First and last Name student: *Doudou DIONE*

# Thesis Project

## Subject: Study of IoT security for e-health in developing countries

## I. CONTEXT AND PROBLEMATIC

### I.1.CONTEXT

The Internet of Things (IoT) paradigm has attracted the attention of large-scale service providers, businesses, and industries, such as healthcare, autonomous vehicles, smart grids, digital agriculture, and many others [1]. IoT enables objects to hear, listen, talk and act intelligently. These objects or devices are equipped with sensors, software, actuators, etc. that allow them to collect and exchange data with each other and can also be placed in different environments. The term IoT (internet of things) first appeared in 1999 in a speech by Kevin ASHTON, a British engineer. It was used to designate a system where physical objects are connected to the Internet [2].

The strong expansion of the Internet of Things in several sectors has not spared the health sector. Indeed, the hospital environment is one of the richest in communicating objects. As a result, the gains in efficiency and precision that these intelligent technologies bring to the sector could well save lives. In particular, these technologies allow for better monitoring of patients, whether they are hospitalized or on an outpatient basis. Remote medical monitoring allows healthcare professionals to monitor patients' vital signs and assess their physiological response to treatment without physically seeing them.

### I.2. PROBLEMATIC

With this large number of IoT applications comes the issue of security and privacy. Without a reliable and interoperable IoT ecosystem, emerging IoT applications cannot achieve high demand and risk losing their full potential. In addition to the security issues typically faced by the Internet, cellular networks, and WSNs, IoT also has its unique security challenges such as privacy issues, authentication issues, management issues, information storage, etc. [3]. Device security is about protecting IoT devices from attacks, while data security is related to protecting the integrity and confidentiality of data generated by IoT sensors and other monitoring instruments. This also applies to user privacy. The first step towards securing IoT devices is risk identification and categorization, in which the impact of different IoT devices is considered. Next, the feasibility principle analyzes implementation complexity, cost, and verifiable details, which address the verifiability of the implementation [4].

Medical IoT systems have become the core of the e-healthcare field, where smart sensors and medical devices are installed to improve the life span and health status of patients. However, this field has suffered various attacks targeting medical systems. In [5], security and privacy issues of IoT were discussed but not actually related to IoMT. Various intrusion detection methods [6] and authentication/authorization [7] were presented to ensure a secure IoT environment with little notice for their application to IoT. But recently additional work has been dedicated to healthcare system security. A generic survey on medical big data analytics has been conducted. Issues and challenges in IoT adoption are discussed to rank them.

On-demand IoT adoption in hospitals was conducted to improve the experience of nurses based on the pros and cons in healthcare technologies.

## II. OBJECTIVE

The objectives of this thesis work:

- A comprehensive bibliographic study on the current state of IoT security in the medical field and medical data then show the problem of their securing.
- Study of new security approaches, their integration in the IoT (limited resource) and the securing of medical data using intelligent and light cryptographic techniques
- Study the effects of blockchain for the security of IoMT and medical data.
- Develop customized blockchain systems of record with enhanced privacy features and limited accessibility.

**Keys word**: IoT, e-health, blockchain, IA, ML, DL

## III. REFERENCES

[1] HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2019). A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things, 100129.
[2] https://www.digora.com/fr/blog/definition-iot-et-strategie-iot
[3] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access, 7, 82721-82743.
[4] Salam, Abdul. Internet of Things for Sustainable Community Development. Springer International Publishing, 2020.
[5] Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. International Journal of Computer Applications, 90(11).
[6] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37.
[7] Trnka, M., Cerny, T., & Stickney, N. (2018). Survey of Authentication and Authorization for the Internet of Things. Security and Communication Networks, 2018.