Comprehensive Security Framework of an Intelligent Wastewater Purification System for Irrigation

Jose M. Jimenez
Integrated Management Coastal Research Institute,
Universitat Politècnica de València,
Valencia, Spain
jojiher@dcom.upv.es

Lorena Parra
Integrated Management Coastal Research Institute,
Universitat Politècnica de València,
Valencia, Spain
loparbo@doctor.upv.es

Laura Garcia
Integrated Management Coastal Research Institute,
Universitat Politècnica de València,
Valencia, Spain
laugarg2@teleco.upv.es

Jaime Lloret
Integrated Management Coastal Research Institute,
Universitat Politècnica de València,
Valencia, Spain
jlloret@dcom.upv.es

Miran Taha
Department of Computer Science
University of Sulaimani,
Kurdistan region, Iraq
miran.abdullah@univsul.edu.iq

Pascal Lorenz
Network and Telecommunication Research Group,
University of Haute Alsace
Colmar, France
lorenz@ieee.org

Abstract— **Although Internet of Things (IoT) is a growing and evolving technology, attackers are exploiting the multiple weaknesses of IoT devices. Some attackers even employ these devices to perform massive attacks, which can greatly affect the Internet. Furthermore, the data centers for the obtained data from sensing IoT devices are comprised of several devices: hardware, software and the communication equipment. Therefore, the data center requires a secure and controlled environment. It is then evident the necessity of implanting end-to-end integral security in IoT environments. In this paper, we propose an integral security method for our previously published intelligent wastewater purification system for irrigation. The security is performed from the physical device to the data stored at the data center including its transport utilizing different technologies and going through various pieces of equipment.**

Keywords- IoT; Sensors; Actuators; Security; LoRaWAN; Attacks.

I. INTRODUCTION

The Internet of Things plays an extraordinary role in all aspects of life. Moreover, billions of "things" are communicating to each other: from TVs, fridges and cars to smart meters, health monitors, agriculture monitors and wearables. Therefore, communication through wireless networks, cloud computing and data communication among IoTs are increasing [1]. This opens-up exciting new opportunities for research in academia and industry. However, it also opens the door to a variety of new security threats.

The weaknesses of the IoT devices allow accessing the systems where they are being employed. There is a rapid growth of botnets according to the report in [2]. Botnets are a net of bots or robots that can perform autonomously and automatically and can be jointly controlled. If attackers employ these bots, it may lead to major attacks to the Internet. Furthermore, the report indicates that many attacks to the corporative network are unleashed after compromising vulnerable servers and computing resources.

Wastewater treatment systems for irrigation benefit from using different IoT technologies for monitoring and managing information of the irrigation process. A smart irrigation system relies on sensors and online services for improved efficiency. Users can control the system from a remote device and can configure it using a cloud service.

These systems face different types of attacks which can be physical attacks, network attacks and system attacks. For physical attacks, the problem includes destroying or stealing the components of the IoT devices. For communication attacks, the lack of security and vulnerability of the channel for data communication allow the attacker to sniff information from the network. In the system, unsecure data storage allows the attacker to obtain information from the cloud environment. Therefore, unauthorized people may modify and steal information from the system.

There are some existing researches that proposed security measures against the attacks to IoT systems. A design of IoT based on smart security and monitoring for farming is proposed in [3]. Therefore, IoT systems based on smart security and monitoring devices for agriculture are being developed. In the proposal described in [4], real time notifications are provided based on information analysis and processing used for the identification of rodents and threats. Furthermore, IoT challenges and opportunities are presented in [5], where tasks such as trusted sensing, computation, communication, privacy, and digital forgetting are addressed.

In this paper, we analyze and mitigate the security threats faced by a smart irrigation system by designing security architectures that safeguard the IoT devices and data and ensure the correct performance of the IoT system. The main measures can be described as follows:

- Preparing a protective box to protect from the physical damage of IoT components such as sensors, accessing the serial port, and the battery when people or animals tamper with them.
- Providing secure data communication for both wire and wireless connection modes by establishing a VPN (Virtual Private Network) in order to avoid eavesdropping.
- Utilizing a security mechanism to alert and determine the attempt of attacks to the Fog Computing system. Therefore, data encryption and Fog security provides a comprehensive portfolio for cloud service and enterprises.
- Using access management encryption techniques to provide data security when unauthorized people request and want to modify the data.
- Securing the servers at the data center where the data obtained from the sensor nodes is stored.
- Securing the network devices employed to forward the data to the data centers.

The rest of the paper is organized as follows. The related work is presented in Section II. Section III depicts the system description. In Section IV, we present how the system should be secured. Lastly, the conclusion and future work is presented in Section V.

II. Related Work

The security of IoT is important because the world is becoming very sensitive and there is constant fear about threats, thieves and other dangerous situations. Therefore, launching malicious attacks against irrigation systems can have a significant impact on water utilities and their customers. Authors of [6] proposed a smart water management model combining IoT technologies with business processes coordination and decision support systems. They defined the management exploitation layer, coordination layer, subsystems layer, administration layer and the interfaces that enable layer interaction. Their proposed architecture can be used for controlling real water management systems and dealing with many real problems such as physical network definition or mapping identifiers.

The authors of [7] analyzed the security requirements specific to IoT systems by taking into consideration network security, identity management, privacy, trust, and resilience. They presented mechanisms that ensure data confidentiality, integrity, origin authentication and freshness for each IoT technology. A large selection of IoT technologies was analyzed, from single-layer protocols to full protocol stacks.

The security level of LoRaWan (LPWAN, Low Power Wide Area Network) is studied in [8]. It is focused on the security of LoRaWan. The LoRaWan protocol is a MAC (Medium Access Control) layer protocol for LoRa, which provides the communication infrastructure and interfaces for gateway-sensor topologies, node coordination, and medium access. They proposed several countermeasures and changes to the LoRaWan protocol, which rendered all these attack vectors harmless. Many of these countermeasures can be implemented with minimal changes to the LoRa ecosystem.

The authors in [9] proposed a lightweight algorithm, which is based on a set of rules to detect the characteristics of the packets in the network. The proposed approach can detect the malicious packets that are sent to the network. Furthermore, the authors of [10] reviewed the architecture and features of fog computing, including real-time services and fog-assisted IoT applications based on the different roles of fog nodes. They presented security and privacy threats towards IoT applications.

Other authors have studied partial solutions to punctual problems related to the security of the system, but they do not provide an integral solution. The principal contribution of our proposal is an integral security solution for the complete system. It includes structured proposals based on four differentiated categories based on where the attacks are intended for in order to achieve security for all physical devices as well as the flow of forwarded data and stored data. On our proposed solution, we address a wide variety of devices, network equipment and data that integrate different technologies. The use of multiple technologies leads to an increase of the complexity of the solution.

III. System Description

In this section, we will describe the location of the devices and the different technologies used by our intelligent wastewater purification system for irrigation.

As it can be seen in Fig. 1, our system is distributed in different locations. In some of them, we have implemented groups formed by nodes that can contain sensors or actuators. Red circles with black dots inside identify groups of sensor nodes. The black dots of each circle represent a sensor node. Stars identify actuators nodes. The data is transmitted wirelessly using LoRaWan between all the nodes and among the node groups. Besides, there is a remote location, which will be reached through wired technology, where our data storage center and the equipment to carry out the work with Artificial Intelligence (AI) are located.

Both the sensor nodes and the actuator nodes are distributed in external locations. For this reason, they will be protected by integrating them in watertight boxes to withstand water, weather variations and possible animal attacks.

From one of the group of nodes, that is located in an urban area, a WAN connection is established with the remote location through an Internet Service Provider (ISP). In the remote location, the network devices that are connected to the ISP and to the different available equipment are deployed. The Data Center and the equipment that utilizes AI to process the information collected by the sensors is deployed at the remote location as well. Behavior patterns will be detected through AI and decision rules will be applied in the actuator nodes according to the detected patterns.

The vulnerabilities of the systems to control water, which is performed through actuator nodes in our water

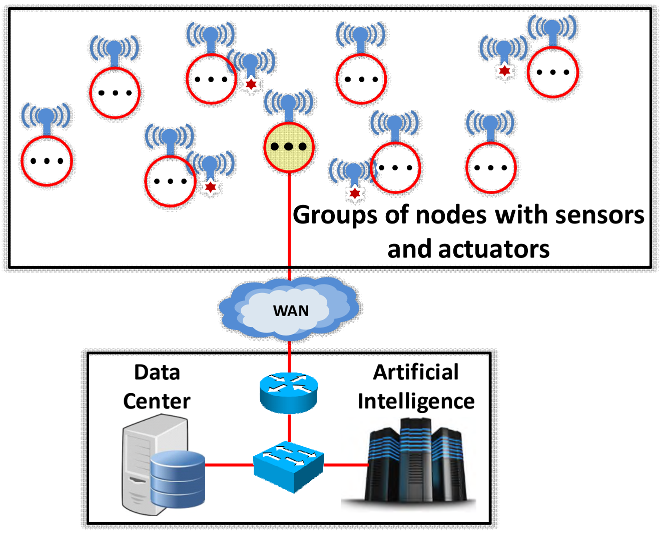

Figure 1. Location of devices and equipment.

management proposal, may compromise the objective of our system. Severe problems of both irrigation saturation and shortage as well as an unwanted lack of control of the water purification system may be generated. Furthermore, attackers may obtain the control of the nodes so as to perform massive attacks, which may affect the Internet.

IV. Securing the System

For our system, it is paramount to guarantee the availability and accessibility to all the devices at any time.

At the report in [2], an attack to a water and wastewater treatment plant managed by an international company, the attackers compromised the internal network by launching an attack from a server located on the demilitarized zone (DMZ). It was discovered that the attackers performed the following steps:

- The DMZ server had been violated due to a bad policy that allowed establishing RDP connections.
- The server was violated and controlled through different IPs (Internet Protocol) by different attackers that were enemies to the company.

Those attackers performed more attacks to other plants of the same company.

All systems that manage information or provide a service are susceptible of being attacked. Irrigation and water management systems may not manage information that must remain private but ensuring the correct performance of the system is crucial. Furthermore, these systems are not only susceptible of attacks from people with malicious intentions but also may be affected by animals, weather conditions and people that accidentally compromise the system. The scenario where people is interested in controlling the waterflows of the canals according to their own interests is also possible.

The main problem with IoT devices is that they are not designed considering that their security is paramount on certain fields. Once the network security is stablished, it is important to perform a penetration test on the different components that comprise the system so as to verify the effectiveness of the solution.

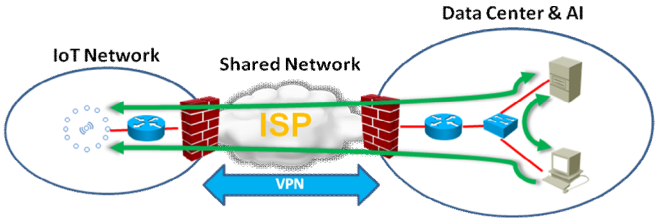

Figure 2. Basic scheme of security and data flow.

In the next sections, we describe and propose the solutions for our system. Fig. 2 shows the basic security scheme that we will implement on our system. The three network areas that we are going to utilize can be observed. They are the IoT network area, the ISP network area, and the network area of the data center and the AI equipment.

As it can be seen, two firewalls will protect the areas of the network that belong to us from the shared network. The green arrows represent the data flows that will be established between the IoT network, the data center and the AI. Considering the way the system performs its functions and its vulnerabilities, attacks can be classified into four categories: physical attacks, attacks on the data in transit, attacks on the management system and attacks on the data.

A. *Physical attacks*

Physical attacks comprise those attacks that require the physical access to the device. In the case of our proposed system, removing the sensors, accessing the nodes through the serial port or removing the batteries are some of the physical attacks that can be performed.

Another important thing to consider in our system is the possible presence of animals that could bite the wires or take the devices. Thus, nodes should be enclosed on a protective box so as to protect the device from possible attackers and the elements. The box should include a combination lock and the password to the lock should only be known by the administrator of the system. Moreover, considering that the nodes are deployed over several irrigation canals, there is a possibility of losing the devices in case of flooding or extreme rain. This security issue cannot be avoided, but the system includes the mechanisms so as to alert of malfunctioning or lost nodes. Therefore, the administrator would know to replace the damaged devices in case of these types of events.

It is also important to consider that most of the nodes, as well as network devices and the computers employed on our system, are provided with different access ports. For all the equipment, we will only utilize the ports necessary to transmit the information or to access the administration of the different devices and equipment. We will disable the rest of the ports so as to avoid the unauthorized access from attackers external to the project.

Another important remark is reducing the usage of USB (Universal Serial Bus) memory drives or other external memory devices. These elements are connected to the computing resources and may be infected with malware. By utilizing just the necessary ports and previously analyzing them, it is possible to avoid subsequent attacks. Furthermore, physical security is also very important at the transmission network and at the different storage and computation devices.

B. *Attacks on the data in transit*

These attacks would aim at making the system unable to communicate or intercepting the transmitted data so as to gain knowledge on the information gathered by the system.

It is necessary for our system to be protected against eavesdropping and tampering. In order to achieve it, the combination of forwarded data encryption and the protection of the networks where the transmission is performed should be performed. Attackers may try accessing through the physical network infrastructure or through the software components provided by the services of the network itself. The impact of an attack performed utilizing software components would probably be greater [11].

Our proposed system utilizes both wired and wireless communication, and both types of communication should be secured. The most effective way of establishing greater security over the wired network is having a proprietary telecommunications service comprised of an optic fiber network. However, this proposal is not viable. For this reason, for the wired communication, a VPN will be established so as to avoid eavesdropping and access to the network.

As for LoRaWan, replay attacks, jamming techniques and wormhole attacks could compromise the communications [8]. Replay attacks consist on fooling the device by utilizing old information that has been retransmitted. However, the attacker should know the channels and the employed frequencies so as to sniff the transmission. This attack is addressed by keeping track of frame counters as seen in Fig. 3. Jamming consists on disrupting radio transmissions by transmitting high power radio signals in the vicinities of the nodes. The spreading factor and transmissions on the same frequency may cause interferences among the devices. Although this attack is difficult to avoid, it is easier to detect, and proper actions can be taken so as to re-establish communication. If the nodes of the network begin to lose the connection, the communication frequency should be changed. Lastly, wormhole attacks consist on capturing packets and replaying to the source so as to avoid them reaching the gateway. Regretfully, this type of attacks is hard to detect but utilizing previous analyzed data, abnormal behaviors could be detected.

Authentication between end-device and the network is one of the implemented security measures. Moreover, LoRaWan also incorporates end-to-end encryption [12]. It utilizes AES (Advanced Encryption Standard) with CMAC (Cipher-based Message Authentication Code) and CTR (Counter) to provide integrity and encryption respectively. The authentication is performed with a unique identifier and 128-bit AES key. AES-CMAC is utilized to compute the Message Integrity Code (MIC). Furthermore, LoRaWan already addresses some security issues by implementing several security measures.

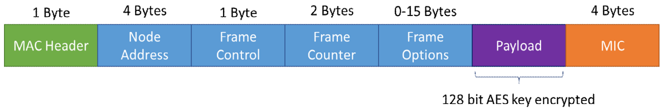

Figure 3. Frame counters.

C. *Attacks on the management system*

Our proposed system utilizes Fog computing so as to manage alerts and control the nodes from the edge. However, an attack on the Fog server could compromise the correct functioning of the system. Fog servers are susceptible of attacks of Denial of Service (DoS), Man in the Middle (MITM) or placing a rogue gateway [13].

The structure of Fog computing implies that DoS attacks would affect the closest networks but not the whole system if several Fog servers are utilized. Furthermore, the utilized protocols and their security mechanisms have to be considered and will become determinant in the success or failure of the attack. Man in the middle attacks could intercept data such as the alerts of the system, resulting in the system not taking the corresponding actions to resolve the problem if these messages are not forwarded. Tracking the messages and detecting abnormal behavior could help in detecting these types of attacks.

If this attack is utilized for eavesdropping, proper encryption techniques should be utilized. Furthermore, the system should be designed so as to avoid the introduction of rogue gateways that could disrupt the correct functioning of the system.

Moreover, all devices must be configured with passwords and access codes that will only be known by the authorized management personal. As usual, the personal entrusted with the management and administration of the system will employ different passwords to access the devices and their personal accounts. Furthermore, different access levels to management privileges will be established according to the activities related to each job position.

If our devices are not provided with a strong authentication system, some of the previously addressed problems may arise. These attacks may be denegation of service, modification and/or data thief, brute force attacks, etc. Device monitoring, freezing accounts and throttling are some of the common measures that we will employ so as to avoid the fraudulent access to the devices. Actualizing firmware and the operating systems of all the utilized devices is critical. All devices and equipment must update throughout their lifespan. Furthermore, the number of equipment with external access to the Internet browser must be reduced.

D. *Attacks on the data*

The data gathered from the system could be compromised by a third party. Unauthorized people could acquire the data or modify it so as to disrupt the correct performance of the system. The aspects that concern data security are integrity, confidentiality and availability [14].

In the case of our proposed system, the integrity and availability of the data is preferred to its confidentiality. However, enough encryption techniques should be utilized so as to provide the system with enough confidentiality. Furthermore, the information stored on Fog servers and the

TABLE I. PROPOSALS TO REJECTS ATTACKS

Attacks	How our proposal refuses the attack
Access to physical device.	Hardening devices and facilities. Access control in the facilities. Alarms. Periodic inspections of the sensor nodes.
Compromised physical Device.	User/password access. Visual identity verification (authentication phase).
Compromised node.	Use of algorithms to detect compromised nodes. Change of trust level. trust elimination.
Malfunctioning or lost the nodes or equipment.	Replacement of the damaged devices.
Power failure.	Equipment protection against failure to supply power. Persistent storage.
Lost data because of failures or battery discharge.	Persistent storage. Authentication.
Access to user date in physical device.	User/password access. Privileges management.
Infestation with Malware.	Reducing the usage of USB memory drives or other external memory devices Control ports.
Loose of connectivity.	Persistent data storage. Authentication.
Identity impersonation.	Visual identity verification (authentication phase). Control ports. Use of short-range technologies. Firewall. Trust policies.
Phishing, active spoofing, compromised data	Hashing and authentication. Use of a trusted chain. VPN IPSec. Firewall.
Network data access using passive spoofing.	Control ports. Ciphered using session key. Key management. Firewall.
Access to network key using passive spoofing. (man-in-the-middle)	Asymmetric encryption. Key-regeneration using trusted chains. Firewall.
Access to private user delivered data using passive spoofing	Asymmetric or symmetric encryption guaranteeing confidentiality. VPN IPSec.
Data modification. Compromised data	Hash function to guarantee data integrity. VPN IPSec.
Overload and/or loose of resources.	Capacity plan and forecast. Control the number of asymmetric operations. Firewall. Persistent data storage.
Erroneous packets delivery	Control sent and received packets. Packet retransmission.
Data storage overload	Distributed data management and storage.
Denial-of-Service / Data availability	Distributed data management and storage. Distributed access to data services. Distributed security processes. Firewall.
Access to not reliable data. Data disclosure.	Data access only through trusted nodes. Session key regeneration.

cloud should be properly protected. Secure passwords to access the data, authentication, encrypted data forwarding, and guaranteeing that user accounts cannot be duplicated are some of the measures to be considered.

At the data center, our data is previously protected by a firewall that prevents the connection of unauthorized users from the shared network (ISP). Moreover, the access permissions and updates of operating systems and firewall software of the different equipment must be adequate. These tasks must be performed on all implemented proprietary network resources as well.

The data of our system must be isolated from the data from any other network at all time. This way, a direct transfer can be avoided. Table 1 summarizes the proposals to reject the attacks.

Fig. 4 shows the summary of the phases of our security system. At the start, the proposals defined in Table 1 should be applied to the different equipment and devices.

V. CONCLUSION AND FUTURE WORK

We have performed a study on the different key points that may affect the security of our intelligent wastewater purification system for irrigation. We define four possible attack categories as being physical attacks, attacks on the communications, attacks on the management system, and attacks on the data. Furthermore, we specify the security measures that we will apply for each category for our system to be considered as secure.

As future work, we will implement the proposed policies in a real environment, we will perform penetration tests so as to verify its viability and we will correct any problem that we may detect. Furthermore, we will consider the implementation of an Ad-hoc network for our system utilizing secure protocols as the one in [15].

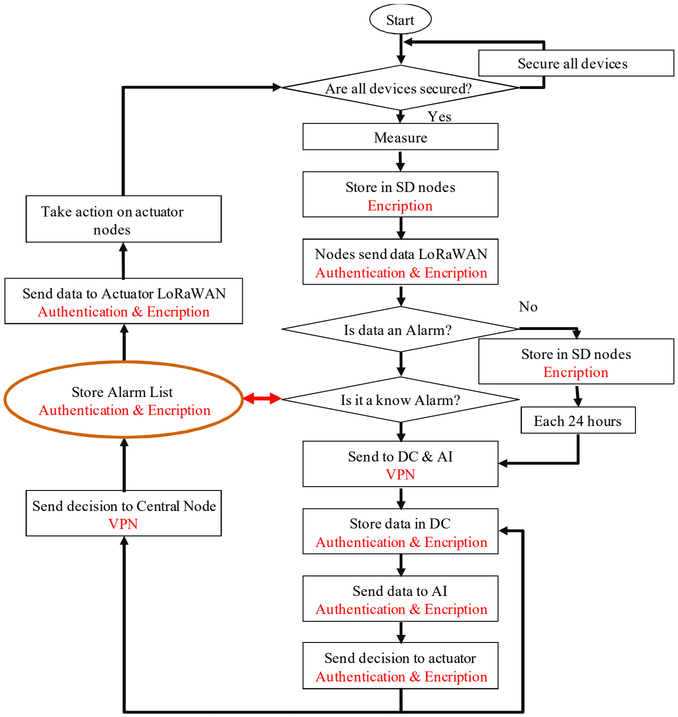
Start
Secure all devices
Are all devices secured?
Yes
Measure
Store in SD nodes
Encription
Take action on actuator nodes
Nodes send data LoRaWAN
Authentication & Encription
Send data to Actuator LoRaWAN
Authentication & Encription
No
Is data an Alarm?
Store in SD nodes
Encription
Store Alarm List
Authentication & Encription
Is it a know Alarm?
Each 24 hours
Send to DC & AI
VPN
Send decision to Central Node
VPN
Store data in DC
Authentication & Encription
Send data to AI
Authentication & Encription
Send decision to actuator
Authentication & Encription

Figure 4. Phases security system.

ACKNOWLEDGMENT

This work has been partially supported by the "Ministerio de Economía y Competitividad" in the "Programa Estatal de Fomento de la Investigación Científica y Técnica de Excelencia, Subprograma Estatal de Generación de Conocimiento" within the project under Grant TIN2017-84802-C2-1-P. This work has also been partially supported by European Union through the ERANETMED (Euromediterranean Cooperation through ERANET joint activities and beyond) project ERANETMED3-227 SMARTWATIR.

REFERENCES

[1] L. Garcia, J. M. Jimenez, M. Taha, and J. Lloret, "Wireless Technologies for IoT in Smart Cities.", Network Protocols and Algorithms, Vol. 10, No. 1, pp. 23-64, 2018.

[2] Cisco Cybersecurity Reports. Available at: https://www.cisco.com/c/en/us/products/security/security-reports.html (Last accessed on 26-11-2018).

[3] S. Laxmi and B. Hemavati, “Design and Implementation of IOT based Smart Security and Monitoring for Connected Smart Farming”, International Journal of Computer Applications, Vol. 179, No. 11, pp. 0975 – 8887, January 2018. DOI: 0.5120/ijca2018914779

[4] T. Baranwal, and K. P. Pushpendr, "Development of IoT based smart security and monitoring devices for agriculture." 2016 6th International Conference in Cloud System and Big Data Engineering, Noida, India, 14-15 January 2016, pp. 597-602.

[5] T. Xu, J. B. Wendt, and M. Potkonjak. "Security of IoT systems: Design challenges and opportunities.", In Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design, San Jose, California, USA, 3-6 November 2014, pp. 417-423.

[6] T. Robles, R. Alcarria, D. M. de Andrés, M. Navarro, R. Calero, S. Iglesias, and M. López. "An IoT based reference architecture for smart water management processes."JoWUA, Vol. 6, No. 1, pp. 4-23, 2015.

[7] D. Dragomir, L. Gheorghe, S. Costea, and A. Radovici. "A Survey on Secure Communication Protocols for IoT Systems.", 2016 International Workshop on Secure Internet of Things (SIoT), Heraklion, Greece, 26-30 September 2016, pp. 47-62.

[8] E. Aras, G. S. Ramachandran, P. Lawrence and D. Hughes. "Exploring the security vulnerabilities of lora.", 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), Exeter, UK, 21-23 June 2017, pp. 1-6.

[9] C. Gkountis, M. Taha, J. Lloret, and G. Kambourakis. "Lightweight algorithm for protecting SDN controller against DDoS attacks." 2017 10th IFIP Wireless and Mobile Networking Conference (WMNC), Valencia, Spain, 25-27 September 2017, pp. 1-6.

[10] J. Ni, K. Zhang, X. Lin, and X. S. Shen. "Securing fog computing for internet of things applications: Challenges and solutions."IEEE Communications Surveys & Tutorials, Vol. 20, No. 1, pp. 601-628, 2017.

[11] Cloud Security Principle 1: Data in transit protection. Available at: https://www.ncsc.gov.uk/guidance/cloud-security-principle-1-data-transit-protection (Last accessed on 26-11-2018).

[12] Gemalto, Actility and Semtech, “LoRaWAN Security: Full end-to-end encryption for IoT application providers”, 2017.

[13] R. Roman, J. Lopez and M. Mambo, “Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges”, Future Generation Computer Systems, Vol. 78, pp. 680-698, 2018.

[14] M. U. Farooq, M. Waseem, A. Khairi and S. Mazhar, “A Critical Analysis on the Security Concerns of Internet of Things (IoT)”, International Journal of Computer Applications, Vol. 111, No. 7, pp. 1-6, 2015.

[15] R. Lacuesta, J. Lloret, M. García and L. Peñalver, “A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation”, IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 4, pp. 629-641, 2013.