International Journal of Scientific and Technical Research in Engineering (IJSTRE)
www.ijstre.com Volume 7 Issue 2 ǁ Mar-Apr 2022.
ISSN: 2581-9941

Authentication System Based on Fingerprint Scanners Network, QR Codes and IoT

José Ignacio Vega Luna[1], Gerardo Salgado Guzmán[1], Francisco Javier Sánchez Rangel[1], José Francisco Cosme Aceves[1], Mario Alberto Lagos Acosta[1], Víctor Noé Tapia Vargas[1]

[1](*Área de Sistemas Digitales, Departamento de Electrónica/Universidad Autónoma Metropolitana-Azcapotzalco, México)*
vlji@azc.uam.mx

Abstract : *Currently, access control systems have incorporated technological advances in wireless communications, biometric techniques, and the Internet of Things (IoT). This has made it possible to develop networks of biometric characteristics reading devices to share identification information and keep an updated database of people authorized to access buildings or restricted areas. This paper presents an authentication system with two security mechanisms integrated by a LoRaWAN of nodes based on a fingerprint scanner and a QR code. To access the building, the user must validate their fingerprint and provide the correct password when reading the QR code. Alternatively, the system administrator can remotely authorize access from an Internet platform. The LoRaWAN communication range was 7.5 kilometers, the false acceptance rate (FAR) was 0.033%, and the false reject rate (FRR) was 0.066%.*

Keywords - *Access control, biometric, IoT, LoRaWAN, wireless.*

I. INTRODUCTION

An access control system has the function of allowing or denying the entry of people or vehicles to buildings, institutions, companies and in general to any type of installation or restricted areas to guarantee the security of individuals or goods [1]. There are several types of access control systems which use different techniques, among which are biometric and proximity systems. Biometric systems perform the recognition of unique physical characteristics of people to verify their identity and allow access. Proximity systems are based on electronic cards or devices that, when placed near a scanner, identify and authenticate the person, for example RFiD cards or code labels, or tags [2].

For some years, biometric systems have been widely used, since they allow identification and authentication to be carried out quickly, securely and efficiently. Within these systems there are two techniques: physiological and behavioral. The first determine the biological or physiological characteristics of people, such as fingerprints, the iris and retina of the eyes, facial identification, the pattern of veins, the shape of the hands, DNA, blood and urine, among other. The second are based on the dynamic characteristics of human behavior, which sometimes depends on environmental conditions, mood or health of people. Some examples are voice recognition, signature, walking and gesticulation, among others [3].

Depending on the characteristics of the installation in which the access control system will be used, it will be the type of system to be implemented. In many installations a combination of more than one technique is used. Physiological techniques are the most used because they are based on characteristics of the human being that are permanent, unique during the life of the human being, measurable and can hardly be falsified or altered Through biometrics it is possible to identify and authenticate a person through of a group of unique and specific characteristics of it. Once the biometric characteristic is obtained, it is compared with the biometric information stored in a repository or database, of other individuals to perform authentication.

Currently, biometrics is used not only in access systems but also in other applications such as electronic passports and identity cards, among other things. Although biometric techniques are quite secure and accurate, more than one biometric source, called multimodal biometrics, is commonly used or combined with other security technologies such as the use of passwords, QR codes, and smart cards to minimize limitations of unimodal biometry [4].

From an operational point of view, access control systems can be of two types: independent or autonomous and networked. The first type uses reader units to identify and authenticate users without using any connection to other units of the same type or to a central station. They have the necessary resources to carry out

their task independently. Its functionality is simple and limited, providing a low level of security. The second type works under the control of a central station or independently, communicating in a network with other units to share information and keep the database of biometric characteristics up to date. They provide a high level of security and allow access to different areas or facilities to be controlled safely [5].

The purpose of this work was to design an access system with two security mechanisms, one biometric and the other using a QR code, for buildings or premises of a company or institution located geographically distant from each other. The user can request access to a building locally via fingerprint and a supplied key by reading a QR code or the administrator can authorize remotely from an IoT platform. The system is based on a LoRaWAN composed of three terminal nodes and a gateway. The terminal nodes and the gateway are located at the access door of each building and integrate a fingerprint scanner and a web server whose URL is invoked when the user reads the QR code associated with it. The nodes share the fingerprint database with each other so that it is updated and consistent in them. The gateway building has a connection to the Internet through a WiFi access point and the distance between this building and the furthest node is 2.5 kilometers.

An important aspect to consider when implementing Internet of Things (IoT-Internet Of Things) solutions is connectivity. In most environments, when there are different Internet connection options, power consumption and range are not a significant issue. However, when there are problems in the supply of electrical energy or in communications, technologies that resolve these limitations must be used.

One of the wireless communication technologies that has become popular in realizing IoT solutions is Low Power Wide Area Networks (LPWAN). This type of networks allows the transmission of information between sensors and actuators with a base station or gateway separated by great distances and using low power consumption. They are mainly used to implement IoT applications, since they can integrate thousands of nodes, powered by batteries, whose duration is several years, in a large area without using expensive infrastructure [6].

The LPWANs that use LoRa (Long Range) technology wireless modulation in the physical layer are called LoRaWAN. LoRa is a technology, similar to WiFi, Bluetooth and ZigBee, that allows communication links to be established over long distances using radiofrequency modulation called Chrip Spread Spectrum (CSS-Chirp Spread Spectrum) [7]. CSS modulation is similar to frequency shift keying (FSK), employing coding gains for higher receiver sensitivity, -168dB, and high interference tolerance. Its efficiency lies in low power consumption and long range at the expense of low data transfer rate. LoRa can achieve ranges of 20 kilometers and has been strongly promoted by LoRaWAN. LoRa represents the physical layer of the ISO OSI model, the type of modulation, frequency and bandwidth, while LoRaWAN is the medium access control standard, establishing the way in which communications are carried out, layers 2 and 3 of the OSI model. LoRa technology works in the radio spectrum that does not require a license in the Industrial, Scientific and Medical (ISM) bands, 868 MHz in Europe, 915 MHz in America and 433 MHz in Asia [8].

LoRaWAN networks use star topology, and the nodes establish the low-frequency wireless link with one or more gateways connected to the Internet. Gateways transmit information to the cloud using a standard IP connection [9]. To transmit over long distances using low power consumption, LoRaWAN uses low speeds, so the bandwidth is much lower compared to other wireless technologies. This is not a problem when using sensors, such as those used in the IoT, that transmit small amounts of information in time windows of seconds to minutes [10]. In this way, LoRaWAN is a protocol specification with an open source LPWAN infrastructure built using LoRa technology and developed and managed by the LoRa Alliance. They allow the creation of bidirectional communication IoT networks, with multiple secure point-to-point communication paths, for mobility and location services. The standards-based approach of LoRaWAN allows the creation of public or private IoT networks with coverage similar to cellular networks [11]. Some cellular phone operators offer LoRaWAN services as they use the cellular network infrastructure of poles and antennas. LoRaWAN applications include monitoring of smart meters and sensors, inventory control, vehicle tracking, smart cities, agriculture, health, and product vending machines, among others [12].

Reviewing the state of the art regarding the research carried out on the technologies used in this work, it can be seen that identification through biometric techniques continues to be a subject of continuous development that uses more sophisticated methods every day. In particular, fingerprints are a topic of interest both in electronic commerce, security applications [13] and in law enforcement [14]. However, since it is in the public domain and used, efforts have been focused on implementing more reliable and secure techniques for scanning fingerprints, such as estimation of the similarity of fingerprints with generative images based on textures and models based on pixels [15], use of optical coherence tomography (OCT) with high resolution images to obtain better images on defective surfaces [16], detection of life of fingerprints to avoid counterfeits [17] and the use of deep convolutional neural network (DCNN) [18], which require considerable computing power and a large amount of information for learning. Regarding LoRaWAN, being the most appropriate communication technology for IoT applications due to low energy consumption, long range and low cost, they enable the implementation of private networks based on an open standard. During the last years LoRaWAN have been used in a variety of applications, such as in smart cities for the monitoring of electric power and water networks [19], in waste and garbage management systems to avoid problems of health and environmental [20]

and in the communication of electric vehicles [21], among others. LoRaWAN use 128-bit Advanced Encryption Standard (AES-128) and two layers of security, one for the network and one for the application. The first is to authenticate the node and the second is application security to ensure that the LoRaWAN operator does not have access to the end user's application information. To improve security in this type of networks, recent research has aimed to develop secure session key generation methods [22]. Finally, recent research has been directed to the creation of algorithms to more reliably read these codes caused by distortions caused by the position of the cameras using vertex location techniques to remove perspective [23], as well as nested codes that include a greater amount of information and compressed confidential information [24, 25] than the original QR codes [26], based on Hamming code algorithms [27] and micrography QR codes generation [28].

II. MATERIALS AND METHODS

The access system is based on a LoRaWAN composed of four terminal nodes and a gateway. Each terminal node, or reading node, as shown in Fig. 1, is installed at the main door of the buildings. The gateway function is carried out by the scanning node of the building where the Wi-Fi Internet access point is located.

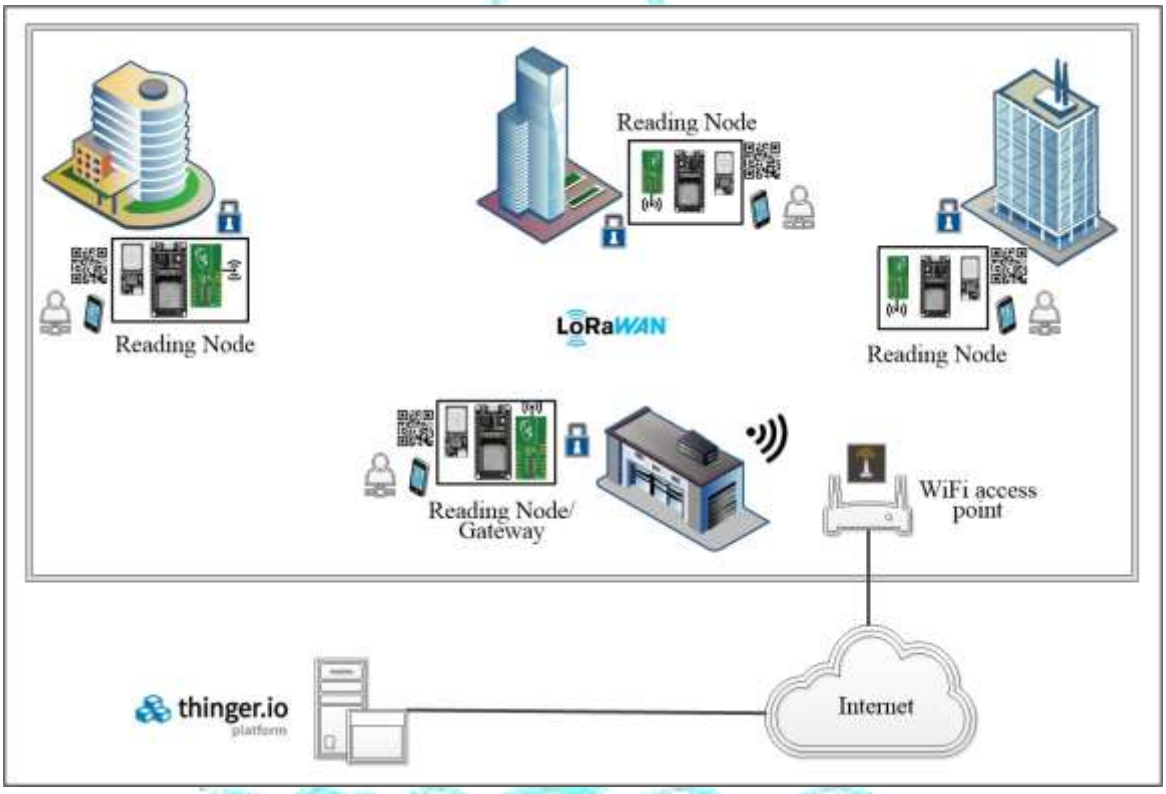

Figure 1. Functional system architecture.

The reading nodes are composed of four elements: the ESP32 MCU module, the fingerprint scanner, the wireless communication module, and the electrical interface, as indicated in Fig. 2.

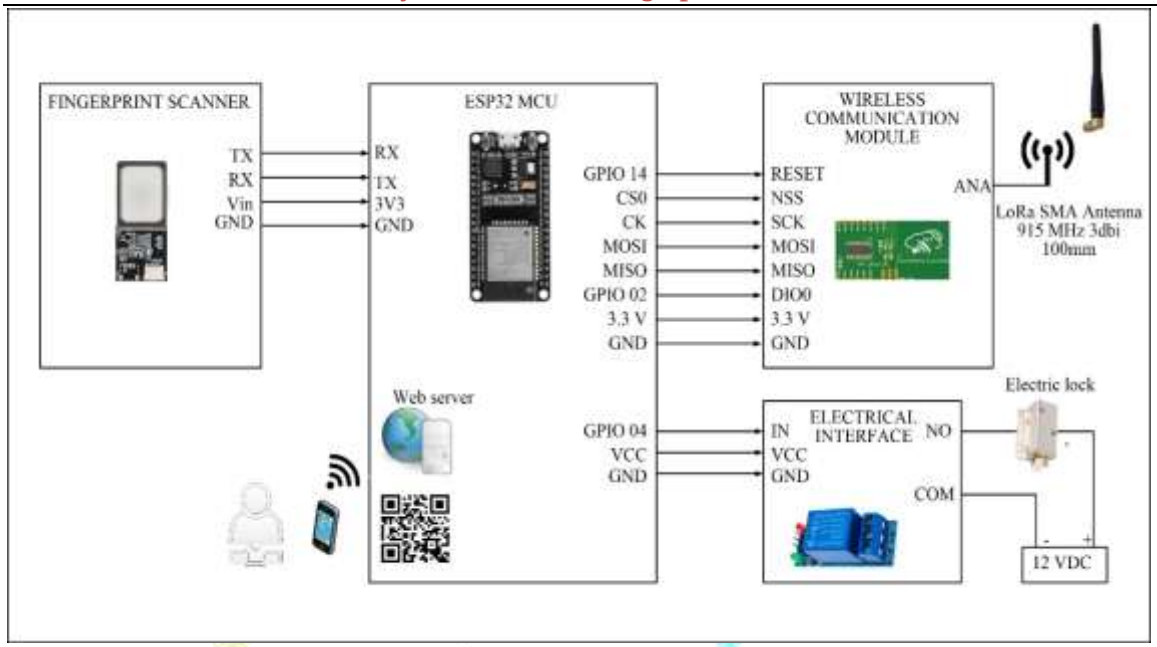

Figure 2. Block diagram of reading nodes.

2.1. The ESP32 MCU

This module integrates a low-cost, low-power ESP32 system on a chip (SoC), which incorporates the following features: a dual-core Tensilica XtensaLX6 microcontroller, 448 KB ROM, 520 KB RAM, WiFi 802.11b/g/n interface, Bluetooth Classic and LE interface with integrated antenna, 3 UART ports, 3 SPI ports, 2 I^2C ports, 25 general purpose inputs/outputs (GPIO) and a charger for lithium-ion battery. The computing power of this microcontroller allows the system to be programmed efficiently and quickly to process both the fingerprint scanning and the application that is invoked when the user reads the QR code. Through the gateway, the Internet and cloud platforms are accessed, allowing easily, quickly and reliably develop IoT applications.

2.2. The fingerprint scanner

The fingerprint scanner used was the GT-511C3 device. This scanner includes an optical sensor and an ARM Cortex M3 CPU to run the fingerprint identification algorithms. It has an area used for the fingerprint of 14x12.5mm, captures images of 202x258 pixels and has a resolution of 450 dpi. The size of the image is 496 bytes plus 2 bytes of checksum. The capture time is less than 3 seconds, the identification time is less than one second, and it can store up to 200 fingerprint images. It has a UART port for serial communication with a controller and a USB v1.1 interface. It provides a false acceptance rate (FAR) of less than 0.001% and a false rejection rate (FRR) of less than 0.001%. The fingerprint scanner was connected to a UART port of the ESP32 MCU module and communication was carried out at 9,600 bps.

2.3. The wireless communication module

The communication module used was the Omniduino Lora Leaf. This bidirectional wireless communication module integrates a RFM95W LoRa transceiver, a helical antenna, an SMA connector for an external antenna and works at a frequency of 868 or 915 MHz at a speed of 0.293 to 37.5 Kbps. The communication protocol with the ESP32 MCU it is through an SPI interface with level shifter. In this work, the Omniduino Lora Leaf was connected to one of the SPI ports of the ESP32 MCU module and to achieve the range required by the LoRaWAN, an external antenna of 915 MHz, 50 ohms, maximum power of 10 W, with gain of 3dbi, vertical polarization and a length of 100 mm.

2.4. The electrical interface

The electrical interface with the building door lock was implemented based on a 5 VDC and 15 A 120 VAC single channel relay module, which includes protection with an optocoupler and two control outputs, one normally open (NO) and the other normally closed (NC). The control input of this module was connected to the

GPIO 04 terminal of the ESP32 MCU module and the electric lock was connected to the NO output of the relay. Using the components listed above, the operation of the system is explained below.

To access one of the buildings, the user must validate her identity using the two security mechanisms, the fingerprint and the password requested by reading the QR code. So then, when the user places their fingerprint, the image is captured and compared by the scanner in the database. The validation result is indicated by the scanner to the ESP32 MCU. If the search was successful, the program running on the ESP32 MCU, sets a flag indicating the above. Next, if the flag is activated, the user must read the QR code, indicated on the door of the building, through an application on a mobile device. The application will request a service from one of two web servers running on the ESP32 MCU. In response, the web server will require, through a web page, that the user supplies the password. If the password is correct, the ESP32 MCU will activate the electric lock through the GPI0 04 terminal. If the password is not correct, after a maximum of three attempts, the identity validation process is aborted.

The second web server is listening for connection requests from the open-source internet platform thinger.io. Through this platform, the administrator can ask the ESP32 MCU to activate the lock or to send the command to the scanner to register a new fingerprint. Remote activation of the lock is used when for some reason the user cannot validate identity locally at a building door and the administrator needs to provide access. When a fingerprint is registered, the program transmits the image to the other reading nodes of the LoRaWAN to keep the database updated in the access system. In the ESP32 programming, the two web servers run in the background and are continuously listening on the corresponding port indicated in the program. During the execution of the main program, the ESP32 MCU module is in a cycle waiting for the fingerprint scanner to perform an identity validation requested by the user. To carry out the operation indicated above, the programming of the ESP32 module was implemented in MicroPython based on the flowchart indicated in Fig. 3. The tasks that the program executes are those that are explained below.

Initially, the GPIO terminals, the UART, WiFi and SPI interfaces of the ESP32 MCU module were configured, as well as the fingerprint scanner and the wireless communication module. Next, the connection of the ESP32 to the local WiFi network was made using the MicroPython network library. Subsequently, the web servers were started using the MicroPython sockets library. This library is an API that allows the use of sockets that provide a connection-oriented service between servers and clients, supporting different communication protocols, including HTTP, HTTPS and others. The implementation of the web servers consisted of the following steps: creation of the stream-type sockets, binding the sockets to the IP address and ports corresponding to the web servers and, in the background, the configuration and startup of the sockets was carried out in listen mode to wait and accept http connection requests from clients to exchange information and close the socket. While the web servers listen in the background, the main program enters the waiting loop for communication with the fingerprint canner. The web page displayed in the user application that performs the reading of the QR code was made in HTML.

III. RESULTS

Two sets of tests were performed. The first set aimed to evaluate the efficiency and accuracy of the access system. It consisted of determining the false acceptance ratio (FAR) and the false rejection rate (FRR) with authorized and unauthorized users. In biometric systems, the FAR allows to measure the average number of false acceptances, it happens when the system erroneously allows access to unauthorized users or impostors. Commonly, the FAR is determined by dividing the false acceptances by the total number of false attempts. The FRR is the average number of failed rejections from authorized or legitimate users. It is obtained by dividing the number of failed rejections by the number of legitimate attempts. To perform this group of tests, a database of 3,000 fingerprint images stored in the fingerprint scanner in one of the LoRaWAN nodes was used. To obtain the FAR, 2,950 fake or impostor users tried to access the node building, of which only one was authorized by the system. This resulted in a FAR=0.033%. To obtain the FRR, 3,000 legitimate users tried to access, of which the system rejected and did not authorize two. This resulted in an FRR=0.066%.

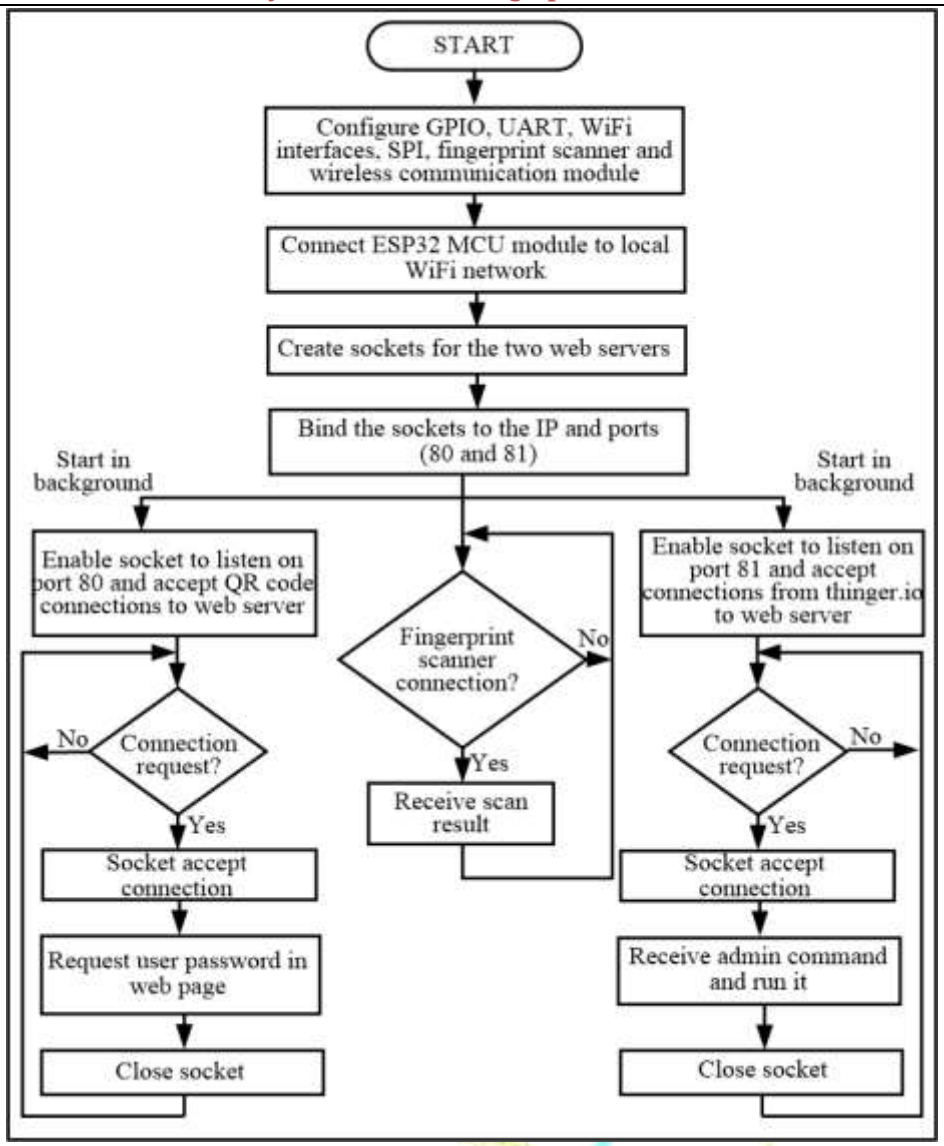

Figure 3. Reading nodes program flowchart.

The second set of tests was used to determine the range of the network. To do this, two line-of-sight nodes were located at different distances and communication between them was carried out. Communication was lost when the distance was 7.525 kilometers, and the Received Signal Strength Indicator (RSSI) magnitude was -83 dBm.

IV. CONCLUSION

Although the maximum distance between the buildings where the access system was implemented is 2.5 kilometers, it has the advantage of being based on a LoRaWAN, so it can be used in places where the distance between the nodes is 7.525 kilometers with line of sight. Another advantage of the system is that the databases of the fingerprint scanners are synchronized in real time. The FAR and FRR values obtained are acceptable and make the system be reliable. These values are slightly higher than those indicated by the supplier of the fingerprint scanner. The limitation of the system is that must be used in conjunction with other security mechanisms or systems, such as CCTV, presence sensors, and even with other biometric devices, so that the administrator can see in real time the user who is authorized remote access or if greater security is needed.

Finally, the fingerprint scanner can store up to 3,000 images, which can be considered limited in some environments, places or installations.

REFERENCES

[1] M. Uddin, S. Islam and A. Al-Nemrat, A Dynamic Access Control Model Using Authorising Workflow and Task-Role-Based Access Control, *IEEE Access, 7*, 2019, 166676-166689.

[2] J. Park, R. Sandhu, M. Gupta and S. Bhatt, Activity Control Design Principles: Next Generation Access Control for Smart and Collaborative Systems, *IEEE Access, 9*, 2021, 151004-151022.

[3] S. Bhatt, T. K. Pham, M. Gupta, J. Benson, J. Park and R. Sandhu, Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future, *IEEE Access, 9*, 2021, 107200-107223.

[4] F. Ghaffari, E. Bertin, N. Crespi, S. Behrad and J. Hatin, A Novel Access Control Method Via Smart Contracts for Internet-Based Service Provisioning, *IEEE Access, 9*, 2021, 81253-81273.

[5] G. Gan, E. Chen, Z. Zhou and Y. Zhu, Token-Based Access Control, *IEEE Access, 8*, 2020, 54189-54199.

[6] 1K. Adachi, K. Tsurumi, A. Kaburaki, O. Takyu, M. Ohta and T. Fujii, Packet-Level Index Modulation for LoRaWAN, *IEEE Access, 9*, 2021, 12601-12610.

[7] E. M. Torroglosa-Garcia, J. M. A. Calero, J. B. Bernabe and A. Skarmeta, Enabling Roaming Across Heterogeneous IoT Wireless Networks: LoRaWAN MEETS 5G, *IEEE Access, 8*, 2020, 103164-103180.

[8] K. Q. Abdelfadeel, D. Zorbas, V. Cionca and D. Pesch, Fine-Grained Scheduling for Reliable and Energy-Efficient Data Collection LoRaWAN, *IEEE Internet of Things Journal, 7(1)*, 2020, 669-68

[9] J. Finnegan, R. Farrell and S. Brown, Analysis and Enhancement of the LoRaWAN Adaptive Data Rate Scheme, *IEEE Internet of Things Journal, 7(8)*, 2020, 7171-7180.

[10] C. Garrido-Hidalgo et al., LoRaWAN Scheduling: From Concept to Implementation, *IEEE Internet of Things Journal, 8(16)*, 2020, 12919-12933.

[11] Y. Liu et al., Efficient Load Balancing for Heterogeneous Radio-Replication-Combined LoRaWAN, *IEEE Transactions on Industrial Informatics (Early Access)*, 2022, 1-1.

[12] E. Sisinni et al., LoRaWAN Range Extender for Industrial IoT, *IEEE Transactions on Industrial Informatics, 16(8)*, 2020, 5607-5616.

[13] W. Jiang, X. Wang, X. Song, Q. Liu and X. Liu, Tracking your browser with high-performance browser fingerprint recognition model, *China Communications. 7(3)*, 2020, 168-175.

[14] D. Valdes-Ramirez et al., A Review of Fingerprint Feature Representations and Their Applications for Latent Fingerprint Identification: Trends and Evaluation, *IEEE Access, 7*, 2019, 48484-48499.

[15] M. P. Yankov, M. A. Olsen, M. B. Stegmann, S. S. Christensen and S. Forchhammer, Fingerprint Entropy and Identification Capacity Estimation Based on Pixel-Level Generative Modelling, *IEEE Transactions on Information Forensics and Security, 15*, 2020, 56-65.

[16] F. Liu et al., A Flexible Touch-Based Fingerprint Acquisition Device and a Benchmark Database Using Optical Coherence Tomography, *IEEE Transactions on Instrumentation and Measurement, 69(9)*, 2020, 6518-6529.

[17] Y. Zhang, C. Gao, S. Pan, Z. Li, Y. Xu and H. Qiu, A Score-Level Fusion of Fingerprint Matching With Fingerprint Liveness Detection, *IEEE Access, 8*, 2020, 183391-183400.

[18] M. Ghafoor et al., Fingerprint Identification With Shallow Multifeature View Classifier, *IEEE Transactions on Cybernetics, 51(9)*, 2021, 4515-4527.

[19] Y. Lalle, M. Fourati, L. C. Fourati and J. P. Barraca, Routing Strategies for LoRaWAN Multi-Hop Networks: A Survey and an SDN-Based Solution for Smart Water Grid, *IEEE Access, 9*, 2021, 168624-168647.

[20] S. Wang, H. Jiang, X. Fang, Y. Ying, J. Li and B. Zhang, Radio Frequency Fingerprint Identification Based on Deep Complex Residual Network, *IEEE Access, 8*, 2020, 204417-204424.

[21] H. Klaina et al., Aggregator to Electric Vehicle LoRaWAN Based Communication Analysis Vehicle-to-Grid Systems Smart Citiest, *IEEE Access, 8*, 2020, 124688-124701.

[22] K. -L. Tsai, F. -Y. Leu, L. -L. Hung and C. -Y. Ko, Secure Session Key Generation Method for LoRaWAN Servers, *IEEE Access, 8*, 2020, 54631-54640.

[23] H. Eugênio Gonçalves, L. Xavier Medeiros and A. Coutinho Mateus, Algorithm for Locating the Vertices of a QR Code and Removing Perspective, IEEE LatAmerica Transactions, 19(11), 2021, 1933-1940.

[24] L. Xiong, X. Zhong, N. N. Xiong and R. W. Liu, QR-3S: A High Payload QR Code Secret Sharing System for Industrial Internet of Things 6G Networks, IEEE Transactions on Industrial Informatics, 17(10), pp2021, 7213-7222.

[25] A. Mohammed Ali and A. K. Farhan, Enhancement of QR Code Capacity by Encrypted Lossless Compression Technology for Verification of Secure E-Document, *IEEE Access, 8, 2020*, 27448-27458.

[26] G. -J. Chou and R. -Z. Wang, The Nested QR Code, *IEEE Signal Processing Letters, 27*, 2020, 1230-1234.

[27] P. Huang, C. Chang, Y. Li and Y. Liu, Efficient QR Code Secret Embedding Mechanism Based on Hamming Code, *IEEE Access, 8*, 2020, 86706-86714.

[28] S. -H. Hung et al., Micrography QR Codes, *IEEE Transactions on Visualization and Computer Graphics, 26(9),* 2020, 2834-2847.