Securing laboratories through internet of things networks: a comprehensive approach for ensuring safety and efficiency

Tamali Abderrahmane[1], Amardjia Nourredine[1], Tamali Mohammed[2]
[1]LIS Laboratory, Department of Electronics, Ferhat Abbas Setif1 University, Setif, Algeria
[2]ENERGARID Laboratory, Department of Electrical Engineering, Tahri Mohammed Bechar University, Bechar, Algeria

Article Info

Article history:

Received May 14, 2023
Revised Jul 13, 2023
Accepted Aug 2, 2023

Keywords:

Internet of things
Message queuing telemetry transport
Node-RED
Raspberry Pi
Security
Virtual private server

ABSTRACT

The design of a secure, intelligent laboratory that incorporates internet of things (IoT) devices and applications is a complex process. One of the main goals is to create a process monitoring system that can collect and analyze data from connected devices such as temperature and pressure sensors, smart locks, and access control systems. This system must operate in real time to ensure that equipment is within reference values. This reduces the risk of contamination and increases reliability. In addition, computer network security is paramount and it is imperative that certain measures such as encryption, multi-factor authentication, and intrusion detection systems are implemented. These measures help to ensure the safety and security of critical information and protect against potential risks. Physical security is also essential to protect scientific equipment and data. This paper provides a comprehensive overview of the critical factors involved in designing a secure, intelligent laboratory. It discusses the benefits of the integration of IoT devices and applications, and the security challenges that must be addressed. The paper also provides recommendations for designing and implementing a secure smart lab.

Corresponding Author:

Tamali Abderrahmane
Department of Electronics, Ferhat Abbas Setif1 University
Setif, Algeria
Email: abdou.t10@gmail.com

1. INTRODUCTION

The internet of things (IoT) has revolutionized the way we interact with the world around us [1]–[5]. With the increasing availability of IoT devices and applications, there is a growing need to explore their potential for enhancing security and efficiency in various domains, including laboratory research. In particular, the integration of IoT devices and applications can provide new insights into the performance of laboratory equipment and processes, enabling better monitoring and control to enhance security, reliability, and efficiency [6]–[11].

In recent years, security of places via IoT networks has received considerable attention. Several studies have focused on addressing the challenges and proposing solutions in this area. Thus, an overview of related work that has contributed to securing laboratories as an important spatial space via IoT networks.

Researches [12]–[16] discussed the challenges and proposed solutions for IoT security in various important environments like homes, industries, and laboratories. They emphasized the need for robust security measures to protect sensitive data and equipment inside the IoT network. Researches [17], [18] examined the security challenges specific to IoT-enabled industries with high-value equipment, such as laboratory automation systems. Their work highlighted the vulnerabilities and risks associated with such systems. They emphasized the importance of implementing robust security mechanisms.

A comprehensive review of IoT security challenges and solutions for environments similar to laboratories was conducted in [19]–[22]. Their study covered various aspects such as privacy, access control, and device authentication. Researches [18], [23], [24] proposed a secure access control model. Their model provided fine-grained access control mechanisms to ensure that only authorized personnel can interact with laboratory resources.

These recent works collectively emphasize the significance of addressing the security challenges in laboratories utilizing IoT networks. They provide insights into the vulnerabilities, risks, and potential solutions for securing laboratory environments. Building upon these studies, our research aims to develop a comprehensive security system that effectively safeguards laboratory resources and ensures the integrity of scientific processes.

In this paper, we aim to explore the potential of IoT devices and applications for securing laboratory machines and networks. Specifically, we will examine the key challenges involved in implementing an IoT-based security system, such as data acquisition and analysis, system integration, and cybersecurity. Additionally, we will discuss the potential benefits of such a system, including improved efficiency, reduced risk of contamination, and enhanced scientific research outcomes.

In addition to discussing the potential benefits of an IoT-based security system for laboratories, we could provide specific examples of IoT devices and applications that have been used in laboratory research. For instance, we could explore how IoT devices can be used to monitor environmental conditions, such as temperature, humidity, and light levels, to maintain stable and consistent conditions for scientific experiments [25]–[27]. Data analysis and visualization, one of the key challenges involved in implementing an IoT-based security system is analyzing and interpreting the large volumes of data generated by IoT devices [28]–[30]. we could explore how data analysis and visualization techniques, such as machine learning algorithms and dashboards, can help to extract insights from this data and make it more accessible and actionable. Integration with existing laboratory equipment and systems. Another challenge involved in implementing an IoT-based security system is integrating it with existing laboratory equipment and systems. We could discuss how this can be achieved through various means, such as retrofitting IoT sensors onto existing equipment or integrating IoT devices with laboratory information management systems (LIMS) [31]–[33]. Cybersecurity, ensuring the security of laboratory machines and networks is a critical consideration when implementing an IoT-based security system. we could explore various cybersecurity measures, such as firewalls, encryption, and intrusion detection systems, and how they can be integrated into an IoT-based security system to safeguard laboratory equipment and data [7]. Case studies, to illustrate the practical implementation of an IoT-based security system in a laboratory setting, we could provide case studies of laboratories that have successfully implemented such systems. These case studies could provide valuable insights into the benefits and challenges involved in implementing an IoT-based security system, as well as highlight the key factors that contribute to success.

2. METHOD

To improve the safety system of a research laboratory, it is necessary to check a large number of parameters. These parameters are summarized in:

- External interactions, E.I due to external guests or lab members.
- Internal interactions, I.I due to actual lab human presence.
- Type of administrative functioning of the laboratory, A.F.L dictated by a bunch of rules.
- The content of the scientific research carried out, T.R.S related to a number Nr of research projects.
- Launched R_i.
- Geolocation of sites, G.S definition of global positioning system (GPS) coordinates, and colocation index.
- Operators, O.P what is represented by all members and visitors.

These components directly or indirectly influence the quality of laboratories in terms of overall safety. The reliability of the laboratory as a result and the socio-economic impact are very much determined by the level of maintenance of laboratory security. In this regard, we envisage a composition based on the access control concept.

It is a fact that an optimization process will only be successful if it is global and has nothing to do with local vision. In this case study, we have to consider multi-criteria optimizations with trends such as:

- Fuzzy logic, with control based on the error made in the global control.
- Neural networks, with the adaptation of the parameters of the control through the training on samples of real cases.
- Genetic algorithms, consider each of the above parameters as a series of genes in a chromosome modeling the security process.

- Techniques based on statistics, following the consolidation of use cases collected from the history of the laboratory.
- Ontology-oriented optimization approaches, use a linguistic corpus to set priorities that can lead to an optimal result.
- Techniques of artificial intelligence (AI), grouping these strategies in a single composition, without forgetting the most recent advances in this field, such as the "AI code interpreter". These take charge of a problem through its statistical data and intelligently emit generated codes capable of dealing with the problem posed, following a textual description.

External interactions, referred to as E.I, are defined by access requests from operators and visitors seeking access to the lab. It is unlikely that the overall security of the lab would be compromised by such a misstep. These interactions are controllable because they are subject to K_{aut} authorizations and are still infrequent P_{freq}. Internal interactions, where I.I, are the cause of the behavior of the laboratory members, which by default have an OK authorization (K_{aut}=1) and are very frequent (P_{freq}>>0). The administrative mode of operation of the laboratory, A.F.L, represents the rules of procedure defined by the board of directors of the laboratory with regard to the access to and the management of the resources. Access to a laboratory resource (access to premises and use of equipment) is subject to a pre-established administrative agreement based on the laboratory rules. All persons having access to the laboratory are more or less granted this personalization. This is equivalent to a parameter K_{ar}=(1-K_{reg}), where K_{ar} is the authorization coefficient for access to resources and K_{reg} is defined by the regulatory security control policy (high K_{reg}, high-security level). The content of the scientific research carried out, as indicated by the T.R.S, in which case the laboratory must sign research and development (R&D) contracts with partners. These contracts are subject to substantial budgets and are therefore scrutinized by the partners, in particular the research funders. The K_{af} parameter is defined as (1-K_f), where K_f is the content of the project covered by a funding contract and is proportional to the value of the funding. The geolocation of sites, denoted G.S, denotes the type of grouping of sites belonging to the same laboratory. The complexity of the security systems to be implemented is likely to affect the implementation of any strategy based on IoT networks. As for the operators, where O.P, the thing in doubt in this context, remains in compliance with the protocols established by the laboratory.

Understanding access control theory (Figure 1) is essential in determining the appropriate users who can access specific resources and the conditions under which they can access them. This theory primarily focuses on four fundamental components, namely:

a. Subjects (users who request access to resources), where E.I. and I.I. are the subjects
b. Objects (the resources that are being accessed), Lab. resources are requested in most of the cases (high performance computing (HPC) and test platform)
c. Permissions (the rights that subjects have to access resources), first access is defined as a number of privileges for any subject
d. Policies (the regulations that determine how subjects are allowed to access objects). The rules are established by the Lab's Board

Managing subjects, permissions, rules, and objects, defines a four-parameter relationship that we have implemented technically by means based on IoT techniques. Details of the implementation are given in section 2.1.

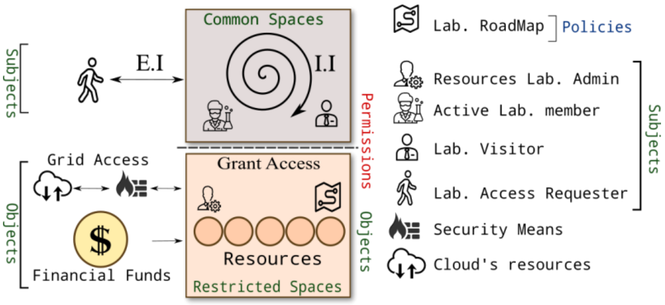


Figure 1. Topology of grants to resources access

There are several types of project research methods that can be employed depending on the nature and objectives of the study [34]–[37]. Some common research methods include experimental research, where controlled experiments are conducted to test hypotheses and determine causal relationships; survey research, which involves collecting data through questionnaires or interviews to gather insights from a specific population; qualitative research, which focuses on exploring subjective experiences and capturing rich, contextual information through methods like interviews, observations, and case studies; and quantitative research, which involves analyzing numerical data to identify patterns, trends, and statistical relationships. Each research method has its strengths and limitations, and the choice of method should align with the research goals to ensure accurate and meaningful findings [38].

The context of the problem of our case can be summed up in the design of an information system (IS) dedicated to the ‘intelligent laboratory’ research premises, the strategy of the IS is based on the access control theory (Figure 1). The technical infrastructure implemented and adopted will be secure. From what was discussed in the previous section and these applications in terms of complexities, the recommendations are matched, including a process of supervision system.

This system must be able to acquire the data in order to be able to send the appropriate commands for maintaining the reference values and setpoints, and without forgetting the conditioning of the security of the system of the laboratory(ies) against any attack without forgetting the protection of intellectual property and property relating to the same laboratory.

According to Figure 2, the laboratory security policy outlines several measures to ensure the safety and integrity of a laboratory environment. First, a physical access control system is recommended, which may involve implementing key card access, biometric scanners, or turnstiles. This restricts entry to authorized personnel only. Additionally, doors and windows should be kept locked when not in use to prevent unauthorized individuals from gaining access.

Installing security cameras is another suggested measure, serving as a deterrent against theft and vandalism while aiding in the identification of any unauthorized individuals attempting to enter the lab. Creating a comprehensive security policy is crucial, detailing procedures for maintaining laboratory security, and ensuring that all staff members are informed and adhere to these protocols. Personnel should receive training in laboratory security procedures, covering topics such as recognizing and reporting suspicious activities, safe handling and disposal of hazardous materials, and response protocols in the event of a security breach. Regular security audits are recommended to identify any weaknesses and implement corrective measures.

Maintaining a log [39] of all visitors to the laboratory, including their names, affiliations, and reasons for visiting, helps monitor access and track individuals. Visitors should also be required to wear identification badges while inside the lab for easy identification. Hazardous materials should be stored in a secure location accessible only to authorized personnel, and proper disposal procedures must be followed, including appropriate labeling, packaging, and transportation.

Any suspicious activity, including unauthorized access [40], theft, vandalism, or any other unusual behavior, should be promptly reported to the laboratory supervisor (for a given K_{reg}). Swift reporting enables timely response and mitigates potential risks. By implementing these measures, laboratory security can be significantly enhanced, safeguarding the facility, its occupants (as admin, staff. researcher or even visitors, each with specified K_{aut}), and valuable resources. Admin, grants privileges to all other resource laboratory operators, which gives an ability to the electronic embedded system to recognize and give access to researchers acting as a dedicated member of the laboratory rooms.

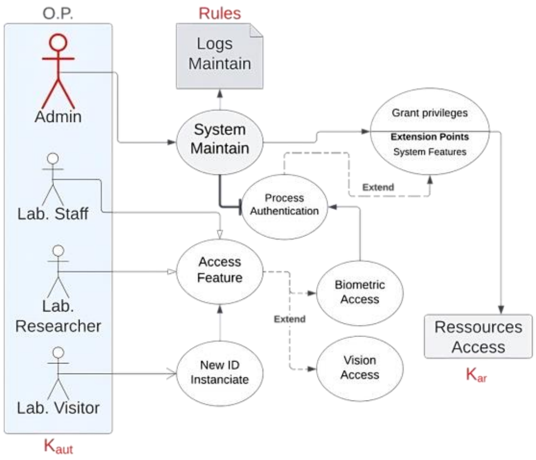


Figure 2. Use case diagram of resources laboratory access-based security approach [41]

2.1. Main concept behind the project

Our contribution is illustrated by the following Figures 3 and 4 which provide a general overview of our IoT network design from the point of view of connections (links), data exchange (communications) and combined services (tools, protocols, and means).

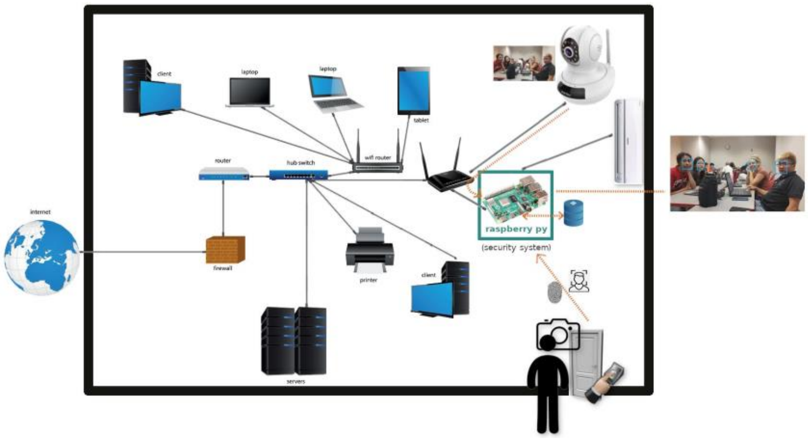


Figure 3. The IoT computer network with the security system at the laboratory level

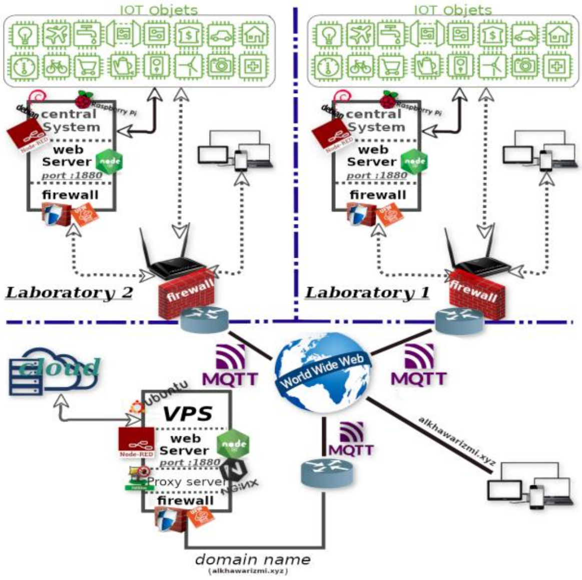


Figure 4. General vision of the connectivity of the IoT computer network and the security mechanism used at the level of the whole system

The system we propose can be divided into two parts: a local part at the laboratory level and a remote-control part in the extended network. The local part consists of computer equipment in the laboratory, such as computers, servers, and printers. These devices are connected to a central node (switch/hub) in a wireless or wired manner. The central node has access to the outside world. This network creates a local computer network in the laboratory. The most important challenge in securing this network is computer security [34], [42]. Another important challenge is protecting expensive equipment in the laboratory, such as servers, high-performance computers, and workstations.

To address these challenges, we propose configuring firewalls in our network to optimally confront attacks from the outside and to manage traffic effectively. We also propose installing an intelligent IoT system of security, control, and optimization in the network. This system is protected by a firewall in a router and a proxy server in a controller system. The controller system is a microcontroller with high computing capacity (Raspberry Pi in our case). The microcontroller processes information collected by objects in the IoT network, makes decisions, and then takes actions based on the calculated results.

As an example of an IoT object, we propose adding a fingerprint detector to the front door of the laboratory. This would allow only authorized individuals to enter the laboratory and would prevent unauthorized individuals from entering. The fingerprint detector could also be used to detect faces using machine learning technology. We believe that the system we propose can significantly improve the security of laboratory networks.

A controllable/motorized surveillance IP camera inserted for real-time supervision or by saving the shots in a secure interesting database linked to the processing systems and accessible by the person who has the power to access it. The application of AI for the detection of individuals in the laboratory is an intelligent and modern way of monitoring the time when the person in charge of monitoring is absent.

The second part is the operation of a network connected to the internet and with other laboratory networks to allow remote control in a fast, accessible and secure way as much as possible. The allocation of a virtual private server (VPS) and a personal domain name through domain name hosting companies and computer hardware resources; such as random access memory (RAM) and storage capacity (cloud), amount of computation either mathematical (logic central processing unit (CPU)) or much more graphically oriented (graphics processing unit (GPU)), is a very effective way to make this network targeted for a feasible design.

In our case, material resources with the storage and domain name are hosted in a company named ‘Octenium web hosting Algeria’ as a VPS machine under Ubuntu as OS. The same machine is maintained for additional installation and configuration of a firewall and a proxy server. An open-source information sharing and messaging protocol that provides non-permanent communications between devices by transporting their messages called message queuing telemetry transport (MQTT), for "message queuing telemetry transport", it is used to allow two devices using different technologies to communicate. Web giants including Amazon Web Services (AWS) or Microsoft use MQTT to upload data to their cloud platform [43]. This protocol is used for communication between the virtual private server and security systems in laboratory computer networks. We therefore obtain an integrated and secure process and a large network contains computer sub-networks operating on the principle of the IoT [7], [44].

2.2. The Node-RED environment

Node-RED, a software tool created by (international business machine) IBM Watson, is an open-source solution designed for interconnecting hardware devices, APIs, and online services in innovative and practical ways [45]. Developed using JavaScript and built upon Node.js as its web server foundation, Node-RED employs a visual programming paradigm known as graphical programming or flows. These flows consist of predefined code blocks called nodes that execute specific tasks. Facilitating seamless stream composition, Node-RED provides a browser-based stream editor, enabling the assembly of streams through the utilization of an extensive palette of nodes. The constructed flows can be instantly deployed during runtime through a single click. Within the editor, one can craft functions in JavaScript, Python, C++, and other languages, employing a feature-rich text editor. Additionally, a built-in library allows the preservation of valuable functions, templates, or flows for future reuse. Streams generated within Node-RED are stored using javaScript object notation (JSON), enabling effortless import and export for sharing purposes. An online stream library provides the avenue for sharing these innovative streams with the global community.

Node-RED, while prominently associated with visualizing the intricacies of the IoT, can also be employed for a spectrum of applications, serving as a rapid assembler of service flows. The nomenclature might not immediately convey its purpose; however, the inclusion of Node in the name is attributed to the tool's implementation as a node application. From the end-user perspective, this detail remains an internal implementation aspect. Available as open-source software, Node-RED was developed by IBM's Emerging Technology organization. It's integrated into the starter application of Bluemix IoT, IBM's cloud platform. Alternatively, it can be independently deployed as a Node.js application.

For IoT endeavors with Node-RED, integration with the IoT foundation service within your Bluemix application is crucial. Bluemix, initially launched by IBM in 2014 and merged with IBM cloud in 2017, serves as a cloud platform. The IoT service enables device registration and connection. Subsequently, inbound and outbound MQTT nodes can be employed within your streams. To delve deeper, consider exploring the current Bluemix IoT samples. Most of them use Node-RED to define streams where incoming sensor data from “things” is processed and stored in databases and/or commands are sent to devices as shown in Figure 5.

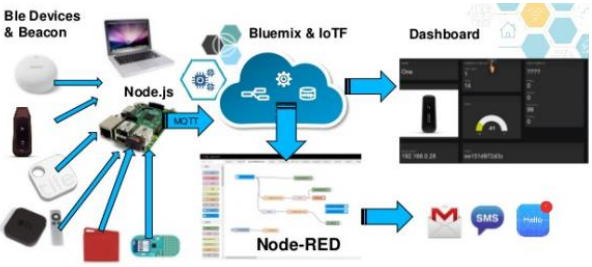


Figure 5. Functional illustration of Node-RED

3. RESULTS AND DISCUSSION

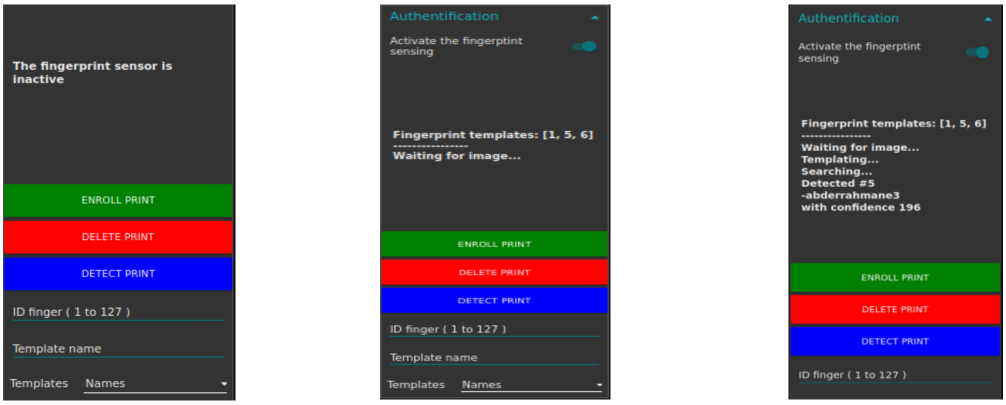
The purpose of this study was to explore the potential of IoT technology for enhancing laboratory security. To this end, we developed a prototype system that incorporates multiple sensors and controls, including a fingerprint sensor, IP camera with person detection and video recording, temperature, humidity and brightness sensors, fan and light controls, and door opening control. The system was designed using Node-RED framework and included a web interface that allowed for local and remote monitoring of the laboratory environment.

In this section, we present the results of our testing and evaluation of the prototype system. Specifically, we examine the performance of each sensor and control component, as well as the overall effectiveness of the system in providing enhanced laboratory security. We also discuss the potential benefits and drawbacks of using IoT technology for laboratory security, and consider areas for future research and development. Overall, the results of this study demonstrate the potential of IoT technology for enhancing laboratory security, and suggest that further research is needed to fully explore the capabilities of these systems. We hope that our findings will contribute to ongoing efforts to improve laboratory security, and inspire further innovation in this important area.

3.1. Scenario

The case to be treated is defined as being a need for security in the first link and to supervise, control parameters in a laboratory (laboratory networks):

a. A fingerprint sensor in front of the entrance door, for individual authentication and allowing only those who have authorization to enter and refusing who does not by capturing what was in front of the door at each time, with a possibility of face detection by the use of machine learning technology feels good credibility. In Figure 6(a) we have the graphical interface of the supervision process of fingerprint authentication in inactive process status, whereas Figure 6(b) in the process of being sensed, and Figure 6(c) is the case of detection with positive authentication. The same in Figures 7(a), (b), and (c), we have the inactive case, the active process of taking a capture, and is the case of detection with positive authentication respectively. The door will be opened if we had a positive authentication as in Figure 8(a) otherwise the door will still be closed as in Figure 8(b).



(a)

The fingerprint sensor is inactive

(b)

Activate the fingerptint sensing

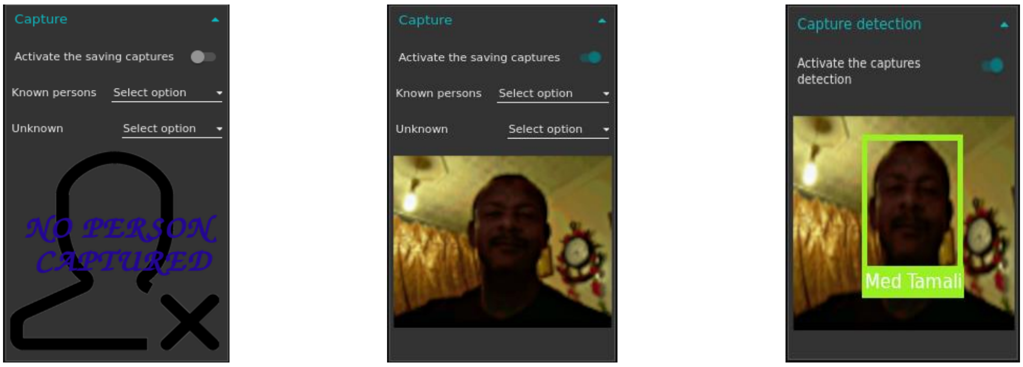
```
Fingerprint templates: [1, 5, 6]
----------------
Waiting for image...
```

(c)

Activate the fingerptint sensing

```
Fingerprint templates: [1, 5, 6]
----------------
Waiting for image...
Templating...
Searching...
Detected #5
-abderrahmane3
with confidence 196
```

Figure 6. The graphical interface represents the supervision process of authentication by fingerprint detector, (a) inactive process, (b) in the process of being sensed, and (c) case of detection with positive authentication



(a) (b) (c)

Figure 7. Process of capturing the person in front of the door, (a) inactive process or the case where there is no voluntary in front of the door, (b) a captured person, and (c) detection process after capture

(a) (b)

Figure 8. Presentation on a prototype of the authentication process, (a) access granted by opening the door and (b) access denied by closing or remaining closed the door

b. The use of an IP camera for supervision in the laboratory with the power to control its motors for 360°x160° visual scanning as shown in Figure 9, control of infrared lights for night vision, and recording of video clips according to the desire for recovery from past events as shown in Figure 10.

Face detection, an application of object detection within the realm of AI, involves the utilization of computer technology to locate and recognize human faces within digital images. The functionality of face detection technology spans diverse domains, encompassing security, biometrics, law enforcement, entertainment, and personal safety. It facilitates the real-time monitoring and tracking of individuals. Notably, in the context of image or video analysis, face detection serves the purpose of pinpointing regions of interest for the assessment of age, gender, and emotional states through facial expressions. Within a facial recognition framework, which involves the mathematical mapping of distinct facial attributes into a facial print for data storage, the preliminary face detection data becomes indispensable. This data guides the algorithms responsible for identifying the specific portions of an image or video that are requisite for the generation of a comprehensive facial print [46], [47]. Once identified, the new faceprint can be compared to the stored faceprints to determine if there is a match as shown in Figure 11. In Figure 11(a) we have an inactive face detection process, while Figure 11(b) in an active process with a known lab member detected.

c. The measurement of some environmental parameters as shown in Figure 12, namely, the temperature, the luminosity and the humidity and then to make actuations according to conditions.

Temperature control by detecting first, as shown in Figure 12(a), if the temperature exceeds thresholds, a fan instead of an air conditioner is triggered. Similarly for humidity detection, as shown in Figure 12(b), one would open or close the door, if the humidity is below/above a specific value. A light dependent resistor (LDR) detects the brightness level of light at a given location. we measure luminosity (as shown in Figure 12(c) in front of the door in the event that a person is there and there is too little luminosity, so a flash (torch) will be lit for the captured phenomenon to take a clear image capture.

d. Door control (opening/closing) with simple clicks, with the power to know its status as shown Figure 13.
e. If holder(s) of access rights to the administration part of the laboratory system want to see and consult the image captures of people who have visited the lab, the possibility is offered.
f. He still has the choice to delete all captured images (the system stores and compresses a copy).
g. All parameters of the principal small single-board programmable computer (Raspberry PI) and the parameters of the VPS like the used operating system, microprocessors, memory status and other information are present as shown in Figure 14.

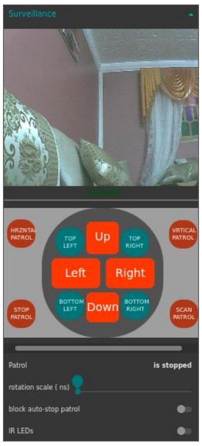


Figure 9. The engine monitoring and control part and some real-time options

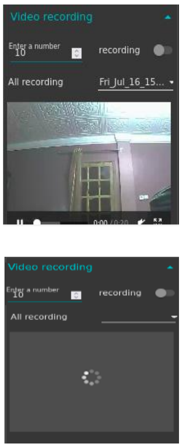
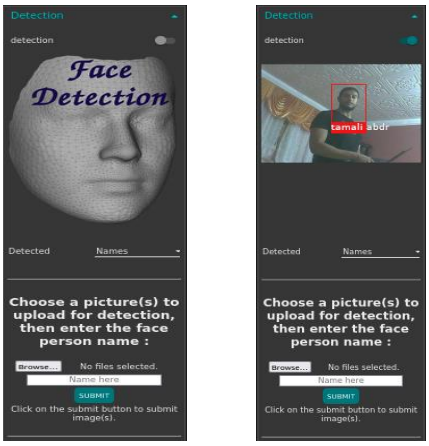
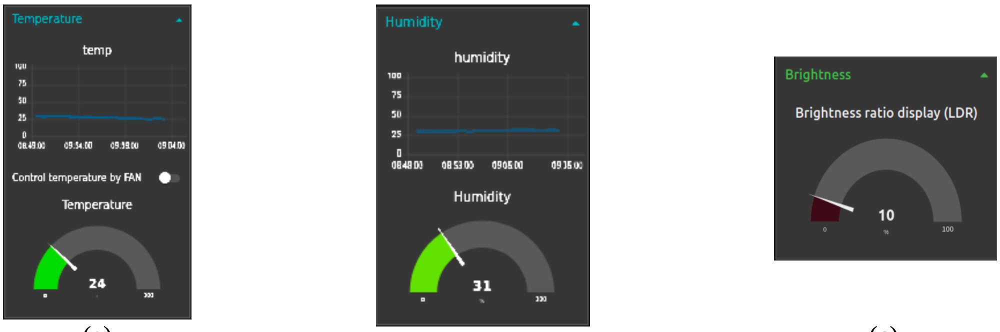


Figure 10. The recording and playback part of what is recorded


Detection
detection
Face Detection
Detected
Names
Choose a picture(s) to upload for detection, then enter the face person name :
Browse...
No files selected.
Name here
SUBMIT
Click on the submit button to submit image(s).
Detection
detection
tamali abdr
Detected
Names
Choose a picture(s) to upload for detection, then enter the face person name :
Browse...
No files selected.
Name here
SUBMIT
Click on the submit button to submit image(s).

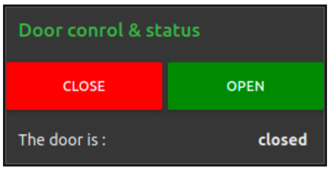
(a) (b)

Figure 11. Real-time face detection, (a) inactive process and (b) active process



(a) (b) (c)

Figure 12. Measuring parameters and constantly displaying them in a readable way with dashboard gauge controls node, (a) temperature, (b) humidity, and (c) brightness



The door is : closed

Figure 13. The control and status block of the laboratory door

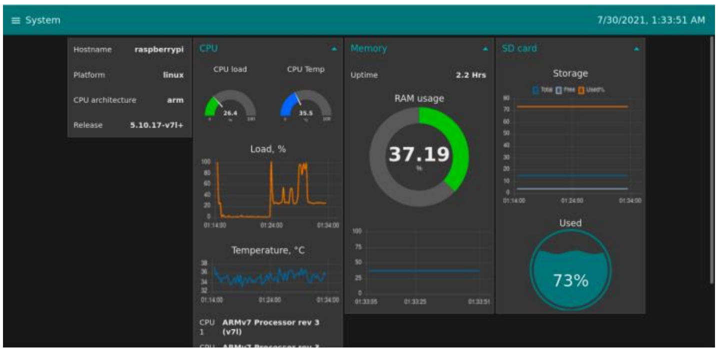
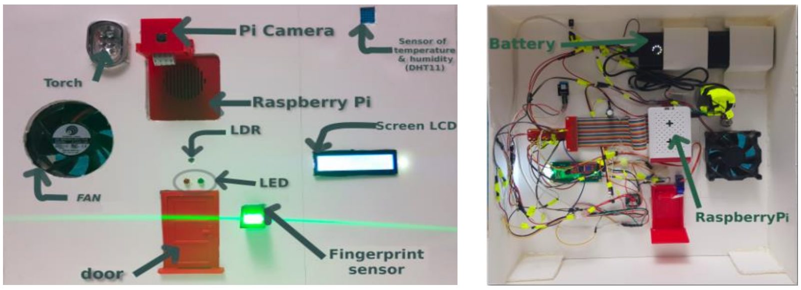


Figure 14. The system parameters representation page (Raspberry Pi)

3.2. Prototype

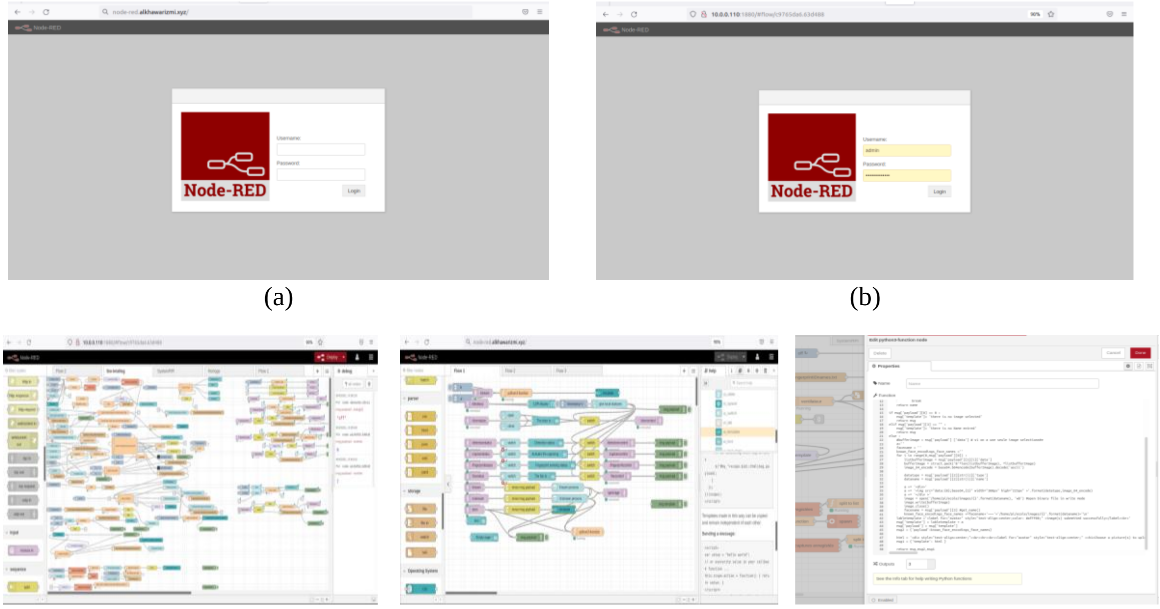
Figure 15 shows an overview of our prototype system, in Figure 15(a) is the front view and Figure 15(b) is the other side view. The system was designed to provide enhanced security for laboratory environments by incorporating multiple sensors and controls, including a fingerprint sensor, IP camera with person detection and video recording, temperature and humidity sensors, brightness sensor, fan and light controls, and door opening control. Our primary objective was to evaluate the performance of each sensor and control component, as well as the overall effectiveness of the system in providing enhanced laboratory security.



(a) (b)

Figure 15. The prototype and its components, (a) in front and (b) the assembly carried out (the prototype from behind)

The system was designed logically using Node-RED firmware (Figure 16) and included a web interface that allowed for local and remote monitoring of the laboratory environment. In Figures 16(a) and (b) we have two security interfaces for access with username and password to the development part in the VPS and in the Raspberry Pi (locally) respectively, we have a very complex programmed and configured process as shown in Figures 16(c) and (d) the programming and configuration interface in the Raspberry Pi and in the VPS respectively of which each node can have several lines of programming code like the function node in Figure 16(e).

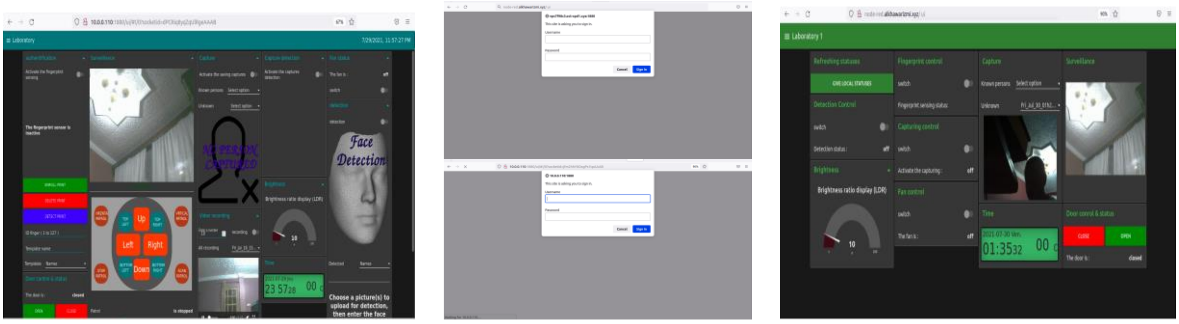


(a) (b)

(c) (d) (e)

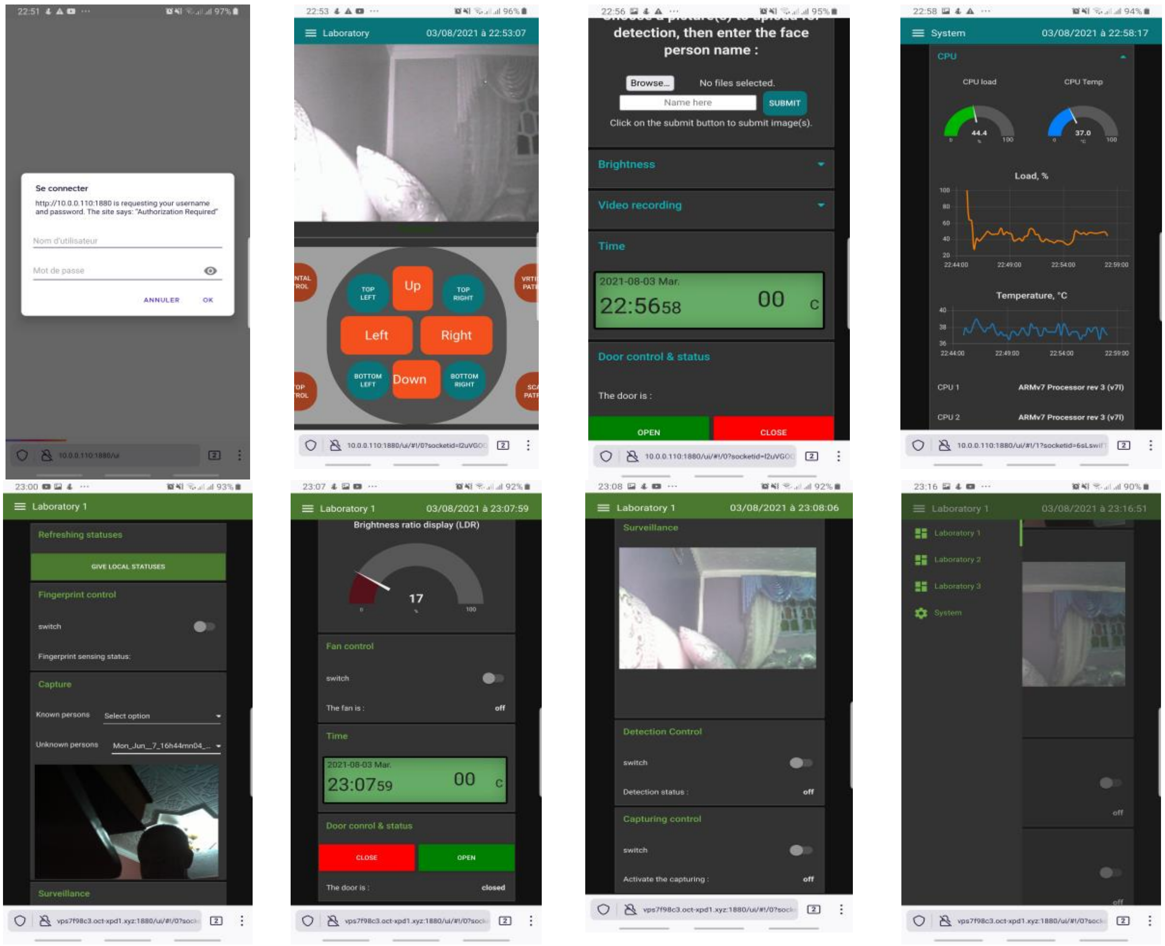
Figure 16. Development parts, (a) and (b) represent security interfaces for access with username and password to the development part in the VPS and in the Raspberry Pi respectively, (c) and (d) represent screenshots of the programming and configurations part in the Raspberry Pi and in the VPS respectively, and (e) example of a function node contains lines of programming in Python3 language

Figures 17(a) provide an example of our local web interface used to monitor the lab environment with secure access as in Figures 17(b) and (c) is our web interface used to monitor the laboratory environment but through access from outside the local network of each laboratory. As can be seen, the interface provides real-time readings for temperature, humidity, and brightness, as well as a live video feed from the IP camera. The interface also allows for remote control of the fan, lights, and door, providing a high degree of flexibility and control over the laboratory environment. In Figure 18 we have the phone version interfaces identical to that in Figure 17.



(a) (b) (c)

Figure 17. Interfaces of the dashboard (on desktop PC), (a) is screenshots of the page generated by the Raspberry Pi localy, (b) of the access security pre-pages with username and password generated on our VPS and that generated by the local web server respectively, and (c) is screenshot of the page generated by the VPS



Se connecter

http://10.0.0.110:1880 is requesting your username and password. The site says: "Authorization Required"

Nom d'utilisateur

Mot de passe

ANNULER OK

detection, then enter the face person name :

Browse... No files selected.

Name here SUBMIT

Click on the submit button to submit image(s).

The door is :

The fan is : off

The door is : closed

Known persons: Select option

Unknown persons: Mon_Jun__7_16h44mn04_...

Detection status : off

Activate the capturing : off

CPU 1 ARMv7 Processor rev 3 (v7l)

CPU 2 ARMv7 Processor rev 3 (v7l)

Figure 18. Dashboard interfaces (on mobile phone)

Through this assembly and all the logic behind it, we were confronted with many fundamental notions, in terms of object-oriented programming (case of Node.js server, Python, HTML for HyperText Markup Language, and structured query language (SQL)), manipulation under the operating system Linux, configuration of systems/software/applications, the implementation of firewalls of different methods and management of incoming/outgoing flows.

The achievements are numerous, starting from the use, and the manipulation of microcontroller and peripheral equipment to the programming of the Node-RED interface following the logical assembly of the Raspberry PI 3 machine. Experience is invaluable with the number of logical or material objects to manipulate. The concepts used are among the most recent, which qualifies the opportunity as unique. The document relates and briefly describes the steps necessary to develop an assembly and program it under Node-RED for possible other use.

In essence, employing access control theory enables us to prioritize criteria based on their level of significance, which enhances our ability to be more adaptable and flexible. However, the system is more susceptible to threats when it comes to grant-related funding for development programs, whereas access-related situations have lower risks and less external pressure on the laboratory. Accessing a laboratory is comparable to gaining entry to a computer center by authorized personnel or through an authentication server setup.

4. CONCLUSION

In conclusion, our study has demonstrated the potential of IoT technology for enhancing laboratory security. Our prototype system, which incorporated multiple sensors and controls including a fingerprint sensor, IP camera with person detection and video recording, temperature and humidity sensors, brightness sensor, fan and light controls, and door opening control, was designed using Node-RED firmware and included a web interface that allowed for local and remote monitoring of the laboratory environment.

Our testing and evaluation of the system showed that each sensor and control component performed effectively, and that the system as a whole provided enhanced laboratory security. In addition, we discussed the potential benefits and drawbacks of using IoT technology for laboratory security, and highlighted areas for future research and development. Overall, our findings suggest that IoT technology has the potential to provide a new paradigm for laboratory security, offering granular control over access to different parts of the laboratory and providing real-time monitoring of the laboratory environment. However, the use of IoT devices also introduces new security risks, and it is important to ensure that these devices are properly secured to prevent unauthorized access or tampering. We believe that our study will be of interest to researchers and practitioners in the field of laboratory security, as well as to those interested in the application of IoT technology in other domains. We hope that our work will inspire further innovation in this important area, and contribute to the development of more secure and efficient laboratory environments.

ACKNOWLEDGEMENTS

No research grant or contract, and all authors are contributing equally to the development of this research. Additionally, no request for funds was necessary. We thank all the teachers especially Dr Bouida Ahmed and colleagues who contributed practical and/or intellectual assistance.

REFERENCES

[1] P. Gajendran, G. S. Setty, S. Vasanth, C. A. Kumar, and R. M. Kumar, “IoT based Circuit Breaker with Access Control,” in *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, Jun. 2023, pp. 928–933, doi: 10.1109/ICSCSS57650.2023.10169319.

[2] M. Krommyda, E. Sdongos, S. Tamascelli, A. Tsertou, G. Latsa, and A. Amditis, “Towards Citizen-Powered Cyberworlds for Environmental Monitoring,” in *2018 International Conference on Cyberworlds (CW)*, Oct. 2018, pp. 454–457, doi: 10.1109/CW.2018.00090.

[3] Z. Mi and G. Wei, “A CoAP-Based Smartphone Proxy for Healthcare with IoT Technologies,” in *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)*, Nov. 2018, pp. 271–278, doi: 10.1109/ICSESS.2018.8663785.

[4] J. Dofe, A. Nguyen, and A. Nguyen, “Unified Countermeasures against Physical Attacks in Internet of Things - A survey,” in *2021 IEEE International Symposium on Smart Electronic Systems (iSES)*, Dec. 2021, pp. 194–199, doi: 10.1109/iSES52644.2021.00053.

[5] S. Avadut and S. K. Udgata, “A Deep Learning based IoT Framework for Assistive Healthcare using Gesture Based Interface,” in *2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)*, Nov. 2022, pp. 6–12, doi: 10.1109/IoTaIS56727.2022.9975885.

[6] F. Chen and C. Yin, “A Novel Method to Resolve the Dynamic IP Address for the Server-Side Gateway over the Internet of Things,” in *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*, Sep. 2012, pp. 1–3, doi: 10.1109/WiCOM.2012.6478338.

[7] D. Guinard, V. Trifa, and E. Wilde, “A resource oriented architecture for the Web of Things,” in *2010 Internet of Things (IOT)*, Nov. 2010, pp. 1–8, doi: 10.1109/IOT.2010.5678452.

[8] P. C T, S. K. G A, and D. Mehta, “Multi Level Key Exchange and Encryption Protocol for Internet of Things (IoT),” *Computer Systems Science and Engineering*, vol. 35, no. 1, pp. 51–63, 2020, doi: 10.32604/csse.2020.35.051.

[9] D.-Y. Kao and S.-C. Hsiao, “The dynamic analysis of WannaCry ransomware,” in *2018 20th International Conference on Advanced Communication Technology (ICACT)*, Feb. 2018, pp. 159–166, doi: 10.23919/ICACT.2018.8323682.

[10] Kaspersky, “Kaspersky DDoS Intelligence Report for Q2 2016,” *Securelist*. 2016. [Online]. Available: https://securelist.com/kaspersky-ddos-intelligence-report-for-q2-2016/75513/

[11] Y. Zhang, S. Wang, H. Xia, and J. Ge, “A Novel SVPWM Modulation Scheme,” in *2009 Twenty-Fourth Annual IEEE Applied Power Electronics Conference and Exposition*, Feb. 2009, pp. 128–131, doi: 10.1109/APEC.2009.4802644.

[12] F. Mehdipour, “A Review of IoT Security Challenges and Solutions,” in *2020 8th International Japan-Africa Conference on Electronics, Communications, and Computations (JAC-ECC)*, Dec. 2020, pp. 1–6, doi: 10.1109/JAC-ECC51597.2020.9355854.

[13] N. Mishra and S. Pandya, “Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review,” *IEEE Access*, vol. 9, pp. 59353–59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

[14] N. Tewari and G. Datt, “A Systematic Review of Security Issues and challenges with Futuristic Wearable Internet of Things (IoTs),” in *2021 International Conference on Technological Advancements and Innovations (ICTAI)*, Nov. 2021, pp. 319–323, doi: 10.1109/ICTAI53825.2021.9673353.

[15] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, “An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security,” *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10250–10276, Oct. 2020, doi: 10.1109/JIOT.2020.2997651.

[16] M. Khudhair Al-Gburi and L. A. Abdul-Rahaim, “Secure smart home automation and monitoring system using internet of things,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 28, no. 1, pp. 269–276, Oct. 2022, doi: 10.11591/ijeecs.v28.i1.pp269-276.

[17] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, “Industrial Internet of Things: Challenges, Opportunities, and Directions,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018, doi: 10.1109/TII.2018.2852491.

[18] 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*, vol. 9, pp. 107200–107223, 2021, doi: 10.1109/ACCESS.2021.3101218.

[19] A. N. Doss, D. Shah, G. F. Smaisim, M. Olha, and S. Jaiswal, “A Comprehensive Analysis of Internet of Things (IOT) in Enhancing Data Security for Better System Integrity - A Critical Analysis on the Security Attacks and Relevant Countermeasures,” in *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Apr. 2022, pp. 165–167, doi: 10.1109/ICACITE53722.2022.9823817.

[20] A. Qashlan, P. Nanda, and X. He, “Security and Privacy Implementation in Smart Home: Attributes Based Access Control and Smart Contracts,” in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Dec. 2020, pp. 951–958, doi: 10.1109/TrustCom50675.2020.00127.

[21] Z. Zulkifl *et al.*, “FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs,” *IEEE Access*, vol. 10, pp. 15644–15656, 2022, doi: 10.1109/ACCESS.2022.3149046.

[22] S. M. Rukmony and S. Gnanamony, “Rough set method-cloud internet of things: a two-degree verification scheme for security in cloud-internet of things,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2, pp. 2233–2239, Apr. 2023, doi: 10.11591/ijece.v13i2.pp2233-2239.

[23] M. U. Aftab *et al.*, “A Hybrid Access Control Model With Dynamic COI for Secure Localization of Satellite and IoT-Based Vehicles,” *IEEE Access*, vol. 8, pp. 24196–24208, 2020, doi: 10.1109/ACCESS.2020.2969715.

[24] H.-C. Chen, C.-H. Chang, and F.-Y. Leu, “Implement of agent with role-based hierarchy access control for secure grouping IoTs,” in *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Jan. 2017, pp. 120–125, doi: 10.1109/CCNC.2017.7983092.

[25] R. Ab Rahman, U. R. Hashim, and S. Ahmad, “IoT based temperature and humidity monitoring framework,” *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 1, pp. 229–237, Feb. 2020, doi: 10.11591/eei.v9i1.1557.

[26] M. G. Kibria and M. T. A. Seman, “Internet of things based automated agriculture system for irrigating soil,” *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 3, pp. 1752–1764, Jun. 2022, doi: 10.11591/eei.v11i3.3554.

[27] A. Dahir, M. Omar, and Y. Abukar, “Internet of things based agricultural drought detection system: case study Southern Somalia,” *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 1, pp. 69–74, Feb. 2023, doi: 10.11591/eei.v12i1.4117.

[28] R. V. Chandraiah and A. Ramalingappa, “Secure authentication and data aggregation scheme for routing packets in wireless sensor network,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 3, pp. 3217–3226, Jun. 2023, doi: 10.11591/ijece.v13i3.pp3217-3226.

[29] M. Parmar and P. Shah, “Internet of things-blockchain lightweight cryptography to data security and integrity for intelligent application,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 4, pp. 4422–4431, Aug. 2023, doi: 10.11591/ijece.v13i4.pp4422-4431.

[30] G. Thahniyath, P. Mishra, and S. R. Moorthy, “Two phase secure data collection technique for wireless sensor networks,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 1, pp. 512–520, Apr. 2022, doi: 10.11591/ijeecs.v26.i1.pp512-520.

[31] G. Piho, J. Tepandi, and M. Parman, “Towards LIMS (Laboratory Information Management Systems) software in global context,” in *MIPRO 2012 - 35th International Convention on Information and Communication Technology, Electronics and Microelectronics - Proceedings*, 2012, pp. 721–726.

[32] D. O. Skobelev, T. M. Zaytseva, A. D. Kozlov, V. L. Perepelitsa, and A. S. Makarova, “Laboratory information management systems in the work of the analytic laboratory,” *Measurement Techniques*, vol. 53, no. 10, pp. 1182–1189, Jan. 2011, doi: 10.1007/s11018-011-9638-7.

[33] K. Boyar, A. Pham, S. Swantek, G. Ward, and G. Herman, “Laboratory Information Management Systems (LIMS),” in *Cannabis Laboratory Fundamentals*, Cham: Springer International Publishing, 2021, pp. 131–151, doi: 10.1007/978-3-030-62716-4_7.

[34] M. Al-Sadoon and A. Jedidi, “A secure trust-based protocol for hierarchical routing in wireless sensor network,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 4, pp. 3838–3849, Aug. 2022, doi: 10.11591/ijece.v12i4.pp3838-3849.

[35] M. A. Hatem, B. A. Hameedi, and J. N. Hasoon, “Lightweight digital imaging and communications in medicine image encryption for IoT system,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 21, no. 4, pp. 771–783, Aug. 2023, doi: 10.12928/telkomnika.v21i4.24766.

[36] R. R. Chowdhury, A. C. Idris, and P. E. Abas, “Device identification using optimized digital footprints,” *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 12, no. 1, pp. 232–240, Mar. 2023, doi: 10.11591/ijai.v12.i1.pp232-240.

[37] D. D. Khudhur and M. S. Croock, "Developed security and privacy algorithms for cyber physical system," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 6, pp. 5379–5389, Dec. 2021, doi: 10.11591/ijece.v11i6.pp5379-5389.

[38] A. Benbatouche and B. Kadri, "Design and realization of low-cost solenoid valve remotely controlled, application in irrigation network," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 3, pp. 1779–1788, Jun. 2022, doi: 10.11591/eei.v11i3.4123.

[39] L. Xu, D. Huang, and W.-T. Tsai, "Cloud-Based Virtual Laboratory for Network Security Education," *IEEE Transactions on Education*, vol. 57, no. 3, pp. 145–150, Aug. 2014, doi: 10.1109/TE.2013.2282285.

[40] S. Hashemi and M. Zarei, "Internet of Things backdoors: Resource management issues, security challenges, and detection methods," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, Feb. 2021, doi: 10.1002/ett.4142.

[41] Y. H. Elawady and A. S. Tolba, "A general framework for remote laboratory access: A standarization point of view," in *The 10th IEEE International Symposium on Signal Processing and Information Technology*, Dec. 2010, pp. 485–490, doi: 10.1109/ISSPIT.2010.5711755.

[42] V. T. Kannan and R. Chakravarthi, "Efficient addressing schemes for internet of things," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 4, pp. 4415–4429, Aug. 2022, doi: 10.11591/ijece.v12i4.pp4415-4429.

[43] P. Pierleoni, R. Concetti, A. Belli, and L. Palma, "Amazon, Google and Microsoft Solutions for IoT: Architectures and a Performance Comparison," *IEEE Access*, vol. 8, pp. 5455–5470, 2020, doi: 10.1109/ACCESS.2019.2961511.

[44] M. A. Naagas, A. R. Malicdem, and T. D. Palaoag, "DEH-DoSv6: A defendable security model against IPv6 extension headers denial of service attack," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 274–282, Feb. 2021, doi: 10.11591/eei.v10i1.2670.

[45] A. Sinharay *et al.*, *A Novel Approach to Unify Robotics, Sensors, and Cloud Computing Through IoT for a Smarter Healthcare Solution for Routine Checks and Fighting Epidemics*. Switzerland: Springer, Cham, 2016, doi: 10.1007/978-3-319-47063-4_59.

[46] O. Sbai and M. Elboukhari, "Deep learning intrusion detection system for mobile ad hoc networks against flooding attacks," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 11, no. 3, pp. 878–885, Sep. 2022, doi: 10.11591/ijai.v11.i3.pp878-885.

[47] G. C. Sekhar and A. Rajendran, "A secure framework of blockchain technology using CNN long short-term memory hybrid deep learning model," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 28, no. 3, pp. 1786–1795, Dec. 2022, doi: 10.11591/ijeecs.v28.i3.pp1786-1795.

BIOGRAPHIES OF AUTHORS

Tamali Abderrahmane born in 1995, received the Master degree in Telecommunications systems from Tahri Mohammed Bechar university, currently a PhD student in Networks and Telecommunications at Ferhat Abbas Setif1 University, likes substantive and group work. Having programming skills, electronic application development, manipulation of Linux environment, development of robotic machine under ROS environments and IoT applications. He can be contacted at email: abdou.t10@gmail.com.

Amardjia Nourredine received the engineering degree in electronics in 1982 from ENPA (Ecole Nationale Polytechnique d'Alger), Algeria, his Master of Science degree in electrical engineering in 1985, from Fairleigh Dickinson University, New Jersey, USA, and his State Doctorate (Ph.D.) in communications in 2007 from University of Setif, Algeria. He joined the Electronics Department, University of Setif as an assistant professor in 1986. He has granted to the level of associate professor in 2007. He is a member of the LIS laboratory, University of Setif. His research interests include discrete transforms, image processing, filter design techniques, systolic architectures and fast algorithms for signal processing applications. He can be contacted at email: amardjianour@univ-setif.dz.

Tamali Mohammed graduated from USTO-MB as state Engineer in Electrical engineering, he received his M.Sc. in 1996 in Energetical physics from Bechar University and the Ph.D. degrees from UST-MB of Oran, Algeria in 2007 and in 2013, he became Professor in Electrical Engineering. He is head of the SimulIA research team at the ENERGARID Lab. His fields of interest included power electrical system, scientific computing tools, sustainable development, environmental studies applied to distributed electrical network optimization, system theory application on power system. He actually worked as a research professor at the University of Bechar from 1986 until today. He can be contacted at email: tamali.mohammed@univ-bechar.dz.