Using Fog Computing to manage data confidentiality in the Internet of Things: the case of an electronic bracelet to relieve prison overcrowding in Senegal

Dr. GAYE Abdourahime
Department of Computer Engineering and Communication
University Alioune DIOP
Bambey, Senegal
abdourahime.gaye@uadb.edu.sn

Ms. SENE Dieynaba
Department of Computer Engineering and Comminication
University Alioune DIOP
Bambey, Senegal
senedieynaba87@gmail.com

***Abstract*—This work deals with the problem of prison overcrowding in Senegal and the use of electronic bracelets to reduce this overcrowding. Electronic bracelets collect a variety of data such as location, movements, communication data and biometric data. However, data security is a major concern. The aim of the work is to protect this data by using Internet of Things (IoT) and Fog Computing technologies to limit the data collection perimeter, thereby reducing the transfer of massive amounts of data to remote data offices. The architecture implemented aims to collect only the necessary data from remand and correctional office controlled by departmental courts, to comply with data protection laws and to implement security policies to prevent external attacks. This approach aims to guarantee data confidentiality while enabling the use of electronic bracelets to improve the prison situation in Senegal.**

Keywords—Internet of Things, security, Jail overcrowding, electronic bracelets, Fog Computing, data protection

I. INTRODUCTION TO THE PENITENTIARY SITUATION IN SENEGAL

The prison situation in Senegal is considered to be in a poor state. Prisons are overcrowded and under-equipped, leading to inhumane detention conditions and health problems for inmates. According to the National Statistics and Demography Agency (ANSD) report on Senegal's Economic and Social Situation SES 2019 published in January 2022, we have 37 prisons. The prison population stood at 11,576 individuals in 2019, including 241 minors [1].

Prison overcrowding frequently leads to health and safety problems for both inmates and penitentiary staff. Cells are often overcrowded, leading to hygiene and safety problems. Inmates are often forced to sleep on the floor or share beds.

With this in mind, the Senegalese government has launched some initiatives to improve the prison situation, including the use of electronic bracelets to relieve overcrowding. Electronic bracelets will be introduced to reduce the number of committal orders and avoid lengthy detentions.

The aim of this study is to guarantee data protection for devices, in this case the electronic bracelet, by implementing privacy management using IoT and Fog Computing technologies to minimize data collection.

II. PRINCIPLE OF ELECTRONIC BRACELETS MONITORING

An electronic bracelet is a portable device that tracks and monitors a person's movements. It is often used as an alternative to imprisonment for people who have been given a suspended or conditional prison sentence.

The bracelet, usually attached to the ankle, is fitted by a prison warden at the prison registry office. Operation is simple: if the prisoner leaves his or her accommodation during the hours when he or she is obliged to be there, or leaves the surveillance perimeter without authorization, an alarm is triggered at the surveillance center. The prison warden, after carrying out a telephone check, immediately notifies the relevant judge. A probation officer tries to contact the prisoner to find out what's going on. Depending on the outcome, the judge decides what action to take [2,3,4].

Electronic bracelets can collect a variety of data, including:

- **position**: geolocation technologies, such as GPS or cell phone networks, can be used to track an individual's position in real time;
- **movement**: sensors are used to track the user's movements, such as steps, physical activities and sleep times;
- **communication data**: communication data, such as phone calls and text messages, can also be collected to monitor the user's social interactions;
- **biometric data**: biometric data such as body temperature, heart rate, physical activity levels and stress levels can be collected to monitor the user's health.

It is important to note that the use of this data must comply with data protection and privacy laws and regulations, and users must give their consent. A crucial aspect to consider is the risk of hacking into the data collected by electronic wristbands. Without adequate security measures, this data can be exposed, raising major concerns about the confidentiality of detention information.

This risk of security breach reinforces the importance of an IoT and Fog-based solution, which we offer, to ensure data protection and confidentiality of sensitive detention-related information.

978-1-6654-7824-3/21/$31.00 ©2021 IEEE

III. Fog Computing for data security in the Internet of Things (IoT)

Used in the world of the Internet of Things, Fog Computing is as close as possible to the physical world and connected objects. It enables data to be stored and analyzed at the edge of the network. Processing capabilities are then included in the routers to which the objects are connected. Its vocation is not to replace the cloud, but to complement it for specific applications. Normally, data is processed in a cloud or datacenter, which means a certain amount of latency due to the journey (virtual or physical) it has to make. Thanks to Fog Computing, some data can be processed as close as possible to the connected object, considerably reducing processing time. Only the most important information is transmitted, thus relieving network traffic [5,6,7,11,12,13,14,15].

To guarantee data confidentiality, several solutions are often proposed in Fog Computing for the Internet of Things to protect users' personal data:

- **data encryption**: protects sensitive information stored or transmitted by IoT devices by transforming it into a code unreadable by unauthorized persons. Encrypted data can only be decoded with a decryption key, which reinforces its confidentiality;
- **limiting data collection**: to minimize the risk of privacy breaches, it's important to limit the amount of data collected by IoT devices. Companies need to think carefully about the types of data they collect and how often, ensuring that data is collected ethically and legally;
- **data access control**: companies need to implement data access control protocols to ensure that only authorized people have access to sensitive data stored or transmitted by IoT devices. Access control protocols can include passwords, two-factor authentication codes and other security measures;
- **reduced data transfer**: Fog Computing enables data to be processed at the edge of the network, close to its source, reducing the need to transfer massive amounts of data to remote data centers. This reduces the risk of privacy breaches by minimizing opportunities for data to be intercepted or compromised during transfer;
- **real-time data processing**: Fog Computing enables data to be processed in real time, reducing the time during which data is exposed to privacy risks. Data is processed immediately at source, before being transmitted to remote data centers, reducing the risk of privacy breaches;
- **privacy protection**: Fog Computing can help protect users' privacy by providing local processing of sensitive data. Sensitive data can be processed locally, without the need for transmission to remote data centers. This reduces the risk of privacy breaches by minimizing the opportunities for data to be compromised.

IV. Proposal Architecture Management for IoT Data Privacy with Fog Computing

A. *Overview of the players management data monitoring system*

Data management in the context of prisoner monitoring involves several players, each with specific responsibilities and legal obligations. Here are some of the players involved in data management:

- **Penitentiary authorities**: are responsible for managing data relating to prisoners, including information on their sentence, behavior, security and movements. They are also responsible for managing data relating to prison security, including video images, audio recordings and biometric data;
- **Judicial authorities**: such as judges and prosecutors, have access to inmate data as part of their work. They can use this data to make decisions about parole, early release or other aspects of prisoners' sentences;
- **Law enforcement agencies**: may have access to inmate data as part of a criminal investigation. They can use this data to identify suspects, accomplices or witnesses to a crime.

B. *Our architecture's network model for data monitoring system in Senegal's prison*

Our proposed model architecture is composed of the following three entities:

- **Monitoring Center (MC):** the place where prison authorities monitor and control the system or processes remotely. It uses the data processed and stored by the Fog network to provide services to users. Managed by the penitentiary authorities, its main role is to monitor wristband holders and intervene in the event of non-compliance with court-ordered conditions for wearing the wristband. The conditions for wearing bracelets vary according to the judge's assessment of the offences committed by the future holder;
- **Fog**: courts where wristband holders are authenticated. Since wristband holders have to go to the surveillance center to be rolled up in the system and have their wristbands fitted. We find it necessary to do this in the court where the judgment was handed down, to save time and resources. This task is carried out by the penitentiary authorities in the courts, who are responsible for winding and fitting the bracelet, to relieve the penitentiary authorities at the center, who do this at the same time as the monitoring;
- **users**: who are assimilated to bracelet holders (device). The latter collects data (location, health, etc.) and sends it to more advanced processing nodes for processing.

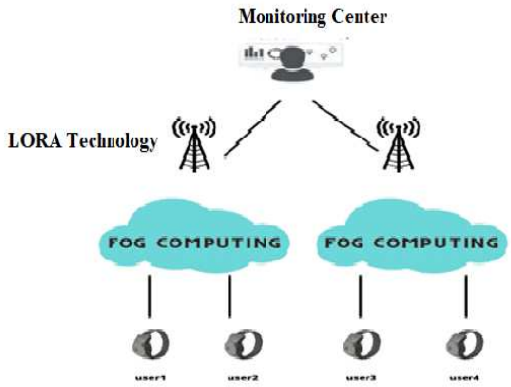

Fig.1. Our proposed model architecture

If the judge decides that a prisoner is to be placed under electronic monitoring, the prisoner is given a set time for going out, and a restricted area, i.e. the places where he or she is allowed to go. The court's prison authorities are responsible for winding the prisoner into the system and fitting the bracelet. Supervision is handled by the prison authorities at the center.

If the person is already in prison, the penitentiary authorities at the house correction are responsible for winding the bracelet into the system and fitting it.

In the event of non-compliance, for example if the inmate is late for work, a prison officer will call to find out why. If the delay becomes recurrent, the judge is informed so that the appropriate decisions can be taken. But the prisoner can also apply to the judge for permission to leave, if he or she needs to.

V. SENEGAL ASSOCIATED ELECTRONIC BRACELET MODEL

There are several aspects to bracelet design. First, we need to design the case, which must be ergonomic, lightweight and comfortable to wear. The size, shape and materials used must be carefully selected to meet users' needs.

A. Functional diagram

The devices and tools used to design the bracelet [8, 9, 10]:

- The NEO-6MV2 is a Global Positioning System (GPS module) used for navigation. The module simply verifies its location on earth and provides output data that is the longitude and latitude of its position. It is part of a family of stand-alone GPS receivers featuring the high-performance u-blox 6 positioning engine;
- The ESP32 is a popular microcontroller and system-on-a-chip (SoC) that is widely used in the development of IoT projects. Designed and manufactured by Expressif System, like Arduino it is a development board. This means it has all the functionality we'll need to create our project. We're choosing to use ESP32 communication to deploy a prototype of my project, but in the future we plan to use LoRa technology instead of WI-FI and Satellite to cover the MAC's radius;

LoRa technologies make IoT solutions accessible to emerging markets in asset monitoring, agriculture and the environment. These solutions provide long-range connectivity of over 15 km (Sigfox and LoRa communicate with 25mW of power over radii of 60km and 15km respectively, covering the perimeter of departmental courts). They use disconnected modes where power consumption is only necessary when the object has data to transmit. They feature high capacity, currently supporting up to 1 million nodes, battery life in excess of 10 years, and reduced synchronization overload without bounce on mesh networks. To ensure communication, LoRa technology is based on the LoRaWAN (Longue Range Wide Area Network) protocol. It ensures bidirectional communication [16, 17];

The use of function diagrams allows us to represent the internal operating process of our device and the evolution of data transmission.

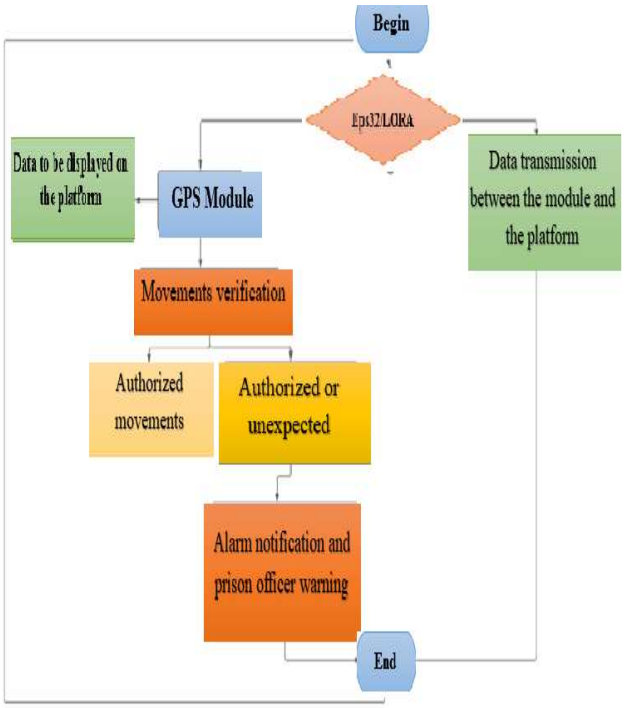

Fig.2. Functional diagram

B. System implementation

In our test platform, we present some of the interfaces linked to the system's actors, i.e. those of the Coordinator, Judge and Supervisor.

After launching the home page, we access the Coordinator area with its various functionalities.

In the Supervisor's area, we have the option of viewing the detainees assigned to the system.

If we click on locate, we can access the map representing the inmate's delimitation zone.

If the inmate does not comply with the rules, the supervisor can send notification messages to those in charge..

ACKNOWLEDGMENT AND CONCLUSION

Protecting data confidentiality in the IoT context is a central issue. Fog computing plays an essential role in managing the data generated by the IoT. Sensors that send

data over a wired or wireless transmission medium via the transmission unit must transmit the huge amount of data generated by objects without loss of information, and include strict measures to ensure that no external intervention occurs. The use of Fog Computing offers cost benefits by reducing bandwidth, minimizing energy costs, increasing data management efficiency and improving productivity, while enabling flexible scalability and growth in line with business needs.

The use of electronic bracelets can have an impact on the privacy of the people who wear them. People's movements are constantly monitored and recorded, which can raise issues of confidentiality and security. Authorities need to ensure that the information gathered is used appropriately and not disclosed to unauthorized third parties. Our architecture based on IoT and Fog Computing technologies proposed for the design of a prisoner monitoring system takes into account the issues linked to data confidentiality management with the delimitation of the information collection zone. Our proposed solution enables inmate enrolment to be carried out at departmental courts and Arrest and Correction Houses (MACs), unlike existing solutions where this operation is only possible at the Monitoring Center.

For the implementation of our solution, we opted to use ESP32 as the communication type in order to have a test prototype. The detailed presentation of our own implemented solution enabled us to highlight its mode of operation, its advantages and disadvantages compared with the existing system in our country, which uses centralised management unlike our proposal. It enabled us to identify the people likely to benefit from these schemes and the players involved, and to assess the system from the point of view of data confidentiality.

Our solution also enabled us to reduce the costs associated with preventive detention, particularly in terms of administration, the economy and health. It enabled us to highlight the growing importance of these technologies in modern society, as well as their potential for solving concrete problems while tackling the challenges that accompany them. The results of our work are not presented here, in view of the need to protect people's privacy.

In the future, however, we plan to use LoRa technology as a persistent option due to its specific advantages, such as its extended range and low energy consumption. This strategic decision is part of our drive to optimize connectivity for IoT devices, offering a robust, energy-efficient solution in line with the challenges facing the field.

To protect your privacy, some screenshots may not be displayed on the document.

REFERENCES

[1] ANSD, National Ecomic and social Situations Report (Microsoft Word - SES_2019.docx (ansd.sn)), (2019).

[2] Senegal : « The electronic bracelets could relieve prison overcrowding in Senegal? », BBC News Afrique, (2022)

[3] France : « Electronic bracelets: how do prisoners get round them? », The Point, (2020).

[4] United States: « California inmate escaped from jail, found six weeks later after cut off his GPS monitor », CNN, (2019).

[5] Adila MEBREK : Doctoral thesis from UTT, Fog Computing for IoT, (2020).

[6] Dr. Abdourahime GAYE and Dr. Dieynaba MALL: Analysis of authentication mechanisms and identity management in IoT: the resource constraints and security needs, (2021).

[7] Abdourahime GAYE and Ousmane NDIAYE: Analysis of mechanisms for resource management in IOT: performance of mutual authentication in the context of fog and edge-fog computing, (2023).

[8] Espressif Systems, ESP32 Technical Reference Manual, (2023).

[9] Frédéric Genevey and Jean-Pierre Dulex, Course to learn the basics of electronics and programming on Arduino, (2018).

[10] Gérard Rozsavolgyi and Aide of Sylvain Austruy, Accelerated course, (2023).

[11] UIT-T : Data Networks, Open Systems Communication and Security - Secure applications and services - Security of the Internet of Things (IoT). Switzerland, (2019).

[12] Insider: THE INTERNET OF THINGS. Here's what over 400 IoT decision-makers say about the future of enterprise connectivity and how IoT companies can use it to grow revenue, (2020)

[13] Leandro Loffi, Carla Merkle Westphall, Lukas Derner Grudtner, Carlos Becker Westphall: Mutual Authentication for IoT in the Context of Fog Computing. *11th International Conference on Communication Systems & Networks (COMSNETS)*, 367 – 374(2019).

[14] H. Rahimi, A. Zibaeenejad, and A. A. Safavi: A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies. IEEE 9th Annu. Inf. Technol. Electron. Mob. Commun. Conf., 81–88(2018).

[15] Fagen Li, Jiaojiao Hong, Anyembe Andrew Omala: Efficient certificateless access control for industrial Internet of Things. Future Generation Computer Systems 18(6):1089-1101(2016).

[16] Aly Benfattoum, From LORA technology to the LORAWAN network, In Frugal Technology, 2016.

[17] Djamel Eddine Kouicem, Security of Internet of Things for systems of systems, Compiègne Technology University, 2020.