General Letters in Mathematics (GLM)

Journal Homepage: <http://www.refaad.com/views/GLM/home.aspx>

Definition of a lightweight cryptographic solution to secure health data on IoT and cloud

Akram Chhaybi^{a,*}, Saiida Lazaar^{a,*}

^a *ERMIA TEAM. National School of Applied Sciences of Tangier, ABDELMALEK ESSAADI University, Morocco*

Abstract

The Internet of Things (IoT) and the Cloud Computing are among the main technologies influencing the quality and efficiency of our social and economic activities. Their importance is quite notable in several areas such as remote medical care and healthcare monitoring systems. These later face difficulties most of them are the expensive costs for the chronic diseases and the hospitals charges specially during the pandemic time. All these issues have led to the creation of new solutions for enhancing the quality of the healthcare systems. In this paper, we focus on the network architecture security including healthcare monitoring systems based on IoT and Cloud Computing. We present a recent review on the research field and we propose a secure solution based on lightweight cryptography in accordance with the limited resource environments within which health data are exchanged. The proposed solution is guaranteeing data confidentiality and ensuring integrity and authenticity.

Keywords: Authenticity, Cloud, Confidentiality, Healthcare, Integrity, Internet of Things, lightweight cryptography

1. General Introduction

In the last 30 years, the Internet of Things (IoT) has seen a rapid development in all areas. According to Dr. Ujjwal Rao [10], for every 100 hospitals, there are 14 medical errors each year; which means that 43 million patients are exposed to health risks. In a recent study related to Melbourne [10], for 4 months almost 61.5% of patients have at least one medication error. In addition to these issues, one can notice that there exist other constraints related to medical resources demonstrating a serious fact on the quality care of the patients because the lack of professional environments providing nurses and doctors, and the high costs of medical and medication especially for chronic diseases. These issues lead to innovative solutions such as healthcare monitoring systems based on IoT and Cloud Computing where the patient can wear devices that collect the body's data such as temperature, heartbeat, etc. The collected data are sent to the supervisors (doctors) for analysis. We note that these personal data could face some risks from their exposition to passive or active attacks. Thus, there is a huge need to secure these sensitive data from the source to the destination and vice versa. The objective of our work is to contribute with cryptography for securing the medical data exchanged over constrained environments. We target the design of a global solution that guarantees confidentiality and authentication. The rest of this paper is structured as follows. In section 2, we provide a deep review of the main works in the literature. In section 3, we describe our

*Corresponding author

Email addresses: akramchhaybi1@gmail.com (Akram Chhaybi), slazaar@uae.ac.ma (Saiida Lazaar)

doi:[10.31559/glm2021.10.2.6](https://doi.org/10.31559/glm2021.10.2.6)

Received 30 Apr 2021 : Revised : 25 May 2021 Accepted: 25 Jun 2021

proposed solution based on lightweight cryptography. We close the article with a conclusion and some recommendations for a future work.

2. Review of relevant literature

The healthcare surveillance systems are mechanisms geared to taking care of human health where medical data are exchanged on networks encompassing Internet of Things (IoT) and cloud computing technologies. The interest in this field has attracted the attention of a large number of researchers, especially with the spread of the Covid-19 pandemic, which has led to the overcrowding of hospitals. Remote medication for chronic disease is needed in heightened pandemic circumstances. In our contribution, we present a review of some recent and relevant works published between 2012 and 2020 and dealing with healthcare monitoring systems.

In 2020 [1], the authors presented a model of health monitoring based on such sensors as ZigBee, RFID Tags, mobile phone sensing, WSN measurement nodes attached to WSN gateway, database and web server for storage. The model is divided on four main parts where the first part is the collection of data; it contains three sensors used to collect the human body information such as the temperature, the heart rate and the oxygen saturation. The second part corresponds to the transmission of data to the cloud. The third part corresponds to the reception of the data; and the last part is the monitoring of the data. Four layers were used: Wireless sensor layer, network layer, Internet layer, service layer where the sensor sends the information to the network layer, and cloud-computing layer. The proposed solution fails to discuss and to guarantee the security aspect of the transmitted data.

In 2019 [2], an extended architecture based on three layers, including patient, cloud and doctor was presented. The first layer is a biomedical sensor that collects the data of the patient like the oxygen or temperature, it encrypts and send the data to the cloud using the Wi-Fi with IoT system with three basic sensors. To avoid man in middle attacks, data stored on the cloud layer are encrypted with AES 128-bits. The last layer is the doctor/specialist layer where the doctor can log into the cloud to read the patient's information, and to check if there are any unusual activity and emergency case. Authors show the benefits of the system like Wi-Fi based connection that gives fast connection and low power between the patient module and the doctor module. Unfortunately, this system is vulnerable to Wi-Fi attacks.

In 2017 [3], Chen et al. presented a scheme for healthcare management. The patient can upload or download the data on health information after being authenticated. A key generation center (KGC) and public and secret keys are used. The system uses an IoT medical sensor that collect the patient's biological data and a mobile device connected with IoT sensor. A GPS localization of the patient is used for emergency. The KGC generates the keys by using a unique ID for every user during the registration phase in the KGC, plus the contact information and an International Mobile Equipment Identity (IMEI). The KGC sends the keys to the users and it generates the certification for the authentication part as it is shown on figure 1.

Figure 1: Intelligent and health monitoring system architecture [3].

The data sent to the hospital from the patient transit from a cloud's database using a digital signature, a decryption mechanism is started. The IoT sensor gets the biological data and send it to the mobile phone using the cloud public's key to encrypt the data and to send them to the cloud with a certification.

A smart health solution monitoring was proposed in 2017 [4] regarding an IoT and a cloud computing architecture using a machine learning classifier to detect the pathology. The system framework captures the signal through the IoT sensor and send it to the gateway device which is a smart phone, then the cloud receives the uploaded data to be analyzed by the doctor. The authentication of the communicating entities is verified on the cloud server. The machine learning algorithm classifies the signals as normal or pathological using the learning machine classifier. Nevertheless, the learning machine needs a time to learn in addition to the requirement of an expensive server.

Preda et al [7] proposed in 2017 a healthcare IoT-Cloud architecture with a sensing service targeting the enhancement of the sensor accessibility as described on figure 2.

Figure 2: A Cloud-IoT Based Sensing Service for Health Monitoring [7].

The work deals with the IoT and the cloud considering that the IoT's devices are very limited and the cloud is virtually unlimited in the storage. A proposition for facing these issues is that the cloud will benefit from the flexibility of the data dynamic storage, reinforced by a secure accessibility of the patient's data. The architectural solution is based on three layers: Data collection, Data management and

Application service. Moreover, the smart hospital network is based on six layers: Data Processing, Data Integration, Cloud Computing, Network Structure, Knowledge Reasoning Layer, and Visualization Layer.

Soyata et al. [6] presented in 2015 an emulsion of health monitoring systems through various phases: Data Acquisition, Data Transmission, and Cloud Processing. The work recommended machine-learning techniques as illustrated on figure 3.

Figure 3: Components of a remote patient monitoring system based on IoT-Cloud architectures [6].

Some problems are discussed like the battery that cannot be rechargeable or replaceable and the low energy that can be a challenge in the data quality. Authors recommended pattern recognition and machine learning techniques in the wearable sensors. However, the used machine learning methods needed a time to deal with this type of industry.

In [5] (2013) authors presented a platform for a secure monitoring and sharing generic data in the cloud through smartphones, Bluetooth, sensors and cloud technologies as shown on figure 4.

Figure 4: Platform for a secure monitoring and sharing of generic health data on the Cloud [5].

Some privacy problems were solved by using a proxy server that re-encrypt the data before to be transferred to the last user.

In 2012 [8], Zhang et al published a tele-medicine secure platform based on Internet of Things and on the cloud; they discussed the most communication protocol used to overcome the authentication and the security issues as demonstrated on figure 5.

Figure 5: A Platform Based on IoT and Cloud Computing for Ambient Aiding Living and Telemedicine [9].

The model secures the communication using a coupling between SSL protocol (Secure Sockets Layer) and Remote Method Invoking (RMI). The quality of service (QoS) is improved in a dynamic environment on the cloud supporting the health monitoring systems. Some problems were detected and were related to IoT interoperability, system security, and streaming QoS.

3. A proposed lightweight and secure solution for health monitoring

According the review above, we propose a secure solution for healthcare monitoring systems encompassing IoT and cloud. The proposed solution targets the security of the transmitted health data; it also aims to reduce the energy consumption in a resource-limited environment as illustrated on figure 6. It is mainly based on a lightweight cryptography guaranteeing authenticity, data integrity and confidentiality.

Figure 6: The proposed lightweight cryptographic solution.

To ensure data integrity and authentication, we propose the use of some lightweight hash functions standardized by the NIST. The solution is applied according to three layers: Collection layer, Transmission

layer and Receiving layer: The sensor collects the data from elder's body, then send them to the smart-phone using a local area network or a Bluetooth technology. The used sensor is depending on the health situation of the patient's such as an Electrocardiogram (ECG) for hearth muscle or an electrocardiography for muscles activity (EMG). The encryption system will be installed on the smartphone to save the energy in the sensors as much as possible. To authenticate the patient, we propose to use a hash function where the mechanism is described on figure 7. On figure 7, 'D' represents the input data, 'F' the lightweight hash function, 'E' the encryption algorithm and 'D' the decryption algorithm.

Figure 7: Integrity and encryption solution.

The application will be installed on the patient's smartphone where the data are encrypted by a lightweight encryption algorithm and the hash value is generated with a lightweight hash function. The whole data (encrypted and hash) are sent through the transport canal. From the other side, the server will decrypt the data, calculate a new hash value and then perform a comparison between the two hash functions to ensure integrity and authentication.

4. Conclusion

In this paper, we presented a recent review on some selected healthcare monitoring systems on IoT and cloud environments. We raised some issues related to the security of these systems. To overcome these issues, we proposed the use of the lightweight cryptography, especially a lightweight hash function standardized by the NIST in order to ensure integrity and authentication. In the same context, we recommended the use of the symmetric algorithm AES-128 for the protection of the sensitive data. The algorithm AES-128 is fast and secure, and it is considered by the NIST as a lightweight cryptographic algorithm suitable for data protection on constrained environments.

References

- [1] Su Myat Thaung, Hla Myo Tun, Khin Kyu Kyu Win, Myint Myint Than. Exploratory Data Analysis Based on Remote Health Care Monitoring System by Using IoT Communications. Vol. 8, No.1, 2020, pp. 1-8. doi: 10.11648/j.com.20200801.11 1- <https://doi.org/10.11648/j.com.20200801.11>
- [2] Ali I. Siam, Atef Abou Elazm, Nirmeen A. El-Bahnasaw hada El Banby, Fathi E. Abd El-Samie. Smart Health Monitoring System based on IoT and Cloud Computing. 1st International Conference on Electronic Engineering, Menoufia University, Egypt ICEEM2019, 7-8 Dec. 2019
- [3] Jin-Xin Hu, Chin-Ling Chen, Chun-Long Fan and Kun-hao-Wang. An Intelligent and Secure Health Monitoring Scheme Using IoT Sensor Based on Cloud Computing. Journal of Sensors, Volume 2017 <https://doi.org/10.1155/2017/3734764>

- [4] Ghulam Muhammed, SK Md Mizanur Rahman, Abdulhameed Alelaiwi and Atif Alamri. Smart Health Solution Integration IoT and Cloud: A Case Study of Voice Pathology Monitoring. IEEE Communications Magazine, January 2017. <https://doi.org/10.1109/mcom.2017.1600425cm>
- [5] Danan Thilakanathan, Shiping Chen, Surya Nepal, Rafael Calvo, Leila Alem. A platform for secure monitoring and sharing of generic health data in the Cloud. Elsevier B.V, 2013.
- [6] Moeen Hassanali, Alex Page, Tolga Soyata, Gaurav Sharma, Mehmet Aktas, Gonzalo Mateos, Burak Kantarci, Silvana Andreescu. Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-based Processing: Opportunities and Challenges. IEEE International Conference on Services Computing, 2015. <https://doi.org/10.1109/scc.2015.47>
- [7] Gabriel Neagu, Stefan Preda, Alexandru Stanciu, Vladimir Florian. A Cloud-IoT Based Sensing Service for Health Monitoring. The 6th IEEE International Conference on E-Health and Bioengineering - EHB 2017.
- [8] Salvatore Distefano, Dario Bruneo, Francesco Longo, Giovanni Merlino, Antonio Puliafito. Hospitalized Patient Monitoring and Early Treatment Using IoT and Cloud. Springer Science Business Media New York 2016
- [9] Xiao Ming Zhang, Ning Zhang. An Open Secure and Flexible Platform Based on Internet of Things and Cloud Computing for Ambient Aiding Living and Telemedicine. IEEE, International Conference on Computer and Management, 2011. <https://doi.org/10.1109/caman.2011.5778905>
- [10] Rossana Rivas Luis Vilcahuamán. Healthcare Technology Management Systems. Academic Press Elsevier - ISBN: 9780128114315