks. The trade-off is the achievable data and error rate (i.e. LPWAN protocols do not guarantee delivery of data packets). LPWAN technology falls short in terms of QoS compared to cellular standards and this means that an operator cannot use it to provide the kind of Service Level Agreements (SLAs) that are critical for customers (e.g. fast paced applications requiring high speed collection of large data volumes). However,

LPWAN specifications fits well the requirements of many IoT applications (e.g. smart cities, home automation, industrial automation, environmental monitoring, e-Health) who need to transmit to gateways small data quantities periodically over a long range, while maintaining long battery life (e.g. a wearable health sensor that only transmits when vital measurements exceed some predefined threshold).

LPWAN networks are being deployed now because the cost to deploy the network in unlicensed bands requires much less capital than the cost of its 3G, 4G counterparts. SigFox⁷ and LoRa⁸ are the main competitors in this landscape. The same do other technologies such as Weightless, Ingenu, NB-IoT, and LTE-M⁹ which enable long range devices to be connected to telecommunication networks with the latter two been standardized within 3G and 4G respectively. Typically, an IoT application can be deployed only if the network is already there. However, for vendors that need to deploy IoT applications on their own and run the network by themselves, LoRa is a good option. LoRa supports 2-5Km ranges in urban areas (entire cities can be covered with a few LoRa antennas) and up to 15Km in rural areas. It works in the unlicensed spectrum below 1Ghz which come at no cost. It is an asynchronous protocol, which is optimal for battery lifetime and cost. There are no royalty issues with LoRa (except of the LoRa modulation chip which is produced by Semtech¹⁰).

Leveraging 5G capabilities (i.e. ubiquity, integrated security and network management) a network of LoRa devices can be developed anywhere, without installation of additional network equipment and without the need for network management (which is offered by the cellular network). 5G technology comes with its own authentication, authorization and accounting framework thus minimizing the effort to supporting this functionality in LPWAN networks. Soon, telecom providers will support LPWAN functionality and synergy with 5G.

III. IOT FOR REMOTE HEALTH MONITORING

Holistic approaches based on the integration of recent technological advances in sensor protocols and showing seamless integration of edge and cloud technologies are still missing. iTaaS [7] is a contribution towards this direction that puts existing technologies in place and produces an end-to-end-system for reliable and secure remote health monitoring. iTaaS provides the technology foreground to enable immediate application deployments in health care. The needs of a use case are captured and represented as a rule-based service (referred to as Event Service) for handling patient data, health condition in different disease or health care use cases. iTaaS creates know-how for manipulating sensed user data and provision of personalised advice for an individual's health condition or guidance for daily life activity.

²<https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf>

³https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

⁴<https://www.itgovernance.eu/en-ic/gdpr-report-ic>

⁵<https://oauth.net/2/>

⁶<https://www.bluetooth.com>

⁷<https://www.sigfox.com/>

⁸<https://www.lora-alliance.org/>

⁹<https://www.link-labs.com/lpwan>

¹⁰<https://www.semtech.com>

iTaaS transforms a user's mobile device (e.g. a smart phone) to an IoT gateway which allows for fast and efficient data streams transmission to the cloud. iTaaS includes configurations for (a) the IoT side to support data collection from IoT devices to a gateway on a real time basis and, (b) the cloud back-end side to support data sharing, storage and processing. As a proof of concept iTaaS implements a real time remote patient monitoring system that uses Bluetooth Low Energy (BLE) sensing devices. These are low power sensors that support mobile application connectivity to handheld devices which are already connected to the Internet via WiFi or GSM networks. The gateway (i.e. mobile device) establishes a two-way communication between the front-end (i.e. users carrying wearable sensors and the mobile device connected to these sensors) and, a back-end (i.e. the cloud running services for data monitoring by authorized users subscribing to specific users and sensor information). Captured data are encrypted and streamed to the cloud.

iTaaS patient monitoring application brings high level personalization to patients care. It is easy to define abnormal pattern detection rules regarding physical (e.g. walk ability, tremor), medical (e.g. heart-rate, oxygen saturation in blood), socio-emotional (e.g. relatives to rely on, anxiety) activities of the patient. These rules are defined by a formal caregiver (e.g. a physician) based on the actual needs of the patient, they are embedded into the health monitoring scenario and operate on a publish - subscribe model: vital measurements transmitted by sensors are recorded and only subscribed users (e.g. a physician who monitors the patient) have access to this information. In this scenario, caregivers assign sensors to patients and set lower or upper values for sensor measurements. The caregivers get notified when these values are violated (using a messaging service). The proposed coaching solution keeps patients and caregivers in the loop tracking user's progress, providing a monitoring overview highlighting suspicious patterns and coaching instructions.

A. iTaaS Architecture

iTaaS is a Service Oriented Architecture (SOA) [15] designed as a composition of modular micro-services implementing fundamental functionalities communicating with each other and offering important benefits, such as scalability, reusability multi-tenancy, increased accessibility and security through powerful APIs. iTaaS architecture is organized in two processes, the data collection from the IoT system and the back-end cloud. The sensors are embedded or connect to user devices (e.g. smartphones) that send data to the cloud. The services are REST-based [16] and integrate the system functionalities that are grounded upon four zones as shown in Fig. 1.

The "User Device" includes the IoT data source generators notably users, sensors and smartphones. iTaaS utilized two types of BLE sensors, the Polar H7¹¹ recording heart rate and

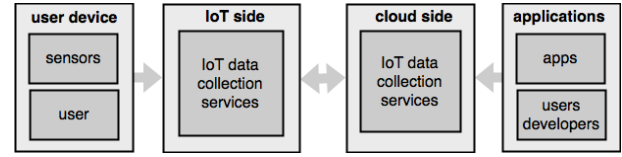


Fig. 1. Generic architecture for data capturing and cloud data management

the Onyx II¹² which monitors oxygen saturation range and heartbeats per minute.

The "IoT side" (gateway) includes various modules such as device pairing, data collection, a lightweight database, linking to the cloud, connectivity, data filtering, event processing and notification services. The gateway supports dynamic and automatic discovery and registration of new sensors: each sensor is declared by its XML schema and this information is registered at the back-end. The gateway runs a service for synchronizing sensors schema information with schema information stored on a local database (so the gateway gets updated about new sensors). The gateway service downloads (from the cloud) the XML schema of the sensors which are entitled to connect and transmit data to the service. iTaaS can accommodate any kind of sensor protocol (e.g. Zigbee) that can be supported by a smart device (the gateway) since the only component that is affected by the decision to select a specific protocol is the BLE scanner (i.e. a service that scans for connected BLE sensors). The rest of the system (i.e. besides the BLE scanner) is sensor agnostic since all data are communicated and processed in a sensor agnostic format (i.e. JSON).

IoT data collection service on the gateway, activates the mechanism to determine which peripheral devices advertise data to the service and establish a GAP¹³ connection with authenticated BLE devices (i.e. sensors in our case). Sensor authentication is carried out by comparing the mac address of the sensor with that defined in the XML. The XML also provides information on what measurements are useful for the application. The respective service implements secure asynchronous communication between the IoT and the cloud. Encoded data are formed in JSON and are exchanged using AJAX calls.

Average sensor values are transmitted to the cloud per regular intervals or on demand. If sensor measurements are within the range of the maximum and minimum thresholds, they are transmitted to the cloud per regular time intervals (e.g. per minute). However, if the measurements violate one of the rules they are transmitted to the cloud per second (i.e. the gateway changes to emergency operation mode).

The local storage service on gateway implements a database using SQLite¹⁴ and a data encryption and decryption module. The database defines the appropriate tables for sensors types (i.e. the XML format of each sensor), sensor measurements,

¹²<http://www.nonin.com/Onyx9560>

¹³<https://learn.adafruit.com/introduction-to-bluetooth-low-energy/gap>

¹⁴<https://www.sqlite.org/index.html>

¹¹<http://www.polar.com>

monitoring rules (downloaded from the cloud). Data encryption (and decryption) is a component that runs prior to data transmission (or receipt) on top of local storage for decoding/encoding data based on the Advanced Encryption Standard (AES). Sensor data can be stored locally and are deleted upon transmission to the JSON cloud storage. For example, data can be stored on local SQLite storage when WiFi connection is lost and transmitted to the back-end when connection is up again.

The cloud implements services for storage, big data processing, publication and subscriptions, event management, user authentication, messaging, services for establishing secure network connections with gateways or users (including encoding and decoding of user data). The big data processing module is responsible for big data analytics (e.g. using Apache Spark¹⁵). Publication and Subscription service acts as a mediator for the data sent to the back-end and the end-users or applications. Using this service, applications or users can subscribe to data produced in the front-end. Sensors are listed as “public entities” and physicians are subscribers to these entities. Each time a new sensor is registered to the system, this component is updated in order to update its context (e.g. sensor name) and its content (e.g. data to be collected such as heart rates). When a new patient-specific sensor is used, a new entity is created. Similarly, when a measurement becomes available by a sensor, a notification is sent to all entities (e.g. users or serviced) subscribed to this information. Data are communicated and processed in NGSI¹⁶, a data exchange format based on JSON.

iTaaS information is stored in the cloud database using MongoDB database¹⁷. The NoSQL format of MongoDB makes it easy to store semi and unstructured data and supports permanent storage for users, sensors, messages, rules, events (e.g. rule violations) and actions undertaken by health care personnel in response to events. All iTaaS services are protected by an OAuth2.0 mechanism. For example, this service checks the database whether to authorize users to access and use the front-end.

Event management service runs also in the cloud and gets input from the publication and subscription service (above). When the sensor data collection service creates a new measurement, the corresponding entities in Publication and Subscription service is updated. The Event Processing service subscribes to this information and gets a notification about the change. This triggers the execution of rules set by the physician (which are stored in the database) to govern the monitoring of the patient wearing the sensor. If the sensor values are within the limits of these rules no action is taken; otherwise (e.g. heart-rate exceeds its threshold), the event monitoring service notifies the physician to take action.

“Applications” or end-users can be (a) physicians (or caregivers) who subscribe to user data, have access to sensor measurements and are entitled to provide coaching instructions

to patients and, (b) administrators or technical specialists that define schemas for new sensors, can create new users and define their access rights. Both, physicians and administrators access the system using a Web application.

iTaaS front-end is implemented in native Android. The back-end is implemented on OpenStack¹⁸ and Fiware¹⁹, an open-source distributed cloud infrastructure funded by the EU. The experimental analysis shows fast data collection, as data is transmitted from the IoT side (i.e. the gateway) to the cloud in less than 130ms. The cloud is capable for responding in real-time to many thousands of user requests and high concurrency (i.e. many requests executing in parallel).

B. Integrating LPWAN into iTaaS

LoRaWare [17] is the technological bridge between LPWAN and the cloud. The focus is on interconnecting LoRa gateways with the cloud. This is a responsibility of the “Network Server” which receives LoRa packets from gateways and ports LoRa payloads to other cloud services. The Network Server applies a sequence of operations (i.e. decrypts, de-duplicates, authenticates LoRa packets) and, finally transforms LoRa packets to JSON format. For outgoing packets the same solution is applied in reverse order: packets are encrypted and transmitted to target gateways.

Fig. 2 highlights LPWAN ecosystem consisting of (a) sensing platform, (b) back-end (cloud) implementing (among other services) a Network Server and, (c) applications which run in the cloud and allow consumers (end-users) to receive information from selected devices (sensors). The sensing environment is implemented based on products by Ideetron. The Lorank8²⁰ gateway enables connection and communication with many thousands end nodes up to many Kms (if mounted on a high point with free sight). Each LoRa Node has one Nexus Board²¹ with a micro-controller and a PCB antenna for the transmission of RF packets. The sensors (e.g. temperature, humidity and motion sensors) are mounted to a Nexus Demoboard which connects to the Nexus Board.

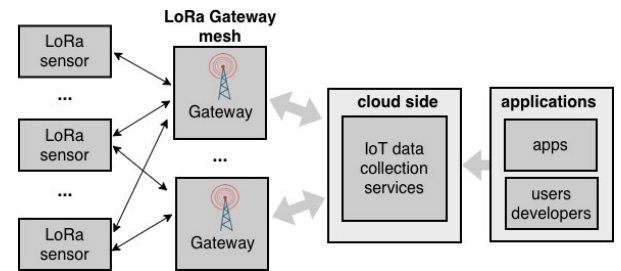


Fig. 2. LPWAN ecosystem.

Sensors are not associated with a specific gateway: data transmitted by a sensor will be received by all gateways in

¹⁵<https://spark.apache.org>

¹⁶<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EU+Standards>

¹⁷<https://www.mongodb.com/scale/nosql-database-comparison>

¹⁸<https://www.openstack.org>

¹⁹<https://www.fiware.org>

²⁰<https://www.ideetron.nl/lora/?lang=en>

²¹<https://webshop.ideetron.nl/LoRa/>

range. Each gateway will forward the received packets to the Network Server. The intelligence and complexity of the LoRa sensing network is pushed to the network server which manages the active connections. The LoRa nodes (i. e. sensors) transmit LoRa modulated packets which are captured by one or more gateways (up-link transmission). A gateway receives LoRa packets from sensors in range and re-transmits them to the cloud (i.e. to the Network server) using an IP protocol (e.g. UDP). This operation is carried-out using the packet forwarder²², an open source software by Semtech which runs on every gateway. Conversely, LoRa gateways receive down-link messages from the Network server from where they are forwarded to LoRa devices.

The Network Server manages active sessions (i.e. devices that have joined the network), serves new LoRa nodes when they join the network, decodes and decrypts the physical LoRa payload, de-duplicates the received packets (which may be captured by multiple gateways), authenticates the packets to make sure that they are not due to attacks (e.g. denial of service attacks). Also, it manages the state of each node using mac-commands (e.g. to change data rate, channels, etc.). Finally, it maps LoRa context (i.e. sensor names, types) and content information (i.e. measurements) to NGSI.

In order to study the range efficiency of LoRa protocol, two Lorank 8 gateways are placed 5.7Km apart from each other. The first one is placed in an urban area and the second one in a sub-urban area of the city of Chania. Two mobile LoRa nodes transmitted 74 temperature and humidity measurements (i.e. 37 each node). The longest effective range was 923m and 1,23Km for the gateway placed in the urban and sub-urban area respectively. The error rate increases with the distance. Despite the high error rate, its worth noting that more than 80% of transmitted packages were received successfully up to 350m and 700m from the gateway in the urban and sub-urban area respectively. These results are below expectations. This could be due to noise interference and the non-uniform ground terrain with many obstacles that hinder transmission in the area of the experiment.

IV. CONCLUSIONS

Holistic approaches showing seamless integration of recent technological advances in protocol, IoT and cloud technologies are still missing. iTaaS is a contribution towards this direction. iTaaS enables engineering of reliable and secure coaching systems able to respond to dynamic and complex situations. Its ambition is to increase acceptance of the solutions by people with minimum exposure to technology (e.g. the elderly). Incorporating Low Power Wide Area Network (LPWAN) protocols into iTaaS is straightforward. The interface to the LPWAN is the Network Server which runs in the cloud. The cloud supports unified management of LoRa payloads with minimum additional effort. The results indicate that lots of experimentation is still necessary for tweaking LoRa parameters in order to achieve closer to the optimal (i.e. theoretical) performance.

The future research direction is the definition of patterns to specific sensor data, in order to allow users to be notified according to different patterns and not only static conditions and thresholds. Extending iTaaS framework to support emerging service provision models dictated by the adoption of new generation cellular protocols (i.e. 5G) coupled with advanced security mechanisms for the cloud and the IoT are challenging directions for future research.

REFERENCES

- [1] A. Vogt and T. Schultheiss, "The iot survey 2019," 2019. Teknowlogy Group.
- [2] A. R. Biswas and R. Giaffreda, "Iot and cloud convergence: Opportunities and challenges," in *IEEE World Forum on Internet of Things (WF-IoT)*, (Seoul, South Korea), pp. 375–376, Mar. 2014.
- [3] C. Theummler, A. Paulin, and A. Lim, "Determinants of next generation e-health network and architecture specifications," in *IEEE International Conference on e-Health Networking, Applications and Services (HEALTHCOM 2016)*, (Munich, Germany), pp. 1–6, 9 2016.
- [4] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Communications Surveys and Tutorials*, vol. 19, pp. 855–873, 11 2017.
- [5] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the internet of things," *IEEE Access*, vol. 6, pp. 6900–6919, 5 2017.
- [6] N. Le, M. Hossain, A. Islam, D.-Y. Kim, Y.-J. Choi, and Y. Jang, "Survey of promising technologies for 5g networks," *Mobile Information Systems*, pp. 2777–2790, 12 2016.
- [7] E. G. Petrakis, S. Sotiriadis, T. Soutanopoulos, P. T. Renta, R. Buyya, and N. Bessis, "Internet of things as a service (itaas): Challenges and solutions for management of sensor data on the cloud and the fog," *Internet of Things*, vol. 3–4, pp. 156–174, Sept. 2018.
- [8] S. Guoqiang, C. Yanming, Z. Chao, and Z. Yanxu, "Design and implementation of a smart iot gateway," in *IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, (Beijing, China), pp. 720–723, 12 2013.
- [9] K. Douzis, S. Sotiriadis, E. Petrakis, and C. Amza, "Modular and generic iot management on the cloud," *Future Generation Computer Systems (FGCS)*, vol. 78, pp. 369–378, Jan. 2018.
- [10] S. Balabanis, S. Sotiriadis, and E. Petrakis, "Internet of things platform in cloud computing for enhanced living," *Cloud Computing for Enhanced Living Environments: Algorithms, Architectures and Platforms (Cloud4ELE)*, *IEEE Cloud Computing*, vol. 3, pp. 28–34, Nov. - Dec. 2016.
- [11] Khanna, D. (2018). Use of Artificial Intelligence in Healthcare and Medicine. International Journal Of Innovations in Engineering Research And Technology.
- [12] O. A. W. Group, "Openfog architecture overview," Feb. 2016.
- [13] K. Nagaraj, C. Killian, and J. Neville, "Structured comparative analysis of systems logs to diagnose performance problems," in *Proceedings of the 9th USENIX conference on Networked Systems (NDSI'12)*, (San Jose, CA, USA), pp. 22–26, Apr. 2012.
- [14] Tadapaneni, N. R. (2016). Overview and Opportunities of Edge Computing. Social Science Research Network.
- [15] T. Erl, *SOA Principles of Service Design*. Upper Saddle River, NJ, USA: Prentice Hall, 2007.
- [16] S. Schreier, "Modeling restful applications," in *ACM International Workshop on RESTful Design (WS-REST'11)*, (Hyderabad, India), pp. 15–21, 3 2011.
- [17] K. Tsakos and E. Petrakis, "Service oriented architecture for interconnecting lora devices with the cloud," in *Proc. of 33rd Intern. Conference on Advanced Information Networking and Applications (AINA 2019)*, (Kunibiki Messe, Matsue, Japan), pp. 1082–1093, Apr. 2019.
- [18] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "Nist cloud computing reference architecture," 2011. National Institute of Standards and Technology, US Department of Commerce.
- [19] T. Garfinkel and M. Rosenblum, "A virtual machine introspection-based architecture for intrusion detection," in *Proceedings of Network and Distributed Systems Security Symposium*, pp. 191–206, 5 2012.

²²https://github.com/kersing/packet_forwarder