IoT scheme for surveillance system and laboratory security access

I Fushshilat1,* and Y Yogasmana2

1 Department of Electrical Engineering Education, Universitas Pendidikan Indonesia, Jalan Dr. Setiabudhi No.229, Bandung, Indonesia
2 Department of Mechanical Engineering Education, Universitas Pendidikan Indonesia, Jalan Dr. Setiabudhi No.229, Bandung, Indonesia

*imanf@upi.edu

Abstract. This paper proposes to design a modern surveillance system and laboratory access using digital technology, through the concept of the Internet of Things (IoT) which is becoming one of the trending topics in the development of world technology nowadays. IoT makes several electronic devices such as actuators, biometric sensors, RFID Reader, servers, and IP cameras are connected to an Internet network. Thus, those devices can be accessed anytime anywhere outside laboratory. Identification of visitors are using RFID cards or biometrics sign such as fingerprints or faces that have been recognized by the system and every time visitors come to laboratory, they are recorded directly into the server automatically, IP camera allows displaying in real-time condition of the Laboratory, The system is utilizing the indoor sound system as a device for conducting teleconferences and appealing for information to visitors to the laboratory remotely via the internet, all of these are very useful for establishing a better security and surveillance system and facilitating work of laboratory administrators.

1. Introduction

As facility for education, and research. Laboratory has a lot of data, component, tools, device, valuable instrument that needs security [1]. Nowadays, most of Surveillance and security system of laboratory is still done in the conventional way handled manually by a laboratory staff / admin, whereas these opportunities can be optimized through a technology system.

Internet becomes technology that has developed very rapidly in this century, internet support devices such as smartphones, tablets, and computer. Internet is accessible by someone, anywhere and anytime [2]. In its application, internet does not only act as a provider of information such as news, knowledge, email, shopping, entertainment, etc. but also the concept of the Internet of Things (IoT) can be used as a media to connect / control a device in real time, anytime and anywhere.

IoT is a communication paradigm that refers to the idea of connecting daily life objects to Internet, where the object is combined with a microcontroller. In the other side, transceivers are able to communicate and configured with certain protocols so that it can interact between an object and others to achieve certain goals without human intervention [3]. Briefly IoT is a technology that facilitates interconnection between systems so that they can be connected to each other [4].

This paper proposes to design the laboratory security access and supervision using IoT technology to improve the security system in the laboratory. This system integrates several electronic devices such
as IP cameras, Motor DC, solenoid, RFID, controller in a network so each other can communicate and be controlled remotely by the administrator/ laboratory staff, it can improve the laboratory security access and laboratory supervision.

2. Related work
Many studies have been conducted on electronic-based security access. For instances, the door access security system that can be controlled via Bluetooth [5]. The digital smart door security system integrated through several components such as Solenoid Actuators, RFID and Zigbee [6]. Wireless communication modules, Security system Non-contact based access has been by utilizing PSTN telephone tones that commonly known as DTMF (Dual Tone Multi Frequency) using Arduino as Controller and Solenoid as actuator which is mounted on the door as access security [7].

The use of biometrics as the key to access to a security system has also been studied, one of them by [8] was discussed about Fingerprint-based automatic door lock system to identify entry person access, then data from the fingerprint reading is sent to central communications and then forwarded to users via the telephone network, so user can find out who is entering the room. Meanwhile, a smart house model uses biometrics face detection as an identification feature of entry access, camera taking a photo of the visitor's face then through the face recognition method, smart home detects and identifies the faces of visitors so that foreigners cannot enter the house, only faces that have been registered in the system database can be entered into the house [9]. The development of other access security systems based on electronic was developed by utilizing GSM modules for receiving phone calls from users, then they can detect Caller ID which is used as the authorization key to access the system [10].

Based on the comparison with some relevant study results, we proposed an innovation design laboratory security access and surveillance system that adopted IoT technology by combining several electronic components with each other connected to an internet network, to improve security and to facilitate supervision in the laboratory, and to facilitate the work of Laboratory Staff.

3. System work scenarios
Laboratory users who will access the laboratory devices must go through the Laboratory door which has an electronic lock that can only be opened through RFID, or uses biometric sign such as fingerprints and faces that have been registered in the database server computer, Laboratory users must do a tapping identity card that has been equipped with an RFID chip (RFID Card) that has been previously registered, so that it can be recognized by the system, besides that it can also use Biometrics features such as faces or fingerprints that have previously been registered to the database server so can be recognized by the system, so everyone who enters the Laboratory will be recorded in database on server computer. For certain cases, if someone does not have authentication id to enter the laboratory and laboratory officers are not there, then user can contact the laboratory officer or administrator to request access into the laboratory by contacting the admin through taking a picture by scanning their face on face recognition camera. And then, the face data are stored on the server in order to be verified by the admin. If he approved, then user is able to enter the laboratory. Laboratory administrators can provide access by opening doors through electronic devices such as computers, hand phone or tablet that is connected to the internet, thus the administrator can provide access anytime anywhere even though outside the laboratory.

The IP Camera installed in the Laboratory allows Laboratory administrators to conduct remote monitoring through computer media, hand phone, tablet or electronic gadget that are connected to the Internet. Indoor Sound System can be used to provide advice or information remotely via the internet to laboratory users through administrator electronic gadgets or other users who have access to authorization and authentication to the Server.
4. System architecture

The architecture of the supervision system and laboratory access security proposed in this paper consists of several components including Controlled Device, Node Controller, Accesses Identifier, Router, Server, IP Camera, Indoor Sound System as shown in Figure 1.

Controlled device is a series of devices installed on objects that will be controlled by security access, for example such as doors, gates, windows, cabinets, lockers, and so on. Controlled Device consists of several components such as an electric motor and an electric solenoid as an electronic actuator, an electric motor functions as a door, gate or device driver which will be controlled remotely, Electronic solenoid as a key that will be attached to the door, gates and other objects where the lock and release systems are carried out electronically, then the components of limit switch and proximity sensor as a position sensor for the door or other objects that will be controlled movement, Mechanical Structure is a mechanical framework composed by several metals assembled in such a way that serves to convert the rotation of an electric motor into a motion that can be used to open and close the door or gate of the laboratory.

The Node Controller component responds to the data coming from a Sensor on a controlled device, access identifier and admin command then process it to make decisions to controlling the actuator on the controlled device, on this architecture a component of node controller handles a packet of controlled devices, this is because a node controller has limited General Purpose Input Output (GPIO) which is to receiving data and performing controls. Access Identifier consists of RFID Reader and fingerprint and face scanner, RFID Reader functions to read data from RFID cards that are owned by visitors, as well as fingerprint and face scanner both function to read data from biometric features, namely fingerprints and faces that are owned by visitors. User data as a result of verification and identification of Access Identifiers are then sent to the Node Controller to be identified and verified according to the data on the server.

The router functions to regulate data traffic from the Node Controller, IP Cam to Server and or vice versa in a network. In this communication the Router functions as an Access Point where the Node Controller and IP Cam communicate with the Server via Wireless Router. Beside it, Router also functions to manage data traffic from the Server to Admin or User and vice versa through the Internet network. The server is the center of the system with activities including: database storage, provider of User Interface Graphs, giving the action command to the node controller. IP Cam serves to perform live monitoring of the conditions of the laboratory, and record it in videos stored on the server, admin can see the condition of the laboratory live through a GUI that can be opened in electronic gadgets outside laboratory whenever and wherever, via Internet, Indoor Sound System can be used as an audio tool when conducting a teleconference can also be used by the admin to convey appeals or information to laboratory visitors, and appeal can be carried out remotely from outside the laboratory via gadget connected to the Internet.
5. Block diagram system

Work details of the proposed System are shown in Figure 2. The Node Controller controls the actuators that is DC motor and Solenoid DC that are connected to the GPIO Pin through a power gain module, controlling of actuator is done digitally by issuing logic 1 or 0 to the GPIO to turn on and turn off the actuator, Sensor input, Limit Switch and Proximity Sensors send digital signals 1 or 0 directly to Node Controller via the GPIO pin which states the position of the Controlled Device, the input signal is read and processed by the Node Controller to determine the action, different from actuator and sensor components, Components in access identifier are RFID Reader and Biometrics Sensor use the communication protocol in its Digital communication with Node Controller, therefore a special pin, Serial Communication Pin (UART) is used which consists of Pin RXD and TXD for access identifier that uses the UART communication protocol, whereas for Access Identifier is using Serial Peripheral Interface (SPI) communication protocols, special pin pins such as MISO, MOSI, SCK, and RST are used for Node Controllers to communicate.

Access Identifier transfers data read from the user in form of a unique RFID Card ID, and digital data from the scanning of biometric sign to the Node Controller then process data which is matched with the database contained on the server then decide whether the visitor / user has access rights or not to enter the laboratory.

Node Controller has been programmed to do all actions needed by system, using programming languages that are compatible with Arduino on the basis of languages C and C++. Node Controller is Embedded System which has a control base ESP8266 chip that already have features to communicate via Wi-Fi, technically it can be a WeMos module or NodeMCU. Node Controller communicates with the server to transfer the data and commands via wireless router where Node Controller has a unique Internet Protocol (IP) that can be recognized locally by the server or other device in a local network. Node Controller can access the database on the server, then server can give node controller commands
to take action. IP Camera components are connected to the server via wireless router, digital data from the IP camera visualization are stored on the hard disk server, both video recording and live video that show the real-time condition of laboratory. Indoor Sound System connects to the server computer through wired or wireless connection, server can directly access to the Indoor Sound System when they want to appeal or provide information to laboratory visitors.

Laboratory admin can perform action commands to Controlled Devices with services provided by web server engine found on server computer, through Graphics User Interface (GUI) on electronic gadget, Computers or tablets that are connected to internet. GUI provided by the server computer when accessed by the laboratory admin via gadget, allow admin to control the controlled device, see the condition of live streaming laboratories and make audio call announcement to laboratory visitors. For technical requirements, setting and troubleshooting, admin laboratory can directly control the server computer through remote desktop applications located on the server computer remotely via the internet.

6. Detail component
To form the proposed system, requires several components both hardware and software, table 1 shows the list of hardware utilization and its specifications, including controlled devices (actuators), sensors, microcontrollers, camera, and internet peripherals.

Table 1. Hardware requirements

| No | Hardware                  | Specification                                      |
|----|---------------------------|----------------------------------------------------|
| 1  | Motor                     | DC 12 V, Torque: 20 Kg.Cm                          |
| 2  | Solenoid Lock             | DC12V, 2A                                         |
| 3  | Limit Switch              | SPDT Roller Level ARM                              |
| 4  | Proximity Switch          | Photoelektric Difuse reflection                    |
| 5  | Node Controller           | NodeMCU/ WeMos D1                                  |
| 6  | Wireless Router           | 2.4 Ghz, 10/100 WAN LAN, IEEE 802.11n, IEEE 802.11g, IEEE 802.11b |
| 7  | RFID Reader               | 13.56 Mhz, USB Connection                          |
| 8  | IP Camera                 | 1280 effective Pixel, 30 fps                       |
| 9  | Sound System              | Surround, Bluetooth Support                        |
| 10 | Biometric Attendance Machine | Finger Print Scan, Face Scan, USB interface, DC supply, SDK |
| 11 | Internet Connection       | 2 Mbps                                             |

Table 2 shows the list of software utilization with its specifications, including software that works for website services, database provider, remote desktop to remote computer server, camera viewer software (option because it can be embedded directly on web pages), and software for programming microcontrollers.
Table 2. Software requirements

| No | Software           | Specification/Type |
|----|--------------------|--------------------|
| 1  | Web Server         | Apache             |
| 2  | Database           | MySQL              |
| 3  | Remote Desktop     | Team Viewer        |
| 4  | IP Cam Viewer      | iSpy               |
| 5  | µController IDE    | Arduino            |

7. Conclusions and further work
In this paper, a digital surveillance and laboratory access security system are proposed using the IoT concept that integrates several electronic components in an Internet network so that each other is connected and accessible anywhere at any time outside the laboratory. We have explained system work scenario, system architecture, system block diagram and detail of the components needed to make the system. We hope it can improve security and facilitate supervision in the laboratory, and can facilitate the work of administrators/Laboratory staff.

In the future we will try to design the proposed system and will implement it in our work environment at the Industrial Electronics Laboratory, Faculty of Technology and Vocational Education, Universitas Pendidikan Indonesia.

References
[1] Fushshilat I, Rahmat A, Somantri Y and Haritman E 2018 Laboratory management: digital laboratory information system (DLIS) concept IOP Conference Series: Materials Science and Engineering 434 012286
[2] Bermúdez-Ortega J, Besada-Portas E, López-Orozco J A and Jesús M 2017 A new open-source and smart-device accessible remote control laboratory 2017 4th Experiment@ International Conference (exp. at’17) 143-144 IEEE
[3] Poongothai M, Subramanian P M and Rajeswari A 2018 Design and implementation of IoT based smart laboratory 2018 5th International Conference on Industrial Engineering and Applications (ICIEA) 169-173 IEEE
[4] Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M and Ayyash M 2015 Internet of things: A survey on enabling technologies, protocols, and applications IEEE communications surveys & tutorials 17(4) 2347-2376
[5] Hadis M S, Palantei E, Ilham A A and Hendra A 2018 Design of smart lock system for doors with special features using bluetooth technology 2018 International Conference on Information and Communications Technology (ICOLACT) 396-400 IEEE
[6] Park Y T, Sthapit P and Pyun J Y 2009 Smart digital door lock for the home automation TENCON 2009-2009 IEEE Region 10 Conference 1-6 IEEE
[7] Rangkuti H A and Simatupang J W 2015 Security lock with DTMF polyphonic tone sensor 2015 International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology (ICACOMIT) 119-122 IEEE
[8] Ping W, Guichu W, Wenbin X, Jianguo L and Peng L 2010 Remote Monitoring Intelligent System Based on Fingerprint Door Lock 2010 International Conference on Intelligent Computation Technology and Automation 2 1012-1014 IEEE
[9] Sahani M, Nanda C, Sahu A K and Pattnaik B 2015 Web-based online embedded door access control and home security system based on face recognition 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015] 1-6 IEEE
[10] Raju N G, Vikas J, Appaji S V and Hanuman A S 2018 Smart Lock Controlled using Voice Call 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT) 97-103 IEEE